ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SIMULACIÓN Y ANÁLISIS DE MECANISMOS DE DEFENSA ANTE LOS ATAQUES DE DENEGACIÓN DE SERVICIOS (DoS) EN REDES DE ÁREA LOCAL CONVERGENTES

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

JORGE POLIVIO CHÁVEZ ZAPATA
jorge.chavez@redescorp.com

DIRECTOR: RODRIGO FABIÁN CHANCUSIG CHUQUILLA
rodrigch@panchonet.net

Quito, Octubre del 2011

DECLARACIÓN

Yo, Jorge Polivio Chávez Zapata, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Jorge Polivio Chávez Zapata

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Jorge Polivio Chávez Zapata, bajo mi supervisión.

_____

Ing. Rodrigo Chancusig

DIRECTOR DEL PROYECTO

DEDICATORIA

Dedico este trabajo a mis padres y hermanos.

A ellos.

AGRADECIMIENTOS

Especialmente agradezco a Dios, por darme la vida y aliento para nunca desistir, por darme la fortaleza y ayuda para levantarme en aquellos momentos difíciles. A mis padres, María del Carmen Zapata y Ángel Polivio Chávez, que con su apoyo, ánimos, amor y forma de afrontar la vida, sirvieron de ayuda y fueron ejemplo de valentía y responsabilidad para culminar uno de mis mas ansiados anhelos, a mis hermanos Henry (Zuco) y Shirley (Niko), por su ayuda, compañía, sonrisas y ánimos, a mis abuelitas, a la memoria de mi tía y a todas aquellas personas familiares, amigas y amigos que creyeron en mí y que de una u otra forma pusieron su granito de arena para poder lograr mi cometido.

Agradezco a Alberto Arévalo, querido amigo y ex estudiante de la Escuela Politécnica Nacional, que con sus consejos, ayuda y ánimos en aquellos momentos difíciles fueron también parte de éste logro.

Mi más profundo agradecimiento a mi director de Proyecto de Titulación, Ing. Rodrigo Chancusig, gran persona, ser humano y ejemplo de profesor que incondicionalmente me extendió su mano cuando lo necesitaba y ayudó en la realización de este proyecto.

A profesores que me brindaron sus conocimientos y en especial a aquellos que me brindaron su apoyo y a la Escuela Politécnica Nacional, prestigiosa universidad que hizo de mí tal profesional, que puede desenvolverse sin inconvenientes si la ocasión lo amerita.

Polo.

SIMULACIÓN Y ANÁLISIS DE MECANISMOS DE DEFENSA ANTE LOS ATAQUES DE DENEGACIÓN DE SERVICIOS (DoS) EN REDES DE ÁREA LOCAL CONVERGENTES

CONTENIDO

FIGURAS

TABLAS

RESUMEN

En el presente proyecto de titulación, se realiza una revisión a los ataques informáticos, en específico los de Denegación de Servicio y busca concientizar a administradores, supervisores o encargados del área informática a precautelar sus redes de datos, para en lo posible mitigar este tipo de amenazas y sus efectos negativos que causan en los sistemas.

Para brindar un mejor entendimiento en el área y en los temas que se vayan desarrollando, el proyecto está dividido en cuatro capítulos. Brevemente se comenta cada uno de ellos, y sus temas tratados.

El Capítulo 1, ofrece una introducción a las redes de datos, en el cual se revisan conceptos fundamentales de red, equipos de networking, intranets, seguridades, hacking, simulación y pruebas de intrusión. Pretende dar una idea breve y global de todos aquellos aspectos involucrados en una red de área local y del proyecto en particular.

El Capítulo 2, presenta la investigación en lo que refiere a ataques de Denegación de Servicio. Además, se realiza una breve revisión a los ataques DoS distribuidos, sus herramientas, detección y posibles mecanismos de defensa, para dar una visión más amplia y poder así, implementar redes más seguras y confiables que permitan en lo posible mitigar ataques DoS e incluso otro tipo de amenazas.

El Capítulo 3, muestra la parte experimental, donde se simulan varios ataques DoS, para conocer cómo se comporta un sistema dado ante este tipo de amenazas y como los demás servicios podrían ser afectados. En un escenario real con servicios de voz, datos y video que en primera instancia han sido ya implementados.

El capítulo 4, muestra de forma breve, las leyes y sanciones que actualmente rigen en el Ecuador en contra de los delitos informáticos y temas afines, así como los organismos encargados de aplicarlos.

PRESENTACIÓN

Los ataques de Denegación de Servicio difieren en su objetivo, forma y efecto a la mayoría de ataques que se efectúan contra sistemas informáticos y redes de comunicaciones, ya que su objetivo no reside en recuperar ni alterar datos, sino el de dañar la reputación del servicio e impedir el desarrollo normal del mismo.

Para visualizar cómo se comporta un sistema particular ante este tipo de amenazas, se implementó un escenario simple, con servicios de voz, datos y video, para posteriormente simular algunos de los principales ataques DoS.

Tras la simulación realizada, los ataques DoS por inundación TCP SYN, UDP, ICMP e INVITE lanzados desde un único computador a servicios específicos, no llegan a saturar el canal de comunicaciones, debido a las altas velocidades de transmisión. Sin embargo, uno o más servicios pueden verse afectados, ya sea por el agotamiento de sus recursos o por que dependen de otros.

En la actualidad, debido a la mejora de las comunicaciones, sistemas operativos, computadores y recursos. Para poder colapsar totalmente un sistema, se requieren de cientos e incluso miles de computadores que lancen el ataque de forma conjunta (ataque distribuido de denegación de servicio, DDoS), razón por la cual, éste tipo de ataques en una red de área local resultaría difícil de realizar. No obstante, como se observará posteriormente, aquellos equipos que no están bien provistos, como por ejemplo, equipos de hogar u oficina, pueden ser presa fácil desde una única fuente de ataque, pudiendo incluso comprometer a otros servicios que dependen de él.

En general, toda red de datos sin importar su ubicación y tamaño es vulnerable a cualquier tipo de amenaza ya sea física o informática. Conocer éstas amenazas, ayudará en gran medida a prevenirlas, por lo que la auditoría de una red de datos, realizar pruebas de intrusión y definir políticas de seguridad, son un factor fundamental en lo que refiere al correcto funcionamiento y disponibilidad de los servicios.

1. MARCO TEÓRICO

En este capítulo se realiza una revisión a las redes de datos, en específico, las redes TCP/IP; además, de forma breve se tratan temas relacionados al Hacking, la seguridad informática, tipos de simulación y tipos de test de intrusión. El conocimiento de estos temas servirán de soporte y ayuda a una mejor comprensión del presente proyecto de titulación. Si lo comentado no es del interés del lector, se puede obviar este capítulo e ingresar directamente al tema de *ataques de denegación de servicios (DoS)*, que corresponde a los capítulos dos y tres.

1.1 INTRODUCCIÓN A LAS REDES DE DATOS

En su nivel más elemental una red de computadoras, llamada también red de ordenadores o red informática, consiste en al menos dos equipos interconectados entre sí que permiten compartir información, recursos y servicios haciendo uso de técnicas, enlaces físicos o inalámbricos y programas informáticos.

Una red de datos tiene tres niveles que son: software de aplicaciones, software de red y hardware de red.

1.1.1 SOFTWARE DE APLICACIONES

Formado por programas informáticos que se comunican con los usuarios de la red permitiendo así compartir la información y los recursos. Por ejemplo: arquitecturas P2P[1] y cliente-servidor.

1.1.2 SOFTWARE DE RED

Consiste en programas informáticos que establecen protocolos o normas, para que los computadores puedan comunicarse entre sí.

[1] **P2P. -** Llamada también red punto a punto. Los computadores en red actúan en partes iguales, o pares, es decir, cada computador puede tomar la función de cliente o de servidor.

1.1.3 HARDWARE DE RED

Está formado por los componentes materiales que unen a las redes de computadoras de los cuales se destacan los medios de transmisión, que se encargan de transportar las señales emitidas por las computadoras y su adaptador de red, que permite acceder al medio físico, recibir unidades de información desde el software de red y transmitir instrucciones y peticiones a otras computadoras.

1.2 MODELO TCP/IP

El modelo TCP/IP fue creado por DARPA, una agencia del Departamento de Defensa de los Estados Unidos en la década de 1970, con el propósito de establecer una red que permita que los mensajes sean enrutados o reenrutados en más de una dirección. Los protocolos relacionados son gestionados por la Internet Engineering Task Force (IETF) y todas las especificaciones son publicadas como un set de Request For Comment (RFC)[2].

La estructura fundamental de la red TCP/IP es la de un sistema de conmutación de paquetes y sus protocolos son usados actualmente en la evolución de la red ARPANET denominada INTERNET la cual es una colección de distintas redes físicas interconectadas entre sí.

1.2.1 CAPAS DEL MODELO TCP/IP

TCP/IP está basado en un modelo de referencia de cuatro niveles o capas. Todos los protocolos que pertenecen al conjunto de protocolos TCP/IP se encuentran en los tres niveles superiores de este modelo.

---

[2] **RFC.-** Los Request for Comments , son una serie de notas de trabajo publicadas por el Internet Engineering Task Force (IETF) sobre investigación y desarrollo de Internet, cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet siendo explicados de forma detallada y teniendo un título y número único asignado. http://www.rfc-editor.org/RFCoverview.html#history

Las capas se encuentran jerarquizadas y cada una se construye sobre su predecesora. De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior; a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados.

Figura 1. 1 Capas Modelo TCP/IP

1.2.1.1 Capa Aplicación

Asimilable a las capas 5 (sesión), 6 (presentación) y 7 (aplicación) del modelo OSI[3], interactúa con la capa transporte entregando y recibiendo mensajes de ésta. Algunas de las aplicaciones más utilizadas son:

TELNET (Telecommunication Network), FTP (File Transfer Protocol), DNS (Domain Name System), SMTP (Simple Mail Transfer Protocol), NNTP (Network News Transport Protocol), HTTP (Hypertext Transfer Protocol), entre otros.

---

[3] El modelo de referencia OSI (Open System Interconnection), lanzado en 1984 por la ISO (International Standards Organization) , es un marco de referencia, un modelo conceptual que no define ni especifica interfaces y protocolos, únicamente establece criterios generales sobre cómo concebir las redes de datos.

1.2.1.2 Capa Transporte

Establece comunicación extremo a extremo entre procesos de capa aplicación en hosts distintos. Entre los protocolos de capa transporte se tienen:

TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

1.2.1.3 Capa de Red o Internet

Aísla las capas superiores de la tecnología de red utilizada debajo de ellas y es la responsable de proporcionar el paquete de datos (datagrama). Entre los protocolos de capa de red se tienen:

IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol).

1.2.1.4 Capa Interfaz de Red

Agrupa a la capa 1 (física) y 2 (enlace de datos) del modelo OSI[3], denominada también capa enlace o capa Host-red y es la encargada de establecer la verdadera interfaz con el hardware de red.

1.2.2 PROTOCOLO TCP (TRANSMISSION CONTROL PROTOCOL)

Es un protocolo de capa 4 según el modelo OSI, actualmente documentado por IETF en el RFC 793.

TCP es un protocolo orientado a conexión que garantiza una comunicación extremo a extremo añadiendo funciones necesarias para ser utilizada por procesos de capa aplicación que requieran confiabilidad, control de flujo, transferencia continúa del flujo de datos, circuitos virtuales, multiplexaje, comunicación full duplex.

1.2.2.1 Formato de un segmento TCP[4]

+	Bits 0 - 3	4 - 7	8 - 15	16 - 31
0	Puerto Origen			Puerto Destino
32	Número de Secuencia			
64	Número de Acuse de Recibo (ACK)			
96	longitud cabecera TCP	Reservado	Flags	Ventana
128	Suma de Verificación (Checksum)			Puntero Urgente
160	Opciones + Relleno (opcional)			
224	Datos			

Figura 1. 2 Formato de un Segmento TCP

Puerto de origen (16 bits): Puerto TCP del programa de aplicación origen.

Puerto destino (16 bits): Puerto TCP del programa de aplicación destino.

Número de secuencia (32 bits): Sirve para comprobar que ningún segmento se ha perdido, es utilizado por el destino para ubicar el segmento en su lugar adecuado dentro del flujo de datos enviado y su significado varía dependiendo del valor de SYN.

- Si el flag SYN está activo (1), indica el número inicial de secuencia utilizado para sincronizar los números de secuencia ISN (Initial sequence number).

- Si el flag SYN no está activo (0), el número de secuencia es el de la primera palabra del segmento actual, es decir, el número de secuencia del primer byte de datos.

Número de acuse de recibo (ACK) (32 bits): Si el flag ACK está puesto a activo, entonces en este campo contiene el número de secuencia del siguiente paquete que el receptor espera recibir.

Longitud de la cabecera TCP (4 bits): Especifica el tamaño de la cabecera TCP en unidades de 32-bits e indica cuántos bytes hay entre el inicio del paquete TCP y

[4] **RFC 793.-** Protocolo de Control de Transmisión, http://www.rfc-es.org/rfc/rfc0793-es.txt.

el inicio de los datos. El tamaño mínimo es de 20 bytes, y el máximo es de 60 bytes.

Reservado (4 bits): Reservado para uso futuro, deberían ser puestos a cero.

Bits de control (flags) (8 bits): Se tienen 8 flags o banderas. 2 fueron añadidas al campo reservado más las 6 anteriormente especificadas.

CWR o "Congestion Window Reduced" (1 bit): Este flag se activa (1) por parte del emisor para indicar que ha recibido un paquete TCP con el flag ECE activado. Se lo utiliza para el control de la congestión en la red, RFC 3168.[5]

ECE o Explicit Congestion Notification o "ECN-Echo" (1 bit): Indica que el receptor puede realizar notificaciones ECN. La activación de este flag se realiza durante la negociación en tres pasos para el establecimiento de la conexión. Este flag también fue añadido a la cabecera en el RFC 3168.[4]

URG o "urgent" (1 bit): Si está activo significa que el segmento lleva información urgente en el campo de datos.

ACK o "acknowledge" (1 bit): Si está activo, indica que el campo con el número de acuse de recibo es válido. Es usado junto con SYN y FIN.

PSH o "push" (1 bit): Indica que los datos de ese segmento y los datos que hayan sido almacenados anteriormente en el buffer del receptor deben ser transferidos a la aplicación receptora lo antes posible.

RST o "reset" (1 bit): Un valor 1 termina la comunicación de forma abrupta y unilateral.

SYN o "synchronize" (1 bit): Se usa para iniciar una conexión entre hosts o computadoras y sincronizar los números de secuencia.

[5] **RFC 3168.-** The Addition of Explicit Congestion Notification to IP, http://tools.ietf.org/html/rfc3168

FIN (1 bit): Se lo activa al no haber más datos para enviar por parte del emisor, el paquete que lo lleva activo es el último de una conexión.

Ventana (16 bits): Especifica el número de bytes que el receptor puede almacenar en sus buffers internos.

Suma de verificación (checksum) (16 bits): Es una suma de verificación utilizada para comprobar si hay errores en la pseudo cabecera TCP[6], cabecera y datos.
Puntero urgente (16 bits): Si el flag URG está activado, entonces indica el desplazamiento respecto al número de secuencia que indica el último byte de datos marcados como "urgentes".

Opciones (número de bits variable): La longitud total del campo ha de ser múltiplo de una palabra de 32 bits (si es menor, se ha de rellenar al múltiplo más cercano), y el campo que indica la longitud de la cabecera ha de estar ajustado de forma adecuada, utilizado para proporcionar una serie de opciones adicionales.

Datos (número de bits variable): Pueden ser datos de cualquier protocolo de nivel de aplicación. No forma parte de la cabecera, es la carga (payload) con los datos del paquete TCP.

Las conexiones TCP se componen de tres etapas que son:

1.2.2.2 Establecimiento de la Conexión

Para establecer la conexión entre 2 hosts, utiliza tres formas de control llamado negociación en tres pasos (3-way handshake). Una negociación en cuatro pasos (4-way handshake) es usada para la desconexión.

---

[6] **Pseudo Cabecera TCP.-** Es de 12 bytes y añadida para propósitos de cálculo de checksum de forma obligatoria. Incluye, la dirección IP origen y destino, 8 bits a "0", el campo de protocolo y la longitud del paquete.

Normalmente una de las entidades (Servidor) abre un socket en un determinado puerto TCP y se queda a la escucha para aceptar conexión de los clientes. Es común referirse a esto como passive open o apertura pasiva.

El lado cliente solicita a TCP abrir una conexión con un servidor en un puerto determinado y dirección IP. Es común referirse a esto como active open o apertura activa.

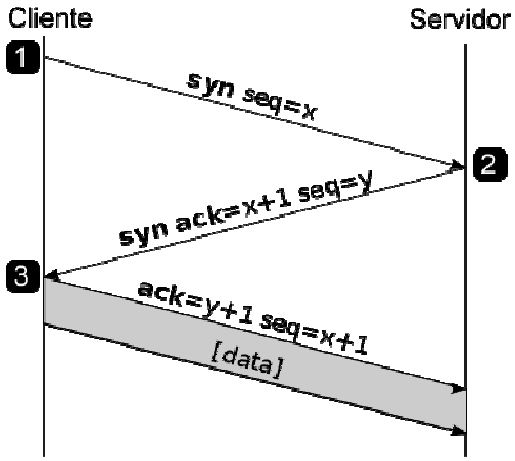


Figura 1. 3 Establecimiento de una Conexión TCP

1. El lado cliente realiza una apertura activa de un puerto enviando un segmento de sincronización SYN con un número inicial de secuencia (x). El tamaño de la ventana de recepción y el máximo tamaño del segmento de datos que puede recibir el cliente como parte de la negociación en tres pasos.

2. En el lado del servidor se comprueba si el puerto está abierto, en caso de no estarlo, se envía al cliente un paquete de respuesta con el bit RST activado, indicando el rechazo del intento de conexión.

En caso de que el puerto se encuentre abierto, el lado servidor responde a la petición SYN válida del cliente, con un segmento SYN, número inicial de secuencia (y), un ACK (x+1), el tamaño de su ventana de recepción y el tamaño de segmento de datos que puede recibir el servidor.

3. Finalmente, el cliente debería responder al servidor con un ACK(y+1), completando así la negociación en tres pasos (SYN, SYN/ACK y ACK) y la fase de establecimiento de la conexión.

De esta forma el cliente notifica que la conexión está abierta a su aplicación y de igual forma el servidor al recibir el ACK (y+1).

1.2.2.3 Envío de Datos

TCP divide el flujo de bytes provenientes de la aplicación en segmentos MTU (Unidad Máxima de Transferencia) de tamaño apropiado y le añade sus cabeceras para luego pasar el segmento resultante a la capa IP, donde a través de la red, llega a la capa TCP del destino.

Si en el caso de que el ACK no es recibido en un tiempo razonable, el paquete será retransmitido. TCP revisa que no haya errores durante el envío usando un checksum que consiste en el complemento a uno de la suma en complemento a uno del contenido de la pseudo-cabecera, cabecera y datos del segmento TCP. Éste es calculado por el emisor en cada paquete antes de ser enviado y comprobado por el receptor.

Al poder detectar paquetes duplicados y perdidos, errores en la transmisión y el uso de números de secuencia, acuses de recibo y temporizadores para detectar pérdidas y retrasos son los mecanismos clave que determinan la fiabilidad y robustez del protocolo.

TCP usa una serie de mecanismos para conseguir un alto rendimiento y evitar la congestión de la red haciendo uso de mecanismos como: El uso de ventana deslizante para controlar que el transmisor mande información dentro de los límites del *buffer* del receptor y algoritmos de control de flujo, tales como: el algoritmo de Evitación de la Congestión (*congestion avoidance*), el de comienzo lento (*Slow-start*), el de retransmisión rápida, el de recuperación rápida (*Fast Recovery*), y otros.

1.2.2.4 Cierre de la Conexión

Tanto el cliente como el servidor pueden iniciar el cierre de una conexión, haciendo uso de una negociación en cuatro pasos (4-way handshake).

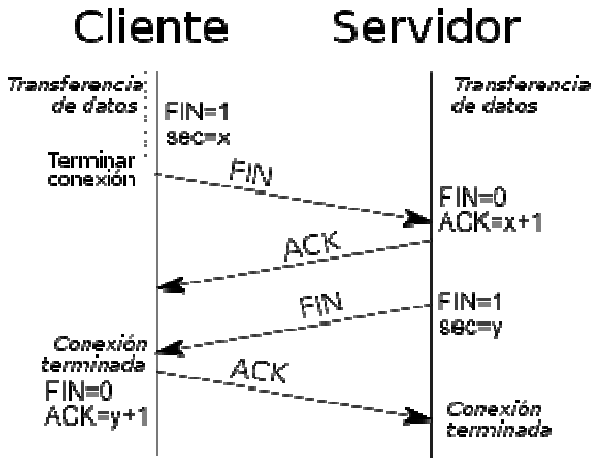


Figura 1. 4 Cierre de una Conexión TCP

1. Cliente o servidor envía un segmento TCP con: Direcciones de socket, número de secuencia correspondiente e indicador de final (FIN=1).

2. El servidor responde con un ACK del número de secuencia + 1 (los mensajes FIN consumen un número de secuencia). Envía un indicador de FIN=0 ya que solo responde a la petición para informar a la aplicación del cierre de la conexión.

3. Posteriormente el servidor envía un segmento TCP con: Direcciones de socket, número de secuencia correspondiente e indicador de final (FIN=1).

4. El cliente confirma la recepción del FIN, con un ACK del número de secuencia recibido + 1 y la conexión habrá finalizado.

Por tanto, una desconexión típica requiere un par de segmentos FIN y ACK desde cada lado de la conexión. El extremo que envía el primer FIN realiza el cierre activo y el otro extremo, el cierre pasivo; sin embargo, la conexión puede quedar media abierta, es decir, solo un extremo finaliza la conexión y el otro no. El lado

que ha dado por finalizada la conexión no puede enviar más datos pero la otra parte si podrá.

1.2.3 PROTOCOLO UDP (USER DATAGRAM PROTOCOL)

Es un protocolo de capa 4 según el modelo OSI actualmente documentado por la IETF en el RFC 768.

UDP es un protocolo no orientado a conexión, no confiable, basado en el intercambio de datagramas. Debido a que no se garantiza la correcta recepción de los mismos los datagramas enviados pueden perderse, duplicarse o llegar en desorden al destino, por lo que cualquier tipo de garantías para la transmisión de la información deberán ser implementadas por capas superiores.

1.2.3.1 Formato del Datagrama UDP[7]

+	Bits 0 - 15	16 - 31
0	Puerto origen	Puerto destino
32	Longitud del Mensaje	Suma de verificación
64	Datos	

Figura 1. 5 Formato de un Datagrama UDP

Puerto origen (16 bits): Puerto UDP del programa de aplicación origen, es opcional debido a que UDP carece de un servidor de estado y el origen UDP no solicita respuestas. En caso de no ser utilizado, debe ser puesto a cero.

Puerto destino (16 bits): Puerto UDP del programa de aplicación destino.

Longitud del Mensaje (16 bits): Campo obligatorio que indica la longitud total en bytes del datagrama UDP incluidos los datos. El valor mínimo es de 8 bytes.

[7] **RFC 768. -** Protocolo de Datagramas de Usuario, http://rfc-es.org/rfc/rfc0768-es.txt.

Suma de Verificación o Checksum (16 bits): Es una suma de verificación que abarca la cabecera, los datos y una pseudo cabecera UDP[8].

El Checksum puede ser opcional, aunque generalmente es utilizado en la práctica.

Datos (número de bits variable): Pueden ser datos de cualquier protocolo de nivel de aplicación. No forma parte de la cabecera, es la carga (payload) con los datos del paquete UDP.

El protocolo UDP se utiliza por ejemplo, cuando se necesita transmitir voz o vídeo, donde resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

1.2.4 PUERTOS TCP Y UDP[9]

En TCP/IP, son números lógicos que se asignan a las conexiones, tanto en el origen como en el destino para comunicarse con una aplicación específica.

Se usan 16 bits para identificar un número de puerto, teniendo un total de 65535 números de puerto posibles. Se puede usar cualquiera, sin embargo, IANA es la encargada de su asignación y establece tres categorías:

1. Los puertos inferiores al 1024 son puertos reservados[9] para el uso del sistema operativo y usado por "protocolos bien conocidos".

2. Los comprendidos entre 1024 y 49151 son denominados "registrados" y pueden ser usados por cualquier aplicación.

---

[8] **Pseudo Cabecera UDP.-** Es de 12 bytes y añadida para propósitos de cálculo de checksum de forma opcional. Incluye, la dirección IP origen y destino, 8 bits a “0”, el campo de protocolo y la longitud del paquete.

[9] IANA, Port Numbers, http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

3. Los comprendidos entre 49152 y 65535 son denominados dinámicos o privados.

1.2.5 PROTOCOLO IP (INTERNET PROTOCOL)

Es un protocolo de capa 3 según el modelo OSI actualmente documentado por IETF en el RFC 791. Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas y son la unidad básica de transferencia de datos en la capa Internet.

Es un protocolo no orientado a conexión, no confiable, llamado también del mejor esfuerzo o best effort, no provee de mecanismos para determinar si un paquete alcanza o no su destino, únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

IP es el elemento común en la Internet , el actual y más popular protocolo de red es IPv4 que utiliza direcciones de 32 bits. IPv6 es el sucesor de IPv4 debido al agotamiento de las direcciones disponibles y utiliza direcciones de 128 bits.

1.2.5.1 Formato del Datagrama IP[10]

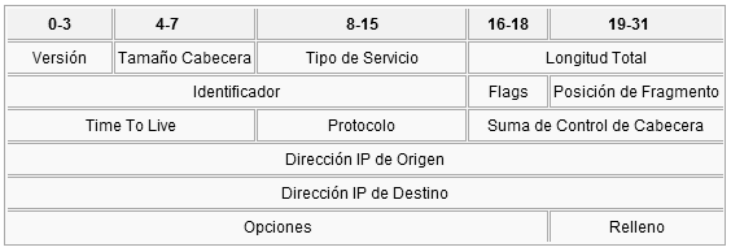


Figura 1. 6 Formato de un Datagrama IP

Versión (4 bits): Indica la versión del protocolo IP.

[10] **RFC 791.-** Protocolo Internet, http://rfc-es.org/rfc/rfc0791-es.txt

Longitud del encabezado o IHL (Internet Header Length) (4 bits): Define el tamaño de la cabecera en unidades de 32 bits, siendo el valor mínimo 5 bytes y máximo 60 bytes, por defecto la cabecera es de 20 bytes.

Tipo de servicio (8 bits): Indica como el datagrama debe ser procesado. Los 5 bits de menos peso son independientes e indican características del servicio:

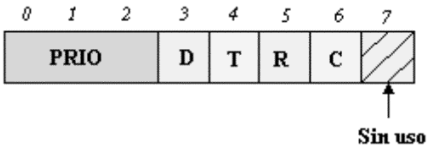


Figura 1. 7 Formato Campos Tipo de Servicio

Bit 7: sin uso, debe permanecer en 0.
C- Coste: 1 - Costo mínimo, 0 - Costo normal.
R- Confiabilidad (Reliability): 1 - Máxima fiabilidad, 0 - Fiabilidad normal.
T- Tasa de transferencia (Throughput): 1 - Máximo rendimiento, 0 - Rendimiento normal.
D- Retardo de transmisión (Delay): 1 - Mínimo retardo, 0 - Retardo normal.

La norma especifica que sólo se puede poner a 1 uno de los campos D, T, R y C. Con esto, el usuario decide a qué quiere dar prioridad para su mensaje.

PRIO (3 bits): Se utiliza en casos de congestión y están relacionados con la precedencia de los mensajes y un indicador que determina el nivel de urgencia basado en el sistema militar de precedencia (Message Precedence) de la CCEB (Combined Communications-Electronics Board).

000: De rutina.
001: Prioritario.
010: Inmediato.
011: Relámpago.
100: Invalidación relámpago.
101: Procesando llamada crítica y de emergencia.

110: Control de trabajo de Internet.
111: Control de red.

Longitud total (16 bits): Define el tamaño total del datagrama en bytes (cabecera y datos).

Identificador: Son campos que permiten la identificación de datagramas. Se usa en caso de que el datagrama deba ser fragmentado para poder distinguirlos, cada fragmento individual tendrá la misma identificación.

Flags (3 bits): utilizado para especificar valores relativos a la fragmentación.

Bit 0: Reservado; debe ser 0.
Bit 1 (DF): 0 puede ser fragmentado, 1 no puede ser fragmentado.
Bit 2 (MF): 0 = Último Fragmento, 1 = Mas fragmentos.

Posición de Fragmento (13 bits): Indica luego de cuantos bits viene el siguiente fragmento. El primer paquete de una serie de fragmentos contendrá en este campo el valor 0.

TTL o Tiempo de vida (8 bits): Indica el número máximo de saltos (Paso por Routers o enrutadores) por los que puede pasar un datagrama antes de ser descartado. Este campo disminuye con cada salto evitando así que la red se sobrecargue de datagramas perdidos.

Protocolo (8 bits): Este campo, en notación decimal, contiene el código numérico asignado por IANA de un protocolo de capa superior.

Suma de Control de Cabecera o Checksum (16 bits): Permite detectar errores únicamente en la cabecera no en los datos.

Dirección IP de origen (32 bits): Indica la dirección IP de la máquina origen.

Dirección IP de destino (32 bits): Indica la dirección IP de la máquina destino.

Opciones (Variable): Campo opcional. Puede contener opciones que permiten implementar pruebas y control de la red.

Relleno (Variable): Usado para asegurar que el tamaño, en bits, de la cabecera es un múltiplo de 32 bits. El valor usado es el 0.

Datos: Como se dijo anteriormente, el tamaño máximo de un datagrama es de 65536 bytes. Las redes en Internet utilizan diferentes tecnologías por lo tanto el tamaño máximo de un datagrama varía según el tipo de red.

Por tal razón se define el MTU (Maximun Transfer Unit) como el tamaño máximo de datos que se puede transferir. La fragmentación del datagrama se lleva a cabo a nivel de Router o Enrutador, es decir, durante la transición de una red con una MTU grande a una red con una MTU más pequeña.

1.2.6 PROTOCOLO ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

Es un protocolo de capa 3 según el modelo OSI, actualmente documentado por la IETF en el RFC 792. Debido a que IP es un protocolo no confiable, los datagramas pueden perderse o llegar defectuosos. ICMP se encarga de informar de las incidencias en la red enviando mensajes de error y de control. ICMP no toma decisión alguna al respecto, la responsabilidad queda a cargo de las capas superiores.

Los mensajes ICMP viajan en el campo de datos de un datagrama IP, por tanto, no se garantiza la entrega del mensaje ICMP. Si el mensaje se pierde o llega con error no se crea un nuevo mensaje ICMP, éste simplemente se descarta.

Mensajes ICMP de error no son generados para: datagramas que contienen mensajes ICMP de error, datagramas con direcciones multicast o especiales y para un datagrama fragmentado que no sea el primero.

Son dos aplicaciones las que utilizan directamente el protocolo ICMP como son Ping[11] y Traceroute[12]. La versión de ICMP para IPv4 es conocida como ICMPv4, IPv6 tiene su protocolo equivalente ICMPv6.

1.2.6.1 Formato de un Mensaje ICMP[13]

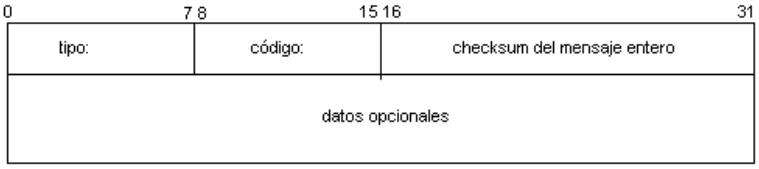


Figura 1. 8 Formato de un Mensaje ICMP

Tipo (8bits): Indica el tipo de mensajes ICMP y son definidos por la IANA ICMP Parameters[14].

Código (8bits): Refiere al código de error que provocó el mensaje ICMP y depende del tipo de mensaje ICMP. RFC 792.

Checksum (16 bits): Se lo utiliza para detectar errores en el mensaje completo ICMP.

Datos (Variable): En los mensajes de error se tiene la cabecera IP y los 8 primeros bytes del campo de datos incluyendo así los puertos TCP y UDP. En los

---

[11] **Ping.-** Permite conocer si un destino es accesible o no, enviando mensajes echo request y echo reply, muchas veces se lo utiliza también para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos.

[12] **Traceroute.-** Determina la ruta que sigue un datagrama desde el origen a un destino, utiliza el mensaje Time exceded, se calcula hasta un límite de 30 saltos (por default), más allá el destino se considera inalcanzable.

[13] **RFC 792.-** Protocolo de Mensajes de Control Internet, http://www.rfc-es.org/rfc/rfc0792-es.txt

[14] IANA, ICMP Parameters, http://www.iana.org/assignments/icmp-parameters

mensajes de consulta lleva información adicional dependiendo del tipo de pregunta.

1.3 COMPONENTES DE UNA RED DE DATOS

1.3.1 EL ORDENADOR O COMPUTADOR

También denominados host; generalmente son sitios de trabajo (incluyendo ordenadores personales).

1.3.2 TARJETAS DE RED O NIC (NETWORK INTERFACE CAR)

Se encargan de convertir las señales eléctricas o de radio frecuencia que viajan por un medio de transmisión en señales que puedan ser interpretadas por el ordenador.

Cada tarjeta de red tiene asignado un identificador único conocido como dirección MAC (Media Access Control), que consta de 48 bits. Dicho identificador permite direccionar el tráfico de datos de la red del emisor al receptor adecuado.

1.3.3 SERVIDORES

Son computadores o aplicaciones informáticas, que proveen servicios a otras computadoras denominadas clientes. Entre los tipos más comunes de servidores se tienen:

- Servidor de Archivos, encargados de almacenar distintos tipos de archivo y permitir distribuirlos a otros clientes en la red.

- Servidor de Impresión, controlan una o más impresoras aceptando trabajos de impresión de otros clientes de la red.

- Servidor de Correo, en forma general se encarga del almacenamiento, envío, recepción y enrutamiento de los correos electrónicos (e-mail) para los clientes de la red.

- Servidor de Telefonía, realizan funciones relacionadas con transmisiones de voz.

- Servidor Proxy, el término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro, es decir, es un intermediario. Cuando un equipo de la red desea acceder a una información o recurso, el servidor proxy realiza la comunicación y entrega el resultado al equipo debido a que en unos casos no es posible la comunicación directa y en otros porque el proxy añade una funcionalidad adicional.

- Servidor de Acceso Remoto (RAS), un servidor RAS controla las líneas de módem u otros canales de comunicación de la red, para que las peticiones conecten con la red de una posición remota.

- Servidor Web, almacena documentos HTML (HyperText Markup Language), imágenes, archivos y demás material Web para ser distribuido a clientes que lo soliciten en la red.

- Servidor de Autenticación, encargado de verificar que un usuario pueda conectarse a la red.

- Servidor de Base de Datos, es definido por el modelo cliente-servidor y provee servicios de base de datos a otros programas u otras computadoras.

- Servidor de Resolución de Nombres de Dominio (DNS), este tipo de servidores resuelven nombres de dominio sin necesidad de conocer su dirección IP.

1.3.4 IMPRESORAS

En la actualidad, las impresoras son capaces de actuar como un elemento más de la red, sin necesidad de un dispositivo intermediario como un "servidor de impresión o print server".

1.3.5 REPETIDOR

Dispositivo de capa física que se encarga de regenerar y amplificar señales eléctricas u ópticas. Son utilizados para superar las distancias limitadas por la atenuación del medio.

1.3.6 PUENTE O BRIDGE

Opera en la capa física y de enlace de datos, puede dividir una red muy grande en segmentos más pequeños o puede unir dos redes separadas.
Realiza filtraje para controlar el tráfico, regenera la señal, segmenta dominios de colisión e interconecta redes LAN similares (Ethernet-Ethernet), de diferente velocidad (Ethernet-FastEthernet) o redes diferentes (Ethernet-TokenRing).

Dado que el bridging ocurre a nivel de enlace, se lleva a cabo: control de flujo de datos, manejos de errores, direccionamiento físico y el manejo de acceso al medio.

1.3.7 SWITCH O CONMUTADOR

Es un tipo de bridge o puente mejorado, es decir, más inteligente. Son usados para interconectar dos o más segmentos utilizando el direccionamiento MAC. La conmutación de paquetes es más rápida que en un bridge o puente ya que son basados en hardware.

Debido a que cada puerto de un Switch forma parte de un solo dominio de colisión, permiten preservar el ancho de banda en la red al utilizar la

segmentación, cada puerto aprende dinámicamente las direcciones MAC de los equipos que le son conectados y es capaz de aprender varias direcciones por puerto, de esta forma distribuye los paquetes a los puertos destino. Posibilitan múltiples transmisiones simultáneas sin interferir en otras sub-redes.

Según el método de direccionamiento de las tramas los Switchs se clasifican en:

- Store and Forward, cada trama es almacenada en un buffer. Mientras la trama está en el buffer, se verifica la integridad y validez de ésta. Si la trama está libre de errores se hace la conmutación a la dirección de destino, caso contrario se la descarta. Este método asegura operaciones sin errores, pero la desventaja es que la latencia se incrementa con el tamaño del paquete.

- Cut Through, fueron diseñados para reducir la latencia. Estos Switches leen sólo los 6 primeros bytes de datos de la trama, que contiene la dirección de destino MAC, e inmediatamente se lleva a cabo la conmutación y la trama se envía por el puerto destino. No se verifica la integridad de la trama.

- Fragment Free, lee los primeros 64 bytes de cada trama, asegurando que tenga por lo menos el tamaño mínimo y que no se propaguen fragmentos a través de la red. Su latencia es mayor que Cut-Through.

- Adaptive Cut Through, son switches que soportan tanto store and forward como cut through. Estos pueden ser activados por el administrador de la red o el Switch inteligentemente puede escoger entre los dos métodos, basado en el número de tramas con error que pasan por los puertos.

Según la forma de segmentación de las sub-redes los Switches se clasifican en:

- De Capa 2 o Layer 2 Switches

- De Capa 3 o Layer 3 Switches, además de las funciones tradicionales de capa 2, incorporan funciones de capa 3. Entre sus principales características realizan tareas de ruteo, soportan la definición de redes virtuales (VLAN's) y algunos posibilitan la comunicación entre VLAN's sin necesidad de utilizar un router externo.

- De Capa 4 o Layer 4 Switches, incorporan a las funcionalidades de un Switch de capa 3 la habilidad de implementar políticas y filtros a partir de informaciones de capa 4.

1.3.8 ROUTERS O RUTEADORES

Es un dispositivo que opera a nivel de capa 3 (Red). Su principal función es la de pasar la información de una red a otra permitiendo así conectar redes LAN como redes WAN e incluso redes distintas enviando datagramas provenientes de un interfaz de red hacia otro interfaz, soporta rutas redundantes y segmentan la red en dominios individuales de broadcast.

La ruta o camino óptimo hacia otras redes es escogida de una tabla de rutas o tabla de enrutamiento la cual contiene información que describe el próximo hop (salto) que deberá tomar el datagrama IP para llegar a su destino, éstas tablas son almacenadas en una base de datos dentro del Router y son creadas con la ayuda de protocolos de enrutamiento.

Los Routers pueden ser de 2 tipos:

- Estáticos, no determinan rutas por lo que se debe configurar la tabla de enrutamiento, especificando las rutas para los paquetes.

- Dinámicos, tienen la capacidad de determinar la ruta más óptima basada en la información de los paquetes y en la información de otros Routers.

1.3.9 FIREWALL O CORTA FUEGOS

Pueden ser implementados en hardware o software y se los utiliza como mecanismo de protección de la red permitiendo así dar acceso solo a conexiones permitidas y bloquear las no deseadas. Son transparentes para los usuarios conectados a la red.

1.3.9.1 Tipos de Firewalls

Las políticas de accesos en un Firewall deben ser diseñadas poniendo principal atención en sus limitaciones y capacidades ya que los firewalls normalmente sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior. De hecho, los Firewalls no tienen nada que hacer contra técnicas como la Ingeniería Social y el ataque de usuarios internos.

Los firewalls o cortafuegos más habituales son:

1.3.9.1.1 Packet Filter o Filtrado de Paquetes

Fue la primera tecnología de firewalls y trabajan a nivel de capa 3(Red). Se utilizan Routers con filtros y reglas basadas en políticas de control de acceso.

Consisten en filtrar cada paquete de forma independiente en base a: Dirección IP origen, Dirección IP destino, puerto fuente, puerto destino y protocolo, permitiendo y restringiendo las comunicaciones entre dos computadoras.

El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Este tipo de Firewalls al manejar cada paquete de forma aislada son incapaces de reconocer diversos tipos de ataques de denegación de servicio por inundación y por ende se los conoce como firewall Stateless.

1.3.9.1.2 Inspección de Paquetes

Es el firewall más utilizado y recomendado. Se basa en el principio de que cada paquete que circula por la red es inspeccionado, considerando su procedencia y destino. Cumple las mismas funciones que un packet filter.

Adicionalmente registra las conexiones que pasan a través de sí en una tabla, que chequea con cada entrada o salida de un paquete para determinar si lo permite o lo deniega, evitando así los tipos de ataques a los que un packet filter es vulnerable.

1.3.9.1.3 Proxy y Gateways de Aplicaciones

Es el firewall más completo que existe, aunque presenta el menor throughput, mayor procesamiento y el mayor costo. Se diferencia de los 2 anteriores en que adicionalmente tiene la capacidad de revisar hasta la capa 7 (aplicación) y la carga útil (payload) del paquete.

Es vital comprender en primera instancia el concepto de proxy, que es un intermediario entre el usuario y el servicio que se solicita.

El mismo concepto se aplica a la tecnología de firewalls, el proxy recibe y procesa el paquete como si estuviera destinado a él, así determina si el mismo es seguro o no, para dejarlo pasar a su destino verdadero, es decir, cuando un usuario desea un servicio, lo hace a través del Proxy.

1.3.9.1.4 Firewalls Personales

Son aplicaciones que se ejecutan y están disponibles para usuarios finales. Su objetivo es el de controlar el acceso a la red de aplicaciones instaladas y prevenir notablemente los ataques de programas dañinos que penetran en el sistema.

1.3.9.2 Topología de Firewalls

Cada implementación depende del tipo de organización y sus necesidades, por tanto no existe una topología única que garantice la seguridad de cualquier red. Básicamente se utilizan tres modelos diferentes pero se admiten diversas modificaciones de estos según las necesidades.

1.3.9.2.1 Dual-Homed Host

Está constituida como una computadora con dos tarjetas de red actuando como un Router entre dos redes diferentes, pero los paquetes IP no son enrutados de una red a la otra. La ventaja de estos sistemas es su sencillez, la desventaja es que sólo soportan servicios mediante proxy y no filtro de paquetes, debido a que el enrutamiento se encuentra deshabilitado.

Todo el intercambio de datos entre las redes se ha de realizar a través de servidores proxy.

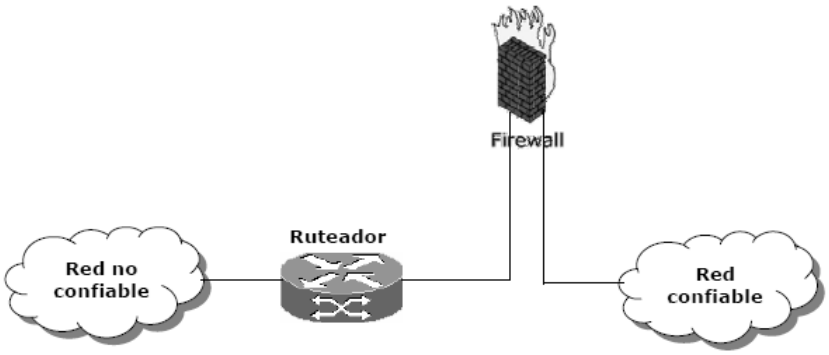


Figura 1. 9 Modelo Dual-Homed Host

1.3.9.2.2 Screened Host

Se usa un Router como primer nivel de seguridad. Éste permitirá filtrar paquetes y la conexión entre redes, configurado de forma que permita bloquear todo el tráfico entre la red externa y los hosts de la red interna excepto un único

denominado bastión, en el cual se instala todo el software necesario para la implementación del firewall.

Esta topología permite soportar servicios tanto de proxy (en el bastión) como de filtro de paquetes (en el router).

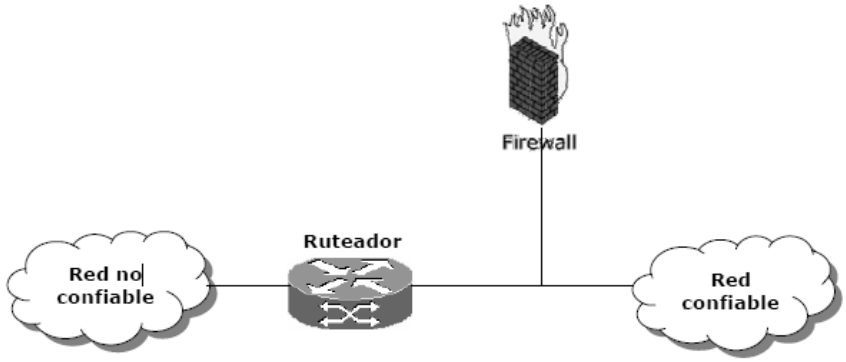


Figura 1. 10 Modelo Screened Host

1.3.9.2.3 Screened Subnet

En este modelo se intenta aislar la máquina vulnerable en el firewall y que podría ser atacada, de forma que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida.
Tanto los servidores públicos como la red interna son protegidos por un firewall. En los servidores públicos se establece una Zona Desmilitarizada (DMZ), que puede definirse como un área pública protegida ofreciendo servicios al interior y exterior de la red. La red interna se comunica con la DMZ mediante enrutamiento (no deberían compartir el mismo segmento de red por razones obvias de seguridad).

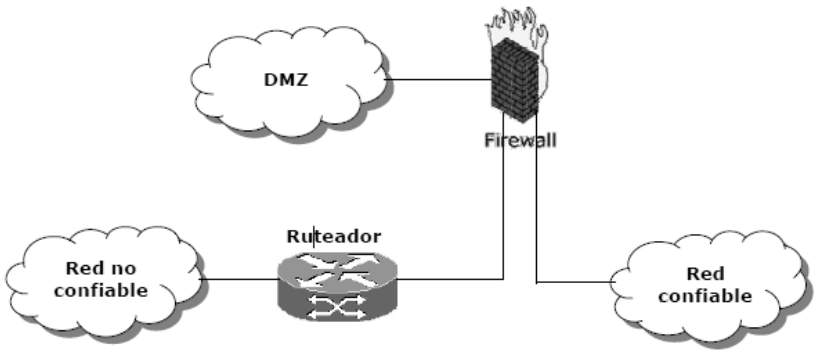


Figura 1. 11 Modelo Screened subnet

Es posible definir varios niveles de DMZ e incluso agregar más Routers para brindar mayor seguridad.

1.4 INTRODUCCIÓN AL HACKING ÉTICO

El crecimiento de Internet ha traído muchas ventajas. Pero al igual que avanzan las tecnologías también crece la inseguridad y evidentemente la seguridad afecta a todos: gobiernos, grandes compañías, bancos, empresas, instituciones, usuarios, entre otros. En el ANEXO 1 se definen algunos términos que servirán de apoyo al mejor entendimiento del tema que refiere a Hacking.

1.4.1 PERFIL DE UN HACKER

Un Hacker es alguien con profundos conocimientos, un experto (Gurú) en una o varias tecnologías relacionadas con la electrónica, informática o telecomunicaciones independientemente de la finalidad con que los usen.

Un verdadero Hacker es aquel que se interesa por la tecnología, alguien que tiene ansias por conocerlo todo, le gusta la investigación y los retos. Un Hacker busca primero el entendimiento del sistema y en segundo lugar busca el poder modificar la información para usos propios o de investigación y los conocimientos que adquiere son difundidos por él, para que otros lo sepan.

Los Ethical Hackers son profesionales de la seguridad, poseen grandes habilidades y deben ser completamente merecedores de confianza. Aplican sus conocimientos con fines defensivos y legales probando la seguridad de los sistemas y descubriendo así sus vulnerabilidades, para luego dar solución o informar de los peligros a los que se exponen y evitar así que delincuentes informáticos irrumpan en sus sistemas o se tenga perdida, robo o destrucción de la información.

Por el contrario un cracker (criminal hacker, 1985) es alguien que viola la seguridad de un sistema informático con fines de beneficio personal o para hacer daño a su objetivo.

Los Hackers son clasificados como:

- Black Hats o Hackers de Sombrero Negro, personas con extraordinarias habilidades y conocimientos informáticos, que realizan actividades maliciosas o destructivas, son conocidos como Crackers.

- White Hats o Hackers de Sombrero Blanco, personas que fomentan el hacking ético aplicando sus habilidades de hacker para fines defensivos, conocidos como analistas de seguridad.

- Gray Hats o Hackers de Sombrero Gris, personas de moral ambigua que trabajan de forma ofensiva y defensiva.

1.4.2 CATEGORÍAS DE ATAQUES O AMENAZAS

Las cuatro categorías generales de ataques o amenazas son:

- Interrupción, donde un recurso del sistema es destruido o se vuelve no disponible.

- Intercepción, una entidad no autorizada consigue acceso a un recurso.

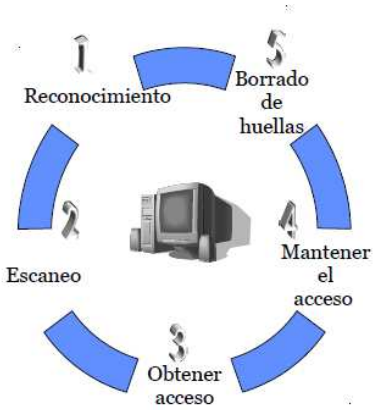
- Modificación, una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo.

- Fabricación, una entidad no autorizada inserta objetos falsificados en el sistema.

1.4.3 MODOS DE HACKING

Generalizando los hackers se basan en ciertos pasos o fases para poder alcanzar sus propósitos.

- Definición del Objetivo
- Reconocimiento
- Rastreo (*escaneo*)
- Acceso
- Mantener el acceso
- Borrado de huellas



1.4.3.1 Definición del Objetivo

Esta es la fase en la cual se define el objetivo a atacar; sea una red, un servidor, una aplicación cliente/servidor, una compañía, una organización, entre otros. En esta primera fase el hacker tiene el reto en su mente y visualiza su objetivo.

1.4.3.2 Reconocimiento

Es la fase previa al ataque donde se busca la forma de obtener la mayor cantidad de información posible del objetivo a atacar. Con o sin autorización, dependiendo del tipo de hacker, se hará uso de cualquier herramienta o medio posible para su propósito.

1.4.3.3 Rastreo o Escaneo

Esta es la fase de pre-ataque. Puede considerarse como la consecuencia lógica de la fase de reconocimiento.

Se detectan las vulnerabilidades y puntos de entrada, es decir, probar la red para detectar hosts accesibles, puertos abiertos, localizar dispositivos de interconexión, detalle de sistemas operativos, servicios, entre otros.

1.4.3.4 Acceso

Se refiere al ataque propiamente dicho y la penetración al sistema. En esta fase se explotan las vulnerabilidades que fueron encontradas en la fase anterior.

El ataque puede ser realizado localmente, offline (sin estar conectado) o sobre la Internet. Los factores para tener un acceso exitoso al sistema dependen de cómo es la arquitectura del sistema y de la seguridad del sistema objetivo o víctima.

1.4.3.5 Mantener el Acceso

Una vez que el Hacker haya ganado el acceso al sistema su prioridad será la de retener los privilegios obtenidos. En esta fase el Hacker incluso usa el sistema objetivo como plataforma de lanzamiento de ataques para escanear y atacar a otros sistemas.

1.4.3.6 Borrado de Huellas

En esta fase el Hacker trata de destruir toda evidencia de su acceso. Realizar lo mencionado le permitirá seguir manteniendo el acceso, no ser detectado y evadir cargos penales.

Existe un sin número de herramientas o aplicaciones que se pueden utilizar para llevar a cabo un ataque informático. En el ANEXO 2 se describen algunas de ellas, divididas según la fase que usa el hacker para alcanzar su propósito.

1.4.4 TIPOS DE ATAQUES

Un ataque no es más que la realización de una amenaza y pueden realizarse por diversos motivos. Los sistemas informáticos usan una diversidad de componentes y se los puede atacar siempre y cuando exista una vulnerabilidad que pueda aprovecharse. A los Ataques se los puede dividir en:

1.4.4.1 Ataques Pasivos

El atacante no altera la comunicación, únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración en los datos. Sin embargo, es posible evitarlos mediante el cifrado de la información y otros mecanismos.

1.4.4.2 Ataques Activos

Estos ataques implican algún tipo de modificación en el flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- Suplantación de identidad, el intruso se hace pasar por una entidad diferente.

- Re Actuación, uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado.

- Modificación de Mensajes, una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.

- Degradación del Servicio, impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Entre estos ataques se encuentran los de denegación de servicio o DoS (Denial of service) que consisten en paralizar temporalmente el servicio de un servidor.

1.5 SEGURIDAD

Las necesidades de seguridad de la información han ido evolucionando con la aparición de Internet. La seguridad de un sistema generalmente es "asimétrica" ya que el pirata informático debe encontrar sólo una vulnerabilidad para poner en peligro el sistema, mientras que el administrador debe corregir todas sus fallas.

Es erróneo pensar que una filosofía de seguridad tradicional, basada en passwords y protección de ficheros, es suficiente para protegerse en una red o Internet ya que la seguridad como tal implica a más de un elemento como son:

- Confidencialidad, tiene que ver con la ocultación de información o recursos.
- Autenticidad, es la identificación y garantía del origen de la información.
- Integridad, refiere a cambios no autorizados en los datos.
- Disponibilidad, posibilidad de hacer uso de la información y recursos deseados.

1.5.1 SEGURIDAD EN UNA RED DE DATOS

La seguridad es un tema que debe preocupar a cualquiera que tenga su red conectada a otra o a Internet y el proceso para diseñar un sistema de seguridad se hace imprescindible debido a la gran variedad de formas de ataque que existen en la actualidad. Por tanto, el conocimiento de éstos ayudaran a la prevención de los mismos y permitirán implementar distintos tipos de mecanismos de seguridad tanto físicos como informáticos para contrarrestarlos.

A continuación se comentará de forma general algunos tipos de seguridades informáticas que podrían ser implementadas en una red de datos o sistema.

1.5.1.1 Autenticación

La autenticación es el proceso en el cual una entidad se encarga de probar la identidad de otra.

La autenticación debe preceder a la autorización ya que la autenticación es el proceso de verificar la identidad de personas, programas y/o procesos, mientras que la autorización es el proceso de verificación para que una persona tenga la autoridad para realizar una cierta operación.

Para distinguir la autenticación de la autorización existen notaciones como son: A1 para la autenticación y A2 para la autorización o se suele usar los términos AuthN y AuthZ.

Los métodos de autenticación normalmente utilizan un protocolo de autenticación que se negocia durante el proceso de establecimiento de la conexión. Una entidad autenticada puede ser una persona que usa un computador, un computador por sí mismo o un programa del computador.

1.5.1.2 Encriptación

Es el proceso que permite proteger la información, codificándola o volviéndola ilegible a terceros mediante el uso de algoritmos de encriptación. Se tienen, básicamente, dos tipos de algoritmos que son: algoritmos de claves privadas o simétricas y algoritmos de claves públicas o asimétricas.

1.5.1.2.1 Algoritmos de clave privada

Se utiliza la misma clave o llave para cifrar y descifrar respectivamente la información. Son muy veloces, pero ambas deben intercambiar las claves o llaves para poder cifrar y descifrar sus mensajes lo que introduce un riesgo, ya que si la llave es interceptada, se pierde la confidencialidad de los mensajes transmitidos.

A estos se los conoce también como algoritmos de: llave secreta (secret key), llave privada (private key), una llave (one key) y única llave (single key).

A la criptografía simétrica pertenecen los cifradores de bloques, los cifradores de flujo y las funciones 'hash'.

a) Cifradores de Bloques: Operan en grupos de bits de longitud fija, llamados bloques. Cuando se realiza el cifrado se toma un bloque de *texto plano* como entrada y produce un bloque de igual tamaño de texto cifrado a la salida. Por el contrario en el descifrado se ingresan bloques de texto cifrado y se producen bloques de texto plano. Por ejemplo, los más conocidos son: DES (Data Encryption Standard) y TDES (Triple-DES).

b) Cifradores de Flujo: Para algunas aplicaciones el cifrado en bloques es inapropiada debido a que el flujo de datos se produce en tiempo real y en pequeños fragmentos. Los cifradores de flujo pueden realizar el cifrado incrementalmente, convirtiendo el texto plano en texto cifrado bit a bit. Por ejemplo, los más conocidos son: RC4 (Rivest Cipher 4, significado alternativo al de Ron's Code utilizado para RC2, RC5 y RC6.) y Seal.

c) Funciones 'hash': Los algoritmos hash son usados para firmas digitales, éstos toman como entrada un mensaje de n bits y dan como resultado una cantidad finita de bits llamados Message Digest. Cabe señalar que el Message Digest varía con la modificación de un solo bit del mensaje de entrada. Por ejemplo, los más conocidos son: MD5 (Message-Digest Algorithm 5), SHA-1 (Secure Hash Algorithm) y RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest).

1.5.1.2.2 Algoritmos de clave pública

Están formados por dos tipos de claves o llaves: una pública y otra privada. La clave o llave pública es utilizada para cifrar y es generalmente distribuida, mientras que la llave privada es utilizada para descifrar los mensajes cifrados con la llave pública. Es meramente imposible obtener una llave privada de una llave pública, haciendo imprescindible que la llave privada sea guardada de forma segura. . Por ejemplo los más conocidos son: RSA (*Rivest, Shamir y Adleman)*) y Diffie- Hellman,

1.5.1.3 Filtrado de Paquetes

Es utilizado para implementar diferentes políticas de seguridad con el objeto principal de evitar el acceso no autorizado mediante el análisis de distintos campos de los paquetes IP como: dirección IP origen, dirección IP destino, Puerto origen, Puerto destino, tipo de protocolo, entre otros. Adicionalmente, Permite reducir la carga en la red descartando paquetes errados broadcast, cuyo TTL ha llegado a cero.

El filtrado de paquetes es transparente para el usuario final, es decir, no requiere conocimientos ni cooperación por su parte. El Filtrado de paquetes se desarrolla a nivel de Capa 3 (red), razón por la cual, estas tareas son generalmente realizadas por un Router o un firewall de capa 3.

También se puede realizar filtrado de la información a nivel de capa 7 (Aplicación) permitiendo así adaptarse a las características propias de los protocolos de ese nivel. Por ejemplo, filtrar URL´s si se trata de tráfico HTTP. Un Firewall de capa 7 (Aplicación) suele denominarse proxy.

1.5.1.4 Antivirus

Herramientas que permiten prevenir, evitar, detectar y eliminar virus, programas malignos o código malintencionado en el sistema.

1.6 MODELADO Y SIMULACIÓN [15] [16]

Existen varias herramientas y documentos en la actualidad que permiten modelar y simular un ambiente de pruebas ante gran cantidad de ataques como por ejemplo, los de denegación de servicio (DoS).

---

[15] John Saunders, Ph.D, National Defense University, www.johnsaunders.com/papers/securitysimulation.htm

[16] David Cook, Computers Modeling and Simulation, Defense Software Engineering.

Sin embargo, no existe una herramienta explícita que permita realizar éste tipo de pruebas ya que los ambientes de simulación son estudiados e investigados en muchas áreas, razón por la cual, conocer el tipo de herramientas de modelado [17] y simulación[18] que se podrían utilizar, permitirá en lo posible construir y configurar redes más seguras y estables.

1.6.1 ESTADO DEL MODELADO Y SIMULACIÓN EN EL CAMPO DE LA SEGURIDAD INFORMÁTICA

Para realizar pruebas de seguridad informática, se tienen algunas herramientas especiales de simuladores de red. Para su mejor entendimiento se las puede dividir en cinco categorías que son:[19]

1.6.1.1 Guerra de Paquetes o Packet wars

Este tipo de simulación involucra un nivel táctico de ataque/defensa y ha sido puesto a prueba de modo real, haciendo uso de redes con servidores, clientes, equipos de conmutación y enrutamiento.

Probablemente el mejor ejemplo de un laboratorio académico que hace uso de éste tipo de simulación, existe en la Academia Militar de los Estados Unidos (USMA) en West Point, Nueva York, llamada Laboratorio de Guerra de Información de Análisis e Investigación (IWAR).[20]

---

[17] **Modelado.-** Un modelo es una representación matemática, lógica o física simplificada de un sistema real, que tiene por objeto promover el entendimiento.

[18] **Simulación.-** La simulación es la manipulación de un modelo, que representa el comportamiento del sistema.

[19] John H. Saunders. (2002). "Simulation Approaches in Information Security Education" in Proc. 6th National Colloquium for Information System Security Education, Redmond, WA, 2002. At URL: http://cisse.info/CISSE%20J/2002/saun.pdf

[20] Shafer, J, et al. The IWAR Range : A Laboratory for Undergraduate Information Assurance Education. Unpublished paper. Contact dd9182@usma.edu. 2000.

La USMA ha usado su laboratorio para cursos de nivel superior y así poder educar a sus estudiantes en la ciencia y el arte de la seguridad informática.

En el verano del 2001 trabajaron junto con la facultad de la academia de la Fuerza Aérea de los Estados Unidos y la academia de guardia costera para iniciar una competencia anual. Como parte de la competencia los estudiantes pasan un semestre aprendiendo sobre ataques y defensas, para finalmente participar en el intento de atacar los puntos débiles en los sistemas de sus opositores.

Otro ejemplo de éste tipo de simulaciones y competiciones son las realizadas por la SAN´s llamadas ID'ed Net[21], realizada cada año en DEFCONy Rootwars en Toorcon[22].

Estas competencias son probablemente la mejor forma posible de simulación de ataques de red y defensa a nivel de seguridad informática que existen hoy en día.

1.6.1.2 Herramientas de diseño de red o Network Design Tools

En el análisis de seguridad informática, se tienen paquetes de modelado y simulación de redes (NMS) que permiten tener un entendimiento detallado de como un sistema puede comportarse ante diferentes circunstancias.

Estos paquetes NMS continúan creciendo en popularidad y madurez, proporcionando información detallada, interesante y valiosa en el análisis estadístico del tráfico de red, pudiendo ser utilizados para una variedad de tareas como: Diseño de redes a gran escala, permitir la creación de escenarios hipotéticos y tareas relacionadas con la seguridad de redes. Algunos paquetes NMS son:

---

[21] Wargames Lecture Series. September, 2001. http://www.incidents.org/Iowargames/soon.htm

[22] Toorcon Conference. http://www.toorcon.org/. 2001.

La Tabla 1.1 hace referencia a algunos ejemplos de herramientas de diseño de red.

Nombre	Compañía	Contacto
Cnet	Univ Western Australia	www.cs.uwa.edu.au/cnet/
EcoPredictor	Compuware	http://www.compuware.com/
IT DecisionGuru	Opnet Technologies	http://www.mil3.com/
NetCracker	NetCracker Technology	http://www.netcracker.com/
NetRule	Analytical Engines	http://www.analyticalengines.com/

Tabla 1 .1 Programas para simulación de redes

1.6.1.3 Escenarios de Ataque/Defesa

Estas simulaciones son típicamente aplicaciones independientes que pueden ser utilizados como forma de juego para facilitar el aprendizaje.

Estos paquetes son construidos usando herramientas multimedia cómo Macromedia Authorware o Microsoft Visual Basic, para poder ser distribuidas de forma fácil.

Algunos ejemplos de éste tipo de simulaciones pueden ser: InfoChess[23], CyberProtect[24] y the Information Security War gaming System[25].

[23] **InfoChess.-** Se centra en Operaciones de información militar. Unas pocas reglas especializadas son añadidas al juego usual de Chess para simular algunas características de operaciones de información como: Operaciones psicológicas, engaño militar, operaciones de seguridad, guerras en telecomunicaciones y destrucción física, soportados mutuamente por inteligencia para denegar la información, degradar o destruir capacidades de comando y control de los adversarios.

[24] **CyberProtect.-** Fue construida bajo contrato por la Defense Information Systems Agency y gira en torno a la compra (Entrenamiento y recursos de información de seguridad para ser aplicados a la red) y aplicación de medidas de seguridad de información en un entorno de red de área local.

[25] **The Information Security War Gaming System (ISWGS).-** Es un tipo de tutorial de simulación que proporciona un enfoque más profundo sobre tipos específicos de ataques y defens. Los ataques se representan gráficamente usando un paquete multimedia usando flujo de paquetes que se muestran junta a los objetivos específicos y defensas

1.6.1.4 Management Flight Simulators (MFS)

Estas aplicaciones son construidas utilizando un Sistema Dinámico o una herramienta de simulación de eventos discretos.

- **Sistemas Dinámicos:** Utilizan ecuaciones diferenciales para simular el estado de cambio de las cantidades y los flujos a través de varios períodos de tiempo[26].

- **Simulación de eventos discretos:** Utiliza colas para controlar el flujo de elementos a través de un sistema[27].

Son diseñados para ayudar a gerentes de proyecto o directores de programas para entender de mejor forma la interacción de los elementos, ya sean personas, equipos, o dinero a lo largo del ciclo de vida de un sistema.

Un ejemplo de modelo de política de seguridad integrada, fue construido por Graham Winch y Stephen Sturges de la Universidad de Plymouth en Inglaterra[28] y la característica sobresaliente de este modelo y enfoque, es la habilidad de combinar fácilmente muchos elementos aparentemente dispares en un solo modelo.

El propósito de este modelo de seguridad fue ver el impacto global de un ataque de fraude informático en el flujo y reconstrucción de datos en una organización, así como sus efectos subsecuentes sobre el personal, clientes y finanzas.

---

[26] Saunders, John. System Dynamics Basics. Info Tech Talk. Spring 1997. http://www.johnsaunders.com/papers/sysdyn.htm

[27] Law Averill M. and Kelton W. David. Simulation Modeling and Analysis. Third Edition. McGraw-Hill, 2000

[28] Sturges, Stephen and Winch, Graham. Computer Attack: The Role of Modeling in Developing an Integrated Security Policy. Proceedings of the International System Dynamics Conference, Cambridge, MA. 1966.

En la construcción de un MFS, tanto la interfaz de usuario como el motor de simulación, son construidos arrastrando y soltando símbolos con comportamientos ya definidos en función del escenario a simular. Una vez construidas las simulaciones, éstas pueden ser reproducidas utilizando diferentes variables de entrada. El modelo de política de seguridad, permite a los administradores jugar con diferentes roles en la asignación de diferentes porcentajes a la seguridad para luego lanzar posibles ataques.

Una ventaja significativa de éste tipo de aplicaciones es la habilidad de incluso cambiar el modelo sobre la marcha y han sido aplicados en muchas áreas como por ejemplo, en el campo de la tecnología de la información, como el Information Technology Organization Flight Simulator que fue construido por el profesor Margaret Johnson de la Universidad de Stanford después del trabajo de Tarek Abdel-Hamid[29]. Éste simulador permite a grupos jugar con diferentes roles en un proyecto basado en la producción de código informático.

Otro simulador interesante es el Synthetic Environments for Advanced Simulations (SEAS), el cual fue desarrollado en Purdue y ha sido utilizado para juegos cibernéticos de ataques terroristas y otros incidentes de software malicioso[30].

1.6.1.5 Role Playing

Role Playing, no utiliza simulaciones basadas en computador, están orientadas a un escenario cara a cara. Su objetivo es obtener una mejor comprensión de las funciones en las diferentes organizaciones y el personal en la defensa de los ataques a gran escala.

Los ejemplos incluyen The Day After in Cyberspace II[31], la guerra cibernética en CSI 27[32], y Dark Winter[33] .

---

[29] Abdel-Hamed, Tarek, and Madnick, Stuart. Software Project Dynamics: An Integrated Approach. Prentice Hall. 1991.

[30] Chaturvedi, Alok and Mehta, Shailendra. Avoiding A "Electronic" Maginot Line: Simulating Information Security Issues for On-Line Banks. CERIAS. Purdue University Research. 1999

Éste tipo de simulaciones requieren de conocimientos precisos y una planificación cuidadosa para empaquetar una simulación que represente el funcionamiento de las relaciones complejas, ya sea dentro o entre las organizaciones que puedan estar involucradas en un ataque cibernético y defensa.

1.7 TESTS DE INTRUSIÓN [34] [35]

Un test de intrusión o prueba de penetración es un paso previo a todo análisis en sistemas de seguridad o riesgos para una organización. A diferencia de un análisis de vulnerabilidades, se enfoca en la comprobación y clasificación de las mismas y no en el impacto que estas tienen sobre la organización.

1.7.1 TIPOS DE TESTS DE INTRUSIÓN

El resultado de este tipo de pruebas brinda a la organización un documento con una lista detallada de las vulnerabilidades encontradas y recomendaciones a aplicar. Generalmente un test de intrusión se rige por las siguientes fases:

1. Recopilación de información
2. Enumeración de la red
3. Exploración de los sistemas
4. Extracción de información
5. Acceso no autorizado a información sensible
6. Auditoría de las aplicaciones web

---

[31] Anderson, Robert H and Hearn, Anthony C. An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After in Cyberspace II." Rand Corporation Report MR-797-DARPA. 1997.

[32] Bliss, Ron. Cyber -War. 27th Computer Security Institute Conference. 2000.

[33] Roberts, Roxanne. "A War Game to Send Chills Down the Spine." The Washington Post. October 23, 2001

[34] http://www.seguridad.unam.mx/doc/?ap=rss&id=218

[35] http://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias2.shtml

7. Elaboración de informes
8. Comprobación del proceso de parcheado de los sistemas
9. Informe final

Entre algunas de las metodologías existentes para poder realizar un test de intrusión se tienen:

1.7.1.1 Osstmm [36]

El manual de la metodología Open Source para test de intrusión (OSSTMM), representa un estándar de referencia, que permite realizar un test de seguridad en forma ordenada, ya que se divide en varias secciones y es posible identificar, una serie de módulos de test específicos.

Se pueden observar cada una de las dimensiones de seguridad, integradas con las tareas a llevar a cabo en los diferentes puntos de revisión que son:

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las Tecnologías de Internet
- Seguridad en las Comunicaciones
- Seguridad Inalámbrica
- Seguridad Física

OSSTMM no solo se enfoca en los ámbitos técnicos y de operación de seguridad, también se encarga de normar aspectos tales como:

- Las credenciales del profesional a cargo del test.
- La forma en la que el test debe ser comercializado.
- La forma en la que los resultados del mismo deben ser presentados.

---

[36] http://www.osstmm.org/

- Las normas éticas y legales que deben ser tenidas en cuenta al momento de concretar el test.
- Los tiempos que deberían ser tenidos en cuenta para cada una de las tareas.
- Incorpora el concepto de RAVs (Valores de Evaluación de Riesgo) y con ellos la frecuencia con la cual la prueba debe ser ejecutada.

Lo más importante en esta metodología es que los diferentes test son evaluados y ejecutados donde sean aplicables, hasta arribar a los resultados esperados dentro de un periodo de tiempo determinado. Y su utilización está determinada por el informe de cada tarea aun cuando no fueran aplicables en el informe final, adicionalmente menciona que todos los reportes finales que incluyan esta información y las listas de comprobación asociadas y apropiadas pueden incluir un sello[37] y la siguiente declaración:

“Este test ha sido ejecutado en conformidad con el OSSTMM disponible en http://www.osstmm.org y mediante este sello se afirma que está dentro de las mejores prácticas de testeo de seguridad”.

Según las reglas que definen los lineamientos éticos para un test de intrusión OSSTMM con respecto a pruebas de ataques de denegación de servicio, en lo que refiere a los test menciona que:

- “Negación del servicio Distribuida (DDOS) por internet está prohibida”.
- “Cualquier forma de pruebas por inundación, donde una persona, red, sistema o servicio sea saturado desde una amplia y fuerte fuente, está prohibido”.
- “Notificaciones al cliente son requeridas cuando el analista cambie el plan de trabajo, cambie el origen de los análisis, obtenga resultados de alto riego, con antelación a la ejecución de nuevos análisis de alto riesgo y alta

[37] Sello de OSSTMM, http://www.isecom.org/stamps.htm

generación de tráfico, y en caso que hayan ocurrido problemas en el análisis".

1.7.1.2 Issaf (Information Systems Security Assassment Framework) [38]

Se basa en un framework, que detalla las prácticas y conceptos relacionados con todas y cada una de las tareas a realizar en un test de seguridad.

La información del ISSAF, se encuentra organizada por los denominados Criterios de Evaluación, que se componen de los siguientes elementos:

- Una descripción del criterio de evaluación.
- Puntos y Objetivos a cubrir.
- Los pre-requisitos para conducir la evaluación.
- El proceso mismo de evaluación.
- El informe de los resultados esperados.
- Las contramedidas y recomendaciones.
- Referencias y Documentación Externa.

A su vez, los Criterios de Evaluación, se encuentran contenidos dentro de diferentes dominios entre los que es posible encontrar; desde los aspectos más generales, conceptos básicos de la "Administración de Proyectos de Test de Seguridad" hasta técnicas como: la ejecución de pruebas de Inyección de Código SQL o estrategias de cracking de contraseñas.

Una desventaja del framework es que si no se mantiene actualizado, muchas de sus partes pueden volverse obsoletas rápidamente, específicamente las que involucran técnicas directas de testeo sobre determinado producto o tecnología. Sin embargo, más que ser visto como una desventaja, sería un punto a tener en cuenta a la hora de su utilización.

[38] http://www.oissg.org/wiki/index.php?title=ISAAF-PENETRATION_TESTING_FRAMEWORK

1.7.1.3 OTP (OWASP Testing Project) [39]

Promete ser uno de los proyectos más destacados en lo que refiere a test de aplicaciones web. La metodología consta de 2 partes.

En la primera se abarcan los siguientes puntos:

- Principios del testeo
- Explicación de las técnicas de testeo.
- Explicación general acerca del framework de testeo de OWASP.

En la segunda parte, se planifican todas las técnicas necesarias para testear cada paso del ciclo de vida del desarrollo de software.

Otros tipos de test de intrusión como el Penetration Testing Framework de Vulnerability Assessment[40], además de mostrar una metodología a seguir, sugiere herramientas para realizar cada una de sus etapas.

[39] http://www.owasp.org/index.php/Category:OWASP_Testing_Project

[40] http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

2. DENEGACIÓN DE SERVICIO (DoS)

En términos de seguridad informática, un ataque de denegación de servicio (DoS, Denial of Service) es un tipo de ataque de interrupción que tiene como objeto dejar un servicio o recurso inoperativo para que usuarios legítimos no puedan utilizarlos, es decir, son ataques contra la disponibilidad de un servicio, impidiendo el uso normal de los sistemas o de las comunicaciones.

La mayoría de los ataques de denegación de servicio aprovechan las vulnerabilidades relacionadas con la implementación de un protocolo TCP/IP, y pueden dirigirse a equipos Windows (95, 98, NT, 2000, XP, etc.), Linux (Debian, Mandrake, RedHat, Suse, etc.), Commercial Unix (HP-UX, AIX, IRIX, Solaris, etc.) o cualquier otro sistema operativo.

Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio (DDoS, Distributed Denial of Service) el cual es un tipo especial de ataque DoS coordinado y de manera conjunta entre varios equipos.

Los tipos de ataques DoS han ido evolucionando con el tiempo y los más representativos han sido comentados en el ANEXO 3 para ayudar a comprenderlos de mejor forma y así poder visualizar sus tendencias futuras.

2.2 ORIGEN DE LOS ATAQUES DOS / DDOS

La posibilidad de controlar efectivamente los recursos y/o servicios de un sistema ante un ataque de denegación de servicio se complica, debido a que éstos pueden tener varios orígenes, como son:

2.2.1 USUARIOS LEGÍTIMOS

Son aquellos usuarios poco cuidadosos que colapsan el sistema o servicio inconscientemente. Por ejemplo: saturar el disco duro con archivos e información

innecesaria como música, videos, fotos, entre otros.

2.2.2 USUARIOS MALINTENCIONADOS

Son usuarios que aprovechan su acceso o roban el acceso de un usuario legítimo, para causar problemas de forma premeditada o con propósitos ilegales e inmorales.

2.2.3 AGENTES EXTERNOS

Son todos aquellos que no son parte del sistema. Consiguiendo el acceso al recurso o servicio sin necesidad de ser un usuario legítimo.

Por ejemplo: Con el propósito de evitar el origen real del ataque, se falsea la dirección IP de origen.

2.3 MODOS DE ATAQUE DE DENEGACIÓN DE SERVICIO

Los ataques DoS tienen una variedad de formas y se dirigen hacia una variedad de recursos y/o servicios. Existen básicamente 3 modos de ataques que son:

- Consumo de recursos.
- Destrucción o alteración de la información de configuración.
- Destrucción física o alteración de componentes de una red.

2.3.1 CONSUMO DE RECURSOS

Tanto computadoras como dispositivos de interconexión, necesitan de ciertas características y/o requisitos para desempeñar sus funciones de forma ideal, como: ancho de banda, tiempo de procesamiento, acceso, memoria, espacio de disco entre otros. Si a un computador o dispositivo de red se le agotan sus recursos, éste simplemente deja de funcionar como normalmente debería hacerlo, se ralentiza o simplemente deja de operar.

Existen básicamente dos métodos para la realización de un ataque de denegación de servicio con respecto al consumo de recursos:

- Por explotación de vulnerabilidades.
- Por saturación o inundación.

2.3.1.1 Por explotación de vulnerabilidades

Son aquellos que aprovechan una vulnerabilidad en el sistema para volverlo inestable. La vulnerabilidad consiste generalmente, en un fallo en la implementación del software de la aplicación o en una deficiencia en la configuración del recurso/utilidad.

Al enviar uno o varios paquetes construidos de forma mal intencionada, pueden provocar un estado que el programador no previó en el momento del diseño, pudiendo generar: un bucle infinito, ralentizar gravemente la velocidad de ejecución de la aplicación, hacer que deje de funcionar, provocar el reinicio de la máquina o consumir grandes cantidades de memoria; generando en todos los casos, la denegación del servicio ofertado a los usuarios legítimos.

2.3.1.2 Por saturación o inundación

Son aquellos ataques que saturan a un equipo con solicitudes falsas, enviando un gran número de mensajes o paquetes hacia una víctima con la finalidad de que ésta no pueda responder a las solicitudes reales.

Por ejemplo: El procesamiento de un gran número de peticiones o simplemente peticiones complejas puede requerir un amplio tiempo de CPU y/o agotamiento de memoria, la transmisión de un gran número de paquetes o mensajes pueden agotar el ancho de banda de una red. La principal fortaleza de este tipo de ataques reside más en el volumen de tráfico que en su contenido.

2.3.2 DESTRUCCIÓN O ALTERACIÓN DE LA INFORMACIÓN DE CONFIGURACIÓN

Un equipo mal configurado deja de operar correctamente o simplemente deja de hacerlo. Modificando o destruyendo la información de configuración de un equipo se altera su funcionamiento y el equipo o dispositivo de red implicado podría dejar de operar o funcionar como normalmente debería hacerlo.

2.3.3 DESTRUCCIÓN FÍSICA O ALTERACIÓN DE COMPONENTES DE UNA RED

Al tener acceso no autorizado a las instalaciones e incluso a los equipos de una red se pueden realizar un sin número de ataques como: Interrupción del suministro eléctrico, desconexión o apagado de equipos, vandalismo, robo o alteración de sus componentes como: disco duro, memorias, tarjetas, entre otros.

A continuación se realizará una exposición de los ataques DoS más comunes y que algunos han sido registrados por organismos internacionales y grupos de investigación de todo el mundo como el CERT.

2.4 TIPOS DE ATAQUES DE DENEGACIÓN DE SERVICIO (DOS)

En el ANEXO 4 se realiza una comparación de los diferentes tipos de ataques DoS que a continuación se revisarán. En dicha comparación se puede observar que el propósito de gran parte de ellos es el de saturar los sistemas y degradar las comunicaciones, siendo su principal diferencia el tipo o distintos tipos de protocolos y métodos mal intencionados utilizados para alcanzar su propósito.

2.4.1 MAIL BOMBING

Consiste en el envío masivo de mensajes generalmente anónimos a una máquina hasta saturar el servicio. El email spamming es una variante de éste ataque.

2.4.2 OVERDROP

Este Ataque se basa en enviar paquetes incorrectos, de tal forma que el kernel victima produzca los mensajes de error correspondientes, normalmente logeados en fichero y consiguiendo así, llenar el disco duro o la consola de la víctima.

2.4.3 IP FLOODING

Se basa en la inundación masiva de la red con tráfico espurio de datagramas IP, con el objeto de degradar el rendimiento de la red, ralentizar las comunicaciones existentes o para colapsar un equipo. Se da principalmente en redes locales dónde cualquier máquina puede enviar y recibir sin ningún tipo de limitación en el ancho de banda consumido.

