ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA EL DESCUBRIMIENTO Y EVALUACIÓN DE VULNERABILIDADES DE LA RED DE UNA CARTERA DE ESTADO

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

LUIS ALCIDES MENDAÑO MENDAÑO
luiss_lam@hotmail.com

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

MARÍA ELENA HURTADO SANDOVAL
malenahurtado@hotmail.com

DIRECTOR: ING. WILLIAMS FERNANDO FLORES CIFUENTES
fernando.flores@epn.edu.ec

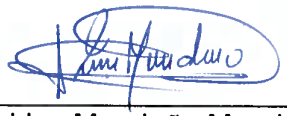
Quito, noviembre 2016

DECLARACIÓN

Nosotros, MARÍA ELENA HURTADO SANDOVAL y LUIS ALCIDES MENDAÑO MENDAÑO, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

María Elena Hurtado Sandoval



Luis Alcides Mendaño Mendaño

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por María Elena Hurtado Sandoval y Luis Alcides Mendaño Mendaño, bajo mi supervisión.

Ing. Fernando Flores
DIRECTOR DEL PROYECTO

AGRADECIMIENTO

A Dios y la Virgen por todas las bendiciones y por darme la fuerza necesaria para lograr mis metas.

A mi Madre y Bárbara Fuchs, por sus acertados consejos, dedicación y sabiduría, por enseñarme que nada es imposible en la vida al ser ejemplo de lucha y esfuerzo.

A mis hermanos, cuñado y amigos por su apoyo incondicional. A mi esposo y compañero de tesis por su comprensión, dedicación y amor, por hacer realidad esta meta.

Al Ing. Fernando Flores por su tiempo y guía en el desarrollo de este proyecto.

María Elena

Agradezco a mi compañera y esposa, quien puso el hombro, día y noche, la misma que me ha ayudado en los peores momentos, y ha luchado igual o más que yo para sacar adelante el presente proyecto, agradezco a mi familia, Alberto, Juan Pablo, Papá, Mamá, Tío Carlos, Abuelita Marti, Abuelito Carlos, por la motivación, el apoyo y la participación que cada uno ha tenido en lo largo de mi carrera universitaria, agradezco de igual manera a mis profesores, que con sus sabios consejos han inspirado mis deseos de superación, agradezco a mis compañeros y amigos, los mismos que compartieron las aulas durante nuestra formación universitaria, para convertirse hoy por hoy, en profesionales.

Luis

DEDICATORIA

A mi hermana y segunda madre,
por demostrarme que los sueños son para hacerlos realidad,
por enseñarme a volar…
A mi querida hija y amado esposo,
por ser el motor de mi vida.
A mi madre,
porque sin ella nada de esto fuera posible.

María Elena

El presente proyecto lo dedico principalmente a Dios, en segundo lugar a mi amada hija, se lo dedico también a los profesores que nos han dado una mano para efectuar de una mejor manera la elaboración del presente proyecto, lo dedico a mi familia, padres, hermanos, tío Carlos, abuelita Martí, quienes han estado siempre preocupados por que supere mis metas, finalmente, y siendo aún muy importante, lo dedico a mi abuelito Dr. Carlos Vásquez, quien desde el cielo sé que festejará nuestros triunfos.

Luis

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El objetivo del presente proyecto es la implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades, con el fin de medir la estrategia de defensa de un sistema informático y realizar recomendaciones de mitigación ante las fallas encontradas.

En el primer capítulo se describe los fundamentos teóricos sobre los diferentes temas necesarios para el desarrollo del presente proyecto, tales como: seguridad informática y hacking ético (tipos de pruebas de penetración, tipos de hackers, fases del hacking ético). Se realiza una descripción de las herramientas de análisis de vulnerabilidades, así como se presenta un resumen de tres metodologías de hacking ético.

En el segundo capítulo se realiza la recopilación y análisis de información tanto de la red perimetral, como aplicaciones expuestas, servidores y puertos que permitan determinar posibles vectores de ataque, además se realiza el diseño de las plantillas necesarias para la documentación de la información obtenida.

En el tercer capítulo se detalla las consideraciones legales que se deben tener en cuenta al momento de realizar un hacking ético, así como la documentación que se debe presentar al finalizar el trabajo. Una vez establecidas las reglas de operación, se realizan las configuraciones de las herramientas para análisis de vulnerabilidades, las cuales nos permiten detectar posibles fallas de seguridad en el objetivo descubriendo malas configuraciones, servicios sin parches, arquitecturas erróneas, entre otros escenarios. Con las vulnerabilidades conocidas se realiza un plan de explotación o ataques el cuál será aprobado por el encargado de seguridad de la organización.

En el cuarto capítulo se realiza la implementación del plan de ataques propuesto y aprobado, el objetivo de esta fase es explotar las vulnerabilidades y adquirir accesos a los servicios de ser posible.

En el quinto capítulo se realiza el reporte de toda la información obtenida, convirtiendo todos los datos conseguidos en información que permita tomar medidas correctivas. Además se presenta un plan de correcciones, en el cual

se indica las actividades a realizar para mitigar las vulnerabilidades encontradas.

El sexto capítulo indica las conclusiones y recomendaciones obtenidas durante el desarrollo del presente proyecto de titulación.

Finalmente se incluye una sección de Anexos donde están: la carta de autorización, el convenio de confidencialidad, un ejemplo del reporte de vulnerabilidades de cada herramienta y el plan de ataques.

PRESENTACIÓN

Debido al avance tecnológico, la seguridad de toda empresa es esencial para mantener protegidos todos sus datos, sistemas y servicios. La información que fluye por las redes puede ser susceptible a diferentes tipos de ataques. De esta manera, datos confidenciales de una organización en manos equivocadas podrían comprometer la integridad de la institución.

Es por eso que con el pasar de los tiempos ha surgido la necesidad de implementar procesos de seguridad más robustos y con ello efectuar técnicas de intrusiones bajo un ambiente controlado, lo cual simule un ataque real. Esta simulación permite encontrar brechas en la seguridad, las cuales un atacante podría aprovechar para infiltrarse en la red de una organización con propósitos malintencionados y de esta forma manipular información, suplantar identidades, colapsar servicios, u otras actividades propias de un delincuente informático.

La función de un hacker ético es efectuar ataques controlados hacia una infraestructura informática específica para detectar y explotar vulnerabilidades potenciales pero sin poner en riesgo los sistemas y servicios auditados.

El presente proyecto busca ser una guía sobre el proceso de implementación de técnicas de hacking ético con el objetivo de poder mitigar fallas de seguridad antes de sufrir un ataque informático, el cual pueda comprometer información valiosa.

CAPÍTULO I

1. FUNDAMENTOS TEÓRICOS

Este capítulo describe los fundamentos teóricos sobre los diferentes temas necesarios para el desarrollo del presente proyecto, tales como: seguridad informática, hacking ético: tipos de pruebas de penetración, tipos de hackers, fases del hacking ético. Se realizará una descripción de las herramientas de análisis de vulnerabilidades, así como se presenta un resumen de tres metodologías de hacking ético.

1.1.SEGURIDAD INFORMÁTICA[1]

La seguridad informática surge de la necesidad de proteger todos los elementos críticos que forman parte de un sistema de información que son: todos los datos, el hardware y software.

La seguridad informática no es un producto que se pueda adquirir, a la vez no puede ser considerado como un servicio, simplemente se debe considerar como un proceso clave para el rendimiento óptimo de una organización.

Si se toma a la seguridad como un proceso, este consiste en mantener un nivel aceptable de riesgo, por lo tanto la seguridad informática es el proceso para asegurar que los recursos de la red sean usados para el fin que fueron creados y a la vez garantizar el acceso restringido a la información.

La seguridad informática tiene como objetivo la protección de la infraestructura de una red, en especial la información contenida o que circula por la misma; por lo tanto se puede decir que es un conjunto de métodos, protocolos, herramientas, estándares, políticas orientados a proteger la privacidad de los datos y por ende minimizar los posibles riesgos de alteración, modificación o reemplazo de la información.

Los elementos fundamentales de la seguridad informática son:

---

[1] Referencias:
Jara, H., y Pacheco, F. G. (2012). *Ethical hacking 2.0*. (1ª ed.). Buenos Aires: Fox Andina.
Sandoval Méndez, L., y Vaca Herrera, A. (2013). *Implantación de Técnicas y Administración de Laboratorio para Investigación de Ethical Hacking*. Tesis de Ingeniería. Escuela Politécnica del Ejército, Ecuador.

- La confidencialidad, para garantizar que solo las personas autorizadas tienen acceso a la información.
- La disponibilidad, para garantizar que los usuarios autorizados tengan acceso a la información en el momento que se requiera.
- La integridad, para asegurar que la información no ha sido adulterada en el camino por personas no autorizadas, y así garantizar la exactitud y totalidad de la información.
- La autenticidad, para garantizar el origen de la información.
- Protección de la información, para reducir las probabilidades de un evento inesperado mediante la aplicación de controles.

Un activo de información es un recurso o bien económico propiedad de una empresa considerado significativo ya que puede contener importante información. En el proceso de determinar el valor de cada activo intervienen cinco factores que son[2]:

- Vulnerabilidad: es la existencia de debilidades en el sistema, diseño o errores en implementación que pueden incitar a comprometer la seguridad del sistema inesperada e indeseablemente.
- Amenaza: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño sobre los elementos de un sistema de información. Los cuatro tipos básicos de operación de las amenazas son:
    - Interrupción, hace referencia al impedimento de la comunicación entre dos entidades, lo que atenta directamente a la disponibilidad.
    - Intercepción, se da cuando los datos que son transmitidos en una comunicación entre dos entidades pueden ser vistos por un tercero, atenta contra la confidencialidad
    - Modificación: involucra a una tercera entidad entre los dos punto principales de una comunicación, permitiéndole modificar la información que se transmiten en ambas direcciones, atenta contra la integridad.

[2] Baltazár, J. M., y Campuzano, J. C. (2011). *Diseño e Implementación de un Esquema de Seguridad Perimetral para Redes de Datos*. Tesis de Ingeniería. Universidad Nacional Autónoma de México, México.

  - Fabricación: es muy similar a la modificación, solo que en ese caso la información transmitida es completamente generada por una tercera entidad, atenta contra la integridad.
- Riesgo: Un riesgo está definido como la probabilidad de que una amenaza explote una vulnerabilidad, además si una amenaza explota una vulnerabilidad se lleva a cabo un ataque.
- Ataques: es un asalto en la seguridad del sistema que esta derivada desde una amenaza. Un ataque es cualquier acción que viola la seguridad.
- Control: se define como una medida de protección empleada, un control es un dispositivo, acción, procedimiento o técnica que elimina o reduce una vulnerabilidad.

1.2.HACKING ÉTICO[3]

1.2.1. Introducción al Hacking Ético

El crecimiento progresivo del uso de la tecnología ha traído muchas ventajas a todos los usuarios de internet, hoy en día se tienen muchas aplicaciones en línea con lo cual ya no es necesario realizar trámites físicamente; pero a la vez este uso de aplicaciones o servicios que una organización ofrece a los usuarios ha llamado la atención de delincuentes informáticos, los cuales están más organizados, y también van adquiriendo día a día habilidades más especializadas para lograr sus objetivos y obtener mayores beneficios.

A medida que la tecnología ha avanzado los ataques o intrusiones pasaron de ser una simple ralentización de un equipo a causar daños mayores (daños de sistemas, robo de información, fraude informático, entre otros.) y con importantes pérdidas económicas. Para los administradores de las redes esto causa un desafío de seguridad por lo que en un intento por frenar estos daños

[3] Referencias:
Jara, H., y Pacheco, F. G. (2012). *Ethical hacking 2.0*. (1ª ed.). Buenos Aires: Fox Andina.
Tori, Carlos. (2008). *Hacking Ético.*(1ª ed.). Rosario: El autor.
Certified Ethical Hacker Review Guide. Recuperado de: http://www.it-docs.net/ddata/863.pdf
Reyes, Alejandro. (2010). *Ethical Hacking.* Recuperado de:
http://www.seguridad.unam.mx/descarga.dsc?arch=2776

restringen los accesos, pero a la vez esto conlleva a que los delincuentes informáticos utilicen ataques más dañinos y estructurados.

Es por ello que la seguridad de toda empresa es esencial para mantener protegidos todos los datos, sistemas y servicios. La información que fluye de una organización pueden ser divulgadas perdiendo confidencialidad de la misma. Es así que muchas organizaciones, optan por contratar expertos para implementar técnicas de intrusiones bajo un ambiente controlado con el fin de conocer cómo se puede infiltrar en la red un atacante real, esta simulación permite encontrar brechas en la seguridad, las cuales pueden ser usadas para manipular información o suplantar identidades. Como resultado de estas pruebas, los administradores podrán realizar mejoras en las configuraciones, accesos e incluso un rediseño para reparar las fallas.

Hacking ético es un conjunto de técnicas que se utiliza para evaluar la seguridad de una red, medir la estrategia de defensa contra vectores de ataques[4] reales, mejorar la seguridad de los sistemas informáticos e identificar las vulnerabilidades de la red para luego analizarlos, medir su nivel de riesgo y recomendar soluciones apropiadas antes de que ocurra pérdida o robo de información.

Se puede decir que una definición completa y concisa de hacking ético es la del autor Alejandro Reyes Plata, que explica lo siguiente:

> El objetivo fundamental del Ethical Hacking (hackeo ético) es explotar las vulnerabilidades existentes en el sistema de "interés" valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc. Con la intención de ganar acceso y "demostrar" que un sistema es vulnerable, esta información es de gran ayuda a las organizaciones al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados. Dicho lo anterior, el servicio de Ethical Hacking consiste en la simulación de posibles escenarios donde se reproducen ataques de manera

[4] Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

> controlada, así como actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que: "Para atrapar a un intruso, primero debes pensar como intruso" (Reyes, 2010, p. 1).

Así mismo, se puede decir que una definición muy acertada de hacker ético es la del autor Pekka Himanen en su libro “La ética del hacker y el espíritu de la era de la información”, que explica lo siguiente:

> En el centro de nuestra era tecnológica se hallan unas personas que se autodenominan hackers. Se definen a sí mismos como personas que se dedican a programar de manera apasionada y creen que es un deber para ellos compartir información y elaborar software gratuito. No hay que confundirlos con los crackers, los usuarios destructivos cuyo objetivo es el de crear virus e introducirse en otros sistemas: un hacker es un experto o un entusiasta de cualquier tipo que pude dedicarse o no a la informática. La ética del trabajo para el hacker se funda en el valor de la creatividad, y consiste en combinar la pasión con la libertad. El dinero deja de ser un valor en sí mismo y el beneficio se cifra en metas como el valor social y el libre acceso, la transparencia y la franqueza (Himanen, 2002, p. 2).

De aquí que los valores fundamentales de un hacker ético sean: pasión, libertad, conciencia social, verdad, anti-corrupción, igualdad social, libre acceso a la información, accesibilidad, actividad, creatividad, curiosidad, interés, preocupación responsable, entre otros.

1.2.2. Tipos de Hackers

- Hacker de sombrero negro o crackers

  Son las hackers maliciosos o delincuentes informáticos, conocidos como crackers, estas personas buscan continuamente romper las seguridades de un sistema de información para provocar daños con beneficios personales y/o monetarios. Estos delincuentes informáticos por lo general buscan el camino de menor resistencia, ya sea por alguna vulnerabilidad, un error humano o cualquier tipo de fallo en la seguridad.

- Hacker de sombrero gris

  Son aquellos que dependiendo de las circunstancias trabajan en ocasiones de manera ofensiva y otras de manera defensiva, ocasionalmente superan los límites de la legalidad.
- Hacker de sombrero blanco

  Son aquellos que utilizan sus habilidades con fines defensivos, de manera que en base a sus destrezas pueden localizar amenazas e implementan contramedidas
- Hacker Ético

  Los hackers éticos son los profesionales de seguridad con amplios conocimientos y habilidades, los cuales realizan ataques a los sistemas informáticos en nombre de los propietarios, esto en busca de fallos de seguridad con la finalidad de proporcionar un informe con todas las vulnerabilidades encontradas y posibles remediaciones.

1.2.3. Tipos de Pruebas de Penetración

Las pruebas de intrusión se enfocan principalmente en las siguientes perspectivas:

- Pruebas de penetración con objeto: se buscan vulnerabilidades en elementos específicos de los sistemas informáticos críticos de la organización.
- Pruebas de penetración sin objeto: esta prueba consisten en examinar la totalidad de los componentes de los sistemas informáticos presentes en la organización.
- Pruebas de penetración ciega: se utiliza únicamente la información pública disponible. Esta prueba de penetración trata de simular los ataques de un ente externo a la organización.
- Pruebas de penetración informadas: aquí se utiliza la información privada, otorgada por la organización acerca de sus sistemas informáticos. En este tipo de pruebas se trata de simular ataques realizados por usuarios internos de la organización que tienen determinado acceso a información privilegiada.

- Pruebas de penetración externas: son realizadas desde lugares externos a las instalaciones de la organización. El objetivo de esta prueba es evaluar los mecanismos perimetrales de seguridad informática de la organización.
- Pruebas de penetración internas: es realizada dentro de las instalaciones de la empresa con el objetivo de evaluar las políticas y los mecanismos internos de seguridad de la organización.

1.2.4. Modalidades de Hacking Ético

- Hacking ético externo caja blanca: la organización nos facilita información de la infraestructura para poder realizar las pruebas, normalmente direcciones IP. El resultado es un informe de todas las vulnerabilidades halladas así como un conjunto de recomendaciones para solucionar cada una de ellas.
- Hacking ético externo caja negra: principalmente es igual que la modalidad de caja blanca, con la diferencia que la organización no facilita ningún tipo de información. Esta modalidad es la que se lleva a cabo en el desarrollo del presente proyecto.
- Hacking ético interno: se examina la red desde adentro, para hacer frente a la amenaza de intento de intrusión, bien por un empleado que pueda realizar un uso indebido o una persona con acceso a los sistemas o un hacker que hubiera conseguido penetrar en la red.

1.2.5. Fases del Hacking Ético

Un ataque se lleva a cabo mediante cinco fases, conocido también como el círculo del hacking, los cuales son reconocidos por *Certified Ethical Hacker*[5]-Certificado Hacker Ético:

[5] El Certificado Hacker Ético es una certificación profesional proporcionada por el Consejo Internacional de Comercio Electrónico (EC-Council).

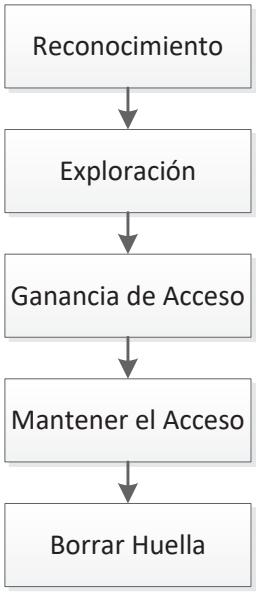


Figura 1.1 Fases del hacking ético

1.2.5.1. Reconocimiento

Es la fase de preparación en la cual se busca recolectar toda la información esencial del objetivo mediante el uso de diferentes herramientas y técnicas. Existen dos tipos de reconocimiento que son:

- Reconocimiento Pasivo

  El reconocimiento pasivo implica la recolección de la información sin tener un contacto directo o conocimientos particulares del blanco a atacar. Este tipo de reconocimiento puede ser tan simple como vigilar un edificio para ver la entrada y salida de los empleados de la organización. Sin embargo este tipo de reconocimiento se lo hace a través de la web, en busca de información sobre una organización o una persona.
- Reconocimiento Activo

  El reconocimiento activo implica la recolección de la información mediante el contacto directo con el objetivo, esto implica un sondeo de la red para descubrir direcciones IP's, hosts, servicios que se ejecutan en la red. Este reconocimiento aumenta el riesgo de ser detectado.

El reconocimiento activo como el pasivo son de gran importancia, debido a la información que se obtiene.

Esta fase es en la que normalmente les toma más tiempo a los hackers ya que de esta depende la estrategia que se utilizará para realizar los siguientes pasos. Por lo general es relativamente fácil descubrir qué tipo de servidores web se están utilizando así como los sistemas operativos que emplea una organización. Esta información permite encontrar alguna vulnerabilidad relacionada con la versión del sistema operativo y explotar la debilidad para obtener acceso al sistema.

1.2.5.2. Exploración (Escaneo)

Esta etapa depende de la información obtenida en la fase de reconocimiento para explorar una red y lanzar un ataque mediante la identificación de vulnerabilidades. Las herramientas que suele usarse en esta fase pueden incluir: escaneo de puertos, mapeadores de red, barridos, escáner de vulnerabilidades.

1.2.5.3. Ganancia de Acceso

En esta fase es donde realmente entra el desempeño de un Hacker, ya que aquí es donde las vulnerabilidades encontradas en las etapas anteriores son explotadas para tener acceso a un sistema. En esta etapa el hacker puede escalar privilegios para obtener un completo control del sistema, así los sistemas intermedios que están conectados a la red también se encuentran comprometidos.

Los ataques pueden ser a nivel de: sistema operativo, red, aplicaciones web, destrezas o mediante el aprovechamiento de configuraciones por defecto o mal configuradas.

Algunos tipos de ataques pueden ser: desbordamiento de búfer (Buffer Oveflow), denegación de servicio (DoS Denial of Service), secuestro de sesión (Session hijacking), romper o adivinar claves usando varios métodos como ataques de fuerza bruta o ataques diccionarios (Password cracking), ataques Man-in-the-middle.

1.2.5.4. Mantener el Acceso

Una vez que se ha conseguido el acceso al sistema comprometido lo que se busca es mantener ese acceso para futuras intrusiones o ataques, esto se puede realizar mediante el uso de puertas traseras (backdoors), troyanos o rootkits[6]. En esta etapa el hacker puede usar algunas herramientas como sniffers para capturar todo el tráfico de la red incluyendo sesiones de Telnet y FTP.

En esta etapa se puede tener la habilidad de subir, bajar, modificar o manipular cualquier tipo de archivos, alterando el funcionamiento de las aplicaciones y configuraciones de los sistemas operativos.

Todos los sistemas comprometidos se pueden utilizar para futuros ataques.

1.2.5.5. Borrado de Huellas

Una vez que el hacker ha ganado el acceso lo que hace, es descubrir y destruir todo la evidencia de sus actividades, esto con el efecto de mantener el acceso y seguir usando el sistema comprometido, para eliminar evidencias de la violación al sistema y/o para evitar acciones legales.

1.2.6. Beneficios del Hacking Ético

Mediante prácticas de hacking ético es posible detectar el nivel de seguridad de una organización, las cuales son las mismas metodologías que usaría un atacante real, de esta forma se podrá medir el grado de exposición que se tiene.

Las pruebas de penetración realizadas por un hacker ético se enfocan en clasificar y comprobar las vulnerabilidades, mas no en el impacto que estas representen a la organización. De aquí que el hacking ético debe ser un paso previo al análisis de seguridad o riesgos.

---

[6] **Rootkit** es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

Al finalizar las pruebas de penetración los resultados son entregados mediante un documento que contiene una lista detallada de las vulnerabilidades encontradas, a la vez que se provee recomendaciones para solucionar los fallos de seguridad. Es importante la entrega de un informe tanto técnico como ejecutivo, de esta manera se garantiza que los empleados técnicos como los administrativos entiendan y tomen conciencia de los riesgos potenciales que la organización presenta y así poder tomar medidas preventivas.

Los beneficios que se obtienen al realizar un hacking ético son muchos, pero de manera general los más importantes son:

- Ofrecer un panorama muy claro acerca de las vulnerabilidades encontradas, lo cual sirve para que se puedan aplicar medidas correctivas a tiempo.
- Deja al descubierto configuraciones no adecuadas en aplicaciones instaladas en los sistemas (routers, servidores, firewall, sistemas de cómputo, switches) los cuales pueden desencadenar graves problemas de seguridad.
- Identificación de fallas en sistemas a falta de actualizaciones.
- Disminuir el tiempo de respuesta requerido para afrontar situaciones adversas.

Cabe mencionar que es muy importante tener en cuenta los aspectos legales en la realización de un hacking ético los cuales deben tenerse muy presentes tanto por las organizaciones que prestan el servicio como por quienes lo contratan, estos aspectos abarcan la confidencialidad, es decir que a la información que se obtenga de la realización de estas pruebas no se le dé un mal manejo o uso más allá de los fines previstos por las pruebas.

En lo que respeta a la organización que contrata el servicio, esta debe garantizar que la información que se provee de las pruebas de penetración es fidedigna para que los resultados sean congruentes y certeros.

1.3.METODOLOGÍAS DE HACKING ÉTICO

Aun sabiendo que la información de una empresa es el activo más valioso, existen fallos de seguridad en la administración, lo cual genera la necesidad de realizar un análisis de los sistemas y verificar si se han cerrado o mitigado las brechas de seguridad. Los encargados de tecnología o directores de área, recurren a grupos de profesionales que ejecuten un análisis de seguridad realizando diferentes pruebas y ataques controlados para poner a prueba dicha seguridad, y verificar si los sistemas son vulnerables a algún tipo de intrusión y evaluar los tiempos de respuesta de las organizaciones ante un ataque real.

Todos los datos recopilados y procesados por los profesionales encargados de realizar la evaluación de vulnerabilidades tienen como base diferentes metodologías de hacking ético hoy por hoy existentes, con el fin de mantener un orden en su ejecución sin descuidar ningún punto de la red, con una correcta y clara presentación de la información obtenida, entre las metodologías más importantes tenemos: OSSTMM, ISSAF, OWASP.

1.3.1. OSSTMM[7]

Manual de la Metodología Abierta de Testeo de Seguridad por su siglas en ingles OSSTMM (Open-Source Security Testing Methodology Manual), es una metodología de pruebas de seguridad ejecutadas en los diferentes niveles de operación.

Este proyecto inicia en el año 2000 con un crecimiento y aceptación por los canales de seguridad. Para el año 2005, OSTMM ya no es considerado solo un marco de mejores prácticas, sino que se convirtió en una metodología para asegurar la seguridad del nivel de operación. En el 2006, el OSSTMM pasa de ser un test en soluciones de firewall y routers a ser un estándar.

Hoy por hoy el ambiente de redes en las organizaciones tiende a ser cada vez más complejo y con infraestructura de diferentes tipos, con la introducción al mercado de las telecomunicaciones de soluciones como; operaciones remotas, virtualización, cloud computing, etc. Las metodologías para una evaluación de

[7] Herzog, Peter. *OSSTMM 3 Open Source Security Testing Methodology Manual, Contemporary Security Testing and analysis*. ISECOM.

vulnerabilidades tiene que ajustarse a dichos requerimientos, para lo cual la OSSTMM realizó algunos cambios en sus versiones y de esta manera cubre pruebas para diferentes ambientes o canales, los cuales son: humano, físico, inalámbrico, telecomunicaciones y redes de datos.

Este manual proporciona un marco común y un estándar permitiendo realizar paso a paso las tareas necesarias para que tanto administradores como profesionales de la seguridad lo utilicen para analizar y ejecutar pruebas de intrusión en los sistemas de redes, con el fin de evaluar los niveles de seguridad informática, y plasmar los resultados de una manera cuantificable.

Su principal propósito está centrado en proporcionar un manual científico para la caracterización precisa de seguridad operacional (OpSec), mediante el análisis y la correlación de los resultados de prueba en una forma confiable y consistente. Algo que se destaca a gran escala de este manual, es su adaptabilidad para cualquier tipo de auditoría, incluyendo pruebas de penetración, hacking ético, análisis de vulnerabilidades, análisis de seguridad, red-teaming[8], blue-teaming[9], entre otras.

El contenido del Manual OSSTMM tiene una estructura dividida por 15 capítulos, con los cuales cubre todos los requisitos necesarios para realizar un buen trabajo de evaluación y auditoría de la seguridad de la información.

Los tres primeros capítulos brindan una base teórica para nivelar conocimientos y fundamentar el contenido futuro que posee el manual, de igual manera hace referencia a la terminología principal empleada en dicho manual, como también directrices para poder aprovechar al máximo los lineamientos de la metodología, a tal punto de realizar un trabajo de un alto nivel y con resultados óptimos para la infraestructura evaluada y respetando los acuerdos planteados de ambas partes.

[8] Red-Teaming: prueba encubierta, en donde sólo un grupo selecto de directores sabe de ella. Esta prueba es la más real y evita se realicen cambios de última hora que hagan pensar que hay un mayor nivel de seguridad en la organización.

[9] Blue-Teaming: el personal de informática conoce sobre las pruebas.

El manual ha optado por dividir el análisis en tres clases, los cuales a su vez se dividen en 5 canales diferentes con los cuales cubren todos los frentes de vulnerabilidad que se puedan presentar, de la siguiente manera:

CLASES	CANALES	DESCRIPCIÓN
Seguridad Física (PHYSSEC)	Humano	Comprende el elemento humano de la comunicación donde la interacción puede ser física o psicológica.
	Físico	Pruebas de seguridad física donde los canales son físicos y de naturaleza no-electrónica. Comprende el elemento tangible de seguridad donde la interacción requiere esfuerzo físico o un transmisor de energía para manipular.
Seguridad del Espectro (SPECSEC)	Wireless	Comprende todas las comunicaciones, señales, y emanaciones que tienen lugar sobre el espectro electromagnético conocido. Esto incluye la seguridad de comunicaciones electrónicas (ELSEC[10]), seguridad de señales (SIGSEC[11]) y seguridad de emanaciones (EMSEC[12]).

[10] ELSEC, son las medidas para negar el acceso no autorizado a la información derivada de la intercepción y el análisis de las radiaciones de comunicaciones electromagnéticas.
[11] SIGSEC, son las medidas para proteger las comunicaciones inalámbricas de accesos no autorizados.
[12] EMSEC, son las medidas para prevenir las emanaciones de las máquinas, que de ser interceptado y analizado podría revelar información transmitida, recibida y ser manipulada o de otro modo ser procesada por equipos de sistemas de información.

CLASES	CANALES	DESCRIPCIÓN
Seguridad de Comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicaciones, digitales o analógicas, donde la interacción tienen lugar a través del teléfono establecido o líneas de la red de telefonía similar.
	Redes de Datos	Comprende todos los sistemas y redes de datos electrónicos, donde la interacción tiene lugar a través de cable establecido y líneas de la red de cable.

Tabla 1.1 Canales de la Metodología OSTMM

El manual OSSTMM maneja un modelo llamado OPSEC[13], el cual se superpone sobre los objetivos para análisis de vectores y canales, es simple de aplicar, debido a que se realiza un conteo de los controles para cada punto interactivo de acceso o confianza, algo muy importante en este manual, es la cuantificación de la superficie de riesgo, la cual se realiza por medio del RAV, esta escala de medida ayuda a cuantificar la cantidad de interacciones incontroladas con el objetivo de evaluación y es calculado por el equilibrio cuantitativo entre operaciones, limitaciones y controles, es importante aclarar que RAV, no mide el riesgo para la superficie de ataque, más bien permite su medida.

Una vez entendido el manejo del manual con sus parámetros y su terminología, dedica un capítulo a cada canal (Humano, Físico, Wireless, Telecomunicaciones, Redes de Datos), dentro del cual se revisan cuatro fases: fase de introducción, fase de interacción, fase de encuesta y fase de intervención. Cada fase presenta diferente grado de profundidad en la auditoría pero cada uno de ellas no es menos importante que otra.

[13] OPSEC (seguridad operacional) es un proceso analítico que clasifica los activos de información y determina los controles necesarios para proteger estos activos.

Finalmente en el capítulo 13 podemos encontrar la presentación de reportes de auditoría de pruebas de seguridad o también conocido como STAR (Security Test Audit Report), por su siglas en inglés, con el cual se presenta un resumen ejecutivo con las actividades realizadas y plasmando los resultados obtenidos.

1.3.2. ISSAF[14]

Marco de evaluación de la seguridad del sistema de información, más conocido como ISSAF (Information Systems Security Assessment Framework), por sus siglas en inglés, fue desarrollado por la OISSG para cubrir las necesidades de organizaciones o empresas que se desenvuelven en un ambiente donde su información es un activo más de la empresa. Muchas empresas descuidan la seguridad de la información, tratando de alcanzar sus metas, es aquí donde OISSG enfoca sus objetivos al desarrollar ISSAF, ofreciendo nuevas capacidades de negocios con la integración de la tecnología al desarrollo de actividades empresariales.

ISSAF es un documento de referencia para la evaluación de la seguridad que estandariza los procesos de pruebas de los sistemas de seguridad, una de sus grandes diferencias con respecto a otros documentos o manuales de evaluación de vulnerabilidades, es que en este documento se encuentra no solo una guía paso a paso de cómo llevar un análisis de la seguridad sino que también facilita las herramientas que muy probablemente entregue la información necesaria para llenar las distintas plantillas de este documento, también indica el cómo y el por qué las medidas de seguridad deberían ser evaluadas.

ISSAF está dirigido a: asesores de vulnerabilidades internas o externas, responsables de la seguridad perimetral, ingenieros y consultores de seguridad, administradores de proyectos de evaluación de seguridad, administradores de redes y sistemas, técnicos y administradores funcionales, grupo de seguridad de la información.

---

[14] OISSG (Open Information Systems Security Group), *Infomation Systems Security Assessment Framework (ISSAF)* Draft 0.2.1, Date: April 30, 2006

El marco de referencia de ISSAF se encuentra desarrollado por 5 fases definidas como: planeación, evaluación, tratamiento, acreditación y mantenimiento, con lo cual estructura la gestión de la seguridad y asegura la viabilidad de compromisos orientados al trabajo, por otro lado presenta un marco de referencia para gestión de compromisos que definen acuerdos con el cliente sobre las tareas a realizar en el proyecto de análisis y explotación de vulnerabilidades, también contiene una sección de mejores prácticas que ayudan a su implementación.

Es muy importante los primeros 9 capítulos para la ejecución del proyecto de análisis debido a que los mismos hacen referencia al marco teórico, se da una visión general de la metodología ISSAF así como sus objetivos, presenta la gestión de contratos y acuerdos donde se especifican consejos claros a tomar en consideración a la hora de implementar el proyecto, se realiza una evaluación del riesgo enfocado al beneficio de la empresa evaluando sus activos y su criticidad de operación. Los capítulos 7, 8, 9 son guías de evaluación para determinar o identificar el nivel de las políticas de seguridad establecidas en las organizaciones, así mismo, presenta modelos de políticas.

En la sección de evaluación de seguridad y control técnico se implementa la metodología de pruebas de penetración, la misma que se divide en 3 fases, conformadas por:

- Fase I: Planeación y preparación.
  Esta fase comprende los pasos iniciales para realizar las pruebas: entrevistas para intercambiar información, planificación, alcance, escalada de privilegios, realización del cronograma, especificación del equipo que trabajará, tiempos de pruebas, entre otros arreglos. Todo esto con el fin de realizar el acuerdo que será firmado entre ambas partes y de esta manera tener la base de trabajo y una protección jurídica.
- Fase II: Evaluación.
  Esta fase a la vez se divide en: recopilación de la información, mapeo de la red, identificación de vulnerabilidades, penetración, ganancia de

acceso y escalamiento de privilegios, enumeración, comprometer usuarios/sitios remotos, mantener el acceso, cubrir pistas.

- Fase III: Reporte, limpieza y destrucción de huellas.
  Esta fase final consiste de un reporte bien estructurado que contenga el resumen de la gestión, alcance, herramientas utilizadas, cronograma real de las pruebas, resultados de las pruebas, así como recomendaciones para remediar los fallos encontrados. Además toda la información que se ha obtenido debe ser borrada al finalizar el trabajo así como se deberán borrar todas las huellas.

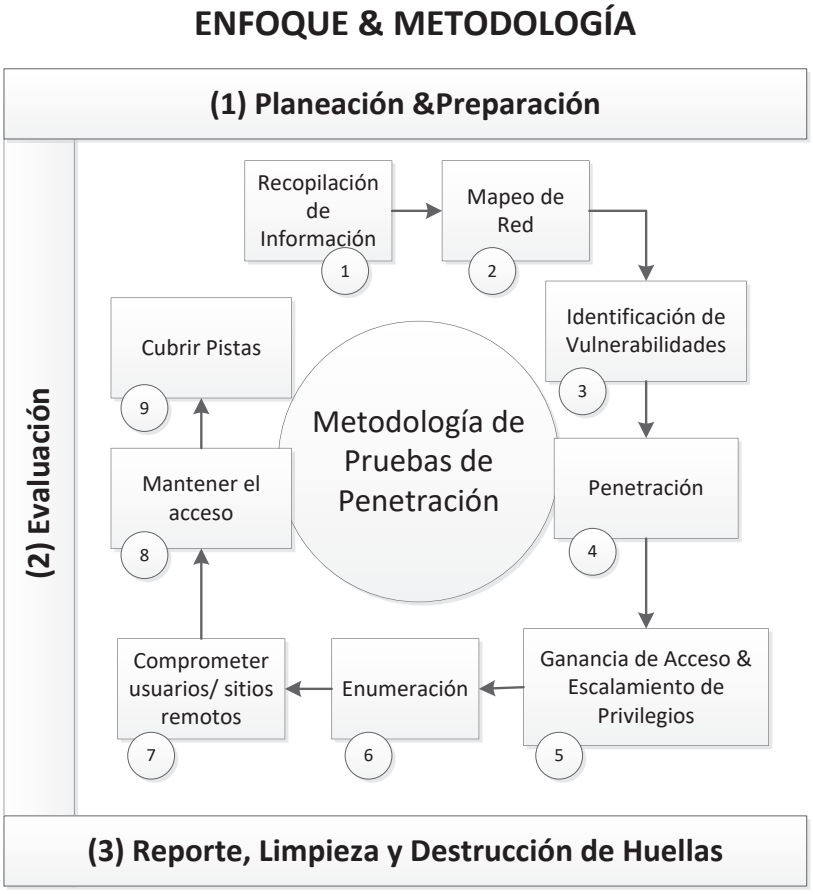


Figura 1.2 Metodología ISSAF

En la parte final del manual se realiza un análisis de la seguridad física, ingeniería social, gestión de operaciones de seguridad, gestión de cambios, concientización de la seguridad, gestión de incidentes.

1.3.3. OWASP[15]

El Proyecto Abierto de Seguridad de Aplicaciones Web o más conocida como OWASP (Open Web Application Security Project) por sus siglas en inglés, es un proyecto abierto a nivel mundial enfocado en mejorar la seguridad en software de aplicaciones, motivando y fomentando de esta manera a los desarrolladores independientes y desarrolladores adjudicados a alguna organización, a elaborar su trabajo brindando confiabilidad en las aplicaciones desarrolladas para el desempeño de negocios.

El mundo está lleno de aplicaciones web, y por tal razón se requiere de un estándar de desarrollo que permita llevar de manera ordenada todo el contenido de internet, si se realiza un análisis de las actividades en línea que efectúa una persona a lo largo de su vida día tras día, se puede evidenciar que la tecnología nos ha facilitado bastantes procesos, como: pago de servicios básicos, acceso a correo, trasferencias, acceso a documentación, etc., incluso se realiza todo esto desde algún aplicativo instalado en teléfono inteligente. Sin embargo, si cada usuario conociera el verdadero riesgo que conlleva utilizar estos aplicativos celulares o computacionales muy probablemente no lo utilizaría, pero tal acción se interpretaría como dar un paso atrás para el desarrollo tecnológico. Es esa la razón crucial de brindar confianza al usuario final para utilizar un programa, y aun sabiendo que los desarrolladores son personas con defectos y virtudes, es muy probable que cometan errores dentro de sus incontables líneas de código al elaborar las tan anheladas aplicaciones. Habiendo tomado este referente se nos hace racional enfocarnos en la seguridad de la información y la seguridad de los códigos fuente que ponemos a disposición del mundo.

OWASP es una comunidad abierta formada por un grupo de voluntarios apasionados por la seguridad informática dedicados a colaborar con la corrección y evolución de aplicaciones web, que relaciona los errores que normalmente se realiza a nivel de código de aplicaciones por los desarrolladores de los mismos, para evaluar los riesgos que puede generar

[15] OWASP Open Web Application Security Project, testing Guide 4.0, 2014 The OWASP Foundation.

estos errores a la empresa y genera un plan de corrección de las aplicaciones encontradas con riesgos.

Al momento el manual de OWASP se encuentra en la versión 4, liberada en el 2014, la misma que mejora la versión anterior en tres aspectos fundamentales:

- Implementación de la guía de desarrolladores y la guía de revisión de código, con el fin de evaluar los controles de seguridad descritos en la propia guía del desarrollador
- Introducción de cuatro nuevos capítulos y controles con un alcance de 87.
- Finalmente alienta a la comunidad a compartir sus experiencias y evaluaciones con el fin de mejorar y ampliar la base del conocimiento

La guía OWASP se encuentra formada por 5 capítulos para su interpretación e implementación: prefacio, características de la guía de pruebas, marco de pruebas de OWASP, pruebas de seguridad de aplicaciones web y reportes.

Para un mejor entendimiento del manual, se introduce un capítulo que sirve como marco teórico el mismo que cubre aspectos importantes además de indicar que es la guía OWASP, también cubre fundamentos importantes de la seguridad informática, gestión de riesgos, pruebas de penetración, entre otras.

Se dedica un capítulo que se enfoca principalmente al personal del área de desarrollo, enfocándose a presentar una guía de un modelo genérico de desarrollo, el cual los lectores deberían seguirlo de acuerdo al proceso de la organización, este modelo se divide en 5 faces de implementación: antes de comenzar el desarrollo, durante la definición y diseño, durante el desarrollo, durante la implementación, mantenimiento y operaciones.