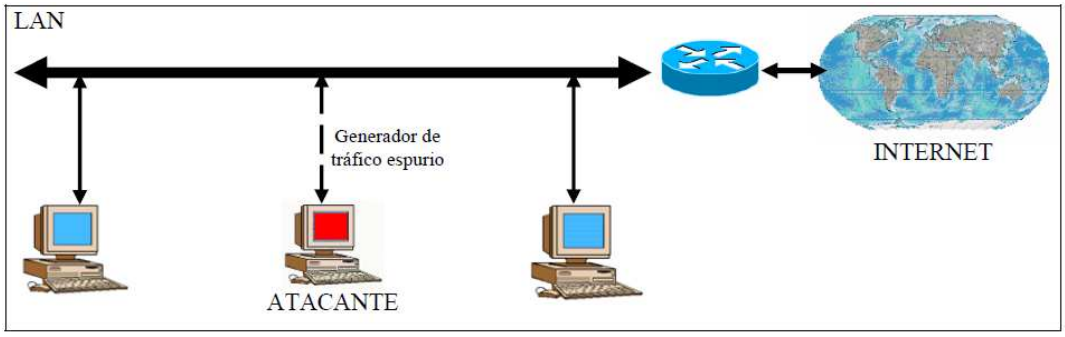


Figura 2. 1 Ataque IP Flooding o inundación de paquetes IP[41].

El tráfico generado en este tipo de ataques IP flooding puede ser aleatorio o dirigido.

2.4.3.1 Aleatorio

Es el más básico y simple para degradar el rendimiento de comunicación del segmento de red. Se generan paquetes falsos o ficticios con origen y destino aleatorio.

---

[41] Seguridad en redes IP, Gabriel Verdejo Álvarez, Universidad Autónoma de Barcelona.

2.4.3.2 Dirigido

Este tipo de ataque además de degradar el rendimiento de la red, busca colapsar a una víctima, enviando una gran cantidad de peticiones que el equipo será incapaz de procesar. En general éste tipo de ataques se da cuando la dirección de origen, destino o ambas es la de la máquina que recibe el ataque, basándose en la generación de datagramas UDP, paquetes TCP o mensajes ICMP de forma masiva.

2.4.4 BROADCAST IP FLOODING

Se puede magnificar el ataque haciendo uso de la dirección de broadcast. La forma más sencilla de éste ataque reside en enviar datagramas IP a la dirección de broadcast de la red, obligando así al router por ejemplo, enviar el paquete a todos los computadores pertenecientes a la red.

También existen variantes dónde se envían peticiones de PING a varios computadores, falseando la dirección IP de origen y substituyéndola por la dirección de broadcast de la red a atacar. De esta forma, todas las respuestas individuales pong (Eco de respuesta a ping) se ven amplificadas y propagadas a todos los ordenadores pertenecientes a la red.

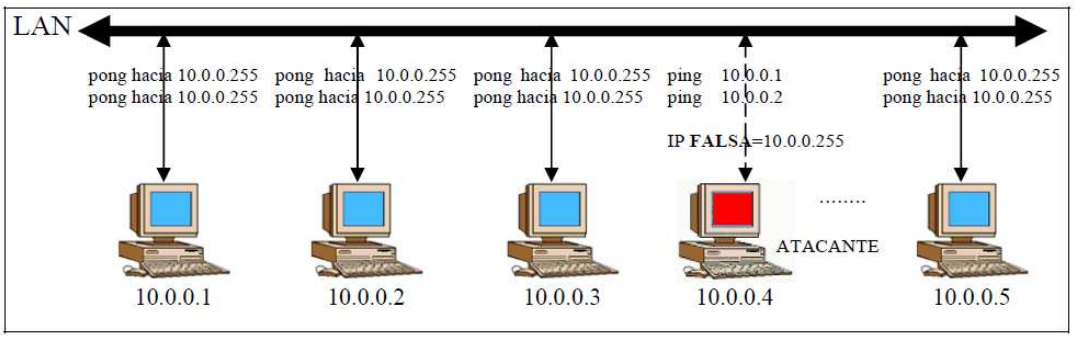


Figura 2. 2 Ataque Broadcast IP Flooding[42]

Smurf y Fraggle son tipos concretos de ataques Broadcast IP Flooding.

---

[42] Seguridad en redes IP, Gabriel Verdejo Álvarez, Universidad Autónoma de Barcelona.

2.4.4.1 Smurf

Estos ataques se basan en transmitir mensajes ICMP de tipo echo-request, es decir, correspondiente a una petición de ping. Estos mensajes llevan como dirección de origen la dirección IP de la víctima (usando IP Spoofing) y como dirección de destino la dirección broadcast de la red o redes que se utilizaran para atacar a la víctima. De esta forma todos los equipos de la red envían mensajes ICMP echo-reply a la víctima.

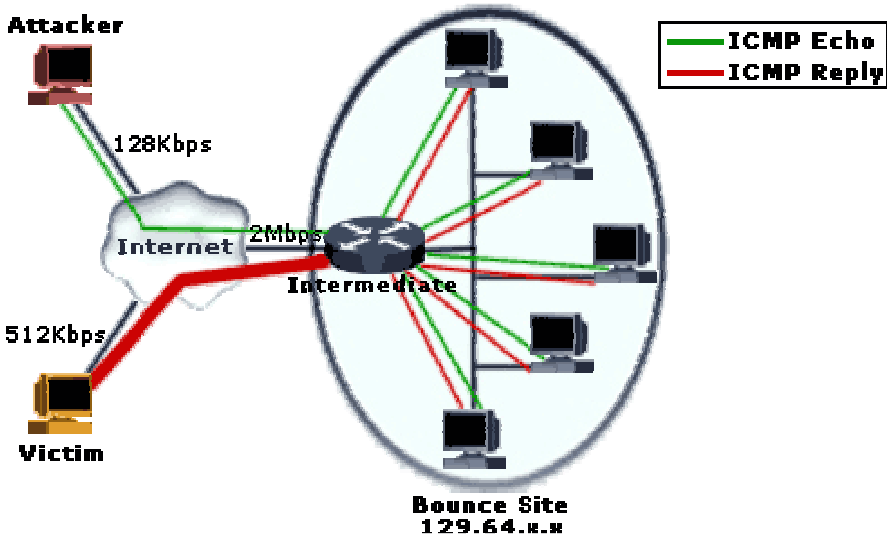


Figura 2. 3 Ataque Smurf[43]

2.4.4.2 Fraggle

Es un tipo de ataque muy similar a smurf pero en vez de emplear mensajes ICMP utiliza datagramas UDP echo. En este caso el atacante envía datagramas UDP al puerto 7 (echo). De esta forma los host que tengan activo el servicio echo reenviarán el paquete a la víctima, y los que no mandarán un mensaje ICMP de error.

2.4.5 ECHO-CHARGEN / BUCLE UDP/ UDP BOMB

Sistemas Linux y UNIX además del servicio echo (puerto 7) suelen tener el

[43] http://www.techexams.net/technotes/securityplus/attacks-DDOS.shtml

servicio chargen (puerto 19). Echo hace exactamente lo que su nombre lo indica y Chargen (Character Generator), genera aleatoriamente un conjunto completo de caracteres ASCII tan rápido como pueda en respuesta a una petición y fue diseñado como mecanismo para pruebas. Este servicio que usa el puerto 19 se encuentra en escucha a datagramas UDP.

El ataque consiste en cruzar ambos servicios echo y chargen, enviando una petición falsa al servicio CHARGEN (que retorna una secuencia de caracteres pseudo-aleatoria) falseando la dirección de origen y como puerto de respuesta, el puerto ECHO (que responde a cualquier petición) de la máquina a atacar, entrando así en un bucle infinito.

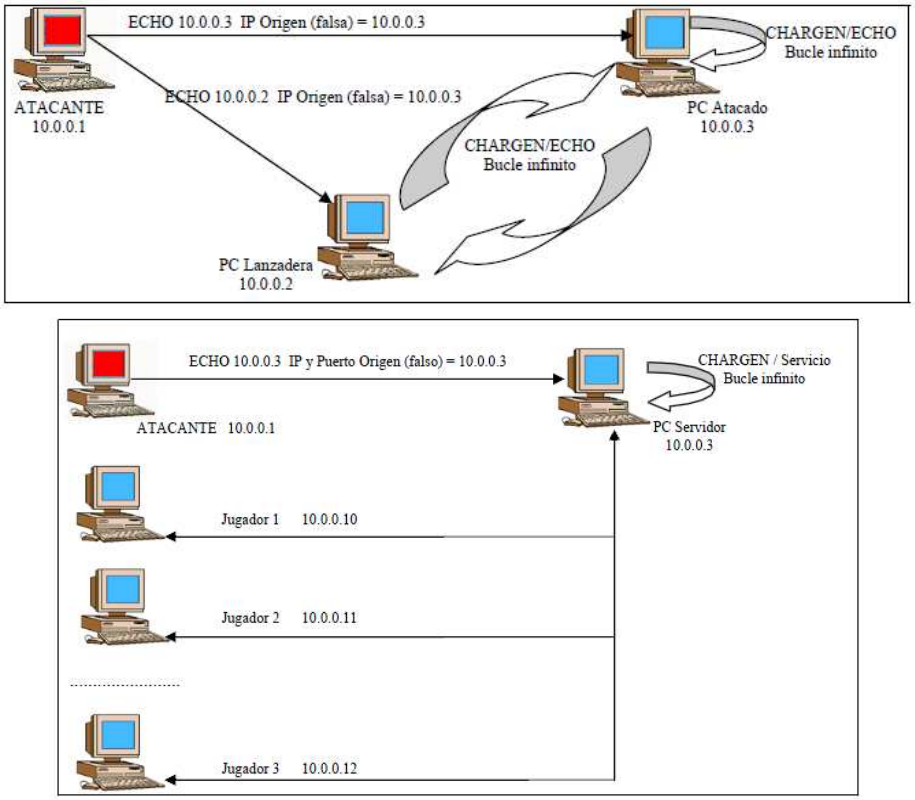


Figura 2. 4 Ataques Chargen/Echo[44]

Estos ataques suelen buscar algún servicio activo como por ejemplo servidores de juego en red que respondan a cualquier datagrama recibido.

[44] Seguridad en redes IP, Gabriel Verdejo Álvarez, Universidad Autónoma de Barcelona.

2.4.6 SNORK

El ataque Snork es similar al Bucle UDP. Consiste en enviar un datagrama UDP que tenga como puerto de origen 7(echo) o 9(chargen) y puerto destino 135 (Microsoft Location Service). El resultado que se consigue es el mismo que con el bucle UDP.

Un solo paquete UDP Snork puede aumentar la utilización de la CPU en un sistema Windows NT al 100% por un período de 5 a 120 segundos. Un ataque continuo fácilmente podría bloquear una máquina. Y si el ataque rebota entre máquinas podría dejar a una red completa inoperable.

2.4.7 ATAQUES A LA PILA TCP/IP

2.4.7.1 TCP SYN Flooding

Esta técnica consiste en enviar una multitud de peticiones de conexión a un ordenador mediante paquetes SYN, pero sin llegar a completar el establecimiento de la conexión con los paquetes ACK respuesta al desafío ACK/SYN de la víctima.

Para mantener las conexiones tcp se crean estructuras en memoria que almacenan datos sobre la conexión. El enviar un gran número de peticiones de conexión TCP se satura la memoria del host atacado, con lo cual no se pueden establecer nuevas conexiones.

Se suelen tener múltiples conexiones “semi-abiertas” en el servidor, al menos hasta que se produzca un timeout que usualmente está en el orden de los 15 minutos. Si se mantiene el flujo de paquetes SYN sin respuesta, provocaría que dicho puerto no pueda establecer nuevas conexiones.

2.4.7.2 Land

Se basa en enviar un paquete TCP con el indicador SYN activo a la misma dirección IP y al mismo número de puerto, en los campos fuente y destino, consiguiendo que el ordenador se responda a sí mismo indefinidamente, volviéndolo inestable al punto de poder colapsar el sistema.

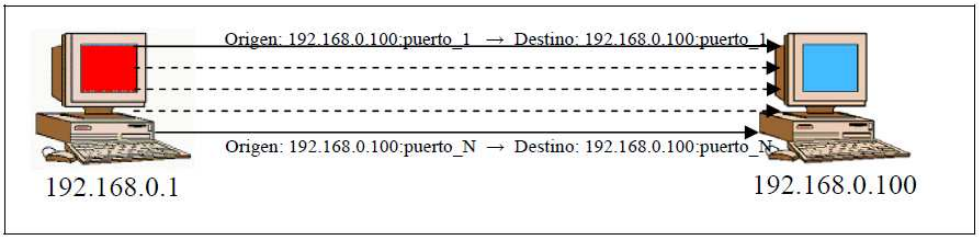


Figura 2. 5 Ataque Land[45]

Usualmente este tipo de ataques suelen ir acompañados con violaciones a los campos de opciones de los protocolos con el objetivo de confundir aun más al computador atacado.

2.4.7.3 WinNuke

WinNuke es un ataque antiguo llamado también OOB nuke. Afectó a sistemas Microsoft Windows 95 y Microsoft Windows NT. Luego fue lanzada una nueva versión afectando también a sistemas Windows 2000 y XP, usando el puerto 139 y/o puerto 445. Sin embargo estas vulnerabilidades fueron corregidas con la ayuda de parches.

El Puerto 139 es uno de los más usados por NetBIOS y el puerto 445 es usado por el Active Directory. Un mensaje Message Block (SMB) incorrecto al ordenador o servidor es enviado a uno de estos puertos provocando la caída del sistema.

Consiste en establecer una conexión enviando un segmento TCP usando el puerto 139 (el puerto de NetBIOS) con el flag URG (Urgente, MSG_OOB)

[45] Seguridad en redes IP, Gabriel Verdejo Álvarez, Universidad Autónoma de Barcelona.

activado e indicando al Winsock del ordenador atacado que envíe los datos llamados datos fuera de banda (out-of-band-data).

Al recibir el paquete con la opción MSG_OOB habilitada, el ordenador atacado, espera una indicación de la posición del paquete en la que terminan los datos urgentes a los que deben seguir los datos normales, pero el indicador OOB del paquete creado indicara el final, no encontrando así datos que sigan a los datos urgentes.

Esto provoco la caída del sistema en muchos equipos Windows y usualmente exigía el reinicio del ordenador para así poder restablecer la comunicación con la red.

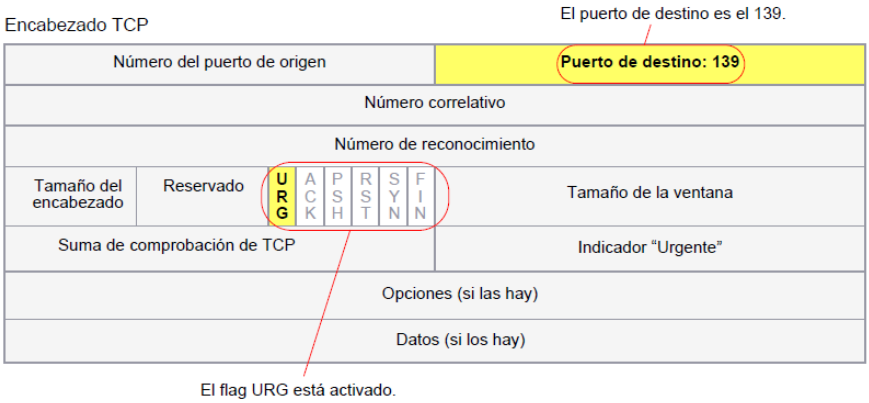


Figura 2. 6 Indicadores de un Ataque Winnuke[46]

2.4.7.4 TCP FIN Flooding

Este tipo de ataque es similar al TCP SYN Flooding y se basa en que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente.

Este es un comportamiento correcto del protocolo TCP, pero algunos sistemas no cumplen con este requerimiento de enviar siempre paquetes RST, independientemente si el puerto está abierto o cerrado, produciéndose una vulnerabilidad que puede ser explotada por parte de un atacante.

[46] NetScreen Technologies, conceptos y ejemplos, Manual de referencia de ScreenOS, Volumen 4: Mecanismos de detección de ataques y defensa.

Como se explico en el capitulo anterior el protocolo TCP se basa en una conexión de tres pasos. Si el paso final no llega a establecerse, la conexión permanece en un estado denominado semiabierto, y al atacar esta vulnerabilidad se produce el mismo resultado que en el caso de TCP SYN Flooding.

2.4.7.5 Inundaciones SYN-ACK o SYN-ACK Flood

Este tipo de paquetes son el segundo paso que usa el protocolo TCP para el establecimiento de conexión en 3 vías y por tal razón debe haber una entrada correspondiente en el TCB (Transmission Control Block).

Navegar por la TCB utiliza recursos de CPU, sobre todo cuando el TCB suele ser grande. Los Ataques aprovechan esta desventaja para enviar una enorme carga de paquetes SYN-ACK con el objeto de aumentar el uso de la CPU de un sistema. Por otra parte, como los paquetes SYN-ACK no pertenecen a una conexión existente, el objetivo atacado tiene que enviar paquetes RST a la fuente degradando también el rendimiento de la red

Un factor interesante es la capacidad de enviar paquetes generados SYN-ACK por terceros mediante un mecanismo de reflexión. Cuando un paquete SYN es enviado a un puerto abierto de un ordenador, éste envía un paquete SYN-ACK a la fuente. Entonces, cualquier ordenador puede ser parte de estos ataques. Un simple paquete SYN enviado a un ordenador genera un SYN-ACK de vuelta a la fuente.

2.4.7.6 Banderas SYN y FIN activadas

Los flags o banderas de control SYN y FIN normalmente no están activadas en el mismo encabezado de un segmento TCP, y sus propósitos se excluyen mutuamente.

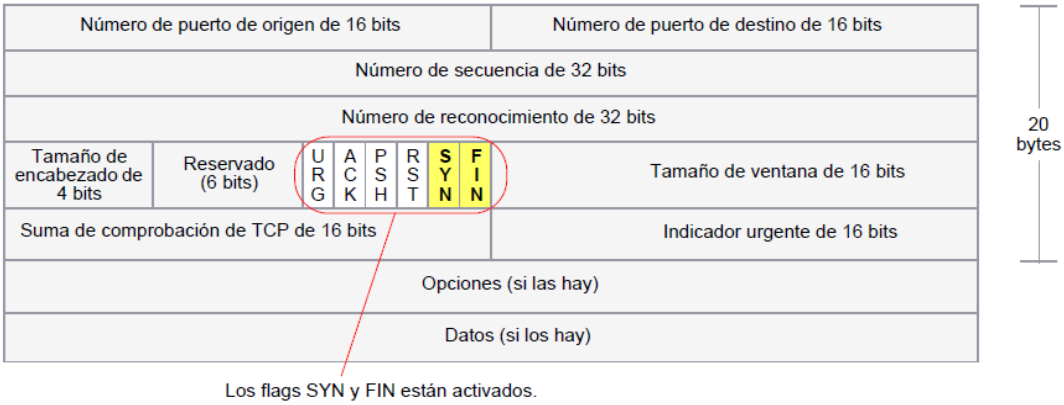


Figura 2. 7 Estructura del Paquete TCP con banderas SYN y FIN activadas[47]

Un encabezado TCP con los flags o banderas SYN y FIN activados representa un comportamiento TCP anómalo y provoca varias respuestas del destino atacado en función del Sistema Operativo que esté utilizando.

Un atacante podría eventualmente explotar estas vulnerabilidades, para conocer qué tipo de respuesta de sistema se devuelve y determinar de este modo el tipo de Sistema Operativo que utiliza y posteriormente atacarlo de alguna otra forma.

2.4.7.7 Bandera FIN y sin bandera ACK

Los segmentos TCP con el flag de control FIN suelen tener también activado el flag ACK para acusar recibo del paquete anterior. Si el flag ACK está desactivado representa un indicio de comportamiento TCP anómalo, no existe una respuesta uniforme ante este hecho. Es posible que el Sistema Operativo reaccione enviando un segmento TCP con el flag RST activado o por el contrario es posible que lo ignore completamente.

Un paquete TCP normal tiene al menos un flag de control activado. Un segmento TCP sin flags de control activados de igual forma representa un evento anómalo y puede dar indicios del tipo de Sistema operativo que se está ejecutando.

[47] NetScreen Technologies, conceptos y ejemplos, Manual de referencia de ScreenOS, Volumen 4: Mecanismos de detección de ataques y defensa.

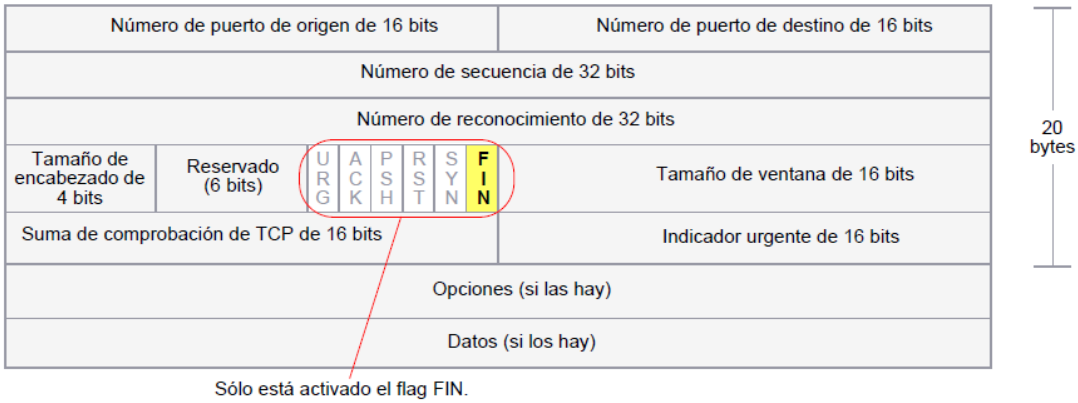


Figura 2. 8 Estructura del Paquete TCP con bandera FIN activada y ACK sin activar[48]

2.4.7.8 Conecction Flood

Los servicios TCP orientados a conexión como por ejemplo telnet, ftp, http, smtp, entre otros pueden soportar un límite máximo de conexiones simultáneas generalmente definidas por un administrador.

Este ataque es similar al Syn Flood y consiste en el intento de monopolizar el límite definido de conexiones, provocando que futuras conexiones no puedan hacer uso del servicio, ya que éstas simplemente serían descartadas.

De igual forma las conexiones expirarán en un tiempo dado y si el ataque se realiza de forma constante y continua se mantendrá saturado el número máximo de conexiones permitidas, denegando así el servicio a futuros usuarios que quieran acceder al servicio.

2.4.7.9 UDP Flood o Inundación UDP

Se basa en el envío de un gran número de datagramas UDP a puertos aleatorios. Si la víctima recibe un datagrama UDP a un determinado puerto cerrado, éste

---

[48] NetScreen Technologies, conceptos y ejemplos, Manual de referencia de ScreenOS, Volumen 4: Mecanismos de detección de ataques y defensa.

devuelve un mensaje ICMP de error. Estos mensajes consumen tiempo de procesamiento y pueden inundar la red degradando su rendimiento.

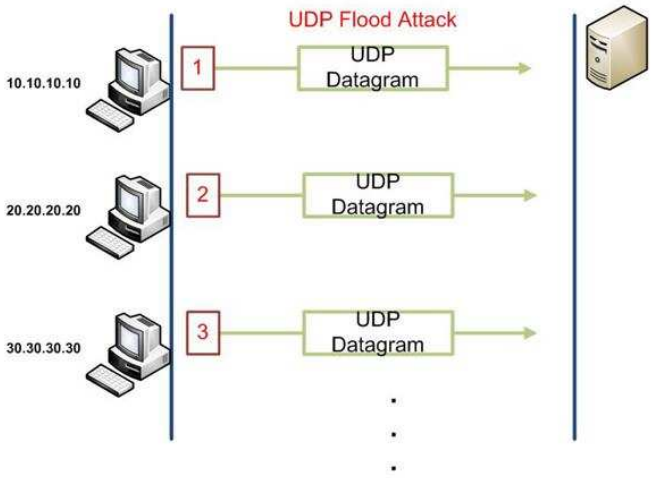


Figura 2. 9 Ataque UDP Flood

2.4.7.10 ICMP Flood o Inundación ICMP

Consiste en enviar de forma continua un gran número de mensajes tipo ICMP echo request (ping), de forma que la víctima o víctimas respondan con mensajes ICMP echo reply (pong). Básicamente es una técnica DoS que pretende agotar el ancho de banda de la víctima.

2.4.7.11 MAC Flooding

Un ataque MAC Flooding consiste en inundar a un switch con tramas, cada una con diferentes direcciones MAC origen, con el objeto de consumir la memoria limitada para almacenar la tabla de traducción de direcciones MAC.

El resultado de éste ataque provoca que el switch entre en un estado llamado modo de failopen, en el que todos los paquetes entrantes se transmiten a todos los puertos y no al específico. Posteriormente el atacante podría incluso hacer uso de un analizador de tráfico como wireshark para capturar información confidencial.

2.4.7.12 ARP Flooding

Los ataques ARP Flooding se basan en el envío masivo de tramas con direcciones MAC origen de forma aleatoria, con el objeto de saturar o llenar las tablas de direcciones MAC (CAM Table) o ARP Cache, impidiendo así, la comunicación desde y hasta los ordenadores conectados a él o con el objeto de provocar un ataque MAC Flooding.

2.4.7.13 WormHole o agujero de gusano

Este tipo de ataque se basa en que un intruso puede interceptar los paquetes de información mientras viajan por alguna parte de la red, y rápidamente reinsertarlo en otro punto físico de la misma red, convenciendo a nodos que utilicen una trayectoria incorrecta formada por dos nodos maliciosos en convivencia entre sí que forman un túnel que es considerado como un medio de comunicación eficaz y legítimo.

Este ataque podría dejar fuera de acción a una red, sin embargo se descubrió que la amenaza puede ser neutralizada a través del uso de paquetes con información del tipo GPS u otros códigos de tiempo[49].

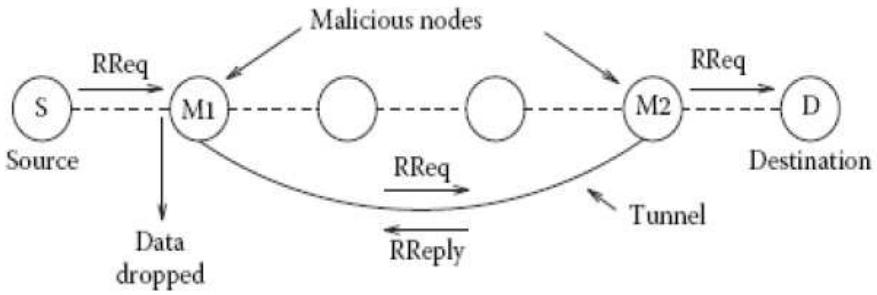


Figura 2. 10 Ataque Wormhole[50]

[49] VSantivirus No. 1048, Descubren nueva amenaza para las redes inalámbricas, 21 de Mayo del 2003, http://www.vsantivirus.com/ar-wormhole-attack.htm

2.4.7.14 Blackholing u hoyo negro

Un ataque Black hole consiste básicamente en la pérdida o descartación de paquetes mediante el re direccionamiento del tráfico a un nodo silencioso o simplemente a ninguno. Puede ser llevado a cabo de forma selectiva (por ejemplo, descartando paquetes para un destino particular, cada cierto tiempo, ciertos paquetes o aleatoriamente, denominado "ataque de agujero gris o Gray hole attack").

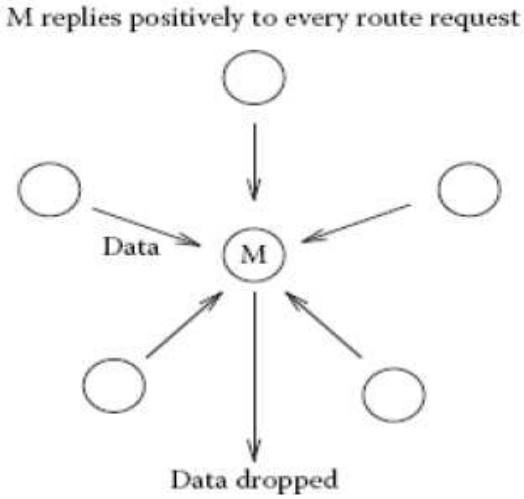


Figura 2. 11 Ataque BlackHole[60]

Por ejemplo:

En redes inalámbricas un ataque blackholing puede ser realizado mediante la creación de puntos de acceso falsos. Un Access Point falso podría ser colocado cerca de la red específica, con características exactamente iguales a las de su original, tales como: ESSID, clave WEP e incluso proporcionar una mejor señal. De esta manera los clientes de forma automática se asociarán con este Acces Point falso y como no proporciona conectividad alguna la comunicación no será posible.

---

[50] Milton Ivan Cañarte Manrique, Daniel Alexander Parra Loayza, Estudio y diseño de un nodo de acceso, que sirva como piloto para la implementación de una red Wireless Mesh en la Facultad de Ingeniería en Electricidad y Computación de la ESPOL, Escuela Superior Politécnica del Litoral.

A nivel de capa 2, haciendo uso del protocolo ARP, envenenando las rutas y re direccionando el tráfico a un nodo silencioso o simplemente a ninguno.

Usando el protocolo DHCP, una vez que el servidor original deje de funcionar o no pueda proporcionar más direcciones, se puede tomar control sobre este para proporcionar información IP errónea a cualquier cliente que intente conectarse a la red.

2.4.7.14.1 Envenenamiento ARP o ARP Poisoning

ARP poisoning es el ataque más fácil para realizar un tipo de ataque blackhole. Consiste simplemente en enviar paquetes ARP no solicitados y diseñados para limpiar las entradas ARP en el cache cuando un nuevo sistema aparece en la red, conteniendo las direcciones MAC e IP que deberían introducirse en las tablas ARP de los sistemas que pertenecen a la misma red física.

Por ejemplo, si un atacante desearía impedir que los sistemas puedan salir de la red física, simplemente se envía de forma continua paquetes ARP con la puerta de enlace o default Gateway apuntando a una dirección MAC inválida. Posteriormente los computadores dentro de la red física actualizarán su tabla ARP y cualquier intento de comunicación con otra red lógica (capa 3) no será posible y los paquetes serán enviados a una dirección física no válida.

SNMP también puede ser usado para corromper tablas ARP ya que las entradas ARP se almacenan en la MIB ipNetToMediaPhysAddress. Con acceso de escritura a la MIB, es posible cambiar las entradas en la caché de la tabla ARP que por lo menos contendría la puerta de enlace predeterminada.

2.4.7.14.2 *Packet forwarding o Reenvío de paquetes*

Un atacante podría modificar o cambiar totalmente las tablas de enrutamiento de forma que los paquetes sean enviados a diferentes destinos que no sean consistentes o simplemente no existan.

2.4.7.14.3 *Spanning Tree attack*

Arquitecturas de capa 2 complejas y con funcionalidades, necesitan de protocolos específicos para la gestión y configuración automática.

La más antigua es Spaning Tree, diseñado para proporcionar una alta disponibilidad a nivel de capa 2 gracias a la comunicación multicast UDP: BPDU (Bridge Protocol Data Unit). Estos paquetes contienen información sin cifrar, comandos y datos, por lo que resultaría fácil realizar una respuesta falsa ya sea de un mejor candidato o que simplemente no existe uno, durante la siguiente elección del candidato raíz o para generar nuevas elecciones mediante el envío de paquetes BPDU con una prioridad más alta que la actual.

Estas debilidades típicas basadas en mensajes de texto plano y la falta de autenticación pueden ser explotadas en otros protocolos, como VTP y DTP (VLAN / dinámico Trunking Protocol) para crear fácilmente blackholes o agujeros negros.

2.4.8 ATAQUES POR FRAGMENTACIÓN

Los ataques de fragmentación atacan debilidades en el re ensamblado de paquetes IP fragmentados con tamaños incorrectos, y estos pueden ser:

2.4.8.1 Ping of Death

Este ataque utiliza las definiciones de longitud máxima de los protocolos así como la capacidad de fragmentación de los datagramas IP, enviando un ping (mensaje

ICMP echo-request) deformado o incorrecto a un destino.

Un ping tiene un tamaño normal de 64 bytes y algunas computadoras no pueden manejar pings mayores al máximo de un paquete IP que es de 64K (65535 Bytes)

incluyendo la cabecera del paquete (20 Bytes) y asumiendo que no hay opciones especiales especificadas.

El protocolo ICMP tiene una cabecera de 8 bytes, de esta forma el tamaño máximo permitido para enviar un mensaje ICMP sería: 65535 - 20 - 8 = 65507 Bytes.

Enviando pings de tamaño mayor al máximo permitido, al ser re ensamblados en el destino se produce un overflow en el buffer, que según el sistema produciría el bloqueo o reinicio del equipo. Afecto a la mayoría de Sistemas Operativos como Unix, Linux, Mac, Windows, impresoras, y routers. No obstante la mayoría de los sistemas han corregido esta vulnerabilidad.

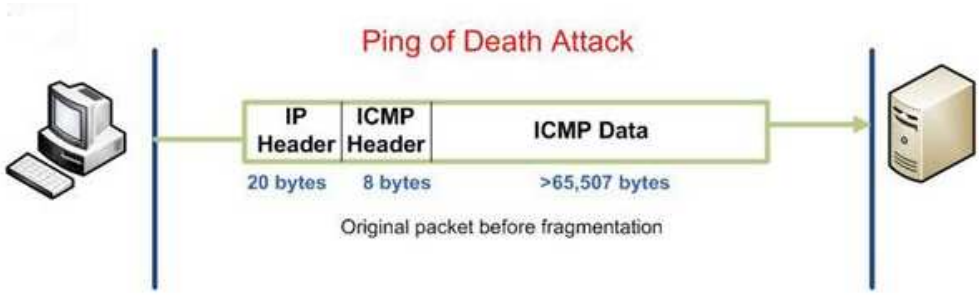


Figura 2. 12 Ataque Ping of Death[51]

Ssping es una variante de Ping of Death, que afecto a Win95 y NT. El ataque consiste en enviar un gran número de paquetes fragmentados y de gran tamaño a la víctima.

2.4.8.2 Teardrop

Es otro ataque famoso que explota la función de re ensamblaje de paquetes IP. Consiste en enviar 2 paquetes IP indebidamente construidos generalmente con errores en el offset y fragmentados. El segundo fragmento enviado es establecido con un valor en el campo de desplazamiento del fragmento que cae dentro del

[51] Seguridad en redes IP, Gabriel Verdejo Álvarez, Universidad Autónoma de Barcelona

bloque anterior.

Al ser los paquetes re ensamblados y tener el problema de que los paquetes se solapan debido a que la suma de “tamaño de desplazamiento” mas el “tamaño de un paquete fragmentado” es distinta a la del siguiente paquete fragmentado, se produce un desbordamiento o sobre escritura en la memoria de el servidor que intenta reensamblarlos, produciendo la caída del sistema, especialmente si está ejecutando un sistema operativo antiguo que tenga esta vulnerabilidad o no haya sido parchado.

Dependiendo de la robustez del sistema operativo se puede perder solo el servicio atacado o incluso llegar a colapsar todo el ordenador.

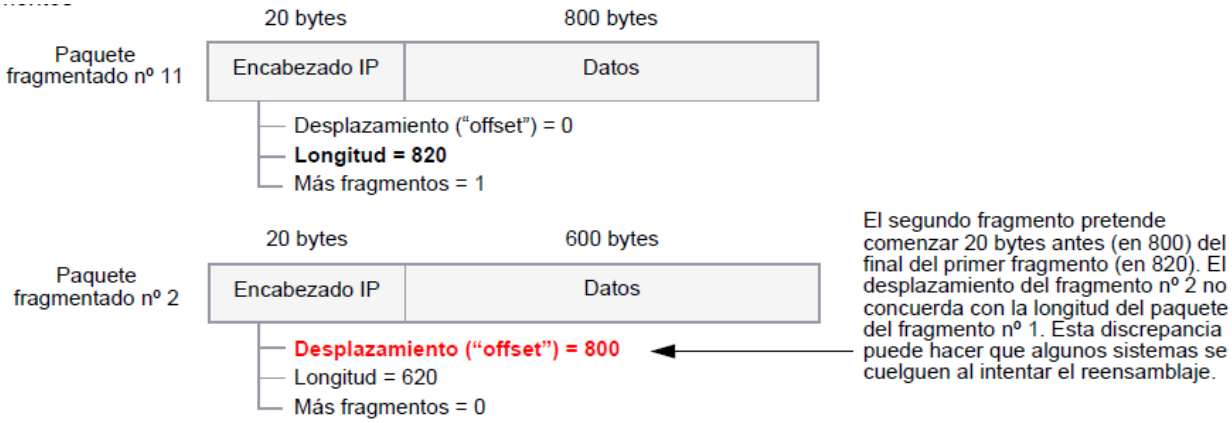


Figura 2. 13 Discrepancia entre Fragmentos IP[52]

2.4.8.3 NewTear

El ataque NewTear es una versión modificada del ataque Teardrop que afecta a sistemas Windows antiguos y que no han sido parchados. Consiste en explotar el error o problema con la forma en que Microsoft maneja ciertas excepciones de la pila TCP/IP, causada por información de encabezados UDP incorrectos.

[52] NetScreen Technologies, conceptos y ejemplos, Manual de referencia de ScreenOS, Volumen 4: Mecanismos de detección de ataques y defensa.

2.4.8.4 Bonk

El ataque Bonk afecta a sistemas Windows que han sido parchados ante el ataque Teardrop. Aunque no permite rangos de puertos UDP, envía datagramas UDP corruptos al Puerto DNS 53 y se basa en manipular el campo fragment offset o desplazamiento de fragmentos de los paquetes TCP/IP (éste campo le dice al sistema cómo reconstruir un paquete que fue fragmentado).

Al manipular éste campo, provoca que el destino atacado vuelva a re ensamblar el paquete y debido a que es demasiado grande para ser re ensamblado, el sistema se cuelga o cae. Un simple reinicio suele ser suficiente para recuperarse del ataque, pero es posible que los datos que no fueron guardados en el momento del ataque se pierdan

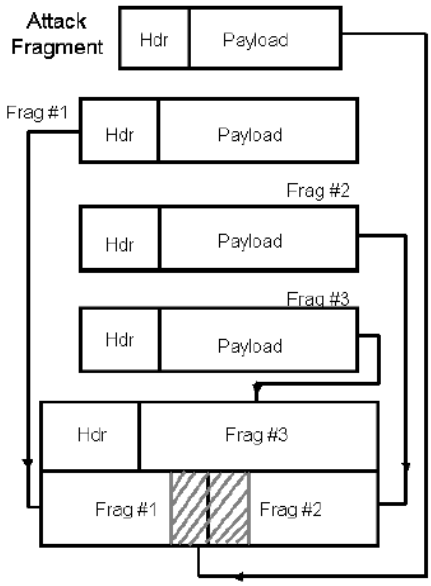


Figura 2. 14 Solapamiento de Fragmentos

2.4.8.5 Boink

El ataque Boink es una versión modificada del ataque Bonk, permitiendo enviar el ataque a un rango de puertos y no solo al 53. De igual forma que en el ataque Bonk no se ha demostrado que cause un daño significativo a los sistemas, y un simple reinicio suele ser el remedio, pero podría causar problemas si los datos no

fueron guardados en el momento en que la máquina fue atacada. Generalmente el principal problema de Boink y Bonk es la pérdida de datos.

2.4.8.6 SynDrop

Syndrop es una mezcla de Teardrop y TCP SYN Flood, que afecto a plataformas Linux y Windows 95/NT.

2.4.8.7 Nestea

Es un ataque específico de Linux similar al ataque Teardrop que de igual forma al manejar de manera incorrecta un determinado tipo de fragmentos ensamblados, ciertas pilas TCP/IP fallan. Las versiones anteriores al kernel 2.0.34 fueron vulnerables a éste tipo de ataques.

2.4.8.8 Jolt y Jolt2

Jolt y Jolt2 son ataques similares que envían un flujo continuo de fragmentos malformados, con el fin de consumir todos los recursos del procesador provocando que los sistemas de destino se ralenticen o se bloqueen.

Se diferencian en que jolt utiliza fragmentos de mensajes ICMP y jolt2 además puede utilizar fragmentos de datagramas UDP.

Sin embargo, en la mayoría de los casos, las máquinas solo se ven afectadas mientras la tormenta de paquetes se envía, cuando ésta se detiene, su estado inicial se restablece.

2.4.8.9 Targa3

Targa3 es un tipo de ataque de denegación de servicio que consiste en enviar aleatoriamente paquetes IP malformados. Estos errores en los paquetes IP se basan en valores inválidos de las siguientes características: fragmentación,

protocolo, tamaño, valores del encabezado, opciones, desplazamientos, segmentos TCP o marcas de recorrido.

Si se envían una gran cantidad de paquetes malformados, el sistema puede colapsar debido al agotamiento de sus recursos. Targa3 puede ser utilizado contra firewalls y routers, para probar su estabilidad y reacciones ante paquetes inesperados.Targa3 afecto a sistemas Windows 95,98, Me, NT, 2000

2.4.8.10 Fragmentación de mensajes IGMP

Los ataques IGMP (Internet Gorup Management Protocol, Protocolo de gestión de grupos de internet) utilizan una debilidad de este protocolo, o de su implementación. Este ataque es similar a los anteriores ataques por fragmentación, pero se diferencia en que utiliza paquetes IGMP.

2.4.8.10.1 Igmpsyn

El objetivo de éste ataque es congelar el sistema de la víctima, enviando solicitudes IGMP del tipo 1 (para recuperar información sobre los grupos de multidifusión) con direcciones de origen aleatorias. Este ataque afecto a los sistemas Windows 95 y Windows 98.

2.4.8.11 FAWX

Fawx es un ataque IGMP, que interrumpe el funcionamiento del ordenador de la víctima, utilizando paquetes IGMP fragmentados y con un tamaño excesivo para congelar el sistema objetivo.

Afecto a Windows 95, Windows 98 y Windows NT. Fawx2 envía paquetes basura fragmentados al puerto 1389 ocasionando una pantalla azul de error en Windows 95, 98 o 2000.

2.4.8.12 KOD

El ataque Kod o Kiss of Death se basa en enviar a la víctima paquetes IGMP mal formados con el objeto de que la pila TCP/IP caiga, provocando el reinicio instantáneo del computador y un mensaje de error azul en la pantalla. Afecto a sistemas Win 95,98 y 2000.

2.4.9 ATAQUES DOS A SERVICIOS EN VOIP

Se concluirá citando los ataques DoS más comunes con algunos específicos que pueden afectar a redes VoIP y entre ellos se tienen:

2.4.9.1 UDPflood en VoIP

Los ataques de inundación UDP que fueron vistos anteriormente pueden incluso saturar a cualquier dispositivo VoIP.

2.4.9.1.2 Inundación de paquetes RTP o RTPflood

El protocolo RTP (Real-time Transport Protocol), es un estándar creado por la IETF para la transmisión confiable de voz y video a través de Internet.

Al igual que UDPflood, se basa en enviar un gran número de paquetes RTP a un destino específico, con el objeto de saturarlo e impedir su correcto funcionamiento.

Generalmente antes de lanzar el ataque RTPflood es necesario conocer el puerto de escucha de paquetes RTP en el dispositivo que se requiere atacar. Por ejemplo, por defecto los softphones, abren puertos comenzando por el 8000 y secuencialmente se aumenta según se necesite para cada sesión RTP.

2.4.9.1.3 Inundación de paquetes Invite o InviteFlood

El objetivo de InviteFlood, es el de enviar masivamente peticiones INVITE a un servidor con el objeto de colapsarlo. El servidor tratará de atender a todas las llamadas generadas consumiendo una gran cantidad de recursos.

2.4.9.1.4 Teardown

Un ataque Teardown hace uso de peticiones BYE con el objeto de finalizar llamadas en curso. Previamente se requiere conocer el Call-ID cuando el agente de usuario envía al servidor una petición de INVITE para iniciar una nueva conversación. Dicho parámetro puede ser fácilmente capturado haciendo uso de un sniffer.

Los parámetros necesarios para poder ejecutar un teardown son:

- Interfaz de red.
- Usuario.
- Dominio.
- Dirección IP del Servidor SIP.
- CALL_ID.
- Dirección o Usuario origen.
- Dirección o Usuario de destino.

2.4.9.5 Inundación IAX o IAXFlood

Es un ataque de saturación para el protocolo IAX2 de Digium, empleado por PBX Asterisk.

2.4.9.6 SIP-kill

Es un script desarrollado en Perl que permite capturar el tráfico en busca de mensajes INVITE de SIP y su objeto es el de finalizar las nuevas llamadas que detecta.

2.5 ATAQUES DISTRIBUIDOS DE DENEGACIÓN DE SERVICIO (DDOS)

Si bien el objeto del presente proyecto no es el de estudiar los ataques distribuidos de denegación de servicio (DDoS), a continuación se realiza una breve revisión de ellos, sus herramientas, detección y posibles mecanismos de defensa. Esto permitirá al lector tener una visión más amplia y poder implementar redes más seguras y confiables, que permitan en lo posible mitigar ataques DoS e incluso otro tipo de amenazas. Como se observará en el Capítulo 3 (SIMULACIÓN Y ANÁLISIS), simples ataques DoS realizados desde un único host (Atacante), pueden comprometer a parte de un sistema.

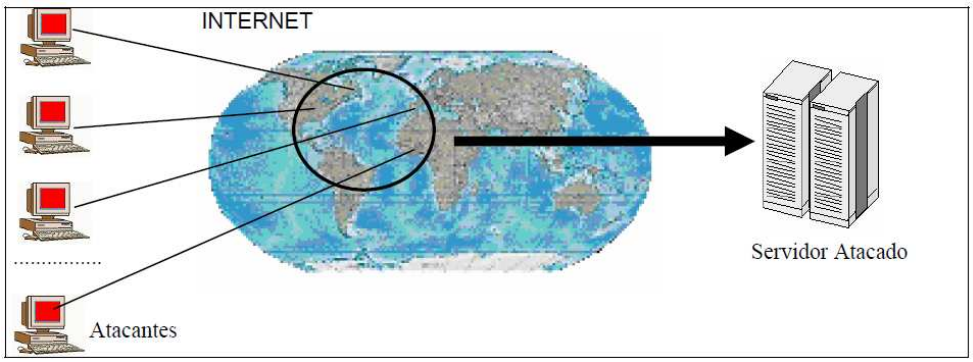


Figura 2. 15 Ataque distribuido de denegación de servicio DDoS[53]

Los ataques de denegación de servicio distribuido (DDOS) son ataques de denegación de servicio (DOS) más sofisticados de coordinación y en el que pueden estar involucrados cientos o miles de ordenadores, existiendo múltiples focos distribuidos y sincronizados, de forma que focalizan su ataque en un mismo destino.

Sin embargo, el ir sembrando los demonios o agentes zombies en los distintos ordenadores puede llevar mucho tiempo y es posible que antes de disponer de una cantidad suficiente de ordenadores; éstos sean descubiertos, y al final nunca pueda lanzarse el ataque planificado.

---

[53] Fernando Limón Martínez, Sistemas Distribuidos De Denegación de Servicio, Madrid Junio del 2000, http://fi.upm.es/~flimon.

Normalmente, la dirección de origen de un ataque DoS es una o varias direcciones suplantadas (“spoofed”) o bien direcciones reales previamente comprometidas por el atacante, con el objeto de no ser localizados y sancionados por los organismos competentes.

Una vez que el atacante o atacantes han conseguido un control de cierto número de ordenadores, los gestionan formando una estructura jerárquica que les permita por un lado mantener su anonimato y por otro, controlar de forma directa una serie de nodos que a su vez replicarán las órdenes recibidas a otros.

2.6 FASES DE UN ATAQUE DDOS

Básicamente un ataque DDoS sigue las siguientes etapas:

- Reclutamiento.
- Búsqueda de vulnerabilidades.
- Utilización de la vulnerabilidad para acceder a la máquina
- Infección de la máquina con el código del ataque.
- Ejecución del ataque.

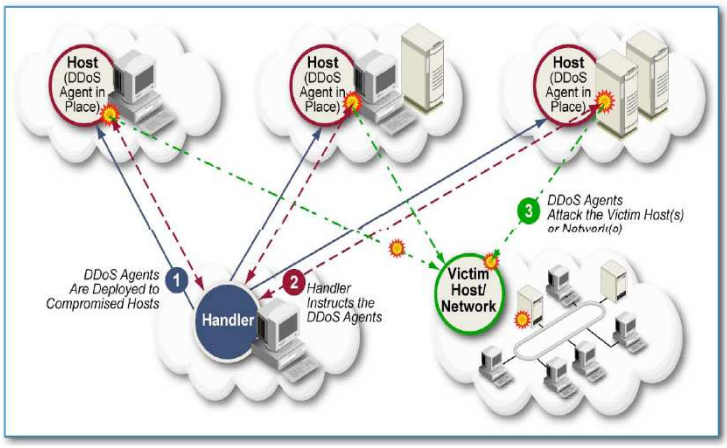


Figura 2. 16 Fases de un Ataque DDoS[54]

[54] Ataques de Denegación de Servicio, Seguridad en Internet, B. Alarcos, E. de la Hoz, Universidad de Alcalá, Dpt. De Automática

2.6.1 RECLUTAMIENTO

Las máquinas que realizan el ataque son usualmente llamadas: zombies, daemons, slaves, o agentes. Se usará el término agente[55] para referirnos a ellos. Frecuentemente un ataque DDoS involucra a cientos o miles de agentes. Así el atacante necesitará enviar solo un comando para que todos los agentes comiencen una inundación a una víctima.

El reclutamiento de máquinas agente puede ser hecho de forma manual, semiautomática, o de una manera totalmente automatizada. Por ejemplo, en el caso de dos herramientas DDoS como trinoo y Shaft, únicamente el proceso de instalación se ha automatizado, mientras que el descubrimiento de máquinas vulnerables se realiza de forma manual.

Los atacantes hoy en día utilizan scripts para automatizar todo el proceso, e incluso usan scanning para identificar las máquinas ya comprometidas para tomar el control. Por ejemplo: Slammer, MyDoom, Bagle-infected hosts.
Incluso algunos gusanos pueden ser utilizados explícitamente para crear redes bots[56] que luego pueden ser utilizadas para diversos fines maliciosos, como los ataques DDoS.

En general, una vez que el atacante haya obtenido el control del host, se instala el agente y se asegura que todos los rastros de la intrusión sean ocultados y que el código se ejecute incluso después de un reinicio, por ejemplo: Redes Phatbot han reportado un número tan grande como 400000 máquinas infectadas[57].

---

[55] **Agentes.-** Son máquinas poco seguras que no disponen de las últimas actualizaciones y parches de software, no están protegidas por un firewall u otro dispositivo de seguridad. En general son máquinas que permiten al atacante tener acceso ilimitado al sistema.

[56] **Bot.-** Denominado también robot, es un programa cliente que se ejecuta en background en un host comprometido. Visualiza ciertos strings que se muestran en un canal IRC, que representan comandos codificados y que el programa bot ejecuta como, invitar a alguien al canal IRC,dar al usuario del canal permisos de operador, escanear un bloque de direcciones, realziar un ataque DoS, entre otros.

[57] Brian Krebs, Worm Tip of the PC Bug Invasion, 5 de Diciembre del 2004, http://www.securityfocus.com/news/8573

2.6.1.1 Ocultamiento de Rastros

El atacante oculta su identidad usando capas entre su equipo y los agentes. Para enviar órdenes a los agentes, se usan una o varias máquinas denominadas handlers o masters. Se usará el término handlers para referirnos a ellos.

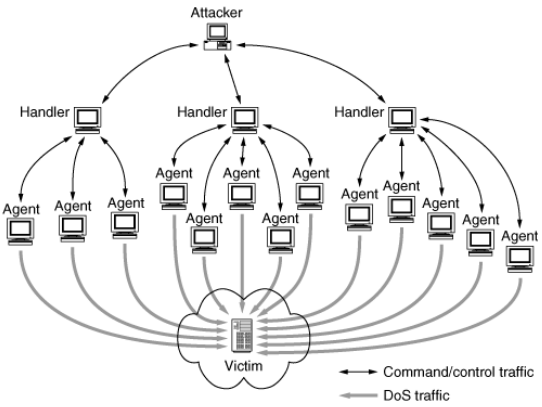


Figura 2. 17 Arquitectura Handler/Agent[58]

Otra forma consiste en que el atacante en secuencia, inicie sesión en varias máquinas, antes de acceder a los handlers. Estas máquinas de intermediario entre la máquina del atacante y los handlers son llamados stepping stones.

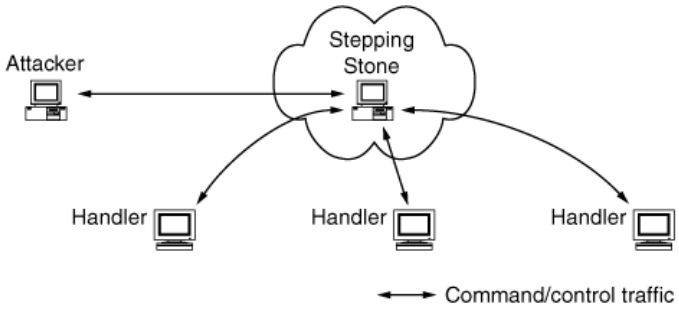


Figura 2. 18 Ilustración de un sitio de alojamiento Stepping Stone[67]

Tanto los handlers como los stepping stones son usados para obstaculizar los intentos de investigación. Por ejemplo, si se encontrara un equipo agente y se lo analizara, toda su comunicación apuntaría a uno de los handlers y una investigación de éstos apuntaría a un stepping stone, y de allí a otro stepping

[58] http://denialofservice.uw.hu

stone. Generalmente los stepping stones son seleccionados de diferentes países y continentes, razón por la cual, se hace muy difícil seguir la pista a la máquina del atacante y así poder desenmascarar su identidad.

O simplemente se oculta el ataque a través del uso de IP spoofing. Los atacantes normalmente forjan el campo de dirección origen para impedir el descubrimiento de las máquinas agente, asumiendo la identidad de un cliente legítimo e incluso varios de ellos.

2.6.2 BÚSQUEDA DE VULNERABILIDADES

El atacante necesita encontrar máquinas que pueda comprometer y que le permitan maximizar un ataque. Por ende, necesitará reclutar máquinas que tengan amplios recursos, buena conectividad y sean poco mantenidas.

El proceso de buscar máquinas vulnerables se denomina scanning. En la actualidad las herramientas de scanning han mejorado y sus funciones de escaneo son hechas de forma automática. Por ejemplo: blended threats[59] y gusanos.

Una vez que los bots[46] obtienen una lista de host vulnerables, informan al atacante usando la botnet[60] .El Atacante entonces recuperara el archivo y lo añadirá a su lista de máquinas vulnerables.

---

[59] **Blended threats.-** Son programas individuales o grupo de programas que proveen varios servicios.En el contexto, el mando y control usando un bot IRC y escaneo de vulnerabilidades**.**

[60] **Botnet.-** Una red de bots sincronizados a través de la comunicación de un canal IRC.

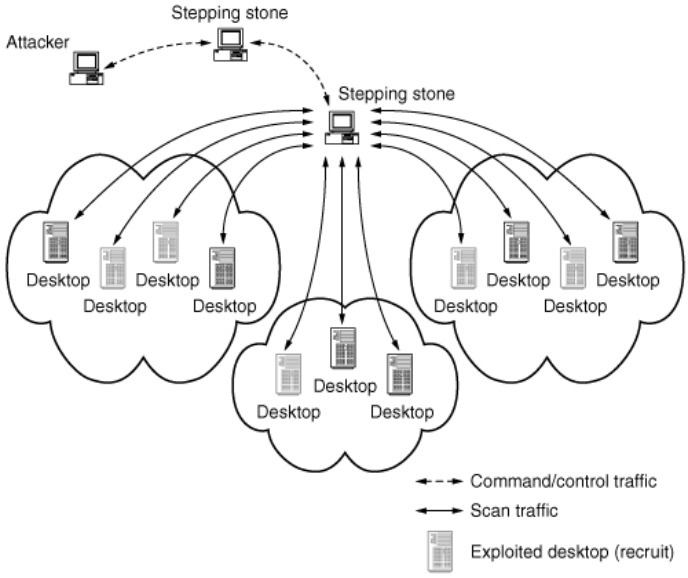


Figura 2. 19 Reclutamiento de agentes[61]

Los Blended threats típicamente incluyen todos o algunos de los siguientes componentes:

- **Un programa de servicio de red de Windows,** por ejemplo, Firedaemon es responsable de registrar programas para ser ejecutados como servidores. Típicamente controla el servidor FTP, por lo que puede estar a la escucha de conexiones entrantes.

- **Scaners,** pueden ser simples scaners SYN como Syncan, caputaradoras de banderas TCP como mscan o con varias características como nmap.

- **Programas DoS básicos**, si bien estos programas pueden parecer anticuados y antiguos, una simple inundación UDP o SYN pueden todavía ser efectivas contra algunos sistemas**.**

- **Un servidor FTP,** permite a un atacante subir archivos al host comprometido.

---

[61] http://denialofservice.uw.hu

- **Servicio de archivos IRC (Warez) bot,** archivos multimedia y programas pirata son conocidos como Warez. Bots que sirven Warez son conocidos como *Warez* bots y tanto bots como clientes IRC son capaces de transferir archivos usando un protocolo llamado *Direct Client-to-Client* (*DCC*).

- **Un bot DDoS o agente DDoS,** herramientas DDoS como *Stacheldraht* y *TFN* comúnmente son encontradas en los blended threats y podrían ser gestionadas por Firedaemon en Windows o *inetd*/*cron* en Unix.

- **Programas exploit locales,** permitirían al atacante tener derechos de administrador**.**

- **Programas exploit remotos,** pueden ser usados para extender el alcance del atacante en la red o usar hosts como stepping stone.

- **Limpieza de registros del sistema**, para ocultar los rastros dejados por el atacante**.**

- **Programas Troyanos,** permiten proveer de puertas traseras para retomar el acceso o realizar cambios en comandos del sistema. Por ejemplo, en sistemas Unix *ifconfig es* remplazado para ocultar el hecho de que la interfaz de red se encuentra en modo promiscuo.

- **Sniffers,** permiten a un atacante analizar el tráfico que circula por la red.

El scanning puede ser realizado con programas separados, que son simplemente conectados al kit blended threat o como en el caso de Phatbot, desarrollados en el mismo programa como módulo. Un scanning IRC bot es representado en la Figura 2-20.

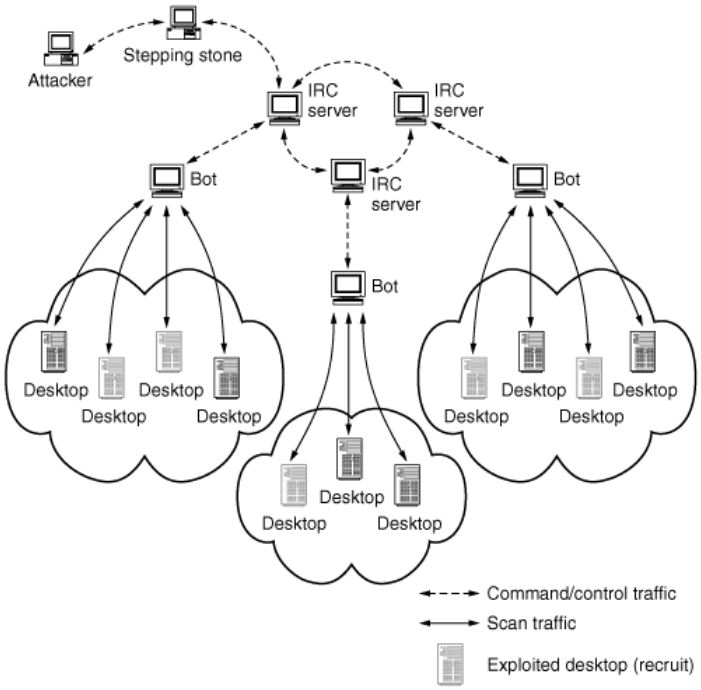


Figura 2. 20 Scanning sofisticado para reclutamiento[62]

Otra forma de realizar scanning para identificar máquinas vulnerables es un gusano, el cual, es un programa automatizado que se propaga desde una máquina vulnerable a otra.

Un gusano tiene 3 funciones primarias distintas:

1) Scanning, para buscar máquinas vulnerables.
2) Exploitation, el cual compromete máquinas y establece un control remoto.
3) Payload, código que se ejecutan con el objeto de lograr alguna función de ataque.

Ya que un gusano está diseñado para propagarse, una vez que infecta a la máquina, el ciclo de escaneo/infección se repite tanto en la máquina como en las máquinas infectadas.

El payload puede ser simplemente una copia del gusano o puede ser un completo set de programas cargados en el sistema de archivos. Los gusanos de internet

[62] http://denialofservice.uw.hu

son el método cada vez más popular de reclutar agentes DDoS, por lo que el payload frecuentemente incluye el código del ataque DDoS.

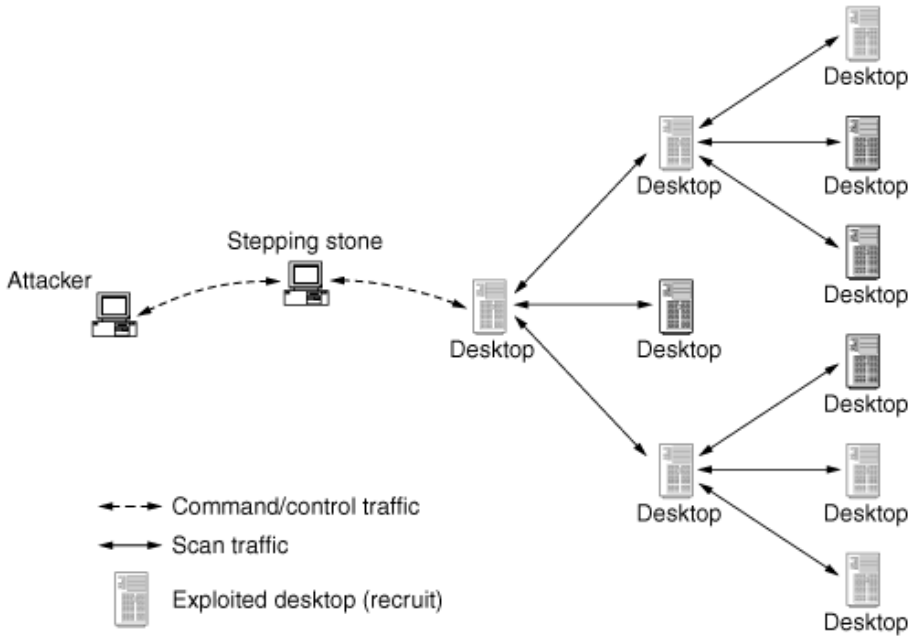


Figura 2. 21 Reclutamiento por gusanos[63]

Los gusanos eligen las direcciones para escanear usando varios métodos, como:

a) Aleatoria: Aleatoriamente se elige todos los 32 bits de una dirección IP (Si se usa IPv4), escaneando enteramente la red internet indiscriminadamente.
b) Rango de direcciones aleatorias: Aleatoriamente se eligen únicamente los primeros 8 o 16 bits de la dirección IP y se escanean las direcciones comprendidas en el rango dado.

c) Por lista: Se usa una lista de direcciones potenciales para ser escaneadas, haciendo caso omiso de cualquier rango de direcciones que parece estar vacías o altamente seguras.

d) Información encontrada en máquinas infectadas: Al ser una máquina infectada, el gusano examina el registro de la máquina con detalles de

[63] http://denialofservice.uw.hu

comunicación en busca de direcciones para escanear. Por ejemplo, un registro de explorador Web contiene direcciones de sitios Web visitados recientemente, y un archivo known_hosts contiene las direcciones de los destinos contactados a través del protocolo SSH (Secure Shell).

2.6.3 UTILIZACIÓN DE LA VULNERABILIDAD PARA ACCEDER A LA MÁQUINA

El atacante necesita explotar una vulnerabilidad en la máquina que pretende reclutar para ganar el acceso, es decir, tomar control de la máquina. Sin embargo, los exploits típicamente siguen un ciclo de vida de explotación de vulnerabilidades que decaen al momento en el que aparece y se aplica un parche para tal vulnerabilidad.

Una vez que una o más vulnerabilidades han sido descubiertas, el atacante incorpora los exploits para esas vulnerabilidades en su toolkit DDoS. De hecho, algunas herramientas DDoS toman ventaja de varias vulnerabilidades para propagar su código a tantas máquinas como sea posible.

Para facilitar su acceso, el atacante ejecuta un programa que se mantiene a la escucha de intentos de conexión entrantes en un puerto específico. Este programa es denominado como backdoor.
Una vulnerabilidad que no puede ser mitigada por parches y que algunos blended threats toman ventaja, son los passwords débiles. Algunos exploits contienen una lista de passwords comunes y usan estos paswwords en fuerza-bruta o de manera iterativa, una después de otra.

Esto algunas veces causa que el sistema exceda el límite de intentos y cause una condición de bloqueo, una forma de seguridad para el sistema, pero perjudicial para usuarios legítimos ya que no pueden acceder al sistema.

2.6.4 INFECCIÓN DE LA MÁQUINA CON EL CÓDIGO DEL ATAQUE[64]

El atacante necesita decidir el modelo de propagación para instalar su código malicioso, pudiendo ser: central repository o cache, back-chaining o pull y tel autonomous, push, o forward propagation.

2.6.4.1 Central repository o cache

El atacante coloca el malware en un repositorio de archivos como por ejemplo: Un servidor FTP o un sitio Web y cada host comprometido descarga el código de éste repositorio. Atacantes que instalan agentes trinoo y Shaft usan tales métodos centralizados.

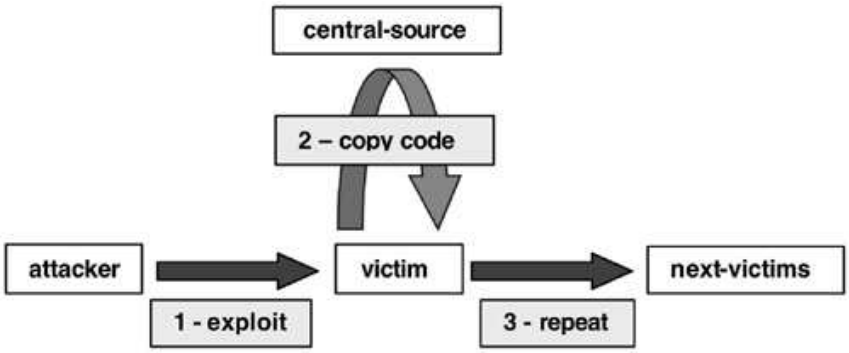


Figura 2. 22 Propagación con central repository[64]

2.6.4.2 Back-chaining or pull

El atacante lleva sus herramientas desde un host inicialmente comprometido a otros que este host compromete.

---

[64] CERT, Kevin J. Houle, George M. Weaver, Trends in Denial of Service, Octubre del 2001, Attack Technology, http://www.cert.org/archive/pdf/DoS_trends.pdf.

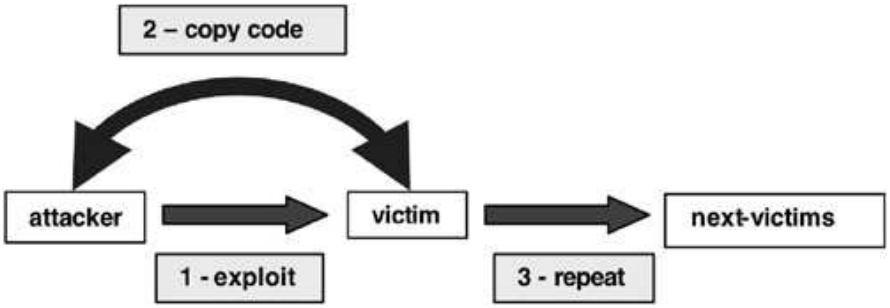


Figura 2. 23 Propagation with back chaining[64]

2.6.4.3 Autonomous, push o forward propagation

Combina en un solo proceso propagación y exploit. La diferencia con back chaining es que en lugar de realizar una copia de dicho malware después de haber comprometido un host, el exploit por si mismo contiene el código malicioso a ser propagado al siguiente host.

El gusano lleva una herramienta DDoS como payload, y lo planta en cada máquina infectada.

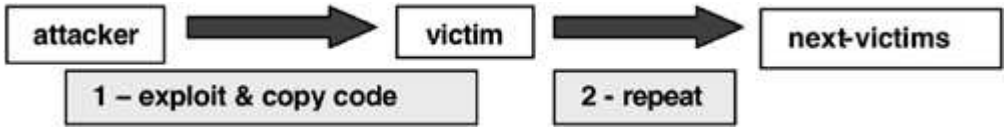


Figura 2. 24 Figura 2-29 Propagación Autonomous[64]

En la actualidad, gusanos han incorporado encripción en el exploit y código de ataque. La encripción es usada para prevenir la detección de exploit con secuencias de código conocidos por antivirus o firewalls.

2.6.5 EJECUCIÓN DEL ATAQUE

Una vez que se han reclutado un gran número de agentes, el atacante se comunica con ellos usando herramientas que le permitan controlar el ataque, recoger estadísticas sobre el comportamiento de los agentes y definir los detalles del ataque.

2.6.5.1 Comandos Directos

Algunas herramientas como trinoo crean una red handler/agente, en el que el atacante controla la red enviando comandos al handler. Los comandos pueden ser enviados en texto claro, cifrados, o en secuencias numéricas de bytes.

Para que algunos handlers y agentes como trinoo, Stacheldraht y Shaft puedan funcionar, el hanlder debe aprender las direcciones de los agentes y recordarlos después de un reinicio ya sea del computador o del programa.

Usualmente la lista de agentes se guardan en un archivo que el handler mantiene y lo usa para mantener información del estado acerca de la red DDoS, en algunos casos no existe autenticación del handler , de hecho, cualquier computador puede enviar comandos a algunos agentes DDoS y éstos responderán[65].

Los atacantes a veces toman el control de otra red DDoS[66]. Algunas herramientas que usan una arquitectura handler/agente protegen el acceso remoto al handler usando passwords y algunos tratan de proteger la comunicación handler/agente con passwords o cifrado.

Los handlers incluso encriptan su lista de agentes usando cifradores RC4 y Blowfish para evitar la divulgación de la identidad de los agentes ya que podrían ser expuestos enviando determinados comandos.

Otras herramientas como Stacheldraht permiten encripción entre el atacante y el handler, pero no entre handlers y agentes. Con el paso del tiempo estos handlers se pudieron rastrear y en muchos casos remover.

---

[65] Análisis de trinoo, TFN, Stacheldraht, Shaft y Mstream mostraron formas en las que tanto handlers y agentes podrían ser detectados o controlados.

[66] Análisis de trinoo, TFN y Stacheldraht mostraron debilidades que podrían ser usadas para tomar el control de la red DDoS.

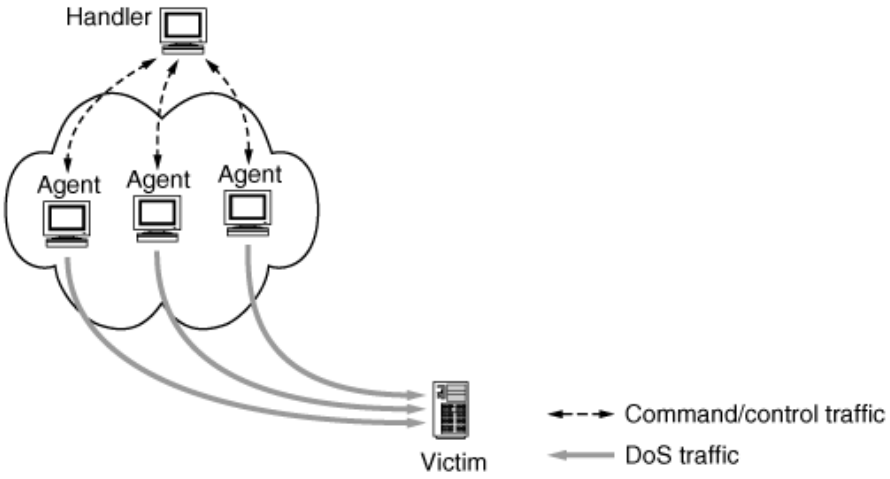


Figura 2. 25 Tráfico de control visto desde el lado del agente[67]

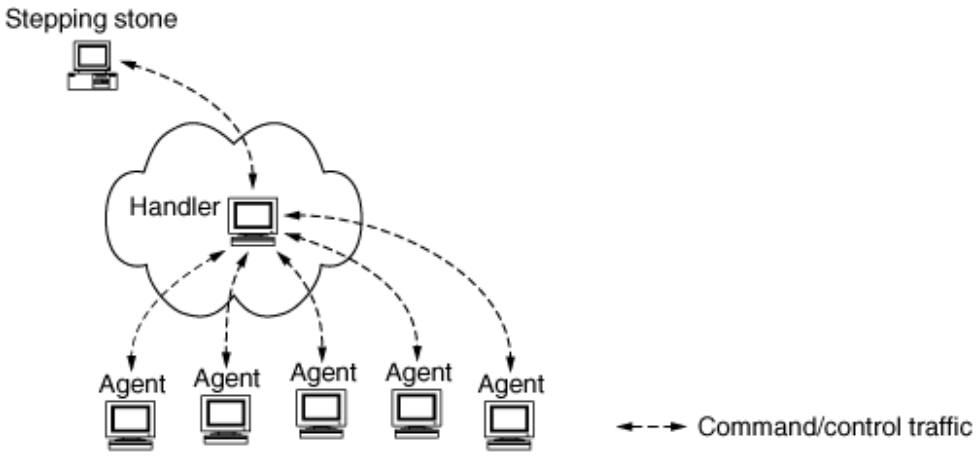


Figura 2. 26 Tráfico de control visto desde el lado del handler[67]

Una comunicación directa tiene algunas desventajas para un atacante, debido a:

- Los handlers necesitan almacenar la identidad de los agentes y frecuentemente una máquina agente almacena la identidad del handler, por lo que si una máquina es descubierta por el investigador toda la red DDoS podría ser identificada.
- Los patrones de comunicación directa generaban eventos anómalos que un administrador de red podría fácilmente identificar.

[67] http://denialofservice.uw.hu

- Tanto agentes como handlers tienen que estar en estado de listo para recibir mensajes, razón por la cual, los administradores de red pueden identificarlos rápidamente, visualizando la lista de puertos abiertos y procesos no identificados.

- El atacante necesita escribir su propio código de mando y control.

- Muchas versiones de Unix tienen límites en el número de descriptores de archivos abiertos que cada proceso puede tener. Incluso si estos límites puede ser aumentados, algunas herramientas DDoS simplemente no podrían ser capaces de añadir nuevos agentes después de llegar a 1024, límite típico para muchos sistemas operativos.

2.6.5.2 Comandos Indirectos

En lugar de ejecutar un programa que se mantenga a la escucha de conexiones entrantes en un puerto específico, tanto los agentes DDoS (bots) como el atacante se conectan a un servidor IRC como cualquier otro cliente de IRC. Como la mayoría de los sitios permiten IRC como canal de comunicación para los usuarios, la comunicación DDoS no crea eventos anómalos.

El rol del handler es interpretado por un simple canal en un servidor IRC, usualmente protegido con un password. Típicamente hay un canal por defecto en el código del bot, al cual se conecta inicialmente para aprender donde está realmente localizado el canal de control actual. Cambios de canal, incluso a través de redes IRC puede ser implementado de ésta manera.

Una vez en el actual canal de control, los bots están listos para responder a los comandos del atacante para escanear, realizar ataques DDoS, actualizarse ellos mismos, cerrarse, entre otros.
La ventaja que tiene el atacante al comunicarse vía IRC son:

- El servidor se encuentra ya ahí y es mantenido por otros.

- El canal no es fácilmente descubierto dentro de miles de otros canales de chat, incluso al ser descubierto, el canal puede ser removido únicamente con la cooperación de los administradores del servidor, el cual puede ser difícil de obtener en el caso de servidores extranjeros.

- Debido a la naturaleza distribuida de IRC, no todos los clientes tienen que tener acceso al mismo servidor de IRC para llegar al "canal handler", sólo tienen que acceder a un servidor que este en la misma red de IRC o alianza.

La mayoría de herramientas que aparecieron después de Trinity, toman ventaja de este mecanismo de comunicación alternativa.

Otra forma de stepping Stone para comunicaciones basadas en IRC, es que los atacantes regularmente comprometen máquinas y los convierten en servidores IRC, a menudo usando los puertos no estándar, en lugar del típico 6667/tcp que usualmente utilizan los servidores IRC. Otra forma es convertir algunos bots por proxis TCP en puertos no estándar, que a su vez se conecta a un servidor IRC real en puertos estándar.

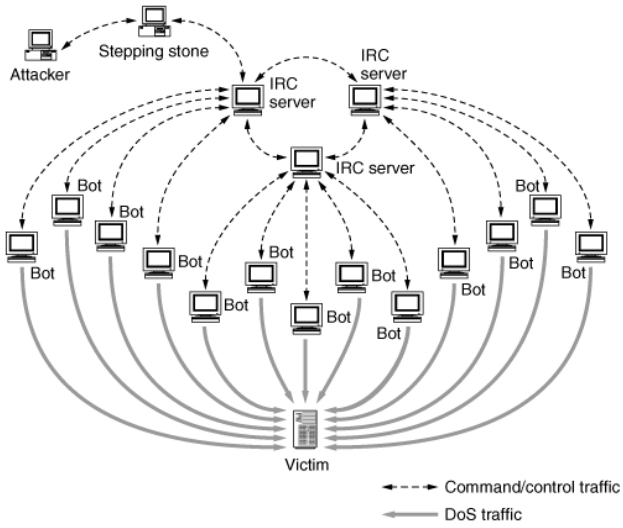


Figura 2. 27 Comunicación del atacante con los agentes (bots) por IRC

2.6.5.3 Fase de Ataque

Algunos ataques son previamente programados en el código que han sido propagados. Sin embargo, la mayoría de ataques ocurren cuando un atacante difunde un comando desde su handler a los agentes.

Dependiendo del tipo de herramienta de ataque usada, el atacante puede o no ser capaz de detener el ataque en curso. La duración del ataque es especificada en el comando del ataque o controlada por valores de las variables por defecto.

A continuación se comentan los ataques de denegación de servicio distribuido (DDOS) más conocidos en la actualidad.

2.7 ATAQUES DISTRIBUIDOS DE DENEGACIÓN DE SERVICIO (DDOS)

Comúnmente los atacantes usan códigos ya escritos por otros y estos códigos son típicamente integrados de forma conjunta en un paquete fácil de usar llamados como herramientas de ataque y usualmente con scripts que automaticen la instalación, llamados blended threats como se vio anteriormente.

2.7.1 HERRAMIENTAS DE ATAQUE

Actualmente se conocen cinco herramientas de ataque distribuidas de denegación de servicio, como son: Trinoo, Tribe Flood Network, Stacheldraht, Shaft y Mstream.

2.7.1.1 Trinoo

Trinoo es un conjunto de herramientas utilizadas para sincronizar equipos que cooperen de forma distribuida, mediante un modelo jerárquico maestro/esclavo (máster/Slave).

El componente maestro es el que realmente realiza el ataque y suele ser instalado de forma secreta en un ordenador denominado Zombie, por ejemplo, es capaz de realizar un ataque UDP Flood a un equipo específico, el cual intentará procesar y responder a cada paquete UDP con mensajes ICMP de Puerto inalcanzable.

El componente cliente se utiliza para controlar al componente principal y permite que los atacantes controlen múltiples componentes maestros de forma remota, mediante el envío de comandos.

W32.DoS.Trinoo es una versión compilada del componente maestro para Windows y también puede ser compilado para plataformas Unix como Linux.

En el caso de Windows cuando W32.DoS.Trinoo se ejecuta, se copia en el directorio \Windows\sistem como service.exe y modifica el registro para ejecutarse cada vez que se inicie el equipo. Una vez que W32.DoS.Trinoo esté en memoria se mantiene a la escucha de un comando desde el componente cliente Trinoo para realizar las tareas asociadas.

En general, una vez obtenido el acceso a un ordenador que disponga de un gran ancho de banda y pueda pasar desapercibido, se procede a la instalación/compilación de todos los programas del proyecto TRINOO (sniffers de red, puertas traseras o backdoors, daemons, root-kits), para luego realizar un rastreo (scanning) de otros ordenadores con vulnerabilidades conocidas en servicios básicos e infectarlos de igual manera y así poder distribuir las herramientas.

Para poder verificar si un ordenador fue infectado, el ordenador de origen suele tener un proceso demonio (daemon) que se encuentra a la escucha del puerto TCP 1524, al cual se enviará una señal por cada ordenador infectado. Otra variante es que cada máquina infectada envíe un e-mail. De ésta forma el atacante puede mantener una lista de los ordenadores que tiene bajo su control.

El diagrama de tres capas utilizado en TRINOO permite que con una infraestructura mínima y sencilla se llegue a controlar un poderoso conglomerado de ordenadores conectados a Internet.