La metodología dedica un capítulo muy importante a la hora de realizar pruebas de seguridad sobre las aplicaciones que se encuentran en producción o que están en proceso de sacar a producción, el mismo tiene como objetivo probar y explicar cómo las pruebas de vulnerabilidades se evidencian dentro de la aplicación debido a la deficiencia con controles de identificación de seguridad. Este capítulo describe 12 subcategorías de la metodología de pruebas de penetración de aplicaciones web, cada una de estas subcategorías

posee la referencia necesaria para ejecutar las pruebas que se presentan, como son: un resumen, como ejecutarlas, técnicas, herramientas, entre otros, ítems que nos ayudarán a realizar las pruebas de seguridad a las aplicaciones de una manera precisa y concisa. Estas subcategorías son:

- Pruebas de introducción y objetivos.
- Pruebas para la recolección de la información.
- Pruebas para la configuración.
- Pruebas de gestión de incidentes.
- Pruebas de autenticación.
- Pruebas de autorización.
- Pruebas de gestión de sesiones.
- Pruebas de validación de ingreso.
- Pruebas de error de código.
- Pruebas para cifrado débil.
- Prueba lógica de negocios.
- Pruebas de clientes – sitio.

Finalmente tendremos un capítulo que nos guía para elaborar los reportes obtenidos durante nuestra fase de pruebas o el proceso de evaluación, es la parte más importante de nuestro trabajo debido a que es aquí donde detallamos toda la información obtenida para entregar a las autoridades pertinentes, por ende, este reporte tiene que ser lo más claro posible y resaltar todo el riesgo encontrado a lo largo de la evaluación.

1.3.4. Comparación de las Metodologías

Para la comparación de las metodologías se consideran los parámetros tomados como referencia en el proyecto de titulación “Análisis de riesgos y vulnerabilidades de la infraestructura tecnológica de la secretaria nacional de gestión de riesgos utilizando metodologías de ethical hacking”[16], las cuales se describen a continuación:

[16] Acosta Naranjo, O.A. (2013). *Análisis de riesgos y vulnerabilidades de la infraestructura tecnológica de la secretaria nacional de gestión de riesgos utilizando metodologías de ethical hacking*. Tesis de Ingeniería. Escuela Politécnica Nacional, Ecuador.

CARACTERÍSTICAS	METODOLOGÍAS		
	OSSTMM	ISSAF	OWASP
Permite realizar pruebas y análisis de seguridad a cualquier sistema informático.	SI	SI	NO
Establece requisitos previos para la evaluación.	NO	SI	NO
Define áreas de alcance.	NO	SI	SI
Contiene plantillas para realizar las pruebas.	SI	SI	SI
Detalla técnicas para cada prueba.	NO	SI	SI
Contiene pruebas de ejemplos y resultados.	NO	SI	SI
Recomienda herramientas para cada prueba.	NO	SI	SI
Presenta procesos de análisis y evaluación de riesgos.	SI	SI	SI
Define dimensiones de seguridad a evaluar.	SI	NO	NO
Enumera y clasifica las vulnerabilidades encontradas.	NO	SI	NO
Genera reportes e informes.	SI	SI	SI
Presenta contramedidas y recomendaciones.	NO	SI	NO
Contiene referencias a documentos y enlaces externos.	NO	SI	SI
Presenta Evaluación a aplicaciones Web.	SI	SI	SI
Mantiene actualizaciones al día.	SI	NO	SI
Es un estándar.	SI	NO	SI
Presenta acuerdos de confidencialidad.	SI	SI	NO

Tabla 1.2 Comparación de Metodologías.

Se puede observar en la tabla 1.2, que cada metodología presenta parámetros importantes, por lo que para la implementación del presente proyecto se considera sugerencias de cada una dependiendo de la fase que se realice.

1.4.PROTOCOLOS SIMPLES PARA GESTIÓN DE REDES[17]

Entre los protocolos para gestión de redes podemos nombrar los siguientes:

- **Protocolo de control de transmisión (TCP)**

  Es una de los principales protocolos de la capa de transporte del modelo TCP/IP. Este protocolo garantiza que los datos serán entregados a su destino sin errores y en el mismo orden en que se transmitieron, también proporciona mecanismos para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto del puerto.

  TCP está documentado en el RFC 793 y sus principales características son:

  - ✓ Orientado a la conexión: permite que dos máquinas que están comunicadas controlen su estado de la transmisión.
  - ✓ Operación Full-Duplex: una conexión TCP es un par de circuitos virtuales, cada uno en una dirección. Solo los dos sistemas finales sincronizados pueden usar la conexión.
  - ✓ Revisión de errores: una técnica de checksum es usada para verificar que los paquetes no estén corruptos.
  - ✓ Acuses de recibo: sobre el recibido de uno o más paquetes, el receptor regresa un acuse de recibo al transmisor indicando que recibió el paquete.
  - ✓ Control de flujo: si el transmisor está desbordando el buffer del receptor por transmitir demasiado rápido, el receptor descarta paquetes. Los acuses fallidos que llegan al transmisor le alertan para bajar la tasa de transferencia o dejar de transmitir.

[17] Villalobos B., V. A. (2014). Protocolos simples para gestión de redes. Recuperado de: http://es.slideshare.net/EquipoSCADA/unidad-vi-tema-8-scada

- ✓ Servicio de recuperación de paquetes: el receptor puede pedir la retransmisión de un paquete, si el paquete no es notificado como recibido.

- **Protocolo de internet (IP)**

  El protocolo IP es parte de la capa de Internet del conjunto de protocolos TCP/IP. Es uno de los protocolos de internet más importantes ya que permite el desarrollo y transporte de datagramas de IP (paquetes de datos), aunque sin garantizar su entrega. En realidad, el protocolo IP procesa datagramas IP de manera independiente al definir su representación, ruta y envío.

  Las principales características de este protocolo son:

  - ✓ Protocolo no orientado a conexión.
  - ✓ Fragmenta paquetes si es necesario.
  - ✓ Direccionamiento mediante direcciones IP lógicas de 32 bits.
  - ✓ Si un paquete no es recibido, este permanecerá en la red mediante un tiempo finito.
  - ✓ Realiza el “mejor esfuerzo” para la distribución de paquetes.
  - ✓ Tamaño máximo de paquetes de 65635 bytes.

  Solo se realiza verificación por suma al encabezado del paquete, no a los datos que éste contiene.

- **Protocolo de control de transmisión / Protocolo de internet (TCP/IP)**

  El protocolo de red TCP/IP se podría definir como el conjunto de protocolos básicos de comunicación de redes, que permite la transmisión de información en redes de ordenadores.

  En algunos aspectos TCP/IP representa todas las reglas de comunicación para internet, y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes de datos.

Debido a que el conjunto de protocolos TCP/IP originalmente se creó con fines militares, está diseñado para cumplir una cierta cantidad de criterios, entre ellos:

- ✓ Dividir mensajes de paquetes.
- ✓ Usar un sistema de direcciones.
- ✓ Enrutar datos en la red.
- ✓ Detectar errores en la transmisión de datos.

- **Protocolo UDP**

  UDP (User Datagram Protocol) es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Se limita a recoger el mensaje y enviar el paquete por la red. Para garantizar la llegada el protocolo exige a la máquina de destino del paquete que envió un mensaje (un eco), si el mensaje no llega se envía de nuevo.

  UDP es un protocolo sencillo que implementa un nivel de transporte orientado a datagramas, tiene las siguientes características:

  - ✓ No es orientado a conexión.
  - ✓ No es fiable por tres razones: pueden perderse datagramas, pueden duplicarse datagramas y pueden desordenarse datagramas.

- **Protocolo de resolución de dirección (ARP)**

  El protocolo ARP tiene un papel clave entre los protocolos de capa de internet relacionados con el protocolo TCP/IP, ya que permite que se conozca la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP, por eso se lo llama protocolo de resolución de direcciones.

  Para que las direcciones físicas no puedan conectar con las direcciones lógicas, el protocolo ARP interroga a los equipos de la red para averiguar sus direcciones físicas y luego crea una tabla de búsqueda entre las direcciones lógicas y físicas en una memoria caché.

- **Protocolo simple para la administración de red (SNMP)**

  Es un protocolo que permite administrar y diagnosticar una red. Es un estándar de administración de redes basado en un conjunto de protocolo TCP/IP, que permite la consulta a los diferentes elementos que constituyen una red.

  El sistema de administración de red se basa en dos elementos principales: un supervisor y agentes. El supervisor es el terminal que le permite al administrador de red realizar solicitudes de administración. Los agentes son entidades que se encuentran al nivel de cada interfaz. Ellos conectan a la red los dispositivos administrados y permiten recopilar información sobre los diferentes objetos.

  Toda la información de los equipos está en una base de datos MIB (Management Information Base). Esta base de datos con estructura de árbol es recogida por el agente del protocolo simple para la gestión de red y comunicada al sistema de administración de red.

1.5.HERRAMIENTAS DE HACKING ÉTICO

Para realizar una prueba de penetración es necesario sumar a los conocimientos de hacking ético, otros aspectos importantes como: metodologías, documentación, entre otros. Todos esos conocimientos vienen de la mano con las herramientas que forman parte de algunas etapas de una prueba de penetración.

De acuerdo a su funcionalidad e importancia que dan los profesionales de seguridad se mencionan algunas de las herramientas más utilizadas en pruebas de penetración, debido a que son mejor valoradas por los investigadores de seguridad para llevar a cabo auditorías de seguridad informática y de redes, así como prácticas de hacking ético:

- **Netcraft**

  Es una herramienta en línea para monitoreo, con la cual es posible identificar el tipo de servidor y el sistema operativo, tiempo de actividad

del servidor. El uso de esta herramienta es a través de un navegador y la información recopilada es de tipo pasivo.

- **Whois**

  Whois es un servicio de consulta para obtener toda la información disponible públicamente sobre cualquier nombre de dominio registrado. Estos datos Whois incluyen información como: fechas de creación y fecha de vencimiento del registro de nombres de dominio, servidores de nombre, contactos administrativos y técnicos designados, ubicación, entre otros.

- **Nslookup**

  Es un comando utilizado a través de CLI, incluido en múltiples sistemas operativos como Windows, Linux o Unix. Este comando nos permitirá hacer una resolución de nombres, en otras palabras, identificar la dirección IP.

- **Dnsenum**

  Herramienta para listar toda la información DNS acerca de un dominio y descubrir bloques de direcciones IP no continuos, su instalación y uso está disponible para Linux.

- **Fierce**

  Es una herramienta de reconocimiento, que realiza escaneo de dominios y direcciones IP no-continuas.

- **Dmitry**

  Esta herramienta recolecta información aplicando consultas whois, búsqueda de subdominios, búsqueda de direcciones de correo, etc.

- **Robtex**

  Es un sitio web, que permite encontrar información de DNS, es de uso gratuito, su modo de empleo es ingresando la dirección IP o el dominio en el sitio web de Robtex.

- **Maltego**

  Es una herramienta o plataforma que permite generar imágenes de la relación existente entre dns, direcciones ips, compañías, etc., se encuentra disponible para instalación tanto en Linux como para Windows.

  Esta herramienta puede ser usada en la fase de recopilación de información o para determinar las relaciones y enlaces entre: redes sociales, infraestructura de red, dominios, direcciones IP, DNS, bloques de red, sitios web, etc.

- **Whatweb**

  Herramienta que permite identificar tecnología utilizada en sitios web, su uso está disponible para Linux y su ejecución es a través de una consola de comandos.

- **Nmap**

  Nmap es una herramienta de escaneo de redes, se usa para auditorías de seguridad. Puede instalarse tanto en Linux, Windows y Mac.

  Nmap es una herramienta de línea de comandos donde se debe indicar cuál será él o los objetivos y la serie de parámetros que afectarán la forma en que se ejecuten las pruebas y los resultados que se obtienen.

  Nmap permite identificar qué servicios se están ejecutando en un dispositivo remoto, así como la identificación de equipos activos, sistemas operativos en el equipo remoto, existencia de filtros o firewalls. Así como escaneo de: puertos, servicios, vulnerabilidades, redes, scripts.

- **Nessus**

  Nessus es un programa de escaneo de vulnerabilidades el cual es soportado por diferentes sistemas operativos. Consiste en un demonio que realiza el escaneo en el sistema objetivo, y un cliente que muestra

el avance e informa sobre el estado de los escaneos. Desde la consola se puede realizar escaneos programados.

Algunas de sus características son: dispone de una actualización permanente, tiene reporte de riesgos con caracterización, puede escanear varias máquinas de manera simultánea, tiene la posibilidad de integrarse con otras herramientas como nmap y metaexploit.

- **Openvas**

  Es un conjunto de diferentes servicios y herramientas que ofrecen una solución completa y potente de escaneo, análisis y administración de vulnerabilidades, es libre y gratuito.

  Openvas realiza presenta un informe de las vulnerabilidades encontradas así como las posibles soluciones. Este escáner tiene un servicio de actualizaciones diarias de los test de vulnerabilidades de red y es multiplataforma.

- **Ettercap**

  Es una herramienta que nos permite capturar el tráfico que circula por una red LAN, soporta el estudio activo y pasivo de muchos protocolos e incluye características de análisis de red y host.

  Es una herramienta multiplataforma.

- **Wireshark**

  Es una herramienta multiplataforma utilizada para realizar análisis de paquetes de red, permite observar de forma detallada cabeceras de protocolos. Es muy útil para capturar y monitorizar todos los paquetes de red para poder solucionar e incluso prevenir posibles problemas.

- **Hydra**

  Esta herramienta se usa para comprobar la seguridad de las contraseñas de un sistema o red. Su funcionamiento se basa en el uso

de diccionarios, los cuales contienen todas aquellas posibles combinaciones que se quiera probar.

- **Metasploit Framework**

  Metasploit Framework es una herramienta para desarrollar y ejecutar exploits[18] contra una máquina remota. Desarrollado en Ruby, lo usan profesionales de seguridad para explotar vulnerabilidades, simular ataques. Algunas de sus características son: tiene una amplia base de datos de exploits, contiene diversos payloads de ejecución, dispone de soporte para post-explotación, permite atacar diferentes plataformas.

- **Kali-Linux**

  Kali-Linux es un sistema operativo basado en Linux Debian, el mismo que fue desarrollado a partir de la distribución backtrack, este sistema reúne una serie de herramientas preinstaladas que ayuda a los profesionales y estudiantes de seguridad informática a realizar acciones como: captura de tráfico (mediante: wireshark, yersinia, etc.), escaneo de puertos (mediante: nmap, dnmap, etc.), análisis de vulnerabilidades (mediante: nmap, openvas-scanner, etc.), explotación de vulnerabilidades (mediante: THC-Hydra, exploitdb, etc.), etc.

  Kali Linux está tomando posicionamiento en la comunidad para realizar auditorías y evaluación de seguridades, es un sistema con licencia GPL, el mismo que puede instalarse en una máquina virtual o directamente en una máquina de trabajo, también posee una versión LITE, la cual nos permite hacer una evaluación del sistema sin la necesidad de instalarlo.

[18] Exploit es un fragmento de software, fragmento de datos o secuencia de comando y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información.

CAPÍTULO II

2. ANÁLISIS DE LA RED PERIMETRAL DE LA CARTERA DE ESTADO

En este capítulo se realiza la recopilación y análisis de información tanto de la red perimetral, como aplicaciones expuestas, servidores y puertos que permitan determinar posibles vectores de ataque, además se realizará el formato de las plantillas necesarias para la documentación de la información obtenida.

Este capítulo se divide en dos secciones:

- El primero que es la fase de reconocimiento, el cual se considera la etapa más difícil y la de mayor trabajo ya que de esta dependerá la precisión de los ataques.
- La segunda indicará las plantillas que se usarán para la presentación de información de la fase de recolección.

2.1.RECOLECCIÓN DE INFORMACIÓN

La fase de reconocimiento de información es el primer paso para realizar una auditoría, evaluación o prueba de penetración sobre los sistemas de una organización, esta fase permite definir el objetivo, mapeando y averiguando sus vulnerabilidades de manera que esta información sirva para realizar un ataque.

"Cuanta más información se tenga del objetivo, mayor es la posibilidad de una explotación exitosa[19]". La fase de reconocimiento consiste en la búsqueda de toda la información pública de una entidad, ya sea porque se publicó con conocimiento o por desconocimiento, se busca todas las huellas posibles desde direcciones IP, segmentos o bloques de red, servicios TCP y UDP activos, protocolos de red, ACLs, IDSs o IPs activos, servidores internos, versiones de sistemas operativos, puertos abiertos y aplicaciones, cuentas de correo de los usuarios, nombres de máquinas activas, información del registrador del dominio, ubicación y números de teléfono, ficheros con cuentas

[19] Tomado y traducido de: "*Ethical Hacking and Penetration Testing*", página 53.

y/o credenciales de usuarios, impresoras, cámaras IP, tablas de enrutamiento, banners de sistemas, es decir se busca cualquier información útil para realizar un ataque.

Así como se obtiene conocimiento sobre nuestro objetivo a través de repositorios públicos, también es importante realizar consultas directas a los servicios, rangos de IP's, DNS, etc. Es por ello que se divide esta fase en dos técnicas de recolección de información, una pasiva y otra activa, pero ambas son útiles para adquirir información;

- **Recolección de Información Activa:** se interactúa directamente con el objetivo, por ejemplo: información de los puertos abiertos, servicios que están corriendo y que sistemas operativos se están usando. Sin embargo este tipo de recolección es muy evidente para el otro extremo, por lo tanto es muy fácil ser detectado por un IDS, IPS, firewall y además la presencia de estas actividades genera logs[20].
- **Recolección de Información Pasiva:** no se interactúa directamente con el objetivo, aquí se utiliza motores de búsqueda, redes sociales y otros sitios web. Este método es muy recomendable debido a que no genera ningún log de presencia en los sistemas.

Sin importar la técnica utilizada, aquí el objetivo es explorar todas las avenidas posibles de ataque, esto nos ayudará a tener un panorama global del objetivo y dirigir las pruebas de acuerdo a los vectores encontrados.

La recolección de información es más efectiva y útil cuando se la realiza de manera sistemática. Existen tres pasos fundamentales que se pueden seguir para realizar la fase de recolección:

[20] Un log es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema.

Figura 2.1 Diagrama de flujo - pasos para recolección de información. [21]

Es importante mencionar que en esta fase se usan herramientas que pueden proporcionar información repetitiva, esto se justifica debido a que de esta manera se compara y verifica resultados para eliminar toda aquella información que no es relevante, además cada herramienta utiliza diferentes técnicas: mientras unas realizan consultas a repositorios públicos (recolección pasiva), otras realizan consultas directas a los servidores propios de la organización (recolección activa).

La información recolectada en referencia a nombres de dominio e ip's serán modificados por motivos de confidencialidad.

2.1.1. Fuentes Públicas

Este tipo de recolección se enfoca en Inteligencia de Fuentes Abiertas OSINT (Open Source Intelligence), lo cual consiste en recolectar, procesar y analizar datos públicos con el fin de seleccionar la información que sea útil.

[21] Tomado y traducido de:*"Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide"*

Existen un sinfín de fuentes abiertas de las cuales se puede obtener información, entre las cuales se puede mencionar: medios de comunicación, información pública de fuentes gubernamentales, foros, redes sociales, blogs, bibliotecas online, etc.

2.1.1.1. Buscadores Habituales

Es importante saber qué conoce la web acerca del objetivo, por lo que se realiza consultas a motores de búsqueda comunes como: google, bing y yahoo.

Lo bueno de los motores de búsqueda es que los crawlers[22] suelen indexar información que ha sido borrada pero ha permanecido en el cache de Google.

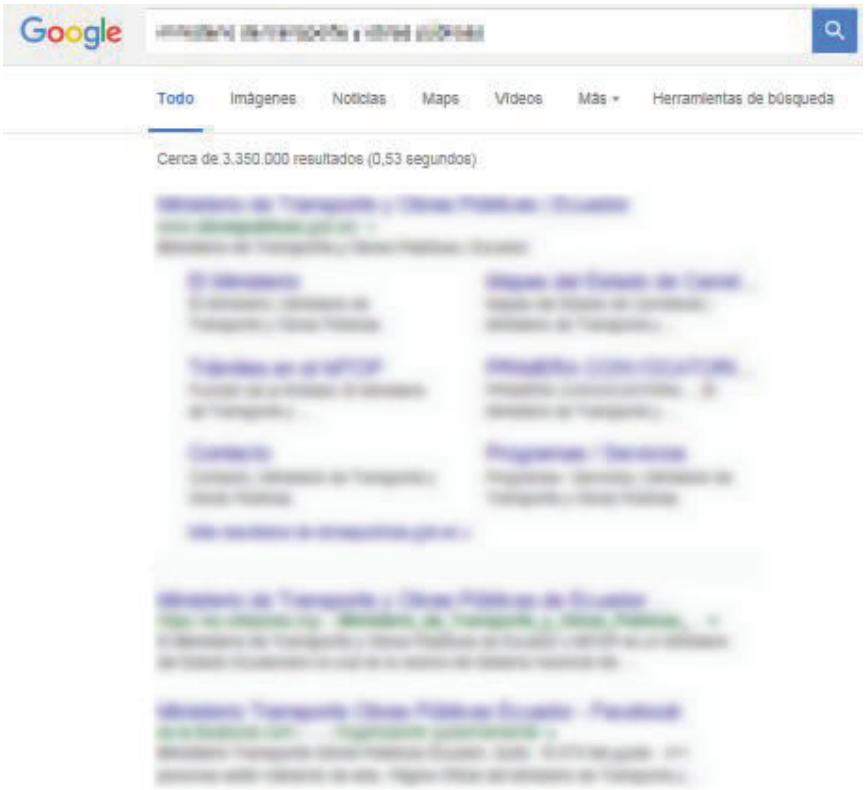


Figura 2.2 Búsqueda del objetivo realizada en Google.

[22]"Un crawler es una **pequeña pieza de software** que va por Internet siguiendo enlaces de las distintas páginas web con un sólo propósito: Tomar información y llevarla a un servidor." Tomado de: http://seoafeira.com/que-es-un-crawler/

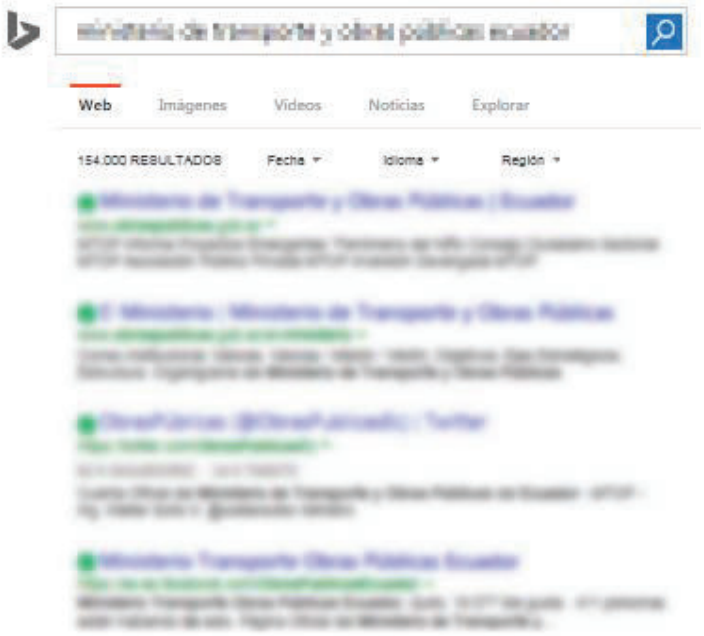


Figura 2.3 Búsqueda del objetivo realizada en Bing.

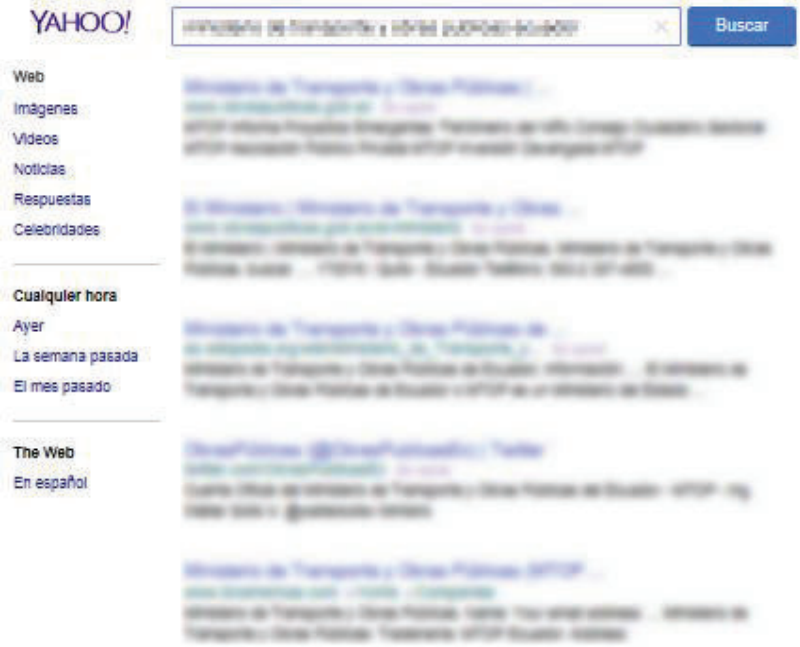


Figura 2.4 Búsqueda del objetivo realizada en Yahoo.

Mediante las búsquedas realizadas e indicadas en las figuras 2.2, 2.3 y 2.4, se obtiene como resultado el un dominio del objetivo evaluado y una palabra clave.

Se continúa con el análisis haciendo uso de búsquedas con mayor precisión, como Google Hacking[23], el cual usa operadores lógicos para encontrar información mucho más exacta.

Se han utilizado diferentes filtros pero los que dan mejores resultados son los siguientes operadores:

- site: búsqueda en un dominio específico.
- NOT (-): excluir información de la búsqueda.

Así, la sintaxis de búsqueda usada es la siguiente:

PALABRA CLAVE –site:dominio

Como resultado de la búsqueda realizada (figura 2.5) se obtienen dos subdominios:

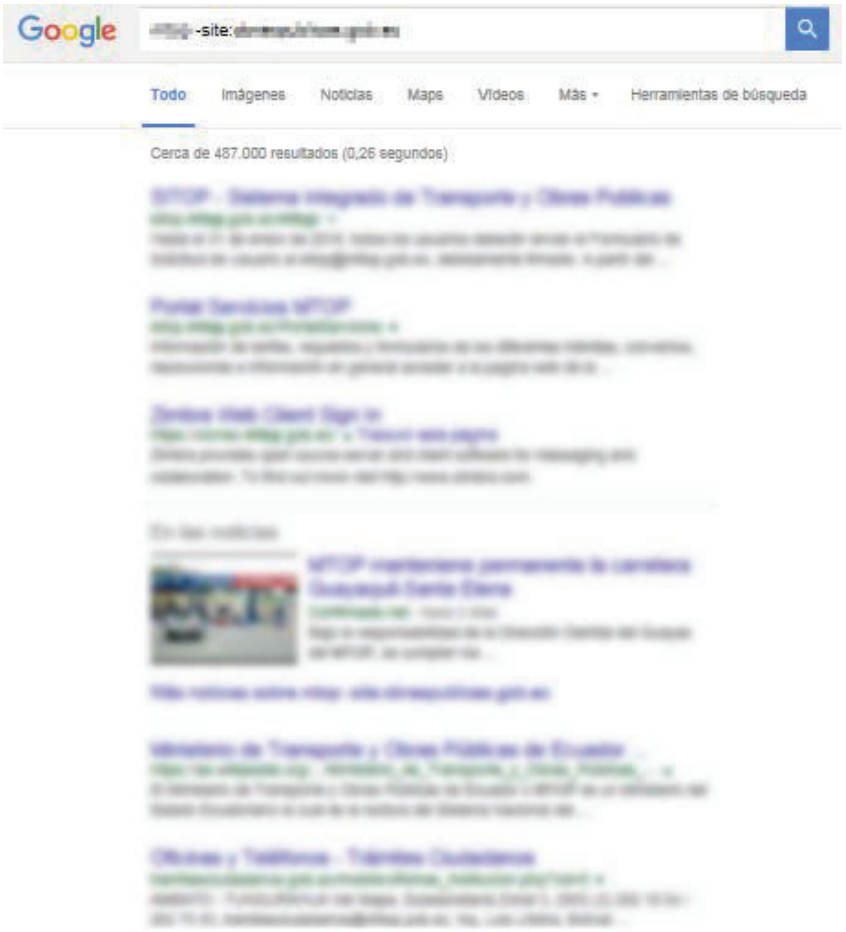


Figura 2.5 Búsqueda utilizando Google Hacking.

[23] Técnica informática que utiliza operadores para filtrar información.

2.1.1.2. Visitar el Sitio Web de la Organización

Se debe visitar el sitio web del objetivo en busca de información general, como: números de contacto, correos electrónicos, enlaces a subdominios, etc., toda información que sea útil.

Es importante mencionar que al ser el objetivo una Institución del Estado, toda la información referente a estructura de la organización, personal, directorio, direcciones de correo, remuneraciones, etc., no es de interés debido a que es información pública como lo establece la Ley de Orgánica de Transparencia y Acceso a la Información Pública[24].

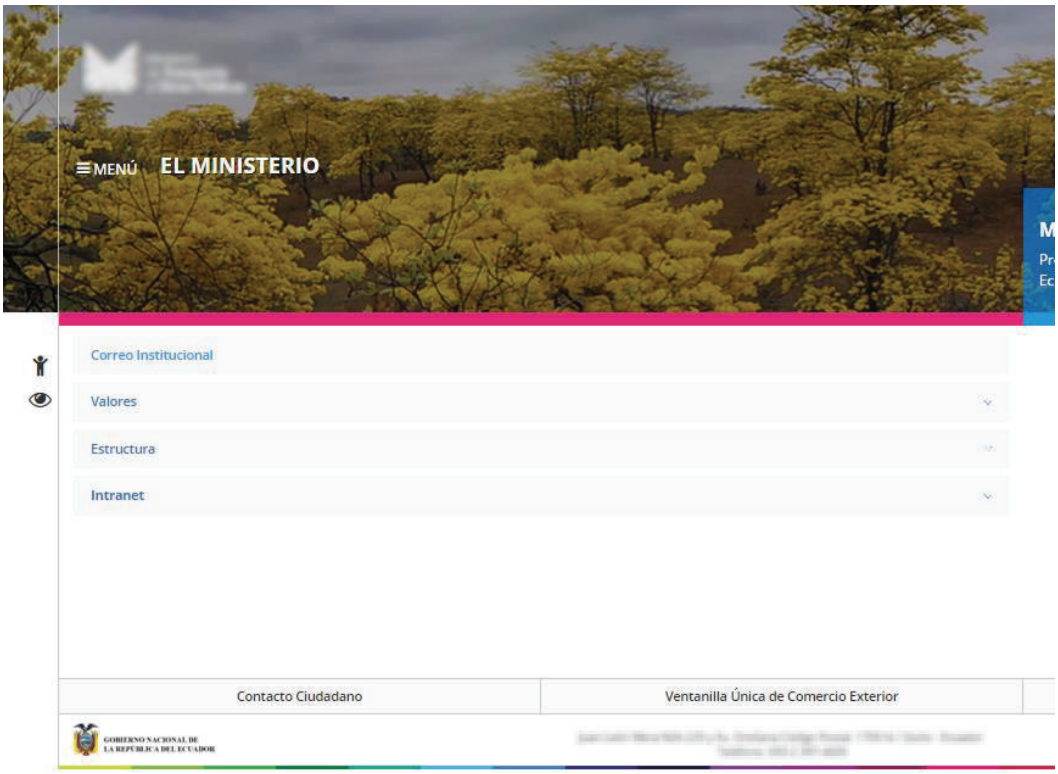


Figura 2.6 Página web del objetivo.

La figura 2.6 muestra los enlaces internos que existen en el sitio web del objetivo, indagando en los enlaces se obtiene la siguiente información:

[24] Art. 1.- Principio de Publicidad de la Información Pública.- El acceso a la información pública es un derecho de las personas que garantiza el Estado.
Las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley.

INFORMACIÓN OBTENIDA	
Dirección:	Juan León
Teléfonos:	593-2 3xxxxxx
Palabras claves:	ABC
Enlaces:	subdominio1.dominio.gob.ec subdominio2.dominio.gob.ec abc.dominio1.com
Directorio:	Nombre de empleados, cargos, área de trabajo, extensiones telefónicas.

Tabla 2.1 Resumen de la información obtenida de la página web.

Mediante los enlaces encontrados se puede identificar los dominios: subdominio1.dominio.gob.ec, subdominio2.dominio.gob.ec, abc.dominio1.com.

2.1.2. Buscadores Especializados

Otra forma de recolectar información en la Web es haciendo uso de herramientas disponibles en línea, las cuales nos permitirán obtener información del objetivo, como: direcciones IP, subdominio, servicios DNS, registradores, etc.

2.1.2.1. Netcraf

Netcraf es una herramienta que realiza un análisis de un dominio entregando información, como: sub-domino, sistemas operativos, direcciones IP, servicios Web, entre otros.

Se realiza el análisis con los dominios y subdominios encontrados anteriormente:

- dominio2.gob.ec
- subdominio2.dominio.gob.ec
- subdominio1.dominio.gob.ec
- abc.dominio1.com
- dominio.gob.ec

En las figuras 2.7 a la 2.11 se puede observar el uso de la herramienta.

Background

Site title	[redacted]	**Date first seen**	October 2012
Site rank		**Primary language**	Spanish
Description	[redacted]		
Keywords	*Not Present*		

Network

Site	http://[redacted]	**Netblock Owner**	CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP
Domain	[redacted]	**Nameserver**	root.andinanet.net
IP address	[redacted]	**DNS admin**	hostmaster@andinanet.net
IPv6 address	*Not Present*	**Reverse DNS**	202.52.152.190.static.pichincha.andinanet.net
Domain registrar	*unknown*	**Nameserver organisation**	whois.networksolutions.com
Organisation	*unknown*	**Hosting company**	Corporacion Nacional de Telecomunicaciones
Top Level Domain	Ecuador (.gob.ec)	**DNS Security Extensions**	*unknown*
Hosting country	EC		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP Quito	190.152.52.202	Linux	unknown	2-Aug-2016
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP Quito	190.152.52.202	Linux	nginx	1-Aug-2016
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP Quito	181.211.36.248	Linux	nginx	1-Apr-2016

Security

Netcraft Risk Rating [FAQ]	1/10		
On Spamhaus Block List	No	**On Exploits Block List**	No
On Policy Block List	No	**On Domain Block List**	No

Figura 2.7 Reporte de dominio2.gob.ec por netcraf.

Background

Site title	[redacted]	**Date first seen**	February 2016
Site rank		**Primary language**	English
Description	*Not Present*		
Keywords	*Not Present*		

Network

Site	http://[redacted]	**Netblock Owner**	[redacted]
Domain	[redacted]	**Nameserver**	root.andinanet.net
IP address	[redacted]	**DNS admin**	hostmaster@andinanet.net
IPv6 address	*Not Present*	**Reverse DNS**	[redacted]
Domain registrar	*unknown*	**Nameserver organisation**	whois.networksolutions.com
Organisation	*unknown*	**Hosting company**	Corporacion Nacional de Telecomunicaciones
Top Level Domain	Ecuador (.gob.ec)	**DNS Security Extensions**	*unknown*
Hosting country	EC		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen (Refresh)
[redacted]	[redacted]	Linux	Apache/2.2.25 Unix mod_ssl/2.2.25 OpenSSL/1.0.1e-fips DAV/2 mod_cluster/1.2.6.Final	8-Apr-2016

Security

Netcraft Risk Rating [FAQ]	1/10		
On Spamhaus Block List	No	**On Exploits Block List**	No
On Policy Block List	No	**On Domain Block List**	No

Figura 2.8 Reporte de subdominio2.dominio.gob.ec por netcraf.

Background

Site title	[redacted]	**Date first seen**	November 2010
Site rank		**Primary language**	English
Description	[redacted] provides open source server and client software for messaging and collaboration. To find out more visit [redacted]		
Keywords	*Not Present*		

Network

Site	http://[redacted]	**Netblock Owner**	[redacted]
Domain	[redacted]	**Nameserver**	root.andinanet.net
IP address	[redacted]	**DNS admin**	hostmaster@andinanet.net
IPv6 address	*Not Present*	**Reverse DNS**	[redacted]
Domain registrar	*unknown*	**Nameserver organisation**	whois.networksolutions.com
Organisation	*unknown*	**Hosting company**	Corporacion Nacional de Telecomunicaciones
Top Level Domain	Ecuador (.gob.ec)	**DNS Security Extensions**	*unknown*
Hosting country	EC		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
[redacted]	[redacted]	Linux	nginx	8-Apr-2016

Security

Netcraft Risk Rating [FAQ]	0/10		
On Spamhaus Block List	No	**On Exploits Block List**	No
On Policy Block List	No	**On Domain Block List**	No

Figura 2.9 Reporte de subdominio1.dominio.gob.ec por netcraf.

Background

Site title	[redacted]	**Date first seen**	February 2016
Site rank		**Primary language**	Spanish
Description	[redacted]		
Keywords	*Not Present*		

Network

Site	http://[redacted]	**Netblock Owner**	Digital Ocean, Inc.
Domain	[redacted]	**Nameserver**	dns1.nodovip.com
IP address	[redacted]	**DNS admin**	soporte@nodovip.com
IPv6 address	*Not Present*	**Reverse DNS**	srv2.rastreodirecto.com
Domain registrar	enom.com	**Nameserver organisation**	whois.enom.com
Organisation	NAMECHEAP.COM, 8939 S. SEPULVEDA BLVD. #110 - 732, WESTCHESTER, 90045, US	**Hosting company**	DigitalOcean
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	US		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Digital Ocean, Inc. 101 Ave of the Americas 10th Floor New York NY US 10013	162.243.85.68	Linux	Apache/2.2.15 CentOS	31-Mar-2016

Security

Netcraft Risk Rating [FAQ]	1/10		
On Spamhaus Block List	No	**On Exploits Block List**	No
On Policy Block List	No	**On Domain Block List**	No

Figura 2.10 Reporte de abc.dominio1.com por netcraf.

Background

Site title	*Not Present*	**Date first seen**	October 2010
Site rank		**Primary language**	English
Description	*Not Present*		
Keywords	*Not Present*		

Network

Site	http://	**Netblock Owner**	
Domain		**Nameserver**	root.andinanet.net
IP address		**DNS admin**	hostmaster@andinanet.net
IPv6 address	*Not Present*	**Reverse DNS**	
Domain registrar	*unknown*	**Nameserver organisation**	whois.networksolutions.com
Organisation	*unknown*	**Hosting company**	Corporacion Nacional de Telecomunicaciones
Top Level Domain	Ecuador (.gob.ec)	**DNS Security Extensions**	*unknown*
Hosting country	EC		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Telconet S.A Guayaquil	200.93.192.100	Linux	Apache	17-Feb-2012

Security

Netcraft Risk Rating [FAQ]	0/10		
On Spamhaus Block List	Yes	**On Exploits Block List**	Yes
On Policy Block List	No	**On Domain Block List**	No

Figura 2.11 Reporte de dominio.gob.ec por netcraf.

En resumen del análisis con la herramienta netcraf, se tienen los siguientes resultados:

SITIO	DOMINIO	DIRECCIÓN IP	SISTEMA OPERATIVO	SERVIDOR WEB
dominio2.gob.ec	dominio2.gob.ec	181.211.36.248	Linux	Nginx
subdominio2.dominio.gob.ec	dominio.gob.ec	186.47.XX.C	Linux	Apache/2.2.25 Unix mod_ssl/2.2.25 OpenSSL/1.0.1e-fips DAV/2 mod_cluster/1.2.6.Final
subdominio1.dominio.gob.ec	dominio.gob.ec	186.47.XX.A	Linux	Nginx
abc.dominio1.com	dominio1.com	162.243.85.68	Linux	Apache/2.2.15 CentOS
dominio.gob.ec	dominio.gob.ec	186.47.XX.B	Linux	Apache

Tabla 2.2 Resumen de información obtenida con Netcraf.

En base a la tabla 2.2 se identifican tres dominios:

- dominio2.gob.ec
- dominio.gob.ec
- dominio1.com

2.1.2.2. Búsqueda Whois

Whois es un servicio de consulta para obtener toda la información disponible públicamente sobre cualquier nombre de dominio registrado. Estos datos Whois incluyen información como: fechas de creación y fecha de vencimiento del registro de nombres de dominio, servidores de nombre, contactos administrativos y técnicos designados, ubicación, entre otros.

Se realiza consultas Whois, con el propósito de descartar todos aquellos dominios que no se encuentren en la dirección física del objetivo analizado, la cual se especifica en la tabla 2.2.

Figura 2.12 Consulta whois a dominio2.gob.ec

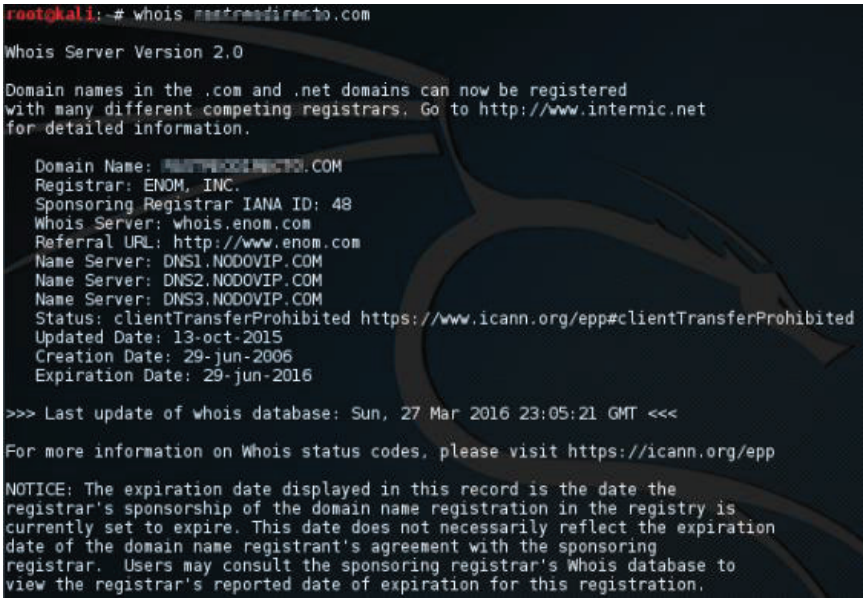


Figura 2.13 Consulta whois a dominio1.com

Figura 2.14 Consulta whois a dominio.gob.ec

Mediante el análisis whois indicados en las tablas 2.12, 2.13 y 2.14, se puede concluir que los dominios dominio2.gob.ec y dominio1.com no se encuentran alojados en la ubicación actual del objetivo, por lo que no se les utilizará en los análisis siguientes.