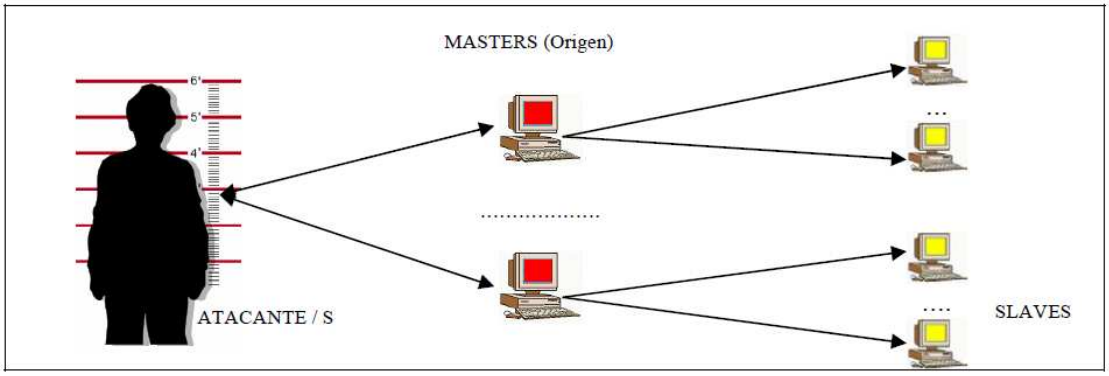


Figura 2. 28 Esquema TRINOO[68]

La comunicación entre las diferentes capas se realiza mediante conexiones TCP para atacante/master, y conexiones UDP para master/slave y slave/master a puertos específicos de cada máquina.

Los demonios de TRINOO situados en los equipos master y slave permiten la ejecución de comandos para iniciar, controlar y detener ataques de denegación tradicionales como ICMP Flooding, SYN Flooding, UDP Flooding, Smurf, entre otros. Para acceder a estos comandos, el atacante realizará una conexión Telnet a los siguientes puertos especificados.

	ATACANTE	MASTER	SLAVE
ATACANTE		27665/TCP	
MASTER			27444/UDP
SLAVE		31335/UDP	

Figura 2. 29 Esquema de Comunicaciones entre las capas de TRINOO

Los comandos aceptados por los demonios de TRINOO son:

[68] Fernando Limón Martínez, Sistemas Distribuidos De Denegación de Servicio, Madrid Junio del 2000, http://fi.upm.es/~flimon

2.7.1.1.1 Comandos Master

- Die, Apagar el servicio.
- Quit, Finalizar la conexión al servicio.
- Mtimer, Indica el tiempo de ataque DDOS en segundos.
- dos IP, Iniciar ataque DDOS sobre la dirección IP especificada.
- mdie passwdord, Parar broadcasts si el password especificado es correcto.
- Mping, Realizar un ping a cada máquina “activa”.
- mdos ip1:ip2:ip3, Realizar un ataque DDOS múltiple sobre las direcciones IP.
- Info, Visualizar información de la versión y opciones.
- Msize, Indicar el tamaño del buffer de los paquetes utilizados en DDOS.
- nslookup host, Realizar una resolución de nombres (DNS).
- Killdead, Elimina los esclavos no activos de la lista.
- Usebackup, Carga la lista de esclavos activos creada por ‘killdead’
- Bcast, Visualizar todos los ordenadores activos en la lista.
- help comando, Proporciona ayuda sobre los comandos disponibles.
- mstop, Finalizar un ataque DDOS (en algunas versiones NO funciona).

2.7.1.1.2 Comandos Slave

- aaa password IP, Realizar DDOS enviando paquetes UDP a la dirección IP.
- bbb password N, Indica el tiempo máximo en segundos del ataque DDOS.
- shi password, Envía la cadena "*HELLO*" a la lista de masters.
- png password, Envía la cadena "PONG" al master que envió el comando.
- d1e password, Finalizar el demonio (daemon).
- rsz size, Especificar el tamaño del los paquetes enviados en el DOS.
- xyz password 123:ip1:ip2:ip3, Realizar DDOS sobre las direcciones IP.

2.7.1.2 Tribe Flood Network

Conocido también como TFN, está compuesto por un conjunto de programas

clientes y demonios que le permiten realizar ataques por generación masiva de paquetes ICMP, SYN o UDP y al tener acceso a un “shell de root” mediante la instalación de un daemon que se mantiene a la escucha en un puerto TCP requerido, permite tener acceso al ordenador atacado cada vez que se desee.

Generalmente una red TFN está formada por Atacantes, Clientes y Demonios, como la reflejada en la Figura 2.30.

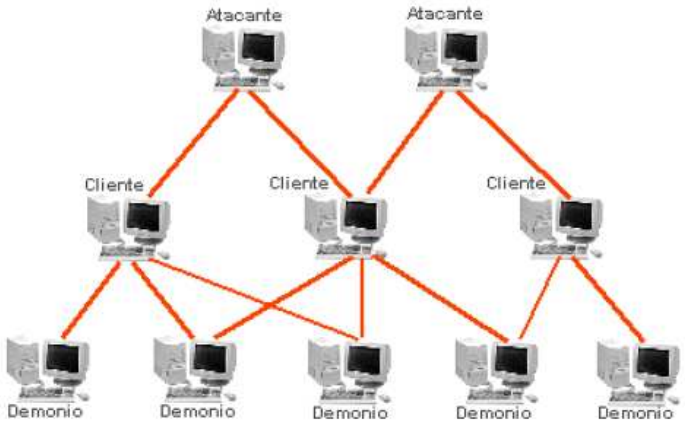


Figura 2. 30 Estructura TFN[69]

El funcionamiento de TFN es muy parecido a TRINOO, diferenciándose entre la parte “client” o cliente que en TRINOO son los masters y la parte de “daemons” o demonios que en TRINOO serían los denominados slaves, además no existe una comunicación basada en TCP o UDP, la comunicación entre los clientes y los demonios se realiza mediante paquetes ICMP_ECHOREPLY.

El atacante entonces controlará a uno o más clientes y cada cliente controlará a una gran cantidad de demonios. Los demonios son los que reciben la orden de realizar un ataque coordinado contra una o más víctimas.

El control de la red TFN se consigue mediante la ejecución directa de comandos enviados a los clientes, los cuales pueden transmitirse por shell remoto a un determinado puerto TCP, basado en: conexiones UDP cliente/servidor,

[69] Fernando Limón Martínez, Sistemas Distribuidos De Denegación de Servicio, Madrid Junio del 2000, http://fi.upm.es/~flimon

conexiones ICMP cliente/servidor, sesión SSH, o un simple Telnet a un puerto TCP.

Aunque el acceso no está protegido para los clientes, los comandos que el cliente envía a los demonios van codificados en forma de número binario en el campo ID del paquete ICMP_ECHO_REPLY, siendo fijo el número de secuencia del paquete: 0x0000, lo que puede hacer que parezca como el primer paquete generado por un comando ping.

Tanto los clientes como los demonios necesitan ser ejecutados con privilegio de root y adicionalmente, el cliente necesita disponer del fichero en el que se encuentra la lista de direcciones IP de los demonios (iplist). En las últimas versiones se ha detectado tratamiento criptográfico en el fichero iplist mediante Blowfish. Los comandos definidos son:

#define ID_ACK 123 /* respuestas al cliente */
#define ID_SHELL 456 /* unirse a un rootshell */
#define ID_PSIZE 789 /* cambiar el tamaño de los paquetes udp/icmp */
#define ID_SWITCH 234 /* cambiar a modo spoofing */
#define ID_STOPIT 567 /* parar la inundación*/
#define ID_SENDUDP 890 /* udp flood */
#define ID_SENDSYN 345 /* syn flood */
#define ID_SYNPORT 678 /* setear el número de puerto */
#define ID_ICMP 901 /* icmp flood */
#define ID_SMURF 666 /* haps! haps! */
El cliente TFN admite los siguientes parámetros:

./tfn <lista_ip> <tipo> [ip] [port]

<lista_ip>, Contiene la lista de direcciones IP a atacar.
<tipo> -1, Tipo de máscara (spoofmask type)
0, Para stop/status.
1, Para realizar UDP Flooding

2, Para realizar SYN Flooding.

3, Para realizar ICMP Flooding.

-2, Tamaño de los paquetes a enviar.

4, Realizar un “root shell” (se debe especificar en que puerto)

5, Realizar un ataque SUMRF, la primera IP es la dirección de origen y las demás son usadas como direcciones de broadcast.

[ip], Dirección de origen (separadas por @ si hay más de una).

[port], Debe especificarse para SYN Flood (0 =aleatorio).

Uno de los puntos fuertes de TFN radica en que muchas herramientas de monitorización de redes no analizan todo el abanico de paquetes del tipo ICMP o simplemente no muestran la parte de datos de estos paquetes, por lo que la detección de éstos puede resultar compleja.

2.7.1.3 Tribe Flood Network 2000 (TFN2K)

Es la herramienta más sofisticada descubierta hasta el momento. TFN2K es una evolución de TFN y aunque su estructura es similar, cambia su terminología. Se denomina Maestro al sistema informático en el que corre el Cliente, y Agente al sistema informático donde se ejecuta el Demonio.

TFN2K hace uso de inundación de paquetes al igual que TFN y permite a los Maestros explotar los recursos de un determinado número de Agentes con el fin de coordinar un ataque a una o más víctimas.

La comunicación entre el Maestro y el Agente se realiza de forma cifrada mediante el algoritmo CAST-256 (RFC-2612). La clave se define en el momento de realizar la compilación, y se utiliza como clave de acceso cuando se ejecuta el cliente.

Todos los datos cifrados se codifican en Base 64 antes de ser transmitidos, se falsifica la dirección IP del maestro (spoof) y se mezcla con una serie de tramas trampas enviadas a direcciones IP aleatorias para complicar un posible rastreo.

Tanto la comunicación Maestro/Agente como el ataque en sí mismo puede realizarse utilizando de forma aleatoria paquetes TCP, UDP o ICMP.

Al contrario de su predecesor, TFN2K es absolutamente silencioso y no contesta a los comandos que recibe. Los comandos no se basan en secuencia de caracteres, sino que van codificados en un byte, viajando como datos de la trama los parámetros particulares de cada comando.

El agente de TFN2K intenta ocultarse cambiando el contenido de argv[0], es decir, cambiando el nombre del proceso. El nombre falso se define en el momento de compilación y puede variar de unas instalaciones a otras. Esto le permite camuflarse como un proceso normal, por lo que difícilmente podrá detectarse en una simple revisión de la tabla de procesos activos.

Se han encontrado agentes en plataformas Linux, Solaris e incluso Windows NT y es fácilmente portable a otras plataformas.

2.7.1.4 Stacheldraht

El término de origen alemán Stacheldraht, podría traducirse por alambre de espino o alambrada de espinos y fue detectada en sistemas Solaris. Un posterior análisis de las fuentes ha demostrado que también puede ser ejecutado en entornos Linux.

Combina características de Trinoo y TFN, añadiendo algunas características más sofisticadas como el cifrado en la comunicación así como mecanismos de actualización automática de los agentes.

Mantiene una jerarquía parecida a Trinoo dónde a los master ahora se los denomina handlers, manipuladores o controladores y a los demonios/daemons se los denomina agents o agentes.

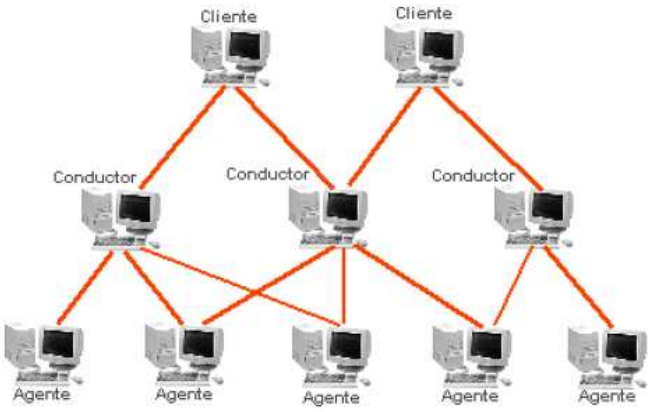


Figura 2. 31 Estructura de STACHELDRAHT[70]

Algunos analistas consideran a Stacheldraht como la competencia directa de TFN2K, pues presentan muchas similitudes en cuanto a su comportamiento y facilidades como inundación de paquetes ICMP, SYN y UDP.

A diferencia de TFN Stacheldraht no proporciona un "shell de root" en las máquinas infectadas, pero dispone de un mecanismo similar a un Telnet (Stacheldraht Term) para la comunicación del cliente con el conductor que incluye cifrado mediante el uso de clave simétrica y una vez establecida la comunicación entre cliente/conductor, se solicita un password que está cifrado mediante crypt().

A partir de ese momento toda la comunicación se realiza de forma cifrada mediante el algoritmo Blowfish. De esta forma, el uso de técnicas de cifrado dificulta la detección de los ordenadores Infectados.

A diferencia de las herramientas TRINOO que usan UDP para las comunicaciones entre master/slave y TFN que utiliza ICMP entre clients/daemons, STACHELDRAHT utiliza los protocolos ICMP y TCP indistintamente para las comunicaciones entre handlers/agentes

La comunicación entre Cliente/Conductor acepta un único argumento que es la dirección del handler, con el que se conecta usando el puerto 16660/TCP. La

[70] Fernando Limón Martínez, Sistemas Distribuidos De Denegación de Servicio, Madrid Junio del 2000, http://fi.upm.es/~flimon

comunicación entre Conductor/Agente usa el puerto 65000/TCP, ICMP_ECHOREPLY

Como todos los programas de este tipo, también tiene la capacidad de modificar su nombre y argumentos para no ser detectado y aparecer como un proceso corriente del sistema.

Otra diferencia que presenta Stacheldraht respecto a otras herramientas como Trinoo y TFN es la posibilidad de actualización de los agentes, haciendo uso del comando rcp que trabaja en el puerto 514/tcp. Primero se descargan los nuevos binarios y se eliminan los antiguos ejecutables para finalmente ejecutar los nuevos con la señal de sistema NOHUP.

En el momento de arranque de un agente, éste primero intenta leer un fichero de configuración en el que se le indica qué conductores le pueden controlar. Este fichero contiene una relación de direcciones IP y está cifrado mediante Blowfish. Para los casos en que falle la localización del mencionado fichero, el propio agente lleva definido en el código una serie de direcciones que debe usar por defecto.

Una vez que el agente ha arrancado y dispone de la lista de conductores, comienza a transmitir tramas del tipo ICMP_ECHOREPLY con ID 666 y conteniendo en el campo de datos la palabra “skillz”.

Todos aquellos conductores que reciben esta trama contestan con otra del mismo tipo, con ID 667 y en el campo de datos la palabra “ficken” y el diálogo entre conductor y agente se mantiene de forma periódica. Lo que permite detectar la presencia de Stacheldraht mediante la monitorización pasiva de la red a través de un sniffer.

2.7.1.5 Shaft

Shaft es otra herramienta ampliamente conocida en los ataques de denegación de

servicio Distribuido. Su estructura es similar a TFN y se basa en la existencia de varios masters/handlers denominados “shaftmasters” que controlan a su vez a varios slaves/agents que pasan a denominarse “shaftnodes”.

El atacante se conecta haciendo uso de un programa cliente a los shaftmasters desde el cual inicia, controla y finaliza los ataques DDOS. SHAFT utiliza el protocolo UDP para el envío de mensajes entre los shaftmasters y shaftnodes.

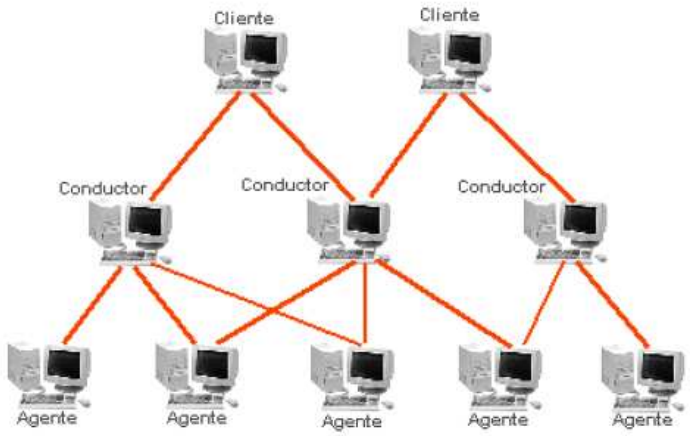


Figura 2. 32 Estructura Shaft[71]

La conexión de un atacante vía TELNET a un shaftmaster se realiza en texto plano (Sin cifrar) y una vez conectado se le pide un password para autorizar su acceso al sistema. Ya que Shaft hace uso del protocolo UDP que no es confiable, utiliza una técnica de tickets para mantener el orden de la comunicación y poder asignar a cada paquete un orden de secuencia.

La combinación del password y el ticket son utilizadas para el envío de órdenes a los Shafnodes para verificar que sean correctos antes de aceptarlos. Tanto el conductor como el agente disponen de su propio conjunto de comandos y el atacante sólo interactúa con el conductor mediante comandos a través de una conexión Telnet.

[71] Fernando Limón Martínez, Sistemas Distribuidos De Denegación de Servicio, Madrid Junio del 2000, http://fi.upm.es/~flimon

Shaft utiliza el cifrado de cesar, el cual se basa en substituir unos caracteres por otros y su comunicación entre los distintos niveles se realiza de la siguiente forma:

	ATACANTE	SHAFTMASTER	SHAFTNODE
ATACANTE		20432/TCP	
SHAFTMASTER			18753/UDP
SHAFTNODE		20433/UDP	

Figura 2. 33 Esquemas de Comunicaciones Shaft

La posibilidad de cambiar los números de los puertos dinámicamente hace que SHAFT sea difícilmente detectable por sistemas convencionales y al igual que las herramientas comentadas anteriormente, trata de esconderse cambiando su nombre de proceso y argumentos de llamada. Por defecto, intenta hacerse pasar por un servidor WWW cambiando su nombre por el de 'HTTP'.

A través del análisis del código fuente se ha detectado la existencia de un cliente por defecto, y definido de la siguiente forma: #define MASTER "23:/33/75/28", que restando 1 al valor decimal de cada caracter (Cifrador de Cesar) obtendremos la dirección IP 129.22.64.17, que corresponde a electrochem1.echem.cwru.edu.

Los autores de Shaft han demostrado tener un interés especial por disponer de estadísticas del ratio de generación de paquetes de cada uno de los agentes. Es posible que esta información les permita optimizar el número de agentes necesarios para ejecutar un ataque, o añadir más en caso de disminuir el nivel estimado de carga para que el ataque proporcione los resultados esperados.

2.7.1.5.1 Comandos de los shaftnodes

- size <tamaño>, Permite especificar el tamaño de los paquetes del DDOS.
- type <tipo_ataque>, Especifica el tipo de ataque a realizar:
    - 0 UDP Flooding
    - 1 TCP Flooding
    - 2 UDP/TCP/ICMP

    - 3 ICMP
- time <segundos>, Especifica la duración del ataque en segundos.
- own <direccion_ip>, Añade la dirección IP a la lista de máquinas a atacar.
- end <direccion_ip>, Elimina la dirección IP de la lista de máquinas a atacar.
- Stat, Visualizar las estadísticas de paquetes.
- Alive, Comprueba que shaftnodes del shaftmaster están activos.
- switch <h> <p>, Cambia la conexión al handler/shaftmaster en el puerto p.
- pktres <pwd><sock><tickt><ps>, Visualiza los paquetes enviados desde shaftnodes.

2.7.1.5.2 Comandos de los shaftmasters

- mdos <host>, Inicia un DDOS al ordenador especificado (envía “own host" a todos los shaftnodes.
- Edos <host>, Finaliza un DDOS al ordenador especificado (envía “end host" a todos los shaftnodes).
- time <segundos>, Especifica la duración en segundos del ataque.
- size <tamaño>, Especifica el tamaño de los paquetes (máximo 8Kbytes).
- type <tipo_ataque>, Especifica el tipo de ataque a realizar:
- UDP, Especifica UDP Flooding
- TCP, Especifica TCP Flooding
- ICMP, Especifica ICMP Flooding
- BOTH, Especifica UCP y TCP
- +node <ip>, Añade un nuevo shaftnode a la lista.
- -node <ip>, Elimina un shaftnode de la lista.
- ns <host>, Realiza una petición de resolución de nombre (DNS).
- Lnod, Listar todos los shaftnodes.
- Pkstat, Estadísticas de los paquetes enviados.
- Stat, Visualizar status global.
- Switch, Asignarse como shaftmaster de los shaftnodes.
- Ver, Visualizar versión

2.7.1.6 MStream

Su estructura es muy similar a los sistemas anteriormente citados, un módulo controlador encargado de gestionar las relaciones con los agentes y un módulo agente. De igual forma, un atacante se conectará con el controlador mediante una sesión Telnet para controlar a los agentes.

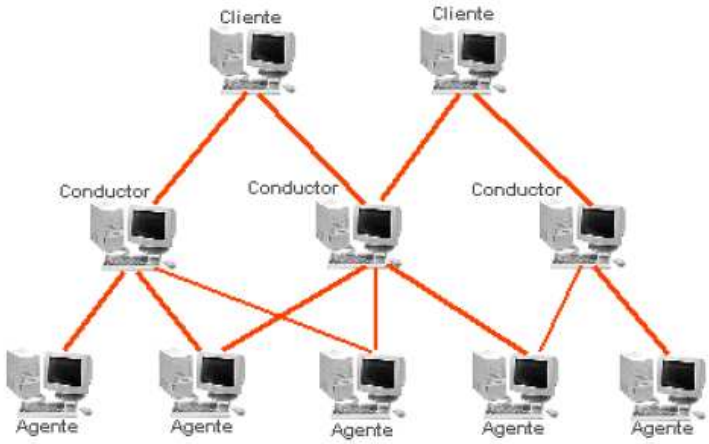


Figura 2. 34 Estructura Mstream[72]

El ataque que generan los agentes es una modificación del ataque conocido como “stream.c”, pues la mayor parte del código del agente se basa en dicho programa. El agente envía paquetes TCP ACK a la víctima, aunque con la particularidad que dichas tramas se encaminan a puertos seleccionados de forma aleatoria y conteniendo una dirección IP de origen falsa.

Al contestar con tramas TCP RST, el sistema atacado baja su rendimiento debido al consumo de CPU por el tráfico de red que debe atender y el rendimiento de la red se degrada. Los routers contestarán a la víctima con tramas ICMP, indicando que el destinatario de la trama TCP RST no existe, lo que también consume aún más ancho de banda.

[72] Fernando Limón Martínez, Sistemas Distribuidos De Denegación de Servicio, Madrid Junio del 2000, http://fi.upm.es/~flimon

La arquitectura de este sistema es similar a los anteriores. Cada conductor puede coordinar un gran número de agentes, cada agente puede estar coordinado por un gran número de conductores y adicionalmente necesitan poseer privilegio de root.

Se han encontrado tres versiones de esta herramienta, y en cada una de ellas varían los puertos y los passwords utilizados para la comunicación entre los distintos componentes.

Basándose en la versión, el conductor se encuentra a la escucha en el puerto 6723/TCP, el password de identificación es “sex” y se encuentra a la escucha en el puerto 9325/UDP para permitir que los agentes puedan registrarse.

Los agentes pueden transmitir dos tipos distintos de paquetes.

- pong, como respuesta a una petición “ping”.
- newserver, indicando que la dirección IP indicada se añade a la lista de agentes. Dicha lista se mantiene en el fichero “.sr”.

Las direcciones IP se codifican añadiendo 50 al valor ASCII de cada caracter de la dirección IP (Cifrador de Cesar).

Cada agente lleva incluido en el propio código la lista de posibles conductores autorizados, con un máximo de tres, lo que obliga a definirlos en el momento de compilar. Los agentes atienden por el puerto 7983/UDP los posibles comandos que les puedan transmitir los controladores. A parte del comando “ping” anteriormente citado, pueden recibir el comando “mstream”.

Existe también el comando “stream”, que es similar a “mstream”, pero que sólo permite lanzar el ataque a una única dirección IP, y en este caso la dirección IP del atacante es la real y no una falsa.

2.8 DETECCIÓN DE ATAQUES

Debido al diseño propio de los protocolos en no proveer de mecanismos válidos de autenticación sobre el origen de un paquete, en la actualidad no existe una solución ideal para evitar y detectar este tipo de ataques.

Sin embargo, con el uso de equipos especiales como: firewalls, herramientas, aplicaciones y siguiendo una serie de recomendaciones en lo posible se puede al menos evitarlos. Siendo la mejor solución, el de tomar todas aquellas medidas que permitan minimizar el riesgo ante éste tipo de ataques.

Entre algunas de las principales recomendaciones, se pueden citar las siguientes:

- Análisis y filtrado de paquetes, con el propósito de mantener la red de datos libre de paquetes falsificados y/o de tráfico de datos que no tengan relación con los servicios prestados en la red. A pesar de que esta medida no garantiza el ser víctimas de un ataque, facilitará el análisis y seguimiento de éste en caso de producirse.

- Uso del Ancho de Banda, especificar un ancho de banda máximo para ciertos tipos de tráfico de aplicaciones o servicios, permitirá detectar cuándo se está produciendo una anomalía, y de esta forma tomar las contramedidas oportunas.

- Herramientas de Auditoría, mediante un conjunto de procedimientos y técnicas permitirán evaluar y detectar las situaciones de debilidad o fortaleza de un sistema informático para su posterior control, con el fin de constatar si sus actividades son correctas de acuerdo a las normativas fijadas en la organización.

En la actualidad, se ha puesto mayor énfasis en la elaboración de herramientas de auditoría para intentar detectar la presencia de éstos sistemas conocidos como Denegación de Servicio y poder prevenirlos. Incluso, algunos antivirus han

incorporado la posibilidad de detectarlos. Pero lamentablemente, van quedando obsoletos al ir apareciendo nuevos o variantes.

2.8.1 SISTEMAS DE DETECCIÓN DE INTRUSOS o IDS

Un sistema de detección de intrusos o IDS (Intrusion Detection System) es una herramienta de seguridad para auditoría que permite detectar o monitorizar el tráfico en la red y así poder descubrir actividades anormales o sospechosas de accesos no autorizados y reducir el riesgo de intrusión que puedan comprometer la seguridad de un sistema. Un IDS no sólo analiza el tipo de tráfico, también revisa el contenido y su comportamiento.

El tráfico de red es comparado con firmas de ataques conocidos, comportamientos sospechosos o patrones previamente definidos, como puede ser: escaneo de puertos, paquetes malformados, entre otros. Dichas firmas permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.

Básicamente, existen tres tipos de sistemas de detección de intrusos que son:

2.8.1.1 N-IDS o *Network IDS*

Es un IDS basado en red que requiere de un hardware exclusivo y que su interfaz funcione en modo promiscuo, de modo que pueda capturar todo el tráfico que circula por la red, para así detectar si se produce alguna actividad maliciosa o anormal.

Generalmente, se suelen encontrar diversos IDS en diferentes partes de la red y son colocados, tanto fuera como en el interior de la red, para analizar aquel tráfico que haya pasado a través del firewall o que se han realizado desde el interior.

2.8.1.2 H-IDS o *Host IDS*

Se encuentra en un host particular y actúa como un daemon o servicio, detectando modificaciones en el equipo afectado, para luego hacer un reporte de sus conclusiones. Analizan la información almacenada en registros de sistema, mensajes, logs, entre otros.

Adicionalmente, captura paquetes de la red que ingresan o salen del host, para verificar las señales de intrusión. Fueron los primeros IDS desarrollados por la industria de la seguridad informática.

2.8.1.3 DIDS o Distributed Intrusion Detection System

Sistema basado en la arquitectura cliente-servidor compuesto de múltiples NIDS que actúan como sensores, centralizando la información de posibles ataques en una unidad que puede almacenar o recuperar los datos de una base de datos centralizada. La ventaja es que en cada NIDS se puede fijar reglas de control para cada segmento de red.

2.8.2 SENSORES

Los IDS hacen uso de sensores, los cuales son elementos pasivos encargados de examinar el tráfico que circula por un segmento de red, pudiendo clasificarse en sensores pull y push.

Los sensores Push al detectar un determinado evento, crean un paquete y lo envían a la consola, por el contrario, los sensores Pull almacenan los eventos detectados hasta que la consola los requiera. La consola será la encargada de recibir la información de los sensores para mostrarla de forma ordenada y entendible al auditor.

Al analizar las muestras obtenidas por la consola se pueden encontrar dos tipos de detección denominadas como: Falsos Positivos o Falsos Negativos.

Los Falsos Positivos refieren a un fallo en la detección, pudiendo no existir realmente. Los Falsos Negativos hacen referencia a un fallo en el sistema que al haber una detección, esta es ignorada o no detectada.

Entre las principales características de un N-IDS se tiene:[73]

- **Reconfiguración de dispositivos externos (firewalls o ACL en routers)**: Comando enviado por el N-IDS a un dispositivo externo (como un filtro de paquetes o un firewall) para que se reconfigure inmediatamente y así poder bloquear una intrusión. Esta reconfiguración es posible a través del envío de datos que expliquen la alerta (en el encabezado del paquete).

- **Envío de una trampa SNMP a un hipervisor externo**: Envío de una alerta (y detalles de los datos involucrados) en forma de un datagrama SNMP a una consola externa como HP Open View Tivoli, Cabletron, Spectrum, entre otros.

- **Envío de un correo electrónico a uno o más usuarios**: Envío de un correo electrónico a uno o más buzones de correo para informar sobre una intrusión seria.

- **Registro del ataque**: Se guardan los detalles de la alerta en una base de datos central, incluyendo información como el registro de fecha, la dirección IP del intruso, la dirección IP del destino, el protocolo utilizado y la carga útil.

- **Almacenamiento de paquetes sospechosos**: Se guardan todos los paquetes originales capturados y/o los paquetes que dispararon la alerta.

- **Apertura de una aplicación**: Se lanza un programa externo que realice una acción específica (envío de un mensaje de texto SMS o la emisión de

[73] Stella, una honeypot virtual de alta interacción para windows xp, Beatriz Martínez Santos, Julio del 2009

una alarma sonora).

- **Envío de un "*ResetKill*"**: Se construye un paquete de alerta TCP para forzar la finalización de una conexión (sólo válido para técnicas de intrusión que utilizan el protocolo de transporte TCP).

- **Notificación visual de una alerta**: Se muestra una alerta en una o más de las consolas de administración.

2.8.3 SISTEMAS DE PREVENCIÓN DE INTRUSOS o IPS

En la actualidad, un sistema de prevención de intrusos o IPS viene a sustituir al IDS tradicional. La diferencia principal que distingue a un IDS (de red) de un IPS (de red) radica en que un IPS no sólo escucha pasivamente a la red para luego enviar alertas sobre actividades sospechosas, adicionalmente tiene la habilidad de bloquear y filtrar inmediatamente las intrusiones, sin importar el protocolo de transporte utilizado y sin reconfigurar un dispositivo externo.

En general un IPS es un sistema de prevención y protección. Presentan una mejora importante sobre los cortafuegos o firewalls tradicionales, ya que toman decisiones basadas en el contenido del tráfico, inspeccionando el flujo de datos en su totalidad, desde la capa 2 a la capa 7 del modelo OSI.

Para ello, se cargan filtros con un conjunto de reglas y condiciones que deben cumplir los paquetes o flujo de datos. Si una nueva vulnerabilidad o paquete malicioso es detectado, se crea un nuevo filtro específico y se lo añade al IPS.

Estos sistemas permiten realizar procesamiento en paralelo, ejecutando miles de chequeos simultáneamente, de modo que, un paquete puede ser procesado rápidamente e independiente del número de filtros que se apliquen. A diferencia de las soluciones de software convencionales que perjudican el rendimiento de la red debido al procesamiento en serie de los paquetes.

Adicionalmente, los IPS poseen técnicas de redundancia y failover, asegurando así, que la red se mantenga operativa en el caso de que se produzca un fallo; también son una excelente herramienta para mantener una red limpia de tráfico de datos no deseado y paquetes malformados, permitiendo incluso controlar y proteger el ancho de banda.

El funcionamiento de un IPS básicamente comienza clasificando los paquetes en base a la cabecera e información de flujo asociada y en función de éstos, los filtros relevantes son aplicados en paralelo. Los paquetes al ser identificados como sospechosos son etiquetados y posteriormente descartados.

Los IPS, aparecen como una solución ideal, sin embargo, presentan también una serie de desventajas y generan serios cuestionamientos sobre su efectividad, como son:

- Utilizan las mismas tecnologías de detección que los IDS.
- Generan puntos únicos de fallo.
- No permiten un modo de detección pasivo como en el caso de los IDS.
- Se pueden generar cuellos de botella si la carga de trabajo es excesiva.
- La capacidad reactiva de un IPS puede generar fácilmente situaciones de negación de servicio.

Si en la actualidad, los IDS tienen problemas de desempeño debido al volumen de datos que pueden llegar a procesar, si conocemos que los IPS no utilizan nuevas tecnologías y sabemos que son más reactivos ¿cómo esperar que éstos detengan eficazmente ataques mientras permite actividades legítimas?

Un sistema IPS ideal bloquearía siempre los ataques y nunca filtraría tráfico legítimo. Sin embargo, el problema de efectividad es serio y la efectividad de los sistemas IPS no dependen de su tecnología, sino del medio ambiente.

Por ejemplo, si un atacante falsifica el origen de un patrón de ataque, de forma que parezca un usuario legítimo, este sistema probablemente lo bloqueará (aun

cuando el patrón de detección del ataque sea correcto), es decir, si la entrada de datos que procesa este sistema es incorrecta desde el punto de vista del contexto, la salida (reacción) del sistema será por definición incorrecta (será sólo correcta para el IDS, dentro de su contexto).

Un IPS debería comprender la estructura de la organización, su proceso de negocio, la infraestructura tecnológica utilizada y demás detalles; es decir, todo el medio ambiente, algo que un ser humano podría hacerlo relativamente bien, pero lamentablemente estos sistemas que emularían por completo el comportamiento de un ser humano están aún muy lejos de nuestro alcance.

En conclusión, tantos los Sistemas IPS como IDS permitirían resolver problemas bien acotados y aquí es donde su efectividad se ha demostrado.

2.8.4 DETECCIÓN DE ATAQUES DDoS

La detección de ataques DoS es una tarea laboriosa y como fue comentado anteriormente en la actualidad no existe una herramienta específica para poder detectarlos. Sin embargo varias entidades y personas especializadas en el área han realizado herramientas, propuestas y recomendaciones que permiten facilitar la detección, por ejemplo:

- El National Infrastructure Protection Center (NIPC) de los Estados Unidos de Norteamerica, ha puesto a disposición pública la herramienta find_ddos[74]. Ésta herramienta busca a través de todo el sistema ficheros con presencia de Trinoo, TNF, TNF2K y Stacheldraht.

- Dave Dittrich y otros han desarrollado la herramienta gag[75] , que permite detectar la presencia de agentes de Stacheldraht. Otra herramienta

---

[74] National Infrastructure Protection Center (NIPC), Herramienta fins_ddos, http://www.fbi.gov/nipc/trinoo.htm

[75] Herramienta gag, http://staff.washington.edu/dittrich/misc/sickenscan.tar

desarrollada por los mismos especialistas es *dds*[76], que al igual que find_ddos permite la detección de agentes de Trinoo, TFN y Stacheldraht.

- Un grupo internacional que trata temas de seguridad en redes (RAZOR), también ha puesto a disposición pública la aplicación Zombie Zapper[77], el cual funciona para todas las herramientas y versiones de DDoS conocidas. Esta herramienta en particular, aunque no puede evitar el ataque permite pararlo, al indicar a un sistema que este generando un ataque Demonio/Agente que cese.

- El Instituto SANS, ha elaborado una serie de recomendaciones en una guía sobre las medidas de prevención que deben adoptarse[78].

2.9 MECANISMOS DE DEFENSA

Básicamente se tienen dos escenarios de protección ante un ataque de denegación de servicio: Se puede tratar de evitar el ataque en su totalidad o reaccionar de forma eficaz al ser detectado.

2.9.1 MEDIDAS PREVENTIVAS

Prevenir que un atacante lance el ataque o mejorar la capacidad, resistencia y habilidad de un sistema para evitar que el sistema caiga; serían las medidas preventivas a tomar ante un ataque de denegación de servicio. Ya que, dificultará a un atacante poder comprometer una máquina. Incluso, cualquier mejora en este ámbito beneficiará en la defensa contra muchas otras amenazas de seguridad como intrusiones y gusanos.

---

[76] Herramienta dds, http://staff.washington.edu/dittrich/

[77] Programa Zombie Zapper, http://razor.bindview.com/tools/index.shtml

[78] Guía del SANS Institute, http://www.sans.org/dosstep/index.htm

2.9.2 MEDIDAS DE REACCIÓN

En muchos casos la reacción es mejor que la prevención, ya que, máquinas nunca podrían experimentar un ataque de denegación de servicio o solo podrían ser atacadas en raras ocasiones. Si los ataques no son frecuentes y los costos de prevención son altos, podría ser mejor invertir menos en prevención y más en reacción.

Estar bien preparados para detectar y reaccionar ante un ataque DoS, será mucho más útil que cualquier cosa que se pueda adquirir o instalar. A diferencia de las medidas de prevención, las medidas de reacción requieren detección.

La eficacia en las medidas de reacción no sólo dependen de lo bien que puedan reducir el efecto del ataque, sino también, en la exactitud del sistema en determinar cuáles defensas son requeridas, cuando invocarlas y dónde implementarlas.

2.9.3 UBICACIONES DE DEFENSA DDOS

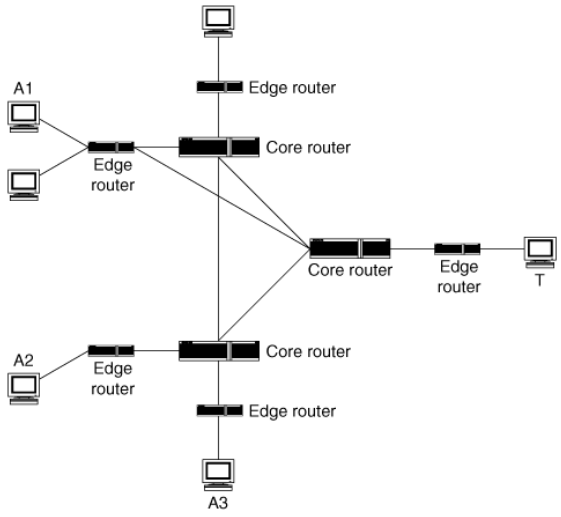


Figura 2. 35 Red simplificada para el estudio[79]

La Figura 2.35 será usada para ilustrar varias ubicaciones de defensa. En esta y

[79] http://denialofservice.uw.hu

figuras posteriores el nodo marcado como T refiere al objetivo atacado y los nodos A1, A2, A3 representan a las fuentes de ataque.

2.9.3.1 Cerca al objetivo

La defensa puede ser localizada en la propia máquina atacada, en un router, firewall, gateway, proxy u otra máquina que este muy cerca al objetivo atacado.

Máquinas cerca al objetivo pueden observar directamente el ataque, además de recibir la más completa información acerca de las características del ataque.

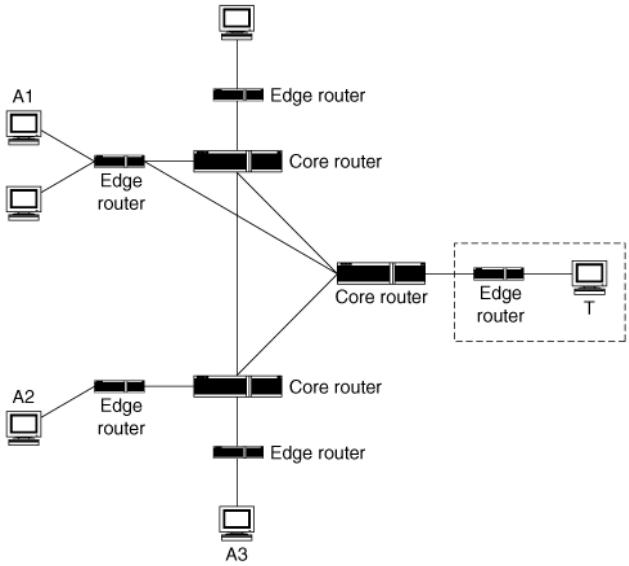


Figura 2. 36 Implementación cerca al objetivo atacado[90]

Sin embargo, existen algunas desventajas como son:

- La mayor, es que un ataque DDoS por definición sobrecarga al objetivo con su volumen y de igual forma podría sobrecargar a la defensa, a menos que este mejor aprovisionado.

- Su posición no es la adecuada como para realizar acciones que requieran un análisis complejo y diferenciación de paquetes legítimos de los del atacante.

- El colocar la defensa cerca al objetivo solo beneficia al objetivo atacado.

2.9.3.2 Cerca al Atacante

En lo posible debe ser implementada cerca a todos o a la mayoría de las ubicaciones donde posiblemente se originan los ataques.

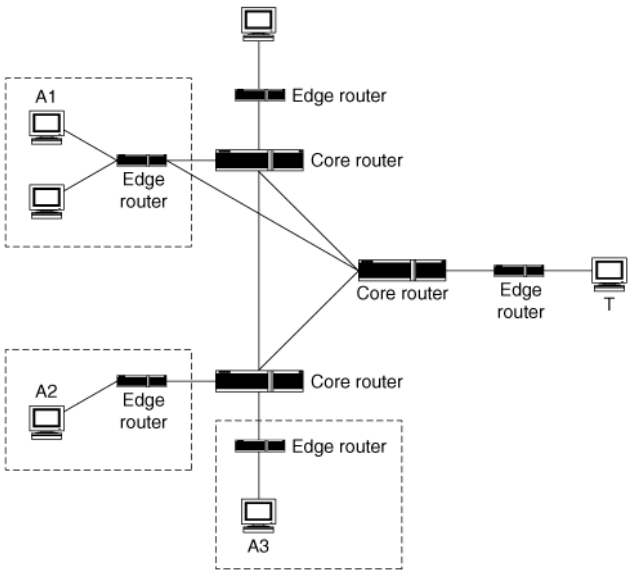


Figura 2. 37 Implementación cerca al atacante[90]

Una ventaja de ésta implementación es que la carga del ataque no es muy grande al lado de la fuente como en el caso del lado del objetivo, permitiendo así, una mejor detección y caracterización.

La desventaja es que podría tener problemas en determinar que se está realizando un ataque, ya que, el mecanismo de defensa debe determinar cuáles paquetes pertenecen al ataque y cuales son legítimos. Además deberían estar localizados cerca a un gran número de máquinas que realizan el ataque.

2.9.3.3 En el medio

Refiere a que la defensa se debe encontrar en el núcleo. Éste tipo de defensas son implementadas en más de un router. Sin embargo, también podría referir a

routers y otros nodos de red que se encuentren cerca al objetivo que no son parte de su red, como un ISP.

Pudiendo el término mitad referirse a borde, y la implementación de locación se puede encontrar muy cerca al objetivo o cerca al atacante, teniendo las características de esas locaciones.

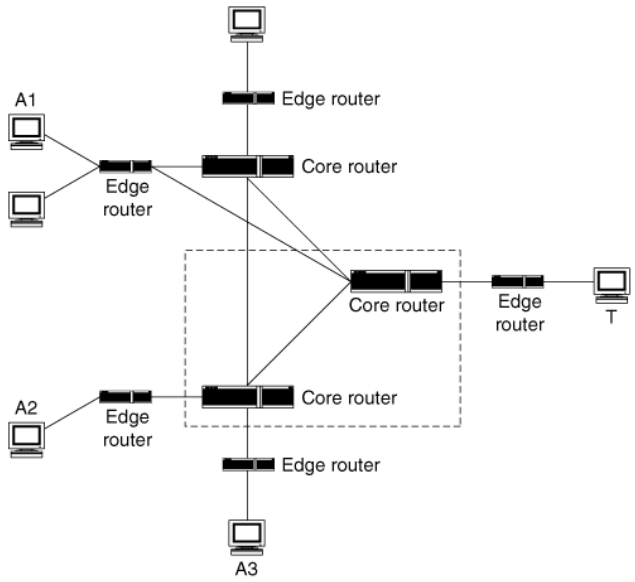


Figura 2. 38 Implementación de la defensa en el medio de internet[90]

Cualquier defensa localizada en un número razonablemente grande de AS (Autonomous Systems) bien elegidas podría dar una excelente cobertura. Si la defensa es eficaz, puede proporcionar sus beneficios a prácticamente todos los nodos conectados a Internet.

Entre las desventajas de éste tipo de implementación se pueden citar las siguientes:

- Los routers son equipos muy ocupados y no pueden dedicar sus recursos solo a manejar y analizar paquetes individuales.

- No pueden realizar un análisis completo de los paquetes como para determinar la presencia, características u orígenes del ataque DDoS.

- Si se equivocan, podrían desechar un gran número de paquetes legítimos.

- Si un router tiene problemas de rendimiento, muchos usuarios se verían afectados.

2.9.3.4 Implementación de Múltiples locaciones

Ésta implementación de defensa se aplica si se deseara proteger a todos los posibles objetivos contra todos los posibles ataques.

Implementar la defensa en más de un lugar o implementar múltiples soluciones que cooperen entre sí en diferentes lugares, son soluciones distribuidas necesarias, debido a que, no existe un punto en la red donde se pueda capturar todos los ataques y no todos los paquetes pasan por un solo punto en Internet.

Sin embargo, se necesita el intercambio de algún tipo de información entre ellas que permitan llegar a un acuerdo común a la presencia y características de un tipo de ataque, siendo ésta una de sus desventajas.

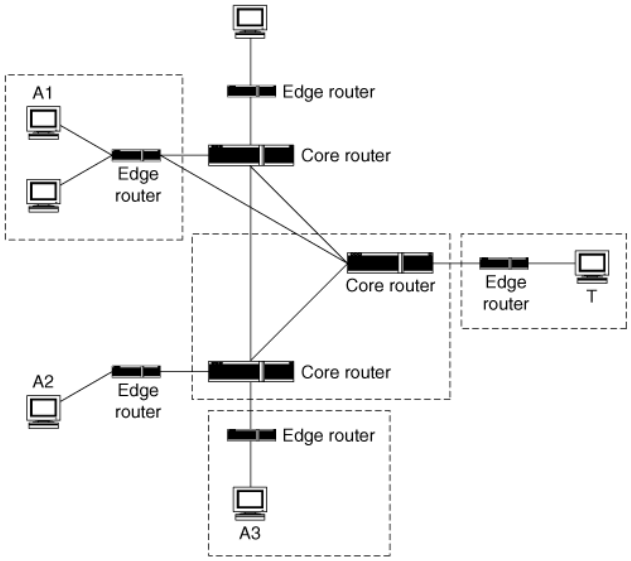


Figura 2. 39 Implementación Distribuida[90]

2.9.4 MECANISMOS PROPUESTOS DE DETECCIÓN Y/O DEFENSA

Durante el taller del CERT Coordination Center's Distributed System Intruder Tools (DSIT)[80], las ideas iníciales acerca de defensas DDoS fueron formadas.

En la actualidad, existen ya varios prototipos de mecanismos de defensa y muchos más se siguen investigando. A continuación serán comentados de forma breve algunos de ellos, dejando a libertad del lector el estudiarlos de forma más profunda y extensa.

2.9.4.1 Pushback

Propuesto por Mahajan, et al.[81] y surgió de los debates de la investigación DSIT realizada por el CERT.
La idea tomada de la práctica es que administradores de red intentan replegar el tráfico ofensivo hacía la fuente de ataque, desconectando el cable en el router u observando el tráfico de red en el equipo de monitoreo, para ver si el tráfico malicioso se detiene. Limitar la tasa de propagación fuera de la víctima (Pushback) alivianará la presión sobre ella, permitiendo el intercambio de tráfico y por un momento sobrevivir hasta que la fuente de ataque sea parada o removida. Esto supone que el tráfico ofensivo no es distribuido.

Hay dos técnicas que están en juego aquí: Local Aggregate Congestion Control (ACC) y pushback.

ACC locales detectan la congestión a nivel del router y elaboran una firma de ataque o en el contexto una firma de congestión, que puede ser traducida en un

---

[80] CERT Coordination Center, Results of the Distributed-Systems Intruder Tools Workshop, Diciembre del 1999, http://www.cert.org/reports/dsit_workshop-final.html.

[81] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, Controlling High Bandwidth Aggregates in the Network, *ACM SIGCOMM Computer Communications Review*, vol. 32, no. 3, Julio del 2002, Páginas: 62-73.

filtro. La firma define un ancho de banda total, un subconjunto de tráfico de red y el ACC local determina una tasa límite adecuada para éste conjunto.

Pushback propaga ésta tasa límite del conjunto a los inmediatos vecinos que contribuyen con la mayor cantidad de tráfico, para que así el resto de la red siga estando operativa.

Generalmente Pushback parece requerir continuas implementaciones de patrones en routers y que éstos mantengan el estado del flujo de tráfico, resultando ser una carga adicional para el router.

2.9.4.2 Traceback

Algunas de las primeras propuestas para la defensa contra ataques DDoS incluían formas de realizar el rastreo a los agentes de una red DDoS.

Una primera propuesta, ICMP Traceback por Bellovin, et al.[82], fue el de enviar un paquete ICMP, probabilísticamente cada n (primeras propuestas incluían un valor de n = 20,000) paquetes, conteniendo una porción del paquete capturado, desde el router observado al destino.

En general, se propone un nuevo mensaje ICMP, emitidos randomicamente por routers a lo largo del camino y enviados randomicamente al destino, para proveer información útil a la parte atacada o al origen.

La desventaja es que bajo un fuerte ataque, el objetivo puede perder esos paquetes debido a la congestión en el equipo de red y algunas redes no permiten mensajes ICMP. Pero incluso así, la muestra de 1/n ocurría y creaba tráfico adicional en dirección de la víctima.

[82] S. Bellovin, M. Leech, and T. Taylor, ICMP Traceback Messages, Internet draft, work in progress, Octubre del 2001.

Propuestas posteriores utilizaron una técnica llamada Probabilistic Packet Marking (PPM). Cada 20000 paquetes de red hacia el destino, un router marcaría un paquete con referencia a sí mismo[83].

Analizando varios paquetes marcados de una fuente dada, la victima por inundación trataría de crear un camino de regreso al atacante o por lo menos hasta el borde más próximo de él.

La propuesta inicial por Savage et al.[84] no dispone de métodos de autenticación de marcas, pero más tarde añadió una propuesta de autenticación y comprobación de integridad. Muchas otras técnicas han sido propuestas en este sentido como técnicas de incluir un solo bit [85].
En la técnica basada en hash[86] se compromete al router a recordar cada paquete que vea, pero por un tiempo limitado. EL SPIE (Source Path Isolation Engine) recuerda paquetes mediante el procesamiento de hashes a través de porciones invariantes de un encabezado IP, por ejemplo: TTL y checksums son removidos. Ésta capacidad de grabación pasiva no necesita estar implementada dentro del router. Los diseñadores SPIE pensaron en colocarlo en cada interfaz del router.

Dean et al.[87] adopta un enfoque algebraico al problema, incorporando información de rastreo parcial dentro de paquetes IP a nivel de router y usa técnicas

---

[83] En el campo de identificación IP de la cabecera, se propone llevar esta marca. Este campo es utilizado para el ensamblado de los paquetes fragmentados. Como sólo el 0,25% del tráfico de Internet son paquetes fragmentados [A1], varios esquemas de marcado de paquetes utilizan este campo para poner su marca. Es probable que estos sistemas no sean interoperables.

[84] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, Practical Network Support for IP Traceback, *Proceedings of ACM SIGCOMM 2000*, Agosto del 2000, Páginas: 295-306.

[85] M. Adler, Tradeoffs in Probabilistic Packet Marking for IP Traceback, *Proceedings of the 34th annual ACM Symposium on Theory of Computing,* ACM Press, 2002, Páginas: 407-418.

[86] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, Hash-Based IP Traceback, *Proceedings of ACM SIGCOMM 2001*, Agosto del 2001, Páginas: 3-14.

[87] D. Dean, M. Franklin, and A. Stubblefield, An Algebraic Approach to IP Traceback, *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, Febrero del 2001, Páginas: 3-12.

algebraicas para codificar información dentro de paquetes y reconstruirlos al lado de la víctima.

Sistemas PPM y algebraico, hacen algunas suposiciones como:

1. Atacantes son capaces de enviar cualquier paquete.
2. Múltiples atacantes pueden actuar juntos.
3. Los atacantes son consientes del sistema de rastreo.
4. Atacantes deben enviar por lo menos miles de paquetes.
5. Routers entre los hosts son generalmente estables, pero los paquetes pueden ser reordenados o perdidos.
6. Los routers no pueden hacer mucho cálculo por cada paquete.
7. Los routers no sean comprometidos en un ataque.

Dos serias desventajas existen en sistemas de rastreo:

1. Soluciones de rastreo a menudo, se vuelven excesivamente complejas y costosas, cuando hay un gran número de fuentes o cuando las fuentes están bien distribuidas.

2. El rastreo por sí mismo no hace nada referente a detener el ataque.

2.9.4.3 D-ward

Propuesto por Mirkovic et al.[88] [89], fue desarrollado en UCLA bajo el patrocinio del programa DARPA Fault Tolerant Network (FTN).

[88] J. Mirkovic, *D-WARD: Source-End Defense Against Distributed Denial-of-Service Attacks*, PhD thesis, University of California Los Angeles, Agosto del 2003, http://lasr.cs.ucla.edu/ddos/dward-thesis.pdf.

[89] J. Mirkovic, G. Prier, and P. Reiher, Attacking DDoS at the Source, *Proceedings of the 10th International Conference on Network Protocols (ICNP 2002)*, Noviembre del 2002, Páginas: 312-322.

Tiene por objeto detectar ataques antes o al momento de que el ataque salga de la red donde reside el agente DDoS.

Es un sistema en línea, transparente a los usuarios en la red, que reúne estadística de tráfico del router de borde en la red de la fuente y los compara con modelos de tráfico de red basados en especificaciones de protocolos de capa aplicación y transporte, lo que refleja un comportamiento normal (legítimo), transitorias (sospechoso), y el comportamiento del ataque.

Basado en éste modelo de tres niveles, D-WARD aplica límites de tasa al router en todo el tráfico de salida a un destino dado. Éstos límites podrían ser dinámicos basados en el tipo y la cantidad de tráfico que circula en la red.

D-WARD tiene la habilidad de rápidamente detectar ataques que puedan crear anomalías, como inundaciones y efectivamente controlar todo el tráfico incluyendo el del ataque.

Limitando la tasa de tráfico y no bloqueándola, éste sistema rápidamente se recupera de falsos positivos. Por diseño, neutraliza los ataques en la red de la fuente, pero requiere una gran implementación (cubriendo la mayoría de fuentes) para lograr la eficacia deseada.

En resumen, la ventaja de D-WARD radica en la detección y control de los ataques, asumiendo que el tráfico de ataque varía lo suficiente de modelos de tráfico normal. Por el contrario, los atacantes todavía pueden realizar ataques de éxito en redes que no estén equipados con este sistema.

2.9.4.4 NetBouncer

Propuesto por O'Brien[90] y también emerge del programa DARPA FTN. Es un mecanismo de legitimidad de cliente que se encuentra en la red de una posible

[90] E. O'Brien. NetBouncer: A Practical Client-Legitimacy-Based DDoS Defense via Ingress Filtering, http://www.networkassociates.com/us/_tier0/nailabs/_media/documents/netbouncer.pdf.

potencial víctima u objetivo.

Idealmente se coloca en el cuello de botella de la red y tiene como objeto permitir únicamente paquetes de usuarios o clientes legítimos. Varios test de legitimidad son realizados en el cliente, por ejemplo, un test ping (ICMP Echo Request) para ver si hay un cliente real detrás de los paquetes que fueron recibidos por el objetivo. Por ejemplo, dicho test se tiene al registrase en una cuenta de correo, en donde al cliente se solicita ingresar una frase o palabra desplegada en una imagen borrosa, asumiendo que solo un ser humano podría realizar y no una máquina.

Otros test, por ejemplo, analizan cuando una conexión en curso cae y si no NetBouncer termina la conexión.

Una vez que el cliente ha probado su legitimidad, es añadido a la pila de clientes legítimos y se le da un trato preferencial sobre aquellos que no han sido todavía legitimados. Esta pila es mantenida usando técnicas de calidad de servicio y garantiza el reparto equitativo de recursos entre usuarios legítimos para prevenir que un atacante pueda heredar las credenciales de un cliente legítimo. Después de un cierto tiempo la legitimidad de un cliente necesita ser reevaluada usando el mismo test u otro diferente.

Sin embargo, NetBouncer asume ciertas propiedades de los clientes como la habilidad de responder a pings, los cuales no todos los clientes soportan, especialmente aquellos que se encuentran detrás de firewalls routers DSL con características adicionales de seguridad

Aunque un cliente sea legítimo, no está protegido contra ataques de suplantación ya que una vez que el cliente haya probado su legitimidad a NetBouncer, el atacante puede usar su identidad. Además, el sistema no es inmune al agotamiento de recursos, debido a un gran número de clientes legítimos o que el atacante puede inundar toda la red y sus mecanismos de defensa.

Como todos, NetBouncer tiene sus ventajas y limitaciones. Entre sus ventajas están:

- Proveen un buen servicio a clientes legítimos, mayormente en todos los casos.
- La ubicación estará cerca a la víctima.
- No requiere de cooperación con otros NetBouncers.

Entre sus desventajas se tienen:

- Se pueden realizar ataques exitosos a la víctima u objetivo, haciéndose pasar por clientes legítimos.
- Netbouncer realiza ciertas suposiciones respecto a clientes y los hará ser excluidos del acceso a los recursos protegidos.
- Test de legitimidad ponen una carga significativa en el NetBouncer y puede agotar los recursos del mecanismo de defensa.

2.9.4.5 Secure Overlay Services (SOS)

Propuesto por Keromytis et al.[91] y su meta es enrutar únicamente el tráfico ideal a los servidores. Tráfico que no se ha confirmado como legítimo de usuarios o clientes, es descartado.

Clientes deberán usar una red sobrepuesta, esencialmente una red sobre la existente para obtener autenticación y llegar al servidor y deberán primero contactar al punto de acceso de la red sobrepuesta antes de acceder a la red.

Estos puntos de acceso envían los paquetes al llamado beacon por medio de un algoritmo de enrutamiento llamado Chord, el cual decide a dónde van los paquetes en ésta red sobrepuesta. El beacon en cambio envía los paquetes a

[91] A. D Keromytis, V. Misra, and D. Rubenstein, SOS: Secure Overlay Services, *Proceedings of ACM SIGCOMM 2002*, Agosto del 2002, Páginas: 61-72.

servlets secretos y son los únicos nodos en la red sobrepuesta que pueden penetrar el firewall en la red protegida

Estos servlets secretos envían los paquetes al firewall y éste dará acceso solo a los paquetes que provengan de las direcciones de los servlet´s secretos para alcanzar la red protegida.

La redundancia integrada en la red sobrepuesta asegurará que si un nodo cae, otro asumirá su cargo y como la ruta tomada por los paquetes hasta el destino final es secreta, contribuyen a la resistencia contra los ataques en el sistema SOS.

Si los atacantes no pueden enviar el tráfico directamente al objetivo o firewall, debido a restricciones de enrutamiento ya que desconoce de sus direcciones IP. La única forma de generar una inundación en el firewall sería pasando a través de la red sobrepuesta.

En resumen, SOS provee comunicación a un usuario legítimo con la red protegida, ofrece resistencia a la falla de un nodo debido a la redundancia y resistencia contra ataques en su propio sistema.

Por el contrario, Sistemas SOS están diseñados para trabajar con servicios privados únicamente ya que requiere cambios en el software del cliente y una extensa infraestructura sobrepuesta.

Se puede también tener una variante a SOS llamado WebSOS[92] que trabaja con un servidor Web público y usa Captcha[93] para legitimidad. Captcha requiere

[92] D. L. Cook, W. G. Morein, A. D. Keromytis, V. Misra, and D. Rubenstein, WebSOS: Protecting Web Servers from DDoS attacks" *Proceedings of the 11th IEEE* International Conference on Networks (ICON 2003), Septiembre del 2003, Páginas: 455-460.

[93] L. von Ahn, M. Blum, N. Hopper, and J. Langford, CAPTCHA: Using Hard AI Problems for Security, Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2003), Mayo del 2003, Páginas: 294-311.

presencia humana ya que los clientes deberían conocer los puntos de acceso para acceder a los servicios protegidos.

El uso de una red sobrepuesta tanto en SOS como WebSOS redefine la topología de enrutamiento y crea una ruta más larga o más lenta al destino. Algunos estudios como el realizado por Andersen et al,[94] muestran que la construcción y uso de una red sobrepuesta puede, algunas veces, ofrecer mejor servicio que usando el enrutamiento estándar de Internet. Pero otros resultados[95], muestran, ralentización de dos a diez veces mayor.

2.9.4.6 Proof of Work

Muchas conexiones son iniciadas por el atacante para agotar el número de conexiones abiertas que un servidor puede mantener. Uno de los objetivos de defensa es preservar estos recursos durante tal ataque. Como defensa, el servidor comienza a manejar estos desafíos[96] [97] [98], de una forma no muy diferente a los del NetbOuncer, para que el cliente solicite una conexión.

Dado que el sistema tiene como objeto proteger los recursos que involucran conexiones de red. El servidor distribuye un pequeño rompecabezas criptográfico a sus clientes que solicitan una conexión y espera por una solución. Si el cliente resuelve el rompecabezas dentro de un período de tiempo, los recursos apropiados se asignan en la pila de red (la parte del sistema operativo que

---

[94] D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, and R. Morris, Resilient Overlay Networks, Proceedings of 18th ACM Symposium on Operating Systems Principles (SOSP 2001), Octubre del 2001, Páginas: 131-145.

[95] A. D Keromytis, V. Misra, and D. Rubenstein, SOS: Secure Overlay Services, Proceedings of ACM SIGCOMM 2002, Agosto del 2002, Páginas: 61-72.

[96] C. Schuba, I. Krsul, M. Kuhn, G. Spafford, A. Sundaram, and D. Zamboni, Analysis of a Denial of Service Attack on TCP, Proceedings of the IEEE Symposium on Security and Privacy, Mayo de 1997, Páginas: 208-223.

[97] A. Juels and J. Brainard, "Client puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks, Proceedings of the Networks and Distributed System Security Symposium (NDSS), Marzo de 1999, Páginas: 151-165.

[98] X. Wang and M. K. Reiter, Defending Against Denial-of-Service Attacks with Puzzle Auctions, Proceedings of the IEEE Symposium on Security and Privacy, Mayo del 2003, Páginas: 78-92.

maneja la comunicación de red). A clientes que fallen en resolver el rompecabezas, se descartará la conexión.

La desventaja radica principalmente en que la actual implementación del protocolo TCP/IP en ambos extremos, tanto cliente como servidor, debería ser modificada para tal propósito y servirá únicamente contra ataques de agotamiento de conexiones y no contra otros tipos de ataque como los de inundación UDP por ejemplo.

2.9.4.7 Defcom

Propuesto por Mirkovic et al.[99]. Detecta un ataque en curso y responde limitando el tráfico mientras sigue permitiendo el tráfico legítimo al sistema.

Se compone de 3 tipos de nodos, pudiendo ser routers o hosts:

- Generadores de alertas.
- Limitadores de tráfico.
- Clasificadores.

Generadores de alerta y clasificadores son implementados en el borde de la red, mientras los limitadores de tráfico en el core de la red.

DefCOM rastrea el ataque desde la víctima hacia todas las fuentes activas de tráfico (ataque o legítimo) usando una red sobrepuesta e intercambiando estadísticas entre nodos de defensa.

Los clasificadores marcan los paquetes, para limitar el tráfico de los nodos.

---

[99] J. Mirkovic, M. Robinson, P. Reiher, and G. Kuenning, Forming Alliance for DDoS Defenses, Proceedings of the New Security Paradigms Workshop (NSPW 2003), ACM Press, Agosto del 2003, Páginas: 11-18.

Los limitadores de tráfico restringen el ancho de banda, preferentemente primero a los paquetes marcados como legítimos, luego a los marcados como sospechosos y finalmente a los no marcados. Esto crea tres niveles de servicio, dando mejor servicio a los paquetes legítimos.

Cualquier Firewall podría asumir el rol de generador de alertas. Los routers de Core deberán ser capaces de observar paquetes marcados para realizar la función de limitadores de tráfico

En resumen, el diseño de DefCOM permite la detección en la red de la víctima, limita el tráfico en el core y bloquea el trafico sospechoso/ataque en la red de la fuente.

2.9.4.8 CossAck

Propuesto por Papadopoulos et al.[100] , desarrollado por la Universidad del Sur de California/ISI y tiene por objeto prevenir ataques que salen de la red de la fuente

Los llamados watchdogs, un plug-in para el programa gratuito de detección de intrusos Snort[101], detectan un potencial ataque mediante el análisis y correlación del tráfico (tiempo, tipo de tráfico).

Ésta técnica actúa en la red de la fuente, provocada por una notificación del objetivo de un ataque DDoS mediante el filtrado del tráfico aparentemente ofensivo. Sin embargo, si el tráfico legítimo se iguala por el motor de correlación, conduciéndose a un falso positivo, el tráfico legítimo será descartado por COSSACK.

A las redes de origen se les impide convertirse en fuentes de ataque, pero una

[100] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan, Cossack: Coordinated Suppression of Simultaneous Attacks, Proceedings of 3rd DARPA Information Survivability Conference and Exposition (DISCEX 2003), Vol. 2, Abril del 2003, Páginas: 94-96.

[101] Sourcefire, Snort*:* The Open Source Network Intrusion Detection System, http://www.snort.org/.

red sin watchdog puede todavía participar en un ataque DDoS. Sin embargo, no se requieren modificaciones a nivel de protocolo o aplicación para la red de origen.

2.9.4.9 Pi

Propuesto po Yaar et al.[102], es una defensa basada en previas técnicas de marcado de paquetes[103]. Se insertan identificadores de ruta dentro de porciones no usadas o subutilizadas de la cabecera del paquete IP. La idea principal es que estas identificaciones de ruta son insertadas por los routers a lo largo de la ruta de red.

El objetivo o víctima podría entonces descartar paquetes con identificadores de ruta que hayan sido claramente identificados como parte de un ataque.

En el esquema base de marcado en Pi, cada router participante marca ciertos bits en el campo de identificación de el paquete IP. La colocación de la marca dentro de este campo es definido por el valor del campo TTL (Time to live) del paquete.

Dado que el valor de TTL es decrementeado cada vez que pasa por un router, se podría decidir parar el marcado en cierta distancia o salto de la red de la víctima para aumentar el alcance de éste esquema y el filtrado Pi puede ser usado, una vez que el esquema de marcado ha sido instalado en la infraestructura.

Éste esquema asume que la víctima conoce como identificar la mayor parte del tráfico de ataque por ejemplo, mediante la selección de una gran porción de tráfico de entrada que lleven la misma marca, los filtros descartaran los paquetes con esa marca dada.

---

[102] A. Yaar, A. Perrig, and D. Song, Pi: A Path Identification Mechanism to Defend Against DDoS Attacks, Proceedings of the IEEE Symposium on Security and Privacy, Mayo del 2003, Páginas: 93-107.

[103] D. X. Song and A. Perrig, Advanced and Authenticated Marking Schemes for IP Traceback, Proceedings of IEEE INFOCOM 2001, Vol. 2, Mazo del 2001, Páginas: 878-886.

Sin embargo, parte del tráfico legítimo podría ser descartado también, debido a que comparte la ruta a la víctima, por la naturaleza adaptiva y fluctuante de la red.

Pi es probable que sufra los mismos problemas de ataques por inundación en el mecanismo de defensa o de su enlace de red como la mayoría de las defensas al lado de la víctima.

2.9.4.10 Siff

Yaar et al, [104] propuso mitigar los ataques de inundación usando un mecanismo al extremo del host que separa el tráfico de internet en dos clases: Privilegiadas y no privilegiadas.

Los host finales pueden intercambiar capacidades que podrán ser usadas en tráfico privilegiado y los router entonces verificarán estas capacidades, las cuales son asignadas de forma dinámica y si los host no tienen un buen comportamiento sus capacidades son revocadas.

Éste esquema no requiere de un mecanismo de sobre posición pero si requiere una modificación del cliente, servidores y también routers.

Los host finales usarán un protocolo de handshake para intercambiar capacidades y entonces el tráfico privilegiado será expedido por la red. En contraste, el tráfico no privilegiado, no recibirá preferencia.

Si un host final con capacidades comienza una inundación, sus credenciales para tráfico privilegiado serán revocadas.

Ésta técnica realiza algunas suposiciones como:

[104] A. Yaar, A. Perrig, and D. Song, SIFF: a stateless Internet flow filter to mitigate DDoS flooding attacks, Proceedings of the IEEE Symposium on Security and Privacy, Mayo del 2004, Páginas: 130-143.

- Tanto cliente y servidor deben actualizar el software del protocolo TCP/IP para incorporar modificaciones necesarias para nuevas capacidades.
- Suplantación de identidad es limitada.
- Procesamiento y mantenimiento es requerido en cada router.
- El nuevo protocolo de red requiere marcar espacio en la cabecera IP.
- Cooperación de clientes y servidores.
- Que cada router marque paquetes y se mantengan estables.

2.9.4.11 Hop-Count Filtering (HCF)

Propuesto por Jin et al.[105], es un proyecto de investigación realizado en la Universidad de Michigan y tiene como objeto la defensa contra ataques DDoS mediante la observación del valor TTL (time to live) en paquetes entrantes a la red del objetivo/víctima que intenten inferir un número de saltos.

El sistema realiza cálculos de cuentas de salto, comenzando con el valor del TTL observado y adivinando el valor TTL inicial. La cuenta de saltos es la diferencia entre el valor inicial del TTL y el observado.

Si un atacante quisiera derrotar éste esquema, debería estar en la capacidad de adivinar correctamente el valor del TTL e insertarlo en sus paquetes, para que así la cuenta de saltos coincida con el valor esperado y que el número de discrepancias no supere un umbral establecido para que el esquema comience a filtrar.

Las tablas de entrada son constantemente actualizadas examinado conexiones TCP establecidas (por ejemplo: éxitos) de forma aleatoria a un sitio dentro de la red protegida.

Este esquema intenta prevenir ataques de tráfico falseado. Nada previene a un

---

[105] C. Jin, H. Wang, and K. G. Shin, Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic, Proceedings of the 10th ACM Conference on Computer and Communication Security, ACM Press, Octubre del 2003, Páginas: 30-41.

atacante lanzar un ataque con orígenes legítimos y llevar correctos valores de TTL.

Como otras defensas al extremo de la víctima, este enfoque no ayudaría a defenderse contra ataques de inundación basados en sobrecargar el enlace de la máquina que se encuentra comprobando los valores de TTL.

3. SIMULACIÓN Y ANÁLISIS DE ATAQUES DOS

En este apartado se presenta la parte práctica o experimental en lo que refiere a los ataques de denegación de servicio.

El escenario propuesto hará referencia a una red de datos convergente sencilla, con servicios básicos de voz, datos y video, que generalmente es implementada por personas con conocimientos básicos de redes e intranets, donde la seguridad de la red no juega un papel primordial en primera instancia.

El simular un ambiente como el comentado permitirá posteriormente realizar un test de penetración, para así, poder visualizar de forma más clara como un sistema sin seguridades puede resultar perjudicial para el correcto funcionamiento del mismo.

Sin embargo, tanto en la simulación como en el test de intrusión, no se aplicará una metodología en particular, debido al hecho de que no pueden ser aplicadas en su 100% y específicamente a que se faltarían a sus lineamientos propuestos. Por el contrario, se regirá por las fases que generalmente se aplican y que servirán como guía, para éste proyecto en particular.

Las fases que se han propuesto para la simulación y posterior test de intrusión, para el caso de estudio son:

1. **Escenario Propuesto:** De cierta forma se presentará un esquema de simulación Packet War, donde se involucra un nivel táctico de ataque/defensa, haciendo uso de servidores, clientes, equipos de conmutación y enrutamiento.

2. **Recopilación de información:** Llamado también fase de footprinting, es la fase donde se recolecta toda aquella información relevante y que servirá de ayuda para la posterior fase.

3. **Exploración de los sistemas:** Esta fase se encarga de listar puertos abiertos, servicios y/o vulnerabilidades presentes.

4. **Extracción de información (Simulación de Ataques):** Es la fase propia de la realización de ataques de denegación de servicio y permitirá obtener información fundamental para el posterior análisis y conclusión de los mismos. Entre los ataques a realizar constan: Inundaciones ICMP, TCP, UDP e INVITE a puertos específicos de los servicios presentes en la red de pruebas.

5. **Informe:** Una vez que se han realizado los diferentes tipos de ataques y haber extraído la información necesaria, el informe final será un resumen general, en el cual se incluirá el análisis, conclusiones y posibles soluciones a los ataques realizados.

3.3.1 ESCENARIO PROPUESTO

3.3.1.1 Consideraciones

Con el objeto de conocer cómo un ataque de denegación de servicio podría afectar a una red de datos convergente, haciendo uso de plataformas Linux y Windows con servicios de voz, datos y video, se han hecho las siguientes consideraciones:

- **Servicios:** Algunos de los servicios más utilizados en la actualidad son: el correo electrónico, internet, telefonía y sistemas de seguridad, razón por la cual, se hará referencia a éstos para ser implementados en la red de datos propuesta.

- **Plataformas del usuario:** Debido a que los sistemas Windows son los que predominan el mercado y los usuarios están mayormente familiarizados con éstos. Se usarán Sistemas Operativos Windows para los hosts de la

red de pruebas y las aplicaciones utilizadas deberán ser compatibles con dicha plataforma.

- **Conexión a Internet:** Tanto servidores como hosts en la red deben tener acceso a Internet.

- **Direccionamiento IP:** Las direcciones IP serán obtenidas dinámicamente por los hosts de la red a través de un servidor DHCP. Para los servidores y sistema de seguridad, serán definidas estáticamente.

- **Seguridad:** La red de datos propuesta no dispondrá de equipos o elementos de seguridad como firewalls, proxy`s u otros que permitan realizar filtrado de paquetes o implementar filtros de seguridad, con el objeto de visualizar las desventajas que se tienen al no ser estos implementados.

- **Acceso:** Los usuarios serán parte de un dominio dado y el acceso a sus ordenadores será por un nombre de usuario y contraseña.

- **Tarjetas de red:** Hosts, servidor de telefonía, cámara IP y equipos de interconectividad dispondrán de interfaces de red 10/100Mbps.El servidor de correo dispondrá de una interfaz 10/100/1000 Mbps.

- **Metodología de test de intrusión y simulación:** Ninguna en específico.

- **Equipo para la realización del ataque:** Ya que un ataque de denegación de servicio puede ser implementado independientemente de la plataforma, se usara aquella plataforma que permita realizar este tipo de ataques de forma plena.

3.3.1.2 Requisitos de Hardware y Software

Ya que el escenario estará basado en una red de datos convergente, con servicios de voz, datos y video, además de acceso a internet, se tendrán los siguientes requisitos y/o requerimientos mínimos.

ROUTER
Descripción
Será el encargado de proporcionar acceso a internet a los usuarios y servidores de la red.
Requerimientos
Interfaz LAN-RJ45:10/100 Mbps Interfaz WAN-RJ45:10/100 Mbps DHCP NAT

Tabla 3. 1 Requisitos del Router

SWITCH
Descripción
Equipo de interconectividad que proporcionará la interconexión en la red.
Requerimientos
Seis puertos LAN-RJ45:10/100 Mbps (Servidor Web/Correo y telefonía, cámara IP, hosts y equipo de ataque)

Tabla 3. 2 Requisitos del Switch

SISTEMA DE SEGURIDAD CÁMARA IP
Descripción
Equipos Autónomos conectados a la red de datos, que trasmiten video en tiempo real.
Requerimientos
1 puerto LAN-RJ45: 10/100 Mbps Acceso vía HTTP y Software de Monitoreo

Tabla 3. 3 Requisitos de la Cámara IP

TELÉFONOS IP
Descripción
Equipos conectados a la red de datos, para brindar servicio de telefonía a los clientes.
Requerimientos
1 puerto LAN-RJ45: 10/100 Mbps Dispositivo o aplicación compatible con el protocolo SIP.

Tabla 3. 4 Requisitos de Teléfonos IP

EQUIPO DE ATAQUE
Descripción
Computador mediante el cual se lanzarán los diferentes tipos de ataque de denegación de servicio.
Requerimientos
Tarjeta de red 10/100 Mbps Sistema Operativo Windows y/o Linux con acceso a la Intranet e Internet Privilegios de Administrador

Tabla 3. 5 Requisitos del Equipo de Ataque

SERVIDOR WEB/CORREO	
Descripción	
Implementado en Plataforma Windows, para proporcionar servicios Web y correo electrónico a los usuarios de la red e internet.	
Requerimientos	
Según los requerimientos propuestos por Microsoft para la instalación de un Sistema Operativo Windows server 2008[106] x64 son:	
Procesador	Mínimo: 1 GHZ Recomendado: 2 GHz Optimo: 3 GH
Memoria	Mínimo: 512 MB RAM Recomendado: 1 GB RAM Optimo: 2 GB RAM
Espacio en Disco	Mínimo: 8GB Recomendado: 40 GB Optimo:80 GB

[106] Requisitos de sistema de Windows Server 2008, http://technet.microsoft.com/es-es/windowsserver/bb414778

El servidor de correo será implementado haciendo uso de Microsoft Exchange Server 2010 x64 y una instalación típica. Para tal propósito según los requerimientos propuestos por Microsoft[107] son:

Procesador	Basado en arquitectura x64
Memoria	Mínimo: 4 GB RAM por servidor más 5 MB de RAM recomendado para cada buzón.
Espacio en Disco	Mínimo: 1.2 GB y 200 MB de espacio disponible en el disco de sistema
Sistema Operativo	Microsoft Windows Server 2008 Ed. Standard x64 Edition o Ed. Enterprise x6

Adicionalmente se necesitan los siguientes requerimientos de Software, que son:

- Windows Server 2008 SP2
- Instalar Active Directory
- Instalar Servidor DNS
- Instalar Internet Information Server
- Instalar .Net Framework 3.5 SP1
- Instalar las actualizaciones de la familia .Net Framework 3.5, Windows Vista x64 y Windows Server 2008 x64.
- Instalar la Administración remota de Windows (WinRM) 2.0
- Instalar Power Shell V2
- Debido a que los 3 roles estarán en el mismo server, se debe instalar Microsoft Office Filter Pack
- Instalar los prerrequisitos para una instalación típica ejecutando el comando " servermanagercmp –ip exchange-typical.xml" desde la consola de comandos en el patch "scripts" del instalador de Exhange.

Nota: Los requisitos reales del Sistema Operativo, variarán en función de la configuración del sistema y de las aplicaciones y/o características instaladas.

Tabla 3. 6 Requisitos Servidor Web y Correo

[107] Requisitos de Microsoft Exchange Server 2010, http://www.microsoft.com/spain/exchange/2010/sysreq.mspx

SERVIDOR DE TELEFONÍA

Descripción

Implementado en Plataforma LINUX, para proporcionar servicios de telefonía a los usuarios.

Requerimientos

Según los requerimientos para la instalación de Ubuntu Sever 10.10[108] son:

Procesador	1 GHZ (Soporta 2 tipos de arquitecturas:: Intel x86 and AMD649
Memoria	128 MB de RAM
Espacio en Disco	500 MB-1GB

Según los requerimientos, Asterisk menciona que en realidad no es dictado por el número de

usuarios o grupos, sino más bien por el número de llamadas simultáneas que se espera que de apoyo. A continuación se presenta una tabla referencial de requerimientos según el número de canales[109]:

Número de Canales	Requisito Mínimo
No más de 5	400 MHz x86, 256 MB RAM
De 5 a 10	1 GHz x86, 512 MB RAM
Hasta 25	3 GHz x86, 1 GB RAM
Más de 25	CPUs de doble núcleo y posiblemente múltiples servidores en una arquitectura distribuida.

[108] Requerimientos Ubuntu Server 10.10, https://help.ubuntu.com/10.10/serverguide/C/preparing-to-install.html

[109] Requerimientos Asterisk, http://astbook.asteriskdocs.org/en/2nd_Edition/asterisk-book-html-chunk/asterisk-CHP-2.html

Para la instalación de Asterisk de forma manual se necesita ciertas las librerías[110] y requerimientos[111]. Nota: Los requisitos reales del Sistema Operativo, variarán en función de la configuración del sistema y de las aplicaciones y/o características instaladas.