Los dominios y subdominios a analizar son:

Dominio y Subdominios	Dirección IP
dominio.gob.ec	186.47.XX.B
subdominio2.dominio.gob.ec	186.47.XX.C
subdominio1.dominio.gob.ec	186.47.XX.A

Tabla 2.3 Resumen de los dominios y subdominios a analizar.

2.1.3. Información de los DNS

2.1.3.1. Resolviendo Nombres con nslookup

Nslookup es una herramienta que permite consultar un servidor de nombre (DNS) y obtener información acerca del dominio o el host.

Entre las diferentes opciones que tiene nslookup, se utilizarán las siguientes:

- NS: devuelve la información respecto a los servidores de nombre de nuestro objetivo.
- MX: devuelve la información de los servidores de correo.

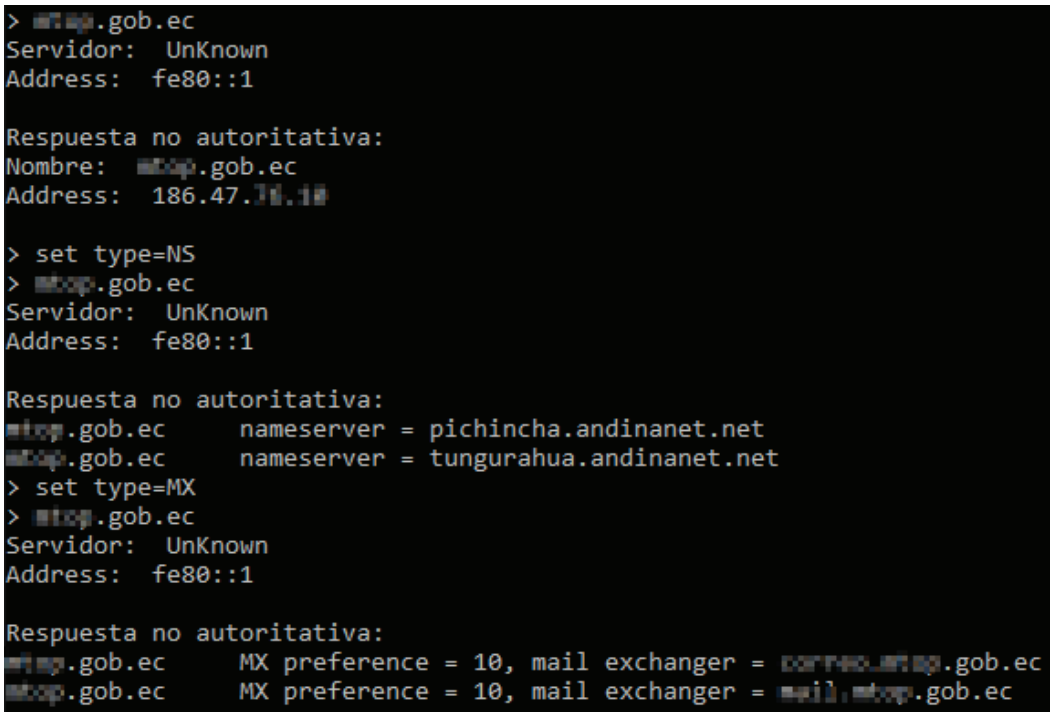


Figura 2.15 Nslookup dominio.gob.ec

Mediante las pruebas realizadas, indicadas en la figura 2.15 se obtienen los siguientes resultados:

- Dirección IP de dominio.gob.ec es 186.47.XX.B
- Servidores de nombre:
  pichincha.andinanet.net
  tungurahua.andinanet.net
- Servidores de correo del dominio: subdominio1.dominio.gob.ec, subdominio3.dominio.gob.ec

2.1.3.2. DNSENUM

Dnsenum es una herramienta creada para listar toda la información DNS acerca de un dominio, la información que nos puede proporcionar es: dirección del host, servidores de nombre, servidores de correo, búsqueda de subdominios a través de fuerza bruta, etc.

Para la consulta al objetivo utilizaremos las siguientes opciones:

- enum: Es un atajo equivalente a la opción "—thread 5 –s 15 -w". Dónde:
  - ✓ thread: define el número de hilos que realizarán las diferentes consultas.
  - ✓ -s: define el número máximo de subdominios a ser arrastrados desde Google.
  - ✓ -w: realiza la consulta whois sobre los rangos de red de la clase C.
- f: Utilizado para realizar una consulta de subdominios a través de fuerza bruta mediante comparación con un archivo de la herramienta llamado "dns.txt"

La sintaxis a usar es:

dnenum –enum dominio.gob.ec –f /usr/share/dnsenum/dns.txt

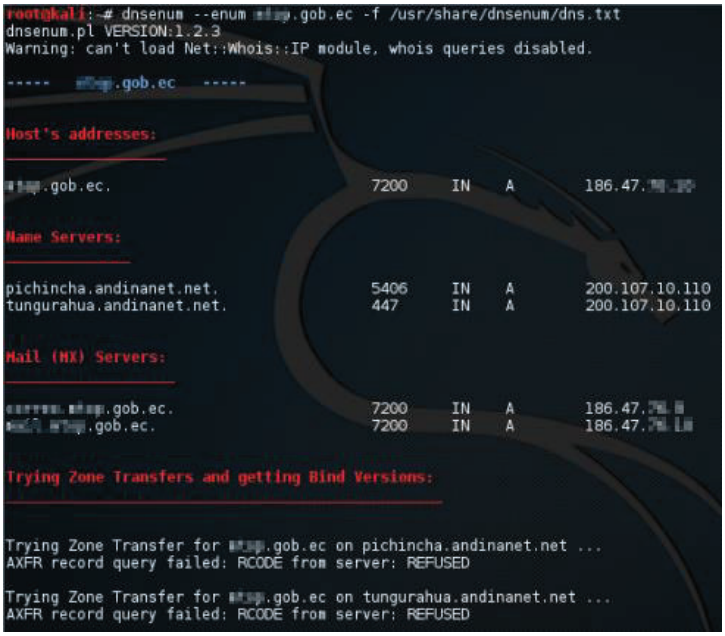


Figura 2.16 Consulta usando DNSENUM a dominio.gob.ec (a)

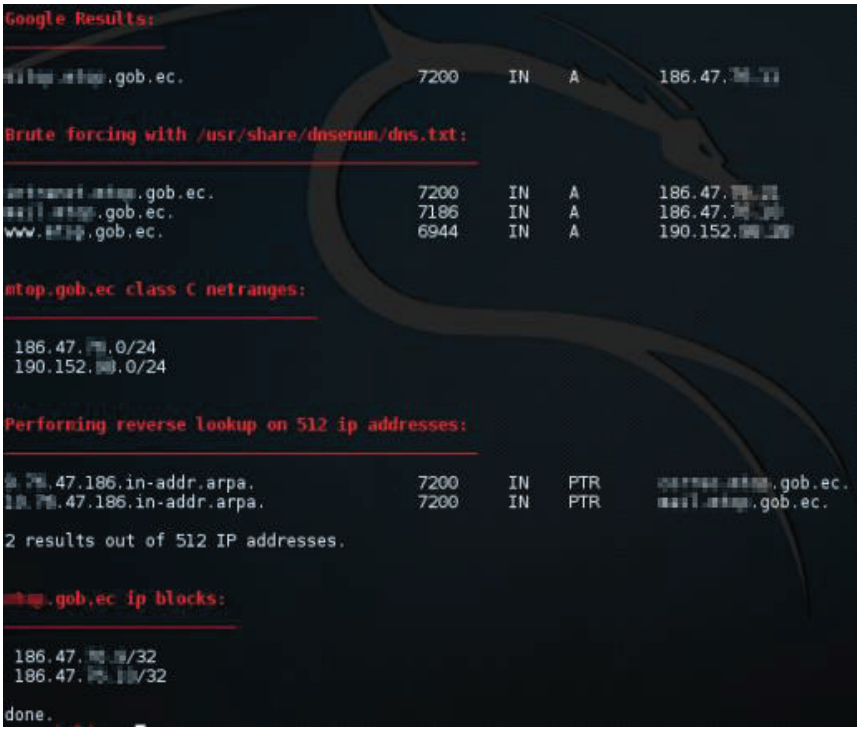


Figura 2.17 Consulta usando DNSENUM a dominio.gob.ec (b)

De las figuras 2.16 y 2.17, se puede obtener la siguiente información:

Subdominios por fuerza bruta	Dirección IP
subdominio4.dominio.gob.ec	186.47.XX.F
subdominio3.dominio.gob.ec	186.47.XX.B
www.dominio.gob.ec	190.152.98.28
Subdominios por google	
subdominio2.dominio.gob.ec	186.47.XX.C
Servidores de nombre	
Tungurahua.andinanet.net	
Pichincha.andinanet.net	200.107.10.110
Servidores de correo	
subdominio1.dominio.gob.ec	186.47.XX.A

Tabla 2.4 Resumen de DNSENUM

2.1.3.3. FIERCE

Es una herramienta de reconocimiento que realiza escaneos rápidos de dominios usando varias técnicas. Destinado a localizar objetivos tanto dentro como fuera de una red corporativa.

La opción dns indica que se utiliza un determinado dominio para el escaneo.

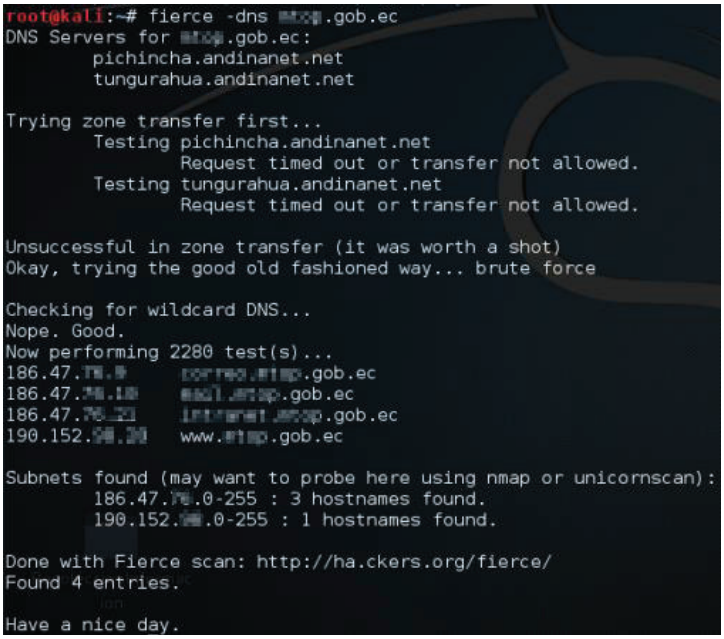


Figura 2.18 Consulta de dominios usando FIERCE.

De la figura 2.18 se obtiene la siguiente información:

Dirección IP	DOMINIO
186.47.XX.A	subdominio1.dominio.gob.ec
186.47.XX.B	subdominio3.dominio.gob.ec
186.47.XX.F	subdominio4.dominio.gob.ec
190.152.XX.XX	www.dominio.gob.ec

Tabla 2.5 Resumen de FIERCE

2.1.3.4. DMITRY

Dmitry (Deepmagic Information Gathering Tool) es una herramienta de línea de comandos que viene pre-instalado en Kali-Linux, tiene la capacidad de recolectar toda la información que sea posible de un objetivo, entre sus principales búsquedas se tiene: consulta whois, búsqueda de subdominios, información recopilada de la página de netcraft, búsqueda de e-mails, de igual manera realiza un análisis de los puertos de un objetivo.

Se utilizan las siguientes opciones:

- w: Indica que se realice una búsqueda whois.
- e: Indica que se realice la búsqueda de algún servidor de correo.
- n: Indica que recopile información del objetivo a través de netcraft.com

- s: Indica que se realice búsquedas de sub-dominios.
- p: Indica que se realice la búsqueda de puertos TCP.

La sintaxis a usar es:

dmitry –w –e –n –s –e –p dominio.gob.ec

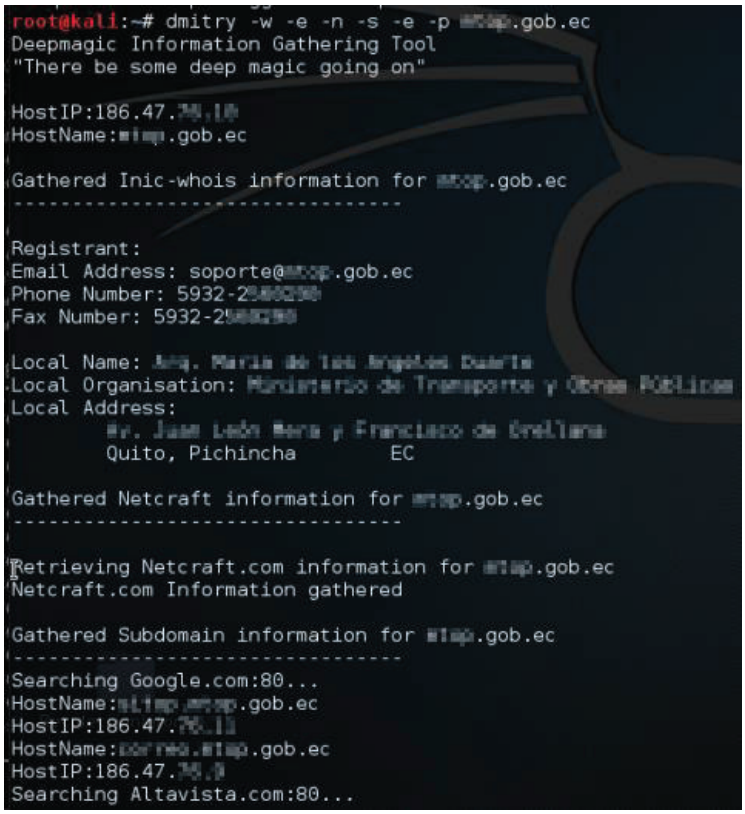


Figura 2.19 Consulta usando DMITRY.

2.1.4. Herramientas para obtener Información a partir de un Dominio

2.1.4.1. Robtex

Robtex es una herramienta que permite encontrar información de un dominio o una dirección IP acerca de: rutas, servidores, dns, listas negras, información de whois, etc.

Adicionalmente esta herramienta permite realizar un nslookup para saber a qué sistema autónomo[25] está conectado la dirección o dominio buscado.

[25] "Un Sistema Autónomo son un grupo de redes o dispositivos (routers) controlados por una sola autoridad administrativa con propósitos de ruteo, pueden tener su propia política de definición de trayectorias de Internet." Tomado de http://www.ecured.cu/Sistemas_Aut%C3%B3nomos

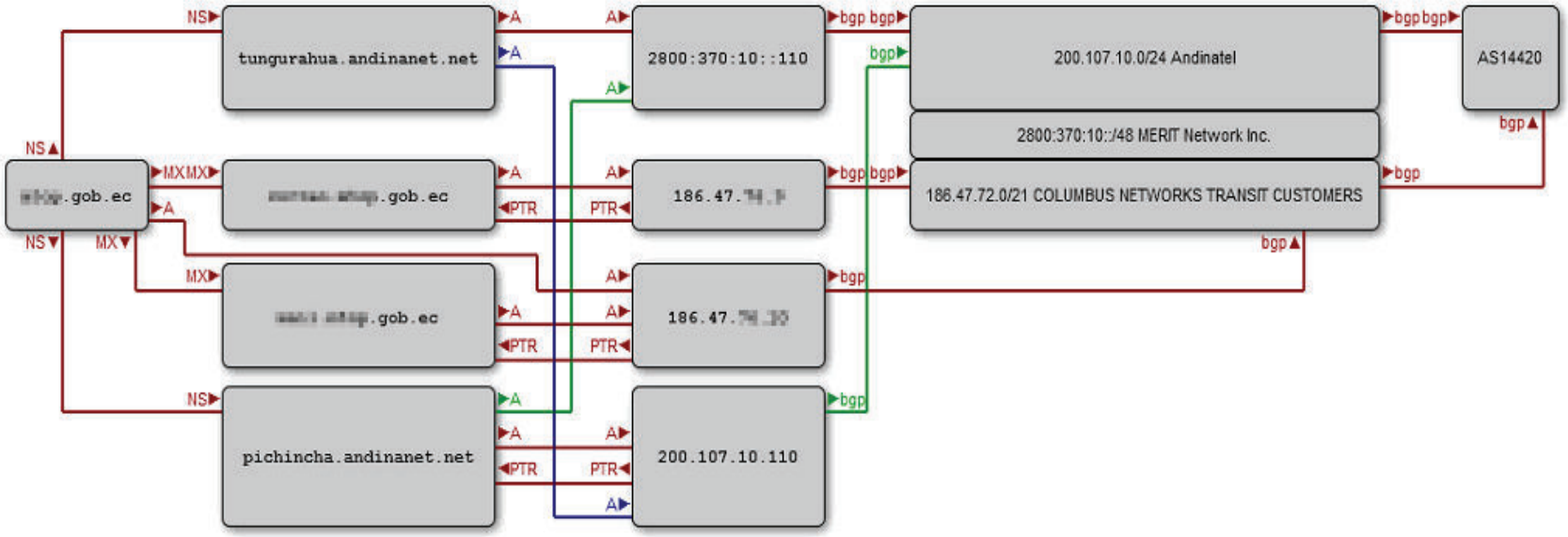


Figura 2.20 Consulta Robtex a dominio.gob.ec (a)

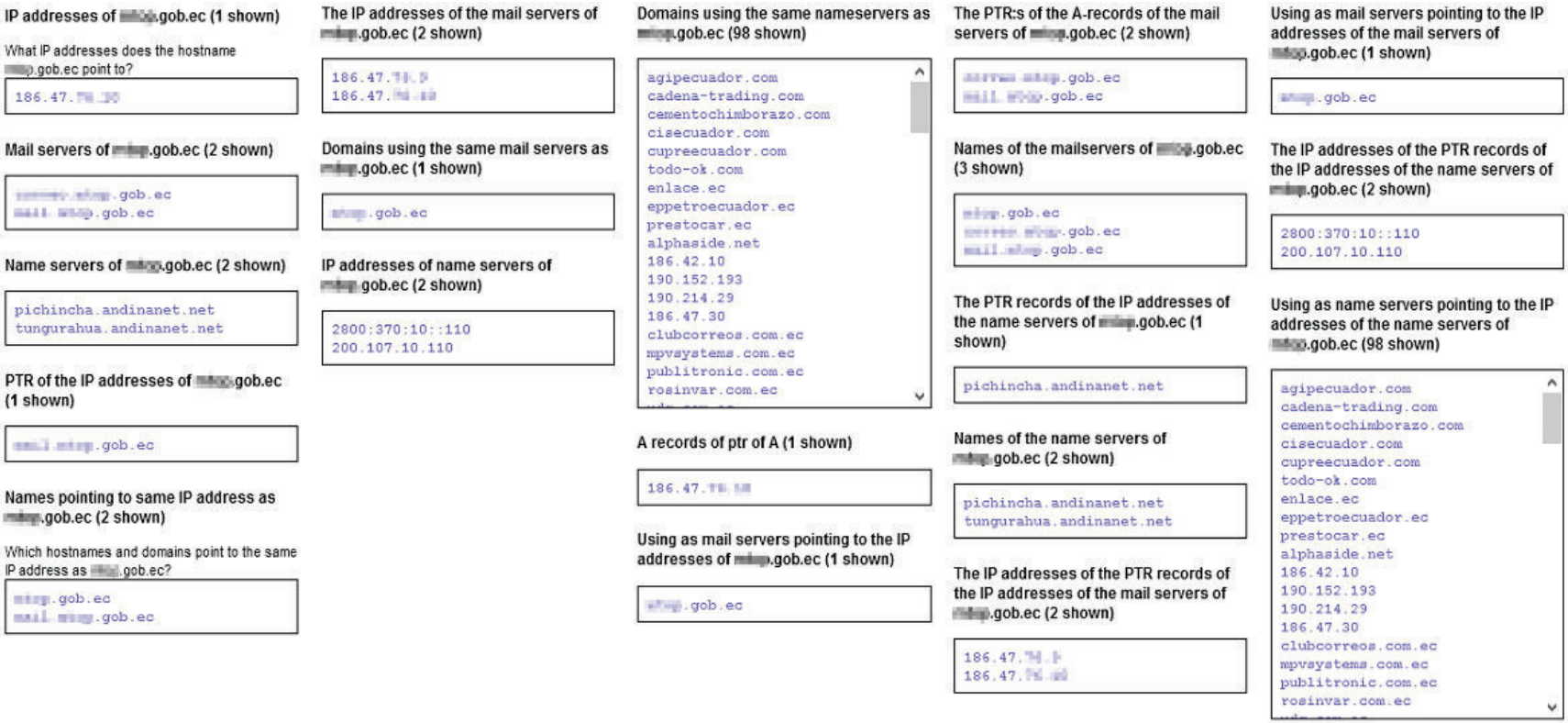


Figura 2.21 Consulta Robtex a dominio.gob.ec (b)

De las evaluaciones indicadas en las figuras 2.20 y 2.21, se obtiene la siguiente información:

Dominio	Sub-Dominios	Direcciones IP
dominio.gob.ec	subdominio1.dominio.gob.ec	186.47.XX.A
	subdominio3.dominio.gob.ec	186.47.XX.B
	subdominio2.dominio.gob.ec	186.47.XX.C

Tabla 2.6 Resumen de información obtenida con Robtex.

2.1.4.2. Maltego

Maltego es una plataforma desarrollada para ofrecer una imagen clara de las relaciones que existen entre: grupos de personas, compañías, organizaciones, infraestructura de internet como; dominios, dns, direcciones IP, bloques de red, etc. Estos diagramas los realiza utilizando inteligencia de fuentes abiertas.

De la figura 2.22 obtenemos la siguiente información:

Dominio	Dirección IP
subdominio1.dominio.gob.ec	186.47.XX.A
subdominio3.dominio.gob.ec	186.47.XX.B
dominio.gob.ec	186.47.XX.B
subdominio2.dominio.gob.ec	186.47.XX.C
subdominio5.dominio.gob.ec	186.47.XX.D
subdominio4.dominio.gob.ec	186.47.XX.F
Rango de direcciones	186.47.XX.0 /25

Tabla 2.7 Resumen de información obtenida con Maltego.

Se puede observar que se identifican nuevas direcciones ip’s.

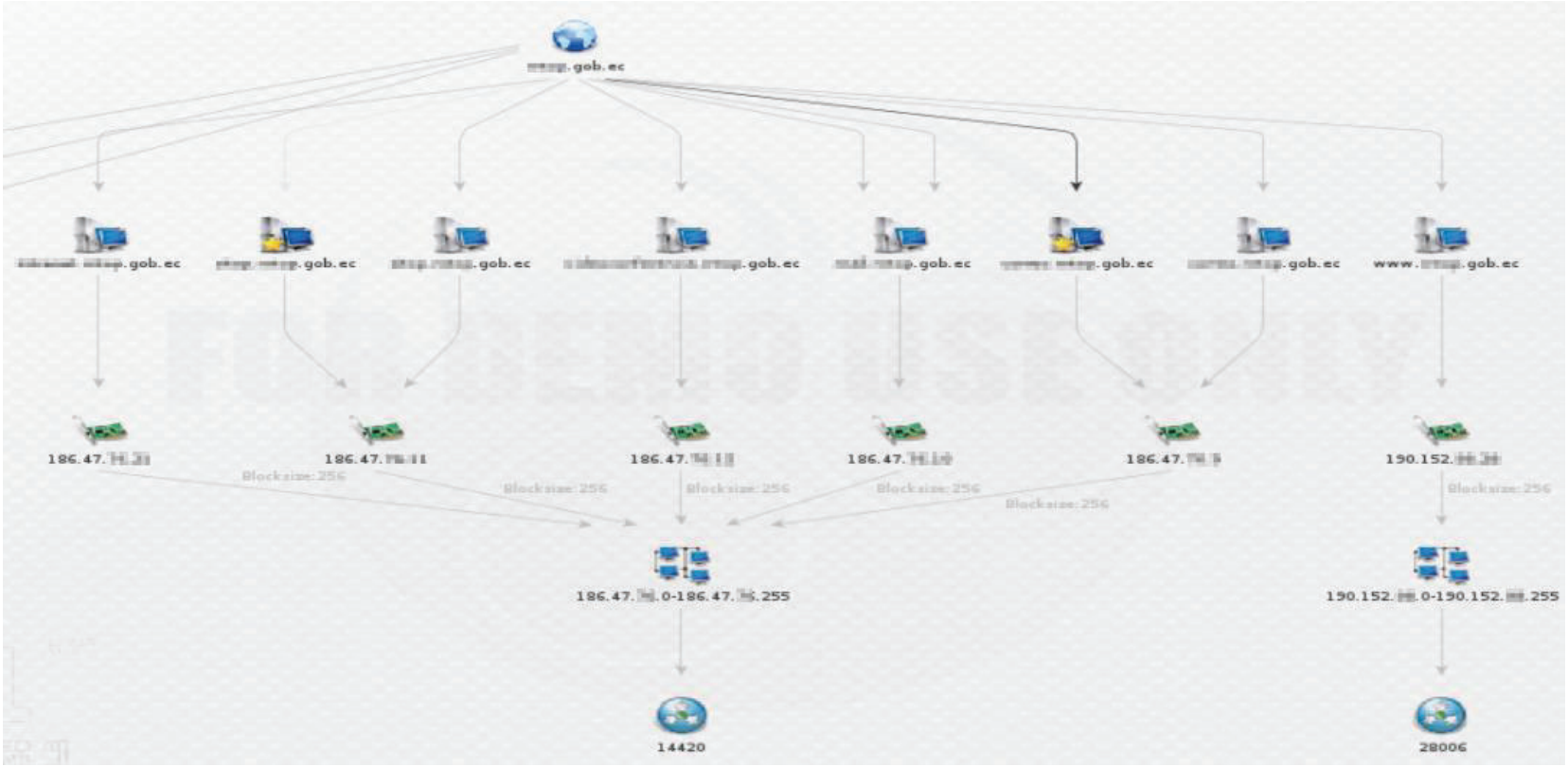


Figura 2.22 Consulta al dominio usando maltego a dominio.gob.ec

2.1.4.3. WhatWeb

WhatWeb es una herramienta que permite identificar sitios web, detectando información de la tecnología web usada, tal como: sistemas de gestión de contenido (CMS), plataformas de blogs, estadísticas/análisis de paquetes, librerías JavaScript, servidores web, dispositivos integrados, números de versión, direcciones de correo electrónico, módulos Web Framework, errores de SQL, etc.

Se utiliza WhatWeb con la opción –v, el cual permite ver la información de forma detallada.

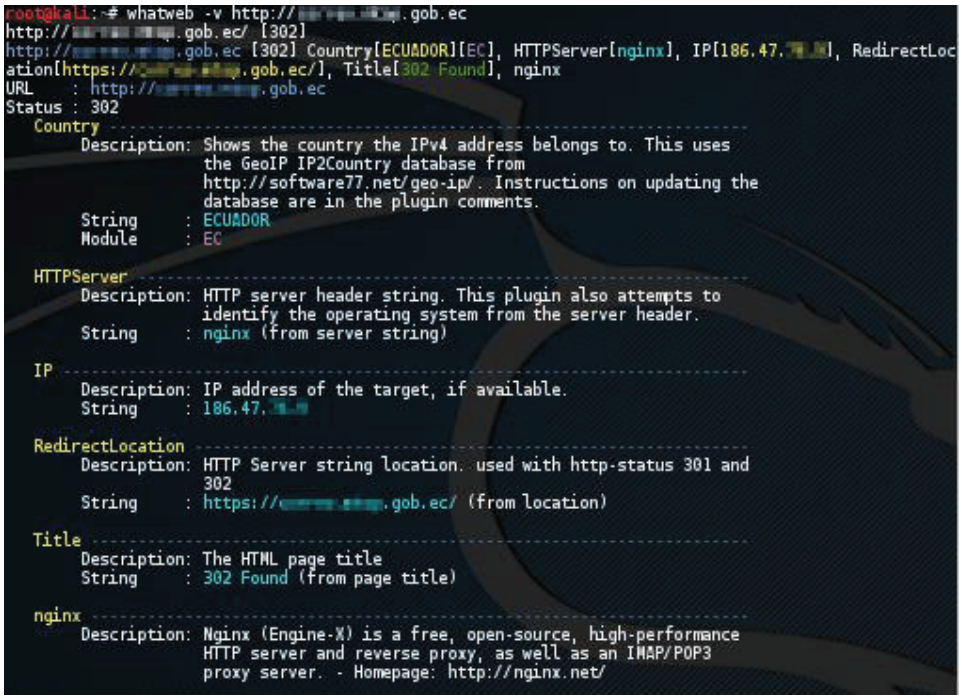


Figura 2.23 Consulta WhatWeb a subdominio1.dominio.gob.ec (a)

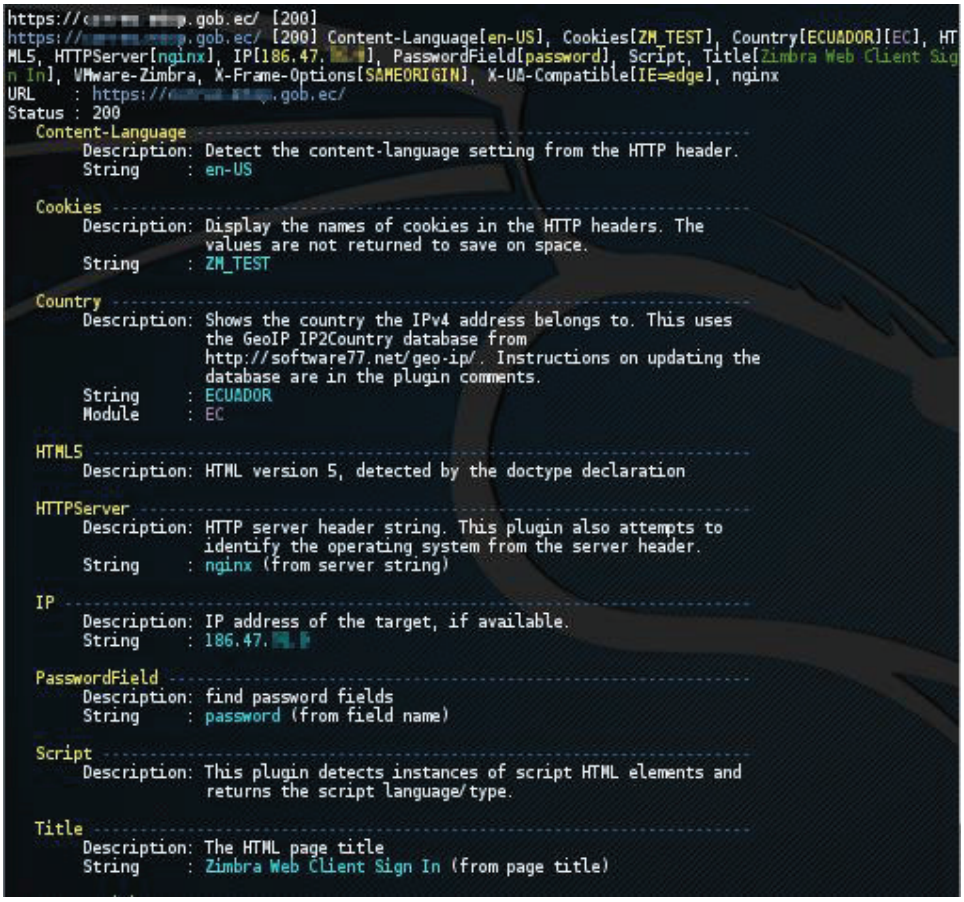


Figura 2.24 Consulta WhatWeb a subdominio1.dominio.gob.ec (b)

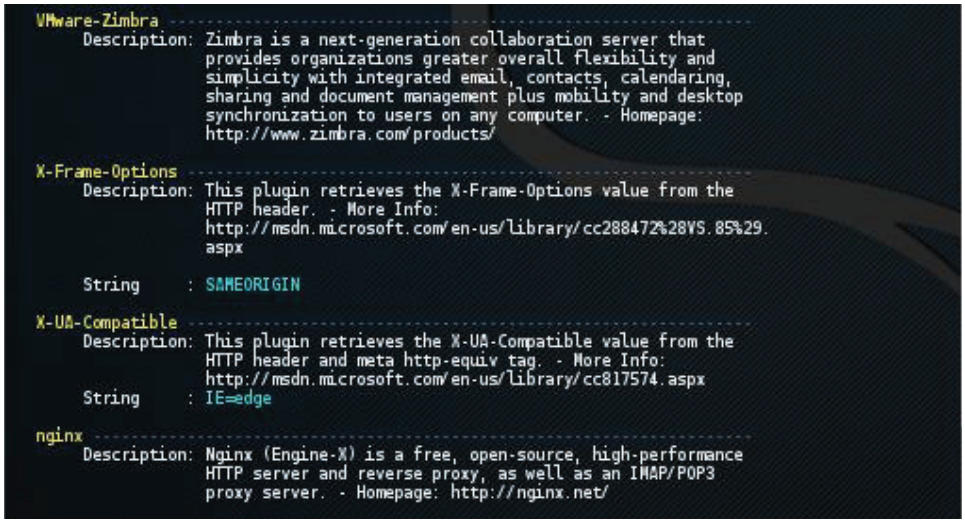


Figura 2.25 Consulta WhatWeb a subdominio1.dominio.gob.ec (c)

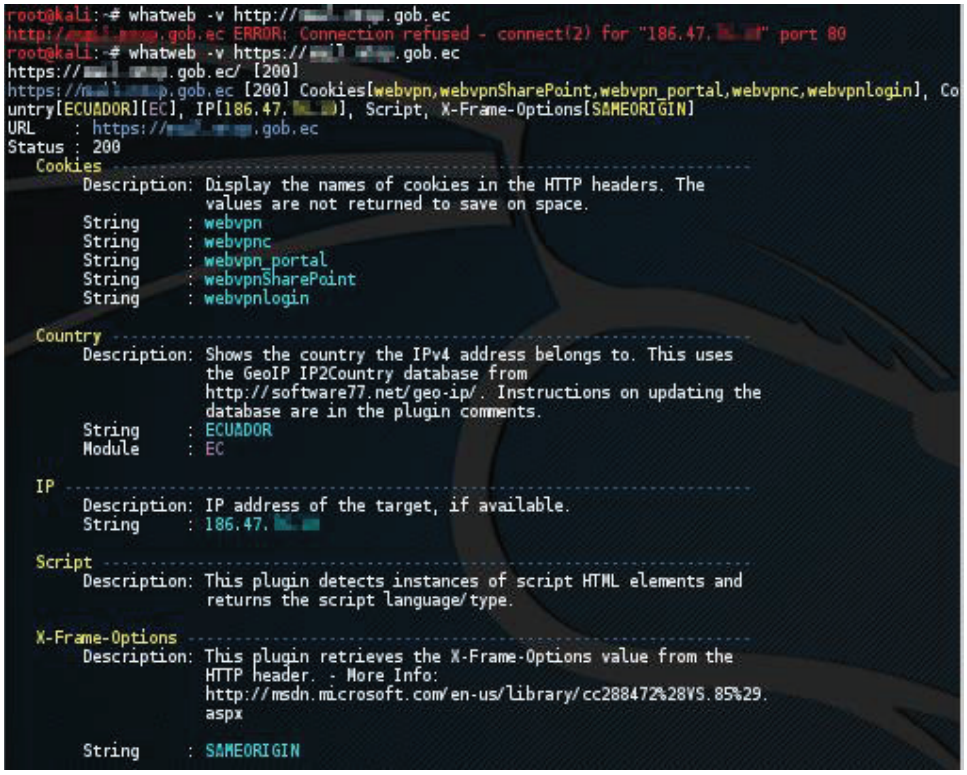


Figura 2.26 Consulta WhatWeb a subdominio3.dominio.gob.ec

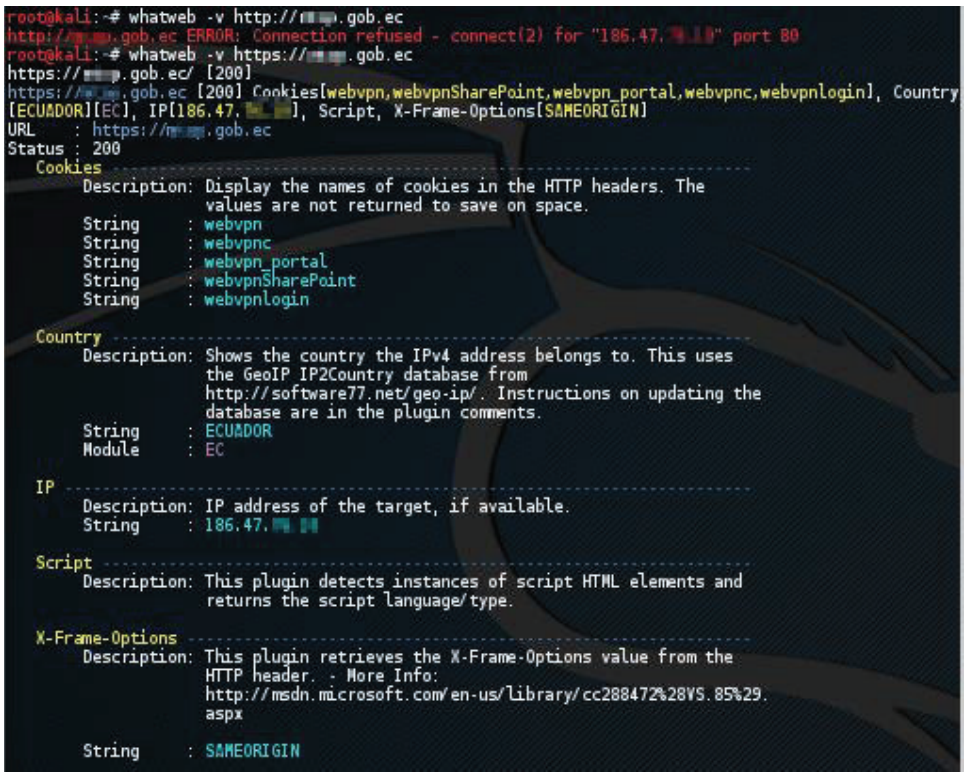


Figura 2.27 Consulta WhatWeb a dominio.gob.ec

Figura 2.28 Consulta WhatWeb a subdominio2.dominio.gob.ec

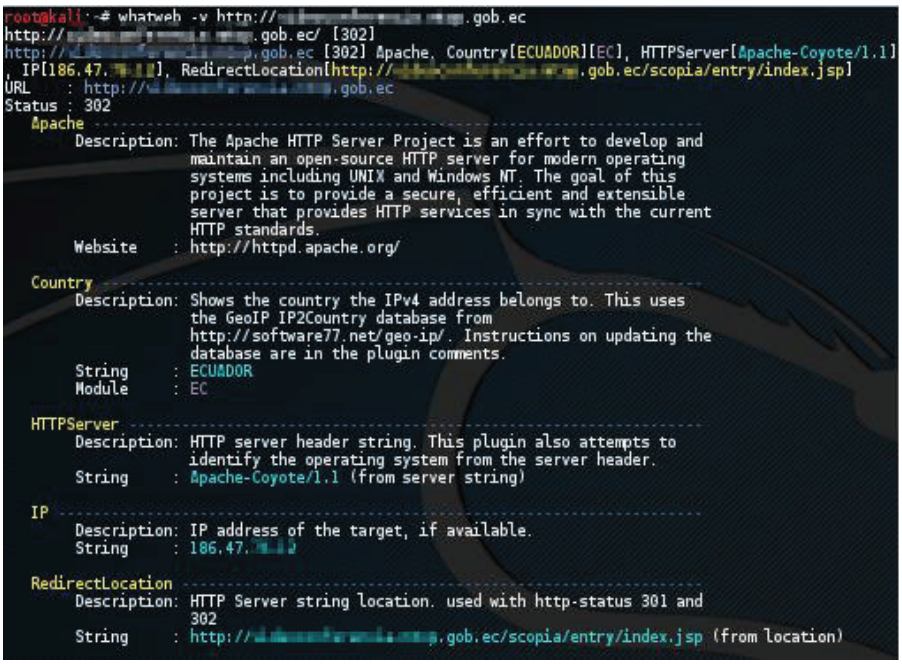


Figura 2.29 Consulta WhatWeb a subdominio5.dominio.gob.ec (a)

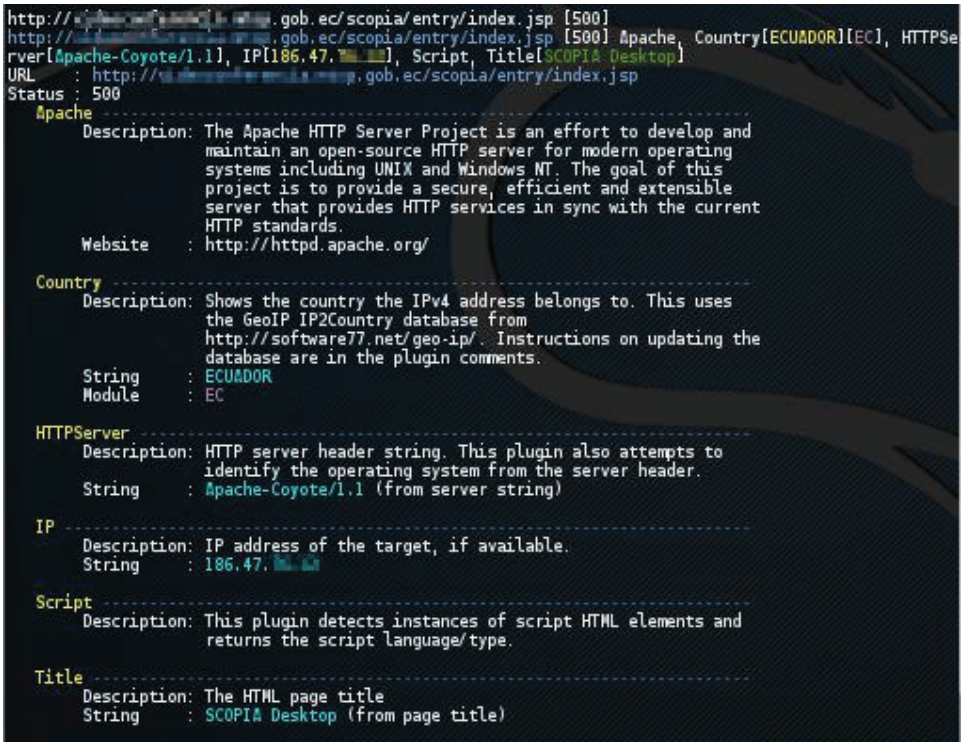


Figura 2.30 Consulta WhatWeb a subdominio5.dominio.gob.ec (b)

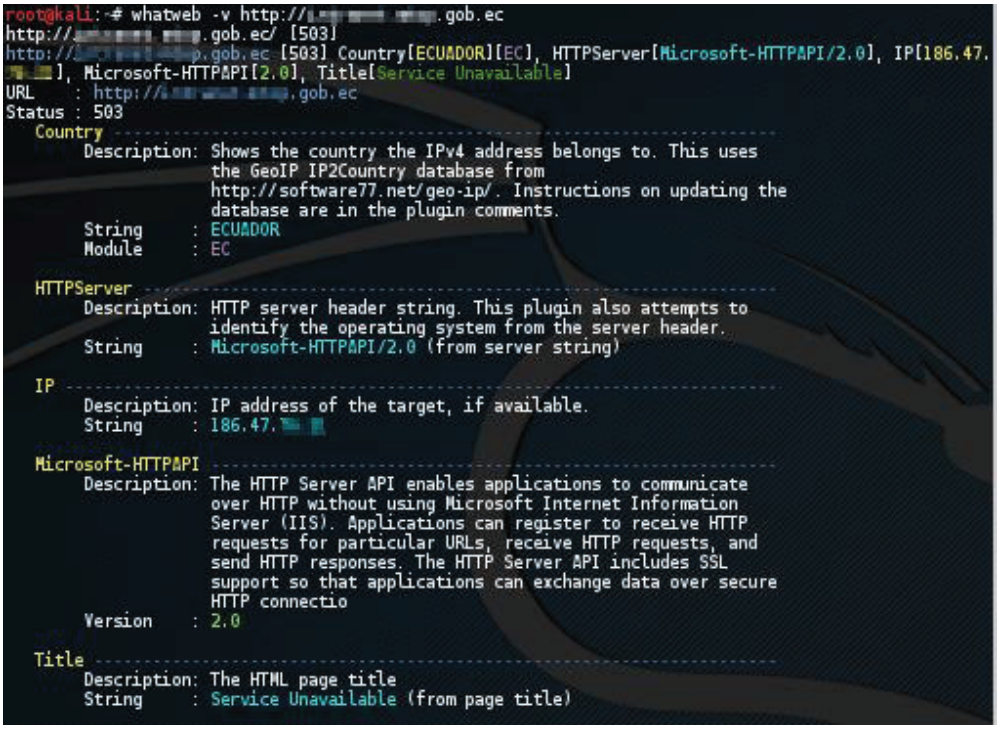


Figura 2.31 Consulta WhatWeb subdominio4.dominio.gob.ec

La información que se obtiene mediante las figuras 2.2 a la 2.31, es la siguiente:

Sub - Dominios	Información de Tecnología Sitio Web
subdominio1.dominio.gob.ec 186.47.XX.A	HTTPServer(nginx), redirection (https:// subdominio1.dominio.gob.ec), título(302 found); x-frame-options(SAMEORIIN);Cookies(ZM_TEST)
subdominio3.dominio.gob.ec 186.47.XX.B	Cookies(webvpn, webvpnc, webvpnportal, webvpnSharePoint, webvpnlogin); x-frame-options (SAMEORIIN)
subdominio2.dominio.gob.ec	Apache(versión:2.2.25)(modulo:md_cluster/1.2.6.Final,mod_ssl/2.2.25); HTTPServer(OS:Unix)(string:Apache, openssl1.0.1e-fips); OpenSSL(versión: 1.0.1e-fips); WebDAV(versión:2)
subdominio5.dominio.gob.ec 186.47.XX.D	HTTPServer(Apache-Coyote/1.1); Redirection(http://v subdominio5.dominio.gob.ec/scopia/entry/index.jsp)
subdominio4.dominio.gob.ec 186.47.XX.F	HTTPServer(Microsoft-HTTPAPI/2.0)

Tabla 2.8 Resumen de información obtenida mediante WhatWeb.

2.1.5. Análisis de la Cabecera de un Correo Electrónico

Esta es una técnica avanzada y de mucha utilidad para recolección de información, se basa en el análisis de las cabeceras de los correos electrónicos, su aplicación puede iniciar con ingeniería social, de tal manera que podamos recibir una respuesta o un correo de algún empleado de la organización.

Dentro de la cabecera podemos encontrar información relevante de funcionalidad del servidor de correo, direcciones lógicas, servicios activos con sus versiones, etc., de igual manera existen herramientas que ayudan a

realizar un análisis automático de las cabeceras de un correo electrónico reuniendo en un pequeño resumen la información importante o de interés.

Se realiza el análisis del encabezado de un correo electrónico, mediante "*Messagge Header Analyzer"*, el cuál es una herramienta de google que extrae información de cada salto que el mensaje ha realizado.

El análisis realizado es el siguiente:

x-store-info:
J++/JTCzmObr++wNraA4Pa4f5Xd6uens6FBov4shFUqw7bfPXCEHeesw3Lv1mvjHhvndWvmd+U1L7eOh
XHs3mpiIobnpmaxNd5vSRzVlehyakJdVHgzmcOTWJxBh2vgx2ny4clWnYtc=
Authentication-Results: hotmail.com; spf=pass (sender IP is 186.47.XX.A)
smtp.mailfrom=xxxxxxx@dominio.gob.ec; dkim=none header.d=dominio.gob.ec; x-hmca=pass
header.id=xxxxxxx@dominio.gob.ec
X-SID-PRA: xxxxxxx@dominio.gob.ec
X-AUTH-Result: PASS
X-SID-Result: PASS
X-Message-Status: n:n
X-Message-Delivery: Vj0xLjE7dXM9MDtsPTE7YT0wO0Q9MTtHRD0xO1NDTD0w
X-Message-Info:
NhFq/7gR1vQRHV6jbdvQfsKUeeVAoUVojAJS6DKEC2GNUUM0G+Idiy+KTMNZNojp7UzXgfa16GF8wKG
24wlvnVQnE7aML20ydhjPrb+a3gMXyg3aPO9D+wyYYsKWtFaHycRpD4rH74WYjrshbZ15xLE8QPZijztV5
VEv9XKVQrZudbV83LLG/5lFhclvoYPrJX4VyAnx0b7573TQ7+fOP+bgjkeha5qvnzG3EWywTPG8rYpyMpC
Dnw==
Received: from ironport-esa01.dominio.gob.ec ([186.47.76.9]) by SNT004-MC3F43.hotmail.com with
Microsoft SMTPSVC(7.5.7601.23143);
Tue, 13 Oct 2015 21:14:06 -0700
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-Anti-Spam-Result: A3GTAQA21R1W/wEAAH8NzWACAgEFvk4
X-IPAS-Result: A3GTAQA21R1W/wEAAH8NzWACAgEFvk4
X-IronPort-AV: E=Sophos;i="5.17,681,1437454800";
d="pdf'?scan'208";a="15521506"
Received: from mxhero.dominio.gob.ec ([172.20.1.XX])
by ironport-esa01.dominio.gob.ec with SMTP; 13 Oct 2015 23:13:40 -0500
Received: from mxhero.dominio.gob.ec (localhost [127.0.0.1])
by mxhero.dominio.gob.ec (Postfix) with ESMTP id D56042207F9
for <bbbbbbb@hotmail.com>; Tue, 13 Oct 2015 23:15:15 -0500 (ECT)
Received: from srvmta.dominio.int (imsva.trendmicro.mtop.int [172.20.0.XX])
by mxhero.dominio.gob.ec (Postfix) with ESMTP
for <bbbbbbb@hotmail.com>; Tue, 13 Oct 2015 23:15:08 -0500 (ECT)
Received: from srvmta.dominio.int (localhost.localdomain [127.0.0.1])
by srvmta.dominio.int (Postfix) with ESMTPS id 74F632630F8
for <bbbbbbb@hotmail.com>; Tue, 13 Oct 2015 23:12:25 -0500 (ECT)

Received: from srvmta.dominio.int (localhost.localdomain [127.0.0.1])
by srvmta.dominio.int (Postfix) with ESMTPS id 65820263182
for <bbbbbbb@hotmail.com>; Tue, 13 Oct 2015 23:12:25 -0500 (ECT)
Received: from srvmailbox.dominio.int (srvmailbox.mtop.int [172.20.1.XX])
by srvmta.dominio.int (Postfix) with ESMTP id 562AF2630F8
for <xxxxxxx@hotmail.com>; Tue, 13 Oct 2015 23:12:25 -0500 (ECT)
Date: Tue, 13 Oct 2015 23:13:52 -0500
From: ABCD <xxxxxxx@dominio.gob.ec>
To: <bbbbbbb@hotmail.com>
Message-ID: <2113224944.1060336.1444796032833.JavaMail.zimbra@dominio.gob.ec>
In-Reply-To: <53119588bfe04dc9a1bf2ff88fa57058@XCH-ALN-016.cisco.com>
References: <53119588bfe04dc9a1bf2ff88fa57058@XCH-ALN-016.cisco.com>
Subject: Fwd: Invitacion a curso de Cisco en Quito - Octubre 19 y 20
Content-Type: multipart/mixed;
boundary="----=_Part_1060332_216635318.1444796032826"
X-Originating-IP: [172.20.1.XX]
X-Mailer: Zimbra 8.5.1_GA_3056 (zclient/8.5.1_GA_3056)
Thread-Topic: Invitacion a curso de Cisco en Quito - Octubre 19 y 20
Thread-Index: AdEBz9Glu70xwqGAQvmFcAGl491qU+gZeIB0
X-TM-AS-GCONF: 11111111
X-TM-AS-SMTP: 1.0 c3J2bXRhLm10b3AuaW50 bWh1cnRhZG9AbXRvcC5nb2luZWM=
X-TM-AS-ERS: -0.0.0.0
X-TM-AS-Product-Ver: IMSVA-9.0.0.1383-8.0.0.1202-21878.004
X-TMASE-Version: IMSVA-9.0.0.1383-8.0.1202-21878.004
X-TMASE-Result: 10--30.027000-5.000000
X-TMASE-MatchedRID: ByVtw1Gj8dPm0FuhFHtATfFtILBSnOCe6HZq9miPpRuGzaXKB9oXvKwY
Ds3ctB1kQwz/wr609j2g+k+FBqVjQa1gHARnFuH2aXN40jz8JFVz1AVC18UYYAbZHUE8HiUoFQC
77iaL3JwJAUQlgZa8S8YCGDCIyvcp2DBKoUnK0AUAz7oVOD+dylQITXWgSBTylQOBog8hQhz90z
sQnttYmD+q/4tk5U2JUHn9+8HdgsOHrihKXvOrRweHIVPdln2t1eNjPetcf+s6oDtQLS8irRbC/
H4tm1daWZoS1zqg3ez0RskjbvixLTWKhqOspR7cVzmaTAOZkvCmCBzY1zXe+LOq6cSMn9PETLle
TKp6hl7cyXfWOujJTlTls+h2BDpNw+Na3+YO+2aF6DSAtFZpkhQ7Wrs+Dn6itXT5sanTkhQiXgb
Io42hj/tC76YC777ZjIA/LFvaNw8BVSVJLZQWXAYeezE34xOR1yFgAZMasi9ZYIEMbqivuAOsHQ
GBf6cYVEf2J0MWMbQV18StrRFSzA4DVEyY5sVQEmmPwoMUJnVJ5vyaF4fRCzP3WYNhkszl82+ZJ
oKeNOUlwMe7O5sKkcl8i/C4dQg46pWPKM1sbY0zvWHRlxWXwkbbuL7Y47c0VS4uT97CBm0kXW0Y
oBgoqnlrUfxPOqs/dUAulK0GzSrETOc2pOXqgE+4wmL9kCTxt5M+xbHmW4oUQhnZW5eYXizh73T
YGM3BFZqFfKJVIGcHMMlZGM3fbFEYyM8bYl0IovR0NV0S/oHSjKYmWkawogP90fJP9eHt
X-TMASE-SNAP-Result: 1.801202.0001-0-1-22:0,12:0
x-mxHero-Origin-Ip: /127.0.0.1:53733
X-Virus-Status: clean
X-mxHero-ClamAV: rule=17;result=clean
Sender: <xxxxxxx@dominio.gob.ec>
Return-Path: xxxxxxx@dominio.gob.ec
X-OriginalArrivalTime: 14 Oct 2015 04:14:06.0788 (UTC) FILETIME=[C4A93840:01D10636]
MIME-Version: 1.0
------=_Part_1060332_216635318.1444796032826

Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: quoted-printable

MessageId	2113224944.1060336.1444796032833.JavaMail.zimbra@[redacted].gob.ec
Created at:	13/10/2015 23:13:52 (Delivered after 14 sec)
From:	[redacted] < [redacted] @[redacted].gob.ec> Using Zimbra 8.5.1_GA_3056 (zclient/8.5.1_GA_3056)
To:	<[redacted]@hotmail.com>
Subject:	Fwd: Invitacion a curso de Cisco en Quito - Octubre 19 y 20
SPF:	pass
DKIM:	none

#	Delay	From *		To *	Protocol	Time received
0	-87 sec	srvmailbox.[redacted].int	→	srvmta.[redacted].int	ESMTP	13/10/2015 23:12:25
1		localhost.localdomain	→	srvmta.[redacted].int	ESMTPS	13/10/2015 23:12:25
2		localhost.localdomain	→	srvmta.[redacted].int	ESMTPS	13/10/2015 23:12:25
3	3 mins	imsva.trendmicro.[redacted].int	→	mxhero.[redacted].gob.ec	ESMTP	13/10/2015 23:15:08
4	7 sec	localhost	→	mxhero.[redacted].gob.ec	ESMTP	13/10/2015 23:15:15
5	-95 sec	mxhero.[redacted].gob.ec	→	ironport-esa01.[redacted].gob.ec	SMTP	13/10/2015 23:13:40
6	26 sec	ironport-esa01.[redacted].gob.ec	→	SNT004-MC3F43.hotmail.com		13/10/2015 23:14:06

Figura 2.32 Análisis de la cabecera de un correo electrónico.

Mediante la revisión manual y el aplicativo se obtiene:

- El correo electrónico se originó desde la dirección IP 186.47.XX.A
- Se identifica nombres y direcciones IP de servidores internos para el correo, como:
  - ✓ mxhero.dominio.gob.ec (176.20.1.136)
  - ✓ srvmailbox.dominio.int (176.20.1.135)
  - ✓ srvmta.dominio.int (176.20.1.115)

2.1.6. Descubrir y Enumerar el Objetivo

En la sección anterior se ha realizado la fase de reconocimiento de información, ya sea por medio de fuentes públicas o en algunos casos interactuando con el objetivo de evaluación.

El siguiente paso es verificar que máquinas se encuentran activas, con el propósito de descartar información que no sea útil, además en esta fase se podrá obtener información acerca de puertos y servicios disponibles, tipo y versión de sistemas operativos utilizados por el objetivo.

2.1.6.1. Barridos de Red Utilizando Paquetes Ping

El primer paso en una prueba de penetración, la mayoría de veces es conocer que hosts están activos, para lo cual existen diferentes herramientas. Uno de los métodos más comunes es usar solicitudes ICMP, es decir, consultas ping.

Ping es una herramienta de diagnóstico que permite identificar el estado de la máquina receptora por medio del envío de paquetes ICMP, adicionalmente por una resolución ARP obtenemos la dirección IP de nuestro objetivo.

Mediante las figuras 2.33 a la 2.38 se indica los barridos de red a los dominios identificados con anterioridad.

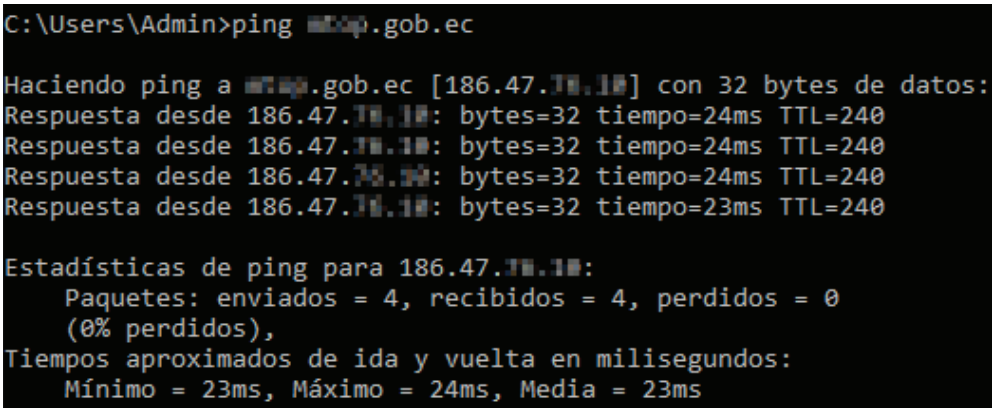


Figura 2.33 Consulta PING a dominio.gob.ec

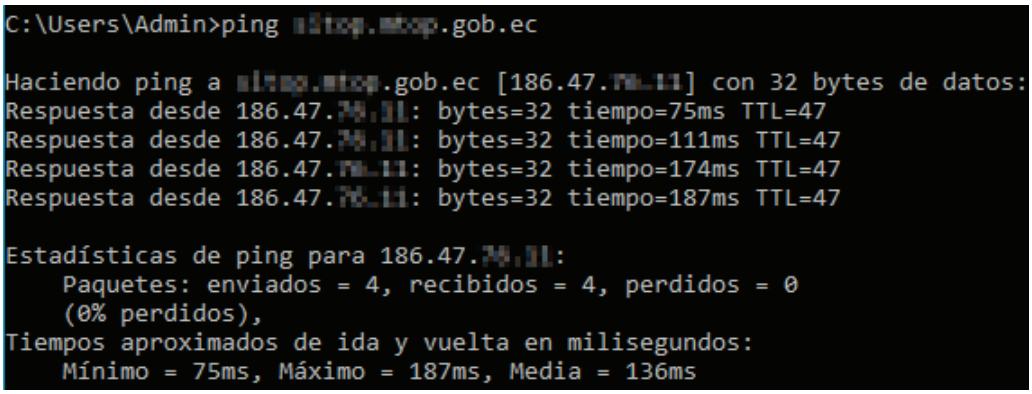


Figura 2.34 Consulta PING a subdominio2.dominio.gob.ec

```
C:\Users\Admin>ping [redacted].gob.ec

Haciendo ping a [redacted].gob.ec [186.47.[redacted]] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 186.47.[redacted]:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

Figura 2.35 Consulta PING a subdominio1.dominio.gob.ec

Se puede ver en la figura 2.35, que el host está inactivo, en este punto es importante considerar que debido al filtrado de paquetes en la implementación de Firewalls, IDS, IPS, y otras defensas en la red las consultas ping son insignificantes, por lo que para evitar estos mecanismos de protección se puede realizar consultas usando paquetes TCP o UDP.

Por lo antes mencionado se realiza una consulta al host de la figura 2.35 utilizando paquetes TCP, evidenciando que el host está activo y se concluye que para el mismo existe un mecanismo de defensa.

```
c:\nmap-7.00>nping --tcp 186.47.[redacted]

Starting Nping 0.7.00 ( https://nmap.org/nping ) at 2016-03-25 07:19 Hora est. PacÝfico, SudamÚrica
SENT (0.4220s) TCP 192.168.1.8:9636 > 186.47.[redacted]:80 S ttl=64 id=29167 iplen=40  seq=3823197100 win=1480
RCVD (0.6090s) TCP 186.47.[redacted]:80 > 192.168.1.8:9636 SA ttl=55 id=0 iplen=44  seq=1567062846 win=14600 <mss 1380>
SENT (1.5730s) TCP 192.168.1.8:9636 > 186.47.[redacted]:80 S ttl=64 id=29167 iplen=40  seq=3823197100 win=1480
RCVD (1.6060s) TCP 186.47.[redacted]:80 > 192.168.1.8:9636 SA ttl=55 id=0 iplen=44  seq=1567062846 win=14600 <mss 1380>
SENT (2.5750s) TCP 192.168.1.8:9636 > 186.47.[redacted]:80 S ttl=64 id=29167 iplen=40  seq=3823197100 win=1480
RCVD (2.6060s) TCP 186.47.[redacted]:80 > 192.168.1.8:9636 SA ttl=55 id=0 iplen=44  seq=1567062846 win=14600 <mss 1380>
SENT (3.5810s) TCP 192.168.1.8:9636 > 186.47.[redacted]:80 S ttl=64 id=29167 iplen=40  seq=3823197100 win=1480
RCVD (3.6120s) TCP 186.47.[redacted]:80 > 192.168.1.8:9636 SA ttl=56 id=0 iplen=44  seq=1567062846 win=14600 <mss 1380>
RCVD (3.8440s) TCP 186.47.[redacted]:80 > 192.168.1.8:9636 SA ttl=56 id=0 iplen=44  seq=1567062846 win=14600 <mss 1380>
SENT (4.5960s) TCP 192.168.1.8:9636 > 186.47.[redacted]:80 S ttl=64 id=29167 iplen=40  seq=3823197100 win=1480
RCVD (4.6270s) TCP 186.47.[redacted]:80 > 192.168.1.8:9636 SA ttl=56 id=0 iplen=44  seq=1567062846 win=14600 <mss 1380>

Max rtt: 263.000ms | Min rtt: 31.000ms | Avg rtt: 72.666ms
Raw packets sent: 5 (270B) | Rcvd: 6 (264B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 4.63 seconds
```

Figura 2.36 Consulta nping -tcp 186.47.XX.A

```
C:\Windows\system32>ping [redacted].gob.ec

Pinging videoconferencia.mtop.gob.ec [186.47.[redacted]] with 32 bytes of data:
Reply from 186.47.[redacted]: bytes=32 time=23ms TTL=119
Reply from 186.47.[redacted]: bytes=32 time=23ms TTL=119
Reply from 186.47.[redacted]: bytes=32 time=23ms TTL=119
Reply from 186.47.[redacted]: bytes=32 time=23ms TTL=119

Ping statistics for 186.47.[redacted]:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 23ms, Average = 23ms
```

Figura 2.37 Consulta PING a subdominio5.dominio.gob.ec

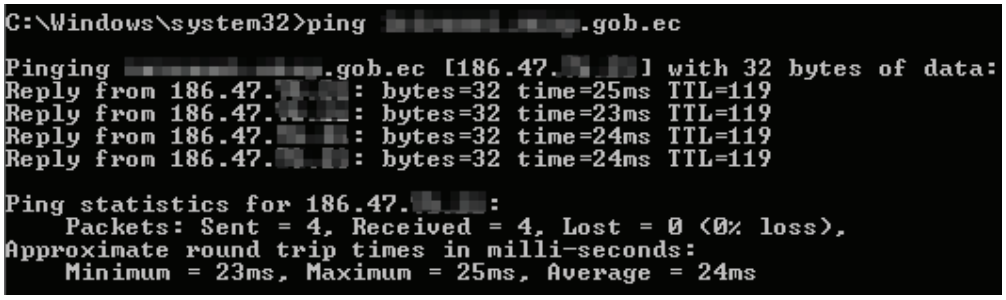


Figura 2.38 Consulta PING a subdominio4.dominio.gob.ec

De las pruebas realizadas se puede obtener la dirección IP por resolución de dominio:

Dominio	Dirección IP
dominio.gob.ec	186.47.XX.B
subdominio2.dominio.gob.ec	186.47.XX.C
subdominio1.dominio.gob.ec	186.47.XX.A
subdominio5.dominio.gob.ec	186.47.XX.D
subdominio4.dominio.gob.ec	186.47.XX.F

Tabla 2.9 Resumen de direcciones IP obtenidas con PING.

Se puede realizar la misma prueba de manera automática al rango de red 186.47.XX.0/24 utilizando nmap, el cual utiliza el protocolo ARP para las consultas. Se hace uso de las siguientes opciones:

- -n, indica que no se realicen consultas al DNS para averiguar el dominio asociado a la dirección IP.
- -sn, indica que solo se van a usar técnicas para reconocer si los host están en funcionamiento, no realiza escaneo de puertos.

La sintaxis usada es:

nmap –n –sn 186.47.XX.0/24

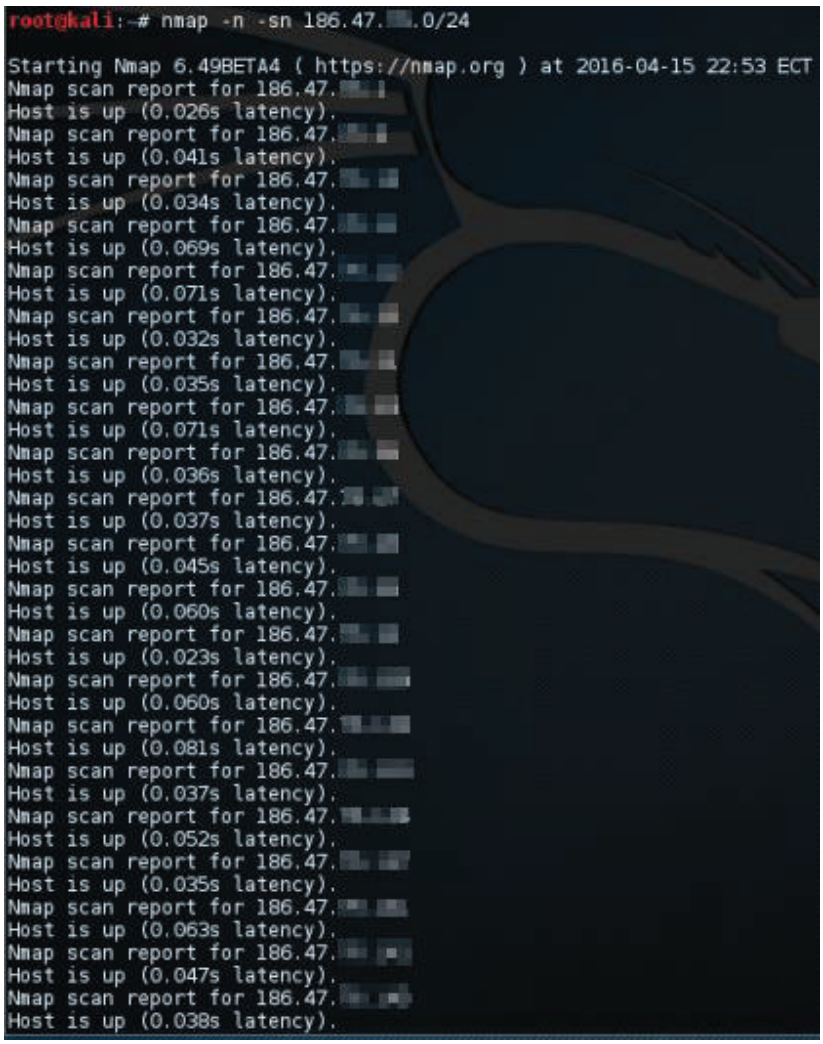


Figura 2.39 Consulta nmap a un rango de direcciones IP. (a)

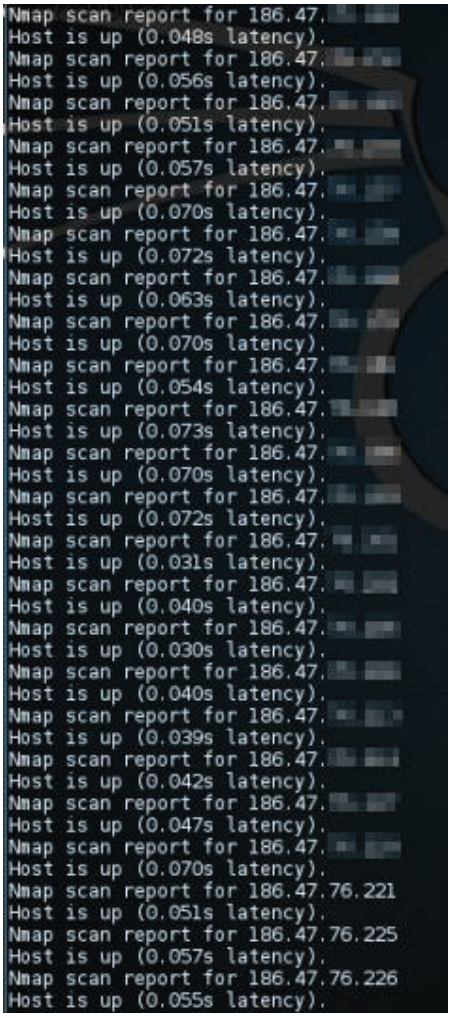


Figura 2.40 Consulta nmap a un rango de direcciones IP. (b)

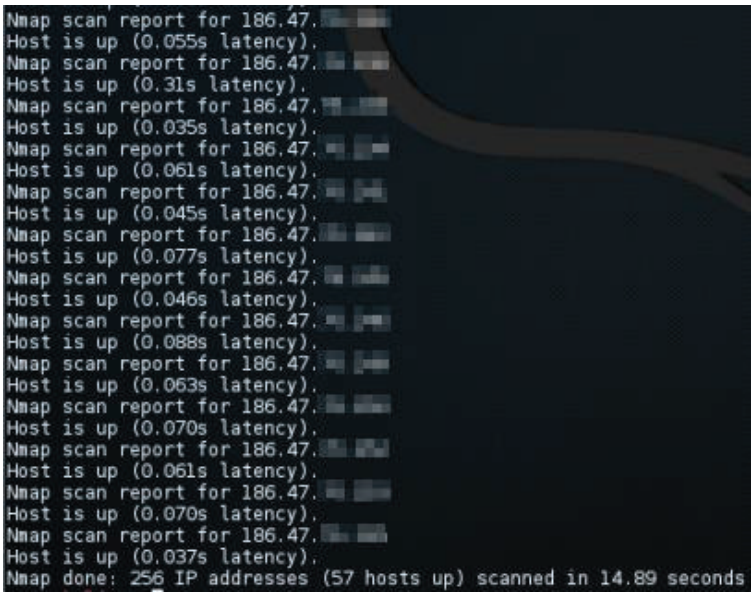


Figura 2.41 Consulta nmap a un rango de direcciones IP. (c)

De las figuras 2.39, 2.40 y 2.41 se puede observar que en el rango existen 57 hosts activos.

2.1.6.2. Traza de Red

En esta fase el objetivo es determinar cuál es la ruta que siguen los paquetes IP desde un host a otro, de esta manera se puede mapear la topología como posibles rutas de acceso.

Desde el punto de vista de un atacante, la información que se puede obtener mediante traceroute es la siguiente:

- El camino exacto entre el atacante y el objetivo.
- Sugerencias relacionadas acerca de la topología de red externa.
- Identificación de los dispositivos de control de acceso, como: firewalls, routers de filtrado de paquetes, etc.
- Si es que la red está mal configurada, puede ser posible identificar el direccionamiento interno.

Mediante las figuras 2.42 a la 2.54 se indica la traza de cada uno de los host's activos identificados mediantes nmap.

```
C:\Users\Admin>tracert 186.47.[redacted]

Traza a la dirección 1.pichincha.andinanet.net [186.47.[redacted]]
sobre un máximo de 30 saltos:

  1     2 ms     1 ms     2 ms  192.168.1.1
  2    23 ms    22 ms    22 ms  18.pichincha.andinanet.net [186.42.168.18]
  3    22 ms    21 ms    22 ms  165.default.location [186.46.4.165]
  4    22 ms    22 ms    21 ms  122.default.location [186.46.4.122]
  5    21 ms    22 ms    21 ms  86.default.location [186.46.4.86]
  6    22 ms    22 ms    24 ms  126.default.location [186.46.4.126]
  7    31 ms    29 ms    27 ms  192.168.211.1
  8    25 ms    24 ms    24 ms  1.pichincha.andinanet.net [186.47.[redacted]]

Traza completa.
```

Figura 2.42 Diagnóstico tracert a 186.47.XX.M

```
C:\Users\Admin>tracert 186.47.[redacted]

Traza a la dirección [redacted].gob.ec [186.47.[redacted]]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    22 ms    57 ms    23 ms  166.default.location [186.46.4.166]
  3    21 ms    22 ms    21 ms  9.pichincha.andinanet.net [186.42.168.9]
  4    22 ms    21 ms    24 ms  37.default.location [186.46.4.37]
  5    22 ms    21 ms    21 ms  86.default.location [186.46.4.86]
  6    22 ms    22 ms    24 ms  130.default.location [186.46.4.130]
  7    22 ms    23 ms    22 ms  192.168.211.1
  8    22 ms    23 ms    21 ms  192.168.211.2
  9     *        *        *     Tiempo de espera agotado para esta solicitud.
 10     *        *        *     Tiempo de espera agotado para esta solicitud.
 11     *        *        *     Tiempo de espera agotado para esta solicitud.
 12     *        *        *     Tiempo de espera agotado para esta solicitud.
 13     *        *        *     Tiempo de espera agotado para esta solicitud.
 14     *        *        *     Tiempo de espera agotado para esta solicitud.
```

Figura 2.43 Diagnóstico tracert a 186.47.XX.A

```
C:\Users\Admin>tracert 186.47.[redacted]

Traza a la dirección [redacted].gob.ec [186.47.[redacted]]
sobre un máximo de 30 saltos:

  1    <1 ms     1 ms    <1 ms  192.168.1.1
  2    24 ms    23 ms    26 ms  158.default.location [186.46.4.158]
  3    22 ms    24 ms    22 ms  17.pichincha.andinanet.net [186.42.168.17]
  4    24 ms    21 ms    26 ms  122.default.location [186.46.4.122]
  5    24 ms    22 ms    23 ms  86.default.location [186.46.4.86]
  6    23 ms    27 ms     *     130.default.location [186.46.4.130]
  7    23 ms    22 ms    22 ms  192.168.211.1
  8    23 ms    24 ms    35 ms  192.168.211.2
  9    25 ms    32 ms    23 ms  mail.mtop.gob.ec [186.47.[redacted]]

Traza completa.
```

Figura 2.44 Diagnóstico tracert a 186.47.XX.B

```
C:\Users\Admin>tracert 186.47.[redacted]

Traza a la dirección 11.pichincha.andinanet.net [186.47.[redacted]]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    25 ms    24 ms    27 ms  10.pichincha.andinanet.net [186.42.168.10]
  3    23 ms    21 ms    25 ms  165.default.location [186.46.4.165]
  4    24 ms    22 ms    37 ms  213.default.location [186.46.4.213]
  5    23 ms    27 ms    22 ms  82.default.location [186.46.4.82]
  6    34 ms    26 ms    22 ms  130.default.location [186.46.4.130]
  7    22 ms    32 ms    22 ms  192.168.211.1
  8    25 ms     *       24 ms  192.168.211.2
  9    25 ms     *      130 ms  [redacted].gob.ec [186.47.[redacted]]
 10    27 ms    23 ms    24 ms  11.pichincha.andinanet.net [186.47.[redacted]]

Traza completa.
```

Figura 2.45 Diagnóstico tracert a 186.47.XX.C

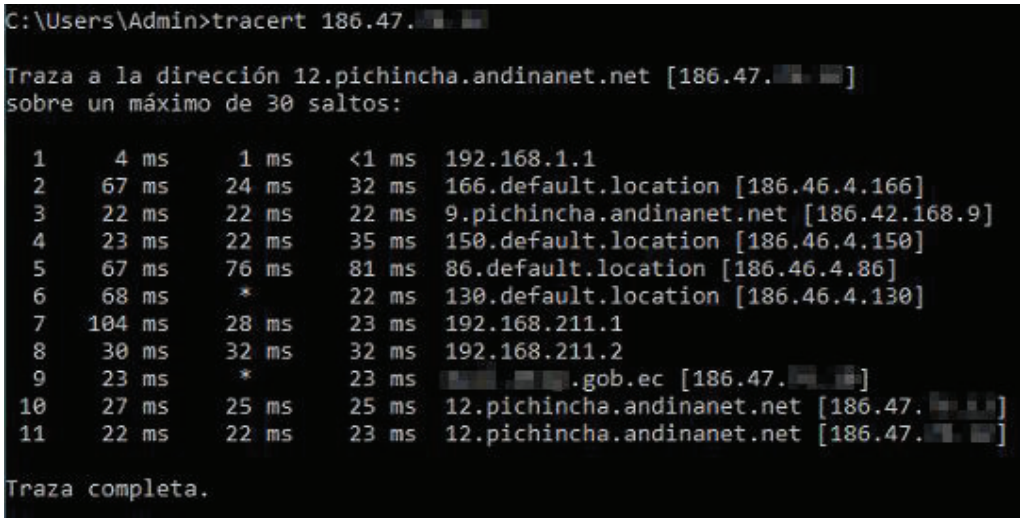


Figura 2.46 Diagnóstico tracert a 186.47.XX.D

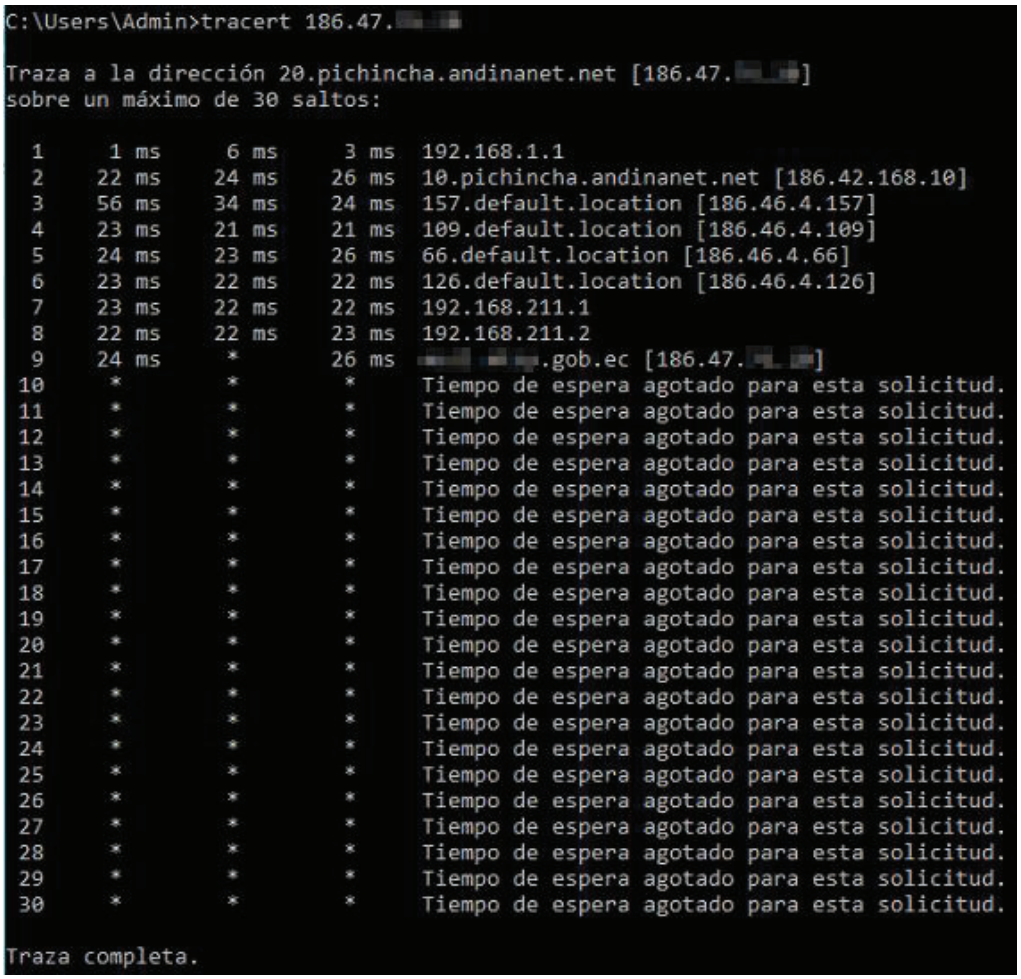


Figura 2.47 Diagnóstico tracert a 186.47.XX.E

```
C:\Users\Admin>tracert 186.47.[redacted]

Traza a la dirección 21.pichincha.andinanet.net [186.47.[redacted]]
sobre un máximo de 30 saltos:

  1     4 ms     1 ms     2 ms  192.168.1.1
  2    24 ms    24 ms    27 ms  18.pichincha.andinanet.net [186.42.168.18]
  3    22 ms    22 ms    21 ms  9.pichincha.andinanet.net [186.42.168.9]
  4    26 ms    22 ms    22 ms  150.default.location [186.46.4.150]
  5    23 ms    22 ms    22 ms  86.default.location [186.46.4.86]
  6    60 ms    55 ms    60 ms  130.default.location [186.46.4.130]
  7    27 ms    25 ms    25 ms  192.168.211.1
  8    22 ms    22 ms    22 ms  192.168.211.2
  9    23 ms     *       87 ms  [redacted].gob.ec [186.47.[redacted]]
 10    27 ms    25 ms    69 ms  21.pichincha.andinanet.net [186.47.[redacted]]