Tabla 3. 7 Requisitos Servidor de Telefonía

3.3.2 RECOPILACIÓN DE INFORMACIÓN

3.3.2.1 Mapa de Red

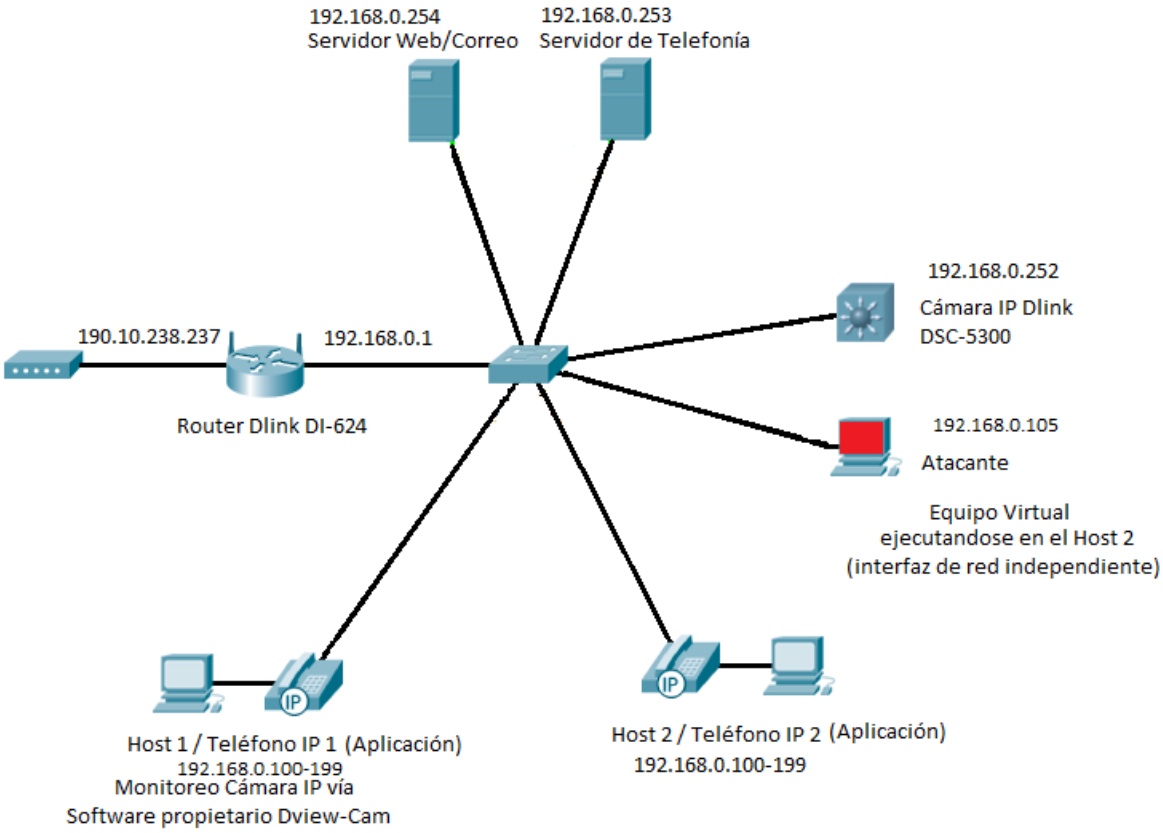


Figura 3. 1 Diagrama de la Red de Pruebas

---

[110] Repositorio Librerías, Ubuntu.wikipedia.org

[111] http://www.voip-info.org/wiki/view/Instalaci%C3%B3n+de+Asterisk+en+Ubuntu+Server+Paso+a+Paso

3.3.2.2 Resumen de Equipos, Características y Servicios

La Tabla 3.8 hace referencia a las características y detalles de los equipos usados en la implementación de la red de pruebas.

EQUIPO/SERVICIO	CARACTERÍSTICAS	SISTEMA OPERATIVO	CUENTAS DE USUARIO	DETALLES
Conexión Internet	2 Mbps/400 Kbps	-	-	-
Router Wireless Dlink DI-624	1 Puerto WAN 4 Puertos LAN 10/100 Mbps	-	Cuenta de Administración	1)Por defecto (No se ha levantado ningún tipo de seguridad o filtro).
Switch Nexxt	8 Puertos LAN 10/100Mbps	-	-	-
Cámara IP Dlink DSC-5300	1 Puerto LAN 10/100 Mbps	-	Cuenta de Administración	1) Se han configurado la dirección IP como estática. 2)Por defecto (No se ha levantado ningún tipo de seguridad o filtro).
Host 1	Proc. 2.4 GHz 1 GB RAM 320 GB HD Tarjeta de red:10/100Mbos CD/DVD RW	Windows XP Professional	Administrador	1) Los servicios y seguridades levantadas son únicamente los realizados al momento de la instalación del Sistema Operativo. 2) Instalado Antivirus. 3) Instalado Dview-Cam Commview y WireShark
Host 2	Proc. 3 GHz Celeron 1 GB RAM 160 GB HD Tarjeta de red:10/100Mbos CD/DVD RW	Windows XP Professional	Administrador	1)Los servicios y seguridades levantadas son únicamente los realizados al momento de la instalación del Sistema Operativo. 2) Instalado Antivirus
Teléfonos (1 y 2)	Software/Aplicación 3CXPhone	-	-	1) Teléfonos básicos implementados por Software compatibles con SIP.

Tabla 3.8 Resumen de Equipos, Características y servicios

EQUIPO/SERVICIO	CARACTERÍSTICAS	SISTEMA OPERATIVO	CUENTAS DE USUARIO	DETALLES
Servidor de Telefonía	Proc. 2.4 GHz 768 MB RAM 20 GB HD Tarjeta de red:10/100Mbos	Ubuntu Server 10.10	Administrador	1) Se ha configurado la dirección Ip como estática. 2) Los servicios y seguridades levantadas son únicamente los realizados por defecto al momento de la instalación del Sistema Operativo. 3) No se ha levantado ningún tipo de seguridad o filtro. 4) Se considera no más de 25 canales simultáneos. 5) Ejecutando SNMP y MRTG
Servidor Web/Correo	Proc. 2.4 GHz C2D 4 GB RAM 320 GB HD Tarjeta de red:10/100Mbos CD/DVD RW	Windows Server 2008 Enterprise x64	Administrador	1) Se ha configurado la dirección Ip del servidor como estática, se han creado zonas de búsqueda directas e inversas en el Servidor DNS para los 3 servicios (Correo, HTTP y telefonía) 2) Los servicios y seguridades levantadas son únicamente los realizados por defecto al momento de la instalación del Sistema Operativo y Exchange 2010. 3) Instalado Active Dir, IIS, NET Framework 4) Instalado Antivirus NOD 32 5) Ejecutando SNMP

Tabla 3. 8 Resumen de Equipos, Características y servicios.

3.3.2.3 Direcciones IP

La Tabla 3.9 y las figuras mostradas a continuación hacen referencia a las Direcciones IP configuradas en los equipos de la red de pruebas.

EQUIPO/SERVICIO	TIPO DIRECCIÓN	DIRECCIÓN IP
Router	WAN-DHCP LAN-Estática	WAN: 190.10.238.237 LAN: 192.168.0.1
Switch	-	-
Servidor Web/Correo	Estática	192.168.0.254
Servidor de Telefonía	Estática	192.168.0.253
Cámara IP	Estática	192.168.0.252
Host 1	Dinámica	192.168.0.100-199
Host 2	Dinámica	192.168.0.100-199
Teléfono IP 1 (SIP)	Misma que Host 1	Misma que Host 1
Teléfono IP 2 (SIP)	Misma que Host 2	Misma que Host 2

Tabla 3. 9 Direcciones IP de los Equipos de la Red de Pruebas

Figura 3. 2 Ejemplo Funcionamiento Cámara IP Dlink DCS-5300

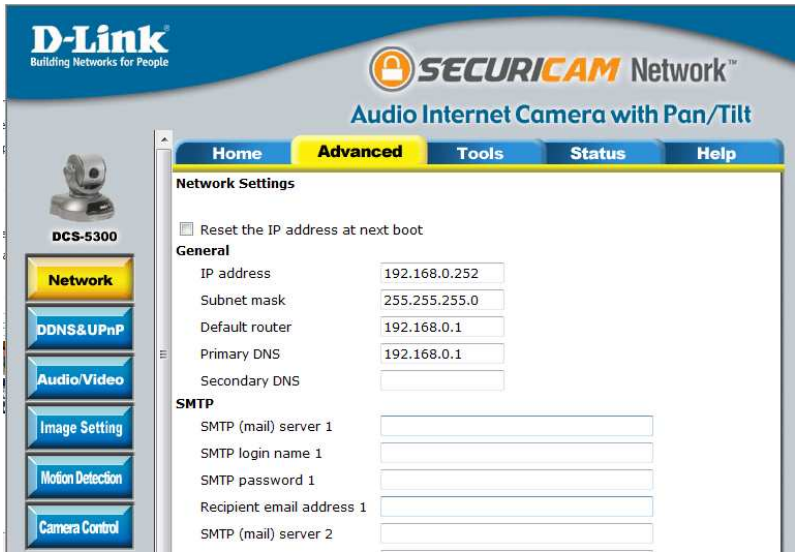


Figura 3. 3 Configuración de red y Acceso Web de la Cámara IP DCS-5300

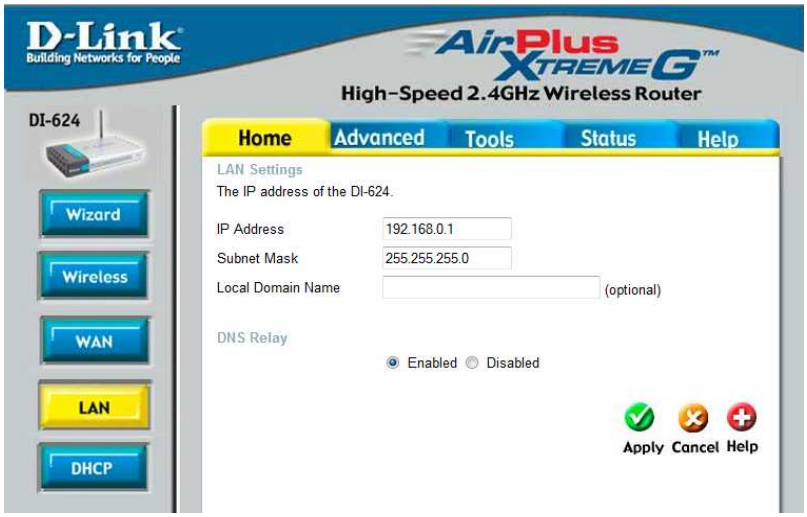


Figura 3. 4 Configuración de red del Router Dlink DI-264

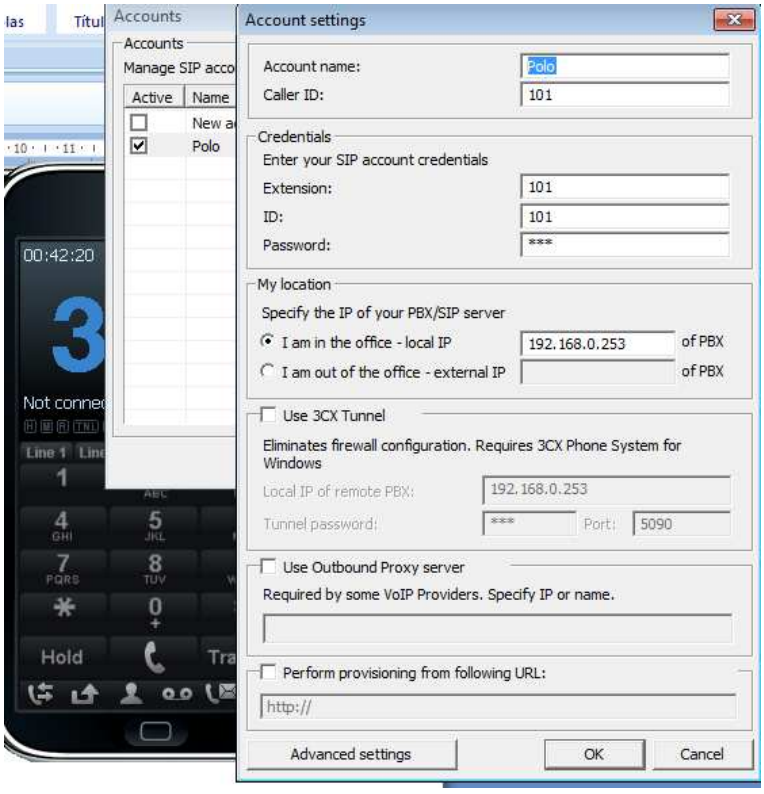


Figura 3. 5 Configuración de Red del Teléfono IP 3CXPHONE

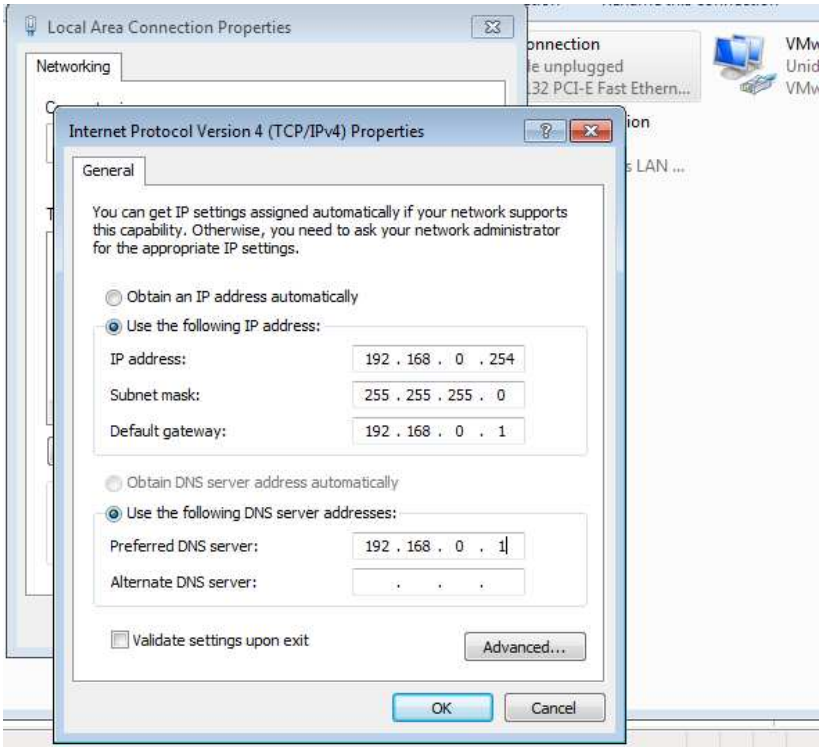


Figura 3. 6 Configuración de Red del Servidor Web/Correo

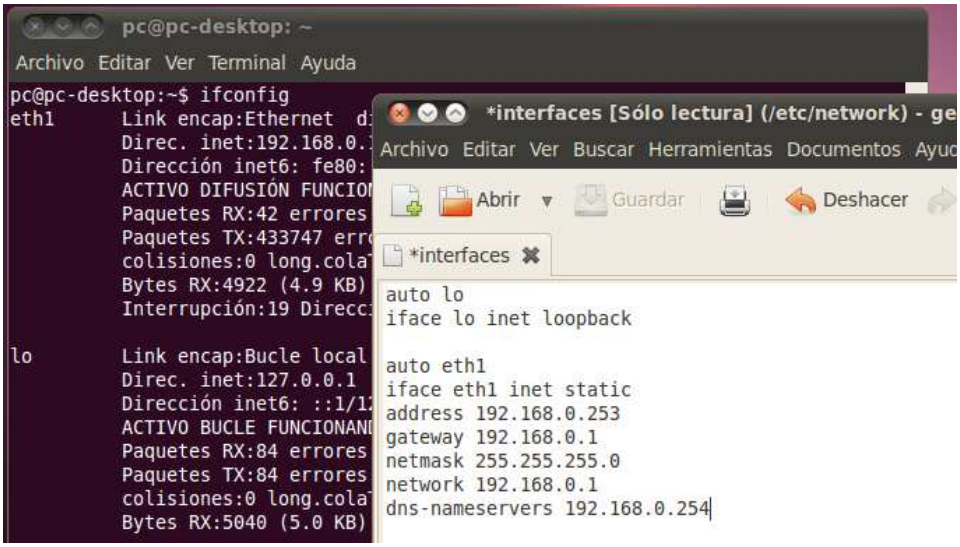


Figura 3. 7 Configuración de Red del Servidor de Telefonía

3.3.2.4 Herramientas

Una vez que se han expuesto los requerimientos y consideraciones necesarias para el caso de estudio, se han definido las herramientas que serán utilizadas, y estas son:

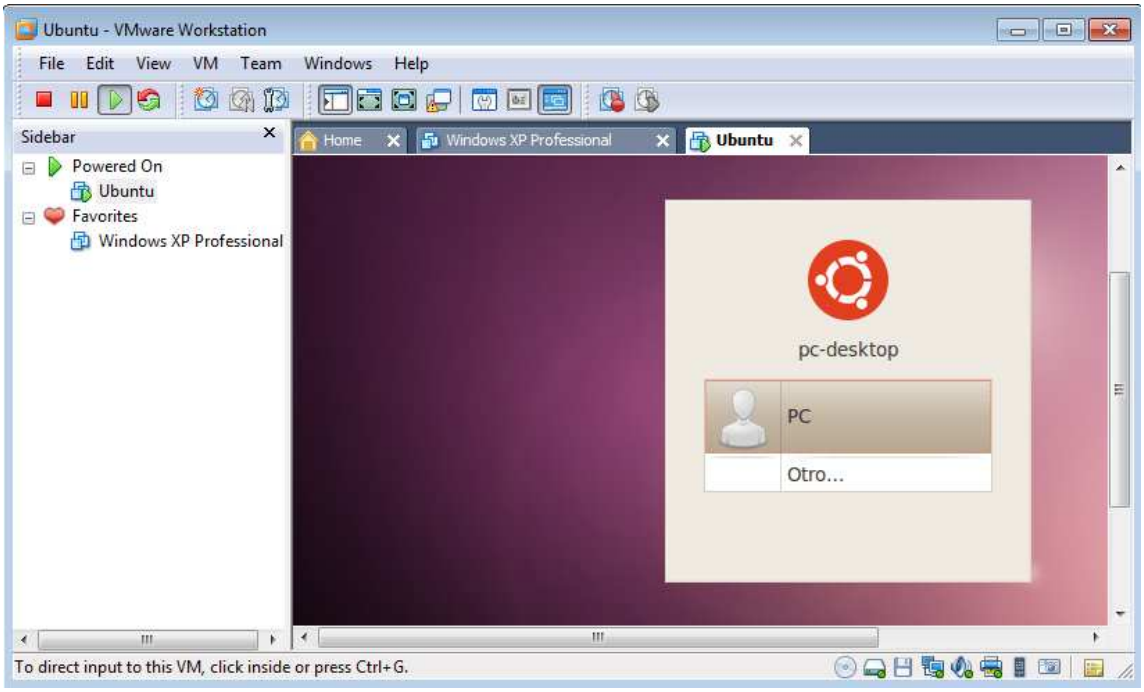
3.3.2.4.1 Para la implementación de servidores y equipo de ataque

Los servidores y el equipo generador del ataque, serán implementados con la ayuda de VMware, debido a sus características de aislamiento, seguridad, flexibilidad, agilidad, portabilidad y para el propósito, la creación de entornos de prueba.

VMWare[112]

Es un sistema de virtualización por software, que permite simular uno o varios sistemas físicos (Computadores) con características determinadas de hardware, permitiéndonos así ejecutar (simular) varios sistemas operativos en un mismo computador de forma simultánea

VMware proporciona un ambiente de ejecución similar al de un computador real con CPU, BIOS, tarjeta de video, tarjeta de red, memoria RAM, sistema de sonido, conexión USB, disco duro, entre otros.



[112] http://www.vmware.com/lasp/

Figura 3.8 Ejemplo de Funcionamiento de Vmware

3.3.2.4.2 Para la ejecución de ataques

Debido a la gran cantidad de herramientas y tipos de ataques de denegación de servicio existentes, el presente proyecto se enfocará únicamente en aquellos ataques más habituales y que podrían afectar a la red propuesta, basándonos en los protocolos que serán utilizados de capa aplicación (HTTP,SMTP, SIP), transporte (TCP y UDP) y de red (IP e ICMP).

Hping [113]

En una herramienta de red muy versátil, capaz de manipular y enviar paquetes TCP/IP ya sean TCP, UDP o ICMP desde línea de comandos.

Algunas Opciones a ser utilizadas con Hping son:

- -q : Quiet, nada se muestra, excepto las líneas de resumen al comenzar y al terminar.
- -n : Sólo salida numérica, no se intentará la búsqueda de nombres para direcciones de host.
- -a : *Spoofing,* utilizado para establecer una dirección IP de origen falsa.
- -S : Bandera SYN activada.
- -s: Incrementa el número de puerto para cada paquete enviado.
- -p : Número de puerto destino.
- -d : Tamaño de los datos.
- --flood: Envía paquetes tan rápido como sea posible , sin preocuparse de mostrar repuestas entrantes.
- --udp : Con este modo se enviarán paquetes UDP.
- --icmp : Con este modo se enviarán paquetes ICMP.

---

[113] http://linux.die.net/man/8/hping3

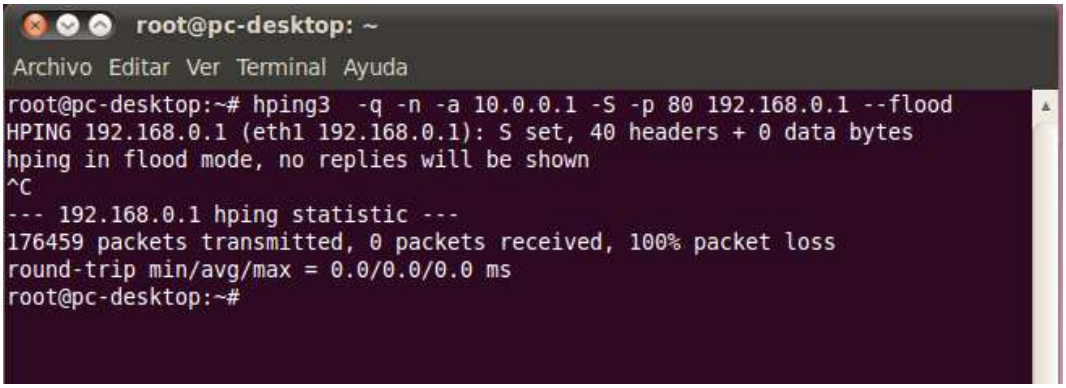


Figura 3.9 Ejemplo de Funcionamiento de Hping

InviteFlood

INVITEflood realiza un envío masivo de peticiones INVITE a un servidor con el objetivo de colapsarlo. El servidor tratará de atender a todas las llamadas generadas consumiendo gran cantidad de recursos.

```
inviteflood eth0 500 192.168.0.2 192.168.0.2 1000000 -a hacker -v

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port   = 192.168.0.3:9
dest   IPv4 addr:port   = 192.168.0.2:5060
targeted UA             = 500@192.168.0.2

Flood User Alias: hacker
Verbose mode

Flooding destination with 1000000 packets

Packet:
0000  49 4e 56 49 54 45 20 73  69 70 3a 35 30 30 40 31
[...]
0420  3a 6f 66 66 20 2d 20 2d  20 2d 20 2d 0d 0a

SIP PAYLOAD for packet 0:
INVITE sip:500@192.168.0.2 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.3:9;branch=c3f8b062-a838-445a-9b37-790000000001
Max-Forwards: 70
Content-Length: 460
To: 500 <sip:500@192.168.0.2:5060>
From: hacker <sip:hacker@192.168.0.3:9>;tag=c3f8cec5-a838-445a-8dee-340000000001
Call-ID: c3f8e8de-a838-445a-bffe-620000000001
CSeq: 0000000001 INVITE
```

Figura 3. 10 Ejemplo de Funcionamiento de Inviteflood

3.3.2.4.3 Para el análisis y monitoreo

Nmap (Network Mapper) [114]

Es una herramienta de código abierto (open source) que sirve para visualizar servicios que se ejecutan, versión y tipo de sistema operativo, efectuar rastreo de puertos, obtener características de hardware de red, identificar computadoras en una red , en resumen se la utiliza para evaluar la seguridad de sistemas informáticos.

[114] http://nmap.org/

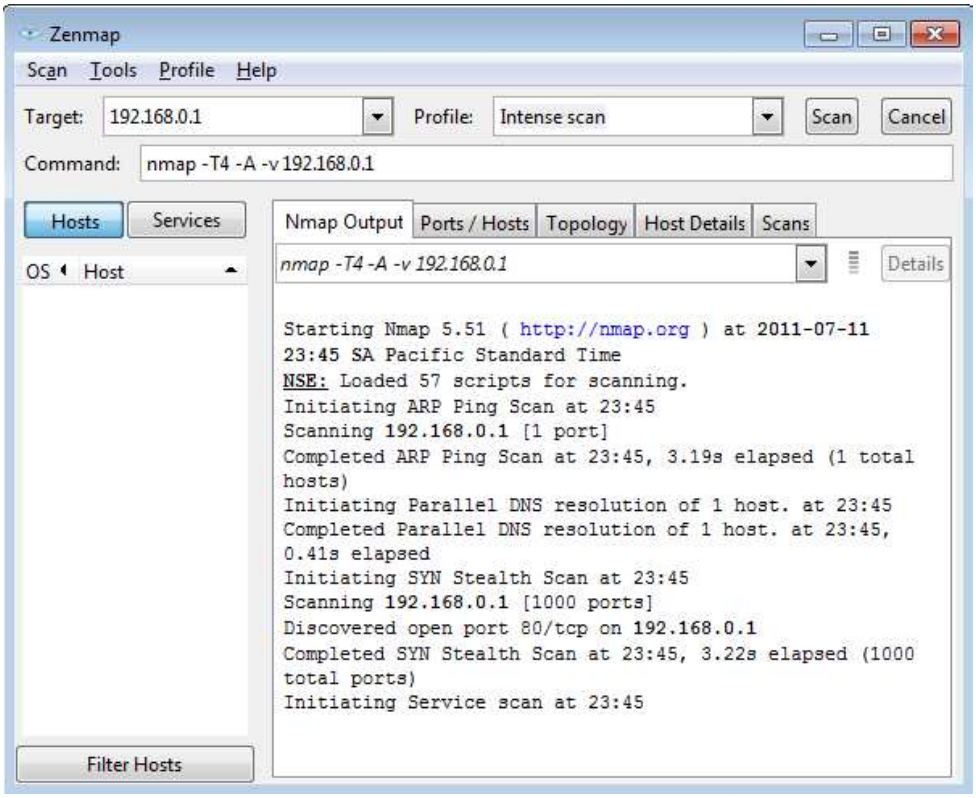


Figura 3. 11 Ejemplo de Funcionamiento de Nmap

CommView[115]

Es una herramienta para análisis y monitorización que permite capturar cada paquete que circula por el segmento de red o computador, permitiendo visualizar información importante como:

- Listado de paquetes.
- Conexiones de red.
- Estadísticas.
- Cuadros de distribución de protocolos.
- Examinar, grabar, filtrar, importar y exportar paquetes capturados.
- Analizador para VoIp, entre otros.

Nota: Se ha utilizado la versión demo de 30 días de CommView.

---

[115] http://www.tamos.com/products/commview/

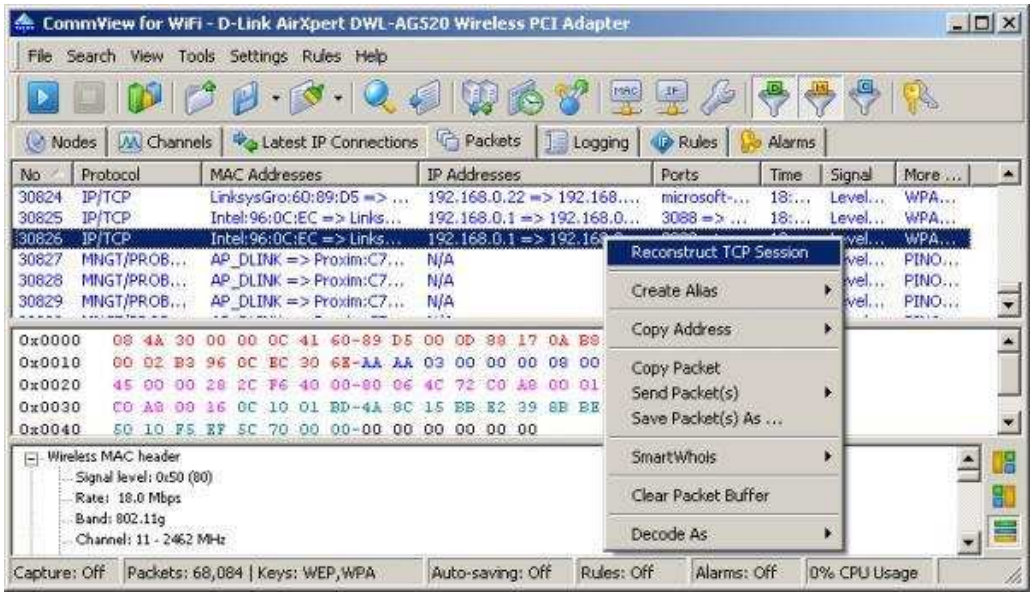


Figura 3. 12 Ejemplo de Funcionamiento de CommView

Wireshark[116]

Wireshark es una herramienta de análisis de protocolos de red, que permite capturar el tráfico que circula por una red de datos y visualizarlo de forma interactiva.

Su funcionalidad es similar a la de tcpdump[117], pero añade una interfaz gráfica y varias opciones de organización y filtrado de información.

Mrtg[118]

MRTG (*Multi Router Traffic Grapher*), es una herramienta para supervisar la carga de tráfico en los enlaces de red, generando páginas HTML con gráficas que proporcionan una representación visual del tráfico. Se basa en Perl y C y funciona bajo UNIX y Windows NT.

---

[116] http://www.wireshark.org/

[117] **Tcpdump.-** es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red. http://es.wikipedia.org/wiki/Tcpdump.

[118] http://www.mrtg.jp/en/es_es/

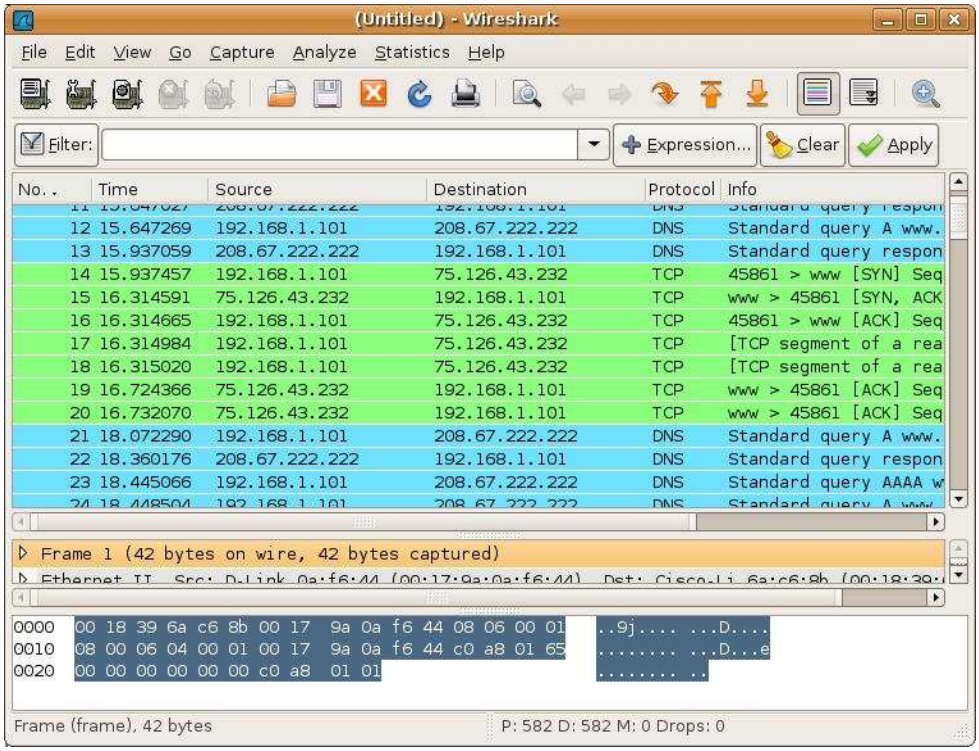


Figura 3. 13 Ejemplo de Funcionamiento de Wireshark

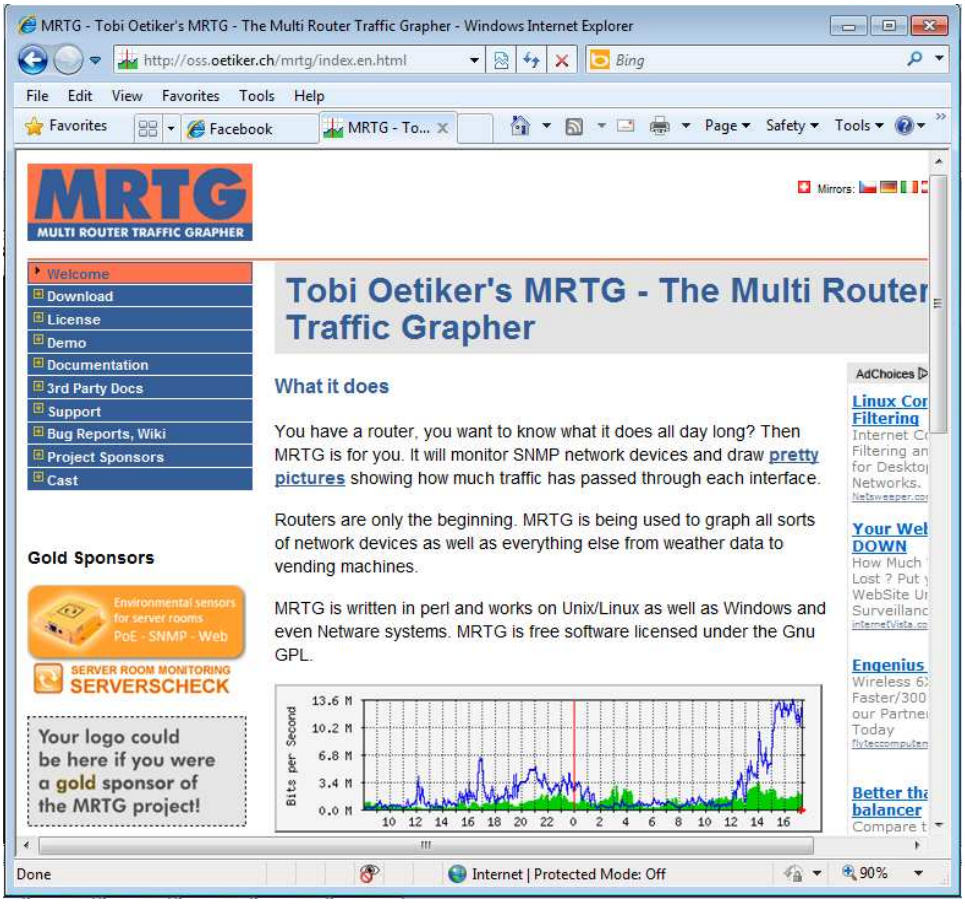


Figura 3. 14 Página de MRTG en Internet

3.3.2.5 Valores de Recursos y estados iniciales

Para un posterior análisis y comparación, se han obtenido valores iníciales de cómo los recursos de red, CPU, memoria y espacio en disco se comportan en un ambiente en reposo (Sin que los clientes hayan tenido acceso a los servicios).

Dichos valores iníciales fueron obtenidos con la ayuda de SNMP, MRTG y CommView, en un intervalo de tiempo mucho mayor al tiempo de los posteriores ataques. Su archivo de configuración como todas las gráficas se encuentran en el ANEXO 5.

3.3.2.5.1 Resumen General de Estados Iniciales

La Tabla 3.11 hace referencia a los estados iniciales de los equipos.

TIPO	SERVIDOR	PROMEDIO
Carga del CPU	Telefonía	1 %
	Web/Correo	4 %
Memoria Libre	Telefonía	201 MB
	Web/Correo	1274 MB
Uso de Disco	Telefonía	21%
	Web/Correo	48%

MB: Mega Bytes

Tabla 3.10 Resumen General de estados iniciales de los Equipos/Servicios

TIPO	SERVIDOR	PROMEDIO
Análisis de Tráfico en la interfaz de red	Telefonía	Entrada: 3576 bps Salida: 360 bps
	Web/Correo	Entrada: 6704 bps Salida: 480 bps
	Cámara IP	Entrada: 680,79 kbps Salida: 324,32 kbps
Conexiones TCP Passive/Active Open	Telefonía	Passive Open: 0cs/min Active Open: 0 cs/min
	Web/Correo	Passive Open: 14cs/min Active Open: 15 cs/min
Conexiones TCP Establecidas	Telefonía	1 cs
	Web/Correo	97 cs
Segmentos TCP	Telefonía	Enviados: 26 segs/min Recibidos:41 segs/min
	Web/Correo	Enviados: 1235 segs/min Recibidos: 1236 segs/min
	Cámara IP	Enviados y Recibidos: 10,11 ksegs/min
Datagramas UDP	Telefonía	Enviados: 9 dts/min Recibidos:12 dts/min
	Web/Correo	Enviados: 74 dts/min Recibidos: 88 dts/min
	Cámara IP	Enviados y Recibidos: 14,65 dts/min

bps: bits x Segundo, **cs:** Conexiones, **cs/min:** Conexiones x minuto, **segs/min:** segmentos x minuto
dts/min: Datagramas x minuto

Tabla 3.10 Resumen General de estados iniciales de los Equipos/Servicios

TIPO	SERVIDOR	PROMEDIO
Paquetes IP	Telefonía	Enviados: 15 pts/min Recibidos: 66 pts/min
	Web/Correo	Enviados: 183 pts/min Recibidos: 132 pts/min
	Cámara IP	Enviados y Recibidos: 10,12 kpts/min
Mensajes ICMP	Telefonía	Enviados: 0 Recibidos: 0
	Web/Correo	Enviados: 2 msgs/min Recibidos: 2 msgs/min
	Cámara IP	Enviados y Recibidos: 1 msgs/min

pts/min: Paquetes x minuto, **msgs/min:** Mensajes x minuto

Tabla 3. 10 Resumen General de estados iniciales de los Equipos/Servicios

3.3.2.6 Exploración de los Sistemas

3.3.2.6.1 Puertos Abiertos y Servicios

La Tabla 3.11 hace referencia a los puertos y servicios de los equipos.

DIRECCIÓN IP EQUIPO	PUERTOS ABIERTOS/SERVICIO
192.168.0.1 Router	• 80/tcp - http • 53/udp – domain • 5000/udp -upnp
192.168.0.254 Servidor Web/Correo	• 25/tcp - smtp /Microsoft Exchange ESMTP • 53/tcp - domain/Microsoft DNS 6.0.6002 • 80/tcp - http/Microsoft IIS httpd 7.0 • 88/tcp - kerberos-sec /Microsoft Windows kerberos-sec • 135/tcp - msrpc /Microsoft Windows RPC • 139/tcp - netbios-ssn • 389/tcp – ldap • 443/tcp - ssl/http/Microsoft IIS httpd 7.0 • 445/tcp -microsoft-ds/Microsoft Windows 2008 microsoft-ds • 464/tcp - kpasswd5 • 587/tcp - smtp/Microsoft Exchange ESMTP • 593/tcp - ncacn_http/Microsoft Windows RPC over HTTP • 636/tcp - tcpwrapped • 808/tcp - ccproxy-http • 912/tcp - vmware-auth/VMware Authentication Daemon(Uses VNC, SOAP) • 3268/tcp - ldap • 3269/tcp - tcpwrapped

Tabla 3.11 Puertos Abiertos

DIRECCIÓN IP EQUIPO	PUERTOS ABIERTOS/SERVICIO
192.168.0.254 Servidor Web/Correo	• 3389/tcp - microsoft-rdp/Microsoft Terminal Service • 6001,6002,6004/tcp - ncacn_http /Microsoft Windows RPC over HTTP • 6005,6006, 6007, 6009/tcp - msrpc/Microsoft Windows RPC • 53/udp - domain/Microsoft DNS 6.0.6002 • 88/udp - kerberos-sec/Windows 2003 Kerberos • 123/udp - ntp/NTP v3 • 137/udp - netbios-ns/Microsoft Windows XP netbios-ssn • 138/udp - netbios-dgm • 161/udp - snmp • 500/udp - isakmp • 389/udp - ldap • 464/udp - kpasswd5682/udp - xfr • 4500/udp - nat-t-ike • 5355/udp – llmnr • 16816/udp - desconocido • 17455/udp - desconocido • 18543/udp - desconocido • 20262/udp - desconocido • 32774/udp – algunas veces rpc12 • 34892/udp - desconocido • 41524/udp - desconocido • 46532/udp - desconocido • 49158/udp - desconocido • 57813/udp - domain/ Zoom X5 ADSL modem DNS • 57843,57958,57977,58002,58075,58178,57419,58631,58640 ,58797,59193,59207/udp - domain/Microsoft DNS 6.0.6002 • 63555/udp – desconocido

Tabla 3.11 Puertos Abiertos

DIRECCIÓN IP EQUIPO	PUERTOS ABIERTOS/SERVICIO
192.168.0.253 Servidor de Telefonía	• 80/tcp - http/Apache httpd 2.2.16 ((Ubuntu)) • 2000/tcp - cisco-sccp? 53/udp - domain • 161/udp - snmp/SNMPv1 server (public) • 513/udp - who • 685/udp - mdc-portmapper • 1053/udp -remote-as • 5000/udp -upnp • 5060/udp - sip/Asterix 1.6.2.7-1ubuntu1.1 • 5093/udp - sentinel-lm • 5353/udp - mdns/DNS-based service discovery • 9/tcp - Workstation • 16832/udp –desconocido • 17302/udp –desconocido • 19541/udp – jcp • 20752/udp – desconocido • 44253/udp – desconocido
192.168.0.252 Cámara IP	• 21/tcp - ftp • 23/tcp - telnet • 80/tcp - http • 5001/tcp - Control • 5002/tcp,udp - Audio • 5003/tcp,udp - Video • 10000/udp – ndmp • 5000/udp -upnp

Tabla 3. 11 Puertos Abiertos

3.3.2.6.2 Vulnerabilidades Encontradas

La Tabla 3.12 hace referencia a las vulnerabilidades encontradas en los equipos.

DIRECCIÓN IP EQUIPO	VULNERABILIDADES
192.168.0.1 Router	• Usuario y password de administrador por defecto. • El servidor DNS acepta peticiones de cualquier equipo. • El servidor DHCP acepta peticiones de cualquier equipo. • No se tienen filtros o restricciones implementadas en el Router.
192.168.0.254 Servidor Web/Correo	• El nombre de comunidad SNMP es el de por defecto (public) y puede ser consultado. • El servidor DNS acepta peticiones de cualquier equipo. • El estado del Firewall, es el de por defecto al momento de la instalación del Sistema Operativo.
192.168.0.253 Servidor de Telefonía	• El nombre de comunidad SNMP es el de por defecto (public) y puede ser consultado. • El estado del Firewall, es el de por defecto al momento de la instalación del Sistema Operativo.
192.168.0.252 Cámara IP	• Usuario y password de administrador por defecto. • Se puede tener acceso Vía Telnet

Tabla 3. 12 Vulnerabilidades Presentes

3.3.2.7 Extracción de Información (Simulación de Ataques)

3.3.2.7.1 Servicios y ataques que serán Testeados

SERVIDOR WEB/CORREO				
Tipo de Ataque	**Dirección IP Asociada**	**Puerto Atacado**	**Protocolo**	**Servicio Asociado al Puerto**
TCP SYN Flood[119]	192.168.0.254	80	TCP	OWA-Microsoft Outlook Web Access
UDP Flood[120]	192.168.0.254	80	UDP	OWA-Microsoft Outlook Web Access
ICMP Flood[121]	192.168.0.254	-	ICMP	Control y notificación de errores del Protocolo de Internet (IP).

Tabla 3. 13 Ataques realizados al Servidor de Correo y HTTP

SERVIDOR DE TELEFONÍA				
Tipo de Ataque	**Dirección IP Asociada**	**Puerto Atacado**	**Protocolo**	**Servicio Asociado al Puerto**
TCP SYN Flood[122]	192.168.0.253	5060	TCP	SIP, Inicio de sesiónes
UDP Flood[123]	192.168.0.253	5060	UDP	SIP, Inicio de sesiones
ICMP Flood[124]	192.168.0.253	-	ICMP	Control y notificación de errores del Protocolo de Internet (IP).
Invite Flood[125]	192.168.0.253	5060	SIP/UDP	SIP, Inicio de sesiones

Tabla 3. 14 Ataques realizados al Servidor de Telefonía

[119] hping3 -q -n -a 10.0.0.1 -S -p 80 --flood 192.168.0.254
[120] hping3 -q -n -a 10.0.0.1 --udp -p 80 --flood 192.168.0.254
[121] hping3 -q -n -a 10.0.0.1 --id 0 --icmp -d 56 --flood 192.168.0.254
[122] hping3 -q -n -a 10.0.0.1 -S -p 5060 --flood 192.168.0.253
[123] hping3 -q -n -a 10.0.0.1 --udp -p 5060 --flood 192.168.0.253
[124] hping3 -q -n -a 10.0.0.1 --id 0 --icmp -d 56 --flood 192.168.0.253
[125] ./inviteflood eth1 101 192.168.0.253 -S 4455 192.168.0.253 1000000000 -a hacker -D 5060

CÁMARA IP				
Tipo de Ataque	**Dirección IP Asociada**	**Puerto Atacado**	**Protocolo**	**Servicio Asociado al Puerto**
TCP SYN Flood[126]	192.168.0.252	80	TCP	Acceso Web
UDP Flood [127]	192.168.0.252	5003	UDP	Canal para streaming de Video
ICMP Flood [128]	192.168.0.252	-	ICMP	Control y notificación de errores del Protocolo de Internet (IP).

Tabla 3. 15 Ataques realizados a la Cámara IP

3.3.2.7.2 Resultados

Los resultados obtenidos de cada uno de los ataques se encuentran en el ANEXO 6.

3.3.2.8 Informe

El informe se encuentra en el ANEXO 7 y está constituido por:

- Objetivo
- Introducción
- Detalle de las pruebas realizadas
- Equipos utilizados
- Comparación de resultados iniciales con cada ataque realizado
- Degradación de los servicios por ataque realizado
- Resumen de ataques de denegación de servicio exitosos
- Conclusiones
- Soluciones y/o recomendaciones

---

[126] hping3 -q -n -a 10.0.0.1 -S -p 80 --flood 192.168.0.252

[127] hping3 -q -n -a 10.0.0.1 --udp -p 5003 --flood 192.168.0.252

[128] hping3 -q -n -a 10.0.0.1 --id 0 --icmp -d 56 --flood 192.168.0.252

4. LEYES Y SANCIONES QUE RIGEN EN EL ECUADOR

Con la aparición de Internet; la cultura, la ciencia y la información se encuentran al alcance de personas de todo el mundo. Pero lamentablemente, el desarrollo de las tecnologías cómo es el caso de internet, ha abierto la puerta a conductas antisociales y delictivas.

El objeto de éste capítulo es dar a conocer las leyes y sanciones ante dichas conductas en el campo de la delincuencia informática en el Ecuador.

4.1 DELITO INFORMÁTICO

El delito Informático, implica actividades criminales que en un comienzo fueron tratadas como figuras de carácter tradicional, como: robo, hurto, fraude, falsificaciones, estafa, entre otros. Hasta la fecha no se tiene una definición universal propia de delito informático, sin embargo, muchos expertos en el tema han formulado conceptos funcionales atendiendo a realidades nacionales concretas, por ejemplo:

Nidia Callegari[129] define al delito informático como: “aquel que se da con la ayuda de la informática o de técnicas anexas”.

Parker[130], define a los delitos informáticos como: “todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio”.

Sin embargo, estas y muchas otras definiciones de delitos informáticos de una u otra forma son ambiguas, debido a que no entregan una delimitación concreta en

[129] Callegari Nidia, Citada por Julio Telles Valdés. Ob. Cita.

[130] Parker, D.B, Citado por Romeo Casabona Carlos M. Poder Informático y Seguridad Jurídica.

la que pueden producirse, desde un punto de vista estrictamente jurídico, además de que no establecen con claridad los efectos susceptibles de punibilidad[131].

Antonio E. Pérez Luño señala que quienes se han preocupado del tema, han debido hacer referencia no sólo "a las conductas incriminadas de lege lata[132], sino a propuestas de lege ferenda[133], es decir, a programas de política criminal legislativa sobre aquellos comportamientos todavía impunes que se estima merecen la consiguiente tipificación penal"[134].

En resumen, la Delincuencia Transnacional y el Crimen Organizado en gran parte han sido establecidas, pero enfrentar este tipo de delincuencia es la tarea a la que se ve avocada el Ministerio Público por mandato constitucional y por disposición legal en el Ecuador.

4.2 LEGISLACIÓN NACIONAL

El Internet en Ecuador ha ido creciendo de forma significativa y las cifras publicadas por la Superintendencia de Telecomunicaciones lo confirman.

Desde la publicación presentada por la Supertel a fecha marzo del 2007, se ha tenido un crecimiento del 26,9% a fecha diciembre del 2010. Por tanto, fue esencial que se formen unidades de investigación tanto policiales como de la Fiscalía para abordar cuestiones con respecto a la delincuencia informática a nivel nacional en su Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas[135].

---

131 Huerta Miranda, Marcelo y Líbano Manzur Claudio, Los Delitos Informáticos, Editorial Jurídica Cono Sur.

132 **De lege lata.-** Expesión latina que significa: Según ley dada o existente.

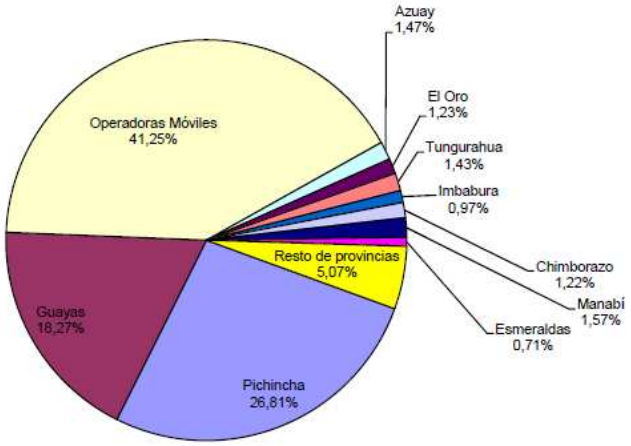
133 **De lege ferenda.-** Expesión latina que significa: Para una futura reforma de la ley.

134 Pérez Luño, Antonio Enrique. Manual de informática y derecho, Editorial Ariel S.A., Barcelona, 1996.

135 LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS http://www.derechoecuador.com/index.php?option=com_content&task=view&id=1939#anchor713582

INTERNET EN EL ECUADOR		
AÑO	USUARIOS ESTIMADOS	PENETRACION
1999	37.538	0,30%
2000	57.627	0,45%
2001	85.630	0,64%
2002	100.663	0,81%
2003	158.579	1,25%
2004	191.903	1,49%
2005	514.020	3,88%
2006	823.483	6,09%
mar-07	833.326	6,13%

a)



b)

Figura 4. 1 a) Estadísticas de Acceso a Internet a Fecha Marzo 2007 [136], b) Estadísticas de Acceso a Internet por provincias a Fecha Diciembre 2010 [138]

DATOS DE CUENTAS Y USUARIOS DE INTERNET POR PROVINCIA.

MES: DICIEMBRE
AÑO: 2010

No.	PROVINCIA	Cuentas Conmutadas	Cuentas Dedicadas	Cuentas Totales	Estimado de Usuarios Conmutados	Estimado de Usuarios Dedicados	Estimado de usuarios totales
1	Azuay	568	11249	11817	2272	74963	77235
2	Bolivar	23	2167	2190	92	15449	15541
3	Cañar	179	2686	2865	716	14148	14864
4	Carchi	89	2057	2146	356	10070	10426
5	Chimborazo	366	9457	9823	1464	54961	56425
6	Cotopaxi	96	4072	4168	384	29433	29817
7	El Oro	206	9704	9910	824	45246	46070
8	Esmeraldas	187	5497	5684	748	33404	34152
9	Galápagos	97	1175	1272	388	6249	6637
10	Guayas	2765	144133	146898	11060	859508	870568
11	Imbabura	251	7521	7772	1004	39878	40882
12	Loja	146	8621	8767	584	41578	42162
13	Los Ríos	33	4654	4687	132	21956	22088
14	Manabí	211	12436	12647	844	55271	56115
15	Morona Santiago	28	661	689	112	6406	6518
16	Napo	35	1998	2033	140	13273	13413
17	Orellana	4	1602	1606	16	10446	10462
18	Pastaza	17	1994	2011	68	12362	12430
19	Pichincha	8962	206642	215604	35848	1254766	1290614
20	Santa Elena	44	2978	3022	176	15284	15460
21	Sto. Domingo	123	2322	2445	492	9233	9725
22	Sucumbios	40	2172	2212	160	12202	12362
23	Tungurahua	374	11094	11468	1496	65984	67480
24	Zamora Chinchipe	15	678	693	60	4147	4207
	Operadoras Móviles			331.662			331.662
	Total general	**14.859**	**457.570**	**804.091**	**59.436**	**2.706.217**	**3.097.315**

El Total general de cuentas totales y usuarios totales incluye el valor de las Operadoras Móviles.

Figura 4. 2 Estadísticas de Acceso a Internet a Fecha Diciembre 2007[138]

En 1999, Ecuador comenzó con la discusión al proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas. Para tal propósito se realizaron cursos, seminarios, encuentros y se conformaron comisiones con el

[136] Superintendencia de Telecomunicaciones, http://www.supertel.gob.ec/

propósito de formular observaciones a la misma por parte de los organismos directamente interesados en el tema como el CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio, entre otros.

Dicha ley en un principio tuvo una serie de falencias. La principal fue la parte penal, debido a que las infracciones a la misma, es decir, los llamados delitos informáticos, eran sancionados de acuerdo a lo dispuesto a nuestro código penal de hace 70 años y aquellas penalidades existentes no tomaban en cuenta adelantos de la informática y telemática. Por tanto, el brindar seguridad al Comercio electrónico se tornaba inútil ante un posible asedio de la criminalidad informática.

Luego de largas discusiones, en abril del 2002 se aprobó el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados delitos informáticos.

A raíz de la aprobación de la Ley, ésta se convirtió en un instrumento que brinda un marco jurídico a las innovaciones tecnológicas relacionadas con la transmisión de información utilizando medios electrónicos y su objeto es el de regular los mensajes de datos, firmas electrónicas, servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico (e-business) y la protección a los usuarios de estos sistemas.

Entre las leyes más sobresalientes que permitirían proteger a un sujeto pasivo ante un ataque informático se pueden citar las siguientes:

El Art. 5.- Confidencialidad y reserva de la ley establece que:

“Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica,

transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia".

En dicho artículo, se establecen los principios de inviolabilidad y refiere a que el secreto de la correspondencia es una garantía establecida por Constitución Política y que todos los mensajes están amparados por estas leyes, independientemente de la forma de envío y sin consideración de su medio o intención y en el caso de que sean violados, existen mecanismos constitucionales de control legal.

Dentro de los principios de confidencialidad y privacidad, la ley también protege a la elaboración, transferencia o utilización de bases de datos. Según el Art.9. , dice que:

"Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.”

Resumiendo, se puede ver con éste artículo que existen principios constitucionales y legales de protección a la información que pueden ser enmarcados en una base de datos acompañados siempre de criterios , respeto al bien ajeno y a la propiedad privada, razón por la cual se requiere de un consentimiento previo, para que sea posible disponer del mensaje recibido e información. Incluso dichas características son nuevamente mencionadas en artículos posteriores.

La Ley considera que si se recopila y se usan datos personales sin un consentimiento previo, existe una violación a los derechos de la privacidad, confidencialidad e intimidad y serán sancionadas de acuerdo a la ley. De ésta forma se protege al consumidor de cualquier tipo de información fraudulenta y de información que no ha aceptado recibir.

De acuerdo a la Constitución Política de la República, en su Título IV, Capítulo 4to, en la sección décima al hablar de la Fiscalía General del Estado, en su Art. 195 señala que:

“La Fiscalía dirigirá, de oficio o a petición de parte, la investigación pre procesal y procesal penal; durante el proceso ejercerá la acción pública con sujeción a los principios de oportunidad y mínima intervención penal, con especial atención al interés público y a los derechos de las víctimas. De hallar mérito acusará a los presuntos infractores ante el juez competente, e impulsará la acusación en la sustanciación del juicio penal.

Para cumplir sus funciones, la Fiscalía organizará y dirigirá un sistema especializado integral de investigación, de medicina legal y ciencias forenses, que incluirá un personal de investigación civil y policial; dirigirá el sistema de

protección y asistencia a víctimas, testigos y participantes en el proceso penal; y, cumplirá con las demás atribuciones establecidas en la ley"[137].

Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que dice:

"El ejercicio de la acción pública corresponde exclusivamente al Fiscal. Sin embargo, el ejercicio de la acción pública de instancia particular, procederá solamente previa denuncia del ofendido. Lo dispuesto en el inciso anterior ha de entenderse sin perjuicio de los derechos del ofendido para acceder al órgano judicial competente, según lo previsto en este Código. El ejercicio de la acción privada corresponde únicamente al ofendido, mediante querella."[138]

Por tanto se puede concluir que el dueño de la acción penal y de la investigación tanto pre procesal como procesal de hechos considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio será el Fiscal. [139]

Por tanto, el Fiscal para esta clase de infracciones contará como señala el Art. 208 [8] con:

"La Policía Judicial realizará la investigación de los delitos de acción pública y de instancia particular, bajo la dirección y control del Ministerio Público, a fin de reunir o asegurar los elementos de convicción y evitar la fuga u ocultamiento de los sospechosos, en el tiempo y según las formalidades previstas en este Código."

Sin embargo, debido a la falta de preparación y equipos tecnológicos apropiados para realizar esta tarea, resulta esencial que se formen unidades Investigativas tanto policiales como de la Fiscalía especializadas en abordar cuestiones de la

---

[137] Constitución Política de la República, http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

[138] Código procedimiento Penal, http://www.cortesuprema.gov.ec/cn/wwwcn/pdf/leyes/codigo_procedimiento_penal.pdf

[139] Dr. Santiago Acurio Del Pino, Perfil Sobre los Delitos Informáticos en el Ecuador, Fiscalía General Del Estado.

delincuencia informática trasnacional y también a nivel nacional. Pudiendo servir también de base para una cooperación internacional ya que la cooperación multilateral de los grupos especiales multinacionales pueden resultar particularmente útiles y ha habido casos en que la cooperación internacional ha sido muy efectiva.

Por tanto, como menciona PHIL WILLIAMS Profesor de Estudios de Seguridad Internacional de la Universidad de Pittsbugh[140].

Es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la Delincuencia Informática, sino también con la infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a este nuevo tipo de delitos transnacionales.

Por tal razón, se crea en el Ecuador el Departamento de Investigación y Análisis Forense de la Fiscalía General Del Estado, el cual se encarga de enforzar la ley y poder brindar el primer paso para poseer un cuerpo especializado para combatir esta clase de criminalidad.

4.3 DELITOS INFORMÁTICOS EN EL ECUADOR

Según la reforma al Código Penal por parte de la Ley de Comercio Electrónicos, Mensajes de Datos y Firmas Electrónicas publicada en Ley No. 67. Registro Oficial. Suplemento 557 del 17 de Abril del 2002 [141] [142], se describen los siguientes delitos informáticos.

---

[140] Williams Phil, Crimen Organizado y Cibernético, sinergias, tendencias y respuestas, Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon, http://www.pitt.edu/~rcss/toc.html

[141] LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS http://www.derechoecuador.com/index.php?option=com_content&task=view&id=1939#anchor713582

[142] http://www.ceda.org.ec/descargas/biblioteca/Codigo%20Penal.doc

4.3.1 DELITOS Y PENALIDADES CONTRA LA CONFIDENCIALIDAD

La reforma al código penal del Ecuador con respecto a la protección de la información: Violación de claves o sistemas de seguridad describe lo siguiente:

Art. 58 a la Reforma del Código Penal Empleando cualquier medio electrónico, informático o afín para violentar claves o sistemas de seguridad y acceder u obtener información secreta y/o confidencial.	
Descripción	**Pena**
Simplemente vulnerar la seguridad	Prisión de 6 meses a un año y multa de $500 dólares de los Estados Unidos de Norteamérica.
Si la información refiere a seguridad nacional, secretos comerciales o industriales. ,	La pena será de uno a 3 años y multa de $500 dólares de los Estados Unidos de Norteamérica.
Divulgación y/o utilización fraudulenta de la información, secretos comerciales o industriales, será	Sancionados con pena de reclusión menor ordinaria de 3 a 6 años y multa de $2000 a $10000 dólares de los Estados Unidos de Norteamérica.
Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información	Sancionados con pena de reclusión menor de 6 a 9 años y multa de $2000 a $10000 dólares de los Estados Unidos de Norteamérica.
Obtención y utilización no autorizada de información	Pena de prisión de 2 meses a 2 años y multa de $ 1000 a $2000 mil dólares de los Estados Unidos de Norteamérica.

Tabla 4. 1 Delitos y Penalidades Contra la Confidencialidad

http://www.ceda.org.ec/descargas/biblioteca/Codigo%20Penal.doc

4.3.2 DELITOS Y PENALIDADES CONTRA LA INTEGRIDAD

La reforma al código penal del Ecuador con respecto a la integridad: Destrucción, inutilización o alteración de la información describe lo siguiente:

Art. 59 a la Reforma del Código Penal De forma maliciosa y fraudulenta, destruir o suprimir documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos.	
Descripción	**Pena**
Todo empleado público o encargado de un servicio público	Serán reprimidos con 3 a 6 años de reclusión menor
Art. 61 a la Reforma del Código Penal Destruir, alterar, inutilizar, suprimir o dañar, de forma temporal o definitiva programas, datos, bases de datos, información o cualquier mensaje de datos.	
Descripción	**Pena**
El que dolosamente lo haga de cualquier modo o utilizando cualquier método.	Prisión de 6 meses a 3 años y multa de $60 a $150 dólares de los Estados Unidos de Norteamérica.
Si se trata de información destinada a prestar un servicio público o vinculado con la defensa nacional.	La pena de prisión será de 3 a 5 años y multa de $200 a $600 dólares de los Estados Unidos de Norteamérica.
Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos.	Prisión de 8 meses a 4 años y multa de $200 a $600 dólares de los Estados Unidos de Norteamérica.

Tabla 4. 2 Delitos y Penalidades Contra la Integridad

4.3.3 DELITOS Y PENALIDADES CONTRA LA AUTENTICIDAD

La reforma al código penal del Ecuador con respecto a la autenticidad: Apropiación de un bien mediante manipulación o modificación de la información, describe lo siguiente:

Art. 62 a la Reforma del Código Penal Apropiación ilícita. Manipulación o modificación del funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.	
Descripción	**Pena**
Los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno.	Serán reprimidos con prisión de 6 meses a 5 años y multa de $500 a $1000 dólares de los Estados Unidos de Norteamérica.
Los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando,	Serán reprimidos con prisión de 6 meses a 5 años y multa de $500 a $1000 dólares de los Estados Unidos de Norteamérica
Si el delito se hubiere cometido empleando los siguientes medios: 1. Inutilización de sistemas de alarma o guarda; 2. Descubrimiento descifrado de claves secretas o encriptadas; 3. Utilización de tarjetas magnéticas o perforadas. 4. Utilización de controles o instrumentos de apertura a distancia. 5. Violación de seguridades electrónicas, informáticas u otras semejantes.	Prisión de uno a 5 años y multa de $1000 a $2000 dólares de los Estados Unidos de Norteamérica,

Tabla 4.3 Delitos y Penalidades Contra la Autenticidad

Art. 63 a la Reforma del Código Penal Con respecto al inciso anterior	
Descripción	**Pena**
El que cometiere el delito utilizando medios electrónicos o telemáticos	Pena de 5 años y multa de $500 a $1000 dólares de los Estados Unidos de Norteamérica

Tabla 4. 3 Delitos y Penalidades Contra la Autenticidad

Las estadísticas de delitos informáticos de Enero a Diciembre del 2010, proporcionada por la Fiscalía General del Ecuador, se presentan a continuación:

Tipo de Delito Informático	Cantidad de Delitos informáticos
Apropiación ilícita utilizando medios informáticos	697
Daños informáticos de servicio publico	86
Daños informáticos de servicio privado	82
Estafa utilizando medios informáticos	1
Total	866

Tabla 4. 4 Delitos informáticos en el Ecuador a fecha 20/12/2010 [143]

[143] http://www.abogados.ec/tag/estadisticas-de-delitos-informaticos-2010/

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Las estadísticas por incidentes de ataques o delitos informáticos a nivel nacional, aunque en la actualidad no son números alarmantes, señalan que van en aumento; algo que no resulta ser sorpresa debido al desarrollo de la tecnología, al mayor uso de la misma y a su mejor conocimiento.

- Siendo Internet un medio por el cual se puede obtener una cantidad enorme de información, se debe tener un control de su acceso y utilización. Ya que personas hacen uso de este medio para aplicaciones innecesarias como: descarga de archivos multimedia e incluso búsqueda de contenidos prohibidos, poniendo así en riesgo la seguridad informática de una organización.

- Las empresas tanto a nivel local como nacional, deben conocer sobre los riesgos a los cuales su sistema informático puede estar expuesto. El desconocimiento de éstos podría ocasionar una gran pérdida económica y dañar su prestigio.

- El conocimiento de ataques y delitos informáticos, a nivel académico; aún es pobre, lo que conlleva al mal uso de la tecnología y pone en riesgo la seguridad de la información e incluso la seguridad personal.

- Las alternativas y metodologías de test de intrusión desarrolladas por organismos o entidades internacionales, sirven de soporte y gran ayuda, para mitigar gran parte de los delitos informáticos, debido a que muchos de éstos son generados por el desconocimiento tanto del administrador como de los usuarios.

- La realización de un test de intrusión para verificar la seguridad en una organización crea una actitud de trabajo en equipo orientado a la seguridad, permitiendo así que el personal pueda conocer la presencia de un intruso o software mal intencionado.

- Actualmente, una de las vulnerabilidades más comunes en las redes de datos sigue siendo el mal uso de la tecnología y la exposición de los equipos de inteconectividad a personal no autorizado. Una simple falla eléctrica o un mal uso de éstos, puede ocasionar una denegación de servicio sin que haya habido un ataque informático de por medio.

- Simular ambientes reales y visualizar como éstos se comportan ante determinadas circunstancias, permite tener una idea clara de cuan segura puede ser una red de datos, y así, crear redes más confiables, sin que la real esté expuesta a los riegos que la simulación conlleva, ya que servicios críticos pueden estar comprometidos.

- En la actualidad, existen una infinidad de ataques informáticos y aplicaciones para realizarlos. Éstos se encuentran al alcance de cualquiera e incluso pueden ser utilizadas por aquellas personas no capacitadas o con pocos conocimientos técnicos, pudiendo poner en riesgo el sistema informático de una organización.

- Un ataque de Denegación de Servicio exitoso puede afectar considerablemente a un sistema y el riesgo es mucho mayor si se manejan datos críticos y en tiempo real. Por lo que administradores de red no pueden dejar cabos sueltos en la red de datos que administran.

- Aunque se tienen una gran variedad de metodologías, el éxito de éstas; dependen enormemente de la habilidad, capacidad y conocimientos de quien las realice.

- Gran parte de los ataques por inundación no solo afectan al objetivo atacado. También pueden afectar a otros servicios, debido a paquetes de respuesta provocados por los del ataque.

- Cualquier servicio en una red de datos puede ser susceptible a un ataque de Denegación de Servicio.

- Equipos Autónomos que brindan algún servicio específico a la red, como por ejemplo una cámara IP son más susceptibles a ataques informáticos; debido a la falta de seguridades a nivel de éstos.

- Mientras más grande sea una red de datos, se debe tener un mayor control, ya que por aplicaciones o programas innecesarios o mal intencionados se podría estar generando tráfico basura y saturando el ancho de banda de la red.

- Si se requiere el monitoreo periódico y prácticamente real de la red. MRTG es una muy buena solución, siempre y cuando sea complementado con alguna otra herramienta, debido al promedio de tiempo de 5 min entre cada captura de información.

- Los sistemas Windows son mayormente afectados por ataques DoS que los LINUX.

- El desconocimiento de las leyes no libra de culpa a las personas que las infringen.

5.2 RECOMENDACIONES

- A nivel académico, el instruir a los estudiantes sobre los diferentes tipos de delitos informáticos y las penalidades que éstos tienen por los organismos de control; se puede crear una cultura tal que permita diferenciar entre el buen y mal uso de la tecnología, ya que en la actualidad la mayoría de las personas desconocen del tema y pueden infringir la ley sin conocerlo.

- Desarrollar metodologías y alternativas para contrarrestar los delitos informáticos, ayudará a las organizaciones, empresas e instituciones a tener redes más seguras y confiables.

- Es necesario concientizar a las personas, administradores y personal acerca del uso de las diferentes herramientas de administración de red como por ejemplo, aquellas que han sido utilizadas en este proyecto de titulación, ya que el factor ético es importante para no caer en un delito informático y realizar actividades que se encuentren al margen de la ley.

- Simular como se comportan algunos dispositivos de red, tales como cámaras IP; frente a determinados ataques informáticos, permitirá conocer los posibles riegos a los cuales se exponen y las medidas que deben tomar para en lo posible contrarrestarlos, antes de hacerlos parte de la red de datos de una organización.

- En lo posible, un sistema debe ser instalado y configurado de tal forma que ocupe la menor cantidad de recursos tanto de sistema (CPU, Memoria, Espacio en Disco) como de red, considerando los requerimientos del servicio presente para no disminuir su rendimiento.

- Una red de datos con seguridades implementadas a nivel de router y con firewalls activos, pueden disminuir considerablemente posibles ataques de Denegación de Servicio desde y hacia la red.

- El acceso a internet debe ser monitoreado y controlado, para evitar la descarga de aplicaciones innecesarias que puedan comprometer al correcto funcionamiento de la red.

- Cambiar las configuraciones por defecto del fabricante de los equipos de interconexión u otros como: routers, switches, cámaras Ip, entre otros.

- Realizar las actualizaciones de Software y Sistema Operativo requeridos en horas no laborables.

- Mantener un control de aplicaciones instaladas, servicios ejecutándose y bloquear todos aquellos puertos innecesarios.

- Si no se requiere, se recomienda deshabilitar Mensajes ICMP en equipos críticos, así como, deshabilitar los LOGS generados por los diferentes servicios.

- Utilizar e instalar Software de casas comerciales conocidas y legítimas. No hacerlo, se puede correr el riesgo de infectar a los equipos e incluso éstos podrían infectar a otros.

- Ecuador aunque ya dispone de una ley tal que permita juzgar y penalizar un delito informático debería ser continuamente puesta en debate y actualizada, ya que los ataques informáticos van difiriendo en su forma, objetivo y efecto.

BIBLIOGRAFÍA

Libros y Manuales

- Andrew S. Tanenbaum, Redes de Computadoras, 3era Edición, Prentice-Hall, 1998.

- William Stallings, Comunicaciones y Redes de Computadoras, 6ta Edición, Prentice-Hall ,2000.

- Chris McNab, Seguridad de Redes, 1ra Edición, Anaya Multimedia,

- SEGURIDAD EN INTERNET. PARTE I: ATAQUES, TECNICAS Y FIREWALLS Jesús Ibáñez Martínez, Antonio Gómez Skarmeta, Humberto Martínez Barberá

- Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks (pdf), http://www.ece.cmu.edu/~adrian/projects/secure-routing/infocom2003.pdf

- Dr. Tom Shider´s ISA Server 2006 Migration Guide, Escrito por Thomas W. Shinder,Debra Littlejohn Shinder,Adrian F. Dimcev

- Handbook of information security, Volumen 3 Escrito por Hossein Bidgoli

- The Internet encyclopedia, Volumen 1 Escrito por Hossein Bidgoli

- CEH:Official certified ethical hacker review guide Escrito por Kimberly Graves

- Sistemas Distribuidos de denegación de servicios Fernando Limón Martínez, flimon@fi.upm.es, http://fi.upm.es/~flimon, Madrid, Junio de 2000, http://panoramix.fi.upm.es/~flimon/ddos.pdf

- The Case for Modeling and Simulation of Information Security John H. Saunders, Ph.D., GSEC, National Defense University

- The Role of Modeling and Simulation in Information Security The Lost Ring Mohammad Heidari, February 3, 2006

Direcciones Electrónicas

- http://www.monografias.com/trabajos24/redes-computadoras/redes-computadoras.shtml
- http://es.wikipedia.org/wiki/Cliente-servidor
- http://es.wikipedia.org/wiki/Peer-to-peer
- http://es.wikipedia.org/wiki/Red_de_computadoras
- http://es.wikipedia.org/wiki/Modelo_OSI
- http://es.wikipedia.org/wiki/Modelo_TCP/IP
- http://es.wikipedia.org/wiki/Transmission_Control_Protocol
- http://tools.ietf.org/html/rfc3168
- http://www.fing.edu.uy/iie/ense/asign/redes2/material/026-Repaso%20TCP.pdf
- http://quegrande.org/apuntes/EI/3/RC/teoria/07-08/tema_6.pdf
- http://es.wikipedia.org/wiki/Udp
- http://es.wikipedia.org/wiki/Internet_Protocol
- http://es.wikipedia.org/wiki/Cabecera_IP
- http://es.kioskea.net/contents/internet/protip.php3
- http://www.profesores.frc.utn.edu.ar/sistemas/ingsanchez/Redes/Archivos/datagramaIP.asp
- http://es.wikipedia.org/wiki/Servidores
- http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

- http://www.profesores.frc.utn.edu.ar/sistemas/ingsanchez/Redes/Archivos/Protocolo_ICMP.pdf
- http://www.iana.org/assignments/icmp-parameters
- http://www.rfc-es.org/rfc/rfc0792-es.txt
- http://tools.ietf.org/html/rfc792
- http://es.wikipedia.org/wiki/Internet_Control_Message_Protocol
- http://www.scribd.com/doc/16000888/SWITCHES-DE-CAPA-3http://es.wikipedia.org/wiki/Router
- http://www.iana.org/assignments/port-numbers
- http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_0.pdfhttp://www.tics.org.ar/index.php?option=com_content&view=article&id=97:conceptos-de-hacking-etico&catid=14:seguridad-informca&Itemid=31
- http://innovotech.byethost31.com/Archivos/pilodx1.pdf
- http://www.ks-soft.net/ip-tools.esp/index.htm
- http://xa.yimg.com/kq/groups/19983860/267895181/name/Primera+Monografia_+Seguridad+Informatica.pdf
- http://nmap.org/
- http://www.hping.org/
- http://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL
- http://technet.microsoft.com/es-es/library/cc731451(WS.10).aspx
- http://jcef.sourceforge.net/doc/introsecurity.pdf
- http://technet.microsoft.com/es-es/library/cc736596(WS.10).aspx
- http://www.netfilter.org/documentation/HOWTO/es/packet-filtering-HOWTO-3.html
- http://technet.microsoft.com/es-es/library/cc736939(WS.10).aspx
- http://es.wikipedia.org/wiki/Autenticaci%C3%B3n
- http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)
- http://estatico.buenosaires.gov.ar/areas/sistemas/FirmaDigital.pdf
- http://www.miginside.com/content/view/650/97/
- http://www.siicex.gob.pe/siicex/resources/capacitacion/6775ce6a-09a5-4b24-b25a-ad1ab2558cac.pdf

- http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos
- http://www.symantec.com/connect/articles/introduction-distributed-intrusion-detection-systems
- http://es.wikipedia.org/wiki/Ataques_de_denegaci%C3%B3n_de_servicio
- http://denialofservice.uw.hu/ch03lev1sec3.html
- http://staff.washington.edu/dittrich/misc/ddos/
- http://www.wired.com/science/discoveries/news/1997/01/1446
- http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html
- http://www.elpais.com/articulo/internet/ataque/denegacion/servicio/colapsa/Telefonica/net/Terra/elpeputec/20060302elpepunet_8/Tes
- https://www.ac.usc.es/docencia/ASRII/Tema_3html/node16.html
- http://hacker-dox.net/Que-Certified.Ethical.Hacker.E/0789735318/ch07lev1sec6.html
- http://hcshack.blogcindario.com/2010/06/00021-ataque-ddos.html
- http://www.worldlingo.com/ma/enwiki/es/WinNuke
- http://articles.techrepublic.com.com/5100-10878_11-1054537.html
- http://es.mcafee.com/common/es/products/fw4/fw4_product_guide.pdf
- http://www.outpost-es.com/support_faq_kb/1000193.html
- http://www.physnet.uni-hamburg.de/physnet/security/vulnerability/newtear.html
- http://osvdb.org/5730
- http://www.wired.com/science/discoveries/news/1998/01/9581
- http://www.physnet.uni-hamburg.de/physnet/security/vulnerability/boink.html
- http://www.techotopia.com/index.php/An_Overview_of_IT_Security_Threats_and_Attacks
- http://www.telecable.es/personales/peta_zeta/irc/guerras.htm
- http://about-threats.trendmicro.com/ArchiveVulnerability.aspx?language=us&name=ARP%20Floodin g%20Attack
- http://www.cert.org/advisories/CA-99-08-cmsd.html
- http://service1.symantec.com/sarc/sarc.nsf/html/W32.DoS.Trinoo.html

- http://www.counterpane.com/bfsverlag.html
- ftp://ftp.fi.upm.es/pub/docs/rfc/26xx/2612
- http://www.cert.org/incident_notes/IN-99-04.html
- http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos
- http://es.kioskea.net/contents/detection/ids.php3
- http://www.virusprot.com/Art40.htm
- http://www.idg.es/iworld/articulo.asp?id=152376
- http://www.cert.org/tech_tips/
- http://www.cert.org/advisories
- http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3925&Itemid=426
- http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3091&Itemid=426
- http://www.monografias.com/trabajos14/delitos-informaticos/delitos-informaticos.shtml
- http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/acurio1.pdf
- http://www.conatel.gob.ec/site_conatel/index.php?option=com_content&view=article&catid=48:normas-del-sector&id=98:ley-de-comercio-electronico-firmas-electronicas-y-mensajes-de-datos&Itemid=103
- http://www.supertel.gob.ec/pdf/estadisticas/acceso_internet.pdf
- http://www.cortesuprema.gov.ec/cn/wwwcn/pdf/leyes/codigo_procedimiento_penal.pdf
- http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf
- http://oss.oetiker.ch/mrtg
- www.hping.org

Listado de Anexos

ANEXO 1: DEFINICIONES Y TERMINOLOGÍA

ANEXO 2: EJEMPLO DE HERRAMIENTAS DE USO DE LOS HACKERS

ANEXO 3: EVOLUCIÓN HISTÓRICA DE LOS ATAQUES DE DENEGACIÓN DE SERVICIO DOS

ANEXO 4: COMPARACIÓN DE ATAQUES DOS y DDOS

ANEXO 5: CONFIGURACIÓN MRTG Y ESTADOS INICIALES

ANEXO 6: RESULTADOS OBTENIDOS DE LA SIMULACIÓN DE ATAQUES DOS EN LA RED DE PRUEBAS IMPLEMENTADA

ANEXO 7: INFORME FINAL

ANEXO 1

Definiciones y Terminología

Definiciones y Terminología

- **Vulnerabilidad:** El término vulnerabilidad puede ser aplicado a diversos campos para el caso de vulnerabilidad informática se refiere a un defecto, error, falencia o brecha en el diseño, configuración o implementación de un sistema que pueda comprometer la seguridad.

- **Amenaza:** Representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad representa el grado de exposición a las amenazas en un contexto particular.

- **Exploit:** Un exploit es una pieza de software o una secuencia de datos con el fin de aprovechar las vulnerabilidades y causar un comportamiento no deseado o imprevisto en programas, hardware o componente electrónico y con frecuencia incluye la violenta toma de control de un sistema.

- **Virus informático:** Un Virus informático tiene por objeto alterar el normal funcionamiento de un sistema sin el permiso o el conocimiento del usuario. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

- **Gusanos:** Es un tipo de virus informático que se auto genera a sí mismo. Permanece en la memoria del sistema consumiendo recursos y dejado al sistema lento o inoperable.

- **Troyanos:** Es un software malicioso que es presentado al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños. Pueden realizar diferentes tareas. En la mayoría de casos crean una puerta trasera o backdoor.

- **Footprinting:** Es el primer paso y el paso más importante que usan los Hackers para obtener información antes de lanzar un ataque, a este paso

se le conoce también como la Fase 2 o Fase de Reconocimiento, la cual será discutida posteriormente en la parte de Modos de Hacking.

- **Herramientas o Utilidades TCP/IP:** Son herramientas informáticas que permiten diagnosticar, analizar y ofrecer información útil de una red de datos.

- **Pirata o Delincuente Informático:** Son aquellos hackers que emplean sus conocimientos con fines ilegales o inmorales, llamados también crackers.

- **Puertos:** Un puerto en informática puede tener dos significados:

    - En un computador, es una interfaz por donde ingresa o se envía información permitiendo conectar físicamente distintos dispositivos como monitores, impresoras, escáneres, discos duros, cámaras digitales, memorias pendrive, etc.

    - En TCP/IP, son números lógicos que se asignan a las conexiones, tanto en el origen como en el destino para comunicarse con una aplicación específica.

- **Ingeniería social:** En la mayoría de los casos, el eslabón más débil es el mismo usuario. Muchas veces es él quien, por ignorancia o a causa de un engaño, genera una vulnerabilidad en el sistema al brindar información al atacante. Cuando ello sucede, ningún dispositivo puede proteger al usuario contra la falsificación: sólo el sentido común, la razón y el conocimiento básico acerca de las prácticas utilizadas pueden ayudar a evitar este tipo de errores.