Traza completa.
```

Figura 2.48 Diagnóstico tracert a 186.47.XX.F

```
C:\Users\Admin>tracert 186.47.[redacted]

Traza a la dirección 24.pichincha.andinanet.net [186.47.[redacted]]
sobre un máximo de 30 saltos:

  1   336 ms     3 ms    <1 ms  192.168.1.1
  2    22 ms    22 ms    24 ms  166.default.location [186.46.4.166]
  3    22 ms    21 ms    21 ms  157.default.location [186.46.4.157]
  4    22 ms    21 ms    21 ms  21.default.location [186.46.4.21]
  5    23 ms    23 ms    22 ms  82.default.location [186.46.4.82]
  6    23 ms    23 ms    22 ms  126.default.location [186.46.4.126]
  7    27 ms    22 ms    23 ms  192.168.211.1
  8    22 ms    21 ms    29 ms  192.168.211.2
  9    23 ms     *       27 ms  [redacted].gob.ec [186.47.[redacted]]
 10    24 ms    22 ms    22 ms  24.pichincha.andinanet.net [186.47.[redacted]]
```

Figura 2.49 Diagnóstico tracert a 186.47.XX.G

```
C:\Users\Admin>tracert 186.47.[redacted]

Traza a la dirección 26.pichincha.andinanet.net [186.47.[redacted]]
sobre un máximo de 30 saltos:

  1     6 ms     1 ms     1 ms  192.168.1.1
  2    25 ms    26 ms    25 ms  158.default.location [186.46.4.158]
  3    23 ms    21 ms    22 ms  17.pichincha.andinanet.net [186.42.168.17]
  4    25 ms    25 ms    25 ms  118.default.location [186.46.4.118]
  5    33 ms    21 ms    37 ms  82.default.location [186.46.4.82]
  6    46 ms    22 ms    22 ms  130.default.location [186.46.4.130]
  7    22 ms    21 ms    23 ms  192.168.211.1
  8    62 ms    22 ms    85 ms  192.168.211.2
  9    26 ms     *       23 ms  [redacted].gob.ec [186.47.[redacted]]
 10    24 ms    22 ms    23 ms  26.pichincha.andinanet.net [186.47.[redacted]]