- **Puertas traseras o Backdoors:** Permiten dar acceso a un sistema en cualquier momento.

ANEXO 2

EJEMPLO DE HERRAMIENTAS DE USO DE LOS HACKERS

HERRAMIENTAS DE USO DE LOS HACKERS

Para un mejor entendimiento, éstas serán divididas según la fase que usa el hacker para alcanzar su propósito.

HERRAMIENTAS DE RECONOCIMIENTO

- **Ingeniería social:** Es la práctica de obtener información confidencial a través de la manipulación de usuarios.

- **Motores de Búsqueda:** Son sistemas informáticos encargados de buscar sitios web y archivos almacenados en servidores web. Mediante estos se puede encontrar información fundamental de un objetivo como la URL de una empresa, dirección, contactos, entre otros. Un ejemplo simple es el caso de google.

- **DNSStuff:** Es un sitio web de pago en el cual se puede verificar el estado y la configuración de los servidores, dominios, direcciones IP entre otros.

- **IPTools:** Servicio web gratuito que ofrece varias utilidades TCP/IP como: Ping, Traceroute, DNS Lookup, entre otros.

- **SiteLogr:** Servicio web gratuito que proporciona información valiosa de cada sitio web. Una característica única es poder dar una estimación de la cantidad de visitas de un sitio web.

- **FreeDNSInfo:** Servicio web gratuito similar a IPTools con una interfaz más agradable.

- **Intodns:** Servicio web gratuito prácticamente igual a dnsstuff que en conjunto con iptools la igualan.

- **WhatsmyIp:** Servicio web gratuito para conocer la dirección IP pública.

HERRAMIENTAS DE RASTREO O ESCANEO

- **HPING:** Es una aplicación gratuita en línea de comandos que permite analizar y crear paquetes TCP, UDP o ICMP

- **NMAP (Network Mapper):** Es una herramienta de código abierto (open source) que sirve para visualizar servicios que se ejecutan, versión y tipo de sistema operativo, efectuar rastreo de puertos, obtener características de hardware de red, identificar computadoras en una red , en resumen se la utiliza para evaluar la seguridad de sistemas informáticos.

- **Netscan:** Es una sencilla aplicación que permite escanear puertos de cualquier dirección IP.

- **Megaping:** Es una aplicación de pago que proporciona una visión general de la configuración de un sistema, desde el análisis de puertos, IP o NetBIOS hasta herramientas de Whois o búsqueda de DNS. Incluye utilidades de red como monitorización de puertos, ping, traceroute, finger, procesos activos en el sistema, uso de memoria, estadísticas de protocolo, entre otros.

- **Httprint:** No es una aplicación de código abierto (open source) sin embargo está disponible gratuitamente para uso personal y permite obtener información importante acerca de los servidores web, detecta y muestra los dispositivos de red, cuando un servidor ha movido su contenido a otros servidores, detecta automáticamente SSL y si el puerto SSL está activado o no.

- **Nessus:** Es un programa de escaneo de vulnerabilidades, que realiza el escaneo en el sistema objetivo y después intentar varios exploits para atacarlo.

HERRAMIENTAS PARA ACCESO

- **Inyección SQL:** Consiste en la modificación, inserción o "inyección" de un código SQL "invasor" dentro de otro código SQL para alterar así su funcionamiento normal, y hacer que se ejecute código malicioso en la base de datos.

- **Telnet:** Usado para acceder remotamente a otra máquina, es decir, sin necesidad de estar físicamente frente a ella.

- **Metasploit Framework:** Es un sub proyecto de *Metasploit* de código abierto (open source). Herramienta que permite desarrollar y ejecutar exploits contra una máquina remota.

HERRAMIENTAS PARA MANTENER EL ACCESO

- **Backdoor (puertas traseras):** Generalmente estos programas se hacen pasar por otros, para que el usuario los instale por error. Es una secuencia especial dentro del código de programación mediante la cual se puede acceder al sistema. Las puertas traseras más simples se encuentran a la escucha en un determinado puerto, el atacante solo tiene que ejecutar un telnet al puerto y podrá acceder al sistema. Algunos ejemplos de puertas traseras son: Back Orifice y NetBus, SubSeven, entre otros.

- **Netcat:** Es una herramienta de código abierto (opensource) que permite a través de línea de comandos y de forma sencilla abrir puertos TCP/UDP en un HOST (quedando netcat a la escucha), asociar una shell a un puerto en concreto (para conectarse por ejemplo a MS-DOS o al intérprete bash de Linux remotamente) y forzar conexiones UDP/TCP.

- **Troyanos:** Es un software malicioso que es presentado al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona

daños. Pueden realizar diferentes tareas, pero, en la mayoría de los casos crean una puerta trasera o backdoor.

HERRAMIENTAS PARA BORRADO DE HUELLAS

- **Auditpol:** Si el sistema atacado tiene las opciones de auditoría activadas puede que delaten un acceso no deseado a la cuenta Administrador. Para poder eliminar esta información se utiliza auditpol la cual permite cambiar las opciones del auditor y anular el registrador de sucesos.

- **Elsave:** Permite eliminar todo lo que haya recogido el registro de sucesos.

- **Evidence Eliminator o Eliminador de Evidencia**: Es una aplicación pagada que permite la eliminación de toda clase de rastros que se hayan realizado al navegar por la Web y también otros relacionado con ello: desde historiales y archivos temporales, hasta referencias propias del inicio y caché de memoria.

- **WINZAPPER:** Es una herramienta gratuita que permite borrar registros de eventos de manera selectiva en el registro de seguridad de Windows NT 4.0 y Windows 2000.

- **Ads Spy:** Es una pequeña herramienta, para listar, ver y borrar ADS (Alternate Data Streams) en Windows 2000/XP.

- **Hijackthis:** Herramienta gratuita que ayuda al usuario a detectar software malicioso para los sistemas Microsoft Windows. Hijackthis no auto detecta ni elimina spyware, sino que puede ayudar al usuario experto a detectarlo, siendo no recomendable el uso por usuarios inexpertos debido al riesgo de borrar software vital del sistema.

ANEXO 3
EVOLUCIÓN HISTÓRICA DE LOS ATAQUES DE DENEGACIÓN DE SERVICIO DoS

EVOLUCIÓN HISTÓRICA DE LOS ATAQUES DE DENEGACIÓN DE SERVICIO DoS

A finales de 1980, fue creado el Centro de Coordinación CERT (Computer Emergency Response Team) originalmente fundado por DARPA, en respuesta a la aparición del primer ejemplar de Malware auto replicable que afecto a internet, llamado gusano Morris.

Hoy en día el objetivo del CERT es trabajar junto a la comunidad Internet para facilitar su respuesta a problemas de seguridad informática que afecten a los sistemas centrales de Internet, dar pasos proactivos para elevar la conciencia colectiva sobre temas de seguridad informática y llevar a cabo tareas de investigación que tengan como finalidad mejorar la seguridad de los sistemas existentes.

En la Década de 1990, después del incidente del gusano Morris, Internet siguió creciendo y los primeros programas para realizar ataques DoS aparecieron y empezaron a causar problemas en los sistemas. Para hacer uso de estos programas se necesitaban computadoras grandes y de redes con altas velocidades de transmisión, lo que dio lugar a robos de cuentas en universidades debido a su facilidad de identificar y cerrar.

a) 1996, se descubre vulnerabilidad en el protocolo TCP/IP, permitiendo la inundación de paquetes con sólo el bit SYN establecido, se convirtió en la primera herramienta popular y eficaz a utilizar para dejar a los servidores inoperativos y no disponibles.

b) 1997, ataques DoS a redes de comunicación en tiempo real (IRC, Internet Relay Chat) empezaron a producirse[144]. Como por ejemplo el ataque de un

[144] Valinor, Definition of IRC Channel Takeover, http://www.valinor.sorcery.net/glossary/channel-takeover.html.

hacker rumano que hizo caer a Undernet, una de las mayores redes IRC del mundo con un ataque de inundación SYN[145].

Un caso digno de mención fue el cierre completo de la Internet debido a un anuncio (no malicioso) de ruta falsa por un único router[146].
Otra técnica efectiva que apareció alrededor de éste año fue una forma de reflejarse, es decir, un ataque DoS amplificado mediante el rebote de los paquetes, llamado ataque smurf (smurf attack).

Otros ataques como: teardrop*,* boink *y* bonk permitieron que un atacante a voluntad haga fallar los sistemas. En su mayor parte, debido a simples errores que fueron corregidos en versiones posteriores de los sistemas operativos afectados. Por ejemplo, hubo una serie de errores en la forma en que Microsoft Windows manejaba los paquetes fragmentados TCP/IP cuando el desplazamiento y longitud de los mismos no coincidían.

c) 1998, la capacidad de controlar un gran número de ordenadores de forma remota para enviar por la red cantidades masivas de tráfico inservible con el objeto de inundar a la víctima o víctimas, dio lugar a la aparición de nuevos ataques denominados DDoS o Distribuidos de Denegación de Servicio.

Prototipos de herramientas para realizar éste tipo de ataques DDoS fueron desarrollados a mediados de éste año siendo el más notable fapi[147]. Estos servían como ejemplo de cómo crear redes DDoS cliente-servidor y fue la prueba de que la coordinación de equipos era posible en un ataque.

---

[145] K. Coale, Romanian Cracker Takes Down the Undernet, Wired News, 14 de Febrero de 1997, http://www.wired.com/news/technology/0,1282,1446,00.html.

[146] V. J. Bono, 7007 Explanation and Apology, Abril de 1997
http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html.

[147] CERT Coordination Center, Results of the Distributed-Systems Intruder Tools Workshop, Diciembre 1999, http://www.cert.org/reports/dsit_workshop-final.html.

Los atacantes preparan la lista de sus ataques mediante un sondeo de víctimas potenciales con el correcto sistema operativo mediante una técnica denominada OS fingerprinting o toma de huella dactilar del sistema operativo[148].

La red de la Universidad de Washington al igual que varios civiles de una agencia espacial de Estados Unidos fueron víctimas de estos ataques durante el mismo periodo de tiempo. Usuarios de muchos lugares estuvieron sujetos a parchear inmediatamente sus sistemas ya que posteriores ataques controlados demostraron claramente que los sistemas sin parches eran propensos a que caigan y sus pantallas se tornen de color azul.

Posteriormente los ataques combinaron múltiples vulnerabilidades de DoS en una sola herramienta, usando scripts shell de Unix. Como por ejemplo: rape o targa (Programa pre compilado para realizar múltiples ataques DoS, fue desarrollado por Mixter llamado como targa.c. siendo más fácil de almacenar, transferir y usar.).

Una herramienta como ésta, tiene la ventaja de permitir a un atacante lanzar múltiples ataques con una única dirección IP, incrementando de ésta forma la probabilidad de éxito en el ataque, pero también significa tener un completo set de versiones pre compiladas de cada una en formato de archivo Unix “tar”.

La misma estrategia fue usada de Nuevo en el año 2003 por *Agobot/Phatbot.* Incluso herramientas DoS combinadas como targa todavía permiten solo a un atacante denegar el servicio de una dirección IP a la vez y requieren el uso de cuentas robadas de sistemas que tengan el máximo ancho de banda posible (predominantemente sistemas universitarios).

d) El verano de 1999 observó el primer ataque a larga escala con nuevas herramientas de denegación de servicio DoS como son: Trinoo*[149],* Tribe Flood

[148] M. Smart, R. Malan y F. Jahanian, Defeating TCP/IP Stack Fingerprinting, Proceedings of the 9th USENIX Security Symposium, Agosto del 2000.

Network (TFN)[150] *y* Stacheldraht[151]*.* Todas estas herramientas fueron simples programas cliente/servidor y agentes.

Un ataque prominente usando la herramienta Trinno[27], fue lanzado contra el servidor IRC de la Universidad de Minnesota y a decenas o más clientes IRC repartidos por todo el mundo y fue lo suficientemente grande para mantener las redes de universidades inutilizables por casi 3 días completos, haciendo uso de al menos 227 computadoras de los cuales 114 pertenecían a computadoras ubicadas en Internet2[30]. La Universidad de Minnesota contó 2500 hosts atacados, siendo ésta solo una subestimación.

El cambio al uso de herramientas distribuidas era inevitable. El crecimiento del ancho de banda que se produjo junto al progreso de Internet2[152] hizo que las herramientas punto a punto simples sean menos efectivas contra las redes bien abastecidas, y los ataques que utilizan un único host para las inundaciones fueron fáciles de bloquear, rastrear y detener.

Ataques similares, aunque a una escala ligeramente menor, continuaron hasta finales del otoño de 1999, utilizando nuevas herramientas que imitan las direcciones origen, haciendo aun más difícil la identificación de los atacantes.
Casi todos estos ataques estaban dirigidos a las redes de IRC, pero hubo muy poca cobertura de noticia de ellos. Tribu Flood Network (TFN), Stacheldraht y luego Tribe Flood Network 2000 (TFN2K) vieron el uso popular, mientras que Shaft se presentó en ataques más limitados.

---

[149] D. Dittrich, The DoS Project's Trinoo Distributed Denial of Service Attack Tool, Octubre de 1999, http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt.

[150] D. Dittrich, The Tribe Flood Network Distributed Denial of Service Attack Tool, Octubre de 1999, http://staff.washington.edu/dittrich/misc/tfn.analysis.txt.

[151] D. Dittrich, The Stacheldraht Distributed Denial of Service Attack Tool, Diciembre de 1999, http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt

[152] Internet2, http://www.internet2.edu/.

En noviembre de 1999, el CERT patrocino por primera vez un taller para discutir y dar respuesta a una situación que se veía como un problema significativo, en razón a herramientas distribuidas que usaban los atacantes incluyendo (scanners distribuidos, sniffers distribuidos, y herramientas de ataques de denegación de servicio distribuidos).

Con el producto de ese trabajo se generó un reporte[18], que abarcó el tema desde múltiples perspectivas (las de los directivos, administradores de sistemas, proveedores de servicios de Internet, y los equipos de respuesta a incidentes).

Este reporte es todavía uno de los mejores para comenzar a entender los ataques distribuidos de denegación de servicio DDos y que hacer al respecto a inmediato, mediano y largo plazo.

Irónicamente, pocos días después de este taller, una nueva herramienta fue descubierta, sin embargo, obedeció a los mismos principios de ataque como Trinoo, TFN y Stacheldraht [20,153,154.]

Esta nueva generación de herramientas incluían características como encripción para que sean difíciles de detectar y contra atacar, varios métodos de ataque, funciones de chat integrado y presentación de informes de las tasas de inundación de paquetes.

En la década del 2000, Ataques de denegación de servicio a mayor escala fueron sucintándose.

a) 2000, un ISP local en Seattle, Washington, llamado Oz.net fue atacado[155]. Posiblemente una inundación ICMP Echo reply haciendo uso de una herramienta

[153] D. Dittrich, The Tribe Flood Network Distributed Denial of Service Attack Tool, Octubre de 1999, http://staff.washington.edu/dittrich/misc/tfn.analysis.txt.

[154] D. Dittrich, The Stacheldraht Distributed Denial of Service Attack Tool, Diciembre de 1999, http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt

[155] D. Richman, Internet Attack Slows Web to a Crawl, Seattle Post-Intelligencer, 18 de Enero del 2000, http://seattlepi.nwsource.com/local/smrf18.shtml.

como Stacheldraht. El ataque no solo era dirigido contra los servidores de Oz.net, sino también a sus routers, los routers de su proveedor Semaphore upstream, y los routers del proveedor upstream UUNet. Se estima que la ralentización en el tráfico de red, afecto el 70% de la región circundante de Seattle.

Pocas semanas después de este ataque, en febrero del 2000, una serie de ataques DDoS perpetraron con éxito varios sitios de marcas importantes de Internet como: la empresa eBay, Yahoo, E * Trade, Buy.com, Amazon.com, Excite.com, y la páginas de sitios de noticias CNN[156].

A pesar de no haber sido tan sofisticados los ataques contra todos estos sitios tuvieron bastante éxito. Por ejemplo el ataque a Yahoo en Febrero del 2000 impidió a los usuarios tener conectividad constante a ese sitio durante tres horas. Como resultado de ello, Yahoo tuvo una pérdida de $ 500000.
Incluso el propio sitio web del FBI fue puesto fuera de servicio durante tres horas en febrero del 2000 por un ataque DDoS[157].

b) 2001, un ataque DDoS reflejado[158] en futuresite.register.com[159] utilizo peticiones DNS falsas bajo la identidad de una víctima y éstas fueron enviadas a muchos de los servidores DNS en todo el mundo para generar tráfico y éstos servidores enviaron la información no deseada a la víctima. La cantidad de tráfico entrante a la dirección IP de la víctima reporto ser de 60 a 90 Mbps. Con un sitio de presentación de reportes, se vio que hubo aproximadamente 220 peticiones de DNS por minuto y por cada servidor DNS que duro alrededor de una semana.

---

[156] A. Harrison, Cyberassaults Hit Buy.com, eBay, CNN, and Amazon.com, Computerworld, 9 de Febrero del 2000, http://www.computerworld.com/news/2000/story/0,11280,43010,00.html.

[157] CNN, FBI Web Site Hacked Last Week, 26 de Febrero del 2000, http://www.cnn.com/2000/TECH/computing/02/26/fbi.hackers/.

[158] V. Paxson, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, ACM SIGCOMM Computer Communications Review, volumen. 31, No. 3, Julio del 2001, Páginas. 38-47.

[159] SANS UNISOG e-mail list, Thread on Register.com DNS Attack, http://staff.washington.edu/dittrich/misc/ddos/register.com-unisog.txt.

En el mismo año, David Moore, Geoffrey Voelker, y Savage Stephan publicaron un artículo titulado " Inferring Internet Denial-of-Service Activity"[160]. En este trabajo se investigo de forma amplia la actividad DDoS en Internet. Técnicas similares para la detección de ataques y evaluación eran ya usadas entre los administradores de red y analistas de seguridad de la red, como por ejemplo el artículo Analyzing Distributed Denial Of Service Tools, escrito por: Sven Dietrich, Goddard Space, Neil Long y David Dittrich[161].

Microsoft, destacado en la industria se ha convertido en un blanco frecuente de ataques. Muchos de ellos han fracasado, sin embargo, algunos llegan a tener éxito. Por ejemplo, en enero del 2001 alguien lanzó un ataque DDoS a uno de los routers de Microsoft, impidiendo que pueda enrutar normalmente su tráfico en las velocidades requeridas[162].

Si bien prácticamente toda la red de Microsoft estaba funcionando y disponible para el uso, muchos usuarios no pudieron hacer uso de ella, debido a que sus solicitudes para traducir los nombres de sitio Web de Microsoft en direcciones IP fueron rechazadas por el router sobrecargado. Este ataque tuvo tanto éxito que la fracción de las solicitudes Web que Microsoft fue capaz de manejar se redujo al 2%.

c) 2002, quizá inspirado por el éxito anteriormente comentado, en octubre del 2002, un atacante dio un paso más y trató de realizar un ataque DDoS al conjunto completo de servidores raíz DNS de Internet.

DNS es un servicio fundamental para muchos usuarios de Internet, por lo que los datos DNS son guardados en servidores que no sean raíz a través de internet y

---

[160] D. Moore, G. Voelker, and S. Savage, Inferring Internet Denial-of-Service Activity, Proceedings of the 10th USENIX Security Symposium, Augosto del 2001, Páginas. 9-22.

[161] S. Dietrich, N. Long, and D. Dittrich, Analyzing Distributed Denial of Service Tools: The Shaft Case, Proceedings of 14th USENIX Systems Administration Conference (LISA 2000), Diciembre del 2000, Páginas. 329-339, http://www.adelphi.edu/~spock/lisa2000-shaft.pdf.

[162] M. Delio, Microsoft Crashes: The Fallout, Wired News, 26 de Enero del 2001, http://www.wired.com/news/business/0,1367,41454,00.html.

se replican a 13 servidores raíz bien provistos y mantenidos. En varios momentos durante el ataque, 9 de los 13 servidores raíz fueron incapaces de responder a las peticiones DNS, y sólo 4 se mantuvieron plenamente operando en todo el ataque.

El ataque duro solo una hora gracias al diseño robusto de DNS y debido a la corta duración del ataque, no hubo un impacto grave en Internet como conjunto. Sin embargo, un ataque más largo y fuerte hubiese sido muy perjudicial.

d) 2003, no fue hasta éste año que un gran cambio en las motivaciones y las metodologías de ataque comenzaron a aparecer.

En primer lugar, spammers comenzaron a utilizar redes distribuidas de la misma manera como los atacantes DDoS en establecer redes de distribución de spam[163]. Como sitios antispam trataron de contrarrestar estos "spam bots", los spammers tomaron represalias atacando a varios sitios anti-spam[164]. Utilizaron herramientas estándar de DDoS, e incluso gusanos como W32/Sobig[165], libraron constantes ataques contra aquellos que percibían ser una amenaza a su negocio muy lucrativo.

En Segundo lugar, otros delitos financieros comenzaron a involucrar el uso de DDoS.En algunos casos, los comerciantes en línea a diferencia de los sitios más grandes como los que fueron atacados en febrero del 2000, también fueron atacados. Ataques similares se libraron también contra sitios de juego en línea y pornografía. En algunos casos se hicieron intentos de extorsión por sumas de decenas de miles de dólares para detener los ataques (una nueva forma de chantaje)[166].

---

[163] K. Poulsen, SecurityFocus, Rise of the Spam Zombies, The Register, 27 de Abril del 2003, http://www.theregister.co.uk/content/55/30414.html.

[164] A. Jesdanun, New computer Virus Variant Floods Web Sites of Anti-Spam Activists, Associated Press, 3 de Diciembre del 2003, http://www.securityfocus.com/news/7575.

[165] J. Leyden, Sobig linked to DDoS attacks on Anti-spam Sites, The Register, 25 de Septiembre del 2003, http://www.theregister.co.uk/content/56/33059.html.

[166] C. Nuttall, Crime Gangs Extort Money with Hacking Threat, The Financial Times, 11 de Diciembre del 2003, http://www.rense.com/general44/hack.htm.

Durante la guerra de Irak, un ataque DDoS fue lanzado a la organización de noticias Al-Jazeera con sede en Qatar, que transmitía imágenes de soldados estadounidenses capturados. El sitio web fue en gran parte inaccesible durante dos días, tras lo cual alguien secuestro su nombre DNS, re direccionando las peticiones a otro sitio web que promovía la causa americana.

En mayo del 2003, el sitio web de SCO experimento ataques de DDoS dejándolo fuera de línea durante períodos prolongados de tiempo. Declaraciones por parte de gestión de la SCO indico que los ataques quizá fueron en respuesta a la batalla legal de SCO sobre el código fuente para Linux y las declaraciones criticando el papel de la comunidad de código abierto en estos juicios[167].

A mediados del año 2003, Clickbank (un servicio de banca electrónica) y Spamcop (una empresa que filtra los correos electrónicos para eliminar el spam) fueron objeto de un gran ataque DDoS[168]. Los ataques aparentemente involucraron a miles de máquinas de ataque. Después de algunos días, las empresas fueron capaces de reducir el tráfico de ataque evitando llegar a un punto de cuello de botella.

e) 2004, ataques motivados financieramente continuaron, junto con la especulación de que los ataques de gusanos se utilizaron para instalar software troyano en cientos de miles de hosts, creando redes bot enormes. Dos programas populares-Agobot, y su sucesor Phatbot[169], han sido implicados en la prestación

---

[167] R. Lemos, Attack on SCO Sites at an End, CNET News.com, 12 de Diciembre del 2003, http://news.com.com/2100-7355_3-5121828.html?tag=nefd_top.

[168] M. Zorz, Logerror, Massive Distributed Denial of Service Attack Hits ClickBank and SpamCop.net, http://www.ds-osac.org/view.cfm?KEY=7E4452434452&type=2B170C1E0A3A0F162820.

[169] LURHQ Threat Intelligence Group, Phatbot Trojan Analysis, 15 de Marzo del 2004, http://www.lurhq.com/phatbot.html.

de spam distribuido y DDoS, en algunos casos estas redes de bots son incluso vendidas en el mercado negro[170].

Dado que Phatbot se aprovecha de los hosts infectados, es una de las formas más avanzadas de la automatización visto hasta la fecha en la categoría de herramientas DDoS o amenaza combinada.

f) El 26 de enero del 2005, UNAM-CERT envió un comunicado en el que se han descubierto varias vulnerabilidades de negación de servicio en el IOS (Internet Operating System) de Cisco. Un intruso remoto podría provocar que un dispositivo afectado recargue el sistema operativo[171].

g) A principios de marzo del 2006, Los portales de Telefónica.net y Terra.es sufrieron un ataque DDoS, recibiendo millones de peticiones en un lapso de tiempo de 2 horas. Los dos portales estuvieron caídos por algún tiempo a horas de la tarde. Fuentes de Telefónica aseguraron que el ataque afecto solo a la velocidad de navegación y a ningún otro servicio. Sin embargo, los usuarios manifestaron su descontento al no poder utilizar el correo electrónico.

h) En Noviembre del 2007, el blog Genbeta, perteneciente al grupo weblogssl.com, recibió una amenaza consistente en la realización de un ataque DDoS, debido a un artículo publicado, acerca del fraude que suponen ciertos programas y páginas webs que ofrecen el servicio de mostrar quien te tiene como no admitido o te ha eliminado del Messenger[172].

i) En febrero del 2008 la amenaza se cumplió.[43] Genbeta sufrió continuos ataques DDos por varios días, ocasionando que sus servicios sean inaccesibles y no se encuentren disponibles a los usuarios, 7 días después el servicio en Genbeta fue

---

[170] J. Leyden, Phatbot Arrest Throws Open Trade in Zombie PCS, The Register, 12 de Mayo del 2004, http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/

[171] Multiples vulnerabilidades de Denegacion de Servicio en Cisco IOS , 26 de Enero del 2005, www.shellsec.net/articulo/2005/01/

[172] Julio Alonso, Ataque de DDOS a Genbeta, 07 febrero 2008, http://www.weblogssl.com/2008/02/07-ataque-de-ddos-a-genbeta , http://bitacora66.com/845

restablecido, sin embargo siguieron sufriendo ataques en menor medida, pero esta vez no fueron suficientes para dejar inoperativos a sus servidores.

j) El 6 de Agosto del 2009, el popular servicio Twitter sufrió un ataque de denegación de servicio produciendo que el servicio se viera interrumpido por un espacio de 2 a 3 horas. El servicio se fue normalizando tras algunas horas desde la caída. El servicio es uno de los más usados, junto a Facebook para compartir contenidos sociales.

k) 2010, Wikileaks siendo en un comienzo victima de éste tipo de ataques llegando incluso a estar fuera de servicio. Desato guerras de ataques DDoS, en los que grupos anónimos salieron a defenderla lanzando ataques contra sitios como el Banco Suizo quien le cerró la cuenta a Julian Assange, PayPal y otros.

ANEXO 4

COMPARACIÓN DE ATAQUES DOS

COMPARACIÓN DE ATAQUES DOS y DDOS

Tipo de Ataque	Causa			Efecto		
				Consumo de Recursos		
	Tipo de Paquetes	Envío masivo de paquetes y/o mensajes	Alteración del equipo o Información de Configuración	Por Explotación de Vulnerabilidades (Fallo del Sistema Operativo o reacción de el)	Por Saturación/ Degradación	
					Sistema	Red
Mail Bombing	SMTP	SI	NO	NO	SI	SI
Overdrop	Mal formado	SI	NO	SI	SI	SI
Smurf	ICMP	SI	NO	NO	SI	SI
Fraggle	UDP	SI	NO	NO	SI	SI
UDP Bomb, Echo Chargen	UDP	NO	NO	NO	SI	NO
Snork	UDP	NO	NO	NO	SI	NO
TCP SYN Flooding	TCP	SI	NO	NO	SI	SI
Land	TCP	SI	NO	NO	SI	SI
WinNuke OOB Nuke	TCP	NO	NO	SI	NO	NO
TCP FIN Flooding	TCP	SI	NO	NO	SI	SI
SYN ACK Flooding	TCP	SI	NO	NO	SI	SI
Banderas SYN y FIN activadas	TCP	SI	NO	NO	SI	SI

Tipo de Ataque	Causa			Efecto		
	Tipo de Paquetes	Envío masivo de paquetes y/o mensajes	Alteración del equipo o Información de Configuración	Consumo de Recursos		
				Por Explotación de Vulnerabilidades (Fallo del Sistema Operativo o reacción de el)	Por Saturación/ Degradación	
					Sistema	Red
Banderas SYN y FIN activadas	TCP	SI	NO	NO	SI	SI
Bandera FIN y sin bandera ACK Flooding	TCP	SI	NO	NO	SI	SI
Conecction Flood	TCP	SI	NO	NO	SI	SI
UDP Flood o Inundación UDP	UDP	SI	NO	NO	SI	SI
ICMP Flood o Inundación ICMP	ICMP	SI	NO	NO	SI	SI
MAC Flooding	TRAMAS MAC	SI	NO	NO	SI	SI
ARP Flooding	ARP	SI	NO	NO	SI	SI
WormHole	-	SI	SI	NO	NO	NO
Blackholing u hoyo negro	-	SI	SI	NO	NO	NO
Envenenamiento ARP o ARP Poisoning	ARP SNMP	SI	SI	NO	NO	NO
Packet forwarding o Reenvio de paquetes	-	NO	SI	NO	NO	NO

Tipo de Ataque	Causa			Efecto		
				Consumo de Recursos		
	Tipo de Paquetes	Envío masivo de paquetes y/o mensajes	Alteración del equipo y/o Información de Configuración	Por Explotación de Vulnerabilidades (Fallo del Sistema Operativo o reacción de el)	Por Saturación/ Degradación	
					Sistema	Red
Ping of Death	ICMP	SI	NO	SI	SI	SI
Teardrop	IP	SI	NO	SI	SI	SI
NewTear	UDP	SI	NO	SI	SI	SI
Bonk	UDP	SI	NO	SI	SI	SI
Boink	UDP	SI	NO	SI	SI	SI
SynDrop	IP TCP	SI	NO	SI	SI	SI
Nestea	IP	SI	NO	SI	SI	SI
Jolt y Jolt2	ICMP UDP	SI	NO	SI	SI	SI
Targa3	TCP	SI	NO	SI	SI	SI
Ssping	ICMP	SI	NO	SI	SI	SI
Igmpsyn	IGMP	SI	NO	SI	SI	SI
Fragmentación de mensajes IGMP	IGMP	SI	NO	SI	SI	SI
FAWX	IGMP	SI	NO	SI	SI	SI
KOD	IGMP	SI	NO	SI	SI	SI

Tipo de Ataque	Causa			Efecto		
				Consumo de Recursos		
	Tipo de Paquetes	Envío masivo de paquetes y/o mensajes	Alteración del equipo y/o Información de Configuración	Por Explotación de Vulnerabilidades (Fallo del Sistema Operativo o reacción de el)	Por Saturación/ Degradación	
					Sistema	Red
TRINOO	UDP TCP ICMP	SI	NO	SI	SI	SI
TRIBE FLOOD NETWORK	UDP TCP ICMP	SI	NO	SI	SI	SI
TRIBE FLOOD NETWORK 2000	UDP TCP ICMP	SI	NO	SI	SI	SI
Stacheldrat	UDP TCP ICMP	SI	NO	SI	SI	SI
Shaft	UDP TCP ICMP	SI	NO	SI	SI	SI
Mstream	TCP ICMP	SI	NO	SI	SI	SI
RTP Flood	RTP	SI	NO	SI	SI	SI
Invite Flood	INVITE	SI	NO	SI	SI	SI

ANEXO 5

CONFIGURACIÓN MRTG Y ESTADOS INICIALES

```
##################################################################################
# Multi Router Traffic Grapher -- Sample Configuration File
##################################################################################

# This file is for use with mrtg-2.5.4c

# Global configuration

LoadMIBs: /usr/share/mibs/netsnmp/UCD-SNMP-MIB.txt,/usr/share/mibs/netsnmp/TCP-
MIB.txt,/usr/share/mibs/netsnmp/HOST-RESOURCES-MIB.txt
workdir: /var/www/mrtg/

# Monitoreo de CPU en el Servidor de Asterisk

Target[server.cpu]:.1.3.6.1.4.1.2021.11.50.0&.1.3.6.1.4.1.2021.11.50.0:public@192.168.0.
253 + .1.3.6.1.4.1.2021.11.52.0&.1.3.6.1.4.1.2021.11.52.0:public@192.168.0.253 +
.1.3.6.1.4.1.2021.11.51.0&.1.3.6.1.4.1.2021.11.51.0:public@192.168.0.253
Title[server.cpu]: Carga del CPU en el Servidor Asterisk
PageTop[server.cpu]: <h1>Carga del CPU en el Servidor Asterisk</h1>
MaxBytes[server.cpu]: 100
ShortLegend[server.cpu]: %
YLegend[server.cpu]: UtilizaciÃ³n de CPU
Legend1[server.cpu]: Porcentaje actual de la carga del CPU
LegendI[server.cpu]: Usado
LegendO[server.cpu]:
XSize[server.cpu]: 500
YSize[server.cpu]: 175
Options[server.cpu]: growright,nopercent
Unscaled[server.cpu]: ymwd

# Monitoreo de CPU en el Servidor de Correo

Target[server.cpu1]: (
.1.3.6.1.2.1.25.3.3.1.2.2&.1.3.6.1.2.1.25.3.3.1.2.2:public@192.168.0.254 +
.1.3.6.1.2.1.25.3.3.1.2.3&.1.3.6.1.2.1.25.3.3.1.2.3:public@192.168.0.254) / 2
Title[server.cpu1]: Carga del CPU en el servidor de Correo
PageTop[server.cpu1]: <h1>Carga del CPU en el servidor de Correo</h1>
MaxBytes[server.cpu1]: 100
ShortLegend[server.cpu1]: %
YLegend[server.cpu1]: UtilizaciÃ³n de CPU
Legend1[server.cpu1]: Porcentaje actual de la carga del CPU
LegendI[server.cpu1]: Usado
LegendO[server.cpu1]:
XSize[server.cpu1]: 500
YSize[server.cpu1]: 175
Options[server.cpu1]: growright,nopercent,gauge
Unscaled[server.cpu1]: ymwd

# Monitoreo de Memoria en el Servidor de Asterisk (Total Vs Memoria Disponible)

Target[server.memory]:
.1.3.6.1.4.1.2021.4.6.0&.1.3.6.1.4.1.2021.4.5.0:public@192.168.0.253
Title[server.memory]: Memoria Libre
PageTop[server.memory]: <h1>Memoria Libre en el Servidor de Asterisk</h1>
```

```
MaxBytes[server.memory]: 100000000
ShortLegend[server.memory]: B
YLegend[server.memory]: Bytes
LegendI[server.memory]: Libre
LegendO[server.memory]: Total
Legend1[server.memory]: Memoria Libre, no incluye swap, en bytes
Legend2[server.memory]: Memoria Total
XSize[server.memory]: 500
YSize[server.memory]: 175
Options[server.memory]: gauge,growright,nopercent
kMG[server.memory]: k,M,G,T,P,X

# Monitoreo de Memoria en el Servidor de Correo (Total Vs Memoria Usada)

Target[server.memory1]:
.1.3.6.1.2.1.25.2.3.1.6.5&.1.3.6.1.2.1.25.2.3.1.5.5:public@192.168.0.254*65536/1000
Title[server.memory1]: Memoria Libre
PageTop[server.memory1]: <h1>Memoria Libre en el Servidor de Correo</h1>
MaxBytes[server.memory1]: 400000000
ShortLegend[server.memory1]: B
YLegend[server.memory1]: Bytes
LegendI[server.memory1]: Usada
LegendO[server.memory1]: Total
Legend1[server.memory1]: Memoria Usada,en bytes
Legend2[server.memory1]: Memoria Total
XSize[server.memory1]: 500
YSize[server.memory1]: 175
Options[server.memory1]: gauge,growright,nopercent
kMG[server.memory1]: k,M,G,T,P,X

# Monitoreo de Uso de Disco Duro en el Servidor de Asterisk

Target[server.disk]:
.1.3.6.1.4.1.2021.9.1.9.1&.1.3.6.1.4.1.2021.9.1.9.1:public@192.168.0.253
Title[server.disk]: Uso de Disco
PageTop[server.disk]: <h1>Uso de Disco en el Servidor de Asterisk</h1>
MaxBytes[server.disk]: 100
ShortLegend[server.disk]: %
YLegend[server.disk]: Utilizado
LegendI[server.disk]: /
XSize[server.disk]: 500
YSize[server.disk]: 175
Options[server.disk]: gauge,growright,nopercent
Unscaled[server.disk]: ymwd

# Monitoreo de Uso de Disco Duro en el Servidor de Correo

Target[server.disk1]: (
.1.3.6.1.2.1.25.2.3.1.6.1&.1.3.6.1.2.1.25.2.3.1.6.1:public@192.168.0.254 ) *100 / (
1.3.6.1.2.1.25.2.3.1.5.1&1.3.6.1.2.1.25.2.3.1.5.1:public@192.168.0.254 )
Title[server.disk1]: Uso de Disco
PageTop[server.disk1]: <h1>Uso de Disco en el Servidor de Correo</h1>
MaxBytes[server.disk1]: 100
ShortLegend[server.disk1]: %
```

YLegend[server.disk1]: Utilizado
LegendI[server.disk1]: C:/
XSize[server.disk1]: 500
YSize[server.disk1]: 175
Options[server.disk1]: gauge,growright,nopercent
Unscaled[server.disk1]: ymwd

Monitoreo de la interfaz de red en el Servidor de Asterisk ifInOctets.10&ifOutOctets.10

Target[192.168.0.253_eth0]:
.1.3.6.1.2.1.2.2.1.10.10&.1.3.6.1.2.1.2.2.1.16.10:public@192.168.0.254
SetEnv[192.168.0.253_eth0]: MRTG_INT_IP="192.168.0.253"
MRTG_INT_DESCR="eth0"
MaxBytes[192.168.0.253_eth0]: 100000
LegendI[192.168.0.253_eth0]: Entrada
LegendO[192.168.0.253_eth0]: Salida
XSize[192.168.0.253_eth0]: 500
YSize[192.168.0.253_eth0]: 175
Options[192.168.0.253_eth0]:growright,nopercent,bits
Title[192.168.0.253_eth0]: AnÃ¡lisis de TrÃ¡fico para la interfaz del Servidor de Asterisk
PageTop[192.168.0.253_eth0]: <h1>Analisis de Trafico para la interfaz del Servidor de Asterisk</h1>

Monitoreo de la interfaz de red en el Servidor de Correo ifInOctets.11&ifOutOctets.11

Target[192.168.0.254_eth0]:
.1.3.6.1.2.1.2.2.1.10.11&.1.3.6.1.2.1.2.2.1.16.11:public@192.168.0.254
SetEnv[192.168.0.254_eth0]: MRTG_INT_IP="192.168.0.254"
MRTG_INT_DESCR="eth1"
MaxBytes[192.168.0.254_eth0]: 100000000
LegendI[192.168.0.254_eth0]: Entrada
LegendO[192.168.0.254_eth0]: Salida
XSize[192.168.0.254_eth0]: 500
YSize[192.168.0.254_eth0]: 175
Options[192.168.0.254_eth0]:growright,nopercent,bits
Title[192.168.0.254_eth0]: AnÃ¡lisis de TrÃ¡fico para la interfaz del Servidor de Correo
PageTop[192.168.0.254_eth0]: <h1>Analisis de Trafico para la interfaz del Servidor de Correo</h1>

Monitoreo de Nuevas Conexiones TCP en el Servidor de Asterisk por minuto

Target[server.newconns]: tcpPassiveOpens.0&tcpActiveOpens.0:public@192.168.0.253
Title[server.newconns]: CreaciÃ³n de Conexiones TCP nuevas
PageTop[server.newconns]: <h1>Nuevas Conexiones TCP en el Servidor de Asterisk</h1>
MaxBytes[server.newconns]: 65536
ShortLegend[server.newconns]: cs/min
YLegend[server.newconns]: Conexiones x Min
LegendI[server.newconns]: Conexiones Passive Open
LegendO[server.newconns]: Conexiones Active Open
Legend1[server.newconns]: Nuevas conexiones entrantes
Legend2[server.newconns]: Nuevas conexiones salientes
XSize[server.newconns]: 500
YSize[server.newconns]: 175

```
Options[server.newconns]: growright,nopercent,perminute

# Monitoreo de Nuevas Conexiones TCP en el Servidor de Correo por minuto

Target[server.newconns1]: tcpPassiveOpens.0&tcpActiveOpens.0:public@192.168.0.254
Title[server.newconns1]: CreaciÃ³n de Conexiones TCP nuevas
PageTop[server.newconns1]: <h1>Nuevas Conexiones TCP en el Servidor de
Correo</h1>
MaxBytes[server.newconns1]: 65536
ShortLegend[server.newconns1]: cs/min
YLegend[server.newconns1]: Conexiones x Min
LegendI[server.newconns1]: Conexiones Passive Open
LegendO[server.newconns1]: Conexiones Active Open
Legend1[server.newconns1]: Nuevas Conexiones entrantes
Legend2[server.newconns1]: Nuevas Conexiones salientes
XSize[server.newconns1]: 500
YSize[server.newconns1]: 175
Options[server.newconns1]: growright,nopercent,perminute

# Monitoreo de Conexiones TCP establecidas en el Servidor de Asterisk

Target[server.estabcons]: tcpCurrEstab.0&tcpCurrEstab.0:public@192.168.0.253
Title[server.estabcons]: Conexiones TCP EStablecidas
PageTop[server.estabcons]: <h1>Conexiones TCP establecidas en el Servidor
Asterik</h1>
MaxBytes[server.estabcons]: 65536
ShortLegend[server.estabcons]:cs
YLegend[server.estabcons]: Conexiones
LegendI[server.estabcons]: Entrantes
LegendO[server.estabcons]:
Legend1[server.estabcons]: Conexiones Establecidas
Legend2[server.estabcons]:
XSize[server.estabcons]: 500
YSize[server.estabcons]: 175
Options[server.estabcons]: growright,nopercent,gauge

# Monitoreo de Conexiones TCP establecidas en el Servidor de Correo

Target[server.estabcons1]: tcpCurrEstab.0&tcpCurrEstab.0:public@192.168.0.254
Title[server.estabcons1]: Conexiones TCP establecidas
PageTop[server.estabcons1]: <h1>Conexiones TCP establecidas en el Servidor de
Correo</h1>
MaxBytes[server.estabcons1]: 65536
ShortLegend[server.estabcons1]: cs
YLegend[server.estabcons1]: Conexiones
LegendI[server.estabcons1]: Entrantes
LegendO[server.estabcons1]:
Legend1[server.estabcons1]: Conexiones Establecidas
Legend2[server.estabcons1]:
XSize[server.estabcons1]: 500
YSize[server.estabcons1]: 175
Options[server.estabcons1]: growright,nopercent,gauge

# Monitoreo de Segmentos TCP en el Servidor de Asterisk
```

```
Target[server.tcp]: tcpOutSegs.0&tcpInSegs.0:public@192.168.0.253
Title[server.tcp]: Segmentos TCP
PageTop[server.tcp]: <h1>Segmentos TCP en el Servidor de Asterisk</h1>
MaxBytes[server.tcp]: 10000000000
ShortLegend[server.tcp]: segs/min
YLegend[server.tcp]: Segmentos TCP x Min
LegendI[server.tcp]: Enviados
LegendO[server.tcp]: Recibidos
Legend1[server.tcp]: NÃºmero de Segmentos TCP
Legend2[server.tcp]:
XSize[server.tcp]: 500
YSize[server.tcp]: 175
Options[server.tcp]: growright,nopercent,perminute

# Monitoreo de Segmentos TCP en el Servidor de Correo

Target[server.tcp1]: tcpOutSegs.0&tcpInSegs.0:public@192.168.0.254
Title[server.tcp1]: Segmentos TCP
PageTop[server.tcp1]: <h1>Segmentos TCP en el Servidor de Correo</h1>
MaxBytes[server.tcp1]: 10000000000
ShortLegend[server.tcp1]: segs/min
YLegend[server.tcp1]: Segmentos TCP x Min
LegendI[server.tcp1]: Enviados
LegendO[server.tcp1]: Recibidos
Legend1[server.tcp1]: NÃºmero de Segmentos TCP
Legend2[server.tcp1]:
XSize[server.tcp1]: 500
YSize[server.tcp1]: 175
Options[server.tcp1]: growright,nopercent,perminute

# Monitoreo de Datagramas UDP en el Servidor de Asterisk

Target[server.udp]: udpOutDatagrams.0&udpInDatagrams.0:public@192.168.0.253
Title[server.udp]: Datagramas UDP
PageTop[server.udp]: <h1>Datagramas UDP en el Servidor de Asterisk</h1>
MaxBytes[server.udp]: 10000000000
ShortLegend[server.udp]: dts/min
YLegend[server.udp]: Datagramas UDP x Min
LegendI[server.udp]: Enviados
LegendO[server.udp]: Recibidos
Legend1[server.udp]: NÃºmero de Datagramas UDP
Legend2[server.udp]:
XSize[server.udp]: 500
YSize[server.udp]: 175
Options[server.udp]: growright,nopercent,perminute

# Monitoreo de Datagramas UDP en el Servidor de Correo

Target[server.udp1]: udpOutDatagrams.0&udpInDatagrams.0:public@192.168.0.254
Title[server.udp1]: Datagramas UDP
PageTop[server.udp1]: <h1>Datagramas UDP en el Servidor de Correo</h1>
MaxBytes[server.udp1]: 10000000000
ShortLegend[server.udp1]: dts/min
```

```
YLegend[server.udp1]: Datagramas UDP x Min
LegendI[server.udp1]: Enviados
LegendO[server.udp1]: Recibidos
Legend1[server.udp1]: NÃºmero de Datagramas UDP
Legend2[server.udp1]:
XSize[server.udp1]: 500
YSize[server.udp1]: 175
Options[server.udp1]: growright,nopercent,perminute

# Monitoreo de Paquetes IP en el Servidor de Asterisk

Target[server.ip]: ipOutRequests.0&ipInReceives.0:public@192.168.0.253
Title[server.ip]: Paquetes IP
PageTop[server.ip]: <h1>Paquetes IP en el Servidor de Asterisk</h1>
MaxBytes[server.ip]: 10000000000
ShortLegend[server.ip]: pts/min
YLegend[server.ip]: Paquetes IP x Min
LegendI[server.ip]: Paquetes IP Solicitados
LegendO[server.ip]: Paquetes IP Recibidos
Legend1[server.ip]: NÃºmero de Paquetes IP
Legend2[server.ip]:
XSize[server.ip]: 500
YSize[server.ip]: 175
Options[server.ip]: growright,nopercent,perminute

# Monitoreo de Paquetes IP en el Servidor de Correo

Target[server.ip1]: ipOutRequests.0&ipInReceives.0:public@192.168.0.254
Title[server.ip1]: Paquetes IP
PageTop[server.ip1]: <h1>Paquetes IP en el Servidor de Correo</h1>
MaxBytes[server.ip1]: 10000000000
ShortLegend[server.ip1]: pts/min
YLegend[server.ip1]: Paquetes IP x Min
LegendI[server.ip1]: Paquetes IP Solicitados
LegendO[server.ip1]: Paquetes IP Recibidos
Legend1[server.ip1]: NÃºmero de Paquetes IP
Legend2[server.ip1]:
XSize[server.ip1]: 500
YSize[server.ip1]: 175
Options[server.ip1]: growright,nopercent,perminute

# Monitoreo de Mensajes ICMP en el Servidor de Asterisk

Target[server.icmp]: icmpOutMsgs.0&icmpInMsgs.0:public@192.168.0.253
Title[server.icmp]: Mensajes ICMP
PageTop[server.icmp]: <h1>Mensajes ICMP en el Servidor de Asterisk</h1>
MaxBytes[server.icmp]: 10000000000
ShortLegend[server.icmp]: msgs/min
YLegend[server.icmp]: Mensajes ICMP x Min
LegendI[server.icmp]: Enviados
LegendO[server.icmp]: Recibidos
Legend1[server.icmp]: NÃºmero de Mensajes ICMP
Legend2[server.icmp]:
XSize[server.icmp]: 500
```

YSize[server.icmp]: 175
Options[server.icmp]: growright,nopercent,perminute

Monitoreo de Mensajes ICMP en el Servidor de Correo

Target[server.icmp1]: icmpOutMsgs.0&icmpInMsgs.0:public@192.168.0.254
Title[server.icmp1]: Mensajes ICMP
PageTop[server.icmp1]: <h1>Mensajes ICMP en el Servidor de Correo</h1>
MaxBytes[server.icmp1]: 10000000000
ShortLegend[server.icmp1]: msgs/min
YLegend[server.icmp1]: Mensajes ICMP x Min
LegendI[server.icmp1]: Enviados
LegendO[server.icmp1]: Recibidos
Legend1[server.icmp1]: NÃºmero de Mensajes ICMP
Legend2[server.icmp1]:
XSize[server.icmp1]: 500
YSize[server.icmp1]: 175
Options[server.icmp1]: growright,nopercent,perminute

Monitoreo de Conexiones HTTP en el Servidor de Correo
httpcurrentconnections&httpconnectionsAttempts

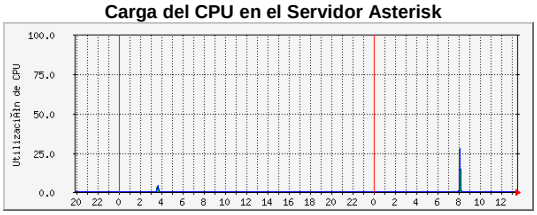
Target[server.http]:
.1.3.6.1.4.1.311.1.7.3.1.12.0&.1.3.6.1.4.1.311.1.7.3.1.14.0:public@192.168.0.254
Title[server.http]: Conexiones HTTP en el Servidor de Correo
PageTop[server.http]: <h1>Conexiones HTTP en el Servidor de Correo</h1>
MaxBytes[server.http]: 10000
ShortLegend[server.http]: cs/min
YLegend[server.http]: Conexiones HTTP x Min
LegendI[server.http]: Numero de Conexiones Actuales
LegendO[server.http]: Numero de intentos de Coneccion
Legend1[server.http]: NÃºmero de Conexiones HTTP
Legend2[server.http]:
XSize[server.http]: 500
YSize[server.http]: 175
Options[server.http]: growright,nopercent,perminute

Monitoreo de Canales SIP en Uso en el Servidor de Asterisk
astChanTypeChannels.4&astNumChannels.0

Target[server.cha]:
.1.3.6.1.4.1.22736.1.5.4.1.7.4&.1.3.6.1.4.1.22736.1.5.1.0:public@192.168.0.253
Title[server.cha]: Canales en Uso en el Servidor de ASterisk
PageTop[server.cha]: <h1>Canales en Uso en el Servidor de ASterisk</h1>
MaxBytes[server.cha]: 10000
ShortLegend[server.cha]: cs
YLegend[server.cha]: Canales en Uso
LegendI[server.cha]: Numero de Canales SIP
LegendO[server.cha]: Total de Canales
XSize[server.cha]: 500
YSize[server.cha]: 175
Options[server.cha]: growright,nopercent,gauge

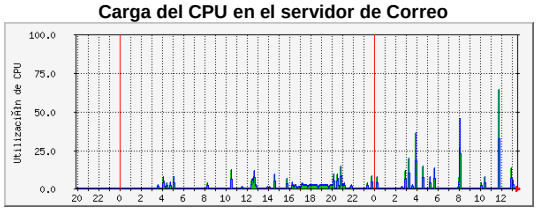
MRTG (Promedio 5 Min) - Tiempo de Monitoreo: 32 horas

Carga del CPU en el Servidor Asterisk



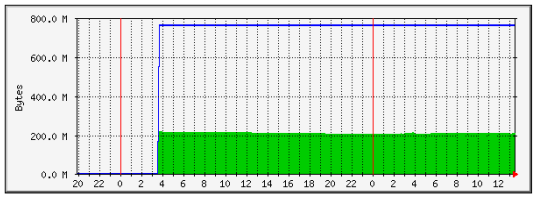
	Max	Average	Current
Usado	27.0 %	1.0 %	0.0 %

Carga del CPU en el servidor de Correo



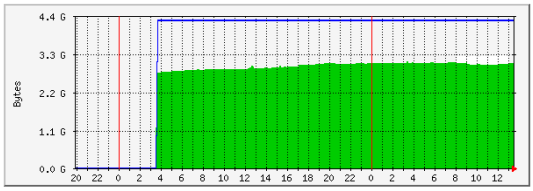
	Max	Average	Current
Usado	64.0 %	4.0 %	0.0 %

Memoria Libre en el Servidor de Asterisk



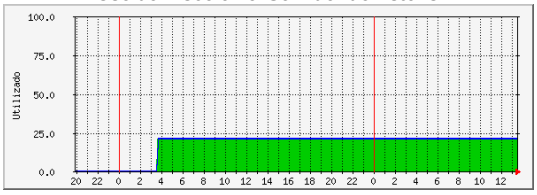
	Max	Average	Current
Libre	215.1 MB	201.0 MB	212.1 MB
Total	762.6 MB	761.6 MB	762.6 MB

Memoria Libre en el Servidor de Correo



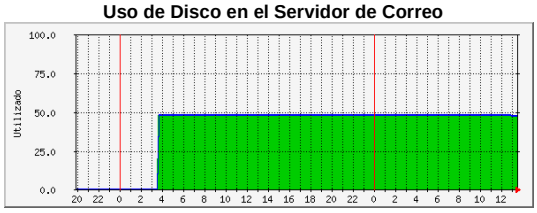
	Max	Average	Current
Usada	3235.6 MB	2974.1 MB	2848.7 MB
Total	4253.9 MB	4248.1 MB	4253.9 MB

Uso de Disco en el Servidor de Asterisk



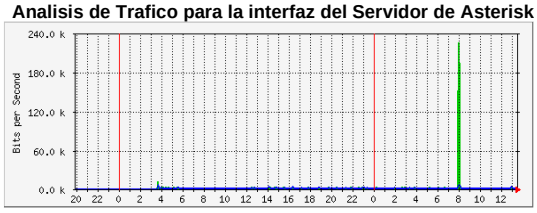
	Max	Average	Current
/	21.0 %	21.0 %	21.0 %
Out	21.0 %	21.0 %	21.0 %

Uso de Disco en el Servidor de Correo



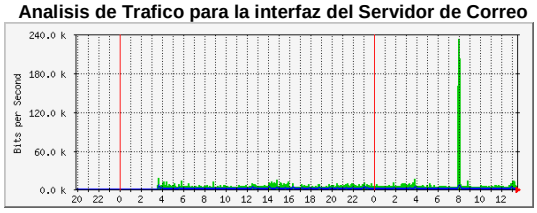
	Max	Average	Current
C:/	48.0 %	48.0 %	47.0 %
Out	48.0 %	48.0 %	47.0 %

Analisis de Trafico para la interfaz del Servidor de Asterisk



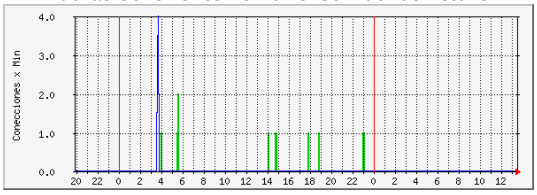
	Max	Average	Current
Entrada	225.8 kb/s	3576.0 b/s	2472.0 b/s
Salida	6040.0 b/s	360.0 b/s	56.0 b/s

Analisis de Trafico para la interfaz del Servidor de Correo



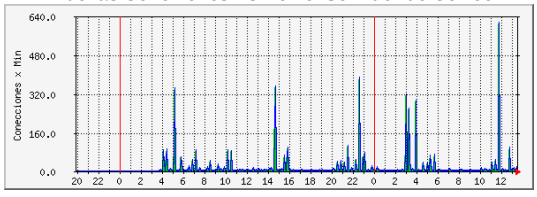
	Max	Average	Current
Entrada	232.5 kb/s	6704.0 b/s	5408.0 b/s
Salida	5904.0 b/s	480.0 b/s	144.0 b/s

Nuevas Conexiones TCP en el Servidor de Asterisk



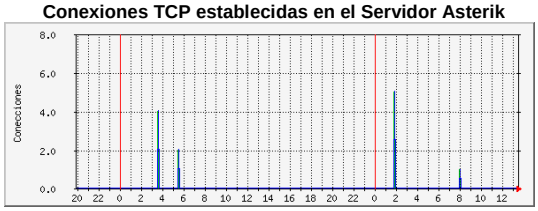
	Max	Average	Current
Conexiones Passive Open	2.0 cs/min	0.0 cs/min	0.0 cs/min
Conexiones Active Open	4.0 cs/min	0.0 cs/min	0.0 cs/min

Nuevas Conexiones TCP en el Servidor de Correo



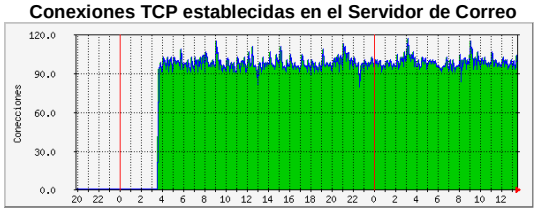
	Max	Average	Current
Conexiones Passive Open	610.0 cs/min	14.0 cs/min	5.0 cs/min
Conexiones Active Open	612.0 cs/min	15.0 cs/min	5.0 cs/min

Conexiones TCP establecidas en el Servidor Asterik



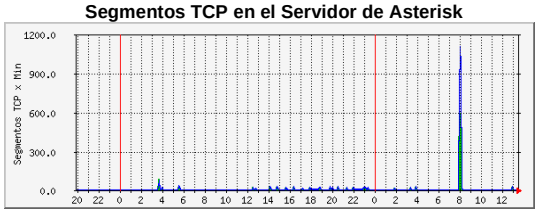
	Max	Average	Current
Conexiones Establecidas	5.0 cs	1.0 cs	0.0 cs

Conexiones TCP establecidas en el Servidor de Correo



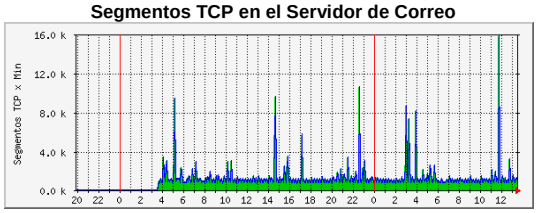
	Max	Average	Current
Conexiones Establecidas	116.0 cs	97.0 cs	99.0 cs

Segmentos TCP en el Servidor de Asterisk



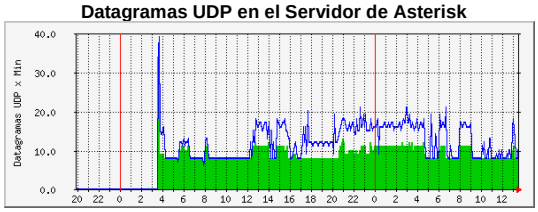
	Max	Average	Current
Enviados	591.0 segs/min	26.0 segs/min	0.0 segs/min
Recibidos	1099.0 segs/min	41.0 segs/min	0.0 segs/min

Segmentos TCP en el Servidor de Correo



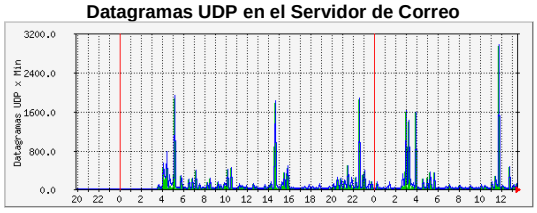
	Max	Average	Current
Enviados	15.8 ksegs/min	1235.0 segs/min	879.0 segs/min
Recibidos	15.8 ksegs/min	1236.0 segs/min	881.0 segs/min

Datagramas UDP en el Servidor de Asterisk



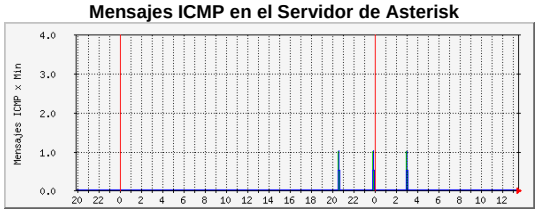
	Max	Average	Current
Enviados	34.0 dts/min	9.0 dts/min	8.0 dts/min
Recibidos	39.0 dts/min	12.0 dts/min	12.0 dts/min

Datagramas UDP en el Servidor de Correo



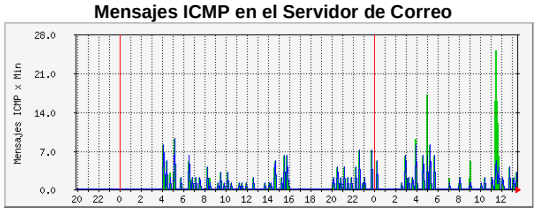
	Max	Average	Current
Enviados	2938.0 dts/min	74.0 dts/min	27.0 dts/min
Recibidos	2952.0 dts/min	88.0 dts/min	48.0 dts/min

Mensajes ICMP en el Servidor de Asterisk



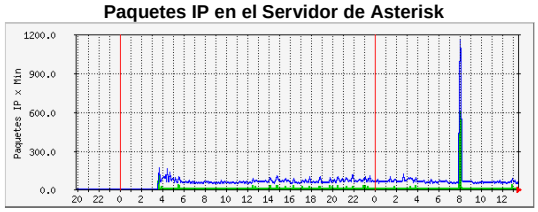
	Max	Average	Current
Enviados	1.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	1.0 msgs/min	0.0 msgs/min	0.0 msgs/min

Mensajes ICMP en el Servidor de Correo



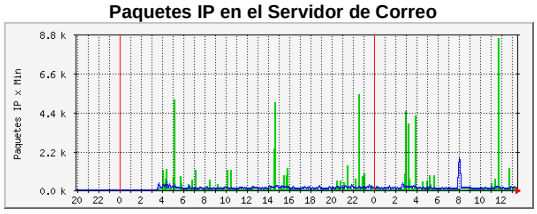
	Max	Average	Current
Enviados	25.0 msgs/min	2.0 msgs/min	0.0 msgs/min
Recibidos	9.0 msgs/min	2.0 msgs/min	0.0 msgs/min

Paquetes IP en el Servidor de Asterisk



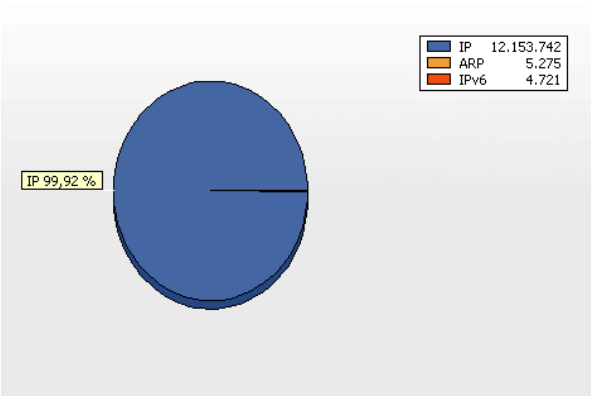
	Max	Average	Current
Paquetes IP Solicitados	603.0 pts/min	15.0 pts/min	8.0 pts/min
Paquetes IP Recibidos	1155.0 pts/min	66.0 pts/min	59.0 pts/min

Paquetes IP en el Servidor de Correo

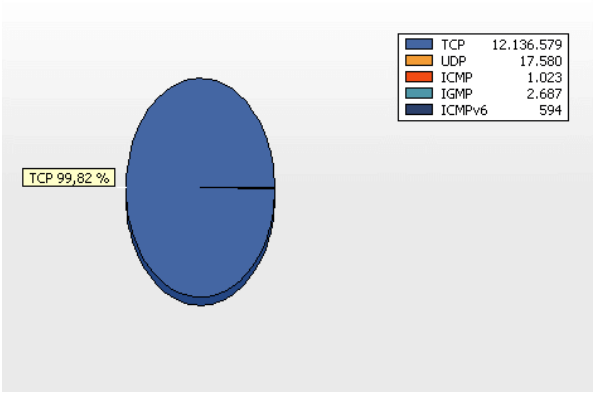


	Max	Average	Current
Paquetes IP Solicitados	8556.0 pts/min	183.0 pts/min	35.0 pts/min
Paquetes IP Recibidos	1807.0 pts/min	132.0 pts/min	119.0 pts/min

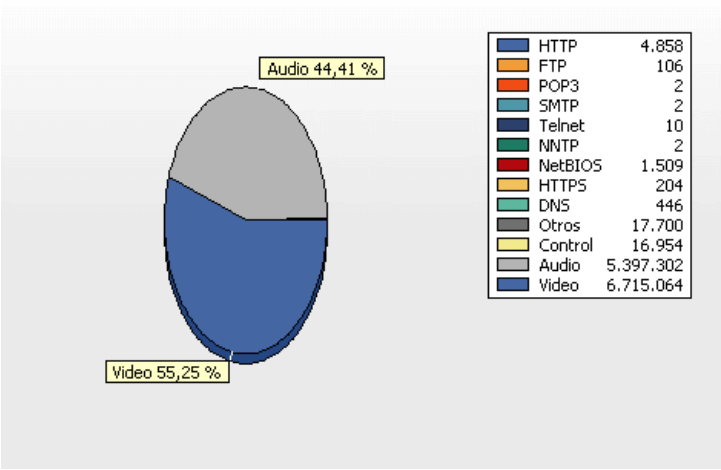
MONITOREO DE ESTADOS INICIALES DE LA CÁMARA IP
CommView - Tiempo de Monitoreo: 20 horas



Paquetes IP



Paquetes TCP, UDP e ICMP



Protocolos de capa aplicación en la Cámara IP

Resumen General de la Cámara IP

Promedio de paquetes por seg.			169
Promedio de bytes por seg.			88.208
Total de paquetes			12.163.864
Total bytes			6.350.936.244
Item \ Dirección	**Entrante**	**Saliente**	**Pasante**
Paquetes	8.081.162	4.064.812	17.764
Bytes	6.127.041.646	222.065.690	1.777.114
Bytes por seg.	85.099	40540	25

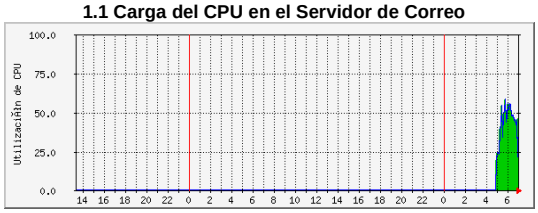
ANEXO 6

RESULTADOS OBTENIDOS Y CAPTURA DE PAQUETES, POR LA SIMULACIÓN DE ATAQUES DoS EN LA RED DE PRUEBAS IMPLEMENTADA

1. ATAQUE SYN FLOOD CONTRA EL SERVIDOR DE WEB/CORREO

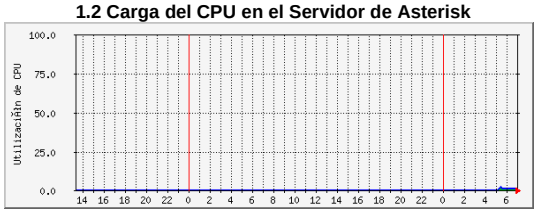
MRTG (Promedio 5 Min) - Tiempo de Monitoreo: 2 horas

1.1 Carga del CPU en el Servidor de Correo



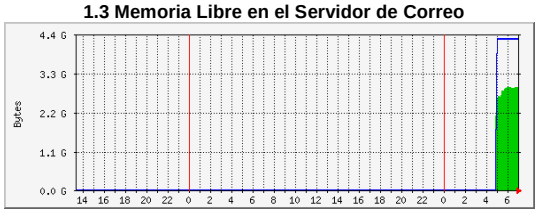
	Max	Average	Current
Usado	58.0 %	43.0 %	46.0 %

1.2 Carga del CPU en el Servidor de Asterisk



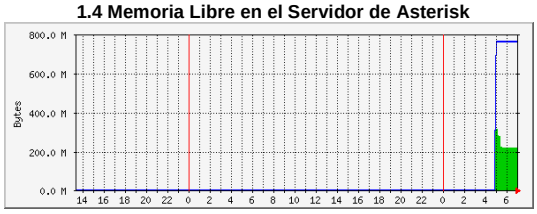
	Max	Average	Current
Usado	2.0 %	1.0 %	1.0 %

1.3 Memoria Libre en el Servidor de Correo



	Max	Average	Current
Usada	2908.8 MB	2753.9 MB	2908.1 MB
Total	4253.9 MB	4222.3 MB	4253.9 MB

1.4 Memoria Libre en el Servidor de Asterisk

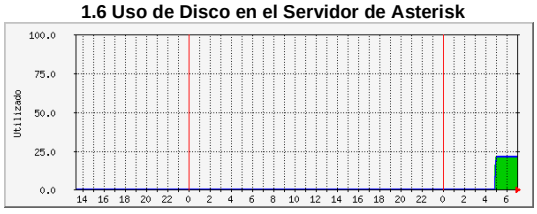


	Max	Average	Current
Libre	314.3 MB	233.2 MB	216.0 MB
Total	762.6 MB	756.9 MB	762.6 MB

1.5 Uso de Disco en el Servidor de Correo

	Max	Average	Current
C:/	48.0 %	48.0 %	48.0 %
Out	48.0 %	48.0 %	48.0 %

1.6 Uso de Disco en el Servidor de Asterisk

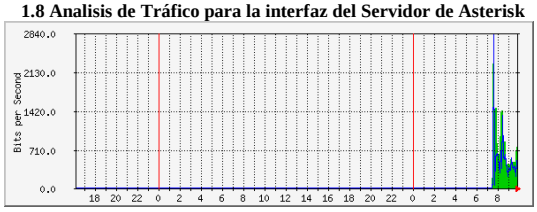


	Max	Average	Current
/	21.0 %	21.0 %	21.0 %
Out	21.0 %	21.0 %	21.0 %

1.7 Analisis de Tráfico para la interfaz del Servidor de Correo

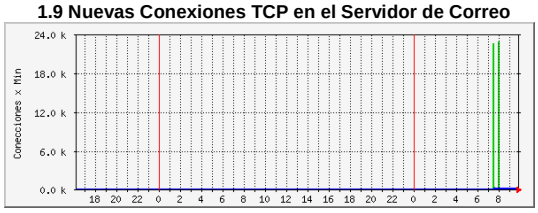
	Max	Average	Current
Entrada	5792.0 b/s	1792.0 b/s	1256.0 b/s
Salida	3056.0 b/s	624.0 b/s	432.0 b/s

1.8 Analisis de Tráfico para la interfaz del Servidor de Asterisk



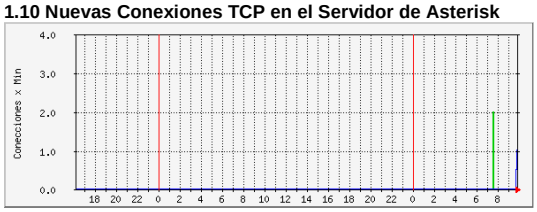
	Max	Average	Current
Entrada	2280.0 b/s	696.0 b/s	760.0 b/s
Salida	2808.0 b/s	528.0 b/s	432.0 b/s

1.9 Nuevas Conexiones TCP en el Servidor de Correo



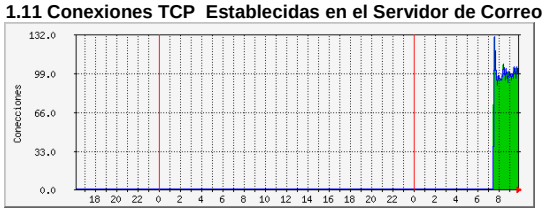
	Max	Average	Current
Conexiones Passive Open	22.8 kcs/min	1578.0 cs/min	1.0 cs/min
Conexiones Active Open	7.0 cs/min	3.0 cs/min	1.0 cs/min

1.10 Nuevas Conexiones TCP en el Servidor de Asterisk



	Max	Average	Current
Conexiones Passive Open	2.0 cs/min	0.0 cs/min	0.0 cs/min
Conexiones Active Open	0.0 cs/min	0.0 cs/min	0.0 cs/min

1.11 Conexiones TCP Establecidas en el Servidor de Correo

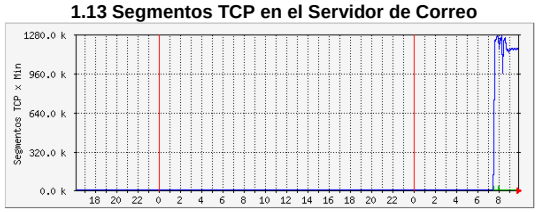


	Max	Average	Current
Entrantes	129.0 cs	98.0 cs	95.0 cs

1.12 Conexiones TCP Establecidas en el Servidor de Asteris

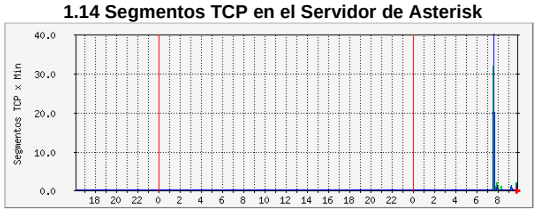
	Max	Average	Current
Entrantes	0.0 cs	0.0 cs	0.0 cs

1.13 Segmentos TCP en el Servidor de Correo



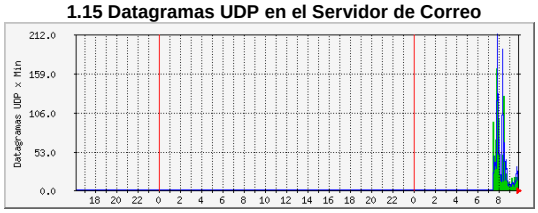
	Max	Average	Current
Enviados	33.5 ksegs/min	3146.0 segs/min	734.0 segs/min
Recibidos	1265.0 ksegs/min	1149.8 ksegs/min	1153.1 ksegs/min

1.14 Segmentos TCP en el Servidor de Asterisk



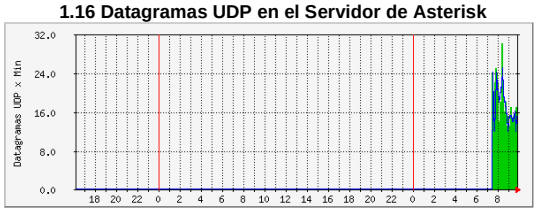
	Max	Average	Current
Enviados	32.0 segs/min	3.0 segs/min	2.0 segs/min
Recibidos	40.0 segs/min	4.0 segs/min	2.0 segs/min

1.15 Datagramas UDP en el Servidor de Correo



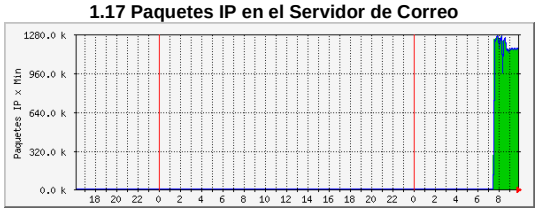
	Max	Average	Current
Enviados	165.0 dts/min	36.0 dts/min	8.0 dts/min
Recibidos	212.0 dts/min	34.0 dts/min	7.0 dts/min

1.16 Datagramas UDP en el Servidor de Asterisk



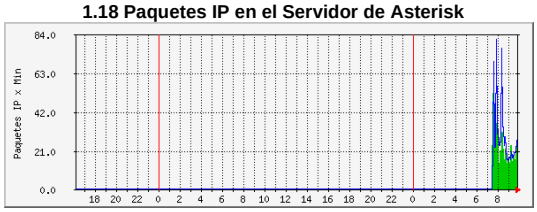
	Max	Average	Current
Enviados	30.0 dts/min	20.0 dts/min	14.0 dts/min
Recibidos	25.0 dts/min	28.0 dts/min	15.0 dts/min

1.17 Paquetes IP en el Servidor de Correo



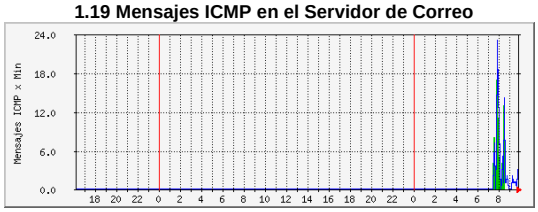
	Max	Average	Current
Paquetes IP Solicitados	1264.5 kpts/min	1152.7 kpts/min	1152.4 kpts/min
Paquetes IP Recibidos	1264.6 kpts/min	1148.9 kpts/min	1152.4 kpts/min

1.18 Paquetes IP en el Servidor de Asterisk



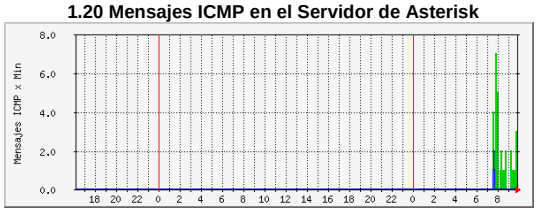
	Max	Average	Current
Paquetes IP Solicitados	52.0 pts/min	20.0 pts/min	19.0 pts/min
Paquetes IP Recibidos	81.0 pts/min	28.0 pts/min	20.0 pts/min

1.19 Mensajes ICMP en el Servidor de Correo



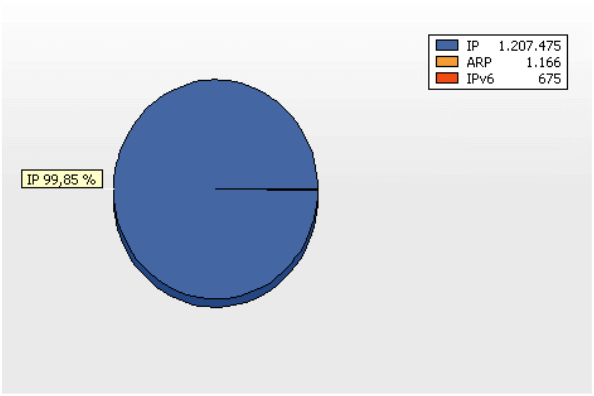
	Max	Average	Current
Enviados	17.0 msgs/min	2.0 msgs/min	0.0 msgs/min
Recibidos	23.0 msgs/min	4.0 msgs/min	1.0 msgs/min

1.20 Mensajes ICMP en el Servidor de Asterisk

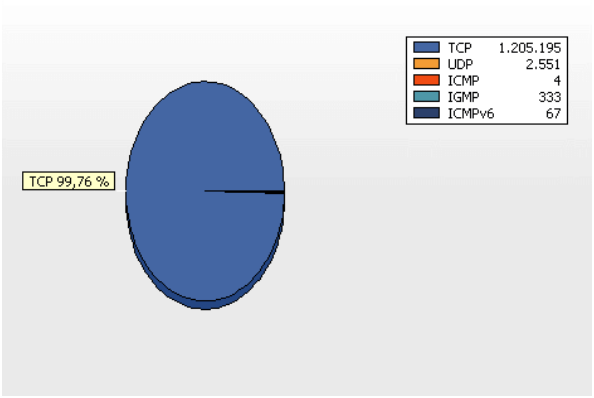


	Max	Average	Current
Enviados	7.0 msgs/min	2.0 msgs/min	1.0 msgs/min
Recibidos	2.0 msgs/min	0.0 msgs/min	0.0 msgs/min

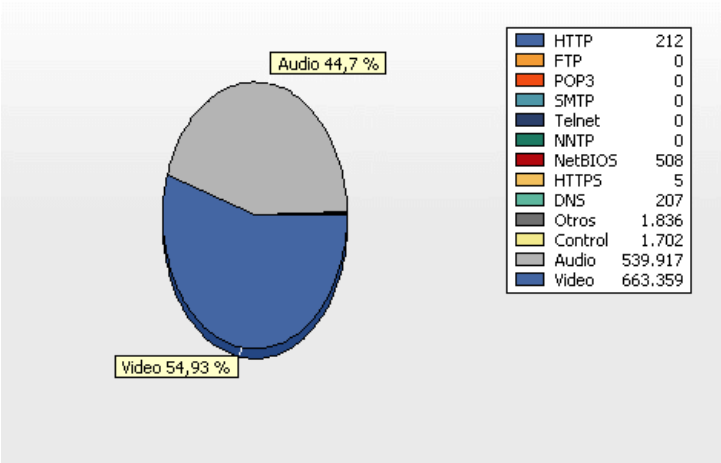
MONITOREO DE LA CÁMARA IP
CommView - Tiempo de Monitoreo: 20 horas