Traza completa.
```

Figura 2.50 Diagnóstico tracert a 186.47.XX.H

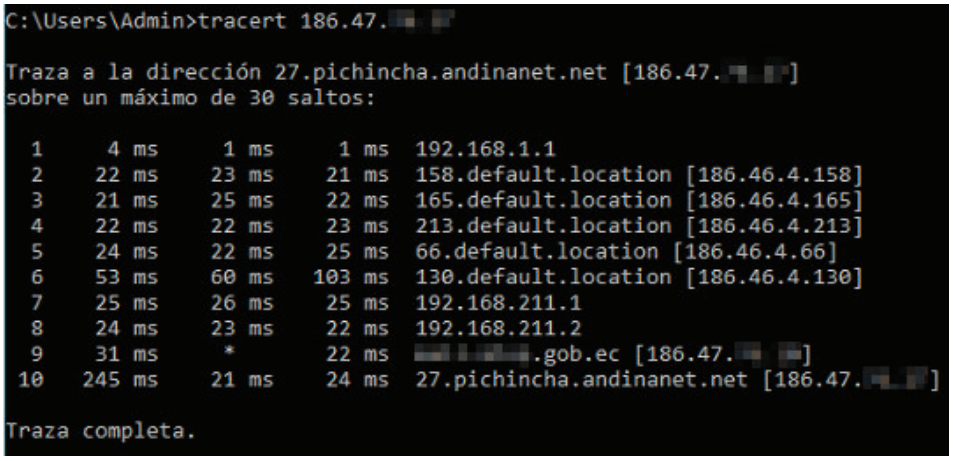


Figura 2.51 Diagnóstico tracert a 186.47.XX.I

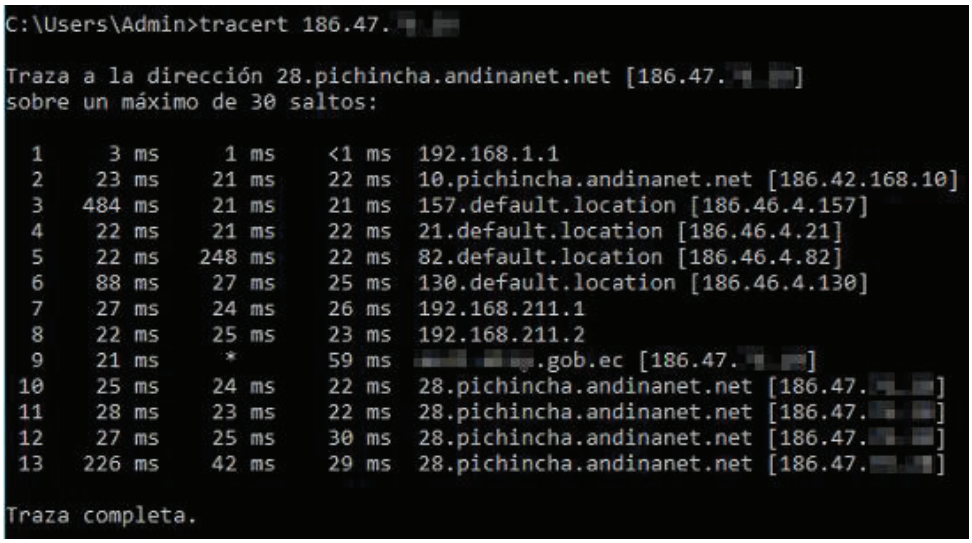


Figura 2.52 Diagnóstico tracert a 186.47.XX.J

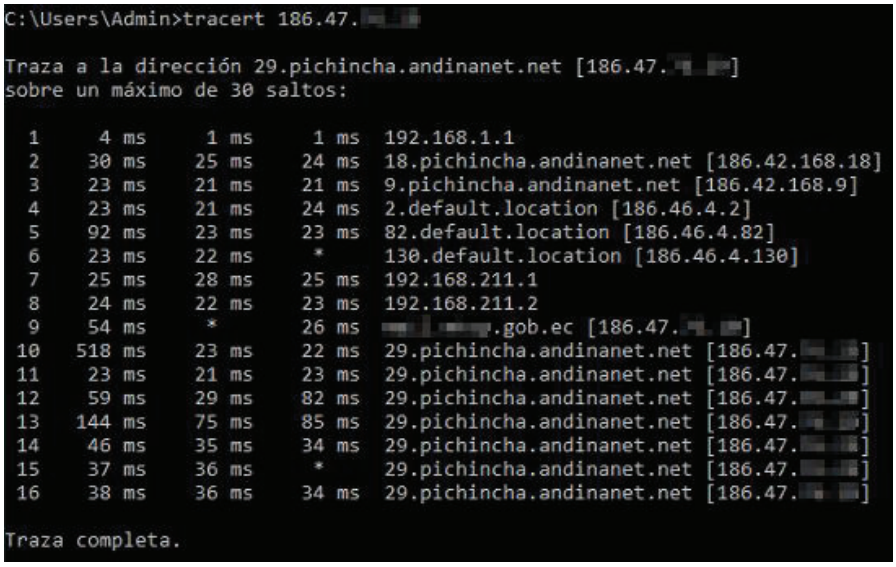


Figura 2.53 Diagnóstico tracert a 186.47.XX.K

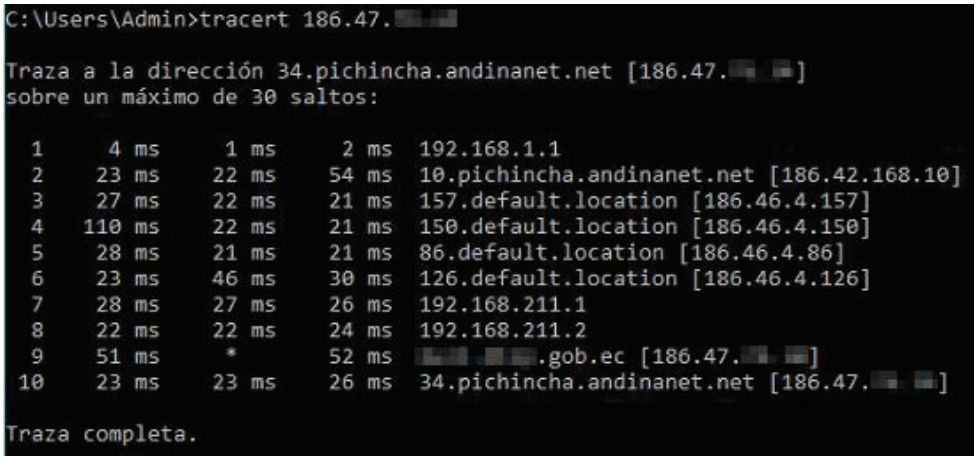


Figura 2.54 Diagnóstico tracert a 186.47.XX.L

De la evaluación anterior podemos concluir que las IP's que siguen el mismo camino y pasan o llegan a la dirección mail.mtop.gob.ec [186.47.XX.B] son:

- 186.47.XX.B
- 186.47.XX.C
- 186.47.XX.D
- 186.47.XX.E
- 186.47.XX.F
- 186.47.XX.G
- 186.47.XX.H
- 186.47.XX.I
- 186.47.XX.J
- 186.47.XX.K
- 186.47.XX.L

Existe una excepción en la IP 186.47.XX.A, la cual debe tener algún tipo de filtro, pero por evaluaciones anteriores sabemos que pertenece al objetivo evaluado.

En los 45 hosts restantes que están activos se realiza el mismo análisis de ruta, y se determina que siguen diferentes caminos comparado a los del objetivo, por lo tanto se descartan las IP's para los siguientes análisis.

2.1.6.3. Escaneo de Puertos

Una vez que se ha identificado los hosts activos en la red del objetivo, el siguiente paso es buscar puertos y servicios asociados con los mismos. El escaneo de puertos es el proceso de descubrir puertos UDP como TCP, los mismos que revelarán los servicios que están corriendo sobre la red, los cuales pueden ser puntos potenciales de ataque.

Para realizar esta fase utilizaremos la herramienta nmap, la cual nos permite realizar diferentes tipos de escaneo dependiendo de la opción que se use y el tipo de información que deseamos obtener, de la siguiente manera:

- sT: permite realizar un escaneo de los puertos TCP para comprobar si existe algún servicio activo y puerto abierto. Este tipo de escaneo es el menos común, debido a que llega a completar las conexiones TCP.
- sU: aunque la mayoría de servicios usan puertos TCP, es importante escanear puertos UDP los cuales podrían ser usados para posibles ataques.
- n: indica que no requiere hacer resolución a los DNS.
- Pn: indica que no se realicen técnicas para saber si el host está arriba, debido a que se conoce que el host está en funcionamiento.

Además es importante conocer la definición del estado de los puertos:

- Abierto: Indica que el puerto se encuentra a la espera de conexiones TCP o paquetes UDP. Estos puertos son usados como vectores de ataque.
- Cerrado: Indica que el puerto no tiene ninguna aplicación escuchando, aunque puede responder a paquetes de pruebas de nmap.
- Filtrado: Nmap no puede determinar si el puerto se encuentra en estado abierto o cerrado debido a un filtrado de paquetes, este filtrado puede ser debido a un firewall, reglas del enrutador, o por el propio equipo.
- No-Filtrado: Indica que el puerto es accesible, pero no se puede determinar si está abierto o cerrado.
- Abierto-Filtrado: Nmap clasifica a los puertos dentro de este tipo cuando no puede determinar si está abierto o filtrado.

- Cerrado-Filtrado: Nmap clasifica a los puertos dentro de este tipo cuando no puede determinar si está abierto o filtrado.

Las figuras 2.55 a las 2.57 indican los puertos TCP detectados, el estado y el servicio que corren sobre los mismos, de cada IP descubierta.

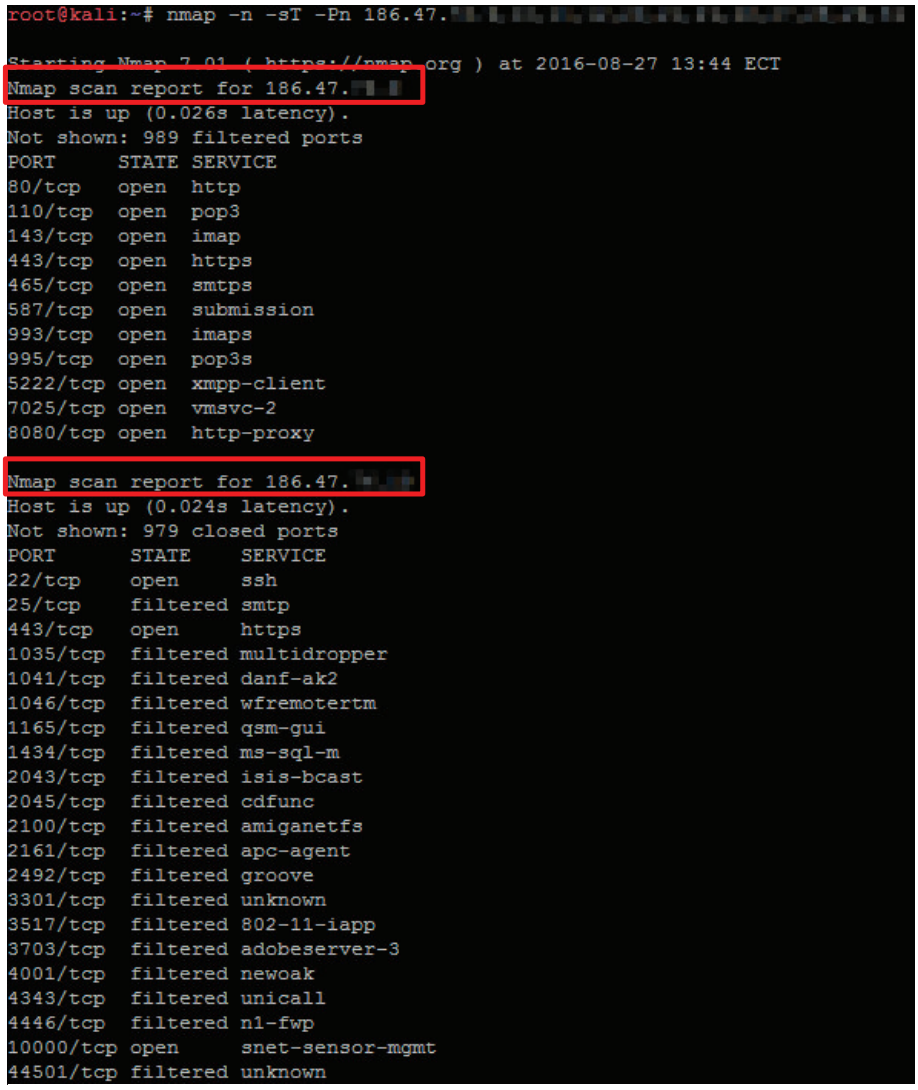


Figura 2.55 Escaneo de puertos TCP abiertos. (a)

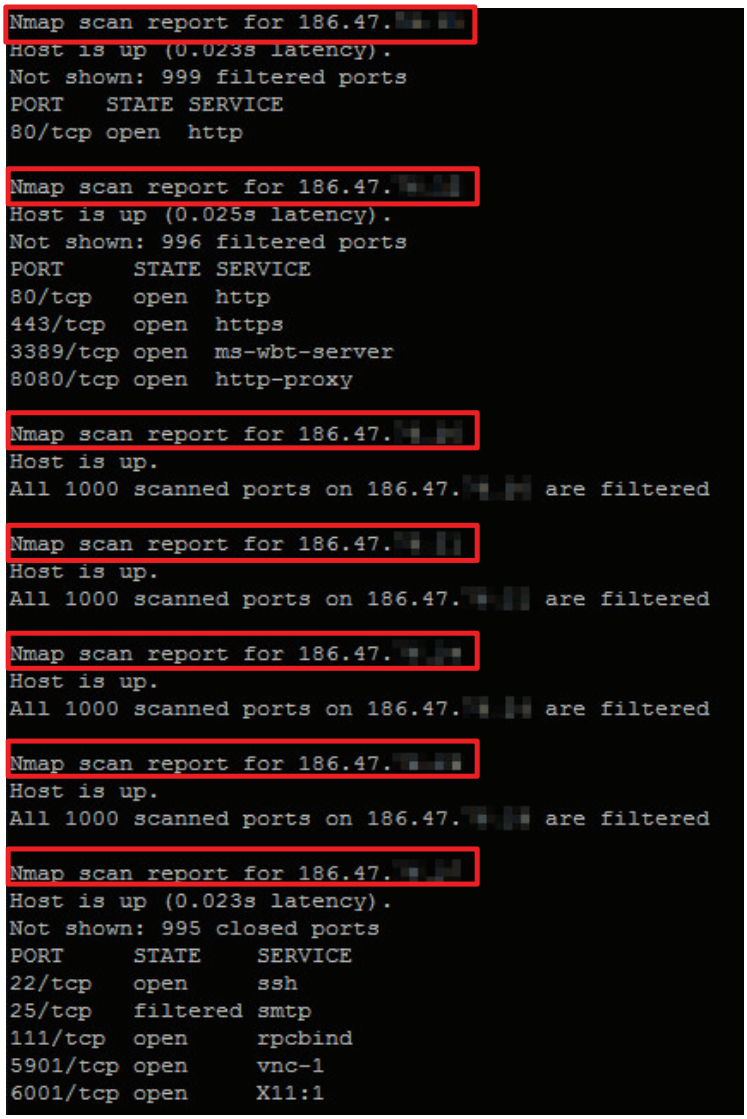


Figura 2.56 Escaneo de puertos TCP abiertos. (b)

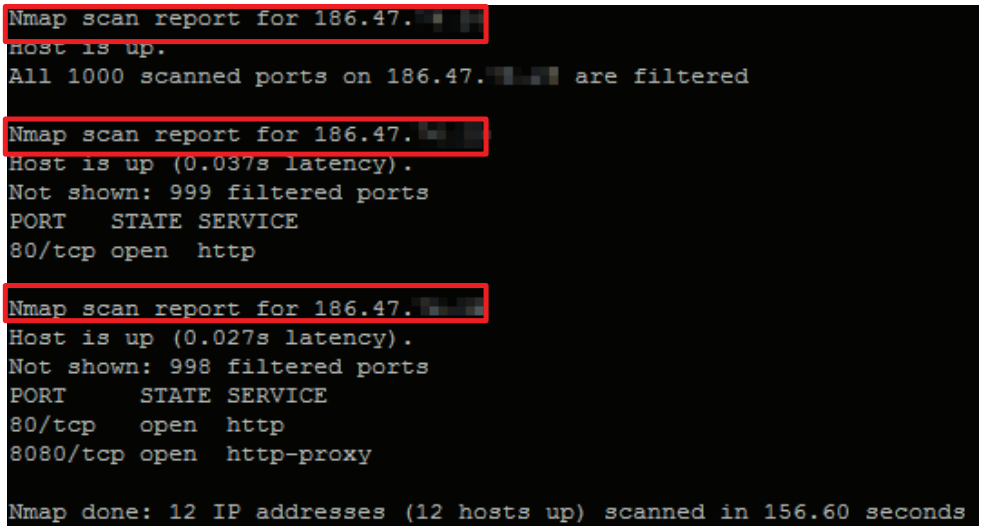


Figura 2.57 Escaneo de puertos TCP abiertos. (c)

Las figuras 2.58 y 2.59 indican los puertos UDP detectados, el estado y el servicio que corren sobre los mismos, de cada IP descubierta

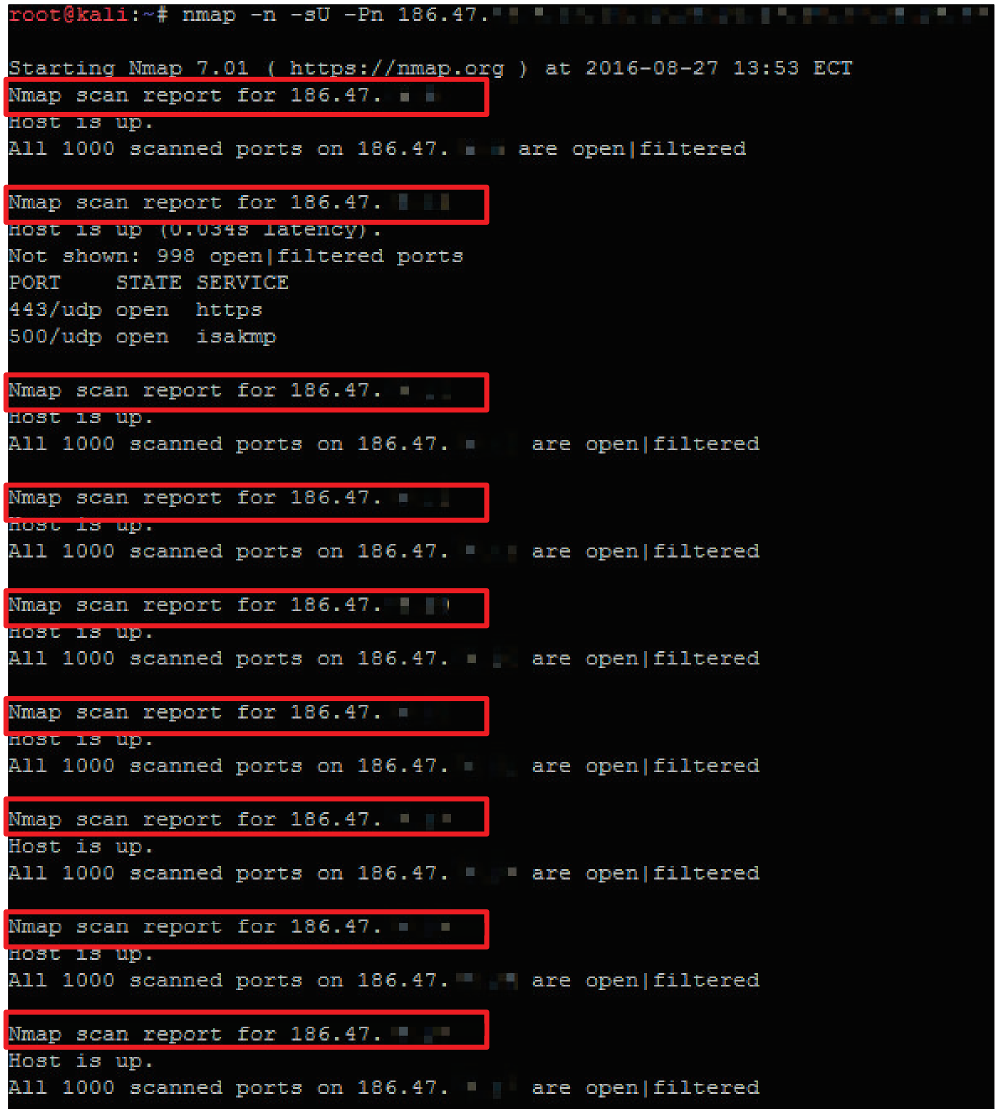


Figura 2.58 Escaneo de puertos UDP abiertos. (a)

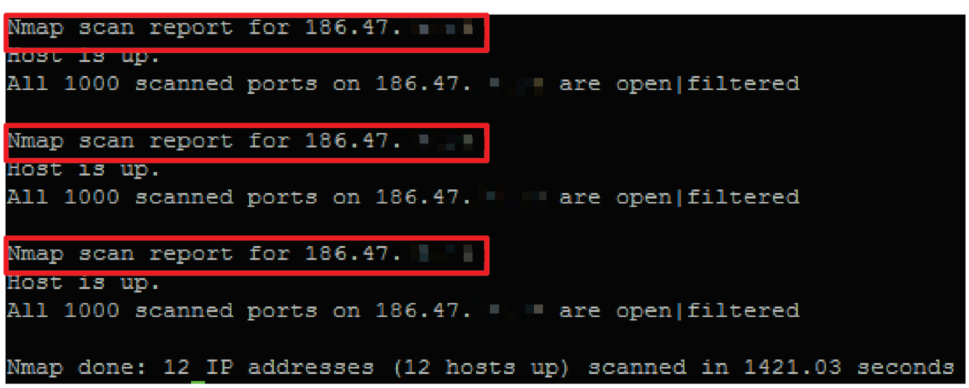


Figura 2.59 Escaneo de puertos UDP abiertos. (b)

2.1.6.4. Escaneo de Versión y Sistema Operativo

Una vez determinados los puertos abiertos en nuestro objetivo, pasaremos a identificar los servicios corriendo en cada uno de los mismos, con el propósito de conocer el número exacto de versión lo cual ayuda a establecer si el servidor es vulnerable a algún tipo de exploit.

El escaneo del sistema operativo o *fingerprinting* de nuestro objetivo es esencial, debido a que muchos exploit son escritos para S.O específicos.

Las opciones que vamos a usar son:

- sV: esta opción escanea tanto puertos TCP como UDP además de habilitar la versión de los servicios activos, con esta opción nmap intenta determinar: el protocolo del servicio, el nombre de la aplicación, número de la versión, nombre de host y tipo de destino.
- -O: detecta el sistema operativo

De la figura 2.60 a la 2.71 se puede observar el uso de nmap para realizar la consulta de la versión y el sistema operativo de cada host identificado.

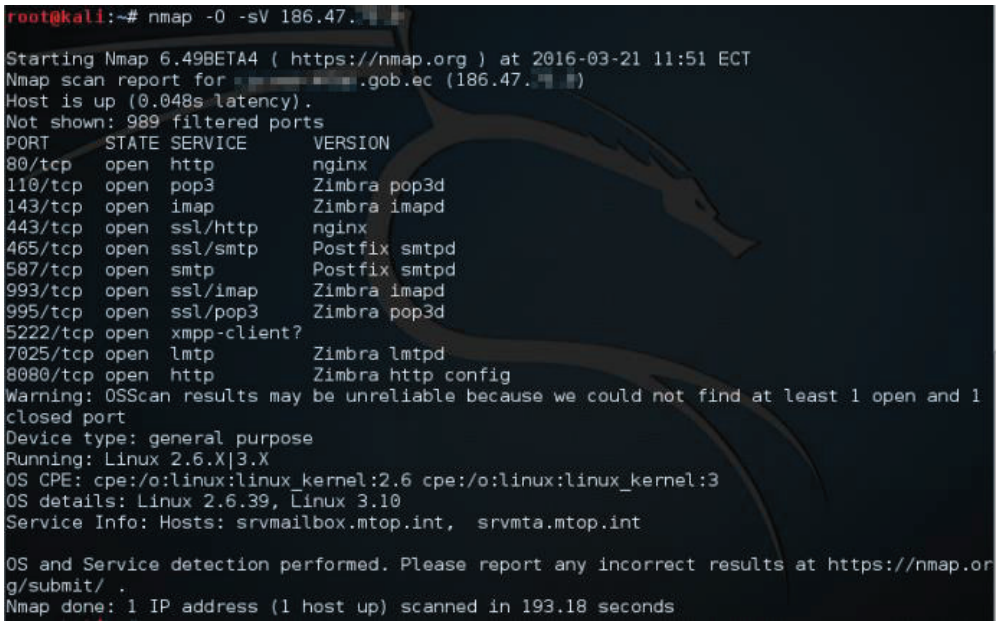


Figura 2.60 Escaneo de puertos y versión de OS a la IP 186.47.XX.A

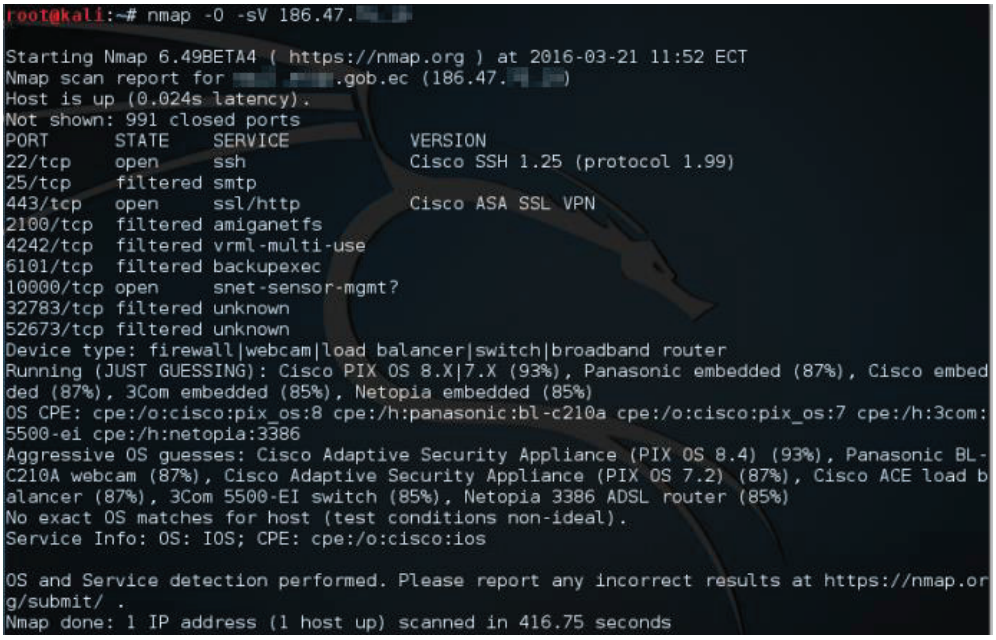


Figura 2.61 Escaneo de puertos y versión de OS a la IP 186.47.XX.B

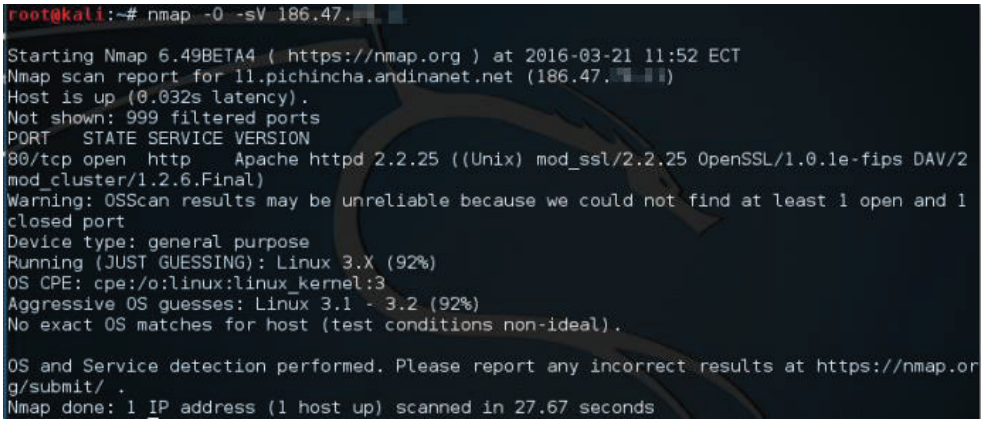


Figura 2.62 Escaneo de puertos y versión de OS a la IP 186.47.XX.C

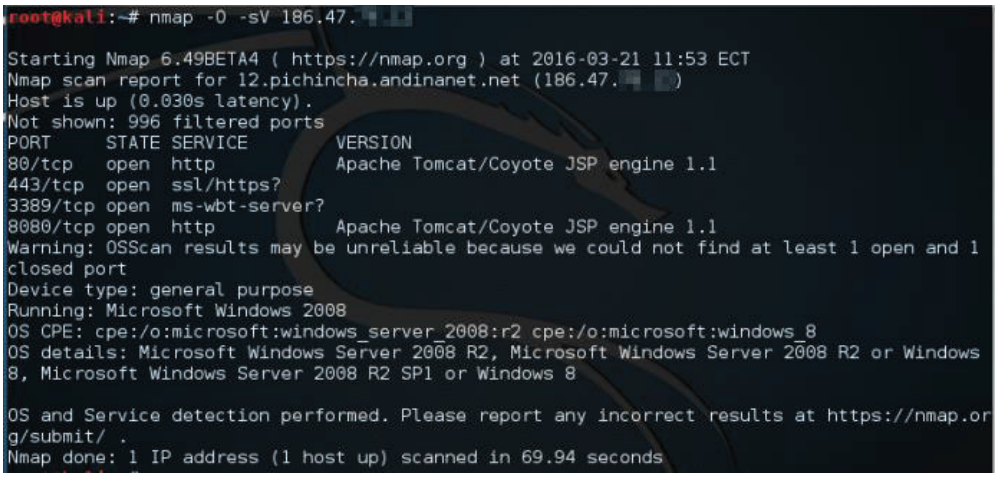


Figura 2.63 Escaneo de puertos y versión de OS a la IP 186.47.XX.D

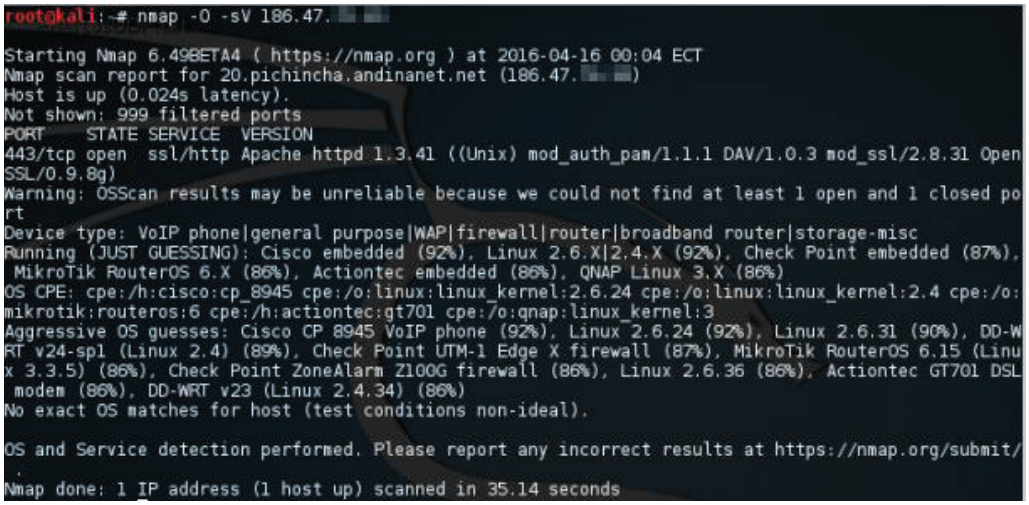


Figura 2.64 Escaneo de puertos y versión de OS a la IP 186.47.XX.E

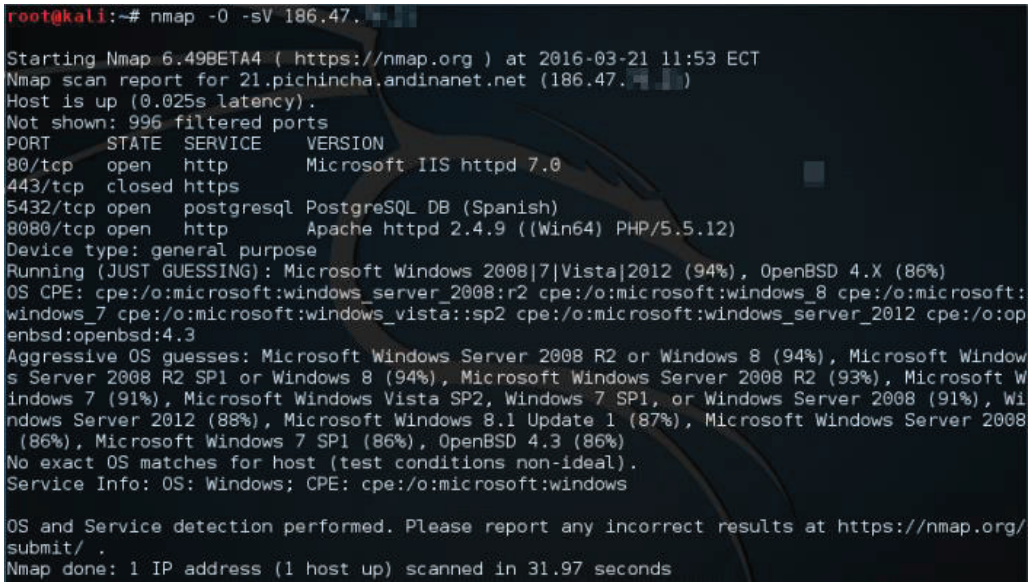


Figura 2.65 Escaneo de puertos y versión de OS a la IP 186.47.XX.F

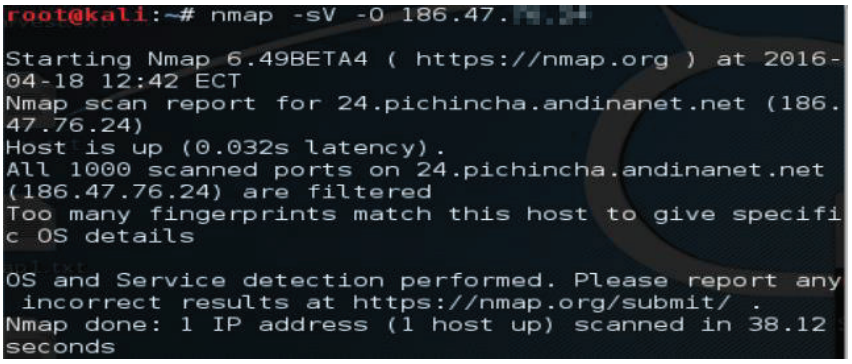


Figura 2.66 Escaneo de puertos y versión de OS a la IP 186.47.XX.G

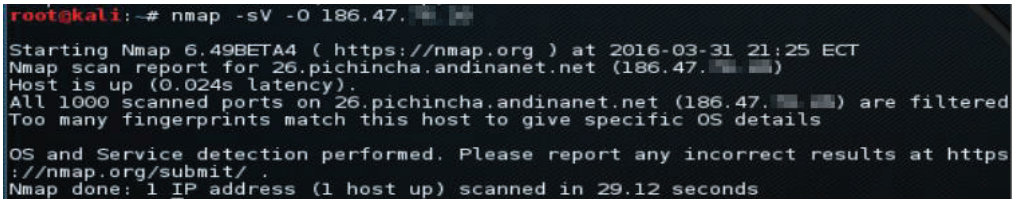


Figura 2.67 Escaneo de puertos y versión de OS a la IP 186.47.XX.H

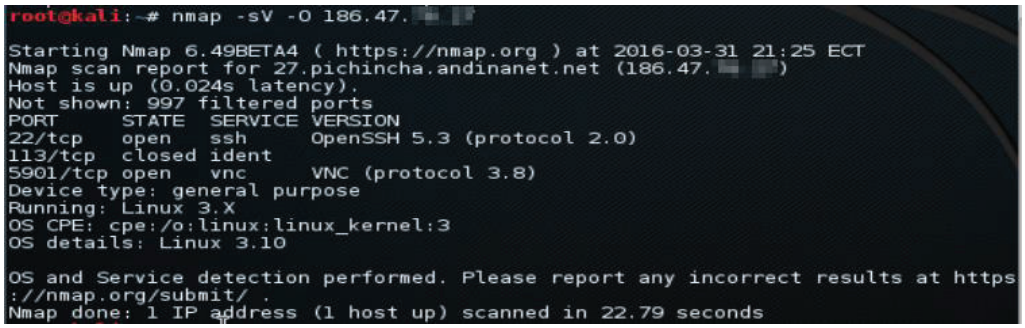


Figura 2.68 Escaneo de puertos y versión de OS a la IP 186.47.XX.I

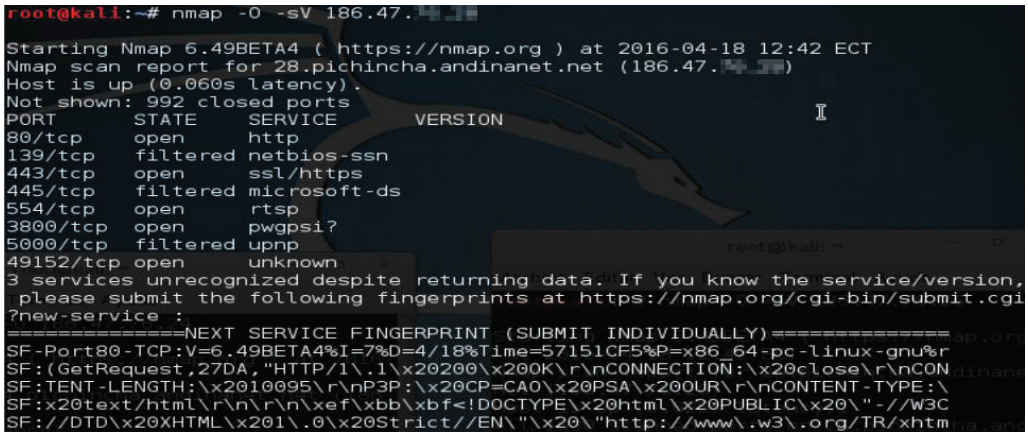


Figura 2.69 Escaneo de puertos y versión de OS a la IP 186.47.XX.J

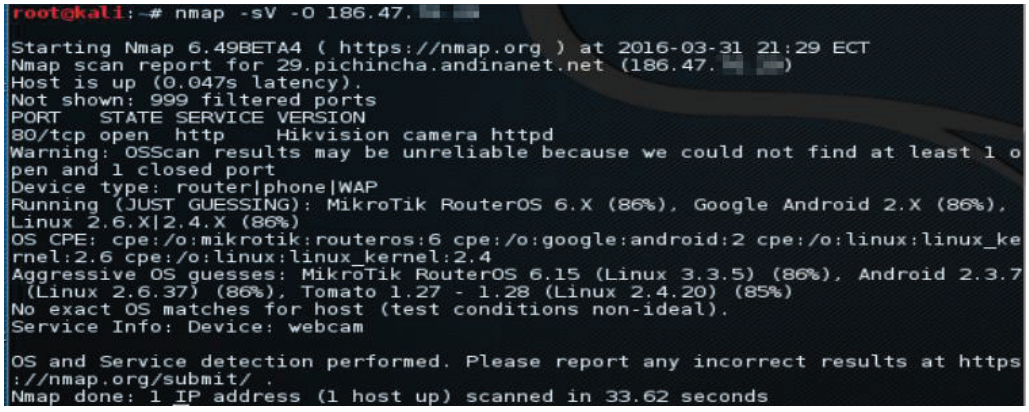


Figura 2.70 Escaneo de puertos y versión de OS a la IP 186.47.XX.K

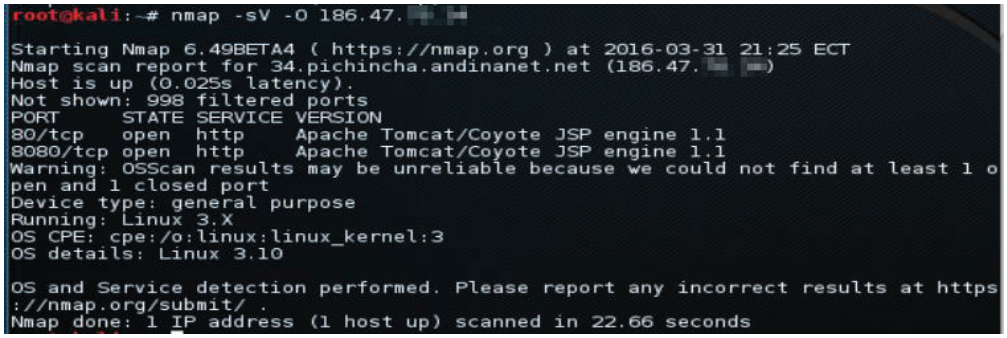


Figura 2.71 Escaneo de puertos y versión de OS a la IP 186.47.XX.L

2.2.PLANTILLA DE LA INFORMACIÓN OBTENIDA

En esta sección se detalla y se llena una parte de las plantillas relevantes de OSSTMM, las cuales permiten organizar toda la información que ha sido obtenida en el desarrollo de la fase de recopilación de información.

El formato de la plantilla a usar, especifica la información referente a:

- Perfil de Red

  Se detalla los rangos de ip activos que pertenecen al objetivo, información de dominios y de transferencia de zonas.
- Lista de servidores

  Se detalla información de la dirección IP, nombre de dominio y sistema operativo de cada servidor encontrado.
- Información del servidor

  Se detalla información de los puertos abiertos, protocolo, servicio y detalle del servicio de cada servidor.

2.2.1. Plantillas de Información Obtenida

Rangos de IP que serán probados y detalle de dichos rangos.
186.47.XX.1 – 186.47.XX.128
Información de los dominios y su configuración.
El dominio relacionado al objetivo es: dominio.gob.ec, con 4 subdominios identificados como: subdominio1.dominio.gob.ec, subdominio3.dominio.gob.ec, subdominio2.dominio, subdominio4.dominio.gob.ec

Información de transferencia de zonas a destacar.
Se obtuvo dos direcciones de servidores de resolución de dominio, pichincha.andinanet.net y Tungurahua.andinanet.net con una sola dirección IP para los dos servidores: 200.107.10.110, con las pruebas realizadas para trasferencia de zonas no se obtuvo éxito.

Tabla 2.10 Información del perfil de la red.

Lista de servidores

Dirección IP	Nombre de dominio	Sistema operativo
186.47.XX.A	subdominio1.dominio.gob.ec	Linux 2.6.x | 3.x, probable 2.6.39 o 3.10
186.47.XX.B	subdominio3.dominio.gob.ec	Cisco PIX OS 7.x | 8.x
186.47.XX.C	subdominio2.dominio.gob.ec	Linux 3.x, probable 3.1 o 3.2
186.47.XX.D	subdominio5.dominio.gob.ec	Windows server 2008 R2.
186.47.XX.E	--	Linux 2.6.X | 3.X | 2.4.X, probable 2.6.24
186.47.XX.F	subdominio4.dominio.gob.ec	Windows server 2008 R2.
186.47.XX.G	--	Unrecognized.
186.47.XX.H	--	Unrecognized.
186.47.XX.I	--	Linux 3.x
186.47.XX.J	--	Unrecognized.
186.47.XX.K	--	Microtik RouterOS 6.15 (linux 3.3.5)
186.47.XX.L	--	Linux 3.x, probable 3.10

Tabla 2.11 Lista de servidores.

2.2.2. Plantilla de Información de Servidor

Dirección IP		Nombre de dominio	
186.47.XX.A		subdominio1.dominio.gob.ec	
Puerto	**Protocolo**	**Servicio**	**Detalles del servicio**
80	http	nginx	Servidor proxy para protocolos de correo electrónico.
110	pop3	zimbra pop3d	Permite al usuario acceder a su cuenta de zimbra usando clientes como Microsoft Outlook, Mozilla Thunderbird u otro software de cliente final.
143	imap	zimbra imapd	Permite al usuario acceder a su cuenta de zimbra usando clientes como Microsoft Outlook, Mozilla Thunderbird u otro software de cliente final.
443	ssl/http	nginx	Servidor proxy para protocolos de correo electrónico.
465	ssl/smtp	postfix smtpd	Postfix es un servidor de correo de software libre, un programa informático para el enrutamiento y envío de correo electrónico.
587	smtp	postfix smtpd	Postfix es un servidor de correo de software libre, es un programa informático para el enrutamiento y envío de correo electrónico.
993	ssl/imap	zimbra imapd	Permite al usuario acceder a su cuenta de zimbra usando clientes como Microsoft Outlook, Mozilla Thunderbird u otro software de cliente final.

Puerto	Protocolo	Servicio	Detalles del servicio
995	ssl/pop3	zimbra pop3d	Permite al usuario acceder a su cuenta de zimbra usando clientes como Microsoft Outlook, Mozilla Thunderbird u otro software de cliente final.
5222	xmpp-client	--	Protocolo que permite mensajes instantáneos.
7025	lmtp	zimbra lmtpd	LMTP, es el protocolo que usan los servidores de Zimbra, cuando tenemos configurado un sistema MultiServer para entregar los mails entre ellos, ya que es más ligero que el SMTP.
8080	http	zimbra http config	Protocolo de comunicación que permite las trasferencias de información con formato de configuración hacia el servidor.

Tabla 2.12 Información del servidor 186.47.XX.A

Dirección IP		Nombre de dominio	
186.47.XX.B		subdominio3.dominio.gob.ec	
Puerto	**Protocolo**	**Servicio**	**Detalles del servicio**
22	ssh	cisco ssh 1.25 (protocolo 1.99)	Protocolo secure Shell que permite la conexión remota al host.
25	smtp	--	Protocolo para trasferencia simple de correo.
443	ssl/http	cisco ASA SSL VPN	http protocol over TLS/SSL.

Puerto	Protocolo	Servicio	Detalles del servicio
2100	amiganetfs	--	Amiga network filesystem.
4242	vrml-multi-use	--	Multi users systems,SANs.
6101	backupexec	--	Backup exec UNIX and 95/98/ME Aent, Veritas Backup Exec Advertiser.
10000	snet-sensor-mgmt	--	SecureNet Pro Sensor https management server or apple airport admin.
32783	unknow	--	--
52673	unknow	--	--
443/UDP	https	udp-response ttl 248	http protocol over TLS/SSL
500/UDP	isakmp	udp-response ttl 248	VPN Key Exchange

Tabla 2.13 Información del servidor 186.47.XX.B

Dirección IP		Nombre de dominio	
186.47.XX.C		subdominio2.dominio.gob.ec	
Puerto	**Protocolo**	**Servicio**	**Detalles del servicio**
80	http	Apache httpd 2.2.25((Unix) mod_ssl/2.2.25 OpenSSL/1.0.1e-fips DAV/2 mode_cluster/1.2.6.Final	Sevidor Web.

Tabla 2.14 Información del servidor 186.47.XX.C

Dirección IP		Nombre de dominio	
186.47.XX.D		--	
Puerto	**Protocolo**	**Servicio**	**Detalles del servicio**
80	http	Apache Tomcat/Coyote JSP engine 1.1	Servidor Web.
443	ssl/https	--	Protocolo de cifrado de comunicación a través de certificados digitales.
3389	ms-wbt-server	--	MS WBT Server, a protocol that is used by Windows Remote Desktop.
8080	http	Apache Tomcat/Coyote JSP engine 1.1	Servidor Web.

Tabla 2.15 Información del servidor 186.47.XX.D

Dirección IP		Nombre de dominio	
186.47.XX.E		--	
Puerto	**Protocolo**	**Servicio**	**Detalles del servicio**
443	ssl/https	Apache httpd 1.3.41	Servicio web, con cifrado de datos.

Tabla 2.16 Información del servidor 186.47.XX.E

Dirección IP		Nombre de dominio	
186.47.XX.F		subdominio4.dominio.gob.ec	
Puerto	**Protocolo**	**Servicio**	**Detalles del servicio**
80	http	Microsoft IIS httpd 7.0	Servidor Web y conjunto de servicios para Microsoft.
443	https	--	Protocolo de cifrado de datos, canal seguro.
5432	postgresql	postgreSQL DB (spanish)	PostgreSQL database server.
8080	http	Apache httpd 2.4.9 ((win64) PHP/5.5.12)	Servidor Web.

Tabla 2.17 Información del servidor 186.47.XX.F

Dirección IP		Nombre de dominio	
186.47.XX.I		--	
Puerto	**Protocolo**	**Servicio**	**Detalles del servicio**
22	ssh	OpenSSH 5.3	Protocolo para acceso remoto.
113	ident	--	Port 113 used for Identification/Authorization service.
5901	vnc	VNC (protocol 3.8)	Virtual Network Computer display 1.

Tabla 2.18 Información del servidor 186.47.XX.I

Dirección IP		Nombre de dominio	
186.47.XX.J		--	
Puerto	**Protocolo**	**Servicio**	**Detalles del servicio**
80	http	--	Protocolo de comunicación que permite la transferencia de información a través de la web.

Puerto	Protocolo	Servicio	Detalles del servicio
139	netbios-ssn	--	Protocolo de aplicación para compartir recursos en red, se encarga de establecer la sesión y mantener las conexiones.
443	ssl/https	--	Protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de Internet.
445	microsoft-ds	--	Servicio de directorio activo necesario para la autenticación y el acceso al directorio activo.
554	rtsp	--	Protocolo de flujo de datos en tiempo real.
3800	pwgpsi	--	--
5000	upnp	--	Conjunto de protocolos de comunicación que permite a periféricos en red, descubrir de manera transparente la presencia de otros dispositivos en la red y establecer servicios de red de comunicación, compartición de datos y entretenimiento.
49152	desconocido	--	--

Tabla 2.19 Información del servidor 186.47.XX.J

Dirección IP		Nombre de dominio	
186.47.XX.K		--	
Puerto	**Protocolo**	**Servicio**	**Detalles del servicio**
80	http	Hikvision camera httpd	Servicio de cámaras.

Tabla 2.20 Información del servidor 186.47.XX.K

Dirección IP		Nombre de dominio	
186.47.XX.L		--	
Puerto	**Protocolo**	**Servicio**	**Detalles del servicio**
80	http	Apache Tomcat/coyote JSP engine 1.1	Implementa las especificaciones de los servlets[26].
8080	http	Apache Tomcat/coyote JSP engine 1.1	Implementa las especificaciones de los servlets.

Tabla 2.21 Información del servidor 186.47.XX.L

[26] El servlet es una clase en el lenguaje de programación Java, utilizada para ampliar las capacidades de un servidor.

CAPÍTULO III

3. DESARROLLO DEL PLAN DE ATAQUES Y ESTABLECIMIENTO DE REGLAS DE OPERACIÓN

En este capítulo se detallarán las consideraciones legales que se deben tener en cuenta al momento de realizar un hacking ético, así como la documentación que se debe presentar al finalizar el trabajo.

Una vez establecidas las reglas de operación, se realizan las configuraciones de las herramientas para análisis de vulnerabilidades, las cuales nos permiten detectar posibles fallas de seguridad en el entorno objetivo descubriendo malas configuraciones, servicios sin parches, arquitecturas erróneas, entre otros escenarios.

Con las vulnerabilidades conocidas se realizará un plan de explotación o ataques el cuál será aprobado por el encargado de seguridad de la organización.

3.1.CONSIDERACIONES LEGALES DEL HACKING ÉTICO

3.1.1. Delitos Informáticos

Un Hacker Ético es un profesional de seguridad el cual debe conocer y tener en cuenta las sanciones legales a las que puede ser sometido y que son parte de las consecuencias de realizar las pruebas sin autorización. Es por esto que las actividades de hacking ético, análisis de vulnerabilidades, pruebas de penetración o auditorias de seguridad deben comenzar a realizarse una vez que se tenga un documento de autorización firmado por la Organización, el cual da permiso expreso al hacker a realizar este tipo de pruebas en la red.

De manera general los delitos informáticos o ciberdelitos[27] se los clasifica en dos categorías:

[27] "Un delito informático es toda aquella acción, típica, anti jurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet." Tomado de: http://ciberdelitoss.blogspot.com/2013/06/definicion.html

- Delitos cometidos por computadoras

  Los delitos cometidos por computadoras, son aquellos donde el equipo es usado como método o medio para realizar actividades criminales, tales como: falsificación de documentación o identidades, acceso no autorizado a archivos con el objetivo de causar fraudes, divulgación de información confidencial, uso no autorizado de programa, alteración de sistemas, intervención de redes en busca de información, entre otros.

- Delitos donde la computadora es el objetivo

  Los delitos donde la computadora es el objetivo, son aquellos donde los delitos van dirigidos hacia el equipo, accesorios o programas con el objetivo de causar daños, provocar pérdidas o impedir el uso de sistemas informáticos. Algunos ejemplos de este tipo de delitos son: programación de códigos con el objetivo de bloquear un sistema o saturar una red, daño del sistema operativo por medio de un virus, sabotaje político o terrorismo en el que se destruye la información o surge un apoderamiento de los centros neurálgicos computarizados, ransomware[28], botnet[29], etc.

3.1.2. Ética y Legalidad

En la actualidad el uso de términos tales como ciberdelincuencia[30], delitos informáticos, etc., se han convertido en un tema común. El inminente avance tecnológico que se experimenta en la sociedad, también supone nuevas formas de vulnerar los sistemas informáticos.

La ciberdelincuencia es uno de los ambientes delictivos con más rápido crecimiento, debido a las facilidades de las nuevas tecnologías. Los ataques en contra de sistemas o redes de la información, como robo o adulteración de datos, estafas bancarias y comerciales, robo de identidades, etc., son parte de

[28] El ransomware es un software malicioso que al infectar un equipo le da al ciberdelincuente la capacidad de bloquear el PC desde una ubicación remota y encripta los archivos tomando el control de toda la información y datos almacenados.

[29] El botnet es un término que hace referencia a un conjunto de red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.

[30] "La ciberdelincuencia se define con carácter general como cualquier tipo de actividad ilegal en la que se utilice Internet, una red privada o pública o un sistema informático doméstico." Tomado de: http://www.bullguard.com/es/bullguard-security-center/internet-security/security-tips/cybercrime.aspx

las actividades delictivas utilizando medios informáticos y a la vez diferentes técnicas como ingeniería social, malware avanzado con técnicas de ofuscación, inyección de código SQL, chantaje o ramsonware, etc.

La rápida propagación y el alcance mundial de este tipo de delitos han creado la necesidad que los gobiernos de todo el mundo implementen medidas para combatir, tratar y prevenir ciberdelitos.

El Convenio de Budapest o Convenio de Cibercriminalidad, es el primer tratado internacional que cubre todas las áreas relevantes a los delitos informáticos y los delitos en Internet. El objetivo de este Convenio es definir un marco de referencia en cuanto a las tecnologías y sus delitos, mediante la adopción de una legislación adecuada y la cooperación internacional, con el fin de aplicar una política penal para la protección de la sociedad. Actualmente Ecuador está analizando adherirse.

La siguiente tabla indica las conductas ilícitas definidas en el Convenio de Budapest:

Conductas Ilícitas definidas en el Convenio de Budapest	
Título 1.- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos	
Artículo 2.- Acceso ilícito	Acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático.
Artículo 3.- Interceptación ilícita	Interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.
Artículo 4.- Ataques a la integridad de los datos	Acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

Artículo 5.- Ataques a la integridad del sistema	Obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.
Artículo 6.- Abuso de los dispositivos	Cuando se cometa de forma deliberada e ilegítima la producción, posesión, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: • un dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad en los artículos 2 y 5; • una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático.
Título 2.- Delitos informáticos	
Artículo 7.- Falsificación informática	Cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que genere datos no auténticos, con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente.
Artículo 8.- Fraude informático	Actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: • la introducción, alteración, borrado o supresión de datos informáticos; • cualquier interferencia en el funcionamiento de un sistema informático.

Título 3.- Delitos relacionados con el contenido	
Artículo 9.- Delitos relacionados con la pornografía infantil	Cuando se cometa de forma deliberada e ilegítima los siguientes actos: • la producción de pornografía infantil con la intención de difundirla a través de un sistema informático; • la oferta o puesta a disposición de pornografía infantil a través de un sistema informático; • la difusión o transmisión de pornografía infantil a través de un sistema informático; • la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático; • la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.
Título 4.- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	
Artículo 10.- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.	Infracciones de la propiedad intelectual que defina su legislación.

Tabla 3.1 Resumen de delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos[31]

La legislación Ecuatoriana desde el 2002 en La ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos más conocida como Ley 67, contempla infracciones informáticas con implicaciones penales, las mismas que posteriormente fueran transcritas al Código Integral Penal.

La siguiente tabla indica las penas y/o multas a los delitos contempladas en la Ley 67:

[31] Tomado de Convenio de Budapest

CAPÍTULO I.- DE LAS INFRACCIONES

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

DELITO	PENA	MULTA (USD)
Acceso no autorizado a información.	6 meses a 1 año	$500 a $1000
Acceso no autorizado a información referente a seguridad nacional, o a secretos comerciales o industriales.	1 a 3 años	$1000 a $1500
Divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales.	Reclusión menor ordinaria de 3 a 6 años	$2000 a $10000
Divulgación o la utilización fraudulenta por parte de la persona o personas encargadas de la custodia o utilización legítima de la información.	Reclusión menos de 6 meses a 9 años	$2000 a $10000
Obtención y utilización no autorizada de información personal.	2 meses a 2 años	$1000 a $2000
Eliminación malintencionada de documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica.	3 a 6 años	No está definido
Falsificación electrónica.	No está definido	No está definido

DELITO	PENA	MULTA (USD)
Daños informáticos a programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica.	6 meses a 5 años	$60 a $150
Daños informáticos destinados a prestar un servicio público o vinculado con la defensa nacional.	3 a 5 años	$200 a $600
Destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos	8 meses a 4 años	$200 a $600
Apropiación Ilícita de bienes a través de manipulación de medios electrónicos.	6 meses a 5 años	$500 a $1000
Delitos utilizando los siguientes medios: inutilización de sistemas de seguridad, descifrado de claves, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia y violación de seguridades electrónicas, informáticas u otras semejantes	1 a 5 años	$1000 a $2000
Delitos de ingeniería social.	5 años	$500 a $1000

Tabla 3.2 Resumen de penas y/o delitos.[32]

[32] Tomado de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

3.1.3. Especificaciones para Realizar un Hacking Ético

Las pruebas de seguridad realizadas por un Hacker Ético deben ser efectuadas de manera ordenada y estructurada. El alcance de las pruebas de seguridad está determinado por las necesidades y preocupaciones del cliente. Un marco de referencia para realizar auditorías de seguridad requiere una planificación previa.

3.1.3.1. Documentos Habilitantes

Considerando las leyes que se encuentran vigentes en Ecuador en relación a los delitos de tipo informáticos (Ver tabla 3.2 Resumen de penas y/o delitos), es importante y necesario contar con documentos habilitantes donde se establezcan los alcances y limitaciones de las pruebas de penetración.

Para el presente proyecto, se consideran los siguientes documentos:

- El **convenio de confidencialidad** (Anexo 1), debe ser firmado por el personal a cargo de realizar las pruebas de seguridad, este documento es básicamente un reglamento, en el cual se describirán el tratamiento de los datos y la confidencialidad, en cuanto a la información que se conocerá, accederá y se tendrá en poder mientras dure las pruebas de penetración.
- La **carta de autorización** (Anexo 2), debe ser firmada por el responsable de la organización (Director de Tecnologías, Oficial de Seguridad, etc.) antes de realizar cualquier tipo de prueba. Este documento deberá incluir una autorización implícita donde se debe incluir al menos la definición del alcance, que es uno de los componentes más importantes en una carta de autorización, es la definición del ámbito de prueba.

3.1.3.2. Elaboración del Informe

En cualquier prueba de penetración, el informe es la parte más importante, el mismo es la clave para una prueba exitosa.

El informe debe ser preparado para el diferente tipo de personal que lo va a leer, debido que a la parte técnica no le interesa los riesgos generales y

posibles pérdidas de la empresa, así como la parte administrativa no está interesada en conocer cómo se explotaron las vulnerabilidades y que máquinas se ven afectadas.

Un informe debe contener la siguiente información:

- **Resumen Ejecutivo**

  Aquí es la parte donde se dirige únicamente a los ejecutivos de la empresa. Este resumen es la parte más esencial al momento de presentar los resultados de las pruebas de penetración, debido a que este puede hacer la diferencia entre un buen o mal informe.

  Debido a que está enfocado a la parte no técnica, se debe asegurar que sea fácilmente comprensible.

  Algunos puntos esenciales para escribir el resumen ejecutivo son los siguientes:

  - ✓ El resumen debe ser preciso, conciso y entendible.
  - ✓ El resumen debe iniciar con una definición del propósito del contrato y como este se llevó a cabo. Se definirá el ámbito de aplicación con mucha precisión.
  - ✓ Se explicarán los resultados de las pruebas y los hallazgos.
  - ✓ Se incluirán las debilidades en general y las contramedidas que no fueron implementadas las cuales causaron la vulnerabilidad.
  - ✓ Se indicará el riesgo general como resultado de las vulnerabilidades.
  - ✓ Por último, se indicará la disminución del riesgo una vez que se implementen las recomendaciones para corregir las vulnerabilidades.

- **Reporte de Remediación**

  El siguiente paso es el resumen, será tener el reporte de remediación, el cual contiene recomendaciones en general, las cuales unas vez implementadas aumentarían la seguridad de la organización. Esta sección es específicamente para el área de Gestión, ya que este grupo es el encargado de reforzar las políticas de seguridad de una organización.

Como se mencionó anteriormente, este grupo puede o no ser técnico; por lo tanto el reporte de remediación debe ser muy preciso y fácil de entender. Se pueden recomendar cosas que mejoren la seguridad en general, así como: un firewall, un sistema de detección de intrusos, etc.

- **Resumen de la Evaluación de Vulnerabilidad**
  Esta sección hace referencia a un resumen de hallazgos. Aquí se presentarán todos los resultados, que serán útiles para que el personal de seguridad pueda entender de mejor manera las vulnerabilidades e implementar contramedidas.
  Existen diferentes formas de representar los resultados de una evaluación de riesgos.
- **Plan de Correcciones**
  Aquí es donde nos enfocaremos al personal técnico, detallando las vulnerabilidades encontradas, los riesgos asociados y actividades para mitigar las mismas.

3.2.ESCANEO DE VULNERABILIDADES

Una vez que se ha recopilado la información del objetivo, el siguiente paso es buscar vulnerabilidades potenciales para comprometer los sistemas.

Un escáner de vulnerabilidades es una herramienta diseñada para evaluar vulnerabilidades de un sistema objetivo basado en un rango de puertos y un conjunto de políticas.

Existe un gran número de bases de datos de vulnerabilidades conocidas, que mantienen un registro de todos los fallos de seguridad recientemente publicados.

Una base de datos de vulnerabilidades públicamente conocida y la cual se usa en el presente trabajo es el CVE (Common Vulnerability and Exposures), permite identificar una vulnerabilidad asignando a cada una un código de identificación único, conocido como CVE-ID.

Para determinar el impacto, los escáneres de vulnerabilidades usan una escala que va del 0 al 10, donde la severidad se considera:

- Baja: si esta entre 0.0 y 3.9
- Media: si esta entre 4.0 y 6.9
- Alta: si esta entre 7.0 y 10.0

3.2.1. OpenVAS

El Sistema Abierto de Evaluación de Vulnerabilidad (OpenVAS, The Open Vulnerability Assessment System) es un marco de referencia que incluye varios servicios y herramientas que ofrecen una solución completa y potente de escaneo y administración de vulnerabilidades, para esto OpenVAS ejecuta las denominas NVT, que son pruebas de vulnerabilidades de red, las cuales son rutinas que analizan la presencia de algún fallo de seguridad en el objetivo.

Antes de usar OpenVAS, se deben ejecutar algunos comandos con el fin de actualizar las Pruebas de Vulnerabilidades de Red (NVT), así como iniciar el servicio y conexiones necesarias. Los comandos necesarios son:

- openvas-setup
- openvas-start

Una vez realizadas todas las configuraciones entramos al navegador y colocaremos la dirección http://127.0.0.1:9392 para abrir “Greenbone Security Assistant”

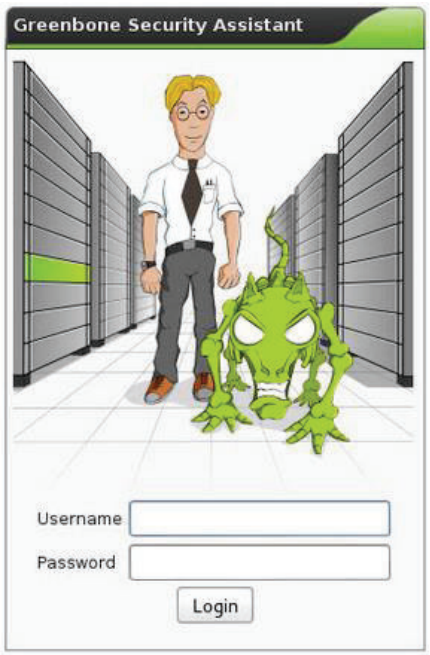


Figura 3.1 Pantalla de inicio de OpenVAS.

Una vez en la interfaz lo primero que se hace es configurar la lista de puertos de cada una de las IP's analizadas:

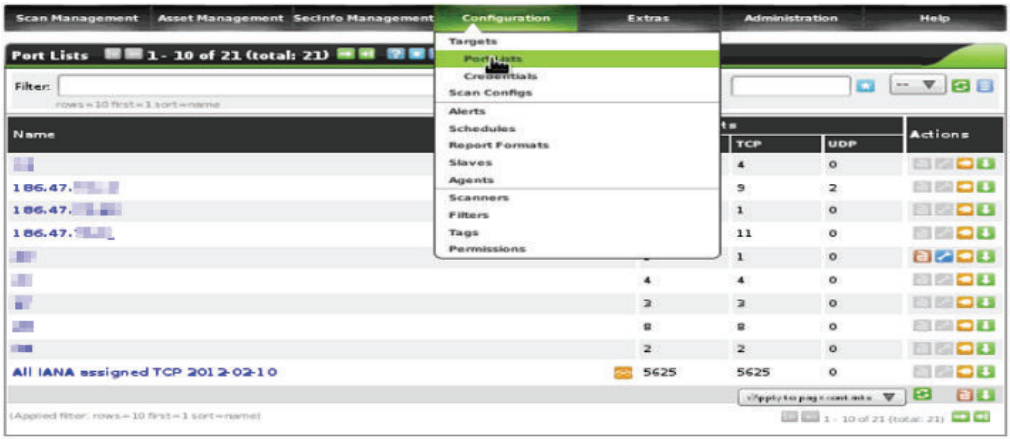


Figura 3.2 Configuración de listas de puertos en OpenVAS.

El segundo paso es crear todos los objetivos a analizar y asociarlos con la lista de puertos correspondiente.

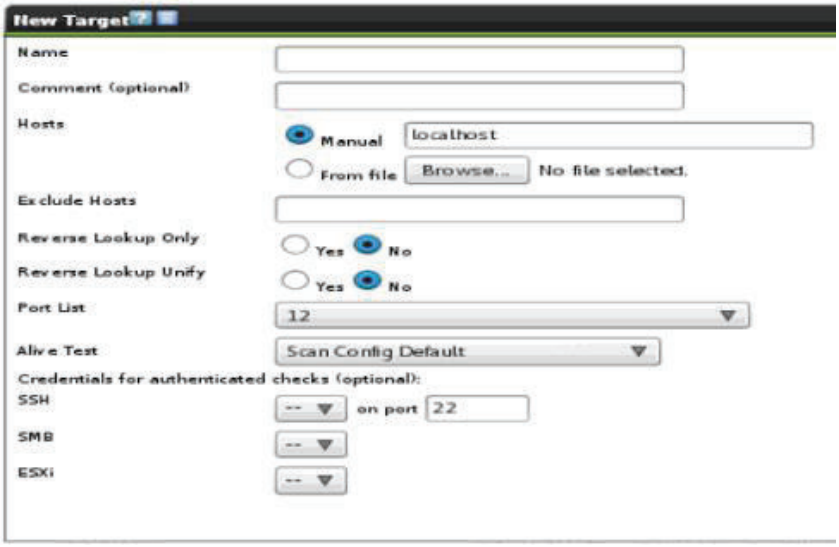


Figura 3.3 Configuración del grupo de host en OpenVAS.

Una vez que el grupo de host ha sido configurado, se crea una nueva tarea, desde el enlace "Task".

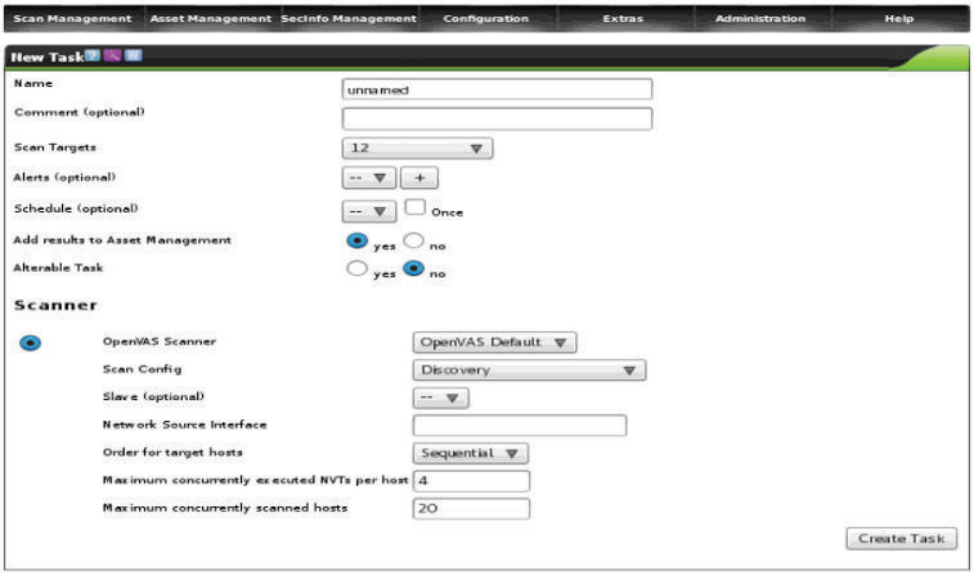


Figura 3.4 Configuración de Tareas en OpenVAS

En la figura 3.4, se puede observar la opción *"Scan Config"* que OpenVAS tiene pre-configurado, para el presente proyecto se utilizará "*Full and very Deep ultimate"* este tipo de escaneo explota la mayoría de NVT's.

OpenVas entrega un informe de los resultados de cada escaneo que realiza, en el Anexo 3 se observa un ejemplo del informe completo de un host analizado.

Una vez realizados los análisis obtenemos los siguientes resultados:

HOST	RESULTADO DEL ESCANEO DE VULNERABILIDADES			
	ALTO	MEDIO	BAJO	LOGS
186.47.XX.A	0	0	0	0
186.47.XX.B	0	3	1	21
186.47.XX.C	1	2	1	13
186.47.XX.D	0	6	2	30
186.47.XX.E	2	12	1	19
186.47.XX.F	10	6	2	22
186.47.XX.I	0	1	2	9
186.47.XX.J	0	0	0	20
186.47.XX.K	0	0	1	9
186.47.XX.L	0	0	1	17

Tabla 3.3 Resultados del análisis de vulnerabilidades con OpenVAS.

A continuación se presenta un resumen de las vulnerabilidades altas encontradas por OpenVas:

IP: 186.47.XX.C	
Vulnerabilidad:	**GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerability**
Severidad:	10.0 (Alto)
Puerto:	80/tcp
CVE-ID:	CVE-2014-6271, CVE-2014-6278
Descripción:	En este host está instalado con GNU Bash Shell, el cual es propenso a la vulnerabilidad de ejecución remota de comandos. La explotación exitosa de esta debilidad permite a los atacantes remotos o locales inyectar comandos shell, lo que permite una elevación local de privilegios o ejecución remota de comandos.
IP: 186.47.XX.E	
Vulnerabilidad:	**LiteServe URL Decoding DoS**
Severidad:	9.3 (Alto)
Puerto:	443/tcp
CVE-ID:	No identificado
Descripción:	El servidor Web remoto colapsa cuando un URL consiste en una cadena larga no válida, un atacante puede usar esta debilidad para hacer caer el servidor continuamente.
Vulnerabilidad:	**Header overflow against HTTP proxy**
Severidad:	7.5 (Alto)
Puerto:	443/tcp
CVE-ID:	CVE-2002-0133
Descripción:	Es posible anular el proxy HTTP mediante el envío de una solicitud inválida, con una cabecera muy larga. Un atacante puede explotar esta vulnerabilidad haciendo colapsar el servidor proxy continuamente o incluso ejecutar código arbitrario en el sistema.

IP: 186.47.XX.F	
Vulnerabilidad:	**php Multiple Vulnerabilities -01 April16 (Windows)**
Severidad:	10.0 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2016-3142, CVE-2016-3141
Descripción:	Este host tiene instalado php con una versión vulnerable a múltiples amenazas. La explotación exitosa de las debilidades puede permitir a un atacante remoto ganar acceso a información potencialmente sensible y así llevar a cabo una denegación de servicio, corrupción de memoria y/o colapso de la aplicación.
Vulnerabilidad:	**php Multiple Vulnerabilities -01 June15 (Windows)**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-4148, CVE-2015-4147, CVE-2015-2787, CVE-2015-2348, CVE-2015-2331
Descripción:	Este host tiene instalado php con una versión vulnerable a múltiples amenazas. La explotación exitosa de las debilidades puede permitir a un atacante remoto ganar acceso a información sensible.
Vulnerabilidad:	**php Multiple Vulnerabilities -02 June15 (Windows)**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-4026, CVE-2015-4025, CVE-2015-4024, CVE-2015-4022, CVE-2015-4021
Descripción:	Este host tiene instalado php con una versión vulnerable a múltiples amenazas. La explotación exitosa de las debilidades puede permitir a un atacante remoto provocar una denegación de servicio, evitar restricciones de extensiones, acceder y ejecutar archivos o directorios con nombres inesperados a través de dimensiones manipuladas y servidores FTP remotos para ejecutar código arbitrario.

Vulnerabilidad:	**php Multiple Vulnerabilities -03 June15 (Windows)**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-3329, CVE-2015-3307, CVE-2015-2783, CVE-2015-1352
Descripción:	Este host tiene instalado php con una versión vulnerable a múltiples amenazas. La explotación exitosa de las debilidades presentes puede permitir a un atacante remoto provocar una denegación de servicio, para obtener información sensible desde el procesamiento de memoria y ejecutar código arbitrario.
Vulnerabilidad:	**php Multiple Remote Code Execution Vulnerabilities July15 (Windows)**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-0273, CVE-2014-9705
Descripción:	Este host tiene instalado php con una versión vulnerable a múltiples amenazas. La explotación exitosa de las debilidades presentes puede permitir a un atacante remoto ejecutar código arbitrario.
Vulnerabilidad:	**php Use-After-Free Remote Code EXecution Vulnerability -01 July15 (Windows)**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-2301
Descripción:	Este host tiene instalado php con una versión vulnerable a múltiples amenazas. La explotación exitosa de las debilidades presentes puede permitir a un atacante remoto ejecutar código arbitrario sobre el sistema objetivo.

Vulnerabilidad:	**php Use-After-Free Denial Of Service Vulnerability - 02 July15 (Windows)**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-1351
Descripción:	Este host tiene instalado php y es propenso a la vulnerabilidad de denegación de servicio. La explotación exitosa de esta debilidad permite a un atacante remoto provocar una denegación de servicios.
Vulnerabilidad:	**php Multiple Vulnerabilities -01 March16 (Windows)**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-6831, CVE-2015-6832, CVE-2015-6833
Descripción:	Este host tiene instalado php con una versión vulnerable a múltiples amenazas. La explotación exitosa de las debilidades presentes puede permitir a un atacante remoto ejecutar código arbitrario para crear o sobre-escribir ficheros aleatorios en el sistema y esto puede conducir a lanzar nuevos ataques.
Vulnerabilidad:	**php 'serialize function call' Function Type Confusion Vulnerability March16 (Windows)**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-6836
Descripción:	Este host tiene instalado php y es propenso a la vulnerabilidad de ejecución de código remoto. La explotación exitosa de esta debilidad puede permitir a un atacante remoto ejecutar código arbitrario cuando un usuario ejecute una aplicación afectada. Los intentos fallidos de explotación probablemente pueden causar una condición de denegación de servicios.

Vulnerabilidad:	**php 'phar x lepath' Function Stack Buffer Overflow Vulnerability March16 (Windows)**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-5590
Descripción:	Este host tiene instalado php y es propenso a la vulnerabilidad de desbordamiento de buffer. La explotación exitosa de esta debilidad puede permitir a un atacante remoto ejecutar código arbitrario. Los intentos fallidos de esta explotación probablemente colapsarían el servidor web.

Tabla 3.4 Análisis de vulnerabilidades con OpenVAS.

3.2.2. Nessus[33]

Nessus es una herramienta de análisis de vulnerabilidades, su categorización en la comunidad y el uso por parte de los profesionales que trabajan en el área de seguridad informática opinan que es una de las herramientas más completas y poderosas en el mercado, brinda una amplia gama de productos, los cuales se ajustan a la necesidad de análisis. Para el propósito de nuestro proyecto utilizaremos NESSUS PROFESIONAL, en la versión de prueba, el cual tiene ciertas limitantes para su aplicación en ambientes reales como son: el número de escaneos, el número de direcciones IP, tiempo de uso, etc.

Nessus llega a posesionarse en el mercado y a calificarse como una de las herramientas más poderosas para auditoría y evaluación de seguridad debido a su gran desarrollo de programas llamados Plugins, los cuales son los encargados de mantener Nessus actualizado con información acerca del descubrimiento de nuevas vulnerabilidades registradas en los dominios públicos.

Para hacer uso de la herramienta mencionada en sus distintas versiones y productos se requiere descargar el instalador a través de la página oficial, allí encontraremos las versiones de prueba o bien las versiones pagadas según sea el requerimiento, dividido por sistema operativo donde se va a instalar, se

[33] Referencia: *http://www.tenable.com/products/nessus-vulnerability-scanner*

sugiere leer la documentación correspondiente al producto para su instalación y configuración.

- **Inicio y configuración de Nessus**

Después de haber descargado e instalado el programa se inicia el servicio a través de Nessus Web Client, el cual abrirá un navegador y posteriormente se ingresa las credenciales de acceso, las mismas que fueron configuradas durante la instalación.

Para el desarrollo del proyecto se ha configurado la herramienta con escaneos dirigidos a cada objetivo, y su configuración se muestra a continuación:

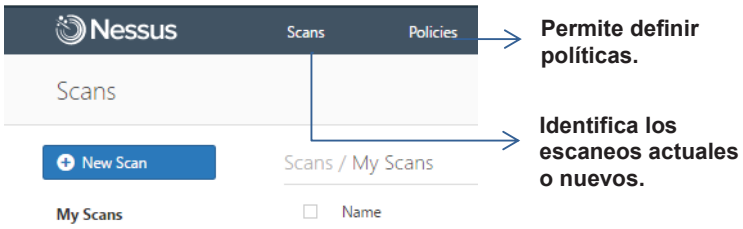


Figura 3.5 Página principal de Nessus.

En la figura 3.5 podemos ver dos opciones de menú, los cuales nos indican:

Scans: Identifica los escaneos actuales o nuevos.
Policies: Permite definir políticas

- **Creación de un escaneo**

Se omite la creación de políticas, debido a que por tratarse de pocas IP's se realiza un escaneo manual.

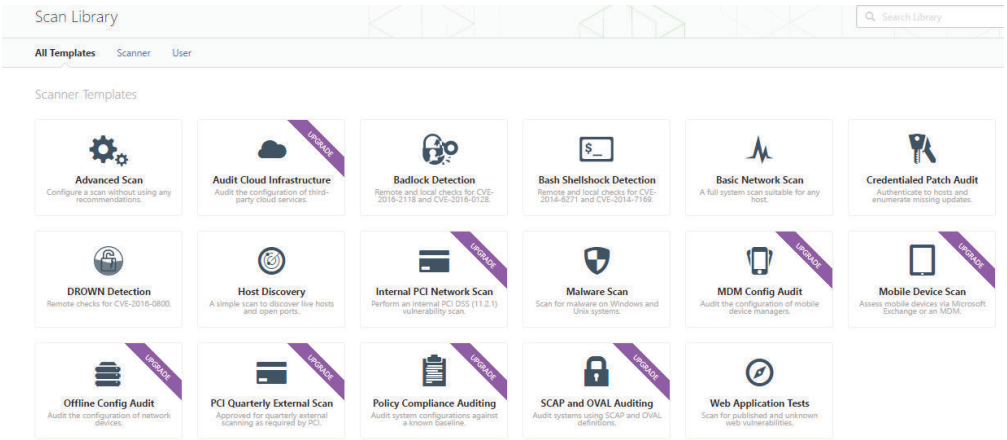


Figura 3.6 Configuración de nuevo escáner de NESSUS.

En la figura 3.6 se puede observar que cada una de las plantillas hace referencia a una configuración específica de escaneo, para realizar un escaneo más personalizado y completo se utiliza un escaneo avanzado, en el cuál se deben especificar los siguientes argumentos:

Básico	General	**Nombre:** nombre de referencia del escaneo. **Descripción:** descripción de referencia. **Carpeta:** ubicación del escaneo dentro de la herramienta Nessus. **Objetivos:** objetivo u objetivos a escanear. **Nota:** es posible ingresar un archivo de texto que contenga la lista de objetivos.
	Programar	Habilitar escaneo programado.
	Notificaciones	**Correo electrónico de destinatario:** permite enviar los resultados a dirección(es) de correo.
Descubrimiento	Descubrimiento de Host	**Ajustes generales:** especifica el comportamiento de Nessus frente al escaneo de host activos. **Métodos de ping:** ARP, TCP, ICMP, UDP. **Tipo de red:** Pública WAN, Privada LAN, Mixta).