1.21 Paquetes IP



1.22 Paquetes TCP, UDP e ICMP



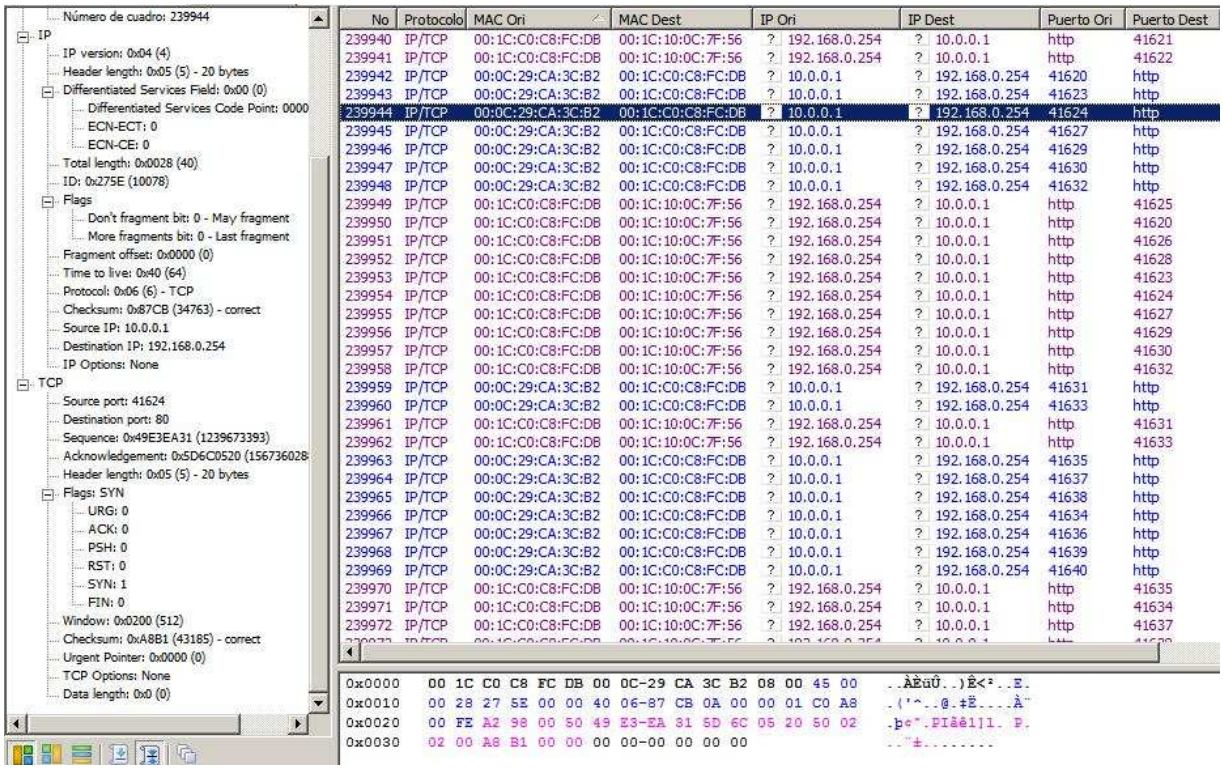
1.23 Protocolos de capa aplicación en la Cámara IP

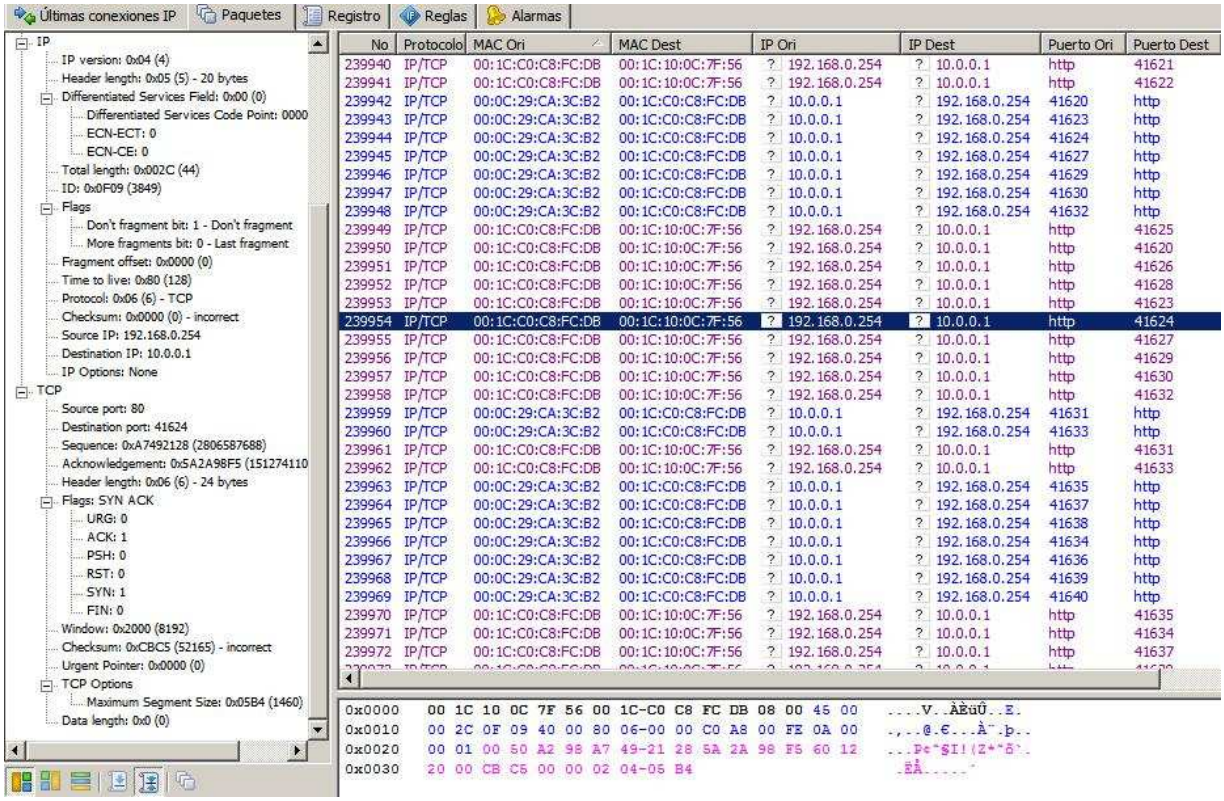
1.24 Resumen General de la Cámara IP

Promedio de paquetes por seg.	168
Promedio de bytes por seg.	88.357
Total de paquetes	1.209.510
Total bytes	636.197.882

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	802.688	403.912	2.716
Bytes	613.757.518	22.052.955	269.950
Bytes por seg.	85.256	40540	37

1.25 Captura de Paquetes de los Protocolos Involucrados

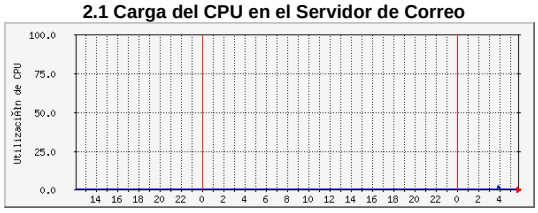




2. ATAQUE SYN FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

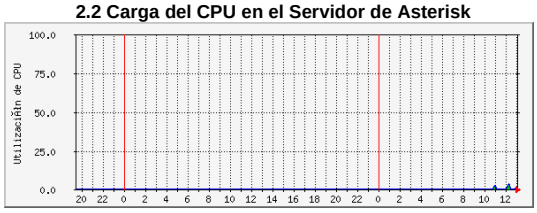
MRTG (Promedio 5 Min) - Tiempo de Monitoreo: 2 horas

2.1 Carga del CPU en el Servidor de Correo



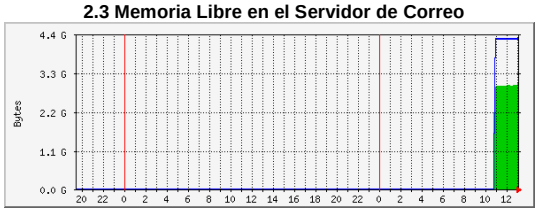
	Max	Average	Current
Usado	2.0 %	1.0 %	0.0 %

2.2 Carga del CPU en el Servidor de Asterisk



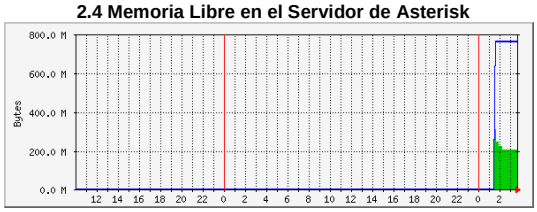
	Max	Average	Current
Usado	3.0 %	1.0 %	1.0 %

2.3 Memoria Libre en el Servidor de Correo



	Max	Average	Current
Usada	2997.2 MB	2909.5 MB	2997.2 MB
Total	4253.9 MB	4216.0 MB	4253.9 MB

2.4 Memoria Libre en el Servidor de Asterisk

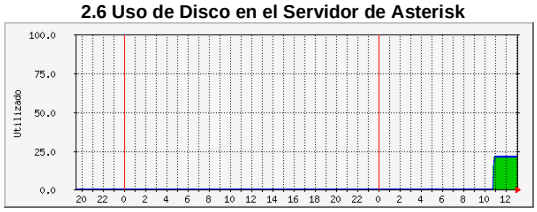


	Max	Average	Current
Libre	309.7 MB	213.9 MB	203.3 MB
Total	762.6 MB	753.2 MB	762.6 MB

2.5 Uso de Disco en el Servidor de Correo

	Max	Average	Current
C:/	48.0 %	48.0 %	48.0 %
Out	48.0 %	48.0 %	48.0 %

2.6 Uso de Disco en el Servidor de Asterisk

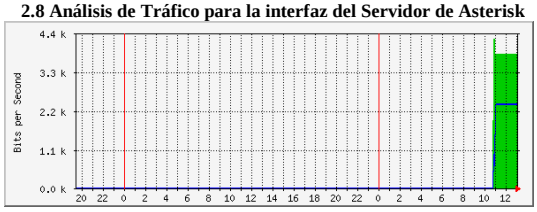


	Max	Average	Current
/	21.0 %	21.0 %	21.0 %
Out	21.0 %	21.0 %	21.0 %

2.7 Análisis de Tráfico para la interfaz del Servidor de Correo

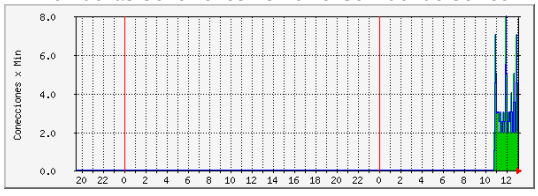
	Max	Average	Current
Entrada	880.0 b/s	248.0 b/s	296.0 b/s
Salida	560.0 b/s	168.0 b/s	264.0 b/s

2.8 Análisis de Tráfico para la interfaz del Servidor de Asterisk



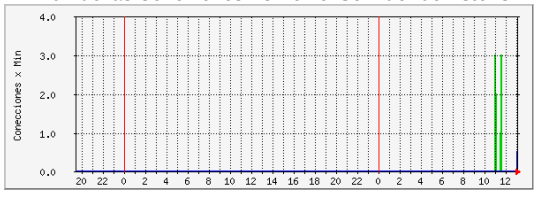
	Max	Average	Current
Entrada	4232.0 b/s	3760.0 b/s	3816.0 b/s
Salida	2368.0 b/s	2256.0 b/s	2368.0 b/s

2.9 Nuevas Conexiones TCP en el Servidor de Correo



	Max	Average	Current
Conexiones Passive Open	8.0 cs/min	3.0 cs/min	3.0 cs/min
Conexiones Active Open	8.0 cs/min	3.0 cs/min	3.0 cs/min

2.10 Nuevas Conexiones TCP en el Servidor de Asterisk



	Max	Average	Current
Conexiones Passive Open	3.0 cs/min	1.0 cs/min	0.0 cs/min
Conexiones Active Open	0.0 cs/min	0.0 cs/min	1.0 cs/min

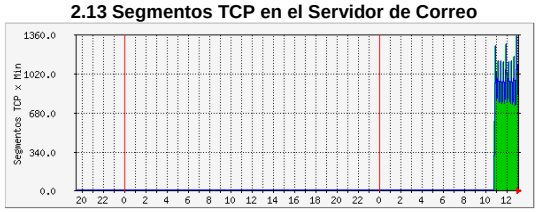
2.11 Conexiones TCP Establecidas en el Servidor de Correo

	Max	Average	Current
Entrantes	117.0 cs	98.0 cs	106.0 cs

2.12 Conexiones TCP Establecidas en el Servidor de Asteris

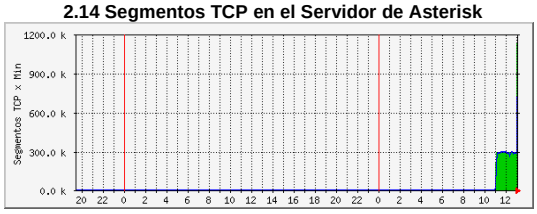
	Max	Average	Current
Entrantes	1.0 cs	1.0 cs	0.0 cs

2.13 Segmentos TCP en el Servidor de Correo



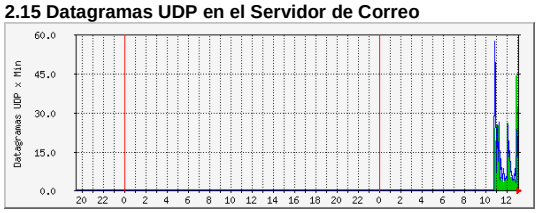
	Max	Average	Current
Enviados	1340.0 segs/min	905.0 segs/min	897.0 segs/min
Recibidos	1341.0 segs/min	906.0 segs/min	897.0 segs/min

2.14 Segmentos TCP en el Servidor de Asterisk



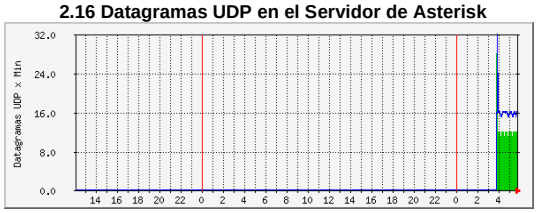
	Max	Average	Current
Enviados	1134.2 ksegs/min	283.3 ksegs/min	1134.2 ksegs/min
Recibidos	1133.1 ksegs/min	282.3 ksegs/min	1133.1 ksegs/min

2.15 Datagramas UDP en el Servidor de Correo



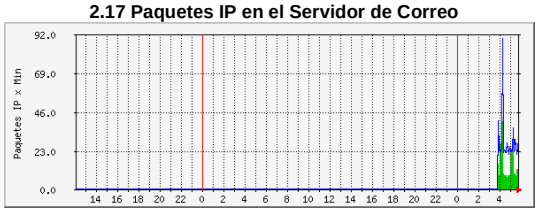
	Max	Average	Current
Enviados	44.0 dts/min	11.0 dts/min	32.0 dts/min
Recibidos	57.0 dts/min	13.0 dts/min	28.0 dts/min

2.16 Datagramas UDP en el Servidor de Asterisk



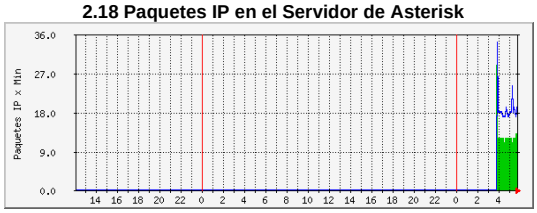
	Max	Average	Current
Enviados	28.0 dts/min	10.0 dts/min	12.0 dts/min
Recibidos	32.0 dts/min	14.0 dts/min	14.0 dts/min

2.17 Paquetes IP en el Servidor de Correo



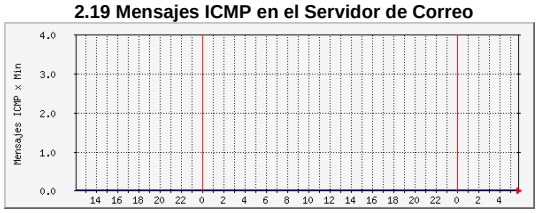
	Max	Average	Current
Paquetes IP Solicitados	40.0 pts/min	12.0 pts/min	8.0 pts/min
Paquetes IP Recibidos	89.0 pts/min	28.0 pts/min	29.0 pts/min

2.18 Paquetes IP en el Servidor de Asterisk



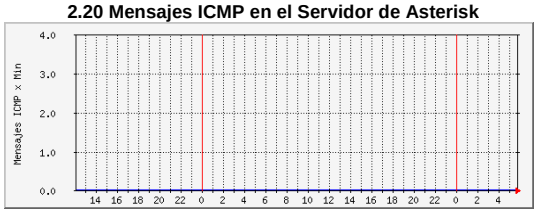
	Max	Average	Current
Paquetes IP Solicitados	272 pts/min	283.4 kpts/min	285.2 pts/min
Paquetes IP Recibidos	275,3 pts/min	282.4 pts/min	284.6 pts/min

2.19 Mensajes ICMP en el Servidor de Correo



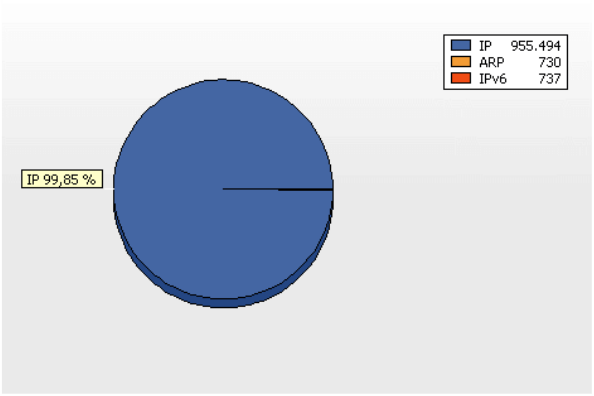
	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

2.20 Mensajes ICMP en el Servidor de Asterisk

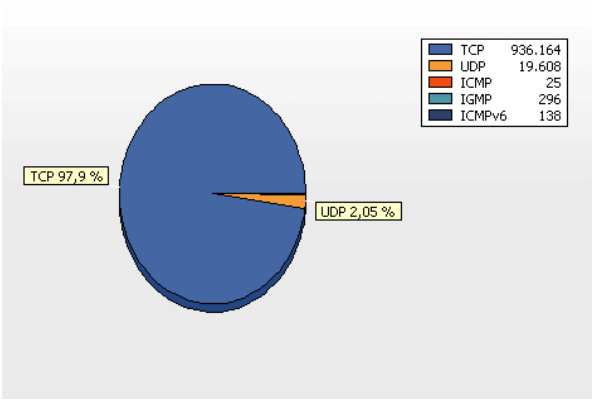


	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

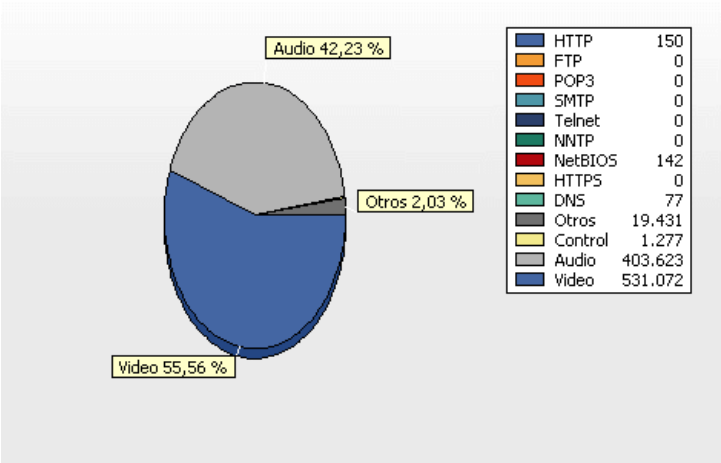
MONITOREO DE LA CÁMARA IP
CommView - Tiempo de Monitoreo: 2 horas



2.21 Paquetes IP



2.22 Paquetes TCP, UDP e ICMP



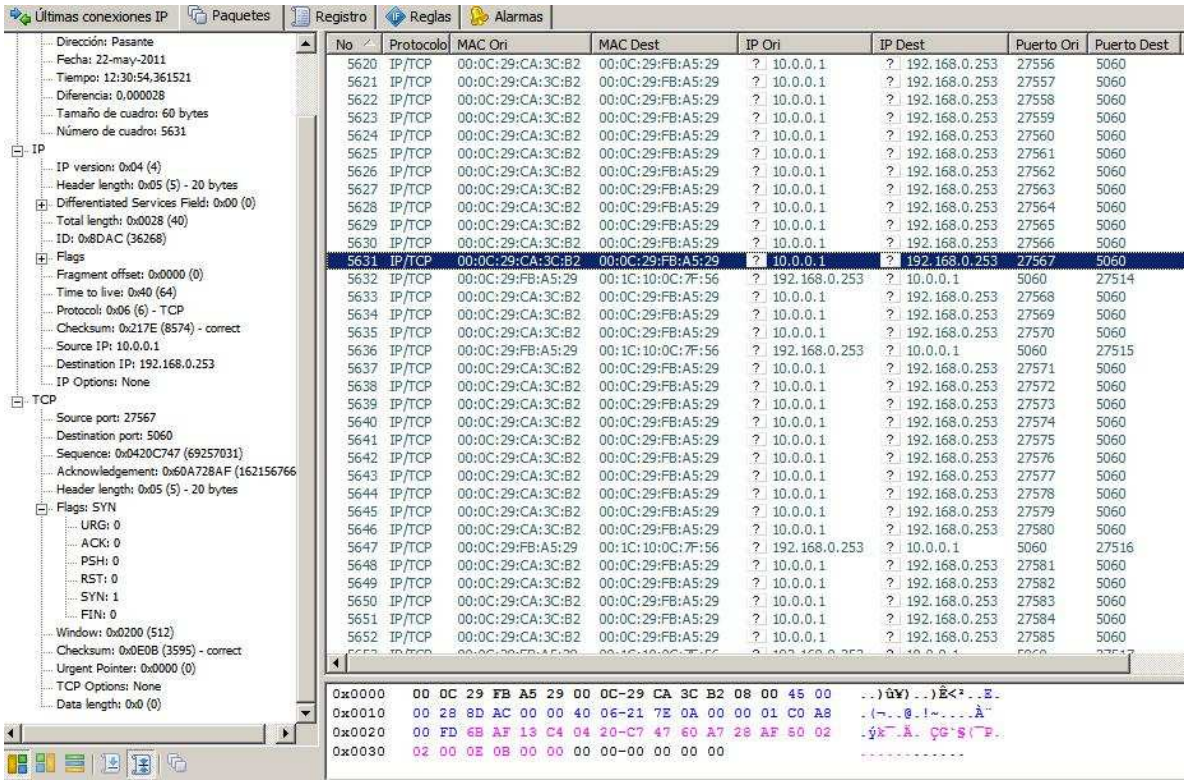
2.23 Protocolos de capa aplicación en la Cámara IP

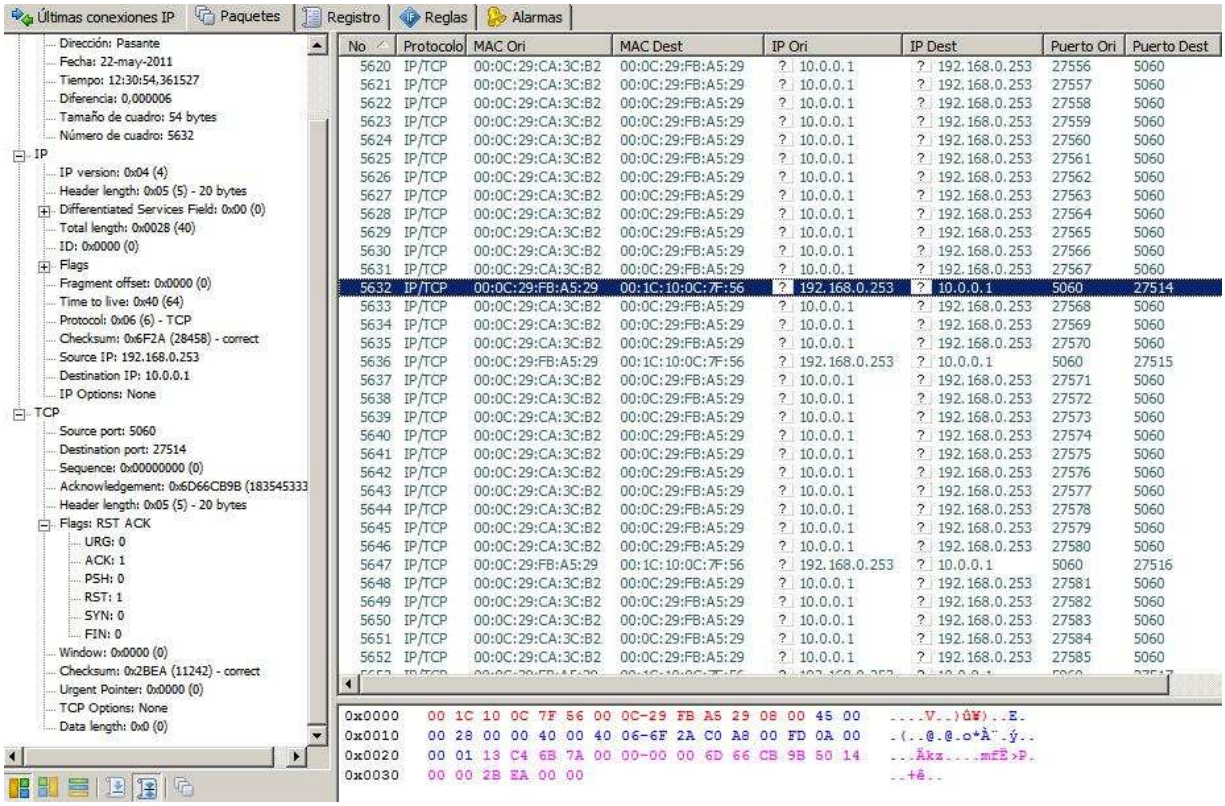
2.24 Resumen General de la Cámara IP

Promedio de paquetes por seg.	133
Promedio de bytes por seg.	71.809
Total de paquetes	957.126
Total bytes	517.041.545

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	632.360	322.645	1.956
Bytes	497.643.580	19.053.426	257.687
Bytes por seg.	69.127	2.647	36

2.25 Captura de Paquetes de los Protocolos Involucrados

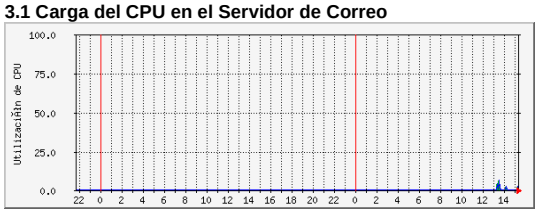




3. ATAQUE SYN FLOOD CONTRA LA CÁMARA IP

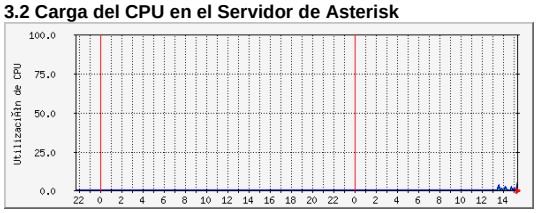
MRTG (Promedio 5 Min) - Tiempo de Monitoreo: 2 horas

3.1 Carga del CPU en el Servidor de Correo



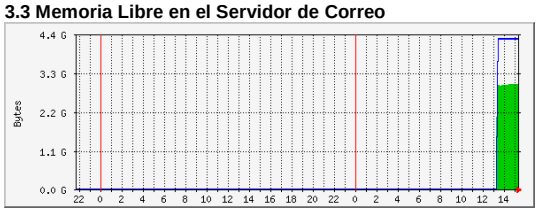
	Max	Average	Current
Usado	4.0 %	1.0 %	0.0 %

3.2 Carga del CPU en el Servidor de Asterisk



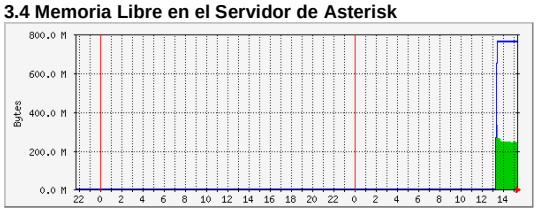
	Max	Average	Current
Usado	4.0 %	1.0 %	5.0 %

3.3 Memoria Libre en el Servidor de Correo



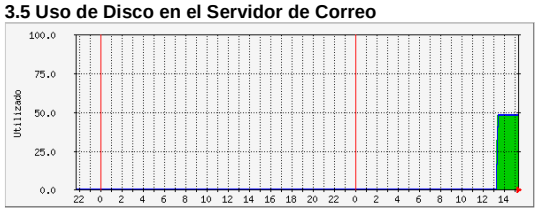
	Max	Average	Current
Usada	2984.6 MB	2927.0 MB	2983.9 MB
Total	4253.9 MB	4202.3 MB	4253.9 MB

3.4 Memoria Libre en el Servidor de Asterisk



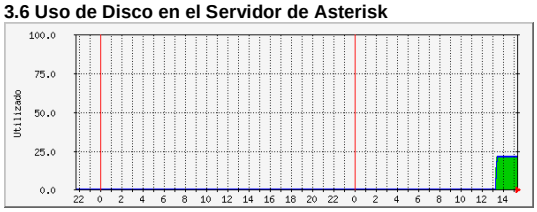
	Max	Average	Current
Libre	330.0 MB	245.1 MB	241.5 MB
Total	762.6 MB	753.4 MB	762.6 MB

3.5 Uso de Disco en el Servidor de Correo



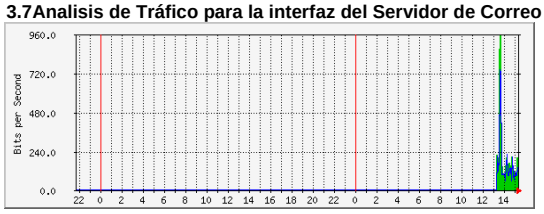
	Max	Average	Current
C:/	48.0 %	48.0 %	48.0 %
Out	48.0 %	48.0 %	48.0 %

3.6 Uso de Disco en el Servidor de Asterisk



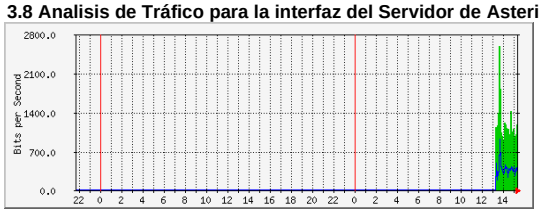
	Max	Average	Current
/	21.0 %	21.0 %	21.0 %
Out	21.0 %	21.0 %	21.0 %

3.7Analisis de Tráfico para la interfaz del Servidor de Correo



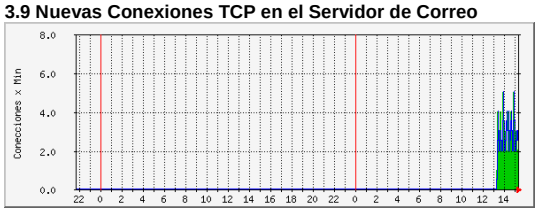
	Max	Average	Current
Entrada	960.0 b/s	200.0 b/s	136.0 b/s
Salida	736.0 b/s	168.0 b/s	128.0 b/s

3.8 Analisis de Tráfico para la interfaz del Servidor de Asteri



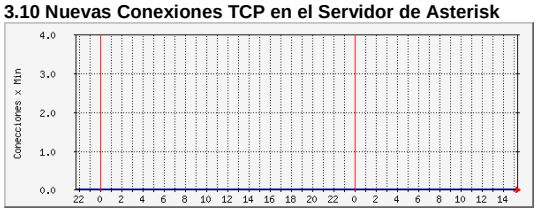
	Max	Average	Current
Entrada	2584.0 b/s	1128.0 b/s	1184.0 b/s
Salida	904.0 b/s	384.0 b/s	440.0 b/s

3.9 Nuevas Conexiones TCP en el Servidor de Correo



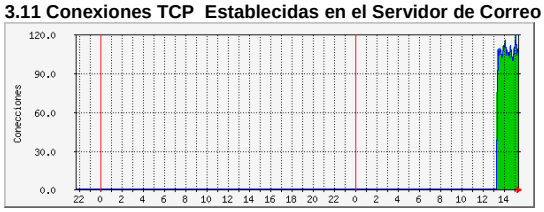
	Max	Average	Current
Conexiones Passive Open	5.0 cs/min	3.0 cs/min	2.0 cs/min
Conexiones Active Open	5.0 cs/min	3.0 cs/min	2.0 cs/min

3.10 Nuevas Conexiones TCP en el Servidor de Asterisk



	Max	Average	Current
Conexiones Passive Open	0.0 cs/min	0.0 cs/min	0.0 cs/min
Conexiones Active Open	0.0 cs/min	0.0 cs/min	0.0 cs/min

3.11 Conexiones TCP Establecidas en el Servidor de Correo

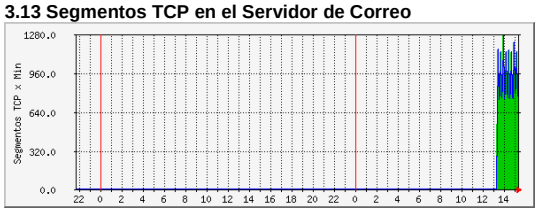


	Max	Average	Current
Entrantes	119.0 cs	105.0 cs	104.0 cs

3.12 Conexiones TCP Establecidas en el Servidor de Asteris

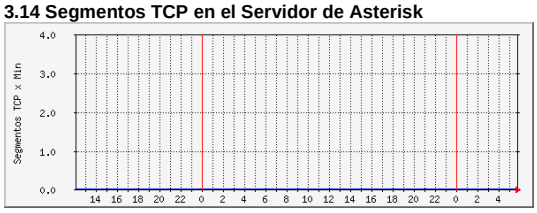
	Max	Average	Current
Entrantes	1.0 cs	0.0 cs	0.0 cs

3.13 Segmentos TCP en el Servidor de Correo



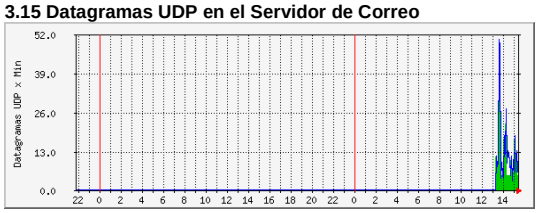
	Max	Average	Current
Enviados	1266.0 segs/min	893.0 segs/min	755.0 segs/min
Recibidos	1268.0 segs/min	894.0 segs/min	755.0 segs/min

3.14 Segmentos TCP en el Servidor de Asterisk



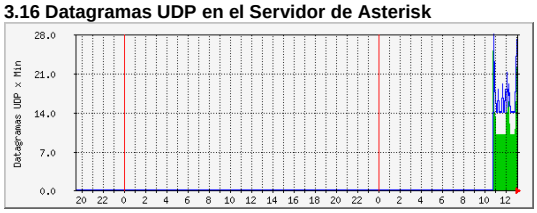
	Max	Average	Current
Enviados	0.0 segs/min	0.0 segs/min	0.0 segs/min
Recibidos	0.0 segs/min	0.0 segs/min	0.0 segs/min

3.15 Datagramas UDP en el Servidor de Correo



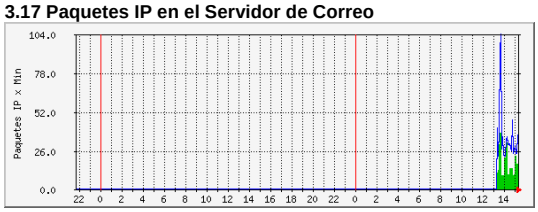
	Max	Average	Current
Enviados	32.0 dts/min	9.0 dts/min	4.0 dts/min
Recibidos	50.0 dts/min	13.0 dts/min	8.0 dts/min

3.16 Datagramas UDP en el Servidor de Asterisk



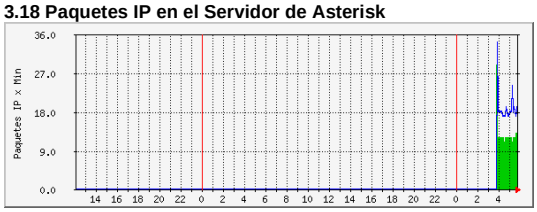
	Max	Average	Current
Enviados	25.0 dts/min	12.0 dts/min	22.0 dts/min
Recibidos	28.0 dts/min	17.0 dts/min	23.0 dts/min

3.17 Paquetes IP en el Servidor de Correo



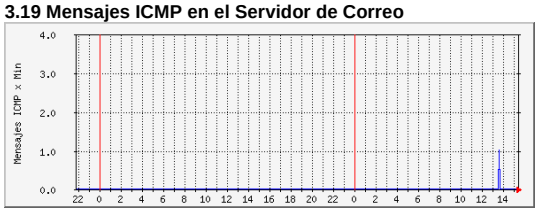
	Max	Average	Current
Paquetes IP Solicitados	38.0 pts/min	14.0 pts/min	10.0 pts/min
Paquetes IP Recibidos	104.0 pts/min	35.0 pts/min	28.0 pts/min

3.18 Paquetes IP en el Servidor de Asterisk



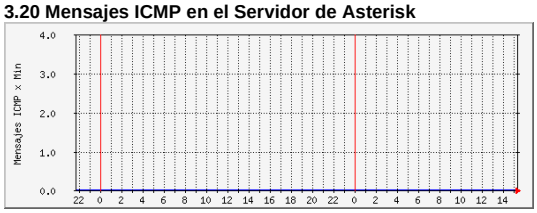
	Max	Average	Current
Paquetes IP Solicitados	29.0 pts/min	13.0 pts/min	12.0 pts/min
Paquetes IP Recibidos	34.0 pts/min	19.0 pts/min	20.0 pts/min

3.19 Mensajes ICMP en el Servidor de Correo



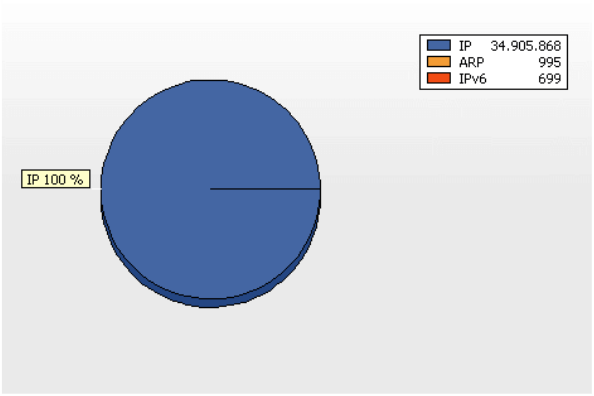
	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	1.0 msgs/min	1.0 msgs/min	0.0 msgs/min

3.20 Mensajes ICMP en el Servidor de Asterisk

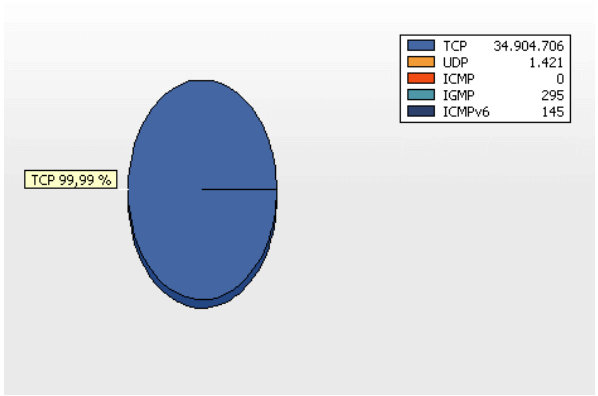


	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

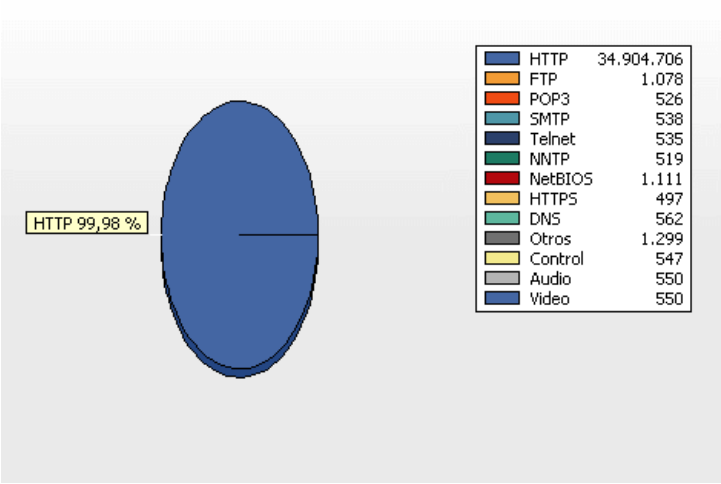
MONITOREO DE LA CÁMARA IP
CommView - Tiempo de Monitoreo: 2 horas



3.21 Paquetes IP



3.22 Paquetes TCP, UDP e ICMP



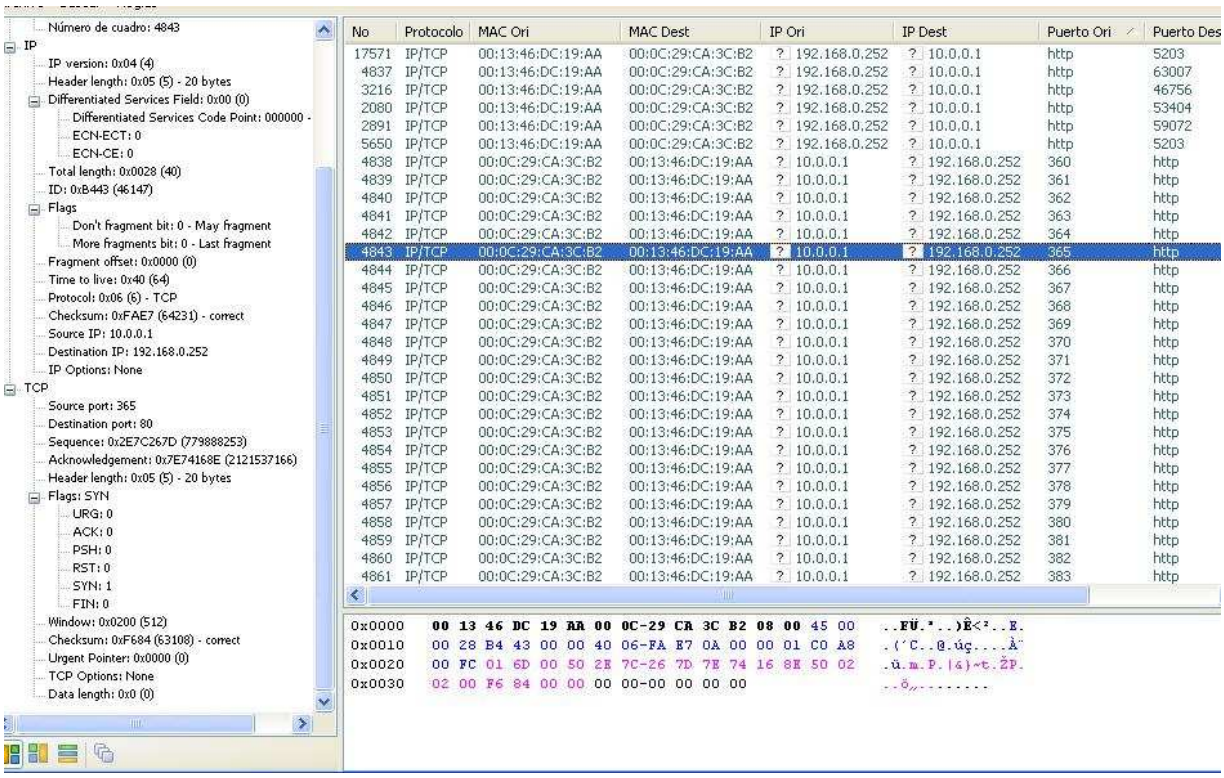
3.23 Protocolos de capa aplicación en la Cámara IP

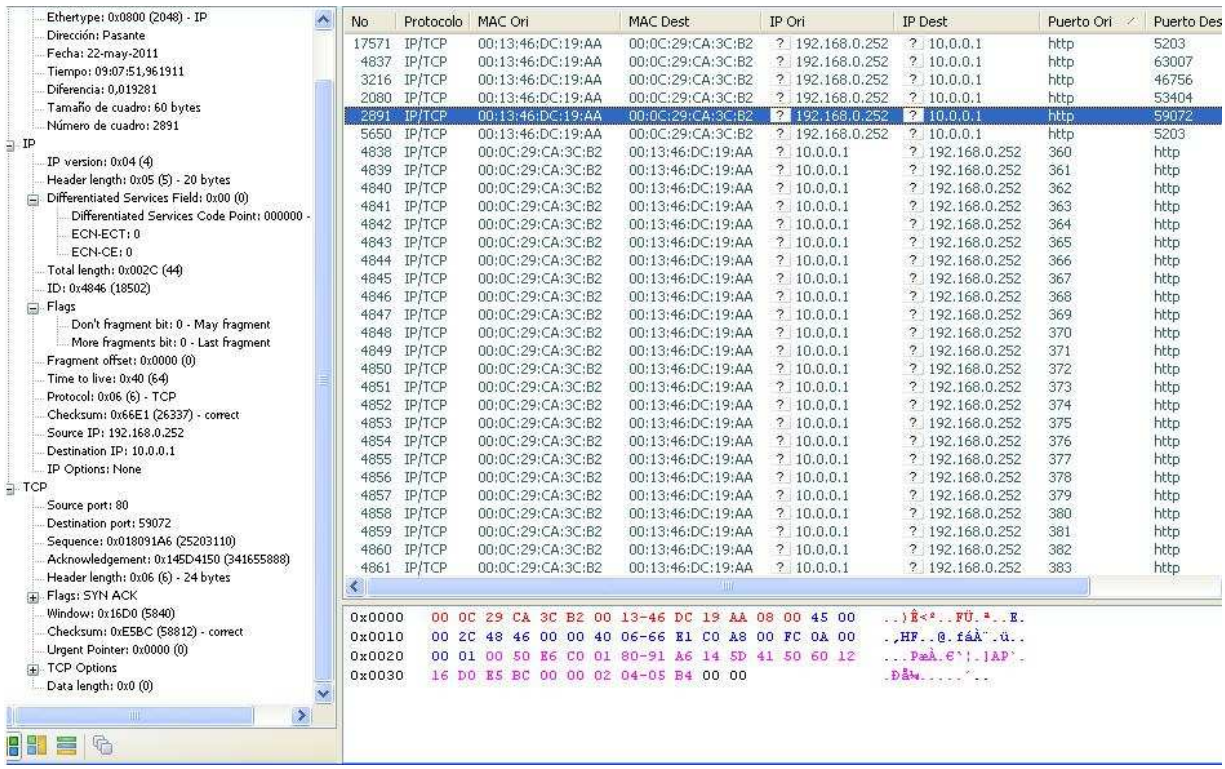
3.24 Resumen General de la Cámara IP

Promedio de paquetes por seg.	4.849
Promedio de bytes por seg.	290.976
Total de paquetes	34.912.201
Total bytes	2.095.016.729

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	227	985	34.906.350
Bytes	94.140	156.342	2.094.487.907
Bytes por seg.	13	22	290.942

3.25 Captura de Paquetes de los Protocolos Involucrados

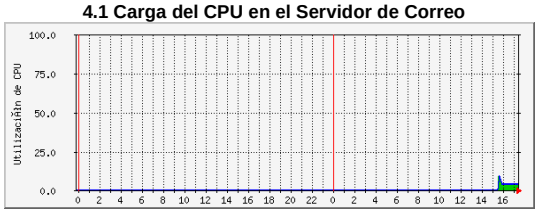




4. ATAQUE UDP FLOOD CONTRA EL SERVIDOR DE WEB/CORREO

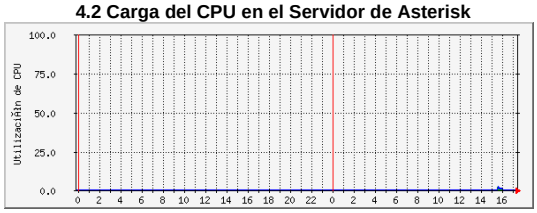
MRTG (Promedio 5 Min) - Tiempo de Monitoreo: 2 horas

4.1 Carga del CPU en el Servidor de Correo



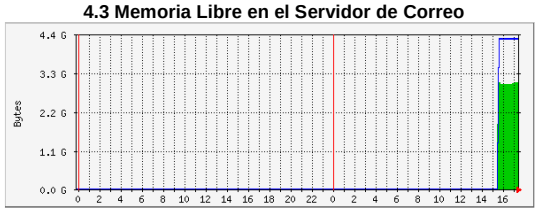
	Max	Average	Current
Usado	9.0 %	4.0 %	4.0 %

4.2 Carga del CPU en el Servidor de Asterisk



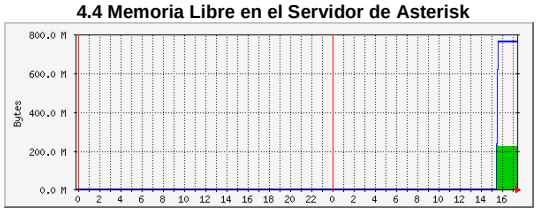
	Max	Average	Current
Usado	2.0 %	1.0 %	0.0 %

4.3 Memoria Libre en el Servidor de Correo



	Max	Average	Current
Usada	3041.0 MB	2953.0 MB	3031.2 MB
Total	4253.9 MB	4186.0 MB	4253.9 MB

4.4 Memoria Libre en el Servidor de Asterisk

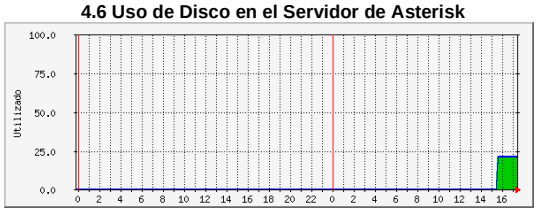


	Max	Average	Current
Libre	225.1 MB	215.6 MB	220.0 MB
Total	762.6 MB	750.4 MB	762.6 MB

4.5 Uso de Disco en el Servidor de Correo

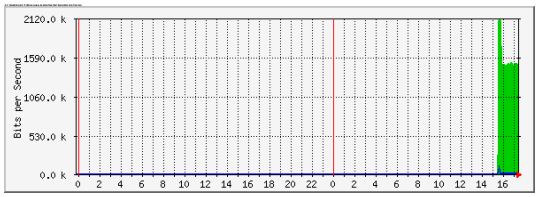
	Max	Average	Current
C:/	48.0 %	47.0 %	48.0 %
Out	48.0 %	47.0 %	48.0 %

4.6 Uso de Disco en el Servidor de Asterisk



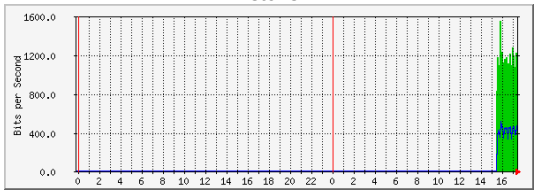
	Max	Average	Current
/	21.0 %	21.0 %	21.0 %
Out	21.0 %	21.0 %	21.0 %

4.7 Analisis de Tráfico para la interfaz del Servidor de Correo



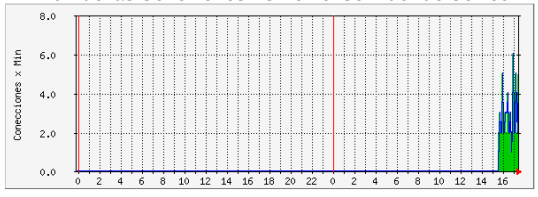
	Max	Average	Current
Entrada	2105.5 kb/s	1528.5 kb/s	1498.4 kb/s
Salida	99.4 kb/s	5360.0 b/s	664.0 b/s

4.8 Analisis de Tráfico para la interfaz del Servidor de Asterisk



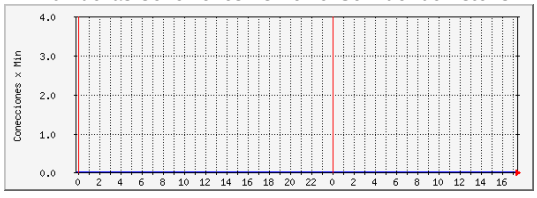
	Max	Average	Current
Entrada	1552.0 b/s	1112.0 b/s	1104.0 b/s
Salida	504.0 b/s	416.0 b/s	456.0 b/s

4.9 Nuevas Conexiones TCP en el Servidor de Correo



	Max	Average	Current
Conexiones Passive Open	6.0 cs/min	3.0 cs/min	5.0 cs/min
Conexiones Active Open	6.0 cs/min	3.0 cs/min	5.0 cs/min

4.10 Nuevas Conexiones TCP en el Servidor de Asterisk



	Max	Average	Current
Conexiones Passive Open	0.0 cs/min	0.0 cs/min	0.0 cs/min
Conexiones Active Open	0.0 cs/min	0.0 cs/min	0.0 cs/min

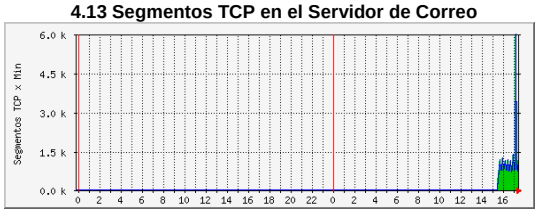
4.11 Conexiones TCP Establecidas en el Servidor de Correo

	Max	Average	Current
Entrantes	119.0 cs	107.0 cs	102.0 cs

4.12 Conexiones TCP Establecidas en el Servidor de Asteris

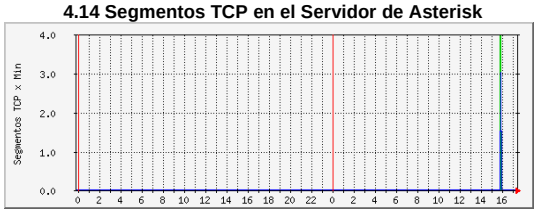
	Max	Average	Current
Entrantes	0.0 cs	0.0 cs	0.0 cs

4.13 Segmentos TCP en el Servidor de Correo



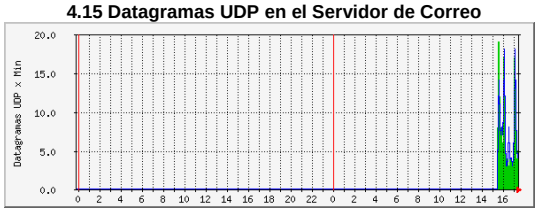
	Max	Average	Current
Enviados	5972.0 segs/min	1092.0 segs/min	1149.0 segs/min
Recibidos	5973.0 segs/min	1093.0 segs/min	1149.0 segs/min

4.14 Segmentos TCP en el Servidor de Asterisk



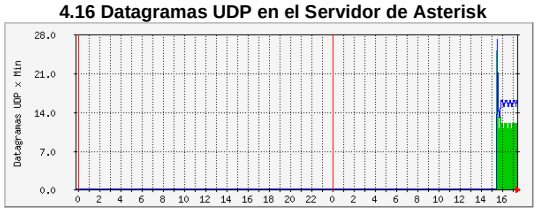
	Max	Average	Current
Enviados	4.0 segs/min	2.0 segs/min	0.0 segs/min
Recibidos	3.0 segs/min	2.0 segs/min	0.0 segs/min

4.15 Datagramas UDP en el Servidor de Correo



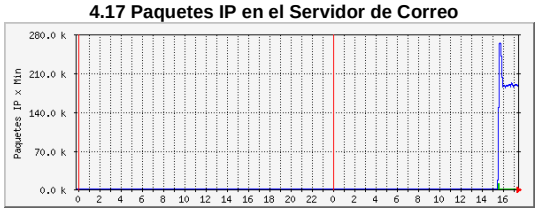
	Max	Average	Current
Enviados	19.0 dts/min	7.0 dts/min	5.0 dts/min
Recibidos	18.0 dts/min	7.0 dts/min	5.0 dts/min

4.16 Datagramas UDP en el Servidor de Asterisk



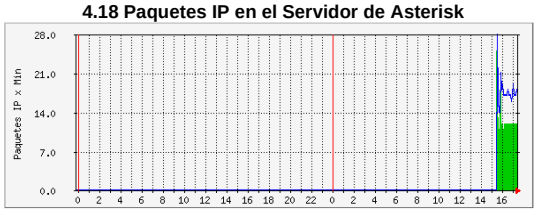
	Max	Average	Current
Enviados	25.0 dts/min	12.0 dts/min	12.0 dts/min
Recibidos	27.0 dts/min	16.0 dts/min	16.0 dts/min

4.17 Paquetes IP en el Servidor de Correo



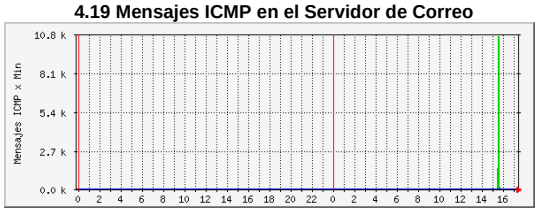
	Max	Average	Current
Paquetes IP Solicitados	10.6 kpts/min	573.0 pts/min	70.0 pts/min
Paquetes IP Recibidos	263.2 kpts/min	191.1 kpts/min	187.3 kpts/min

4.18 Paquetes IP en el Servidor de Asterisk



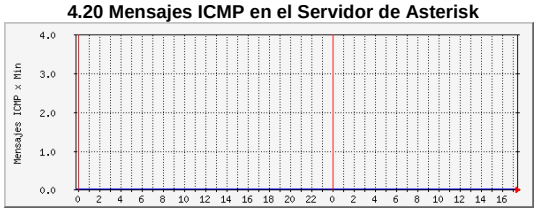
	Max	Average	Current
Paquetes IP Solicitados	25.0 pts/min	13.0 pts/min	12.0 pts/min
Paquetes IP Recibidos	28.0 pts/min	18.0 pts/min	17.0 pts/min

4.19 Mensajes ICMP en el Servidor de Correo



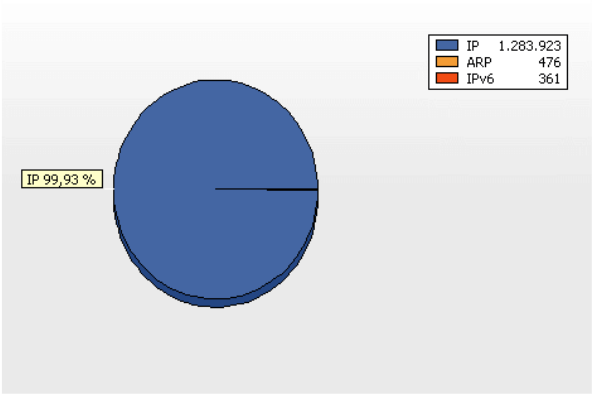
	Max	Average	Current
Enviados	10.6 kmsgs/min	562.0 msgs/min	60.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

4.20 Mensajes ICMP en el Servidor de Asterisk

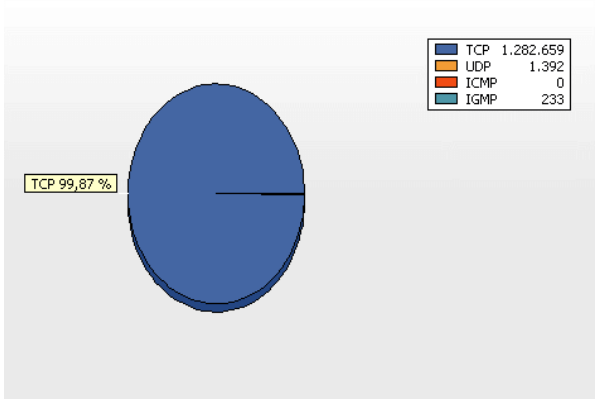


	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

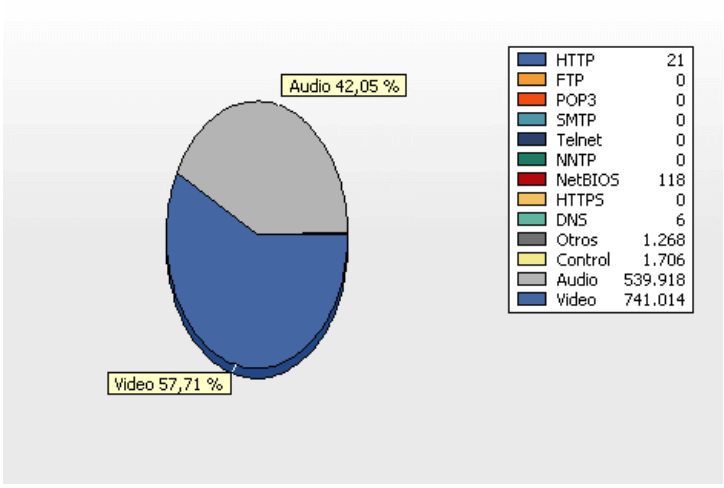
MONITOREO DE LA CÁMARA IP
CommView - Tiempo de Monitoreo: 2 horas



4.21 Paquetes IP



4.22 Paquetes TCP, UDP e ICMP



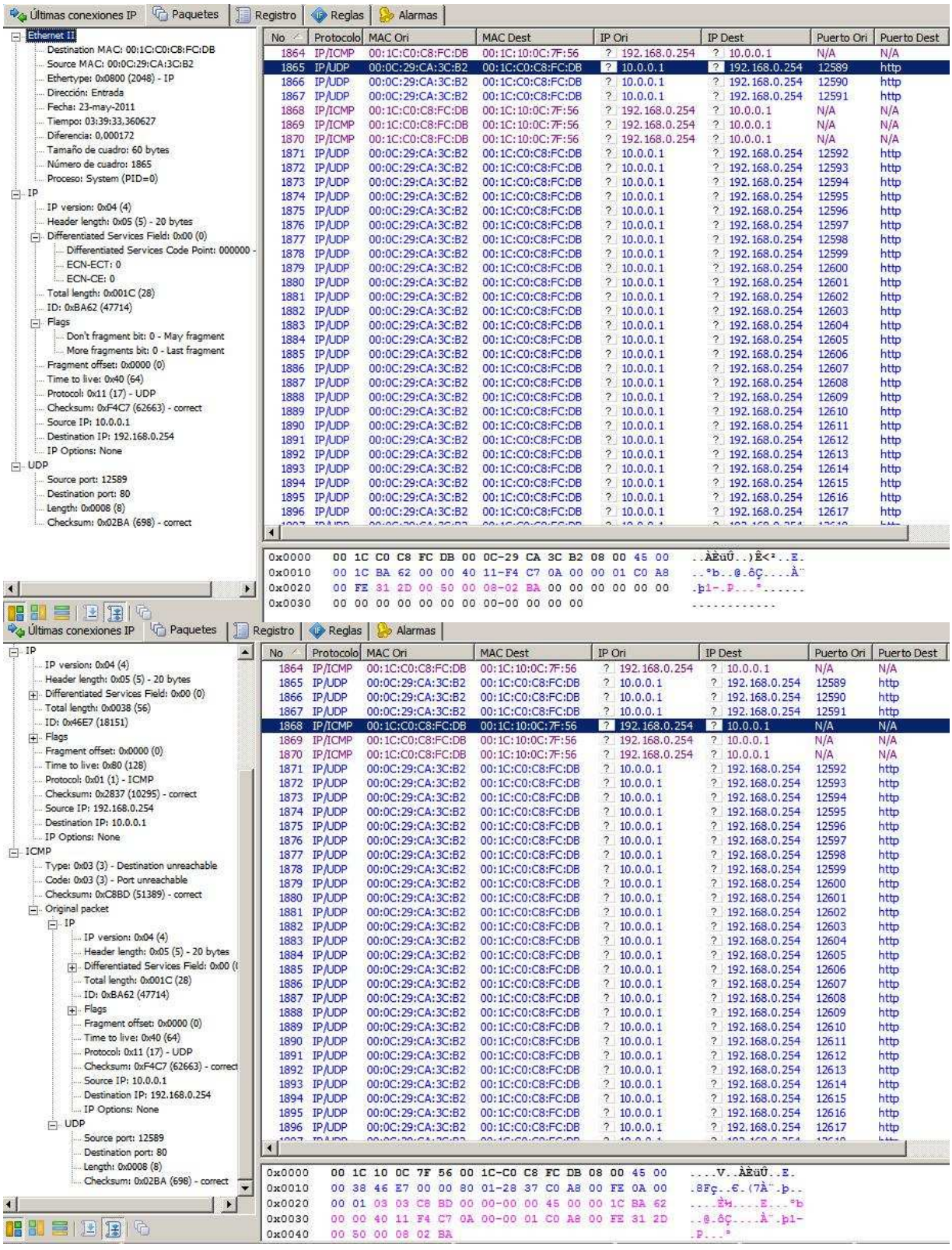
4.23 Protocolos de capa aplicación en la Cámara IP

4.24 Resumen General de la Cámara IP

Promedio de paquetes por seg.	178
Promedio de bytes por seg.	98.160
Total de paquetes	1.284.931
Total bytes	706.747.983

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	854.167	429.623	970
Bytes	683.133.054	23.417.974	101.834
Bytes por seg.	94.893	40540	14

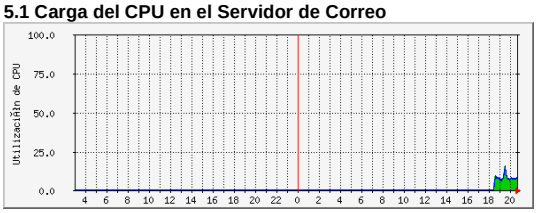
4.25 Captura de Paquetes de los Protocolos Involucrados



5. ATAQUE UDP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

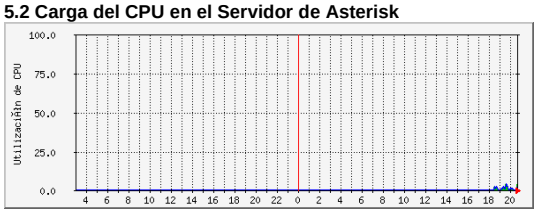
MRTG (Promedio 5 Min) - Tiempo de Monitoreo: 2 horas

5.1 Carga del CPU en el Servidor de Correo



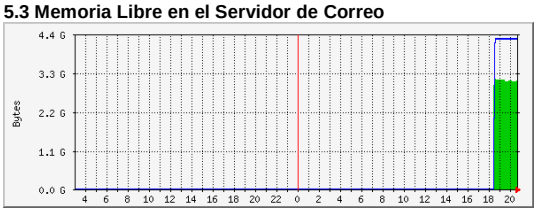
	Max	Average	Current
Usado	12.0 %	5.0 %	6.0 %

5.2 Carga del CPU en el Servidor de Asterisk



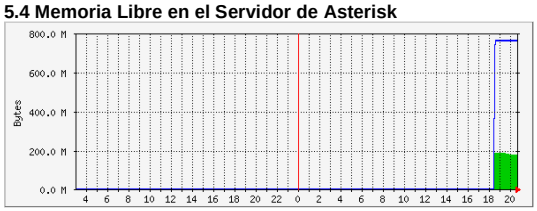
	Max	Average	Current
Usado	4.0 %	1.0 %	4.0 %

5.3 Memoria Libre en el Servidor de Correo



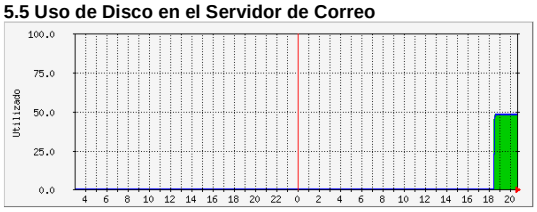
	Max	Average	Current
Usada	3126.3 MB	3077.5 MB	3080.8 MB
Total	4253.9 MB	4245.5 MB	4253.9 MB

5.4 Memoria Libre en el Servidor de Asterisk



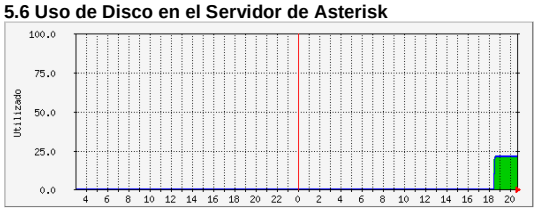
	Max	Average	Current
Libre	187.2 MB	176.6 MB	143.0 MB
Total	762.6 MB	761.1 MB	762.6 MB

5.5 Uso de Disco en el Servidor de Correo



	Max	Average	Current
C:/	48.0 %	48.0 %	48.0 %
Out	48.0 %	48.0 %	48.0 %

5.6 Uso de Disco en el Servidor de Asterisk

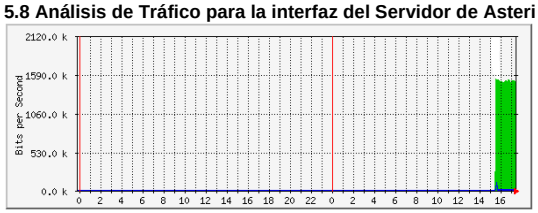


	Max	Average	Current
/	21.0 %	21.0 %	21.0 %
Out	21.0 %	21.0 %	21.0 %

5.7 Análisis de Tráfico para la interfaz del Servidor de Corre

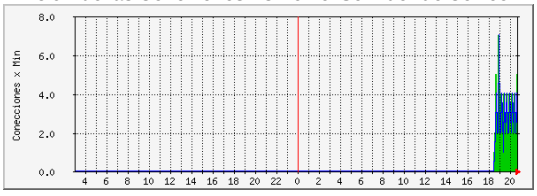
	Max	Average	Current
Entrada	448.0 b/s	176.0 b/s	128.0 b/s
Salida	536.0 b/s	152.0 b/s	136.0 b/s

5.8 Análisis de Tráfico para la interfaz del Servidor de Asteri



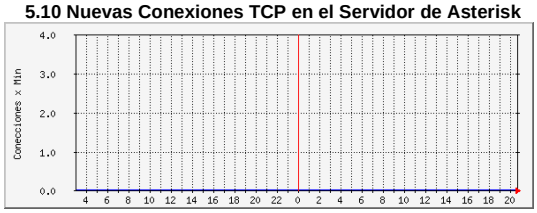
	Max	Average	Current
Entrada	1405.5 kb/s	1428.5 kb/s	1498.4 kb/s
Salida	936.0 b/s	464.0 b/s	552.0 b/s

5.9 Nuevas Conexiones TCP en el Servidor de Correo



	Max	Average	Current
Conexiones Passive Open	7.0 cs/min	3.0 cs/min	5.0 cs/min
Conexiones Active Open	7.0 cs/min	3.0 cs/min	5.0 cs/min

5.10 Nuevas Conexiones TCP en el Servidor de Asterisk



	Max	Average	Current
Conexiones Passive Open	0.0 cs/min	0.0 cs/min	0.0 cs/min
Conexiones Active Open	0.0 cs/min	0.0 cs/min	0.0 cs/min

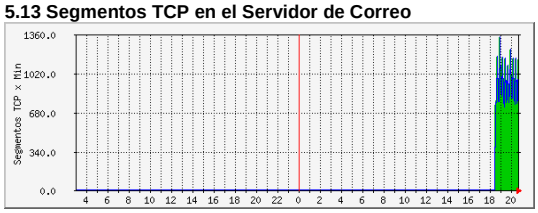
5.11 Conexiones TCP Establecidas en el Servidor de Correo

	Max	Average	Current
Entrantes	127.0 cs	109.0 cs	108.0 cs

5.12 Conexiones TCP Establecidas en el Servidor de Asteris

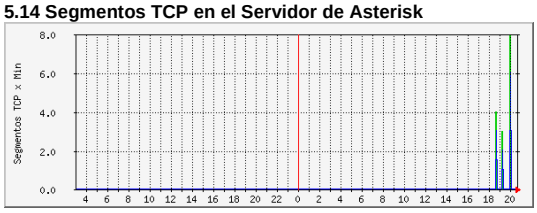
	Max	Average	Current
Entrantes	1.0 cs	1.0 cs	0.0 cs

5.13 Segmentos TCP en el Servidor de Correo



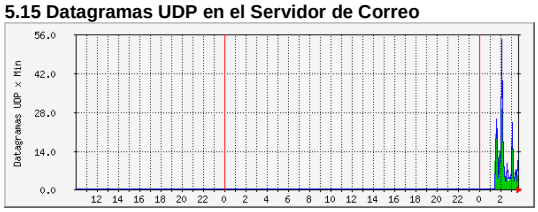
	Max	Average	Current
Enviados	1332.0 segs/min	914.0 segs/min	1139.0 segs/min
Recibidos	1332.0 segs/min	914.0 segs/min	1139.0 segs/min

5.14 Segmentos TCP en el Servidor de Asterisk



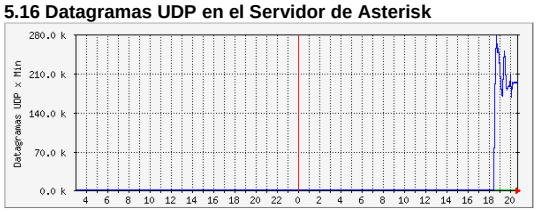
	Max	Average	Current
Enviados	8.0 segs/min	2.0 segs/min	0.0 segs/min
Recibidos	6.0 segs/min	2.0 segs/min	0.0 segs/min

5.15 Datagramas UDP en el Servidor de Correo



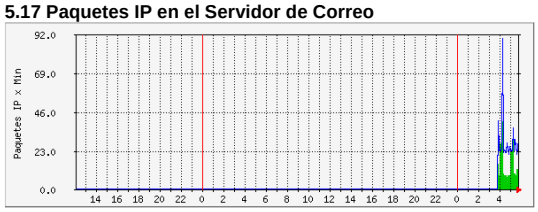
	Max	Average	Current
Enviados	29.0 dts/min	8.0 dts/min	3.0 dts/min
Recibidos	54.0 dts/min	10.0 dts/min	4.0 dts/min

5.16 Datagramas UDP en el Servidor de Asterisk



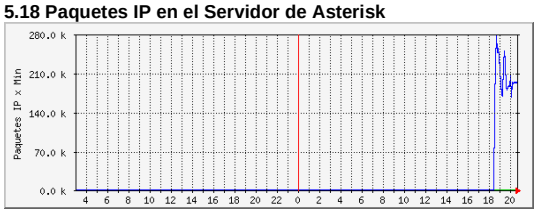
	Max	Average	Current
Enviados	27.0 dts/min	13.0 dts/min	15.0 dts/min
Recibidos	275.6 kdts/min	203.0 kdts/min	192.8 kdts/min

5.17 Paquetes IP en el Servidor de Correo



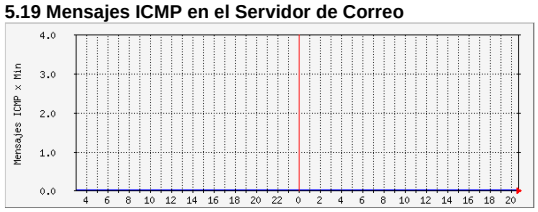
	Max	Average	Current
Paquetes IP Solicitados	40.0 pts/min	12.0 pts/min	8.0 pts/min
Paquetes IP Recibidos	89.0 pts/min	28.0 pts/min	29.0 pts/min

5.18 Paquetes IP en el Servidor de Asterisk



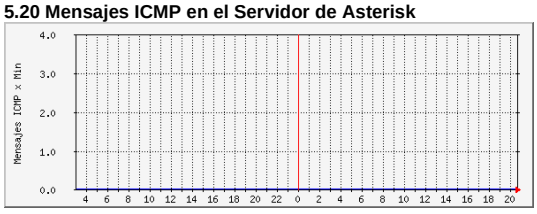
	Max	Average	Current
Paquetes IP Solicitados	28.0 pts/min	14.0 pts/min	15.0 pts/min
Paquetes IP Recibidos	275.6 kpts/min	203.0 kpts/min	192.8 kpts/min

5.19 Mensajes ICMP en el Servidor de Correo



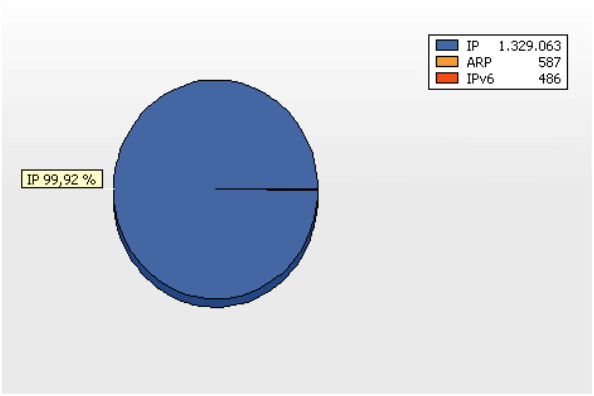
	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

5.20 Mensajes ICMP en el Servidor de Asterisk

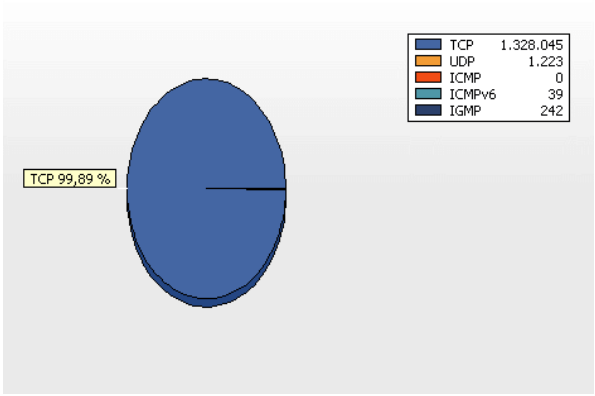


	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

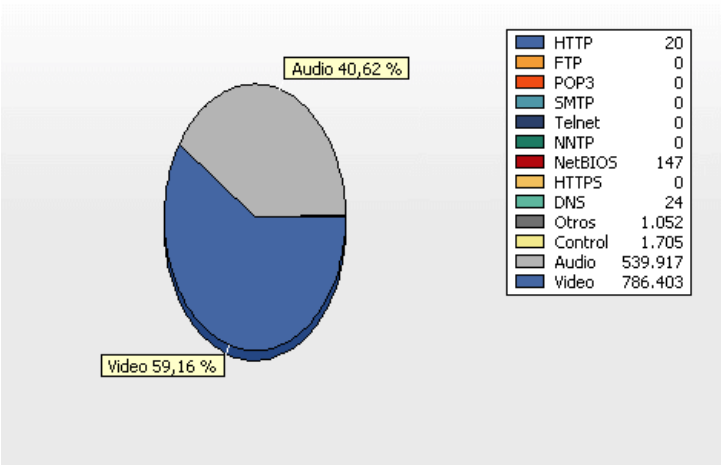
MONITOREO DE LA CÁMARA IP
CommView - Tiempo de Monitoreo: 2 horas



5.21 Paquetes IP



5.22 Paquetes TCP, UDP e ICMP



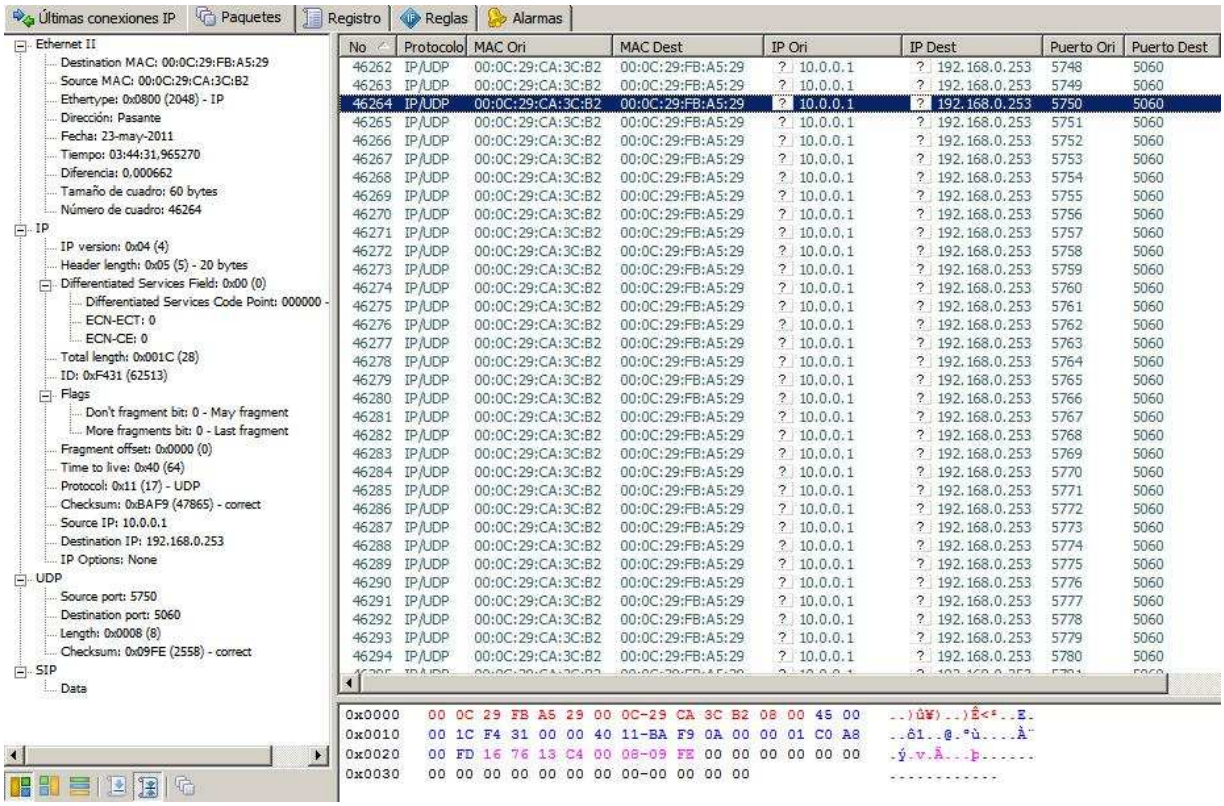
5.23 Protocolos de capa aplicación en la Cámara IP

5.24 Resumen General de la Cámara IP

Promedio de paquetes por seg.	185
Promedio de bytes por seg.	104.488
Total de paquetes	1.330.319
Total bytes	752.307.769

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	884.298	444.517	1.321
Bytes	727.952.961	24.110.078	144.586
Bytes por seg.	101.119	40540	20

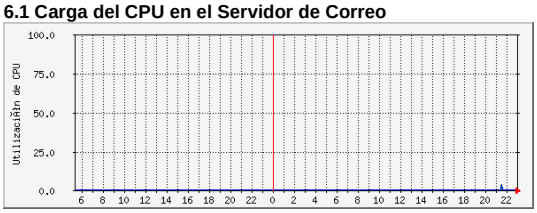
5.25 Captura de Paquetes de los Protocolos Involucrados



6. ATAQUE UDP FLOOD CONTRA LA CAMARA IP

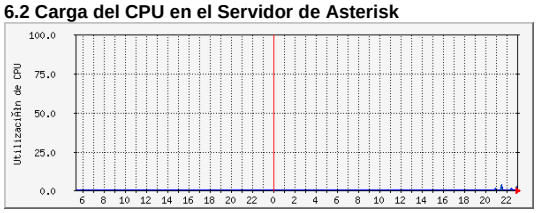
MRTG (Promedio 5 Min) - Tiempo de Monitoreo: 2 horas

6.1 Carga del CPU en el Servidor de Correo



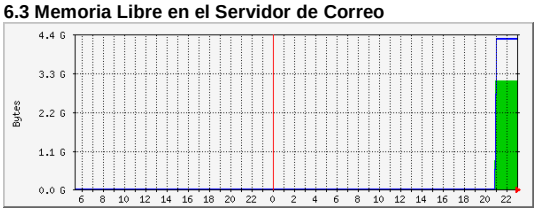
	Max	Average	Current
Usado	3.0 %	1.0 %	0.0 %

6.2 Carga del CPU en el Servidor de Asterisk



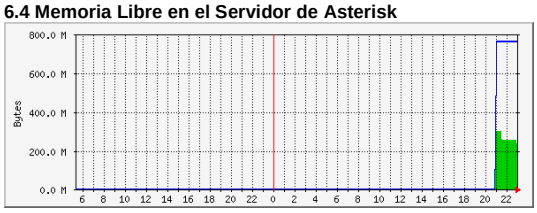
	Max	Average	Current
Usado	3.0 %	1.0 %	2.0 %

6.3 Memoria Libre en el Servidor de Correo



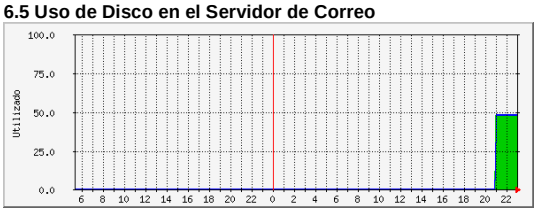
	Max	Average	Current
Usada	3091.9 MB	2996.3 MB	3089.2 MB
Total	4253.9 MB	4133.4 MB	4253.9 MB

6.4 Memoria Libre en el Servidor de Asterisk



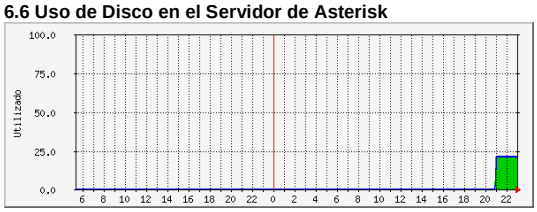
	Max	Average	Current
Libre	300.4 MB	255.2 MB	233.9 MB
Total	762.6 MB	741.0 MB	762.6 MB

6.5 Uso de Disco en el Servidor de Correo



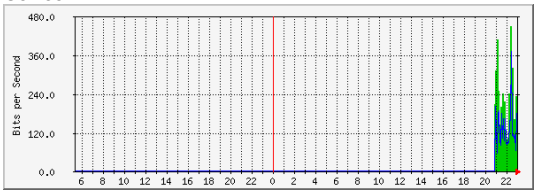
	Max	Average	Current
C:/	48.0 %	47.0 %	48.0 %
Out	48.0 %	47.0 %	48.0 %

6.6 Uso de Disco en el Servidor de Asterisk



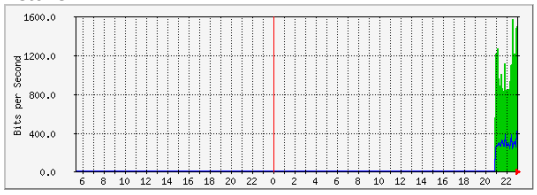
	Max	Average	Current
/	21.0 %	20.0 %	21.0 %
Out	21.0 %	20.0 %	21.0 %

6.7 Analisis de Tráfico para la interfaz del Servidor de Correo



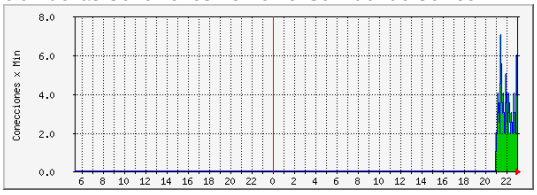
	Max	Average	Current
Entrada	448.0 b/s	192.0 b/s	176.0 b/s
Salida	368.0 b/s	136.0 b/s	152.0 b/s

6.8 Analisis de Tráfico para la interfaz del Servidor de Asterisk



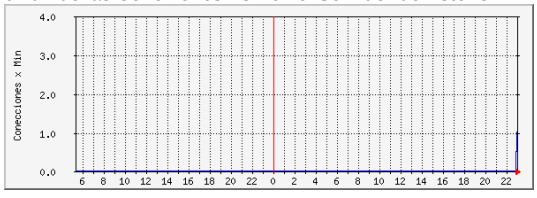
	Max	Average	Current
Entrada	1568.0 b/s	1000.0 b/s	1496.0 b/s
Salida	408.0 b/s	288.0 b/s	416.0 b/s

6.9 Nuevas Conexiones TCP en el Servidor de Correo



	Max	Average	Current
Conexiones Passive Open	7.0 cs/min	3.0 cs/min	3.0 cs/min
Conexiones Active Open	7.0 cs/min	3.0 cs/min	3.0 cs/min

6.10 Nuevas Conexiones TCP en el Servidor de Asterisk



	Max	Average	Current
Conexiones Passive Open	0.0 cs/min	0.0 cs/min	0.0 cs/min
Conexiones Active Open	0.0 cs/min	1.0 cs/min	0.0 cs/min

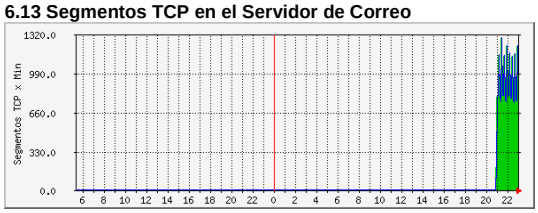
6.11 Conexiones TCP Establecidas en el Servidor de Correo

	Max	Average	Current
Entrantes	113.0 cs	102.0 cs	112.0 cs

6.12 Conexiones TCP Establecidas en el Servidor de Asteris

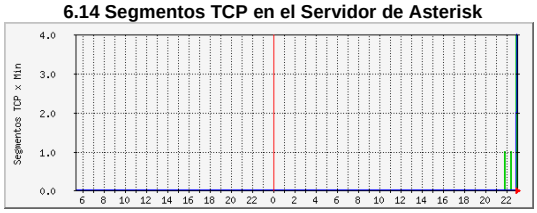
	Max	Average	Current
Entrantes	0.0 cs	0.0 cs	0.0 cs

6.13 Segmentos TCP en el Servidor de Correo



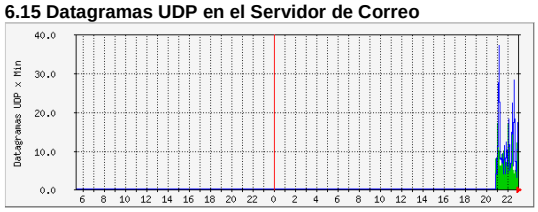
	Max	Average	Current
Enviados	1287.0 segs/min	879.0 segs/min	794.0 segs/min
Recibidos	1287.0 segs/min	880.0 segs/min	794.0 segs/min

6.14 Segmentos TCP en el Servidor de Asterisk



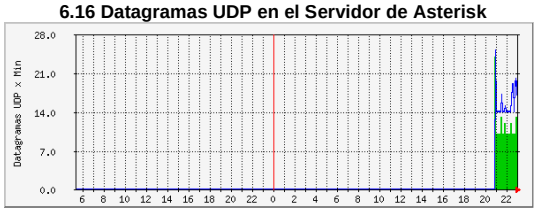
	Max	Average	Current
Enviados	4.0 segs/min	1.0 segs/min	1.0 segs/min
Recibidos	3.0 segs/min	1.0 segs/min	1.0 segs/min

6.15 Datagramas UDP en el Servidor de Correo



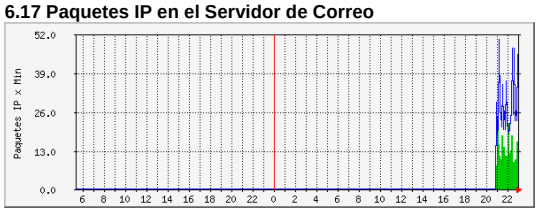
	Max	Average	Current
Enviados	17.0 dts/min	7.0 dts/min	7.0 dts/min
Recibidos	37.0 dts/min	11.0 dts/min	7.0 dts/min

6.16 Datagramas UDP en el Servidor de Asterisk



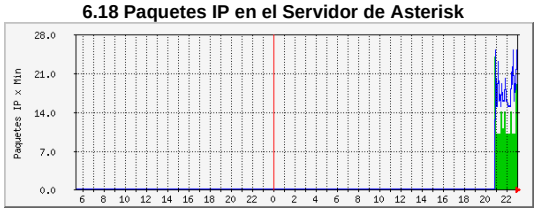
	Max	Average	Current
Enviados	24.0 dts/min	12.0 dts/min	13.0 dts/min
Recibidos	25.0 dts/min	18.0 dts/min	22.0 dts/min

6.17 Paquetes IP en el Servidor de Correo



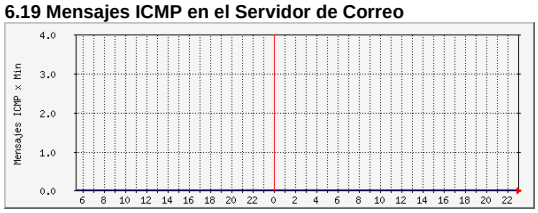
	Max	Average	Current
Paquetes IP Solicitados	22.0 pts/min	12.0 pts/min	12.0 pts/min
Paquetes IP Recibidos	50.0 pts/min	28.0 pts/min	34.0 pts/min

6.18 Paquetes IP en el Servidor de Asterisk



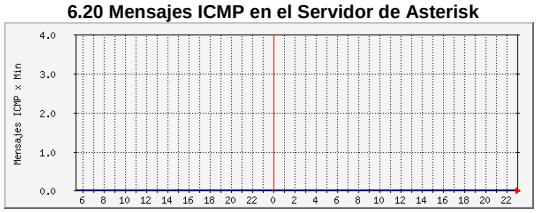
	Max	Average	Current
Paquetes IP Solicitados	24.0 pts/min	12.0 pts/min	15.0 pts/min
Paquetes IP Recibidos	25.0 pts/min	18.0 pts/min	23.0 pts/min

6.19 Mensajes ICMP en el Servidor de Correo



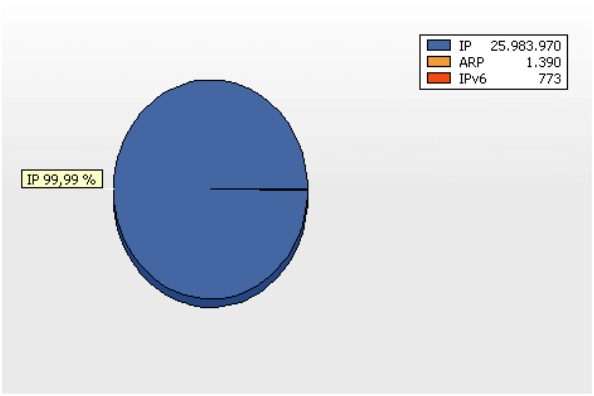
	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

6.20 Mensajes ICMP en el Servidor de Asterisk

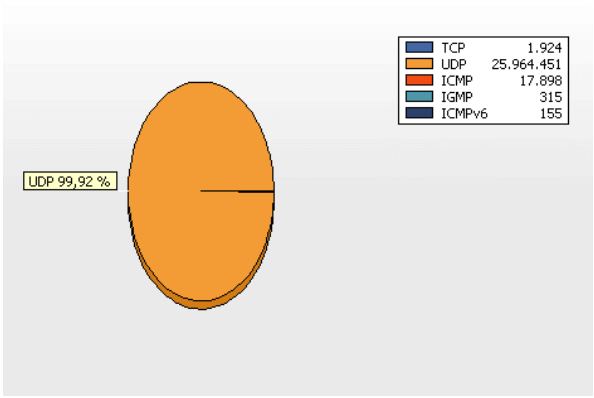


	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

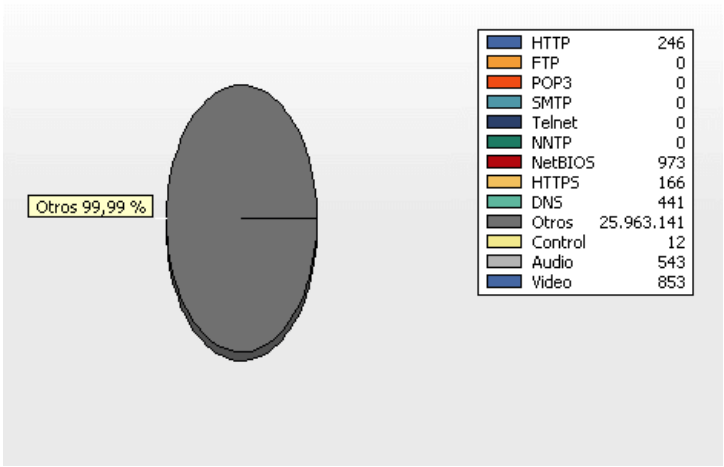
MONITOREO DE LA CÁMARA IP
CommView - Tiempo de Monitoreo: 2 horas



6.21 Paquetes IP



6.22 Paquetes TCP, UDP e ICMP



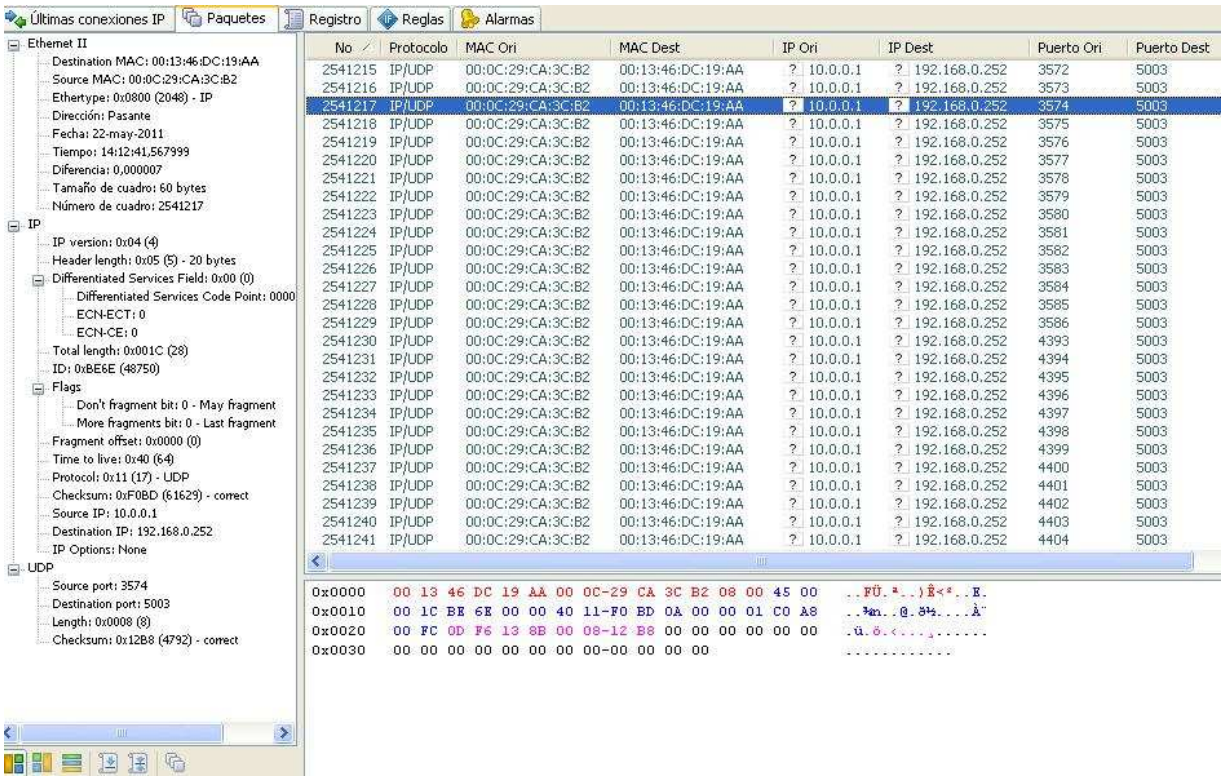
6.23 Protocolos de capa aplicación en la Cámara IP

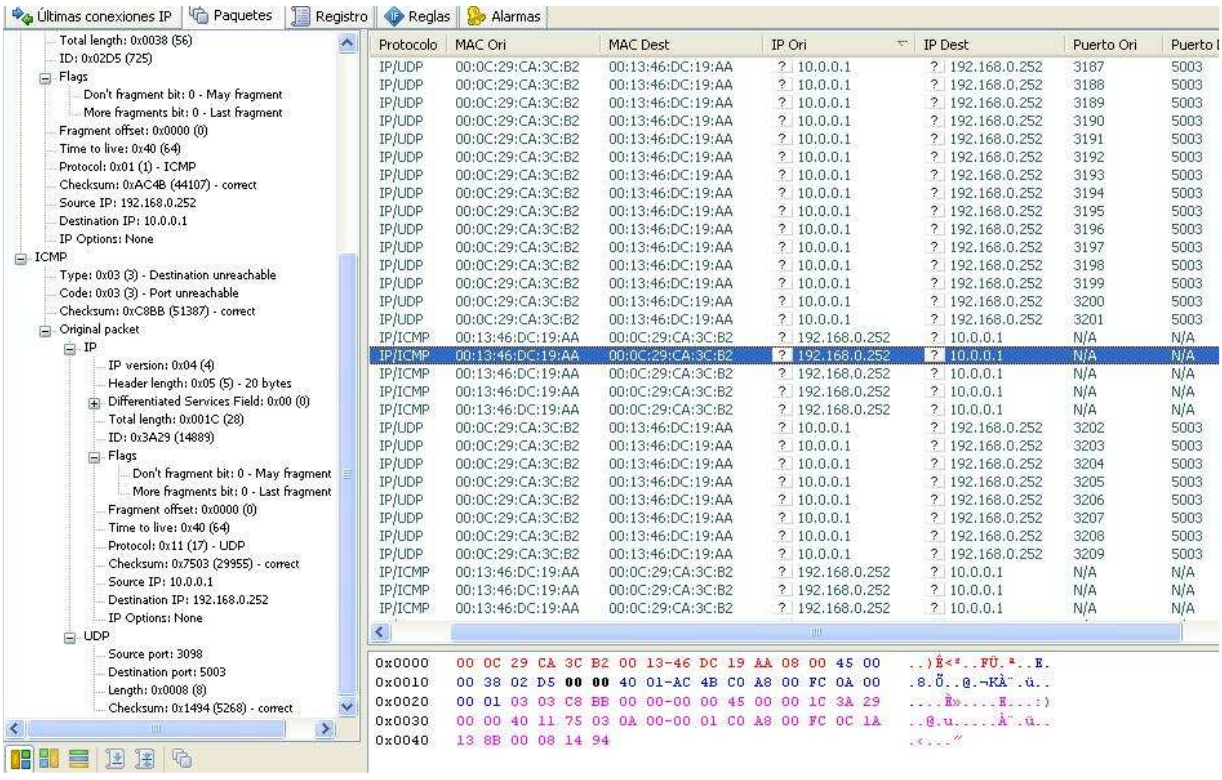
6.24 Resumen General de la Cámara IP

Promedio de paquetes por seg.	40540
Promedio de bytes por seg.	216.775
Total de paquetes	25.990.183
Total bytes	1.560.809.311

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	1.274	1.492	25.983.367
Bytes	946.933	303.647	1.559.315.731
Bytes por seg.	132	42	216.602

6.25 Captura de Paquetes de los Protocolos Involucrados

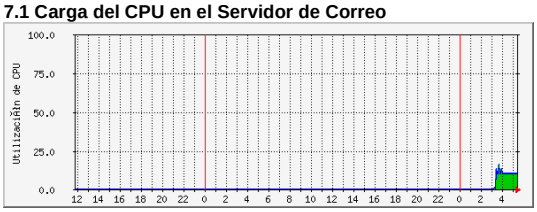




7. ATAQUE ICMP FLOOD CONTRA EL SERVIDOR DE WEB/CORREO

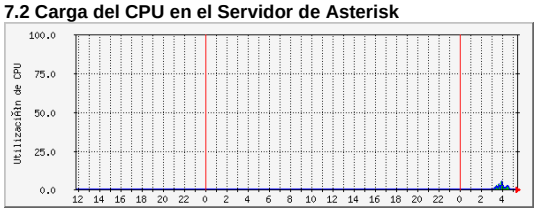
MRTG (Promedio 5 Min) - Tiempo de Monitoreo: 2 horas

7.1 Carga del CPU en el Servidor de Correo



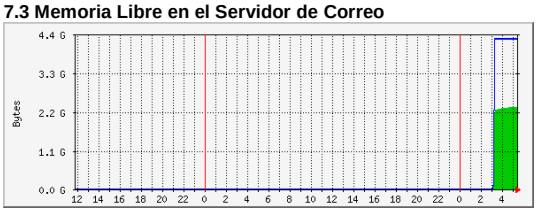
	Max	Average	Current
Usado	16.0 %	9.0 %	10.0 %

7.2 Carga del CPU en el Servidor de Asterisk



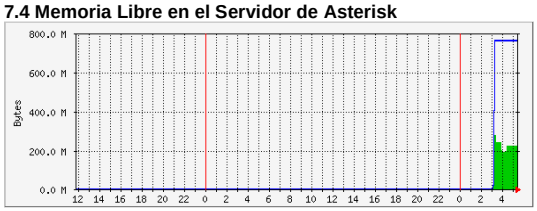
	Max	Average	Current
Usado	5.0 %	1.0 %	1.0 %

7.3 Memoria Libre en el Servidor de Correo



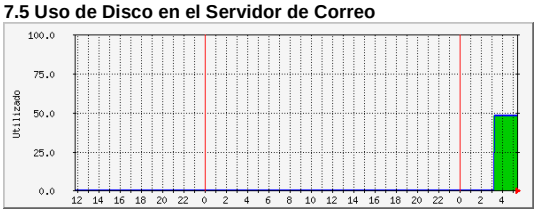
	Max	Average	Current
Usada	2332.0 MB	2213.8 MB	2332.0 MB
Total	4253.9 MB	4109.6 MB	4253.9 MB

7.4 Memoria Libre en el Servidor de Asterisk



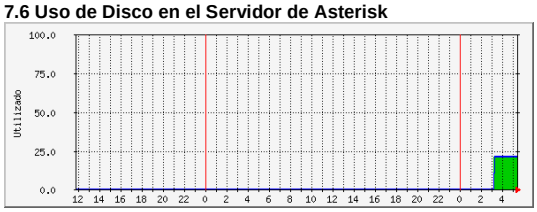
	Max	Average	Current
Libre	275.1 MB	214.0 MB	220.1 MB
Total	762.6 MB	736.7 MB	762.6 MB

7.5 Uso de Disco en el Servidor de Correo



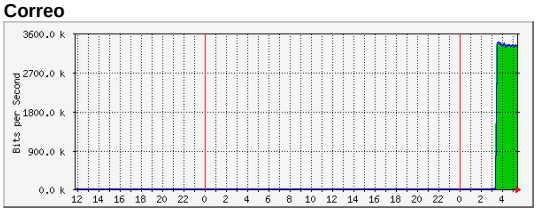
	Max	Average	Current
C:/	48.0 %	48.0 %	48.0 %
Out	48.0 %	48.0 %	48.0 %

7.6 Uso de Disco en el Servidor de Asterisk



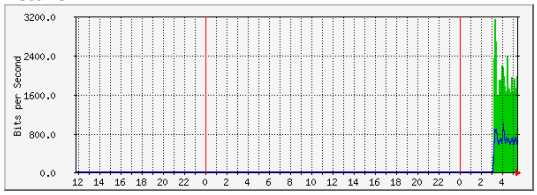
	Max	Average	Current
/	21.0 %	21.0 %	21.0 %
Out	21.0 %	21.0 %	21.0 %

7.7 Analisis de Tráfico para la interfaz del Servidor de Correo



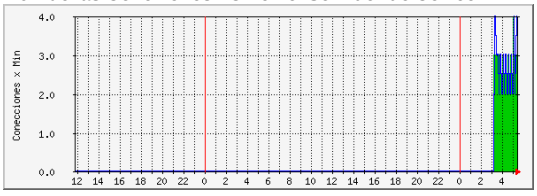
	Max	Average	Current
Entrada	3388.0 kb/s	2901.5 kb/s	3269.0 kb/s
Salida	3387.9 kb/s	2899.0 kb/s	3267.5 kb/s

7.8 Analisis de Tráfico para la interfaz del Servidor de Asterisk



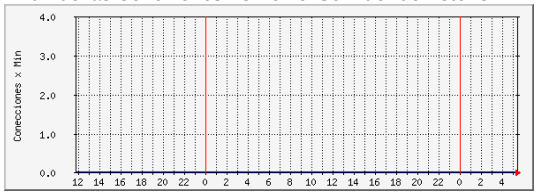
	Max	Average	Current
Entrada	3128.0 b/s	1792.0 b/s	1960.0 b/s
Salida	976.0 b/s	664.0 b/s	680.0 b/s

7.9 Nuevas Conexiones TCP en el Servidor de Correo



	Max	Average	Current
Conexiones Passive Open	4.0 cs/min	3.0 cs/min	2.0 cs/min
Conexiones Active Open	4.0 cs/min	3.0 cs/min	3.0 cs/min

7.10 Nuevas Conexiones TCP en el Servidor de Asterisk



	Max	Average	Current
Conexiones Passive Open	0.0 cs/min	0.0 cs/min	0.0 cs/min
Conexiones Active Open	0.0 cs/min	0.0 cs/min	0.0 cs/min

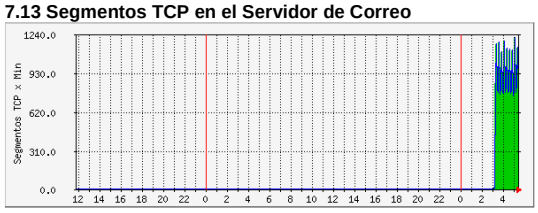
7.11 Conexiones TCP Establecidas en el Servidor de Correo

	Max	Average	Current
Entrantes	132.0 cs	91.0 cs	93.0 cs

7.12 Conexiones TCP Establecidas en el Servidor de Asteris

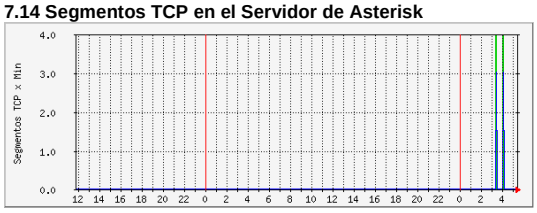
	Max	Average	Current
Entrantes	0.0 cs	0.0 cs	0.0 cs

7.13 Segmentos TCP en el Servidor de Correo



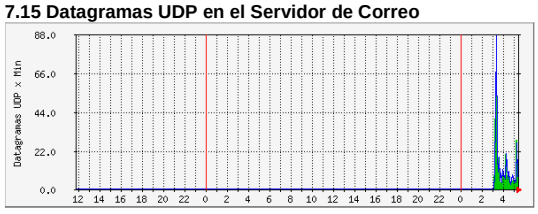
	Max	Average	Current
Enviados	1208.0 segs/min	874.0 segs/min	790.0 segs/min
Recibidos	1211.0 segs/min	875.0 segs/min	790.0 segs/min

7.14 Segmentos TCP en el Servidor de Asterisk



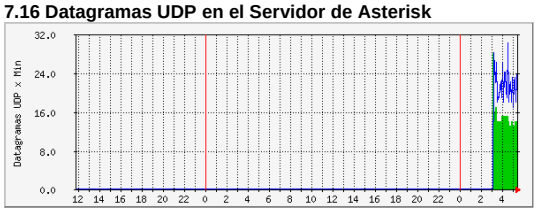
	Max	Average	Current
Enviados	4.0 segs/min	2.0 segs/min	0.0 segs/min
Recibidos	3.0 segs/min	1.0 segs/min	0.0 segs/min

7.15 Datagramas UDP en el Servidor de Correo



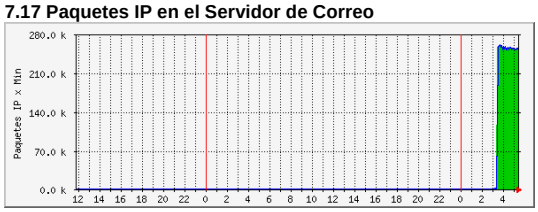
	Max	Average	Current
Enviados	58.0 dts/min	11.0 dts/min	4.0 dts/min
Recibidos	87.0 dts/min	13.0 dts/min	8.0 dts/min

7.16 Datagramas UDP en el Servidor de Asterisk



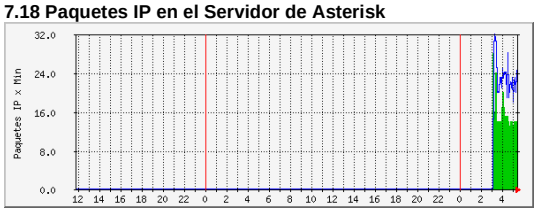
	Max	Average	Current
Enviados	28.0 dts/min	15.0 dts/min	14.0 dts/min
Recibidos	30.0 dts/min	22.0 dts/min	24.0 dts/min

7.17 Paquetes IP en el Servidor de Correo



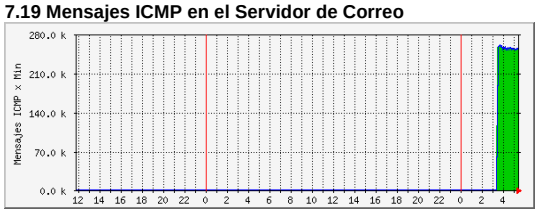
	Max	Average	Current
Paquetes IP Solicitados	259.3 kpts/min	222.0 kpts/min	250.1 kpts/min
Paquetes IP Recibidos	259.3 kpts/min	222.1 kpts/min	250.1 kpts/min

7.18 Paquetes IP en el Servidor de Asterisk



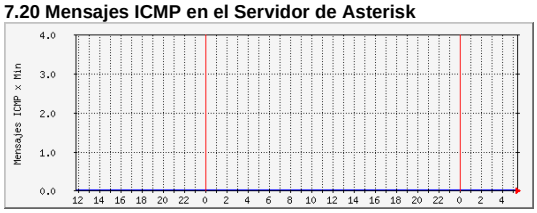
	Max	Average	Current
Paquetes IP Solicitados	28.0 pts/min	15.0 pts/min	14.0 pts/min
Paquetes IP Recibidos	32.0 pts/min	23.0 pts/min	25.0 pts/min

7.19 Mensajes ICMP en el Servidor de Correo



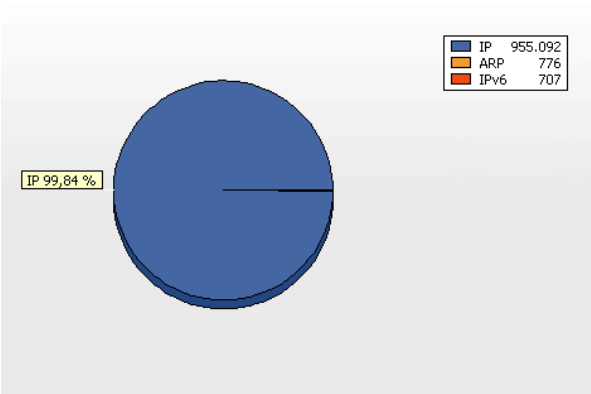
	Max	Average	Current
Enviados	259.3 kmsgs/min	239.1 kmsgs/min	250.0 kmsgs/min
Recibidos	259.3 kmsgs/min	239.1 kmsgs/min	250.0 kmsgs/min

7.20 Mensajes ICMP en el Servidor de Asterisk

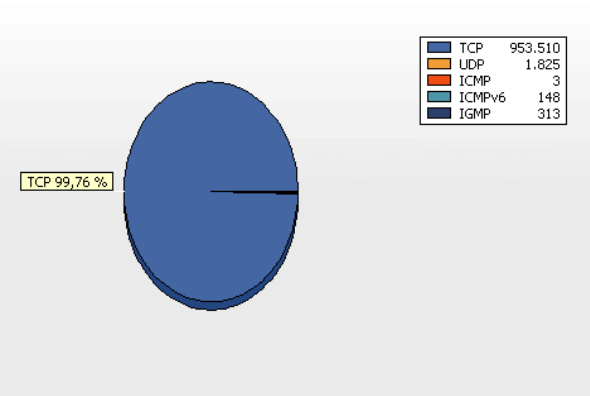


	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

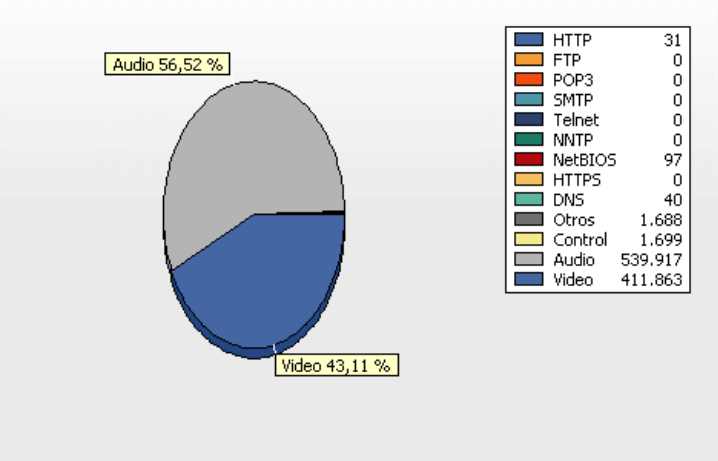
MONITOREO DE LA CÁMARA IP
CommView - Tiempo de Monitoreo: 2 horas



7.21 Paquetes IP



7.22 Paquetes TCP, UDP e ICMP



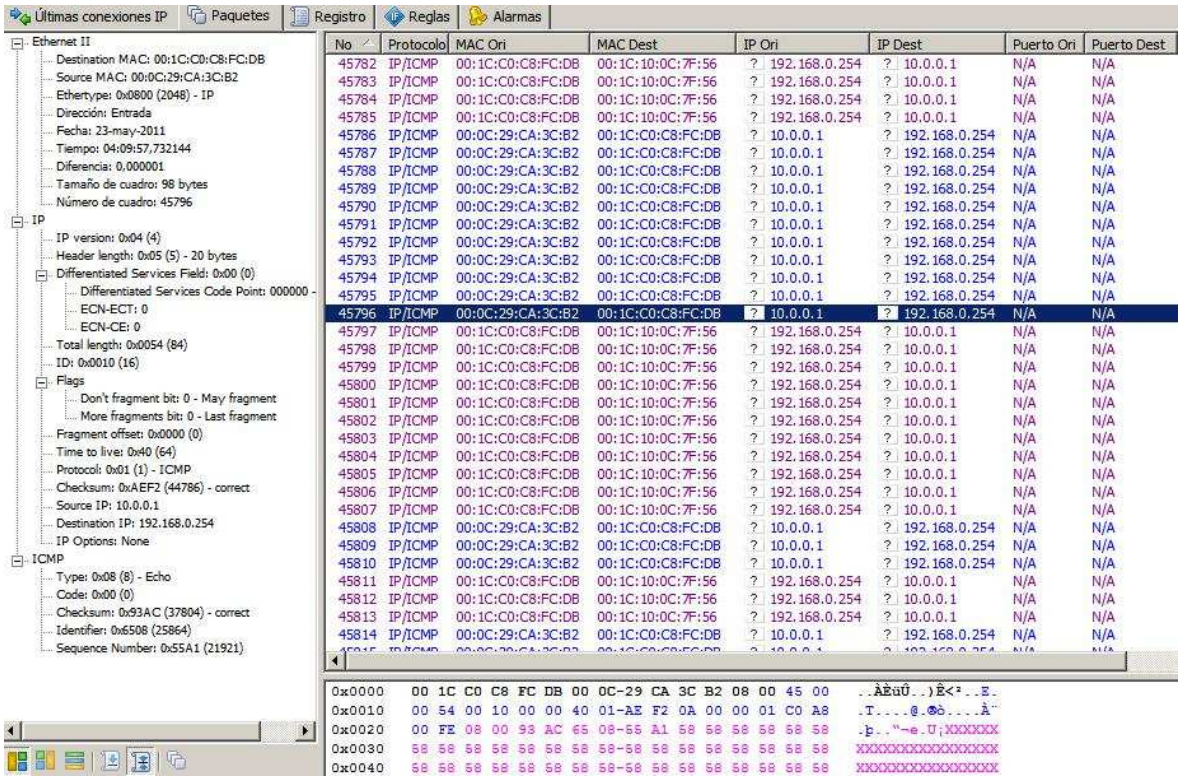
7.23 Protocolos de capa aplicación en la Cámara IP

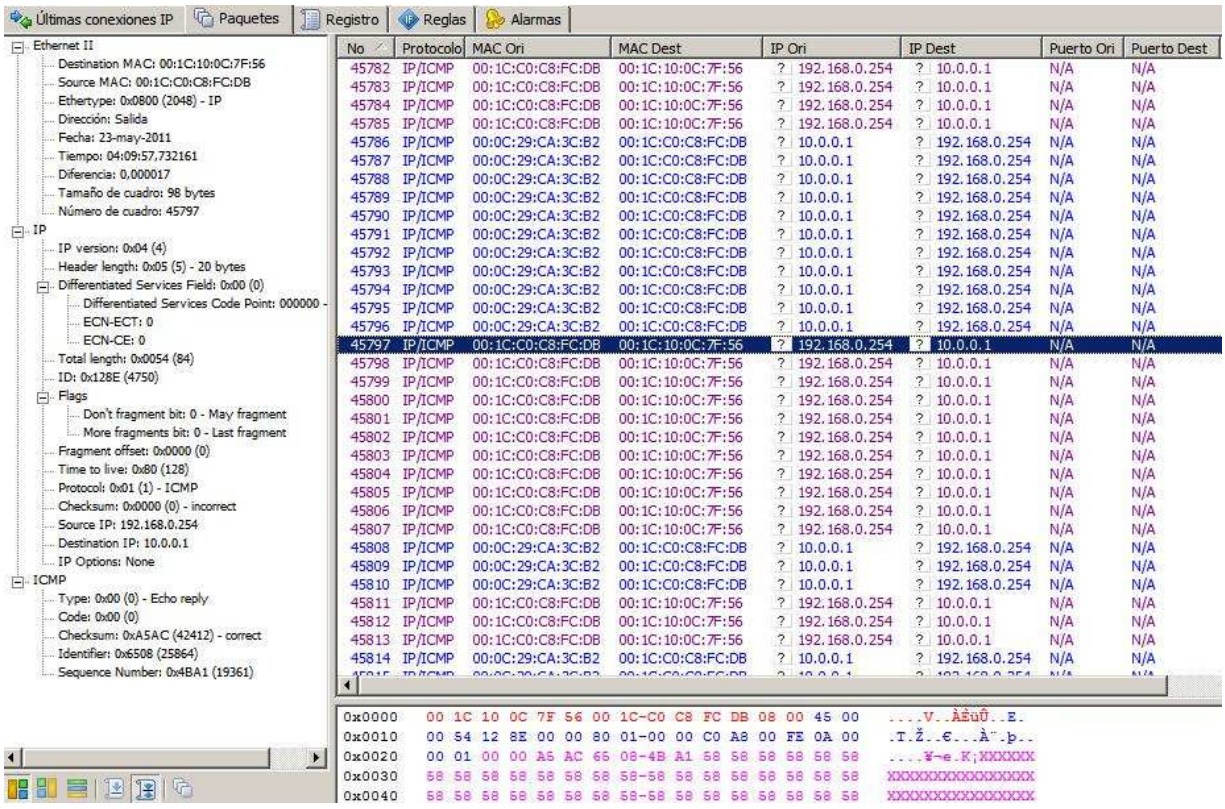
7.24 Resumen General de la Cámara IP

Promedio de paquetes por seg.	133
Promedio de bytes por seg.	39.897
Total de paquetes	956.691
Total bytes	287.231.480

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	635.855	318.830	1.890
Bytes	269.558.022	17.436.287	224.061
Bytes por seg.	37.444	2.422	31

7.25 Captura de Paquetes de los Protocolos Involucrados

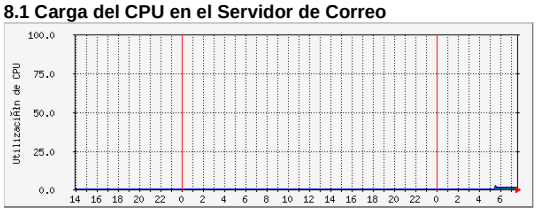




8. ATAQUE ICMP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

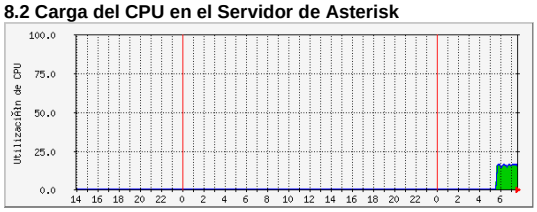
MRTG (Promedio 5 Min) - Tiempo de Monitoreo: 2 horas

8.1 Carga del CPU en el Servidor de Correo



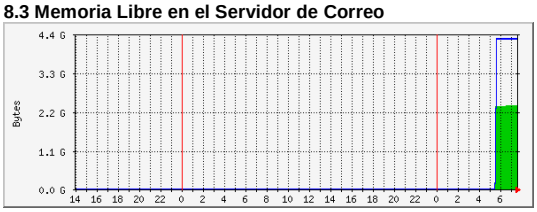
	Max	Average	Current
Usado	2.0 %	1.0 %	1.0 %

8.2 Carga del CPU en el Servidor de Asterisk



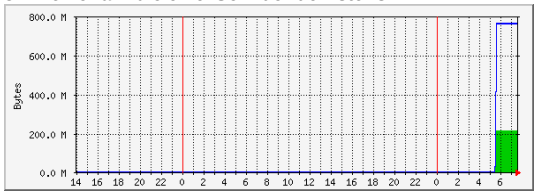
	Max	Average	Current
Usado	16.0 %	14.0 %	14.0 %

8.3 Memoria Libre en el Servidor de Correo



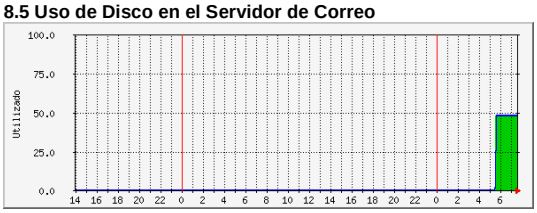
	Max	Average	Current
Usada	2379.9 MB	2278.8 MB	2379.3 MB
Total	4253.9 MB	4102.9 MB	4253.9 MB

8.4 Memoria Libre en el Servidor de Asterisk



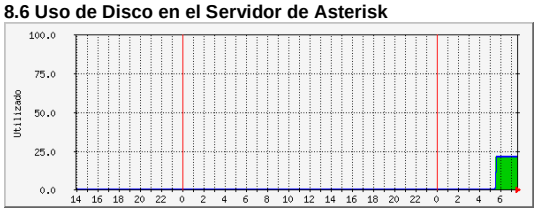
	Max	Average	Current
Libre	212.7 MB	204.3 MB	210.7 MB
Total	762.6 MB	735.5 MB	762.6 MB

8.5 Uso de Disco en el Servidor de Correo



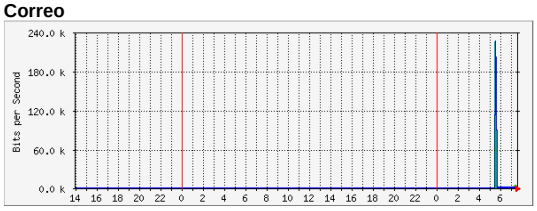
	Max	Average	Current
C:/	48.0 %	48.0 %	48.0 %
Out	48.0 %	48.0 %	48.0 %

8.6 Uso de Disco en el Servidor de Asterisk



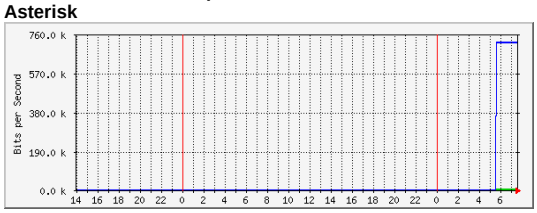
	Max	Average	Current
/	21.0 %	21.0 %	21.0 %
Out	21.0 %	21.0 %	21.0 %

8.7 Analisis de Tráfico para la interfaz del Servidor de Correo



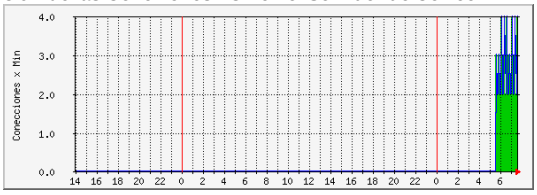
	Max	Average	Current
Entrada	226.3 kb/s	1620 b/s	128.0 b/s
Salida	226.1 kb/s	472 b/s	64.0 b/s

8.8 Analisis de Tráfico para la interfaz del Servidor de Asterisk



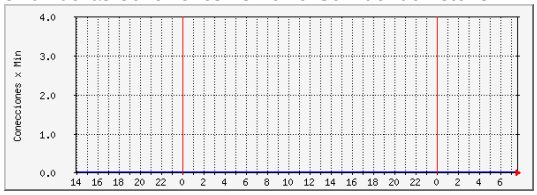
	Max	Average	Current
Entrada	6792.0 b/s	6544.0 b/s	6792.0 b/s
Salida	720.1 kb/s	692.3 kb/s	720.1 kb/s

8.9 Nuevas Conexiones TCP en el Servidor de Correo



	Max	Average	Current
Conexiones Passive Open	4.0 cs/min	2.0 cs/min	4.0 cs/min
Conexiones Active Open	4.0 cs/min	3.0 cs/min	4.0 cs/min

8.10 Nuevas Conexiones TCP en el Servidor de Asterisk



	Max	Average	Current
Conexiones Passive Open	0.0 cs/min	0.0 cs/min	0.0 cs/min
Conexiones Active Open	0.0 cs/min	0.0 cs/min	0.0 cs/min

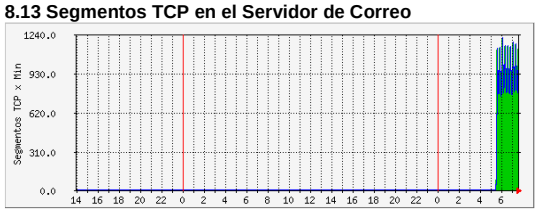
8.11 Conexiones TCP Establecidas en el Servidor de Correo

	Max	Average	Current
Entrantes	100.0 cs	90.0 cs	96.0 cs

8.12 Conexiones TCP Establecidas en el Servidor de Asteris

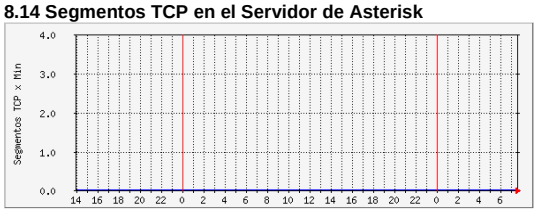
	Max	Average	Current
Entrantes	0.0 cs	0.0 cs	0.0 cs

8.13 Segmentos TCP en el Servidor de Correo



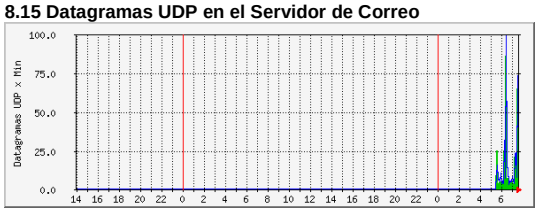
	Max	Average	Current
Enviados	1207.0 segs/min	880.0 segs/min	1122.0 segs/min
Recibidos	1207.0 segs/min	880.0 segs/min	1122.0 segs/min

8.14 Segmentos TCP en el Servidor de Asterisk



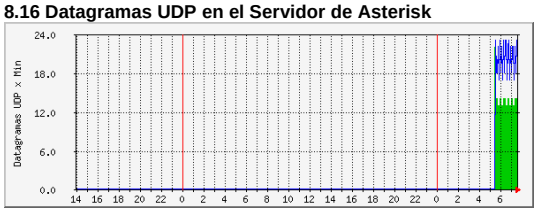
	Max	Average	Current
Enviados	0.0 segs/min	0.0 segs/min	0.0 segs/min
Recibidos	0.0 segs/min	0.0 segs/min	0.0 segs/min

8.15 Datagramas UDP en el Servidor de Correo



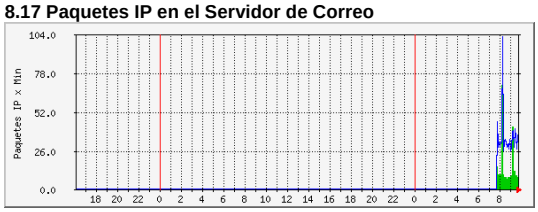
	Max	Average	Current
Enviados	86.0 dts/min	13.0 dts/min	5.0 dts/min
Recibidos	99.0 dts/min	15.0 dts/min	6.0 dts/min

8.16 Datagramas UDP en el Servidor de Asterisk



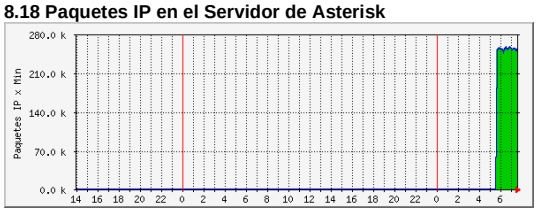
	Max	Average	Current
Enviados	22.0 dts/min	14.0 dts/min	12.0 dts/min
Recibidos	23.0 dts/min	20.0 dts/min	22.0 dts/min

8.17 Paquetes IP en el Servidor de Correo



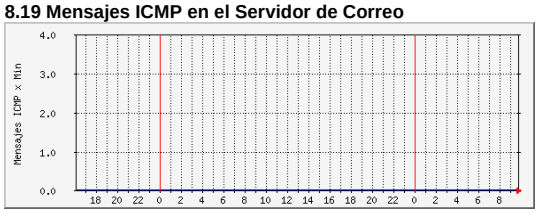
	Max	Average	Current
Paquetes IP Solicitados	70.0 pts/min	12.0 pts/min	8.0 pts/min
Paquetes IP Recibidos	102.0 pts/min	34.0 pts/min	30.0 pts/min

8.18 Paquetes IP en el Servidor de Asterisk



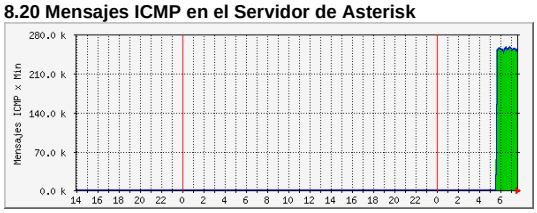
	Max	Average	Current
Paquetes IP Solicitados	257.2 kpts/min	235.4 kpts/min	245.8 kpts/min
Paquetes IP Recibidos	257.2 kpts/min	237.6 kpts/min	245.8 kpts/min

8.19 Mensajes ICMP en el Servidor de Correo



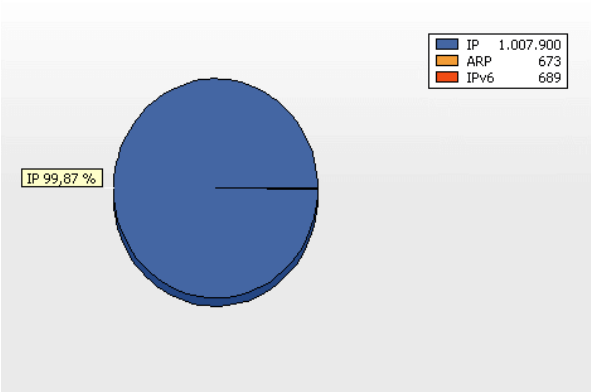
	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

8.20 Mensajes ICMP en el Servidor de Asterisk

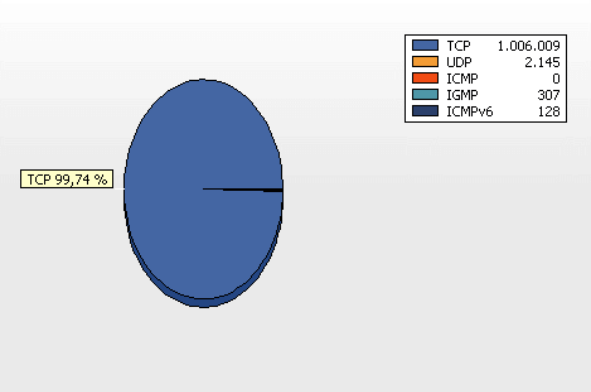


	Max	Average	Current
Enviados	257.2 kmsgs/min	244.8 kmsgs/min	245.8 kmsgs/min
Recibidos	257.2 kmsgs/min	244.8 kmsgs/min	245.8 kmsgs/min

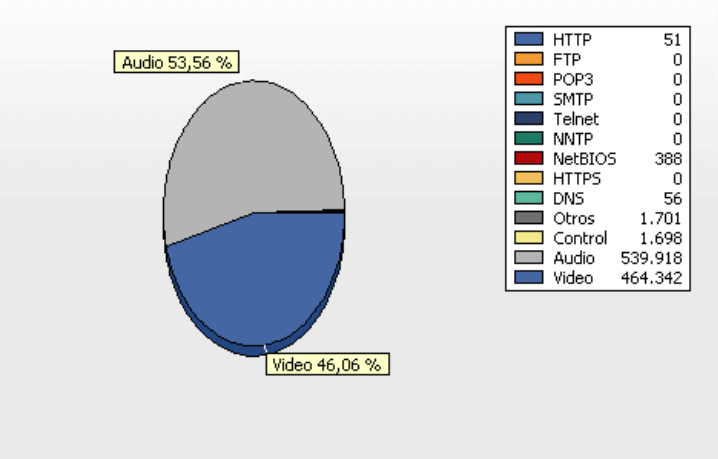
MONITOREO DE LA CÁMARA IP
CommView - Tiempo de Monitoreo: 2 horas



8.21 Paquetes IP



8.22 Paquetes TCP, UDP e ICMP



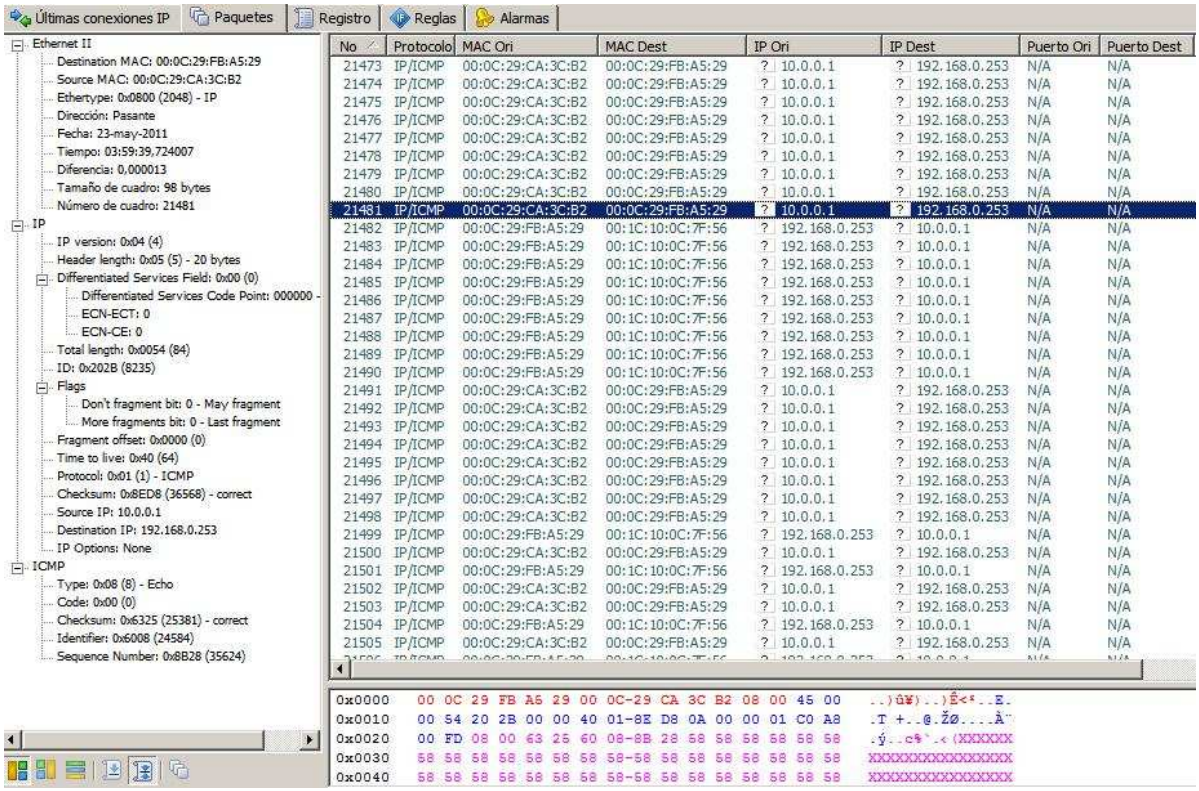
8.23 Protocolos de capa aplicación en la Cámara IP

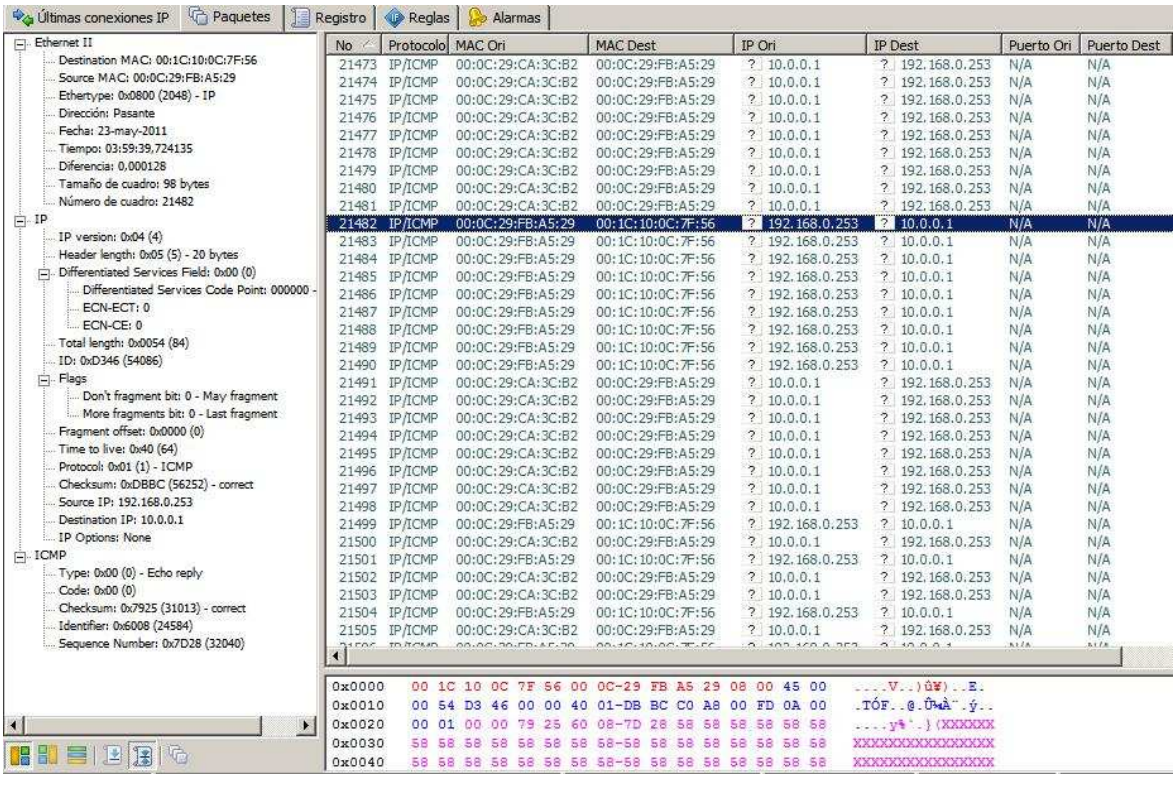
8.24 Resumen General de la Cámara IP

Promedio de paquetes por seg.	140
Promedio de bytes por seg.	58.663
Total de paquetes	1.009.412
Total bytes	422.390.256

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	670.195	337.046	2.021
Bytes	403.661.122	18.423.491	233.774
Bytes por seg.	56.072	2.559	32

8.25 Captura de Paquetes de los Protocolos Involucrados

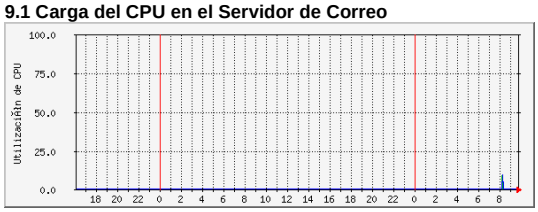




9. ATAQUE ICMP FLOOD CONTRA LA CÁMARA IP

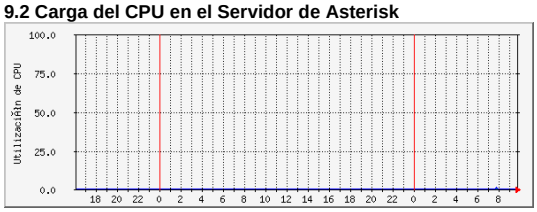
MRTG (Promedio 5 Min) - Tiempo de Monitoreo: 2 horas

9.1 Carga del CPU en el Servidor de Correo



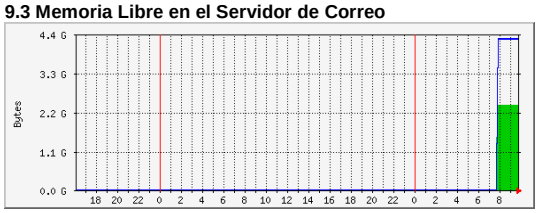
	Max	Average	Current
Usado	9.0 %	3.0 %	0.0 %

9.2 Carga del CPU en el Servidor de Asterisk



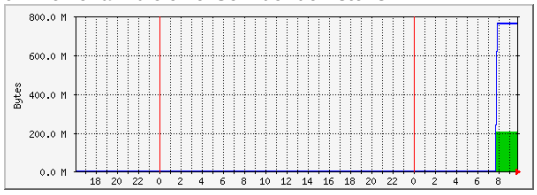
	Max	Average	Current
Usado	1.0 %	1.0 %	0.0 %

9.3 Memoria Libre en el Servidor de Correo



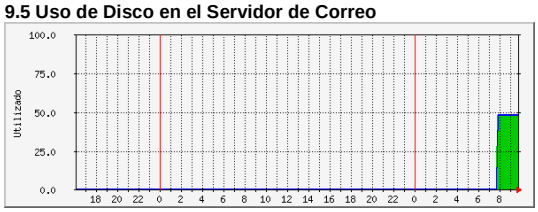
	Max	Average	Current
Usada	2404.2 MB	2362.1 MB	2404.1 MB
Total	4253.9 MB	4189.3 MB	4253.9 MB

9.4 Memoria Libre en el Servidor de Asterisk



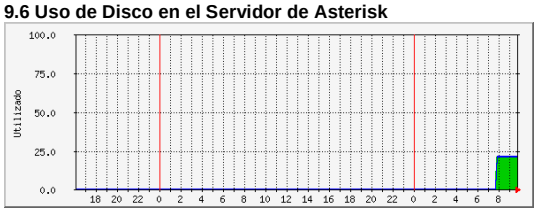
	Max	Average	Current
Libre	205.1 MB	201.3 MB	203.5 MB
Total	762.6 MB	751.0 MB	762.6 MB

9.5 Uso de Disco en el Servidor de Correo



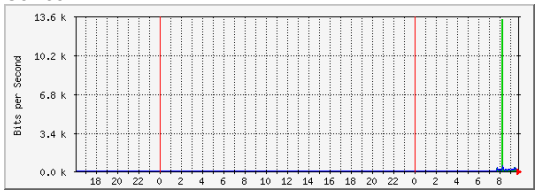
	Max	Average	Current
C:/	48.0 %	48.0 %	48.0 %
Out	48.0 %	48.0 %	48.0 %

9.6 Uso de Disco en el Servidor de Asterisk



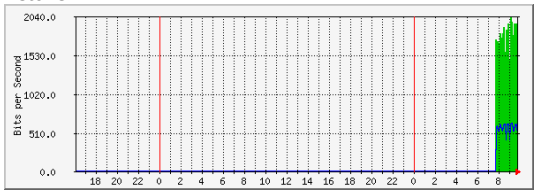
	Max	Average	Current
/	21.0 %	21.0 %	21.0 %
Out	21.0 %	21.0 %	21.0 %

9.7 Analisis de Tráfico para la interfaz del Servidor de Correo



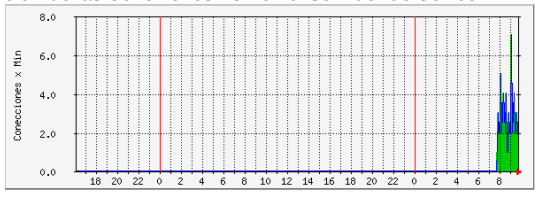
	Max	Average	Current
Entrada	13.3 kb/s	672.0 b/s	136.0 b/s
Salida	416.0 b/s	112.0 b/s	88.0 b/s

9.8 Analisis de Tráfico para la interfaz del Servidor de Asterisk



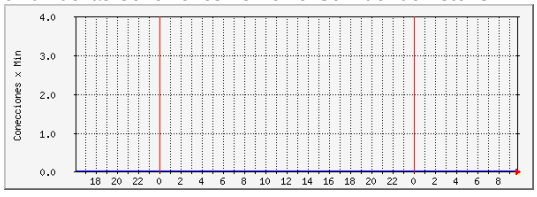
	Max	Average	Current
Entrada	2032.0 b/s	1672.0 b/s	1648.0 b/s
Salida	624.0 b/s	568.0 b/s	448.0 b/s

9.9 Nuevas Conexiones TCP en el Servidor de Correo



	Max	Average	Current
Conexiones Passive Open	7.0 cs/min	3.0 cs/min	2.0 cs/min
Conexiones Active Open	7.0 cs/min	3.0 cs/min	2.0 cs/min

9.10 Nuevas Conexiones TCP en el Servidor de Asterisk



	Max	Average	Current
Conexiones Passive Open	0.0 cs/min	0.0 cs/min	0.0 cs/min
Conexiones Active Open	0.0 cs/min	0.0 cs/min	0.0 cs/min

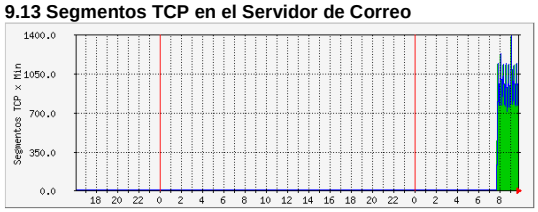
9.11 Conexiones TCP Establecidas en el Servidor de Correo

	Max	Average	Current
Entrantes	109.0 cs	94.0 cs	94.0 cs

9.12 Conexiones TCP Establecidas en el Servidor de Asteris

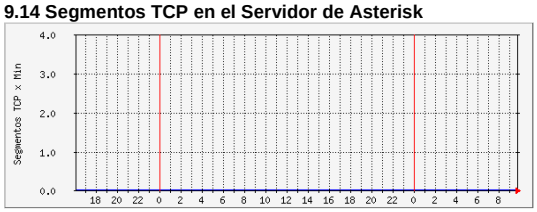
	Max	Average	Current
Entrantes	0.0 cs	0.0 cs	0.0 cs

9.13 Segmentos TCP en el Servidor de Correo



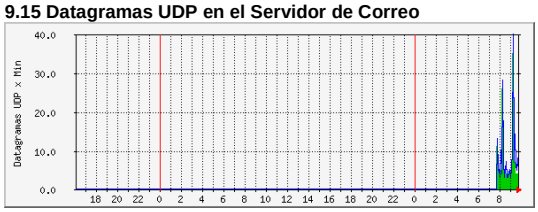
	Max	Average	Current
Enviados	1382.0 segs/min	888.0 segs/min	775.0 segs/min
Recibidos	1383.0 segs/min	890.0 segs/min	776.0 segs/min

9.14 Segmentos TCP en el Servidor de Asterisk



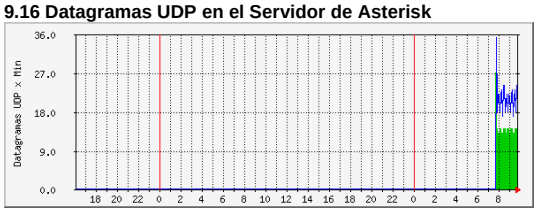
	Max	Average	Current
Enviados	0.0 segs/min	0.0 segs/min	0.0 segs/min
Recibidos	0.0 segs/min	0.0 segs/min	0.0 segs/min

9.15 Datagramas UDP en el Servidor de Correo



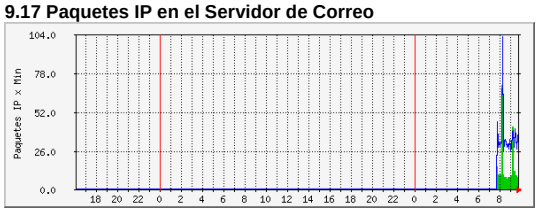
	Max	Average	Current
Enviados	35.0 dts/min	7.0 dts/min	4.0 dts/min
Recibidos	40.0 dts/min	8.0 dts/min	4.0 dts/min

9.16 Datagramas UDP en el Servidor de Asterisk



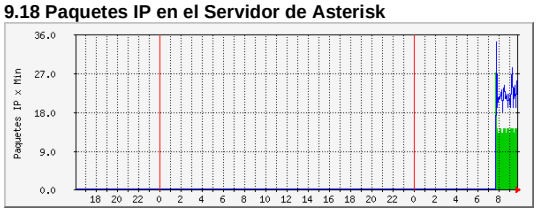
	Max	Average	Current
Enviados	27.0 dts/min	14.0 dts/min	12.0 dts/min
Recibidos	35.0 dts/min	21.0 dts/min	22.0 dts/min

9.17 Paquetes IP en el Servidor de Correo



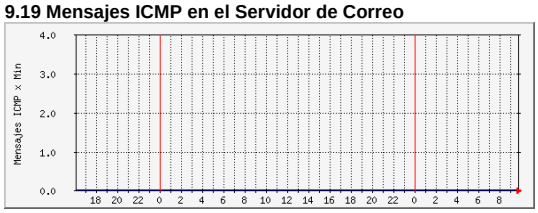
	Max	Average	Current
Paquetes IP Solicitados	70.0 pts/min	12.0 pts/min	8.0 pts/min
Paquetes IP Recibidos	102.0 pts/min	34.0 pts/min	30.0 pts/min

9.18 Paquetes IP en el Servidor de Asterisk



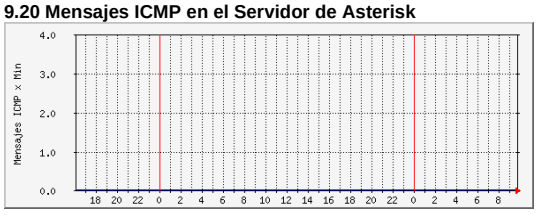
	Max	Average	Current
Paquetes IP Solicitados	27.0 pts/min	14.0 pts/min	12.0 pts/min
Paquetes IP Recibidos	34.0 pts/min	22.0 pts/min	22.0 pts/min

9.19 Mensajes ICMP en el Servidor de Correo



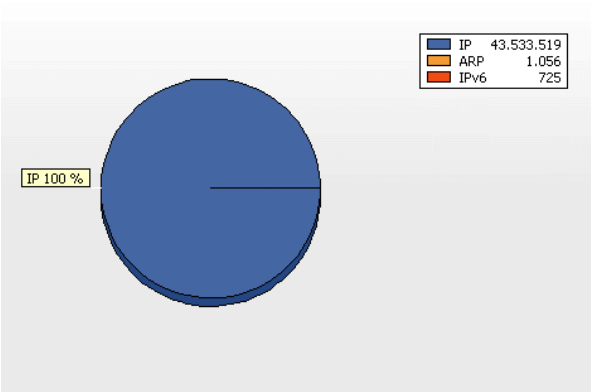
	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

9.20 Mensajes ICMP en el Servidor de Asterisk

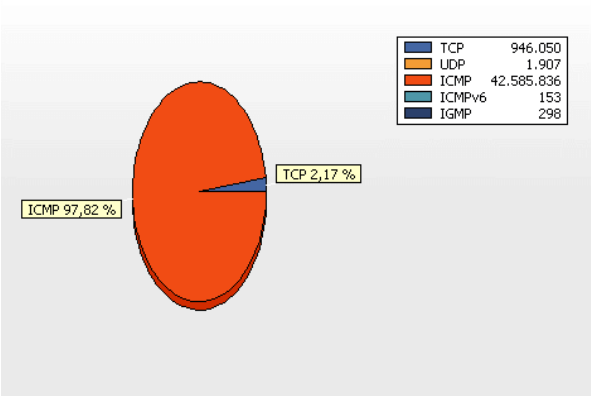


	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

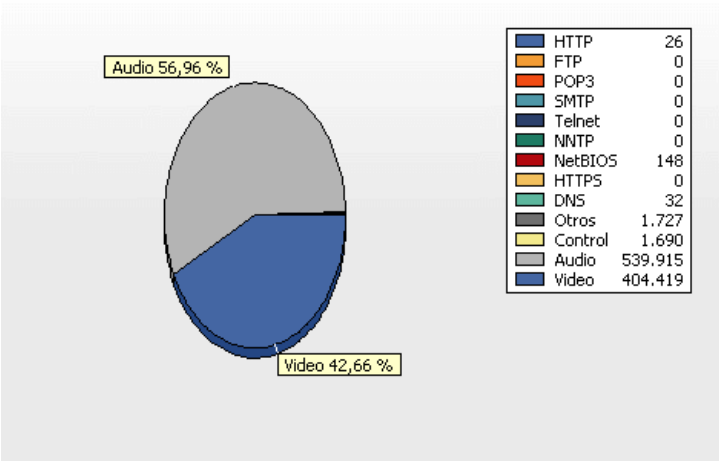
MONITOREO DE LA CÁMARA IP
CommView - Tiempo de Monitoreo: 2 horas



9.21 Paquetes IP



9.22 Paquetes TCP, UDP e ICMP



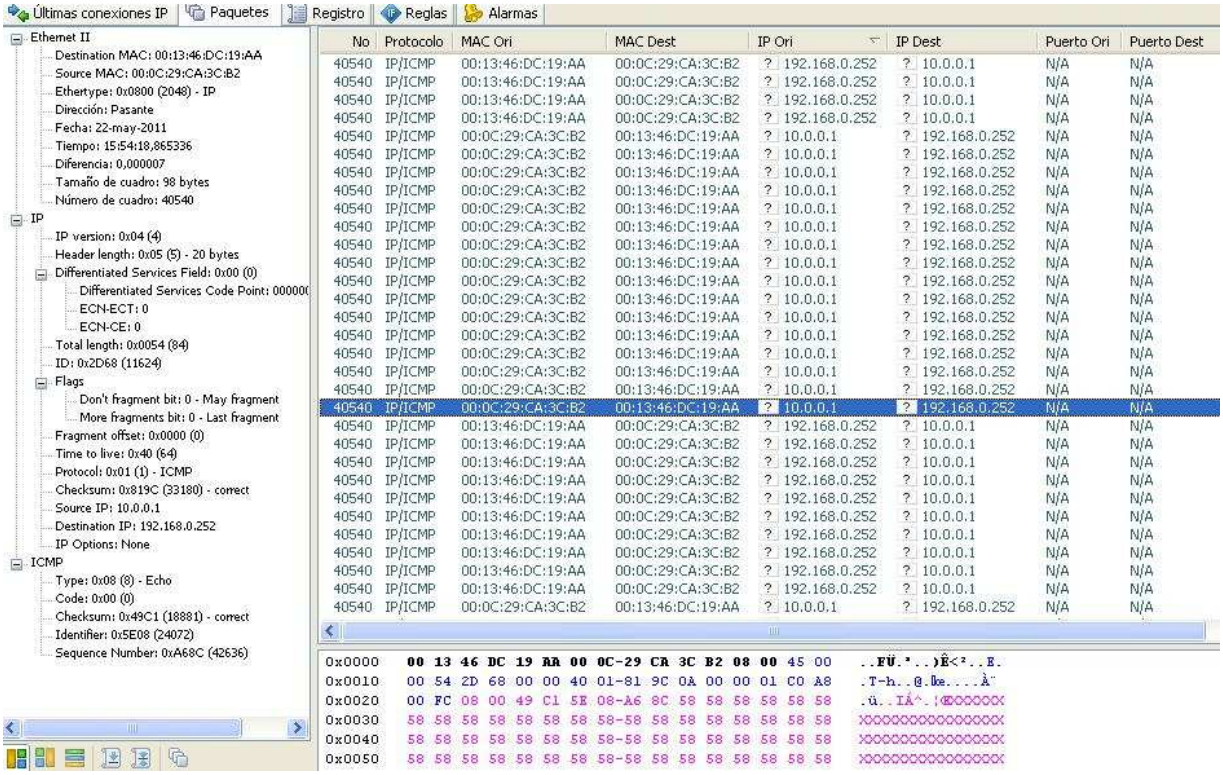
9.23 Protocolos de capa aplicación en la Cámara IP

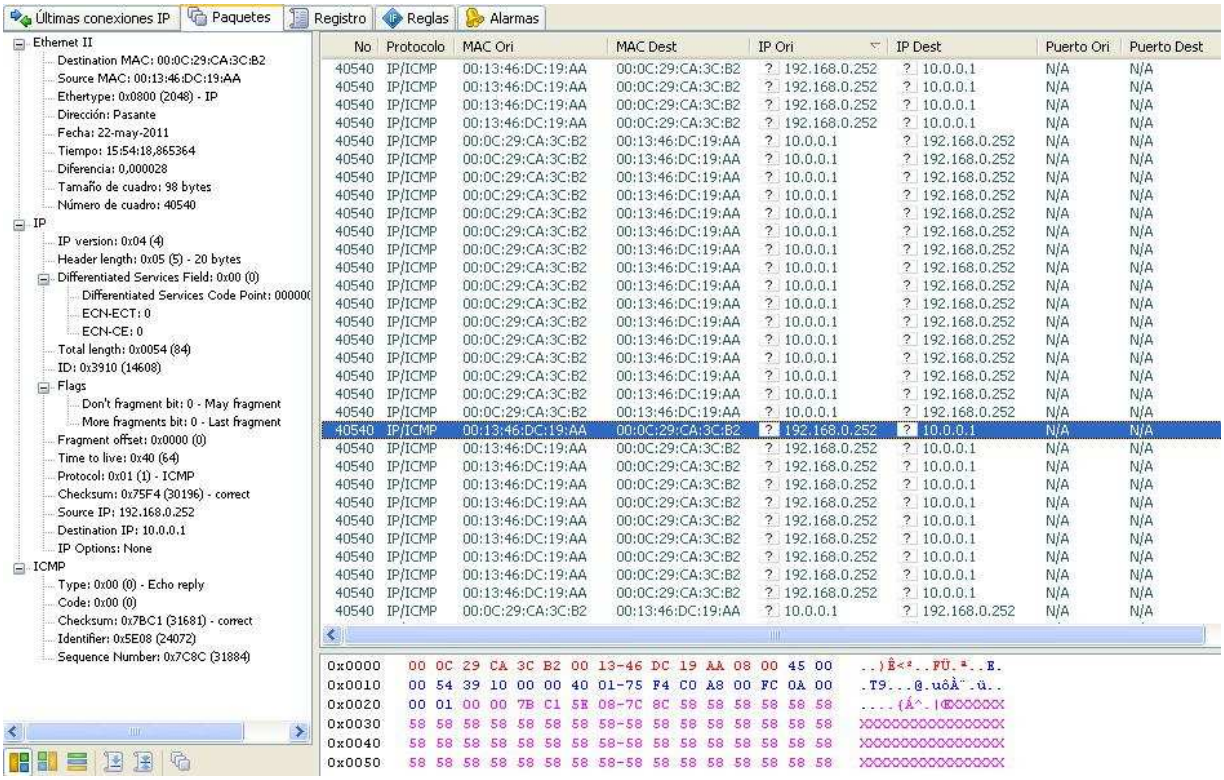
9.24 Resumen General de la Cámara IP

Promedio de paquetes por seg.	6.047
Promedio de bytes por seg.	632.835
Total de paquetes	43.541.598
Total bytes	4.556.435.552