	Escaneo de Puertos	**Puertos:** lista de puertos a escanear. **Enumeración local del puerto:** SSH, WMI, SNMP.
	Descubrimiento de Servicios	**Ajustes generales:** sondeo de puertos para encontrar servicios.
Evaluación	General	Exactitud Antivirus SMTP
	Fuerza Bruta	Permite escanear cuentas por defecto.
	Aplicaciones web	**Ajustes Generales:** Rastreador web, configuración de pruebas de aplicación.
Reporte	Permite modificar el comportamiento de los resultados	

Tabla 3.5 Configuraciones avanzadas de escaneo en Nessus.

Finalmente se guardan los cambios de la configuración y se ejecuta el escaneo.

Nessus entrega un informe de los resultados de cada escaneo que realiza, en el Anexo 4 se observa un ejemplo del informe completo de un host analizado.

Una vez escaneadas todas las direcciones IP, obtenemos los siguientes resultados:

HOST	RESULTADO DEL ESCANEO DE VULNERABILIDADES				
	CRÍTICO	ALTO	MEDIO	BAJO	INFO
186.47.XX.A	0	0	9	3	47
186.47.XX.B	0	0	6	3	27
186.47.XX.C	1	0	2	0	21
186.47.XX.D	1	2	12	2	31
186.47.XX.E	1	6	29	0	37
186.47.XX.F	6	13	8	1	30
186.47.XX.I	0	0	1	2	18
186.47.XX.J	0	0	8	2	31
186.47.XX.K	0	0	1	0	13
186.47.XX.L	0	0	0	0	16

Tabla 3.6 Resultado del análisis de vulnerabilidades de Nessus.

A continuación se presenta un resumen de las vulnerabilidades críticas y altas encontradas por el escáner:

IP: 186.47.XX.C	
Vulnerabilidad:	**GNU Bash Environment Variable Handling Code Injection (Shellshock)**
Severidad:	10.0 (Crítico)
Puerto:	80/tcp
CVE-ID:	CVE-2014-6271
Descripción:	El servidor remoto es afectado por una vulnerabilidad de inyección de comando de GNU Bash conocido como Shellshock. Esto puede permitir a un atacante remoto ejecutar código arbitrario por medio de la manipulación de una variable de entorno dependiendo de la configuración del sistema.
IP: 186.47.XX.D	
Vulnerabilidad:	**MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)**
Severidad:	10.0 (Crítico)
Puerto:	3389/tcp
CVE-ID:	CVE-2014-6321
Descripción:	El host remoto Windows está afectado por una vulnerabilidad de ejecución de código remota debido a un inadecuado procesamiento de paquetes por un canal seguro (Schannel). Un atacante puede aprovechar esta vulnerabilidad mediante el envío de paquetes especialmente diseñados para este servidor de Windows.
Vulnerabilidad:	**MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)**
Severidad:	9.3 (Alto)

Puerto:	3389/tcp
CVE-ID:	CVE-2012-0002, CVE-2012-0152
Descripción:	Existe una vulnerabilidad remota de código arbitrario en la implementación del Protocolo de Escritorio Remoto (RDP) en un host remoto Windows. Si es que RDP ha sido habilitado en el sistema afectado, un atacante puede aprovechar esta vulnerabilidad para causar que se ejecute código arbitrario en el sistema mediante el envío de una secuencia de paquetes RDP especialmente diseñado para esto.
Vulnerabilidad:	**Apache Tomcat 6.0.x < 6.0.43 Multiple Vulnerabilities (POODLE)**
Severidad:	9.3 (Alto)
Puerto:	80/tcp
CVE-ID:	CVE-2010-5298, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470, CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508, CVE-2014-3509, CVE-2014-3510, CVE-2014-3511, CVE-2014-3512, CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568.
Descripción:	La versión del servidor remoto Apache Tomcat puede ser afectado por múltiples vulnerabilidades: • Existencia de un error de desbordamiento de buffer relacionado con un fragmento DTLS inválido, que puede conducir a la ejecución arbitraria de código. Hay que tener en cuenta que esta debilidad solo afecta OpenSSL cuando se utiliza DTLS como cliente o servidor. • Existencia de un error relacionado con el manejo de negociación de DTLS que puede conducir a ataques de denegación de servicios. Notar que esta debilidad solo afecta a OpenSSL cuando se usa DTLS como cliente.

	• Existencia de un error de pérdida de memoria en 'd1_both.c' relacionado con el manejo de paquetes DTLS especialmente diseñados, que permiten ataques de denegación de servicio. • Existencia de un error en la función 'OBJ_obj2txt' cuando varias funciones de impresión 'X509_name_*' son bastante usadas, lo cual genera fuga de datos de la pila de procesos, resultando una divulgación de la información.
IP: 186.47.XX.E	
Vulnerabilidad:	**OpenSSL Unsupported**
Severidad:	10.0 (Crítico)
Puerto:	443/tcp
CVE-ID:	No especificado
Descripción:	El servidor remoto está ejecutando una versión de OpenSSL que ya no se admite. La falta de apoyo implica que no hay nuevos parches de seguridad para el producto que puedan ser liberados por el fabricante. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Vulnerabilidad:	**OpenSSL < 0.9.8s Multiple Vulnerabilities**
Severidad:	9.3 (Alto)
Puerto:	443/tcp
CVE-ID:	CVE-2011-1945, CVE-2011-4108, CVE-2011-4109, CVE-2011-4576, CVE-2011-4577, CVE-2011-4619.
Descripción:	El host remoto está ejecutando una versión de OpenSSL mayor a 0.9.8s. Esas versiones pueden tener las siguientes vulnerabilidades: • Existencia de un error relacionado con firmas ECDSA y curvas binarias. La implementación de curvas sobre campos binarios permitiría un control remoto. Un atacante no autenticado podría determinar la clave privada a través de ataques puntuales.

	• La aplicación del protocolo DTLS es vulnerable a ataques de recuperación de texto plano cuando el descifrado es modo CBC. • Existencia de un error relacionado con los registros SSLv3.0 que puede conducir a la divulgación de memoria. • Existencia de un error relacionado con el procesamiento RFC 3779 que puede permitir ataques de denegación de servicio. Hay que tener en cuenta que esta funcionalidad no está habilitada por defecto y se debe configurar en tiempo de compilación a través de la opción 'enable-rfc3779'. • Existencia de un error relacionado con el reseteo del establecimiento de conexión del servidor de criptografía cerrada (SGC) lo que permite un ataque de denegación de servicio.
Vulnerabilidad:	**OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities**
Severidad:	9.3 (Alto)
Puerto:	443/tcp
CVE-ID:	CVE-2014-0076, CVE-2014-0195, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470.
Descripción:	El host remoto está ejecutando una versión de OpenSSL anterior a 0.9.8w. La librería de OpenSSL puede ser afectada por las siguientes vulnerabilidades: • Existencia de un error de desbordamiento de buffer relacionado con el manejo de un fragmento DTLS inválido, el cual podría provocar la ejecución de código arbitrario. • Existencia de un error relacionado con el manejo del establecimiento de conexión DTLS que puede permitir ataques de denegación de servicio. Tomar en cuenta que esta debilidad solo afecta a OpenSSL cuando se utiliza DTLS como cliente.

	• Existencia de un error no especificado que podría permitir a un atacante provocar el uso de claves débiles, lo que conduce a ataques tipo man-in-the-middle. • Existencia de un error no especificado relacionado con conjunto de cifrado anónimo ECDH el cual puede permitir ataques de denegación de servicio. Tener en cuenta que esta debilidad solo afecta a clientes OpenSSL TLS.
Vulnerabilidad:	**OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow**
Severidad:	7.6 (Alto)
Puerto:	443/tcp
CVE-ID:	CVE-2010-3864
Descripción:	El host remoto está ejecutando una versión de OpenSSL anterior a 0.9.8p / 1.0.0b. Si un servidor TLS es multiproceso y usa el caché SSL, un atacante remoto podría desencadenar un desbordamiento de buffer y colapsar el servidor o ejecutar código arbitrario.
Vulnerabilidad:	**Unsupported Web Server Detection**
Severidad:	7.5 (Alto)
Puerto:	443/tcp
CVE-ID:	No especificado.
Descripción:	El servidor web remoto es obsoleto y ya no es soportado por el fabricante. La falta de apoyo implica que no hay nuevos parches de seguridad para el producto que puedan ser liberados por el fabricante. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Vulnerabilidad:	**OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption**
Severidad:	7.5 (Alto)
Puerto:	443/tcp

CVE-ID:	CVE-2012-2110, CVE-2012-2131
Descripción:	El host remoto está ejecutando una versión de OpenSSL anterior a 0.9.8w. Como tal, la propia biblioteca OpenSSL según los informes, se ve afectada por una vulnerabilidad de corrupción de memoria a través de un error de truncamiento.
Vulnerabilidad:	**OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities**
Severidad:	7.1 (Alto)
Puerto:	443/tcp
CVE-ID:	CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508, CVE-2014-3510.
Descripción:	El servidor remoto está ejecutando una versión de OpenSSL 0.9.8 anterior a 0.9.8zb. La librería de OpenSSL es, por lo tanto, puede ser afectada por las siguientes vulnerabilidades: • Existencia de un error de memoria double-free relacionado con el manejo de paquete DTLS que permite ataques de denegación de servicio. • Existencia de un error de pérdida de memoria relacionado con el manejo de paquetes DTLS, que permiten ataques de denegación de servicio. • Existencia de un error de referencia de puntero NULL relacionado con el manejo de paquetes de cifrado anónimo ECDH y mensajes de reconocimiento diseñados que permiten ataques de denegación de servicio contra los clientes.
IP:186.47.XX.F	
Vulnerabilidad:	**PHP 5.5.x < 5.5.14 Multiple Vulnerabilities**
Severidad:	10.0 (Crítico)
Puerto:	8080/tcp
CVE-ID:	CVE-2014-0207, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487, CVE-2014-3515, CVE-2014-3981, CVE-2014-4049, CVE-2014-4721.

Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.14. Por lo tanto, el servidor puede ser afectado por múltiples vulnerabilidades: • Existencia de un error en el manejo del tamaño de la cadena Pascal relacionado con la extensión Fileinfo y la función 'mconvert'. • Existencia de un error type-confusion relacionado con la extensión de la Librería Estándar PHP (SPL) y la función 'unserialize'. • Existencia de un error relacionado con scripts de configuración y manejo de archivos temporales, que podría permitir el uso de archivos inseguros. • Existencia de un error de desbordamiento de buffer de heap-based relacionado con la función 'dns_get_record', que podría permitir la ejecución de código arbitrario.
Vulnerabilidad:	**PHP 5.5.x < 5.5.29 Multiple Vulnerabilities**
Severidad:	10.0 (Crítico)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-6834, CVE-2015-6835, CVE-2015-6836, CVE-2015-6837, CVE-2015-6838.
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.29. Por lo tanto, el servidor puede ser afectado por múltiples vulnerabilidades: • Existencia de múltiples errores de memoria use-after-free relacionados con la función unserialize(). Un atacante remoto podría explotar este error mediante la ejecución de código arbitrario.
Vulnerabilidad:	**PHP prior to 5.5.x<5.5.31 / 5.6.x<5.6.17 Multiple Vulnerabilities**
Severidad:	10.0 (Crítico)
Puerto:	8080/tcp
CVE-ID:	CVE-2016-1903

Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.31 o 5.6.5 anterior a 5.6.17. Por lo tanto, el servidor puede ser afectado por múltiples vulnerabilidades: • Existencia de un error use-after-free en el archivo file wddx.c. Un atacante remoto puede aprovechar esta debilidad quitando la referencia a la memoria ya liberada para ejecutar código arbitrario. • Existencia de un error en el archivo xmlrpc-epi-php.c. Un atacante remoto puede aprovechar esta vulnerabilidad para divulgar contenidos de la memoria, bloquear el proceso de la solicitud o tener otros impactos.
Vulnerabilidad:	**PHP 5.5.x < 5.5.32 Multiple Vulnerabilities**
Severidad:	10.0 (Crítico)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-8383, CVE-2015-8386, CVE-2015-8387, CVE-2015-8389, CVE-2015-8390, CVE-2015-8391, CVE-2015-8393, CVE-2015-8394.
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.33. Por lo tanto, el servidor está afectado por: • La biblioteca Perl-Compatible Regular Expressions (PCRE) se ve afectada por múltiples vulnerabilidad relacionada con el manejo de expresiones regulares, llamadas de subrutinas y archivos binarios. Un atacante remoto puede explotar esta debilidad para causar una denegación de servicio. • Existe un error en el archivo ext/standard/streamsfuncs.c en la función stream_get_meta_data(). Un atacante remoto puede aprovechar esto la inserción de metadatos maliciosos.

Vulnerabilidad:	**PHP 5.5.x < 5.5.33 Multiple Vulnerabilities**
Severidad:	10.0 (Crítico)
Puerto:	8080/tcp
CVE-ID:	CVE-2016-3141, CVE-2016-3142
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.33. El servidor puede ser afectado vulnerabilidades como: • Existencia de un error use-after-free al manipular datos XML. Un atacante remoto puede explotar esto, a través de diseño de datos XML, para eliminar la referencia de la memoria ya liberada, lo que resulta en la ejecución de código arbitrario. • Existencia de un error out-of-bounds, lo que permite no autenticarse, un atacante remoto podría causar denegación de servicio o ganar acceso a información sensible.
Vulnerabilidad:	**PHP 5.5.x < 5.5.34 Multiple Vulnerabilities**
Severidad:	10.0 (Crítico)
Puerto:	8080/tcp
CVE-ID:	No especificado
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.33. El servidor puede ser afectado vulnerabilidades como: • Existencia de una condición del buffer over-write debido a la validación incorrecta de archivos. Un atacante remoto puede explotar esto, a través de un archivo manipulado, para causar la denegación de servicio o la ejecución de código arbitrario. • Existencia de una falla en la función php_snmp_error(). Un atacante remoto puede explotar esto, mediante un objeto SNMP diseñado, para causar denegación de servicio o ejecutar código arbitrario.

Vulnerabilidad:	**PHP 5.5.x < 5.5.18 Multiple Vulnerabilities**
Severidad:	9.3 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2014-3669, CVE-2014-3670
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.18. El servidor puede ser afectado vulnerabilidades como: • Existencia de un error de desbordamiento de buffer que puede permitir que una aplicación se bloquee o se ejecute código arbitrario. • Existencia de un error de desbordamiento de un entero en la función 'unserialize' que puede permitir ataques de denegación de servicio.
Vulnerabilidad:	**PHP 5.5.x < 5.5.26 Multiple Vulnerabilities**
Severidad:	9.3 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-2325, CVE-2015-2326, CVE-2015-3414, CVE-2015-3415, CVE-2015-3416, CVE-2015-4598, CVE-2015-4642, CVE-2015-4643, CVE-2015-4644.
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.33. El servidor puede ser afectado vulnerabilidades como: • Existencia de múltiples condiciones de desbordamiento de la pila de buffer en la librería PCRE (Perl-Compatible Regular Expression) debido a una validación inadecuada de la entrada user-supplied. Un atacante remoto puede explotar estas condiciones causando un desbordamiento de buffer basado en pila, dando como resultado una denegación de servicio o ejecución de código arbitrario.

	• Existencia de una vulnerabilidad de denegación de servicio en el componente SQLite. Un atacante remoto puede explotar esta condición causando una condición de denegación de servicio.
Vulnerabilidad:	**PHP 5.5.x < 5.5.28 Multiple Vulnerabilities**
Severidad:	9.3 (Alto)
Puerto:	8080/tcp
CVE-ID:	No especificado
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.28. El servidor puede ser afectado vulnerabilidades como: • Existencia de un error use-after-free. Un atacante puede aprovechar esta debilidad, para referenciar memoria liberada y así ejecutar código arbitrario. • Existencia de un error en el archivo zend_exceptions.c debido al uso inapropiado de la función unserialize(). Un atacante remoto puede explotar esta debilidad haciendo colapsar una aplicación que usa PHP. • Existencia de un problema en el archivo zend_exceptions.c. Un atacante remoto puede explotar esta debilidad para provocar un puntero diferenciado NULL o la ejecución de un método inesperado causando el colapso de una aplicación PHP.
Vulnerabilidad:	**PHP 5.5.x < 5.5.30 Multiple Vulnerabilities**
Severidad:	8.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	No especificado
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.30. El servidor puede ser afectado vulnerabilidades como:

	• Existencia de un error de puntero NULL. Un atacante remoto puede aprovechar esta debilidad para provocar una condición de denegación de servicio. • Existencia de una falla de puntero no inicializado. Un atacante remoto puede explotar esta debilidad para causar una condición de denegación de servicio o para revelar información sensible.
Vulnerabilidad:	**PHP 5.5.x < 5.5.19 'donote' DoS**
Severidad:	7.8 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2014-3710
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.20. El servidor puede ser afectado por un error de lectura de out-of-bounds lo que podría permitir que la aplicación se bloquee.
Vulnerabilidad:	**PHP 5.5.x < 5.5.25 Multiple Vulnerabilities**
Severidad:	7.8 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2006-7243, CVE-2015-4024, CVE-2015-4025, CVE-2015-4026
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.25. El servidor puede ser afectado vulnerabilidades como: • Existencia de múltiples fallas relacionadas con las rutas de acceso que contienen el uso de bytes nulos. Un atacante remoto puede aprovechar esta debilidad mediante la combinación de caracteres '\0' con una extensión de archivo seguro, para evitar las restricciones de acceso. • Existencia de una falla en la función multipart_buffer_headers()debido a un manejo inadecuado en las peticiones HTTP. Un atacante puede aprovechar esta debilidad para provocar un

	consumo de recursos de la CPU, lo que resulta en una denegación de servicio.
Vulnerabilidad:	**PHP 5.5.x < 5.5.22 Multiple Vulnerabilities (GHOST)**
Severidad:	7.6 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-0235, CVE-2015-0273, CVE-2015-8866
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.22. El servidor puede ser afectado vulnerabilidades como: • Errores de desbordamiento de la pila de buffer, esto puede permitir a un atacante remoto causar un desbordamiento de buffer, resultando en una condición de denegación de servicio o ejecución de código arbitrario. • Existencia de un defecto use-after-free. Un atacante remoto puede aprovechar esto accediendo a información sensible o colapsando aplicaciones relacionadas con PHP.
Vulnerabilidad:	**Apache 2.4.x < 2.4.10 Multiple Vulnerabilities**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2014-0117, CVE-2014-0118, CVE-2014-0226, CVE-2014-0231, CVE-2014-3523
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 2.4.x anterior a 2.4.10. El servidor puede ser afectado vulnerabilidades como: • Existencia de un error en el módulo 'mod_proxy' que puede permitir a un atacante enviar peticiones especialmente diseñadas al servidor configurado como un proxy inverso lo que puede causar que el proceso hijo se bloquee. Esto podría producir un ataque de denegación de servicio.

	• Existencia de un error en el módulo 'mod_status'. Esto podría permitir a un atacante enviar una solicitud especialmente diseñada para causar el desbordamiento de pila de buffer.
Vulnerabilidad:	**PHP 5.5.x < 5.5.16 Multiple Vulnerabilities**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2014-2497, CVE-2014-3538, CVE-2014-3587, CVE-2014-3597, CVE-2014-5120
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.22. El servidor puede ser afectado por vulnerabilidades como: • Existencia de un error de desbordamiento de un entero, un atacante remoto puede causar una denegación de servicio. • Existencia de múltiples fallas de desbordamiento de buffer en el archivo 'dns.c'. Mediante el uso de un registro DNS especialmente diseñado, un atacante remoto puede explotar esta debilidad para causar una denegación de servicio o ejecución de código arbitrario.
Vulnerabilidad:	**PHP 5.5.x < 5.5.20 'process_nested_data' RCE**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2014-8142
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.20. El servidor puede ser afectado por un error use-after-free debido a un manejo inadecuado de claves duplicadas dentro de las propiedades de un objeto serializado. Un atacante remoto usando un diseño especial de llamada al método 'unserialize' puede explotar esta debilidad para ejecutar código arbitrario en el sistema.

Vulnerabilidad:	**PHP 5.5.x < 5.5.21 Multiple Vulnerabilities**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2014-9427, CVE-2014-9709, CVE-2015-0231, CVE-2015-0232
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.21. El servidor puede ser afectado por vulnerabilidades como: • Existencia de una debilidad de lectura en la función GetCode_() en 'gd_gif_in.c'. Esto permite a un atacante remoto divulgar contenidos de memoria. • Existencia de un error en el manejo inadecuado de claves numéricas duplicadas dentro de las propiedades de un objeto serializado. Un atacante remoto usando un diseño especial puede explotar esta debilidad ejecutando código arbitrario.
Vulnerabilidad:	**PHP 5.5.x < 5.5.23 Multiple Vulnerabilities**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-0231, CVE-2015-2305, CVE-2015-2331, CVE-2015-2348, CVE-2015-2787
Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.23. El servidor puede ser afectado por un error relacionado con la función 'unserialize', lo que puede permitir a un atacante remoto ejecutar código arbitrario.
Vulnerabilidad:	**PHP 5.5.x < 5.5.24 Multiple Vulnerabilities**
Severidad:	7.5 (Alto)
Puerto:	8080/tcp
CVE-ID:	CVE-2015-1351, CVE-2015-1352, CVE-2015-2783, CVE-2015-3329, CVE-2015-3330, CVE-2015-4601, CVE-2015-4602, CVE-2015-4603, CVE-2015-4604, CVE-2015-4605

Descripción:	La versión de PHP ejecutándose en el servidor web remoto es 5.5.x anterior a 5.5.24. El servidor está puede ser afectado por vulnerabilidades como: • Existencia de un error use-after-free en la extensión en la función _zend_shared_memdup(). Un atacante remoto puede explotar este causando una denegación de servicio o tener otro impacto no especificado. • Existencia de un error de desbordamiento de buffer en la función phar_set_inode() en el archivo phar_internal.h' al manipular los ficheros de archivo, tales como tar, zip o phar. Un atacante remoto puede aprovechar esto para ejecutar código arbitrario o causar una denegación de servicio.

Tabla 3.7 Análisis de vulnerabilidades con Nessus.

3.2.3. Análisis de Resultados

El análisis de vulnerabilidades críticas y altas detectadas por las herramientas OpenVAS y Nessus, se realiza con el fin de determinar la precisión de cada una y en base a sus reportes seleccionar la que proporciona mayores resultados.

En las tablas 3.8 a las 3.11, se enumera las vulnerabilidades que tienen un impacto alto encontradas en cada IP y con cada herramienta.

IP	HERRAMIENTA	IMPACTO	PUERTO	VULNERABILIDAD
186.47.XX.C	OpenVAS	10.0 (Alto)	80/tcp	GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerability

IP	HERRAMIENTA	IMPACTO	PUERTO	VULNERABILIDAD
186.47.XX.C	Nessus	10.0 (Crítico)	80/tcp	GNU Bash Environment Variable Handling Code Injection (Shellshock)

Tabla 3.8 Procesamiento de información de la IP 186.47.XX.C

IP	HERRAMIENTA	IMPACTO	PUERTO	VULNERABILIDAD
186.47.XX.D	Nessus	10.0 (Crítico)	3389/tcp	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
		9.3 (Alto)	3389/tcp	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
		9.3 (Alto)	80/tcp	Apache Tomcat 6.0.x < 6.0.43 Multiple Vulnerabilities (POODLE)

Tabla 3.9 Procesamiento de información de la IP 186.47.XX.D

IP	HERRAMIENTA	IMPACTO	PUERTO	VULNERABILIDAD
186.47.XX.E	OpenVAS	9.3 (Alto)	443/tcp	LiteServe URL Decoding DoS
		7.5 (Alto)	443/tcp	Header overflow against HTTP proxy
	Nessus	10.0 (Crítico)	443/tcp	OpenSSL Unsupported
		9.3 (Alto)	443/tcp	OpenSSL < 0.9.8s Multiple Vulnerabilities
		9.3 (Alto)	443/tcp	OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities
		7.6 (Alto)	443/tcp	OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow
		7.5 (Alto)	443/tcp	Unsupported Web Server Detection
		7.5 (Alto)	443/tcp	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption
		7.1 (Alto)	443/tcp	OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities

Tabla 3.10 Procesamiento de información de la IP 186.47.XX.E

IP	HERRAMIENTA	IMPACTO	PUERTO	VULNERABILIDAD
186.47.XX.F	OpenVAS	10.0 (Alto)	8080/tcp	php Multiple Vulnerabilities -01 April16 (Windows)
		7.5 (Alto)	8080/tcp	php Multiple Vulnerabilities -01 June15 (Windows)
		7.5 (Alto)	8080/tcp	php Multiple Vulnerabilities -02 June15 (Windows)
		7.5 (Alto)	8080/tcp	php Multiple Vulnerabilities -03 June15 (Windows)
		7.5 (Alto)	8080/tcp	php Multiple Remote Code Execution Vulnerabilities July15
		7.5 (Alto)	8080/tcp	php Use-After-Free Remote Code EXecution Vulnerability -01 July15 (Windows)
		7.5 (Alto)	8080/tcp	php Use-After-Free Denial Of Service Vulnerability -02 July15 (Windows)
		7.5 (Alto)	8080/tcp	php Multiple Vulnerabilities -01 March16 (Windows)
		7.5 (Alto)	8080/tcp	php 'serialize function call' Function Type Confusion Vulnerability March16 (Windows)

IP	HERRAMIENTA	IMPACTO	PUERTO	VULNERABILIDAD
186.47.XX.F	OpenVAS	7.5 (Alto)	8080/tcp	php 'phar x lepath' Function Stack Buffer Overflow Vulnerability March16 (Windows)
186.47.XX.F	Nessus	10.0 (Crítico)	8080/tcp	PHP 5.5.x < 5.5.14 Multiple Vulnerabilities
		10.0 (Crítico)	8080/tcp	PHP 5.5.x < 5.5.29 Multiple Vulnerabilities
		10.0 (Crítico)	8080/tcp	PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilities
		10.0 (Crítico)	8080/tcp	PHP 5.5.x < 5.5.32 Multiple Vulnerabilities
		10.0 (Crítico)	8080/tcp	PHP 5.5.x < 5.5.33 Multiple Vulnerabilities
		10.0 (Crítico)	8080/tcp	PHP 5.5.x < 5.5.34 Multiple Vulnerabilities
		9.3 (Alto)	8080/tcp	PHP 5.5.x < 5.5.18 Multiple Vulnerabilities
		9.3 (Alto)	8080/tcp	PHP 5.5.x < 5.5.26 Multiple Vulnerabilities
		9.3 (Alto)	8080/tcp	PHP 5.5.x < 5.5.28 Multiple Vulnerabilities

IP	HERRAMIENTA	IMPACTO	PUERTO	VULNERABILIDAD
186.47.XX.F	Nessus	8.5 (Alto)	8080/tcp	PHP 5.5.x < 5.5.30 Multiple Vulnerabilities
		7.8 (Alto)	8080/tcp	PHP 5.5.x < 5.5.19 'donote' DoS
		7.8 (Alto)	8080/tcp	PHP 5.5.x < 5.5.25 Multiple Vulnerabilities
		7.6 (Alto)	8080/tcp	PHP 5.5.x < 5.5.22 Multiple Vulnerabilities (GHOST)
		7.5 (Alto)	8080/tcp	Apache 2.4.x < 2.4.10 Multiple Vulnerabilities
		7.5 (Alto)	8080/tcp	PHP 5.5.x < 5.5.16 Multiple Vulnerabilities
		7.5 (Alto)	8080/tcp	PHP 5.5.x < 5.5.20 'process_nested_data ' RCE
		7.5 (Alto)	8080/tcp	PHP 5.5.x < 5.5.21 Multiple Vulnerabilities
		7.5 (Alto)	8080/tcp	PHP 5.5.x < 5.5.23 Multiple Vulnerabilities
		7.5 (Alto)	8080/tcp	PHP 5.5.x < 5.5.24 Multiple Vulnerabilities

Tabla 3.11 Procesamiento de información de la IP 186.47.XX.F

De las tablas 3.8, 3.9, 3.10, 3.11, se puede concluir que la herramienta que mayor información proporciona es Nessus, por lo cual esas vulnerabilidades son las que se tomarán en cuenta para la fase de explotación.

3.3.PLAN DE EXPLOTACIÓN

Antes de empezar con las pruebas, es necesario validar la actividad de cada sistema, debido a que en fases anteriores se detectó servicios que no son permanentes.

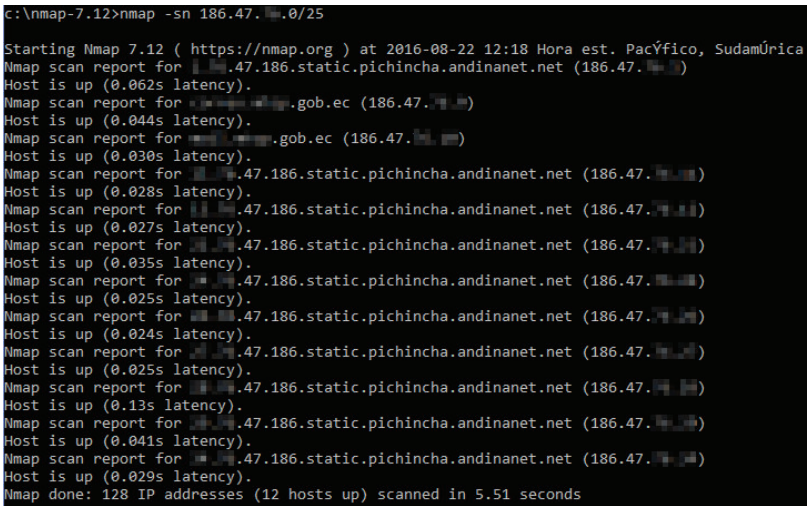


Figura 3.7 Verificación de IP's activas.

HOST	ANTERIORES	ACTIVAS A LA FECHA
186.47.XX.A	✓	✓
186.47.XX.B	✓	✓
186.47.XX.C	✓	✓
186.47.XX.D	✓	✓
186.47.XX.E	✓	✗
186.47.XX.F	✓	✓
186.47.XX.G	✓	✓
186.47.XX.H	✓	✓
186.47.XX.I	✓	✓
186.47.XX.J	✓	✓
186.47.XX.K	✓	✓
186.47.XX.L	✓	✓

Tabla 3.12 Comparación de IP´s anteriores con las activas actualmente.

Una vez identificados los host activos, se realiza un resumen de las vulnerabilidades detectadas por la herramienta Nessus, con el fin de identificar con el personal de la organización aquellas debilidades que se explotarán.

Se indica con color amarillo las vulnerabilidades a explotar.

VULNERABILIDADES	186.47.XX.A	186.47.XX.B	186.47.XX.C	186.47.XX.D	186.47.XX.E	186.47.XX.F	186.47.XX.I	186.47.XX.J	186.47.XX.K
SSL Certificate Cannot Be Trusted	x	x		x	x			x	
SSL Self-Signed Certificate	x	x		x	x				
SSL Version 2 and 3 Protocol Detection	x			x	x			x	
SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	x								
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	x			x	x			x	
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	x			x	x				
IMAP Service STARTTLS Plaintext Command Injection	x								
POP3 Service STLS Plaintext Command Injection	x								
SMTP Service STARTTLS Plaintext Command Injection	x								
POP3 Cleartext Logins Permitted	x								
Web Server Transmits Cleartext Credentials	x					x		x	
Web Server Uses Basic Authentication Without HTTPS	x								
Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key		x							
SSH Protocol Version 1 Session Key Retrieval		x							
SSL Certificate Signed Using Weak Hashing Algorithm		x		x					
SSH Server CBC Mode Ciphers Enabled		x					x		
SSH Weak MAC Algorithms Enabled		x					x		
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits		x		x				x	
GNU Bash Environment Variable Handling Code Injection (Shellshock)			x						
HTTP TRACE / TRACK Methods Allowed			x		x	x			
Apache Server ETag Header Information Disclosure			x						
Vulnerability in Schannel Could Allow Remote Code Execution				x					
Vulnerabilities in Remote Desktop Could Allow Remote Code				x					
Apache Tomcat 6.0.x < 6.0.43 Multiple Vulnerabilities (POODLE)				x					
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection				x				x	

VULNERABILIDADES	186.47.XX.A	186.47.XX.B	186.47.XX.C	186.47.XX.D	186.47.XX.E	186.47.XX.F	186.47.XX.I	186.47.XX.J	186.47.XX.K
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness				x					
SSL Medium Strength Cipher Suites Supported				x					
Terminal Services Encryption Level is Medium or Low				x					
Terminal Services Doesn't Use Network Level Authentication (NLA) Only				x					
SSL Null Cipher Suites Supported				x					
Terminal Services Encryption Level is not FIPS-140 Compliant				x					
OpenSSL Unsupported					x				
OpenSSL < 0.9.8s Multiple Vulnerabilities					x				
OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities					x				
OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow					x				
Unsupported Web Server Detection					x				
OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption					x				
OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities					x				
OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities					x				
OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities					x				
OpenSSL < 0.9.8j Signature Spoofing					x				
OpenSSL < 0.9.8l Multiple Vulnerabilities					x				
SSL Certificate Expiry					x				
OpenSSL < 0.9.8i Denial of Service					x				
OpenSSL < 0.9.8k Denial of Service					x				
Browsable Web Directories					x	x			
OpenSSL < 0.9.8u Multiple Vulnerabilities					x				
OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service					x				
OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities (FREAK)					x				
OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS					x				
OpenSSL < 0.9.8p / 1.0.0e Double Free Vulnerability					x				
CGI Generic XSS (quick test)					x				
CGI Generic Cookie Injection Scripting					x				
CGI Generic XSS (comprehensive test)					x				
CGI Generic HTML Injections (quick test)					x				
OpenSSL < 0.9.8h Multiple Vulnerabilities					x				
Apache HTTP Server httpOnly Cookie Information Disclosure					x				
Transport Layer Security (TLS) Protocol CRIME Vulnerability					x				
OpenSSL < 0.9.8y Multiple Vulnerabilities					x				

VULNERABILIDADES	186.47.XX.A	186.47.XX.B	186.47.XX.C	186.47.XX.D	186.47.XX.E	186.47.XX.F	186.47.XX.I	186.47.XX.J	186.47.XX.K
OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE)					x				
Web Application Potentially Vulnerable to Clickjacking					x	x		x	x
PHP 5.5.x < 5.5.14 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.29 Multiple Vulnerabilities						x			
PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.32 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.33 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.34 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.18 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.26 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.28 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.30 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.19 'donote' DoS						x			
PHP 5.5.x < 5.5.25 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.22 Multiple Vulnerabilities (GHOST)						x			
Apache 2.4.x < 2.4.10 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.16 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.20 'process_nested_data' RCE						x			
PHP 5.5.x < 5.5.21 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.23 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.24 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.27 Multiple Vulnerabilities (BACKRONYM)						x			
PHP 5.5.x < 5.5.13 'src/cdf.c' Multiple Vulnerabilities						x			
Apache 2.4.x < 2.4.12 Multiple Vulnerabilities						x			
Apache 2.4.x < 2.4.16 Multiple Vulnerabilities						x			
PHP 5.5.x < 5.5.15 Multiple Vulnerabilities						x			
SSH Weak Algorithms Supported							x		
Unencrypted Telnet Server								x	
SSL Weak Cipher Suites Supported								x	
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)								x	

Tabla 3.13 Resumen de vulnerabilidades.

La identificación de las vulnerabilidades a explotar se realiza en base a requerimientos específicos de la organización garantizando que no se

realizarán ataques críticos que puedan comprometer la disponibilidad de los servicios.

El plan de explotación (Anexo 5), presenta la siguiente lista de ataques aprobados:

- Escaneo de directorios web.
- Explotación de usuarios y contraseñas por defecto.
- Transmisión Vulnerable de Credenciales en una Aplicación Web.
- Ataques de autenticación por fuerza bruta.
- Autenticación web básica.
- Servicio web sin método de autenticación.
- Clickjacking.
- Procedimiento de uso de un exploit para explotar una vulnerabilidad.

CAPÍTULO IV

4. IMPLEMENTACIÓN DEL PLAN DE ATAQUES Y ANÁLISIS DE LOS RESULTADOS

En este capítulo se realiza la implementación del plan de ataques en el cual se acordó previamente con la organización, evaluada, la no disrupción o alteración de los servicios, el objetivo de esta fase es explotar las vulnerabilidades y adquirir accesos a los servicios de ser posible.

4.1.IDENTIFICACIÓN DE VULNERABILIDADES

En base a la lista de explotaciones aprobadas, se realizará lo siguientes ataques:

- Escaneo de directorios web.
  Vulnerabilidad identificada con el nombre: ***Browsable Web Directories***
- Explotación de usuarios y contraseñas por defecto.
- Transmisión Vulnerable de Credenciales en una Aplicación Web.
  Vulnerabilidad identificada con el nombre: ***Web Server Transmits Cleartext Credentials.***
- Ataques de autenticación por fuerza bruta.
- Autenticación web básica.
  Vulnerabilidad identificada con el nombre: ***Web Server Uses Basic Authentication Without HTTPS.***
- Servicio web sin método de autenticación.
  Vulnerabilidad identificada con el nombre: ***Terminal Services Doesn't Use Network Level Authentication (NLA) Only.***
- Clickjacking
  Vulnerabilidad identificada con el nombre: ***Web Application Potentially Vulnerable to Clickjacking.***
- Procedimiento de uso de un exploit para explotar una vulnerabilidad

4.2. IMPLEMENTACIÓN DEL PLAN DE ATAQUES

4.2.1. Escaneo de Directorios Web

Este tipo de vulnerabilidad permite listar el contenido de directorios de una página web.

Para el presente proyecto, se ha explotado dicha vulnerabilidad mediante el uso de combinaciones simples y comunes, tales como: ../login, …/adminlogin, …/Admin.

Este tipo de pruebas sirven para detectar páginas de autenticación a nivel de administrador o archivos publicados en internet que podrían proporcionar información sensible.

En la figura 4.1 se puede observar que existen varios directorios publicados, realizando una exploración de cada uno de ellos se identificó la página de autenticación del mismo (figura 4.2).

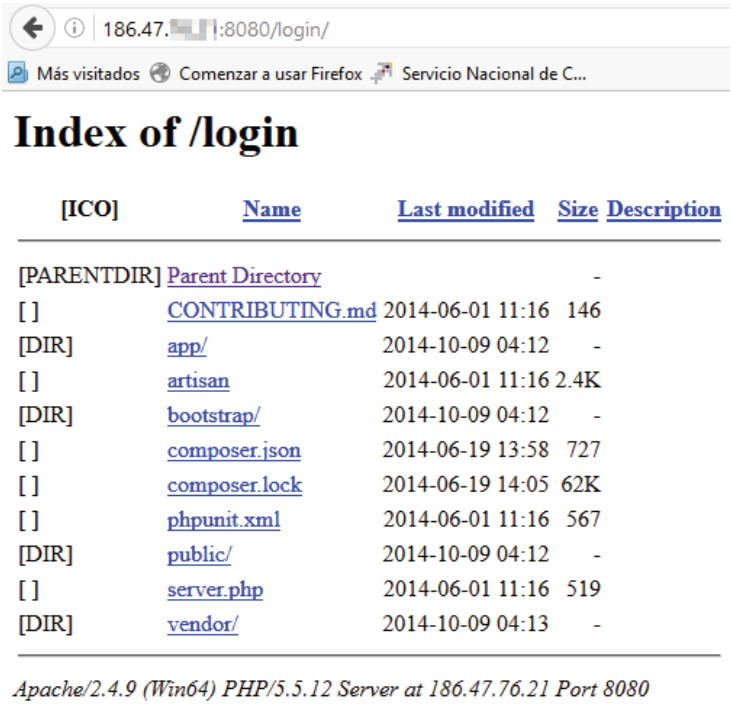


Figura 4.1 Ejemplo de búsqueda de directorios.

Figura 4.2 Página de autenticación a la ip 186.47.XX.F

En la figura 4.3 se puede observar la página de autenticación a nivel de administrador del correo institucional.

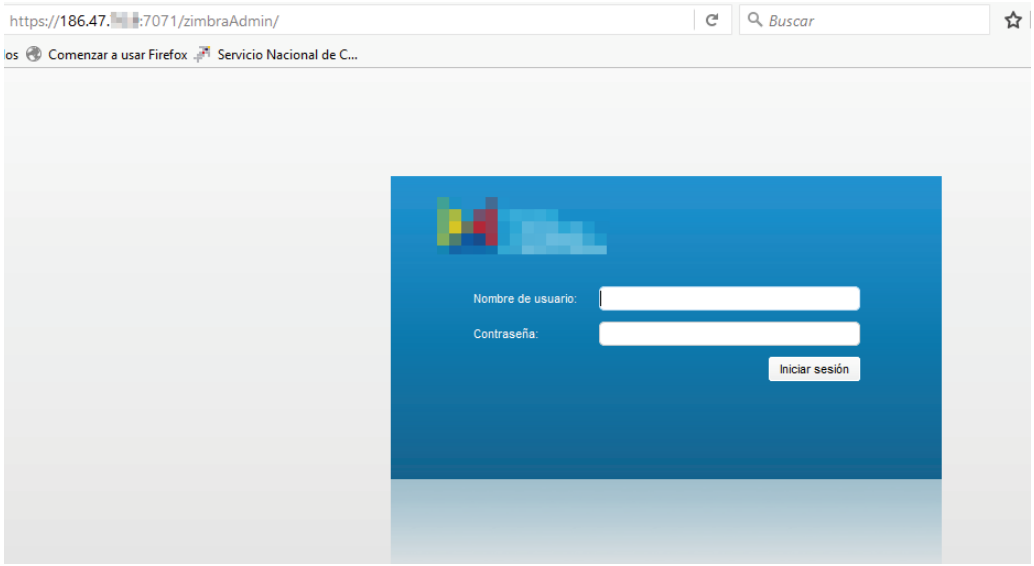


Figura 4.3 Página de autenticación de administrador a la ip 186.47.XX.A

4.2.2. Explotación de Usuario y Contraseña por Defecto

Antes de empezar a explotar este tipo de vulnerabilidades, es necesario identificar las IP's que re-direccionan directamente a alguna página de principal o de autenticación desde un explorador.

En las figuras 4.4 a la 4.10, se puede observar que la pantalla principal es una página de autenticación para ingreso al servicio.

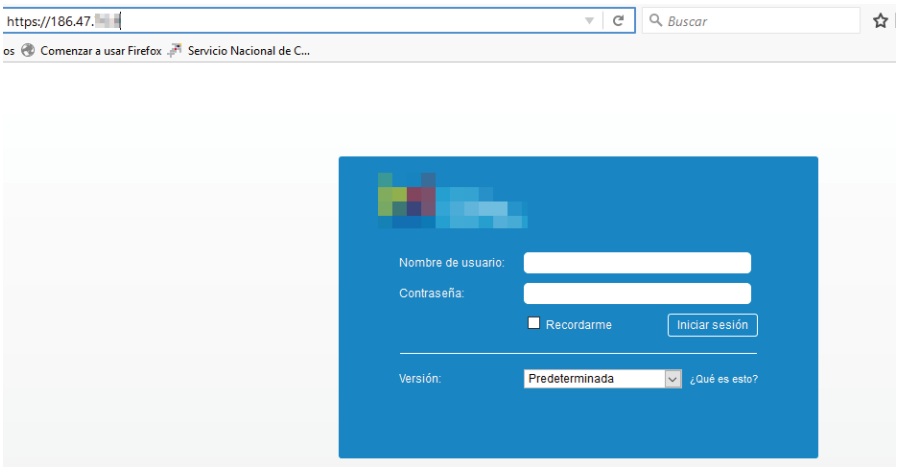


Figura 4.4 Página de autenticación de usuario final a la ip 186.47.XX.A

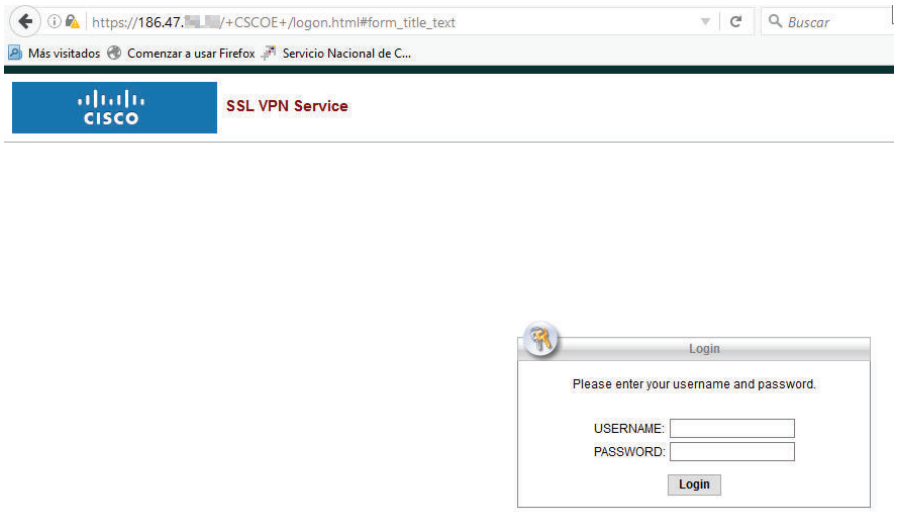


Figura 4.5 Página de autenticación a la ip 186.47.XX.B

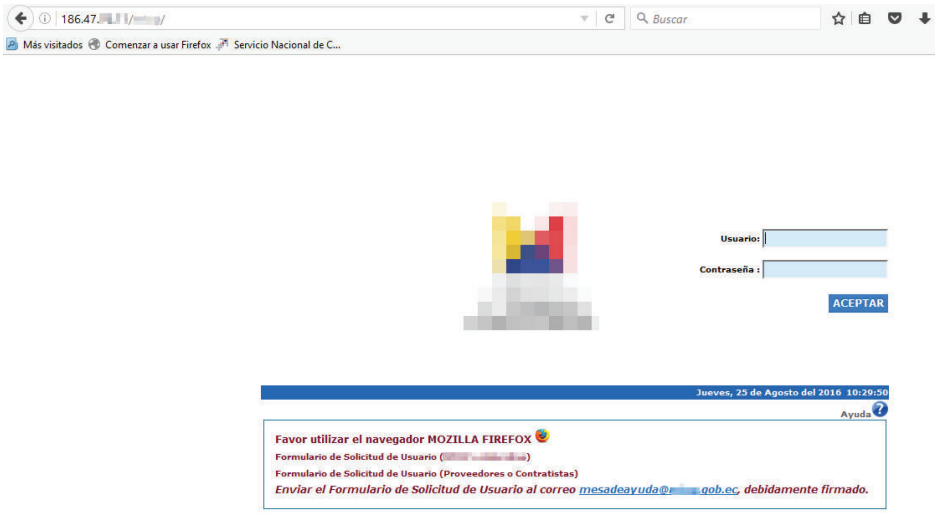


Figura 4.6 Página de autenticación a la ip 186.47.XX.C

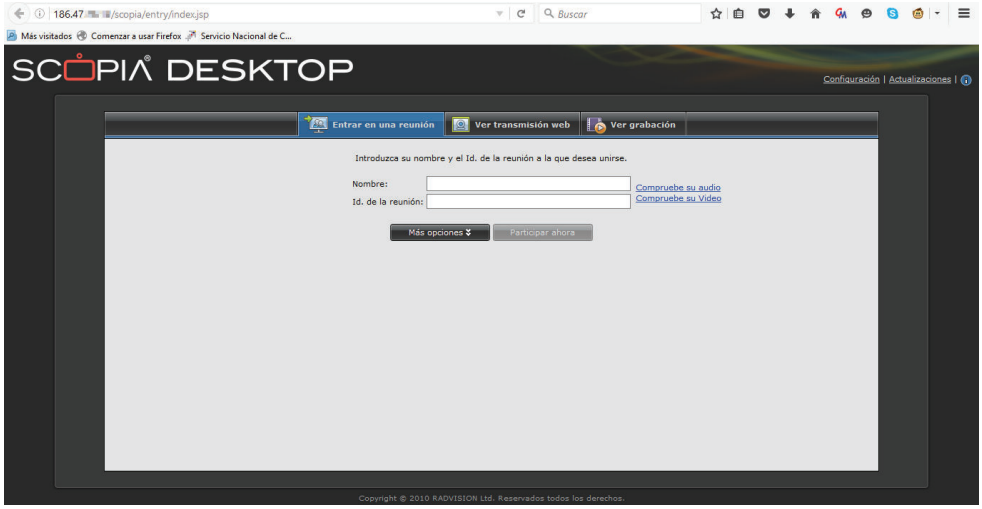


Figura 4.7 Página de autenticación a la ip 186.47.XX.D

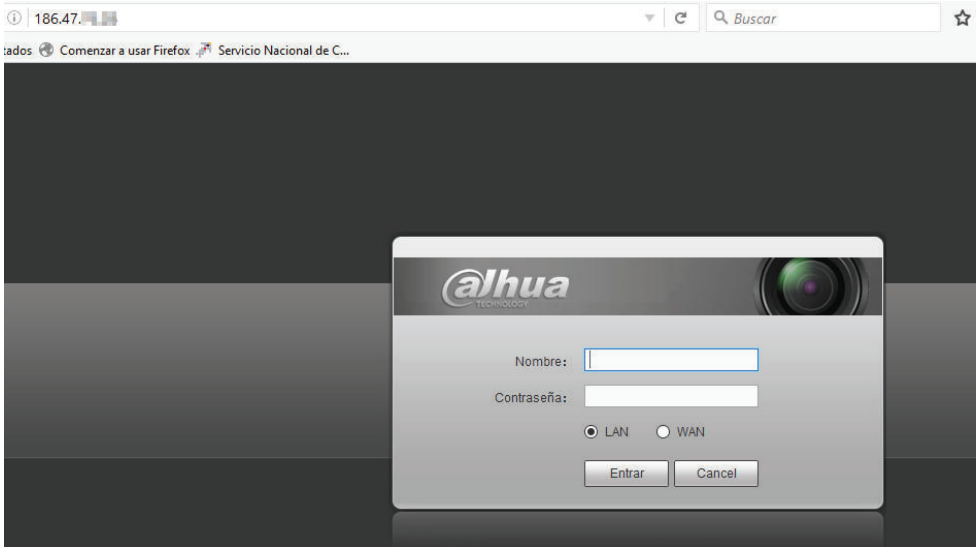


Figura 4.8 Página de autenticación a la ip 186.47.XX.J

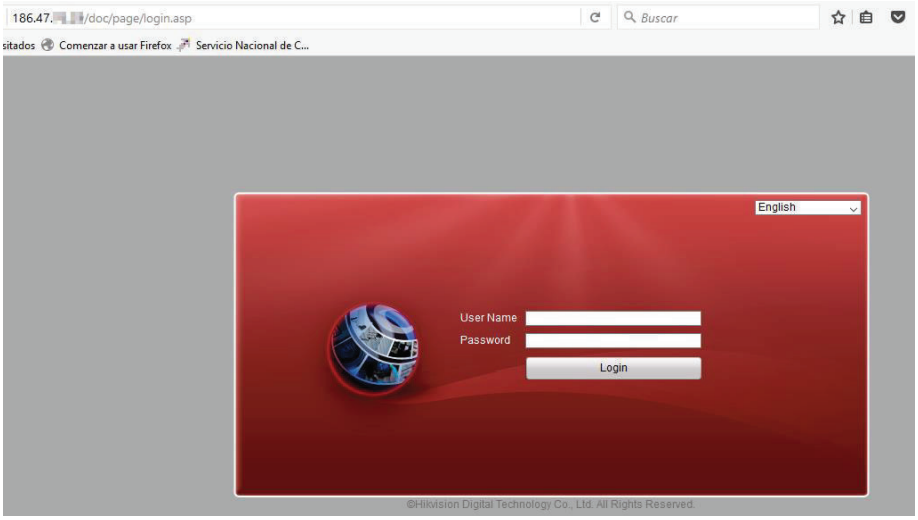


Figura 4.9 Página de autenticación a la ip 186.47.XX.K

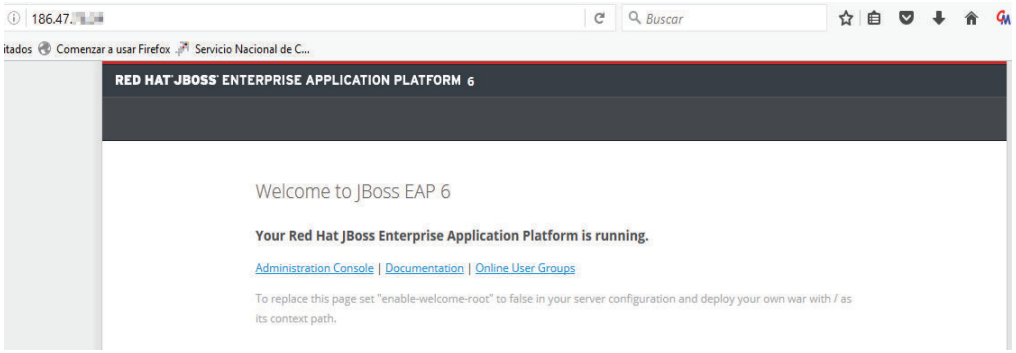


Figura 4.10 Página de autenticación a la ip 186.47.XX.L

Para la explotación de la vulnerabilidad de usuario y contraseña por defecto, se tiene un método muy simple que consiste en elaborar una lista de usuarios y contraseñas comunes que normalmente se usa durante la implementación, los cuales se probarán en las páginas de autenticación identificadas.

La vulnerabilidad se presenta por fallas en la configuración debido a que los administradores o implementadores de soluciones no eliminan o deshabilitan los usuarios y contraseñas por defecto. Ejemplo de este tipo de usuario y contraseña son:

- Usuario: Admin, Administrador, Administrator, root, rootAdmin
- Contraseña: Password, Admin, admin123, root, root123

Resultados:

Host	Página de autenticación	Vulnerable
186.47.XX.A	https://186.47.XX.A/ https://186.47.XX.A:7071/zimbraAdmin/	no
186.47.XX.B	https://186.47.XX.B/+CSCOE+/logon.html#form_title_text	no
186.47.XX.C	http://186.47.XX.C/mtop/AdmLogin	no
186.47.XX.D	http://186.47.XX.D/scopia/entry/index.jsp	NA
186.47.XX.F	http://186.47.XX.F:8080/login/public/	si
186.47.XX.I	No tiene acceso web, solo ssh	NA
186.47.XX.J	http://186.47.XX.J/	si
186.47.XX.K	http://186.47.XX.K/doc/page/login.asp	no
186.47.XX.L	http://186.47.XX.L/	NA

Tabla 4.1 Resumen de páginas de autenticación.

Mediante la tabla 4.1 se puede identificar que dos hosts tienen acceso a los sistemas por medio de autenticación por defecto (figura 4.11 y 4.12), lo que permite ingresar como administradores y ejecutar cambios en los sistemas, el riesgo que presenta es inminente, y a través de esta brecha, es posible obtener información valiosa de la institución o causar daños significativos.

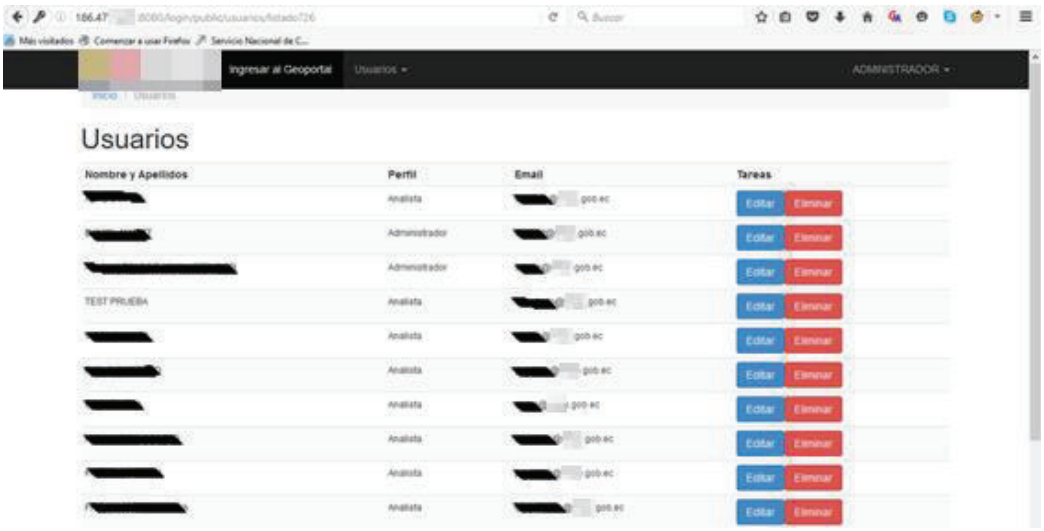


Figura 4.11 Autenticación en la ip 186.47.XX.F

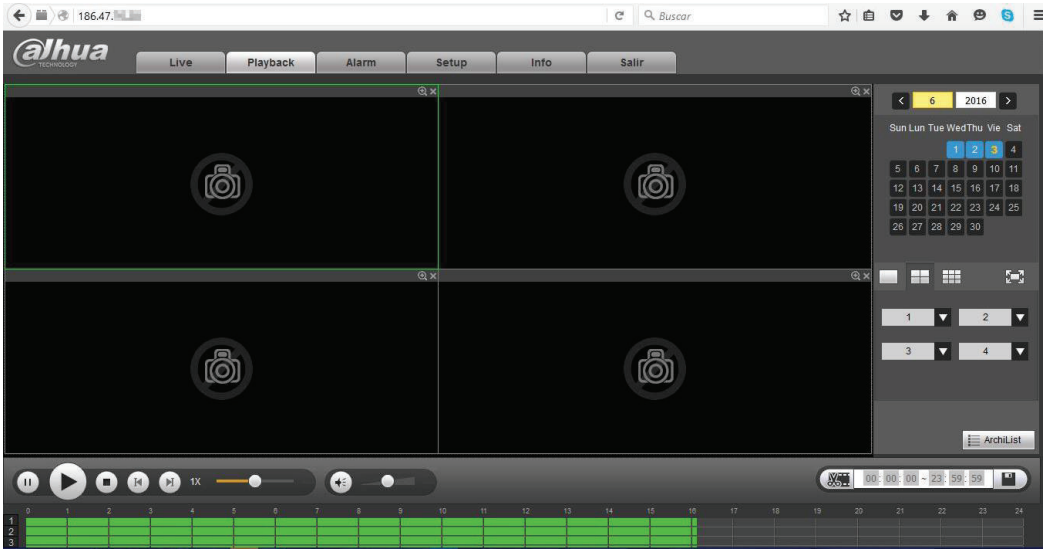


Figura 4.12 Autenticación en la ip 186.47.XX.J

4.2.3. Transmisión Vulnerable de Credenciales en una Aplicación Web

Para este tipo de vulnerabilidad usaremos el ataque man-in-the-middle, el cual consiste en interceptar el tráfico de un host víctima y de esa manera comprobar

cierta información, como usuario, contraseña, streem de caracteres, versiones de SSL, cookies, etc.

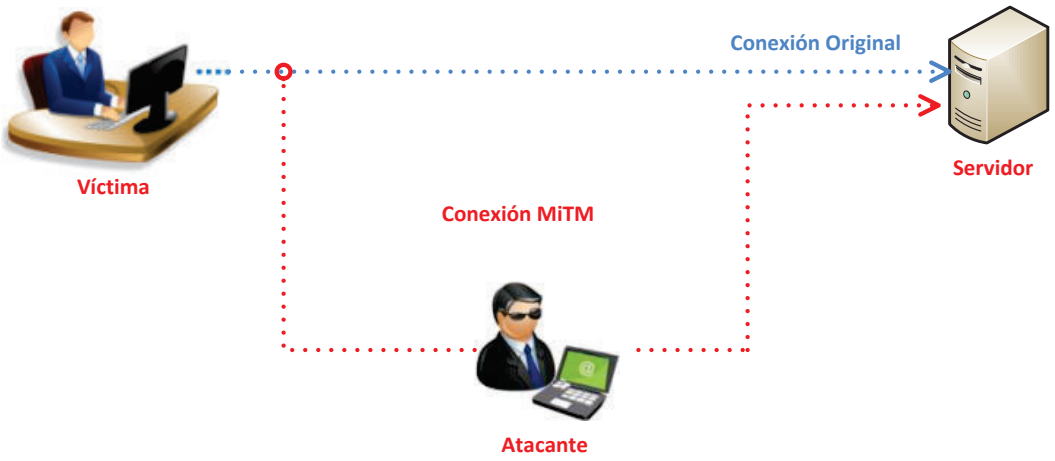


Figura 4.13 Diagrama de ataques tipo Man-in-the-Middle (MiTM).

Para este tipo de ataques se hace uso de dos herramientas:

- Ettercap

  Es una herramienta completa para realizar ataques tipo man-in-the-middle, una de sus principales características es el espionaje de conexiones activas.

  En el presente proyecto se usa Ettercap para envenenamiento ARP, que consiste en establecer a la ip de la máquina atacante como la puerta de enlace de la máquina objetivo, de esta manera el atacante escucha todo el tráfico que genera el objetivo.
- Wireshark

  Es una herramienta multiplataforma de análisis de paquetes de red.

El método de explotación consiste en realizar desde la máquina atacante (ver figura 4.13), las siguientes acciones:

- Escanear los host visibles contra los cuales se podrá realizar el envenenamiento arp, una vez identificado el objetivo, mediante la pestaña *Mitm* de la herramienta activaremos la opción de husmear las conexiones remotas.

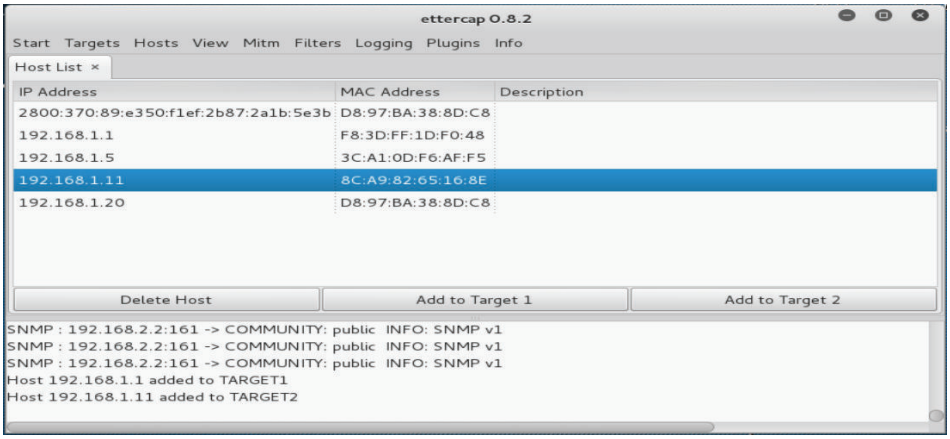


Figura 4.14 Identificación de mac-address y Gateway del objetivo.

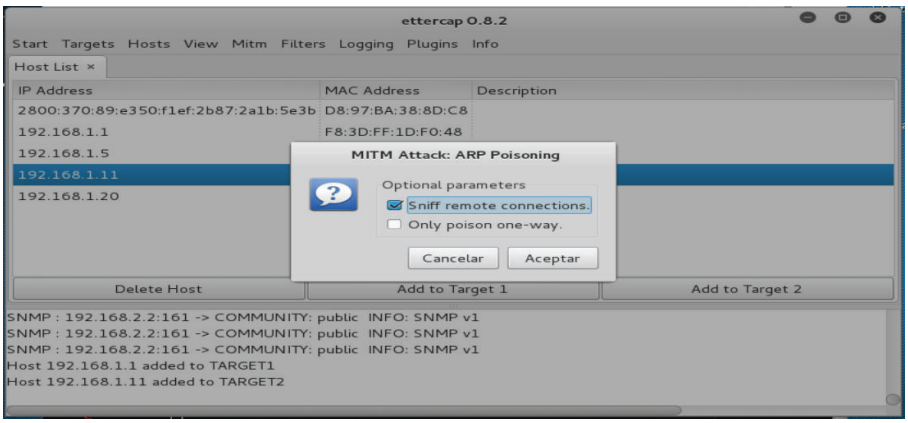


Figura 4.15 Husmeo de las conexiones remotas.

- Ahora se crean las rutas y permisos mediante *iptables*[34] para que el tráfico del objetivo para por la máquina atacante.