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	629.461	317.774	42.588.065
Bytes	364.740.068	17.381.663	4.173.659.970
Bytes por seg.	50.665	2.414	579.756

9.25 Captura de Paquetes de los Protocolos Involucrados

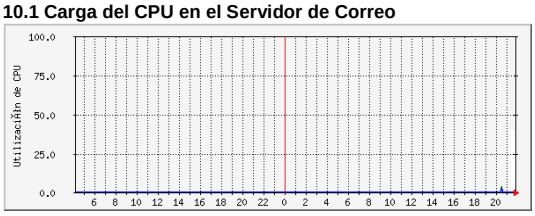




10. ATAQUE INVITE FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

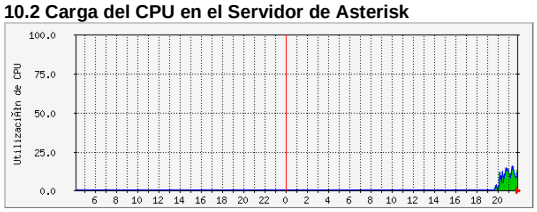
MRTG (Promedio 5 Min) - Tiempo de Monitoreo: 2 horas

10.1 Carga del CPU en el Servidor de Correo



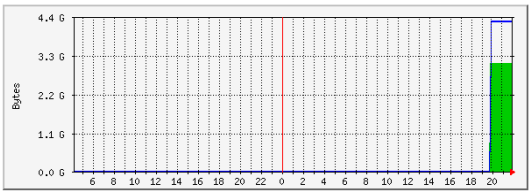
	Max	Average	Current
Usado	3.0 %	1.0 %	0.0 %

10.2 Carga del CPU en el Servidor de Asterisk



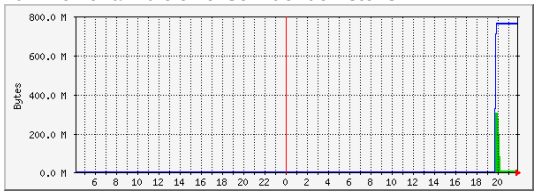
	Max	Average	Current
Usado	15.0 %	9.0 %	13.0 %

10.3 Memoria Libre en el Servidor de Correo



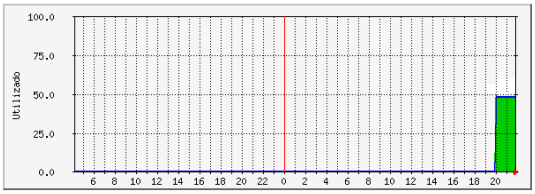
	Max	Average	Current
Usada	3091.9 MB	2896.3 MB	2893.2 MB
Total	4253.9 MB	4133.4 MB	4253.9 MB

10.4 Memoria Libre en el Servidor de Asterisk



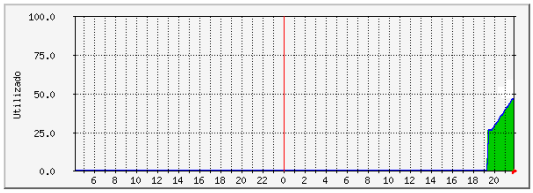
	Max	Average	Current
Libre	305.7 MB	53.7 MB	8402.0 kB
Total	762.6 MB	758.3 MB	762.6 MB

10.5 Uso de Disco en el Servidor de Correo



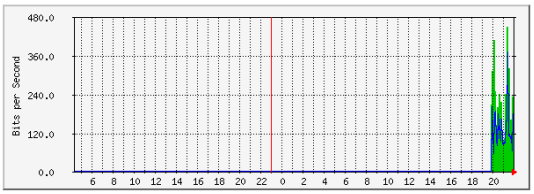
	Max	Average	Current
C:/	48.0 %	47.0 %	48.0 %
Out	48.0 %	47.0 %	48.0 %

10.6 Uso de Disco en el Servidor de Asterisk



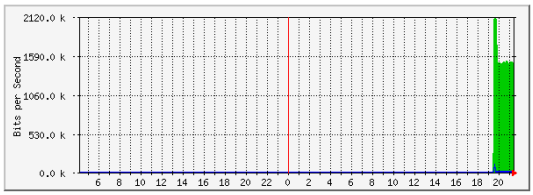
	Max	Average	Current
/	46.0 %	45.0 %	46.0 %
Out	46.0 %	45.0 %	46.0 %

10.7 Analisis de Tráfico para la interfaz del Servidor de Correo



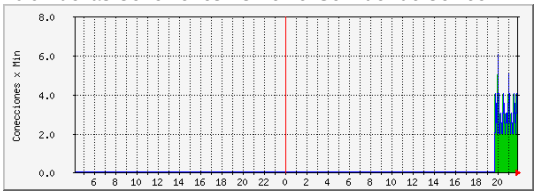
	Max	Average	Current
Entrada	448.0 b/s	192.0 b/s	176.0 b/s
Salida	368.0 b/s	136.0 b/s	152.0 b/s

10.8 Analisis de Tráfico para la interfaz del Servidor de Asterisk



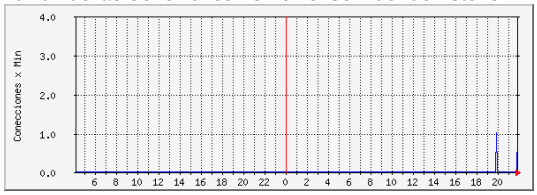
	Max	Average	Current
Entrada	2105.5 kb/s	1528.5 kb/s	1498.4 kb/s
Salida	99.4 kb/s	5360.0 b/s	664.0 b/s

10.9 Nuevas Conexiones TCP en el Servidor de Correo



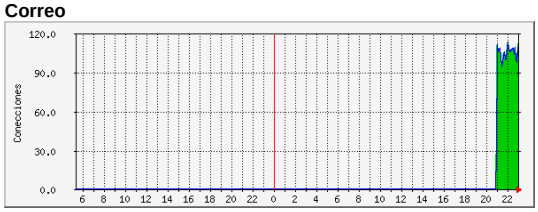
	Max	Average	Current
Conexiones Passive Open	5.0 cs/min	3.0 cs/min	2.0 cs/min
Conexiones Active Open	6.0 cs/min	3.0 cs/min	2.0 cs/min

10.10 Nuevas Conexiones TCP en el Servidor de Asterisk



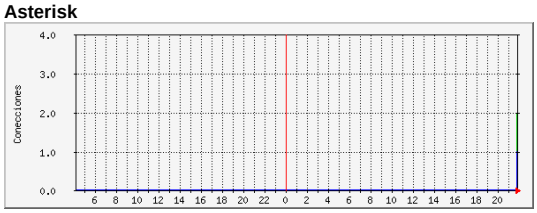
	Max	Average	Current
Conexiones Passive Open	0.0 cs/min	0.0 cs/min	0.0 cs/min
Conexiones Active Open	1.0 cs/min	0.0 cs/min	1.0 cs/min

10.11 Conexiones TCP Establecidas en el Servidor de Correo



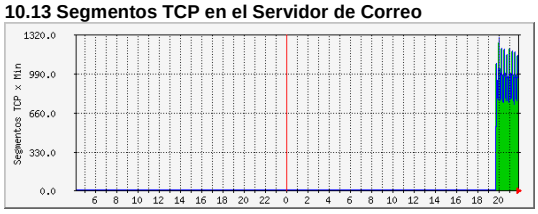
	Max	Average	Current
Entrantes	101.0 cs	95.0 cs	96.0 cs

10.12 Conexiones TCP Establecidas en el Servidor de Asterisk



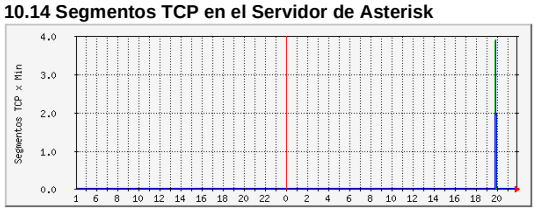
	Max	Average	Current
Entrantes	1.0 cs	2.0 cs	2.0 cs

10.13 Segmentos TCP en el Servidor de Correo



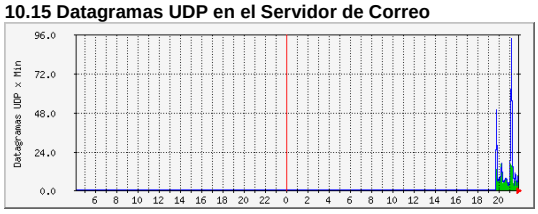
	Max	Average	Current
Enviados	1252.0 segs/min	903.0 segs/min	754.0 segs/min
Recibidos	1286.0 segs/min	905.0 segs/min	755.0 segs/min

10.14 Segmentos TCP en el Servidor de Asterisk



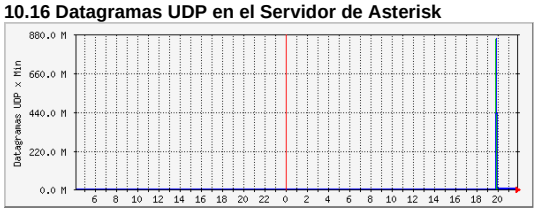
	Max	Average	Current
Enviados	4.0 segs/min	2.0 segs/min	0.0 segs/min
Recibidos	3.0 segs/min	2.0 segs/min	0.0 segs/min

10.15 Datagramas UDP en el Servidor de Correo



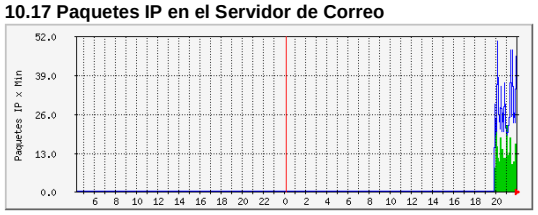
	Max	Average	Current
Enviados	16.0 dts/min	7.0 dts/min	9.0 dts/min
Recibidos	93.0 dts/min	13.0 dts/min	9.0 dts/min

10.16 Datagramas UDP en el Servidor de Asterisk



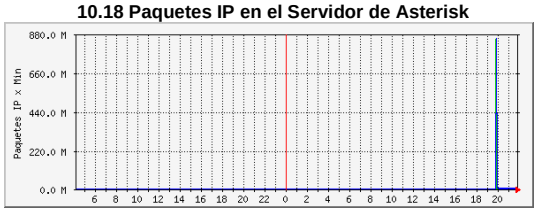
	Max	Average	Current
Enviados	853.3 Mdts/min	33.1 Mdts/min	94.2 kdts/min
Recibidos	853.3 Mdts/min	33.1 Mdts/min	85.4 kdts/min

10.17 Paquetes IP en el Servidor de Correo



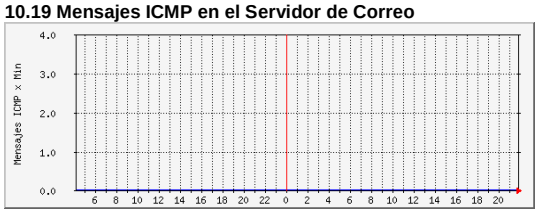
	Max	Average	Current
Paquetes IP Solicitados	22.0 pts/min	12.0 pts/min	12.0 pts/min
Paquetes IP Recibidos	50.0 pts/min	28.0 pts/min	34.0 pts/min

10.18 Paquetes IP en el Servidor de Asterisk



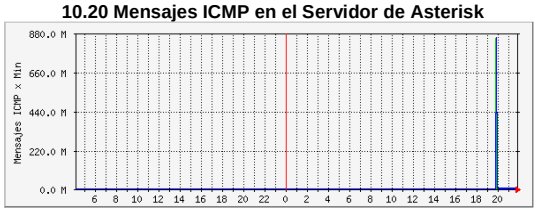
	Max	Average	Current
Paquetes IP Solicitados	853.3 Mpts/min	33.1 Mpts/min	94.3 kpts/min
Paquetes IP Recibidos	853.3 Mpts/min	33.2 Mpts/min	158.3 kpts/min

10.19 Mensajes ICMP en el Servidor de Correo



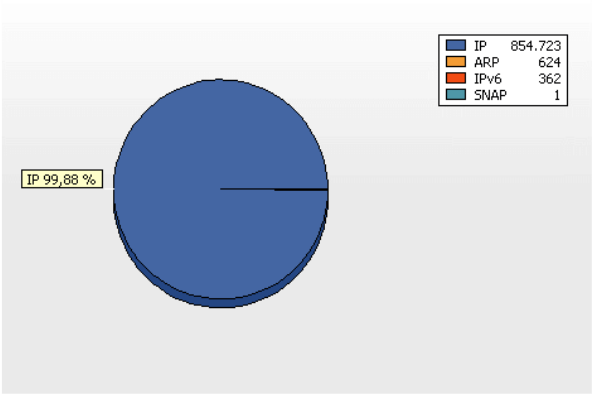
	Max	Average	Current
Enviados	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min
Recibidos	0.0 msgs/min	0.0 msgs/min	0.0 msgs/min

10.20 Mensajes ICMP en el Servidor de Asterisk

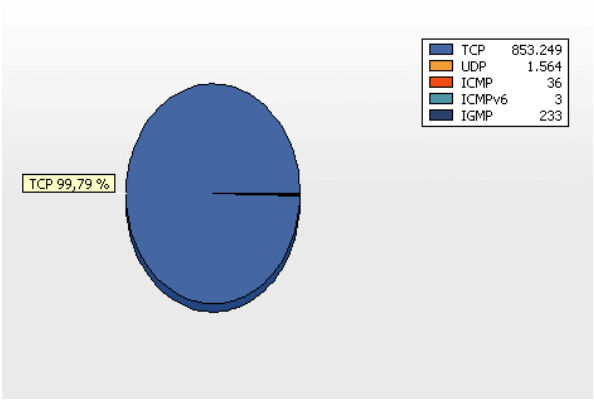


	Max	Average	Current
Enviados	853.3 Mmsgs/min	35.8 Mmsgs/min	0.0 msgs/min
Recibidos	853.3 Mmsgs/min	35.8 Mmsgs/min	48.0 msgs/min

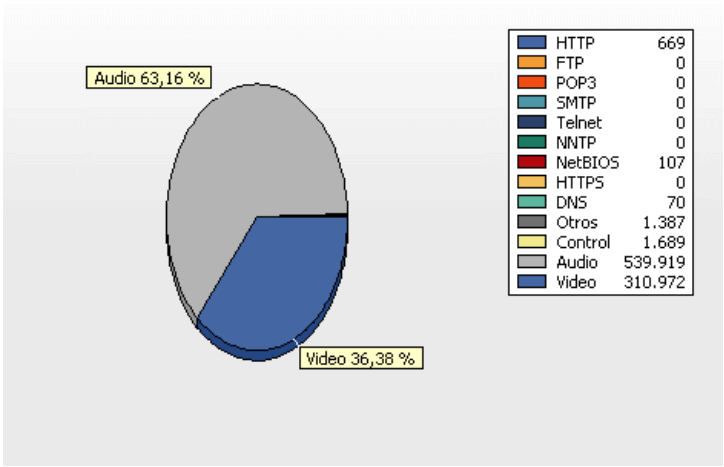
MONITOREO DE LA CÁMARA IP
CommView - Tiempo de Monitoreo: 2 horas



10.21 Paquetes IP



10.22 Paquetes TCP, UDP e ICMP



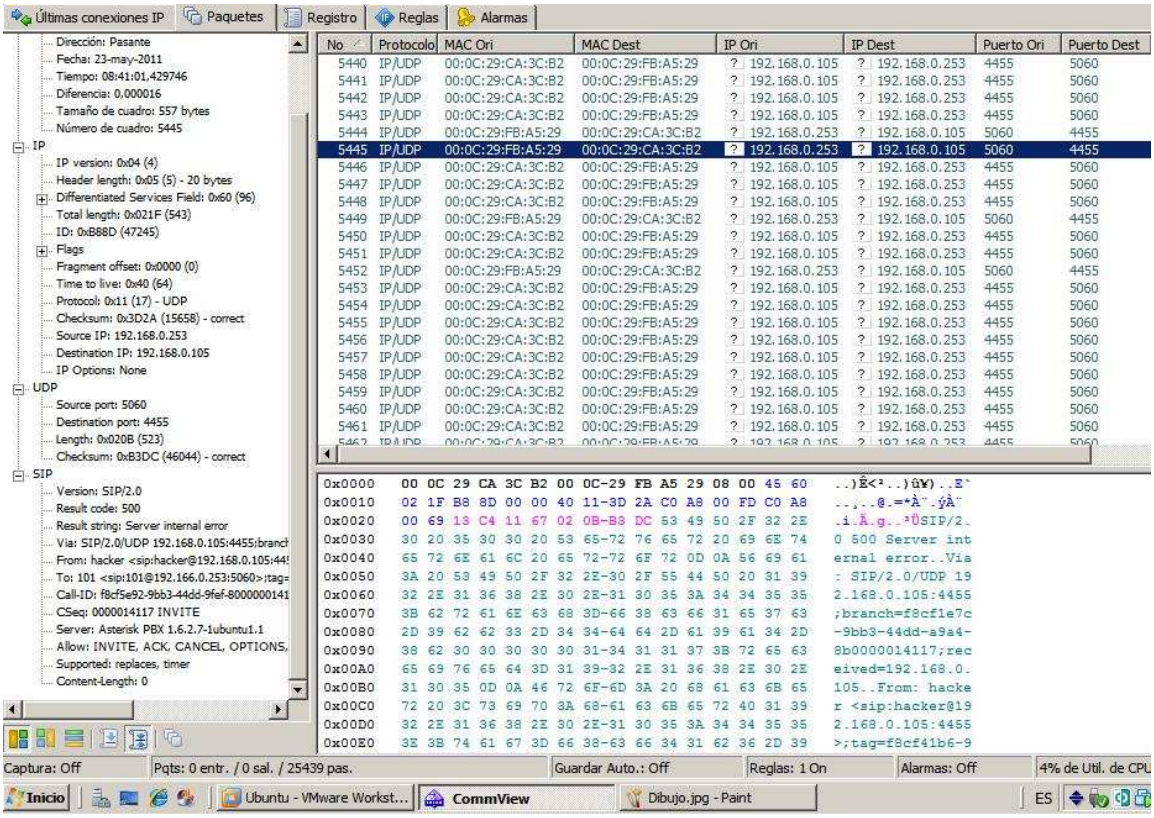
10.23 Protocolos de capa aplicación en la Cámara IP

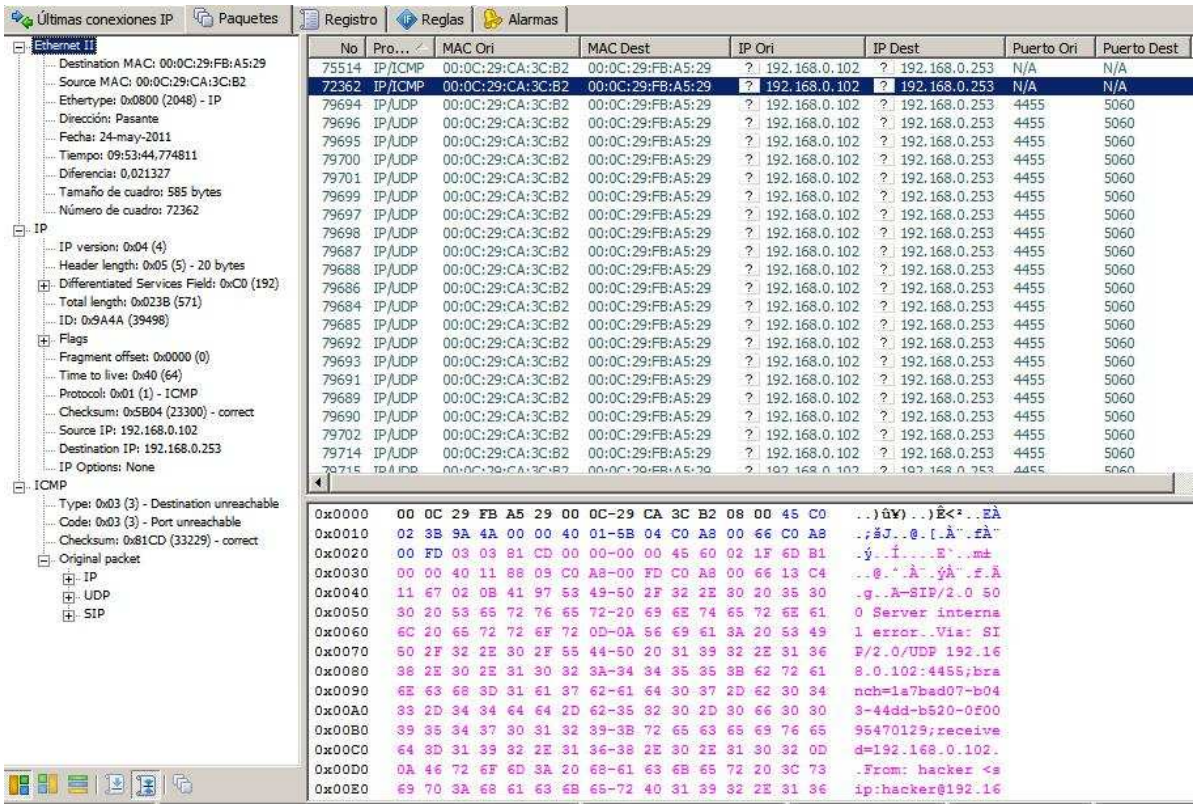
10.24 Resumen General de la Cámara IP

Promedio de paquetes por seg.	119
Promedio de bytes por seg.	27.868
Total de paquetes	855.843
Total bytes	200.678.643

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	568.554	286.053	1.103
Bytes	184.780.067	15.730.991	112.809
Bytes por seg.	25.667	2.185	16

10.25 Captura de Paquetes de los Protocolos Involucrados





ANEXO 7

INFORME

SIMULACIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO

1. OBJETIVO

Comparar y analizar cómo los ataques de Denegación de Servicio por inundación TCP SYN, UDP, ICMP e Invite, afectan a una red de área local convergente propuesta.

2. INTRODUCCIÓN

El presente proyecto propone realizar éste tipo de ataques sobre una red de área local convergente, con servicios de voz, datos y video. Microsoft Exchange 2010 levantado sobre Windows server 2008, asterisk sobre Ubuntu server 10.10, una cámara IP, dos computadoras cliente con sistema operativo Windows y conexión a internet, cuentas de correo electrónico independientes (Acceso a través de Owa ”Outlook Web Access”) y aplicaciones que simulan el tener un teléfono IP, en cada computador.

Una vez implementada dicha red de pruebas, se añadió un tercer computador (atacante), desde el cual se ejecutaron algunos de los ataques de denegación de servicio más comunes como: SYN Flood, UDP Flood, ICMP Flood e Invite Flood, dirigidos a cada uno de los principales servicios de la red de pruebas, con el objeto de visualizar cómo cada ataque afecta al servicio o podría afectar a otros, a través del monitoreo de los mismos.

3. DETALLE DE LAS PRUEBAS REALIZADAS

Las pruebas realizadas fueron desarrolladas en el siguiente orden:

- **Implementación del Escenario de pruebas**

  El haber realizado en primera instancia un escenario de pruebas, basándose en un tipo de simulación parecida a Packet War, donde se involucra un nivel táctico de ataque/defensa, haciendo uso de una red con servidores, clientes, equipos de conmutación, enrutamiento y servicios de voz (Telefonía), datos (Acceso a internet /correo electrónico “Outlook Web Access”) y video (Vigilancia IP), permitió visualizar de forma más clara como un sistema implementado y mayormente usado, se puede comportar ante este tipo de amenazas.

- **Obtención de estados iniciales de los equipos/servicios**

  Como método de comparación, para permitir visualizar posteriormente el comportamiento de los diferentes servicios ante un tipo de ataque en particular, se obtuvieron valores de estados iniciales, como son: Uso de CPU, memoria, espacio en Disco, tráfico de interfaz de red, paquetes enviados y recibidos. El monitoreo fue realizado con MRTG para los servidores, en un lapso de 32 horas y considerando el no acceso a los diferentes servicios, con el objeto de tener un margen mucho más amplio que el del ataque realizado. La cámara IP fue monitoreada con ayuda de la versión demo de CommView.

- **Escaneo de puertos y servicios**

  Se identificaron los puertos abiertos y servicios presentes en cada equipo.
  Lo mencionado permitió conocer los puertos y servicios asociados a ellos, para el posterior ataque, es decir, conocer a que puerto y/o servicio será dirigido el ataque.

- **Identificación de Herramientas para el Ataque**

  Aunque se pueden utilizar un sin número de herramientas y/o aplicaciones para realizar un ataque informático, se opto por usar hping e inviteflood, debido a su simpleza y versatilidad, además de que al ser de licencia GNU (General Public Licence), podría ser utilizada por cualquiera que desee llevar a cabo este tipo de ataques.

- **Ejecución de Ataques**

  Los ataques ejecutados fueron realizados contra aquellos servicios específicos presentes en la red, haciendo uso de las herramientas anteriormente comentadas y generando de forma masiva paquetes SYN TCP, UDP, ICMP e Invite, por un período de tiempo de 2 horas.

- **Análisis y Comparación de Resultados**

  Una vez que se obtuvieron los resultados tanto iniciales como de cada ataque ejecutado. Se exhiben los resultados obtenidos y comparados entre sí, para luego brindar un análisis de las consecuencias que éstos tienen y como podrían afectar a otros servicios.

- **Soluciones y/o Recomendaciones**

  Para finalizar, el informe presenta algunas posibles soluciones y/o recomendaciones, que pueden ayudar a mitigar las consecuencias negativas que se tienen debido a los ataques realizados.

4. EQUIPOS UTILIZADOS

EQUIPO/SERVICIO DIRECCIÓN IP	CARACTERÍSTICAS	SISTEMA OPERATIVO
Conexión Internet **Dir. IP: 190.10.238.237**	2 Mbps/400 Kbps	-
Router Wireless **Dlink DI-624** **192.168.0.1**	1 Puerto WAN 4 Puertos LAN 10/100 Mbps	-
Switch **Nexxt**	8 Puertos LAN 10/100Mbps	-
Cámara IP **Dlink DSC-5300** **Dir. IP: 192.168.0.252**	1 Puerto LAN 10/100 Mbps	-
Host 1 **Dir. IP: 192.168.0.100-199**	Proc. 2.4 GHz 1 GB RAM 320 GB HD Tarjeta de red:10/100Mbos CD/DVD RW	Windows XP Professional
Host 2 **Dir. IP: 192.168.0.100-199**	Proc. 3 GHz Celeron 1 GB RAM 160 GB HD Tarjeta de red:10/100Mbos CD/DVD RW	Windows XP Professional
Teléfonos (1 y 2) **Dir. IP: Misma que Host 1-2**	Software/Aplicación 3CXPhone	-
Servidor de Web/Correo **Dir. IP: 192.168.0.254**	Proc. 2.4 GHz C2D 4 GB RAM 320 GB HD Tarjeta de red:10/100Mbos CD/DVD RW	Windows Server 2008 Enterprise 64-btis
Servidor de Telefonía **Dir. IP: 192.168.0.253**	Proc. 2.4 GHz C2D 768 MB RAM 20 GB HD Tarjeta de red:10/100Mbos	Ubuntu Server 10.10

5. COMPARACIÓN DE RESULTADOS INICIALES CON CADA ATAQUE REALIZADO

En las tablas mostradas a continuación, se presenta un resumen de los resultados obtenidos por cada ataque realizado y su comparación con los resultados antes del mismo, de recursos del sistema y tráfico de red.

4.1 ATAQUE SYN FLOOD CONTRA EL SERVIDOR WEB/CORREO

4.1.1 Detalles del Ataque Realizado

Equipo Atacado	IP Origen del Ataque	IP Falsa del Ataque	Dirección IP Destino	Puerto Atacado	Tamaño de los Datos	Total de Paquetes enviados
Servidor Web/Correo	192.168.0.105	10.0.0.1	192.168.0.254	80	0 bytes	208779562

4.1.2 Comparación de Resultados Iniciales con los del Ataque Ejecutado (MRTG / CommView)

DETALLE DE RECURSOS CONSUMIDOS
ATAQUE SYN FLOOD CONTRA EL SERVIDOR WEB/CORREO

Equipo	Carga del CPU (%)		Memoria Libre (MB)		Uso de Disco (%)	
	Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	4	43	1279,80	1468,4	48	48
Servidor de Telefonía	1	1	201	233.2	21	21

%: Porcentaje Uso de CPU o Disco, MB: Megabytes

TRÁFICO EN LA INTERFAZ DE RED

ATAQUE SYN FLOOD CONTRA EL SERVIDOR WEB/CORREO

Equipo	Tráfico de red (bps)	
	Estado	Estado
	Inicial	Ataque
Servidor Web/Correo	Rx: 6704 Tx: 480	Rx:1792 Tx: 624
Servidor de Telefonía	Rx: 3576 Tx: 360	Rx: 696 Tx: 528
Cámara IP	Rx: 680,79 Kbps Tx: 324,32 Kbps	Rx: 682,04 Kbps Tx: 324,32 Kbps

Tx: Enviados, Rx: Recibidos, bps: bits x Segundo

CONEXIONES TCP

ATAQUE SYN FLOOD CONTRA EL SERVIDOR WEB/CORREO

Equipo	Nuevas (cs/min)		Establecidas (cs)	
	Estado		Estado	
	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	PO: 14 AO: 15	PO: 1578 AO: 3	97	98
Servidor de Telefonía	PO: 0 AO: 0	PO: 0 AO: 0	1	0

PO: Passive Open, AO: Active Open, cs/min: Conexiones x minuto, cs: Conexiones

PROMEDIO DE PAQUETES

ATAQUE SYN FLOOD CONTRA EL SERVIDOR WEB/CORREO

Equipo	TCP (segs/min)		UDP (dts/min)		IP (pts/min)		ICMP (msgs/min)	
	Estado		Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	Tx: 1235 Rx: 1236	Tx: 3146 Rx: 1149,8 ksegs/min	Tx: 74 Rx: 88	Tx: 36 Rx: 34	Tx: 183 Rx: 132	Tx: 1152,7 (kpts/min) Rx:1148,9 (kpts/min)	Tx: 2 Rx: 2	Tx: 2 Rx: 4
Servidor de Telefonía	Tx: 26 Rx:41	Tx: 3 Rx: 4	Tx: 9 Rx:12	Tx: 20 Rx: 28	Tx: 15 Rx: 66	Tx: 20 Rx: 28	Tx: 0 Rx: 0	Tx: 2 Rx: 0
Cámara IP	Tx/Rx: 10,11 ksegs/min	Tx/Rx: 10,04 ksegs/min	Tx/Rx: 14,65	Tx/Rx: 21,25	Tx/Rx: 10,12 kpts/min	Tx/Rx: 10,06 kpts/min :	Tx/Rx: 1	Tx/ Rx: 0

Tx: Enviados, Rx: Recibidos, segs/min: Segmentos x Minuto, dts/min: Datagramas x Minuto, pts/min: Paquetes x Minuto

4.2 ATAQUE SYN FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

4.2.1 Detalles del Ataque Realizado

Equipo Atacado	IP Origen del Ataque	IP Falsa del Ataque	Dirección IP Destino	Puerto Atacado	Tamaño de los Datos	Total de Paquetes enviados
Servidor de Telefonía	192.168.0.105	10.0.0.1	192.168.0.253	5060	0 bytes	209779562

4.2.2 Comparación de Resultados Iniciales con los del Ataque Ejecutado (MRTG / CommView)

DETALLE DE RECURSOS CONSUMIDOS
ATAQUE SYN FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	Carga del CPU (%)		Memoria Libre (MB)		Uso de Disco (%)	
	Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	4	1	1279,80	1344,4	48	48
Servidor de Telefonía	1	1	201	213,90	21	21

%: Porcentaje Uso de CPU o Disco, MB: Megabytes

TRÁFICO EN LA INTERFAZ DE RED
ATAQUE SYN FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	Tráfico de red (bps)	
	Estado	Estado
	Inicial	Ataque
Servidor Web/Correo	Rx: 6704 Tx: 480	Rx: 248 Tx: 168
Servidor de Telefonía	Rx: 3576 Tx: 360	Rx: 3760 Tx: 2256
Cámara IP	Rx: 680,79 Kbps Tx: 324,32 Kbps	Rx: 553,01 Kbps Tx: 21,17 Kbps

Tx: Enviados, Rx: Recibidos, bps: bits x Segundo

CONEXIONES TCP
ATAQUE SYN FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	Nuevas (cs/min)		Establecidas (cs)	
	Estado		Estado	
	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	PO: 14 AO: 15	PO: 3 AO: 3	97	98
Servidor de Telefonía	PO: 0 AO: 0	PO: 1 AO: 0	1	1

PO: Passive Open, AO: Active Open, cs/min: Conexiones x minuto, cs: Conexiones

PROMEDIO DE PAQUETES
ATAQUE SYN FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	TCP (segs/min)		UDP (dts/min)		IP (pts/min)		ICMP (msgs/min)	
	Estado		Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	Tx: 1235 Rx: 1236	Tx: 905 Rx 906:	Tx: 74 Rx: 88	Tx: 11 Rx: 13	Tx: 183 Rx: 132	Tx: 12 Rx: 28	Tx: 2 Rx: 2	Tx: 0 Rx: 0
Servidor de Telefonía	Tx: 26 Rx:41	Tx: 283,3 ksegs/min Rx: 282,3 ksegs/min	Tx: 9 Rx:12	Tx: 10 Rx: 14	Tx: 15 Rx: 66	Tx: 283,4 (kpts/min) Rx: 282,4 (kpts/min)	Tx: 0 Rx: 0	Tx: 0 Rx: 0
Cámara IP	Tx/Rx: 10,11 ksegs/min	Tx/Rx: 7,8 ksegs/min	Tx/Rx: 14,65	Tx/Rx: 163,40	Tx/Rx: 10,12 kpts/min	Tx/Rx: 7,96 kpts/min :	Tx/Rx: 1	Tx/ Rx: 0

Tx: Enviados, Rx: Recibidos, segs/min: Segmentos x Minuto, dts/min: Datagramas x Minuto, pts/min: Paquetes x Minuto

4.3 ATAQUE SYN FLOOD CONTRA LA CÁMARA IP

4.3.1 Detalles del Ataque Realizado

Equipo Atacado	IP Origen del Ataque	IP Falsa del Ataque	Dirección IP Destino	Puerto Atacado	Tamaño de los Datos	Total de Paquetes enviados
Cámara IP	192.168.0.105	10.0.0.1	192.168.0.252	80	0 bytes	208857227

4.3.2 Comparación de Resultados Iniciales con los del Ataque Ejecutado (MRTG / CommView)

DETALLE DE RECURSOS CONSUMIDOS
ATAQUE SYN FLOOD CONTRA LA CÁMARA IP

Equipo	Carga del CPU (%)		Memoria Libre (MB)		Uso de Disco (%)	
	Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	4	1	1279,80	1326,90	48	48
Servidor de Telefonía	1	1	201	245,1	21	21

%: Porcentaje Uso de CPU o Disco, MB: Megabytes

TRÁFICO EN LA INTERFAZ DE RED
ATAQUE SYN FLOOD CONTRA LA CÁMARA IP

Equipo	Tráfico de red (bps)	
	Estado	Estado
	Inicial	Ataque
Servidor Web/Correo	Rx: 6704 Tx: 480	Rx: 200 Tx: 168
Servidor de Telefonía	Rx: 3576 Tx: 360	Rx: 1128 Tx: 384
Cámara IP	Rx: 680,79 Kbps Tx: 324,32 Kbps	Rx: 104 bps Tx: 176 bps

Tx: Enviados, Rx: Recibidos, bps: bits x Segundo

CONEXIONES TCP
ATAQUE SYN FLOOD CONTRA LA CÁMARA IP

Equipo	Nuevas (cs/min)		Establecidas (cs)	
	Estado		Estado	
	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	PO: 14 AO: 15	PO: 3 AO: 3	97	105
Servidor de Telefonía	PO: 0 AO: 0	PO: 0 AO: 0	1	0

PO: Passive Open, AO: Active Open, cs/min: Conexiones x minuto, cs: Conexiones

PROMEDIO DE PAQUETES
ATAQUE SYN FLOOD CONTRA LA CÁMARA IP

Equipo	TCP (segs/min)		UDP (dts/min)		IP (pts/min)		ICMP (msgs/min)	
	Estado		Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	Tx: 1235 Rx: 1236	Tx: 893 Rx: 894	Tx: 74 Rx: 88	Tx:9 Rx: 13	Tx: 183 Rx: 132	Tx: 14 Rx: 35	Tx: 2 Rx: 2	Tx: 0 Rx: 1
Servidor de Telefonía	Tx: 26 Rx:41	Tx:0 Rx: 0	Tx: 9 Rx:12	Tx: 12 Rx: 17	Tx: 15 Rx: 66	Tx: 13 Rx: 19	Tx: 0 Rx: 0	Tx: 0 Rx: 0
Cámara IP	Tx/Rx: 10,11 ksegs/min	Tx/Rx: 290,87 ksegs/min	Tx/Rx: 14,65	Tx/Rx: 11,84	Tx/Rx: 10,12 kpts/min	Tx/Rx: 290,88 kpts/min :	Tx/Rx: 1	Tx/ Rx: 0

Tx: Enviados, Rx: Recibidos, segs/min: Segmentos x Minuto, dts/min: Datagramas x Minuto, pts/min: Paquetes x Minuto

4.4 ATAQUE UDP FLOOD CONTRA EL SERVIDOR WEB/CORREO

4.4.1 Detalles del Ataque Realizado

Equipo Atacado	IP Origen del Ataque	IP Falsa del Ataque	Dirección IP Destino	Puerto Atacado	Tamaño de los Datos	Total de Paquetes enviados
Servidor Web/Correo	192.168.0.105	10.0.0.1	192.168.0.254	80	0 bytes	156529398

4.4.2 Comparación de Resultados Iniciales con los del Ataque Ejecutado (MRTG / CommView)

DETALLE DE RECURSOS CONSUMIDOS
ATAQUE UDP FLOOD CONTRA EL SERVIDOR WEB/CORREO

Equipo	Carga del CPU (%)		Memoria Libre (MB)		Uso de Disco (%)	
	Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	4	4	1279,80	1300,9	48	48
Servidor de Telefonía	1	1	201	215,6	21	21

%: Porcentaje Uso de CPU o Disco, MB: Megabytes

TRÁFICO EN LA INTERFAZ DE RED
ATAQUE UDP FLOOD CONTRA EL SERVIDOR WEB/CORREO

Equipo	Tráfico de red (bps)	
	Estado	Estado
	Inicial	Ataque
Servidor Web/Correo	Rx: 6704 Tx: 480	Rx: 1528,5(Kbps) Tx: 5360
Servidor de Telefonía	Rx: 3576 Tx: 360	Rx: 1112 Tx: 416
Cámara IP	Rx: 680,79 Kbps Tx: 324,32 Kbps	Rx: 759,14 Kbps Tx: 324,32 Kbps

Tx: Enviados, Rx: Recibidos, bps: bits x Segundo

CONEXIONES TCP ATAQUE UDP FLOOD CONTRA EL SERVIDOR WEB/CORREO				
Equipo	Nuevas (cs/min)		Establecidas (cs)	
	Estado		Estado	
	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	PO: 14 AO: 15	PO: 3 AO: 3	97	107
Servidor de Telefonía	PO: 0 AO: 0	PO: 0 AO: 0	1	0

PO: Passive Open, AO: Active Open, cs/min: Conexiones x minuto, cs: Conexiones

PROMEDIO DE PAQUETES								
Equipo	TCP (segs/min)		UDP (dts/min)		IP (pts/min)		ICMP (msgs/min)	
	Estado		Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	Tx: 1235 Rx: 1236	Tx:1092 Rx: 1093	Tx: 74 Rx: 88	Tx: 7 Rx: 7	Tx: 183 Rx: 132	Tx: 573 Rx: 191,1 kpts/min	Tx: 2 Rx: 2	Tx: 562 Rx: 0
Servidor de Telefonía	Tx: 26 Rx:41	Tx: 2 Rx: 2	Tx: 9 Rx:12	Tx: 12 Rx: 16	Tx: 15 Rx: 66	Tx: 13 Rx: 18	Tx: 0 Rx: 0	Tx: 0 Rx: 0
Cámara IP	Tx/Rx: 10,11 ksegs/min	Tx/Rx: 10,68 ksegs/min	Tx/Rx: 14,65	Tx/Rx: 11,6	Tx/Rx: 10,12 kpts/min	Tx/Rx: 10,69 kpts/min :	Tx/Rx: 1	Tx/ Rx: 0

Tx: Enviados, Rx: Recibidos, segs/min: Segmentos x Minuto, dts/min: Datagramas x Minuto, pts/min: Paquetes x Minuto

4.5 ATAQUE UDP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

4.5.1 Detalles del Ataque Realizado

Equipo Atacado	IP Origen del Ataque	IP Falsa del Ataque	Dirección IP Destino	Puerto Atacado	Tamaño de los Datos	Total de Paquetes enviados
Servidor de Telefonía	192.168.0.105	10.0.0.1	192.168.0.253	5060	0 Bytes	158856948

4.5.2 Comparación de Resultados Iniciales con los del Ataque Ejecutado (MRTG / CommView)

DETALLE DE RECURSOS CONSUMIDOS
ATAQUE UDP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	Carga del CPU (%)		Memoria Libre (MB)		Uso de Disco (%)	
	Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	4	5	1279,80	1176,40	48	48
Servidor de Telefonía	1	1	201	176,60	21	21

%: Porcentaje Uso de CPU o Disco, MB: Megabytes

TRÁFICO EN LA INTERFAZ DE RED
ATAQUE UDP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	Tráfico de red (bps)	
	Estado	Estado
	Inicial	Ataque
Servidor Web/Correo	Rx: 6704 Tx: 480	Rx: 176 Tx: 152
Servidor de Telefonía	Rx: 3576 Tx: 360	Rx: 1428,5 (Kbps) Tx: 464
Cámara IP	Rx: 680,79 Kbps Tx: 324,32 Kbps	Rx: 808,95 Kbps Tx: 324,32 Kbps

Tx: Enviados, Rx: Recibidos, bps: bits x segundo

CONEXIONES TCP ATAQUE UDP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA				
Equipo	Nuevas (cs/min)		Establecidas (cs)	
	Estado		Estado	
	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	PO: 14 AO: 15	PO: 3 AO: 3	97	109
Servidor de Telefonía	PO: 0 AO: 0	PO: 0 AO: 0	1	1

PO: Passive Open, AO: Active Open, cs/min: Conexiones x minuto, cs: Conexiones

PROMEDIO DE PAQUETES ATAQUE UDP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA								
Equipo	TCP (segs/min)		UDP (dts/min)		IP (pts/min)		ICMP (msgs/min)	
	Estado		Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	Tx: 1235 Rx: 1236	Tx: 914 Rx: 914	Tx: 74 Rx: 88	Tx: 8 Rx: 10	Tx: 183 Rx: 132	Tx: 12 Rx: 28	Tx: 2 Rx: 2	Tx: 0 Rx: 0
Servidor de Telefonía	Tx: 26 Rx:41	Tx: 2 Rx: 2	Tx: 9 Rx:12	Tx: 13 Rx: 203 (kdts/min)	Tx: 15 Rx: 66	Tx: 14 Rx: 203 (kpt/min)	Tx: 0 Rx: 0	Tx: 0 Rx: 0
Cámara IP	Tx/Rx: 10,11 ksegs/min	Tx/Rx: 11,06 ksegs/min	Tx/Rx: 14,65	Tx/Rx: 10,19	Tx/Rx: 10,12 kpts/min	Tx/Rx: 11,07 ksegs/min :	Tx/Rx: 1	Tx/ Rx: 0

Tx: Enviados, Rx: Recibidos, segs/min: Segmentos x Minuto, dts/min: Datagramas x Minuto, pts/min: Paquetes x Minuto

4.6 ATAQUE UDP FLOOD CONTRA LA CÁMARA IP

4.6.1 Detalles del Ataque Realizado

Equipo Atacado	IP Origen del Ataque	IP Falsa del Ataque	Dirección IP Destino	Puerto Atacado	Tamaño de los Datos	Total de Paquetes enviados
Cámara IP	192.168.0.105	10.0.0.1	192.168.0.252	5003	0 Bytes	161835155

4.6.2 Comparación de Resultados Iniciales con los del Ataque Ejecutado (MRTG / CommView)

DETALLE DE RECURSOS CONSUMIDOS
ATAQUE UDP FLOOD CONTRA LA CÁMARA IP

Equipo	Carga del CPU (%)		Memoria Libre (MB)		Uso de Disco (%)	
	Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	4	1	1279,80	1257,60	48	48
Servidor de Telefonía	1	1	201	255,20	21	21

%: Porcentaje Uso de CPU o Disco, MB: Megabytes

TRÁFICO EN LA INTERFAZ DE RED
ATAQUE UDP FLOOD CONTRA LA CÁMARA IP

Equipo	Tráfico de red (bps)	
	Estado	Estado
	Inicial	Ataque
Servidor Web/Correo	Rx: 6704 Tx: 480	Rx: 192 Tx: 136
Servidor de Telefonía	Rx: 3576 Tx: 360	Rx: 1000 Tx: 288
Cámara IP	Rx: 680,79 Kbps Tx: 324,32 Kbps	Rx: 1056 bps Tx: 336 bps

Tx: Enviados, Rx: Recibidos, bps: bits x Segundo

CONEXIONES TCP ATAQUE UDP FLOOD CONTRA LA CÁMARA IP				
Equipo	Nuevas (cs/min)		Establecidas (cs)	
	Estado		Estado	
	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	PO: 14 AO: 15	PO: 3 AO: 3	97	102
Servidor de Telefonía	PO: 0 AO: 0	PO: 0 AO: 1	1	0

PO: Passive Open, AO: Active Open, cs/min: Conexiones x minuto, cs: Conexiones

PROMEDIO DE PAQUETES ATAQUE UDP FLOOD CONTRA LA CÁMARA IP								
Equipo	TCP (segs/min)		UDP (dts/min)		IP (pts/min)		ICMP (msgs/min)	
	Estado		Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	Tx: 1235 Rx: 1236	Tx: 879 Rx: 880	Tx: 74 Rx: 88	Tx: 7 Rx: 11	Tx: 183 Rx: 132	Tx: 12 Rx: 28	Tx: 2 Rx: 2	Tx: 0 Rx: 0
Servidor de Telefonía	Tx: 26 Rx:41	Tx: 1 Rx: 1	Tx: 9 Rx:12	Tx: 12 Rx: 18	Tx: 15 Rx: 66	Tx: 12 Rx: 18	Tx: 0 Rx: 0	Tx: 0 Rx: 0
Cámara IP	Tx/Rx: 10,11 ksegs/min	Tx/Rx: 16,03 segs/min	Tx/Rx: 14,65	Tx/Rx: 216,37 kdts/min	Tx/Rx: 10,12 kpts/min	Tx/Rx: 216,53 kpts/min :	Tx/Rx: 1	Tx/ Rx: 149,15

Tx: Enviados, Rx: Recibidos, segs/min: Segmentos x Minuto, dts/min: Datagramas x Minuto, pts/min: Paquetes x Minuto

4.7 ATAQUE ICMP FLOOD CONTRA EL SERVIDOR WEB/CORREO

4.7.1 Detalles del Ataque Realizado

Equipo Atacado	IP Origen del Ataque	IP Falsa del Ataque	Dirección IP Destino	Tipo Mensaje ICMP	Tamaño de los Datos	Total de Paquetes enviados
Servidor Web y Correo	192.168.0.105	10.0.0.1	192.168.0.254	Echo Request	56 Bytes	190840408

4.7.2 Comparación de Resultados Iniciales con los del Ataque Ejecutado (MRTG / CommView)

DETALLE DE RECURSOS CONSUMIDOS
ATAQUE ICMP FLOOD CONTRA EL SERVIDOR WEB/CORREO

Equipo	Carga del CPU (%)		Memoria Libre (MB)		Uso de Disco (%)	
	Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	4	9	1279,80	2040,1	48	48
Servidor de Telefonía	1	1	201	214	21	21

%: Porcentaje Uso de CPU o Disco, MB: Megabytes

TRÁFICO EN LA INTERFAZ DE RED
ATAQUE ICMP FLOOD CONTRA EL SERVIDOR WEB/CORREO

Equipo	Tráfico de red (bps)	
	Estado	Estado
	Inicial	Ataque
Servidor Web/Correo	Rx: 6704 Tx: 480	Rx: 2091,5 (Kbps) Tx: 2899,0 (Kbps)
Servidor de Telefonía	Rx: 3576 Tx: 360	Rx: 1792 Tx: 664
Cámara IP	Rx: 680,79 Kbps Tx: 324,32 Kbps	Rx: 299,55 Kbps Tx: 19,37 Kbps

Tx: Enviados, Rx: Recibidos, bps: bits x segundo

CONEXIONES TCP
ATAQUE ICMP FLOOD CONTRA EL SERVIDOR WEB/CORREO

Equipo	Nuevas (cs/min)		Establecidas (cs)	
	Estado		Estado	
	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	PO: 14 AO: 15	PO: 3 AO: 3	97	91
Servidor de Telefonía	PO: 0 AO: 0	PO: 0 AO: 0	1	0

PO: Passive Open, AO: Active Open, cs/min: Conexiones x minuto, cs: Conexiones

PROMEDIO DE PAQUETES
ATAQUE ICMP FLOOD CONTRA EL SERVIDOR WEB/CORREO

Equipo	TCP (segs/min)		UDP (dts/min)		IP (pts/min)		ICMP (msgs/min)	
	Estado		Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	Tx: 1235 Rx: 1236	Tx: 874 Rx: 875	Tx: 74 Rx: 88	Tx: 11 Rx: 13	Tx: 183 Rx: 132	Tx: 222 kpts/min Rx: 222,1 kpts/min	Tx: 2 Rx: 2	Tx: 239,1 kmsgs/min Rx: 239,1 kmsgs/min
Servidor de Telefonía	Tx: 26 Rx:41	Tx: 2 Rx: 1	Tx: 9 Rx:12	Tx: 15 Rx: 22	Tx: 15 Rx: 66	Tx: 15 Rx: 23	Tx: 0 Rx: 0	Tx: 0 Rx: 0
Cámara IP	Tx/Rx: 10,11 ksegs/min	Tx/Rx: 7,94 ksegs/min	Tx/Rx: 14,65	Tx/Rx: 15,20	Tx/Rx: 10,12 kpts/min	Tx/Rx: 7,95 kpts/min	Tx/Rx: 1	Tx/ Rx: 0

Tx: Enviados, Rx: Recibidos, segs/min: Segmentos x Minuto, dts/min: Datagramas x Minuto, pts/min: Paquetes x Minuto

4.8 ATAQUE ICMP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

4.8.1 Detalles del Ataque Realizado

Equipo Atacado	IP Origen del Ataque	IP Falsa del Ataque	Dirección IP Destino	Tipo Mensaje ICMP	Tamaño de los Datos	Total de Paquetes enviados
Servidor de Telefonía	192.168.0.105	10.0.0.1	192.168.0.253	Echo Request	56 Bytes	190730442

4.8.2 Comparación de Resultados Iniciales con los del Ataque ejecutado (MRTG / CommView)

DETALLE DE RECURSOS CONSUMIDOS
ATAQUE ICMP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	Carga del CPU (%)		Memoria Libre (MB)		Uso de Disco (%)	
	Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	4	1	1279,80	1975,1	48	48
Servidor de Telefonía	1	14	201	204,3	21	21

%: Porcentaje Uso de CPU o Disco, MB: Megabytes

TRÁFICO EN LA INTERFAZ DE RED
ATAQUE ICMP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	Tráfico de red (bps)	
	Estado	Estado
	Inicial	Ataque
Servidor Web/Correo	Rx: 6704 Tx: 480	Rx: 1620 Tx: 472
Servidor de Telefonía	Rx: 3576 Tx: 360	Rx: 654,4 (Kbps) Tx: 692,3 (Kbps)
Cámara IP	Rx: 680,79 Kbps Tx: 324,32 Kbps	Rx: 448,57 Kbps Tx: 20,47 Kbps

Tx: Enviados, Rx: Recibidos, bps: bits x Segundo

CONEXIONES TCP
ATAQUE ICMP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	Nuevas (cs/min)		Establecidas (cs)	
	Estado		Estado	
	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	PO: 14 AO: 15	PO: 2 AO: 3	97	90
Servidor de Telefonía	PO: 0 AO: 0	PO: 0 AO: 0	1	0

PO: Passive Open, AO: Active Open, cs/min: Conexiones x minuto, cs: Conexiones

PROMEDIO DE PAQUETES
ATAQUE ICMP FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	TCP (segs/min)		UDP (dts/min)		IP (pts/min)		ICMP (msgs/min)	
	Estado		Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	Tx: 1235 Rx: 1236	Tx: 880 Rx:880	Tx: 74 Rx: 88	Tx: 13 Rx:15	Tx: 183 Rx: 132	Tx: 12 Rx: 34	Tx: 2 Rx: 2	Tx: 0 Rx:0
Servidor de Telefonía	Tx: 26 Rx:41	Tx: 0 Rx: 0	Tx: 9 Rx:12	Tx: 14 Rx: 20	Tx: 15 Rx: 66	Tx: 235,4 kpts/min Rx: 237,6 kpts/min	Tx: 0 Rx: 0	Tx: 244,8 kmsgs/min Rx: 244,8 kmsgs/min
Cámara IP	Tx/Rx: 10,11 ksegs/min	Tx/Rx: 8,39 ksegs/min	Tx/Rx: 14,65	Tx/Rx: 17,87	Tx/Rx: 10,12 kpts/min	Tx/Rx: 8,39 kpts/min :	Tx/Rx: 1	Tx/ Rx: 0

Tx: Enviados, Rx: Recibidos, segs/min: Segmentos x Minuto, dts/min: Datagramas x Minuto, pts/min: Paquetes x Minuto

4.9 ATAQUE ICMP FLOOD CONTRA LA CÁMARA IP

4.9.1 Detalles del Ataque Realizado

Equipo Atacado	IP Origen del Ataque	IP Falsa del Ataque	Dirección IP Destino	Tipo Mensaje ICMP	Tamaño de los Datos	Total de Paquetes enviados
Cámara IP	192.168.0.105	10.0.0.1	192.168.0.252	Echo Request	56 Bytes	190685809

4.9.2 Comparación de Resultados Iniciales con los del Ataque Ejecutado (MRTG / CommView)

DETALLE DE RECURSOS CONSUMIDOS
ATAQUE ICMP FLOOD CONTRA LA CÁMARA IP

Equipo	Carga del CPU (%)		Memoria Libre (MB)		Uso de Disco (%)	
	Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	4	3	1279,80	1891,8	48	48
Servidor de Telefonía	1	1	201	201,3	21	21

%: Porcentaje Uso de CPU o Disco, MB: Megabytes

TRÁFICO EN LA INTERFAZ DE RED
ATAQUE ICMP FLOOD CONTRA LA CÁMARA IP

Equipo	Tráfico de red (bps)	
	Estado	Estado
	Inicial	Ataque
Servidor Web/Correo	Rx: 6704 Tx: 480	Rx: 672 Tx: 112
Servidor de Telefonía	Rx: 3576 Tx: 360	Rx: 1672 Tx: 568
Cámara IP	Rx: 680,79 Kbps Tx: 324,32 Kbps	Rx: 405,32 Kbps Tx: 197,94 Kbps

Tx: Enviados, Rx: Recibidos, bps: bits x segundo

CONEXIONES TCP ATAQUE ICMP FLOOD CONTRA LA CÁMARA IP				
Equipo	Nuevas (cs/min)		Establecidas (cs)	
	Estado		Estado	
	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	PO: 14 AO: 15	PO: 3 AO: 3	97	94
Servidor de Telefonía	PO: 0 AO: 0	PO: 0 AO: 0	1	0

PO: Passive Open, AO: Active Open, cs/min: Conexiones x minuto, cs: Conexiones

PROMEDIO DE PAQUETES ATAQUE ICMP FLOOD CONTRA LA CÁMARA IP								
Equipo	TCP (segs/min)		UDP (dts/min)		IP (pts/min)		ICMP (msgs/min)	
	Estado		Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	Tx: 1235 Rx: 1236	Tx: 888 Rx: 890	Tx: 74 Rx: 88	Tx: 7 Rx: 8	Tx: 183 Rx: 132	Tx: 12 Rx: 34	Tx: 2 Rx: 2	Tx: 0 Rx:0
Servidor de Telefonía	Tx: 26 Rx:41	Tx: 0 Rx: 0	Tx: 9 Rx:12	Tx: 14 Rx: 21	Tx: 15 Rx: 66	Tx: 14 Rx: 22	Tx: 0 Rx: 0	Tx: 0 Rx: 0
Cámara IP	Tx/Rx: 10,11 ksegs/min	Tx/Rx: 7,88 ksegs/min	Tx/Rx: 14,65	Tx/Rx: 15,89	Tx/Rx: 10,12 kpts/min	Tx/Rx: 362,77 kpts/min :	Tx/Rx: 1	Tx/ Rx: 354,88 kpts/min

Tx: Enviados, Rx: Recibidos, segs/min: Segmentos x Minuto, dts/min: Datagramas x Minuto, pts/min: Paquetes x Minuto

4.10 ATAQUE INVITE FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

4.10.1 Detalles del Ataque Realizado

Equipo Atacado	IP Origen del Ataque	Dirección IP Destino	Extensión Usada	Puerto Atacado	Total de Paquetes enviados
Servidor de Telefonía	192.168.0.105	192.168.0.253	101	5060	9895175893

4.10.2 Comparación de Resultados Iniciales con los del Ataque Ejecutado (MRTG / CommView)

DETALLE DE RECURSOS CONSUMIDOS
ATAQUE INVITE FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	Carga del CPU (%)		Memoria Libre (MB)		Uso de Disco (%)	
	Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	4	1	1279,80	1357,60	48	48
Servidor de Telefonía	1	9	201	53,7	21	45

%: Porcentaje Uso de CPU o Disco, MB: Megabytes

TRÁFICO EN LA INTERFAZ DE RED
ATAQUE INVITE FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	Tráfico de red (bps)	
	Estado	Estado
	Inicial	Ataque
Servidor Web/Correo	Rx: 6704 Tx: 480	Rx: 192 Tx: 136
Servidor de Telefonía	Rx: 3576 Tx: 360	Rx: 1528,5 Kbps Tx: 5360
Cámara IP	Rx: 680,79 Kbps Tx: 324,32 Kbps	Rx: 205,33 Kbps Tx: 179,17 Kbps

Tx: Enviados, Rx: Recibidos, bps: bits x segundo

CONEXIONES TCP
ATAQUE INVITE FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	Nuevas (cs/min)		Establecidas (cs)	
	Estado		Estado	
	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	PO: 14 AO: 15	PO: 3 AO: 3	97	95
Servidor de Telefonía	PO: 0 AO: 0	PO: 0 AO: 0	1	2

PO: Passive Open, AO: Active Open, cs/min: Conexiones x minuto, cs: Conexiones

PROMEDIO DE PAQUETES
ATAQUE INVITE FLOOD CONTRA EL SERVIDOR DE TELEFONÍA

Equipo	TCP (segs/min)		UDP (dts/min)		IP (pts/min)		ICMP (msgs/min)	
	Estado		Estado		Estado		Estado	
	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque	Inicial	Ataque
Servidor Web/Correo	Tx: 1235 Rx: 1236	Tx: 903 Rx: 905	Tx: 74 Rx: 88	Tx: 7 Rx: 13	Tx: 183 Rx: 132	Tx: 12 Rx: 28	Tx: 2 Rx: 2	Tx: 0 Rx:0
Servidor de Telefonía	Tx: 26 Rx:41	Tx: 2 Rx 2	Tx: 9 Rx:12	Tx: 33.1 Mdts/min Rx 33.1 Mdts/min	Tx: 15 Rx: 66	Tx: 33.1 Mpts/min Rx 33.1 Mpts/min	Tx: 0 Rx: 0	Tx: 35.8 Mmsgs/min Rx 35.8 Mmsgs/min
Cámara IP	Tx/Rx: 10,11 ksegs/min	Tx/Rx: 7,11 ksegs/min	Tx/Rx: 14,65	Tx/Rx: 13,03	Tx/Rx: 10,12 kpts/min	Tx/Rx: 7,12 kpts/min :	Tx/Rx: 1	Tx/ Rx: 0

Tx: Enviados, Rx: Recibidos, segs/min: Segmentos x Minuto, dts/min: Datagramas x Minuto, pts/min: Paquetes x Minuto

6. DEGRADACIÓN DE LOS SERVICIOS POR ATAQUE REALIZADO

Las tablas mostradas a continuación, resumen los efectos causados por cada ataque realizado y las consecuencias que éstos causaron en los servicios presentes. Los datos obtenidos, son la diferencia de los valores adquiridos antes y después de la ejecución de cada ataque.

Adicionalmente, cabe señalar que, se mostrarán únicamente los valores que, tras la realización del ataque, produjeron un efecto, mas no los que variaron debido al propio sistema.

El estado de los servicios por consecuencia del ataque fueron citados como:

- **Bueno:** Se puede acceder y hacer uso del servicio sin ningún inconveniente (Se encuentra 100% Operativo).

- **Regular:** El servicio presenta leves inconvenientes o demora, pero puede ser utilizado sin problemas.

- **Malo:** El servicio se encuentra ausente, tarda demasiado o tiene demasiados inconvenientes para ser utilizado (Denegación de Servicio).

Ataque # 1		**Estado del Servicio**				**Efectos Producidos a Causa de la Realización del Ataque**
Tipo de Ataque	**Equipo Atacado**	**Acceso a Owa**	**Acceso a Internet**	**Video**	**Telf.**	
SYN Flood	Servidor Web y Correo	**REGULAR**	**MALO**	**BUENO**	**BUENO**	Servidor de Correo • **CPU:** Se incremento en un 39%. • **Tráfico en la interfaz de red:** El tráfico de salida aumentó en 144 bps debido a paquetes SYN-ACK de respuesta. • **Conexiones Active/Passive Open:** Hubo un aumento de 1564 en Conexiones Passive Open, Conexiones Active Open se mantienen bajo el rango. • **Segmentos TCP:** Hubo un aumento de segmentos TCP tanto enviados (1911 segs/min) como recibidos (1148,56 ksegs/min). • **Paquetes IP**: Hubo un aumento de paquetes IP tanto enviados (1152,51 kpts/min) como recibidos (1148,76 kpts/min). Servidor de Telefonía • No hubo efectos producidos a causa de la realización del ataque. Cámara IP • No hubo efectos producidos a causa de la realización del ataque.

Ataque # 2		**Estado del Servicio**				**Efectos Producidos a Causa de la Realización del Ataque**
Tipo de Ataque	**Equipo Atacado**	**Acceso a Owa**	**Acceso a Internet**	**Video**	**Telf.**	
SYN Flood	Servidor de Telefonía	**BUENO**	**BUENO**	**BUENO**	**REGULAR**	Servidor de Correo • No hubo efectos producidos a causa de la realización del ataque. Servidor de Telefonía • **Tráfico en la interfaz de red:** Se tuvo un aumento de 184 bps en el tráfico de entrada y un 1.89 Kbps en el de salida, debido a paquetes SYN-ACK de respuesta. • **Segmentos TCP:** Hubo un aumento de segmentos TCP tanto enviados (283,27 ksegs/min) como recibidos (282,26 ksegs/min). • **Paquetes IP:** Hubo un aumento de paquetes IP tanto enviados (283,38 kpts/min) como recibidos (282,33 kpts/min). Cámara IP • No hubo efectos producidos a causa de la realización del ataque.

<table>
<tr><th colspan="2">Ataque # 3</th><th colspan="4">Estado del Servicio</th><th rowspan="2">Efectos Producidos a Causa de la Realización del Ataque</th></tr>
<tr><th>Tipo de Ataque</th><th>Equipo Atacado</th><th>Acceso a Owa</th><th>Acceso a Internet</th><th>Video</th><th>Telf.</th></tr>
<tr><td rowspan="6">SYN Flood</td><td rowspan="6">Cámara IP</td><td rowspan="6">BUENO</td><td rowspan="6">BUENO</td><td rowspan="6">MALO</td><td rowspan="6">BUENO</td><td>Servidor de Correo</td></tr>
<tr><td>• No hubo efectos producidos a causa de la realización del ataque.</td></tr>
<tr><td>Servidor de Telefonía</td></tr>
<tr><td>• No hubo efectos producidos a causa de la realización del ataque.</td></tr>
<tr><td>Cámara IP</td></tr>
<tr><td>• Tráfico en la interfaz de red: La disminución significativa en el tráfico tanto entrante como saliente, se debió a que la cámara dejo de responder (DoS).
• Segmentos TCP: Hubo un aumento de 280,76 ksegs/min (En su gran parte no fueron procesados).
• Paquetes IP: Hubo un aumento de 280,76 kpts/min (En su gran parte no fueron procesados).</td></tr>
</table>

<table>
<tr><th colspan="2">Ataque # 4</th><th colspan="4">Estado del Servicio</th><th rowspan="2">Efectos Producidos a Causa de la Realización del Ataque</th></tr>
<tr><th>Tipo de Ataque</th><th>Equipo Atacado</th><th>Acceso a Owa</th><th>Acceso a Internet</th><th>Video</th><th>Telf.</th></tr>
<tr><td rowspan="6">UDP Flood</td><td rowspan="6">Servidor Web y Correo</td><td rowspan="6">BUENO</td><td rowspan="6">BUENO</td><td rowspan="6">BUENO</td><td rowspan="6">BUENO</td><td>Servidor de Correo</td></tr>
<tr><td>• Tráfico en la interfaz de red: Hubo un aumento de 1521,79 Kbps en el tráfico de entrada y un 4,88 Kbps en el de salida.
• Paquetes IP: Hubo un aumento de paquetes IP tanto enviados (390 pts/min) como recibidos (190,97 kpts/min).
• Mensajes ICMP: Hubo un aumento de mensajes ICMP enviados de 560 msgs/min, debido a mensajes ICMP de respuesta Puerto inalcanzable.</td></tr>
<tr><td>Servidor de Telefonía</td></tr>
<tr><td>• No hubo efectos producidos a causa de la realización del ataque.</td></tr>
<tr><td>Cámara IP</td></tr>
<tr><td>• No hubo efectos producidos a causa de la realización del ataque.</td></tr>
</table>

<table>
<tr><th colspan="2">Ataque # 5</th><th colspan="4">Estado del Servicio</th><th rowspan="2">Efectos Producidos a Causa de la Realización del Ataque</th></tr>
<tr><th>Tipo de Ataque</th><th>Equipo Atacado</th><th>Acceso a Owa</th><th>Acceso a Internet</th><th>Video</th><th>Telf.</th></tr>
<tr><td rowspan="6">UDP Flood</td><td rowspan="6">Servidor de Telefonía</td><td rowspan="6">BUENO</td><td rowspan="6">BUENO</td><td rowspan="6">BUENO</td><td rowspan="6">BUENO</td><td>Servidor de Correo</td></tr>
<tr><td>• No hubo efectos producidos a causa de la realización del ataque.</td></tr>
<tr><td>Servidor de Telefonía</td></tr>
<tr><td>• Memoria RAM: Disminuyó en 24,40 MB.
• Tráfico en la interfaz de red: Se tuvo un aumento de 1424.92 Kbps en el tráfico de entrada y 104 bps en el de salida.
• Datagramas UDP: Hubo un aumento de 202.98 kdts/ min datagramas UDP recibidos.
• Paquetes IP: Hubo un aumento de 202.93 kpts/min Paquetes IP recibidos.</td></tr>
<tr><td>Cámara IP</td></tr>
<tr><td>• No hubo efectos producidos a causa de la realización del ataque.</td></tr>
</table>

<table>
<tr><th colspan="2">Ataque # 6</th><th colspan="4">Estado del Servicio</th><th rowspan="2">Efectos Producidos a Causa de la Realización del Ataque</th></tr>
<tr><th>Tipo de Ataque</th><th>Equipo Atacado</th><th>Acceso a Owa</th><th>Acceso a Internet</th><th>Video</th><th>Telf.</th></tr>
<tr><td rowspan="8">UDP Flood</td><td rowspan="8">Cámara IP</td><td rowspan="8">BUENO</td><td rowspan="8">BUENO</td><td rowspan="8">MALO</td><td rowspan="8">BUENO</td><td>Servidor de Correo</td></tr>
<tr><td>• No hubo efectos producidos a causa de la realización del ataque.</td></tr>
<tr><td>Servidor de Telefonía</td></tr>
<tr><td>• No hubo efectos producidos a causa de la realización del ataque.</td></tr>
<tr><td>Cámara IP</td></tr>
<tr><td>• Tráfico en la interfaz de red: La disminución significativa en el tráfico tanto entrante como saliente, se debió a que la cámara dejo de responder, debido a los paquetes UDP Flood e ICMP de respuesta de puerto inalcanzable.
• Segmentos TCP: La disminución significativa se debió a que la cámara dejo de responder.
• Datagramas UDP: Hubo un aumento de 216.35 kdts/min (En su gran parte no fueron procesados).
• Paquetes IP: Hubo un aumento de 216.52 kpts/min (En su gran parte no fueron procesados).
• Mensajes ICMP: Se tuvo un aumento de 148.15 msgs/min, mientras la cámara estuvo operativa, debido a mensajes ICMP de respuesta de puerto inalcanzable.</td></tr>
</table>

Ataque # 7		Estado del Servicio				Efectos Producidos a Causa de la Realización del Ataque
Tipo de Ataque	**Equipo Atacado**	**Acceso a Owa**	**Acceso a Internet**	**Video**	**Telf.**	
ICMP Food	Servidor Web y Correo	**BUENO**	**MALO**	**BUENO**	**BUENO**	Servidor de Correo • **CPU:** Aumentó en un 5%. • **Tráfico en la interfaz de red:** Se tuvo un aumento de 2084.8 Kbps en el tráfico de entrada y 2898.5 Kbps en el de salida, debido a mensajes ICMP Echo Request/Reply • **Paquetes IP**: Hubo un aumento de paquetes IP enviados (221.81 kpts/min) y recibidos (221.96 kpts/min) , debido a mensajes ICMP Echo Request/Reply • **Mensajes ICMP:** Hubo un aumento de mensajes ICMP enviados (239.1 kmsgs/min) y recibidos (239.1 kmsgs/min), debido a mensajes ICMP Echo Request/Reply Servidor de Telefonía • No hubo efectos producidos a causa de la realización del ataque. Cámara IP • No hubo efectos producidos a causa de la realización del ataque.

Ataque # 8		Estado del Servicio				Efectos Producidos a Causa de la Realización del Ataque
Tipo de Ataque	**Equipo Atacado**	**Acceso a Owa**	**Acceso a Internet**	**Video**	**Telf.**	
ICMP Food	Servidor de Telefonía	**BUENO**	**MALO**	**BUENO**	**BUENO**	Servidor de Correo • No hubo efectos producidos a causa de la realización del ataque. Servidor de Telefonía • **CPU:** Aumentó en un 13%. • **Tráfico en la interfaz de red:**.Se tuvo un aumento de 650.82 Kbps en el tráfico de entrada y 691.94 Kbps en el de salida, debido a mensajes ICMP Echo Request/Reply • **Paquetes IP:** Hubo un aumento de paquetes IP enviados (235.38 kpts/min) y recibidos (237.53 kpts/min) , debido a mensajes ICMP Echo Request/Reply • **Mensajes ICMP:** Hubo un aumento de mensajes ICMP enviados (244,8 kmsgs/min) y recibidos (244,8 kmsgs/min), debido a mensajes ICMP Echo Request/Reply Cámara IP • No hubo efectos producidos a causa de la realización del ataque.

Ataque # 9		Estado del Servicio				Efectos Producidos a Causa de la Realización del Ataque
Tipo de Ataque	**Equipo Atacado**	**Acceso a Owa**	**Acceso a Internet**	**Video**	**Telf.**	
ICMP Food	Cámara IP	**BUENO**	**BUENO**	**BUENO**	**BUENO**	Servidor de Correo • No hubo efectos producidos a causa de la realización del ataque. Servidor de Telefonía • No hubo efectos producidos a causa de la realización del ataque. Cámara IP • **Paquetes IP:** Hubo un aumento de 352.65 kpts/min, debido a mensajes ICMP Echo Request/Reply • **Mensajes ICMP:** Hubo un aumento de 354.88 kmsgs/min, debido a mensajes ICMP Echo Request/Reply

Ataque # 10		Estado del Servicio				Efectos Producidos a Causa de la Realización del Ataque
Tipo de Ataque	**Equipo Atacado**	**Acceso a Owa**	**Acceso a Internet**	**Video**	**Telf.**	
Invite Flood	Servidor de Telefonía	**BUENO**	**BUENO**	**BUENO**	**MALO**	Servidor de Correo • No hubo efectos producidos a causa de la realización del ataque. Servidor de Telefonía • **CPU:** Aumentó en un 8%. • **Memoria RAM Libre:** Disminuyó en 147,30 MB. • **Uso de Disco:** Aumento en un 24%. • **Tráfico en la interfaz de red:** Se tuvo un aumento de 1524,92 Kbps en el tráfico de entrada y 5000 bps en el de salida, debido a paquetes SIP “Server Internal Error” de respuesta y mensajes ICMP de destino y puerto inalcanzable. • **Datagramas UDP**: Hubo un aumento de datagramas UDP enviados (33,1 Mdts/min) y recibidos (33,1 Mdts/min), debido a paquetes SIP enviados y recibidos. • **Paquetes IP:** Hubo un aumento de paquetes IP enviados (33,1 Mpts/min) y recibidos (33,1 Mpts/min), debido a paquetes SIP y mensajes ICMP de puerto y destino inalcanzable. • **Mensajes ICMP:** Hubo un aumento de mensajes ICMP enviados (35,8 Mmsgs/min) y recibidos (35,8 Mmsgs/min), debido a mensajes ICMP de puerto y destino inalcanzable. Cámara IP • No hubo efectos producidos a causa de la realización del ataque.

7. RESUMEN DE ATAQUES DE DENEGACIÓN DE SERVICIO EXITOSOS

Tipo de Ataque	Equipo Atacado	Efecto a consecuencia del Ataque			
		Servidor web/correo	Servidor de Telefonía	Cámara IP	Router Acceso a Internet
Syn Flood	Servidor web/correo	-	-	-	DoS
	Servidor de Telefonía	-	-	-	-
	Cámara IP	-	-	DoS	-
UDP Flood	Servidor web/correo	-	-	-	-
	Servidor de Telefonía	-	-	-	-
	Cámara IP	-	-	DoS	-
ICMP Flood	Servidor web/correo	-	-	-	DoS
	Servidor de Telefonía	-	-	-	DoS
	Cámara IP	-	-	-	-
Invite Flood	Servidor de Telefonía	-	DoS	-	-

8. CONCLUSIONES

- Tras el ataque SYN Flood contra el servidor web/Correo, el router deja de responder a las peticiones realizadas por los clientes (Se tiene perdida de paquetes del 50/70 por ciento), razón por la cual, el servicio de internet se ve afectado. El servidor de web/correo responde a los paquetes SYN Flood enviados con paquetes SYN-ACK al Puerto 80 del router, debido a la dirección falsa 10.0.0.1. Al finalizar el ataque, el servicio vuelve a restablecerse.

- Iniciado el ataque SYN Flood hacia la cámara IP, ésta deja de responder y nuevos usuarios no pueden acceder a ella. Al finalizar el ataque el servicio vuelve a restablecerse.

- Iniciado el ataque UDP Flood hacia la cámara IP, ésta deja de responder y nuevos usuarios no pueden acceder a ella. Se requiere el reinicio de la cámara para volver a restablecer el servicio.

- Tras un ataque UDP Flood, tanto la cámara como el servidor Web/Correo responden con mensajes ICMP de destino y puerto inalcanzable al router, debido a la dirección IP falsa 10.0.0.1.

- El servidor de Telefonía (Ubuntu server 10.10), no responde con mensajes ICMP de puerto inalcanzable, tras un ataque UDP Flood.

- Los ataques SYN Flood y UDP Flood contra el servidor de telefonía, no provocan una denegación de servicio, pero si se tiene una demora prácticamente imperceptible al momento de marcar a una determinada extensión. No afecta a la calidad del audio.

- El enviar paquetes con una mayor cantidad de datos, se logra un aumento en el uso de CPU y tráfico de la interfaz de red.

- Tras el ataque ICMP Flood contra el servidor web/Correo y telefonía, el router deja de responder a las peticiones realizadas por los clientes (Se tiene perdida de paquetes del 50/70 por ciento), razón por la cual, el servicio de internet se ve afectado. Los servidores responden a los paquetes ICMP Flood echo-request con paquetes ICMP echo-reply al router, debido a la dirección falsa 10.0.0.1.Al finalizar el ataque, el servicio vuelve a restablecerse.

- A consecuencia del ataque Invite flood contra el servidor de telefonía, éste deja de responder y una gran cantidad de recursos principalmente de memoria y espacio en disco son consumidos.

- Al enviar paquetes Invite Flood al servidor de Telefonía, éste responde con paquetes SIP “Server Internal Error” al generador de paquetes Invite y a su vez, éste responde con mensajes ICMP de Destino y puerto inalcanzable al servidor de Telefonía.

- Mensajes ICMP con longitud mayor al tamaño permitido, son descartados por los servidores.

9. SOLUCIONES Y/O RECOMENDACIONES

EQUIPO	SOLUCIONES/RECOMENDACIONES
Servidor Web/Correo	• Instalar actualizaciones y parches de seguridad de Sistema Operativo y Software. • Deshabilitar ICMP. • Implementar y configurar el Firewall a nivel de servidor para realizar filtrado. • Instalación de antivirus y sus respectivas nuevas actualizaciones. • Programar las actualizaciones en horas no laborables. • Deshabilitar servicios no requeridos. • Desinstalar aplicaciones innecesarias. • Utilizar software con licencia y legítimos.
Servidor de Telefonía	• Instalar actualizaciones y parches de seguridad de Sistema Operativo y Software. • Deshabilitar ICMP • Implementar y configurar el Firewall a nivel de servidor para realizar filtrado. Utilizar Iptables y Linux/netfilter para clasificar y limitar el tráfico SIP desde diferentes direcciones IP. • Instalación de antivirus y sus respectivas nuevas actualizaciones • Programar la actualizaciones en horas no laborables • Deshabilitar servicios no requeridos

EQUIPO	SOLUCIONES/RECOMENDACIONES
Servidor de Telefonía	• Desinstalar aplicaciones innecesarias. • Utilizar software con licencia y legítimos. • Deshabilitar los logs generados, por Asterisk
Cámara IP	• Cambiar la contraseña de administrador por defecto. • Por defecto utiliza TCP como protocolo de transmisión, podría utilizarse UDP para tal propósito • Cambiar los puertos por defecto HTTP (80), Control (5001), Audio (5002) y Video (5003) por otros diferentes. • Por defecto UPnP se encuentra habilitado. Si no se requiere su uso, el deshabilitarlo permitirá que el router no envíe paquetes multicast en el Puerto 1900 (ssdp, Protocolo Simple de Descubrimiento de Servicios) a todos los dispositivos en la red. • Instalar actualizaciones de firmware propietarios.
Router	• Limitar el ancho de banda (La tarea podría ser realizada por otro equipo, si el router no dispone de dicha característica). • Cambio de equipo o implementar un servidor proxy. • Cambiar la contraseña de administrador por defecto. • Implementar filtros a nivel IP y MAC • Restringir puertos. • Deshabilitar ICMP. • Instalar actualizaciones de firmware propietarios. • Por defecto UPnP se encuentra habilitado. Si no se requiere su uso, el deshabilitarlo permitirá que el router no envíe paquetes multicast en el Puerto 1900 (ssdp, Protocolo Simple de Descubrimiento de Servicios) a todos los dispositivos en la red.

EQUIPO	SOLUCIONES/RECOMENDACIONES
Switch	• Podría ser cambiado por otro tal, que permita la implementación de VLan´s y Calidad de Servicio.
Hosts/Teléfonos IP	• Evitar el uso de aplicaciones P2P • Instalar actualizaciones y parches de seguridad de Sistema Operativo y Software. • Implementar y configurar el Firewall a nivel de host para realizar filtrado. • Instalación de antivirus y sus respectivas nuevas actualizaciones • Programar la actualizaciones en horas no laborables • Deshabilitar servicios no requeridos • Desinstalar aplicaciones innecesarias. • Utilizar software con licencia y legítimos.