```
echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -F
iptables -X
iptables -Z
iptables -t nat -F

iptables -P FORWARD ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A PREROUTING -i eth1 -p tcp --destination-port 80 -j
REDIRECT $

iptables-save > /etc/iptables.up.rules
```

Figura 4.16 Configuración de rutas y permisos.

[34] Es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red.

- Finalmente, con la herramienta wireshark, se analiza el tráfico del objetivo.

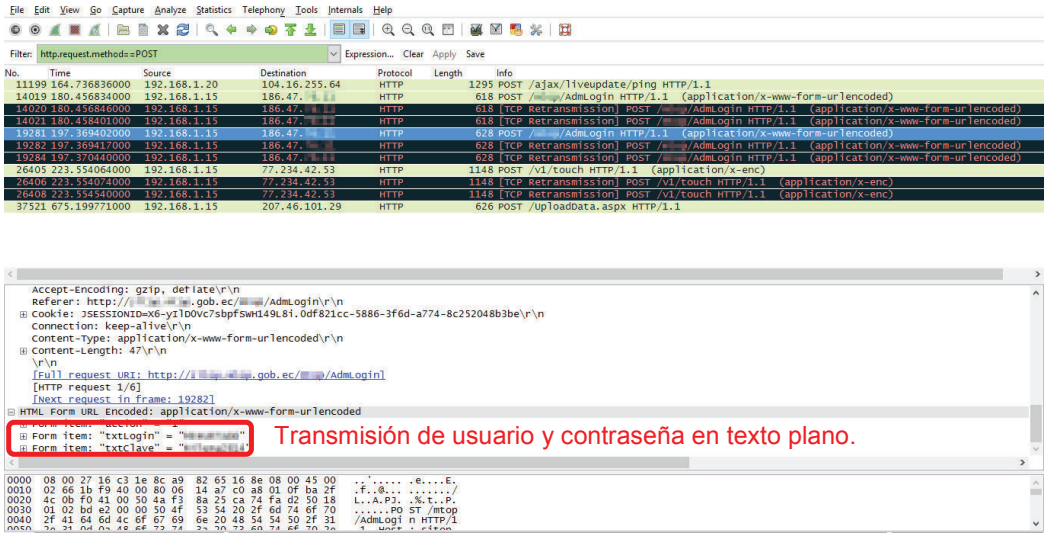


Figura 4.17 Análisis de tráfico del objetivo.

En la figura 4.17 se puede observar que la aplicación usada por el objetivo transmite información en texto plano, lo que se considera como una debilidad crítica, ya que al ser explotada se puede sustraer información sensible.

4.2.4. Ataques de Autenticación por Fuerza Bruta

Para este tipo de ataque se utilizará Hydra, es una herramienta de código abierto que soporta numerosos protocolos de ataque. Esta herramienta realiza búsquedas y consultas de seguridad mediante fuerza bruta con el objetivo de mostrar lo fácil que resultaría ganar acceso no autorizado a un sistema remoto.

Para realizar este tipo de ataque es necesario identificar 4 parámetros de la página de autenticación, los mismos que se obtienen usando el complemento para el navegador denominado *Live HTTP Headers* que permite ver la información de los encabezados de sitios web.

Los parámetros son:

- Formas de envío de datos en un formulario get|post, mediante estos métodos se puede pasar determinados valores de una página a otra.
- Ruta de web de verificación de los parámetros ingresados para la autenticación.

- Etiqueta que hace referencia al usuario y contraseña de la página de autenticación.
- Mensaje de denegación de autenticación.

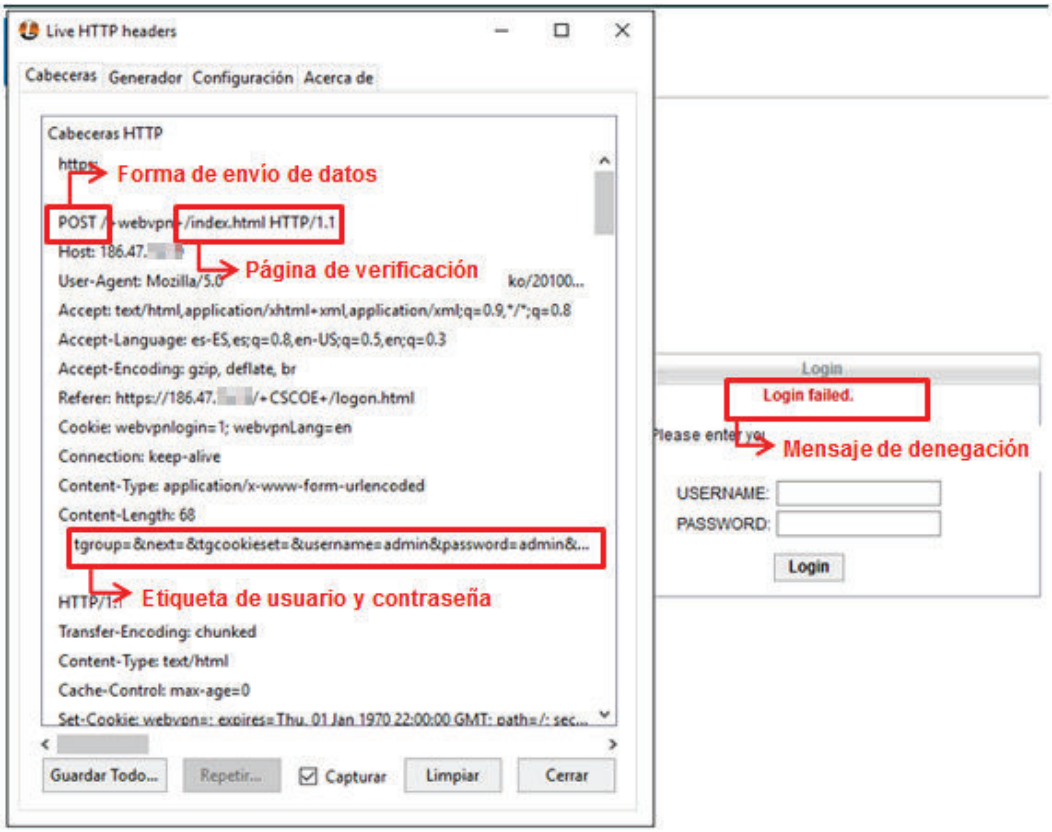


Figura 4.18 Identificación de información mediante Live HTTP headers.

La identificación de información de la figura 4.18, se lo realiza en los cuatro hosts que la tabla 4.1 indica como no vulnerables.

HOST	Forma de envío de datos	Página de verificación	Etiqueta de usuario y contraseña	Mensaje de denegación
1876.47.XX.A	Post	No disponible	username password	El nombre de usuario o la contraseña son incorrectos
186.47.XX.B	Post	Index.html	username password	Login failed
186.47.XX.C	Post	/AdmLogin	Login Clave	Usuario o Clave incorrecta
186.47.XX.K	Get	userCheck	No disponible	User name or password is incorrect. Please enter again.

Tabla 4.2 Resumen de información obtenida por Live HTTP headers.

Según los datos obtenidos en la tabla 4.2, es posible realizar un ataque por fuerza bruta con hydra a las direcciones 186.47.XX.B y 186.47.XX.C.

El comando que se usará en hydra es:

hydra [IP objetivo] http[s]-form[forma de envío de datos] "[ruta de verificación]:[etiqueta de usuario y contraseña]:[mensaje de denegación]" –L [archivo de usuarios] –P [archivo de contraseñas] –t 10 –w 30

Dónde:

- -L indica el usuario o archivo que contiene nombres de usuarios.
- -P indica la contraseña o archivo que contiene contraseñas.
- -t cambia contraseñas en paralelo.
- -w tiempo en segundos de intervalos de pureba.

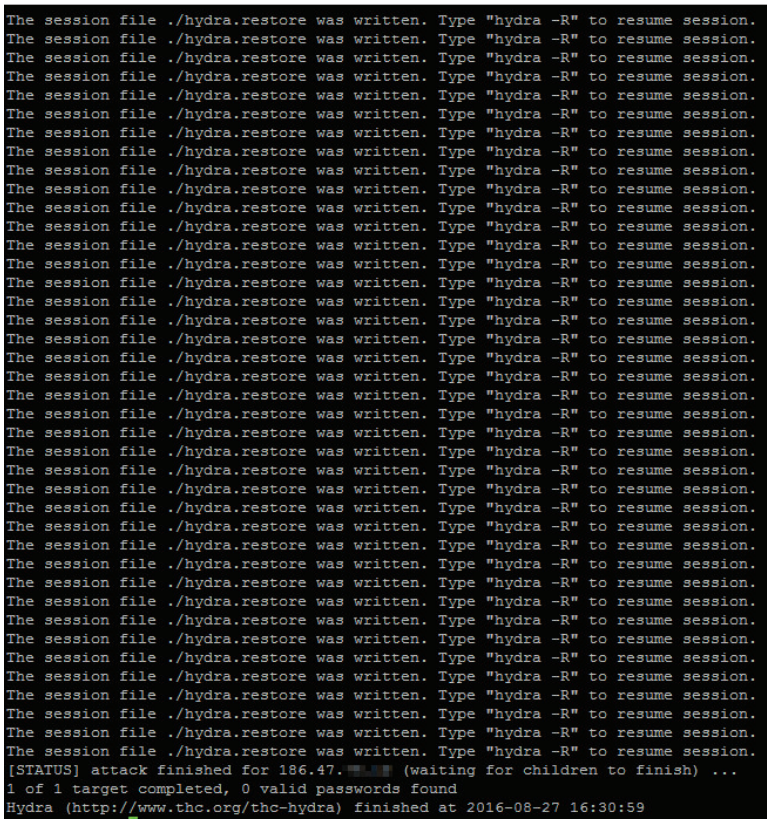


Figura 4.19 Uso de hydra con el host 186.47.XX.B

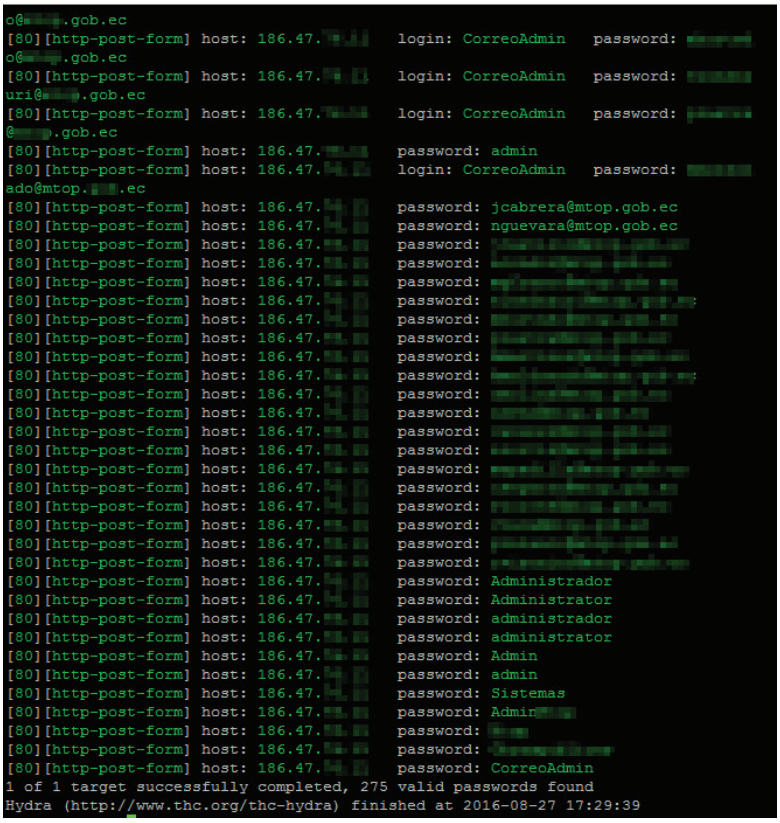


Figura 4.20 Uso de hydra con el host 186.47.XX.C

En la figura 4.20 se puede observar que todos los usuarios y contraseñas usados son válidos, mediante pruebas de autenticación con con los mismos se determina la existencia de un falso positivo, lo que quiere decir que se detecta una vulnerabilidad que en realidad no existe en el servidor.

4.2.5. Autenticación Web Básica

HTTPS, es un protocolo de la capa aplicación que cumple con la trasferencia segura de datos a través de la utilización de cifrado basado en SSL/TLS, diseñado para resistir ataques de tipo man in the middle.

Host	Acceso web	Uso de HTTPS
186.47.XX.A	SI	SI
186.47.XX.B	SI	SI
186.47.XX.C	SI	NO
186.47.XX.D	SI	NO
186.47.XX.F	SI	NO
186.47.XX.G	NO	N/A
186.47.XX.H	NO	N/A
186.47.XX.I	NO	N/A
186.47.XX.J	SI	NO
186.47.XX.K	SI	NO
186.47.XX.L	SI	NO

Tabla 4.3 Identificación de host que usan el protocolo HTTPS.

La tabla 4.5, presenta los equipos que tienen acceso por https obligadamente, los otros equipos no necesariamente establecen un canal seguro para la comunicación permitiendo una debilidad para realizar ataques tipo man-in-the-middle y poder adquirir información en texto plano.

4.2.6. Servicio Web sin Método de Autenticación.

Esta vulnerabilidad se presenta debido a descuidos de administración, puede no ser un sistema crítico pero se podría convertir en un camino de ingreso a los sistemas de la organización.

Se identifica esta vulnerabilidad colocando la dirección IP en el navegador, así se detectó un host con esta debilidad.

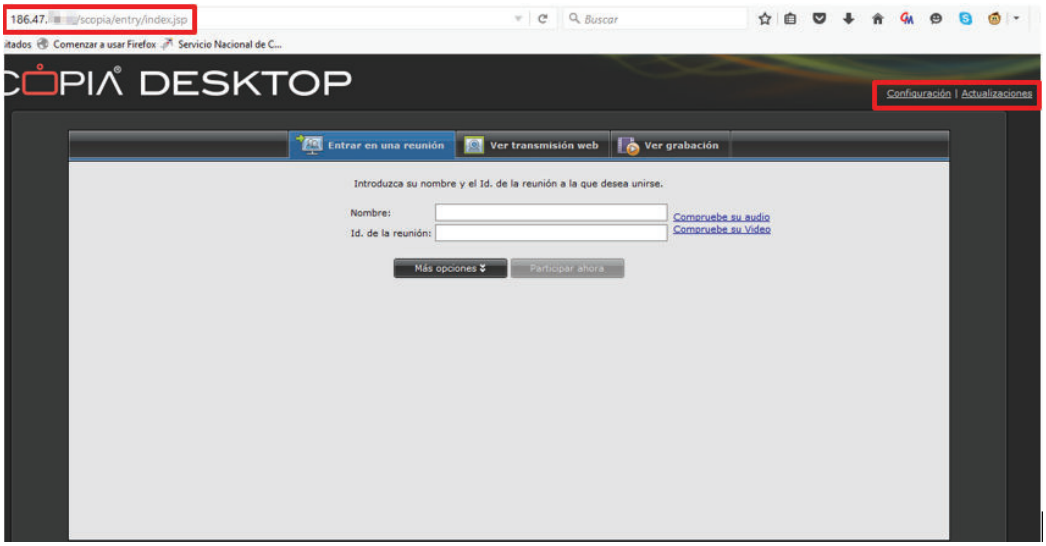


Figura 4.21 Host sin método de autenticación.

4.2.7. Clickjacking

A pesar de no ser una vulnerabilidad crítica, afecta al servidor o a la aplicación web, su principal objetivo es engañar al usuario para dar click en un enlace no deseado.

Para verificar si una página es vulnerable a clickjacking, haremos uso de iframe el cual permite insertar un documento html dentro de otro. Se crea un pequeño código haciendo referencia a cada una de las páginas de autenticación identificadas en la tabla 4.3, se guarda el archivo con la extensión html, se comprueba la debilidad si el archivo se abre correctamente.

De las pruebas realizadas se detecta un host con esta debilidad.

```
<html>
<body>
<iframe scr="http://186.47.[redacted]/doc/page/login.asp">
</body>
</html>
```

Figura 4.22 Uso de iframe para verificar clickjacking.

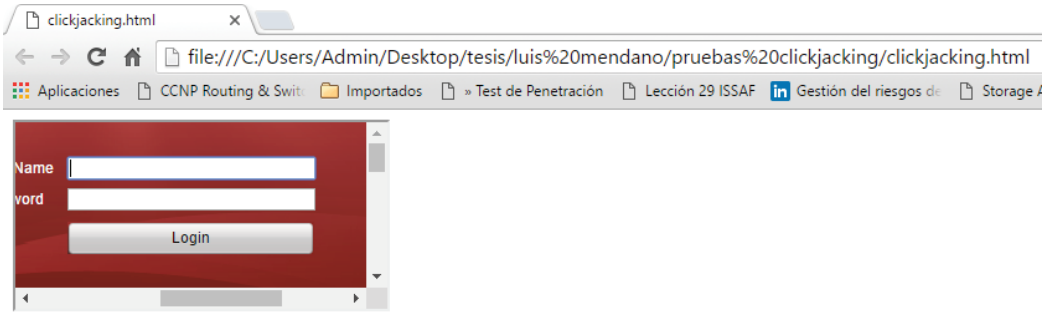


Figura 4.23 Vulnerabilidad clickjacking comprobada.

4.3. PROCEDIMIENTO PARA REALIZAR UN ATAQUE MEDIANTE UN EXPLOIT

Para el uso de un exploit en la explotación de una vulnerabilidad, se debe conocer la herramienta metasploit framework, el cual permite ejecutar exploit sobre un equipo remoto.

Se tomará como ejemplo la vulnerabilidad ***GNU Bash Environment Variable Handling Code Injection (shellshock)***.

El procedimiento es:

a. Inicio del servicio de metasploit framework.

Figura 4.24 Inicio de metasploit framework. (a)

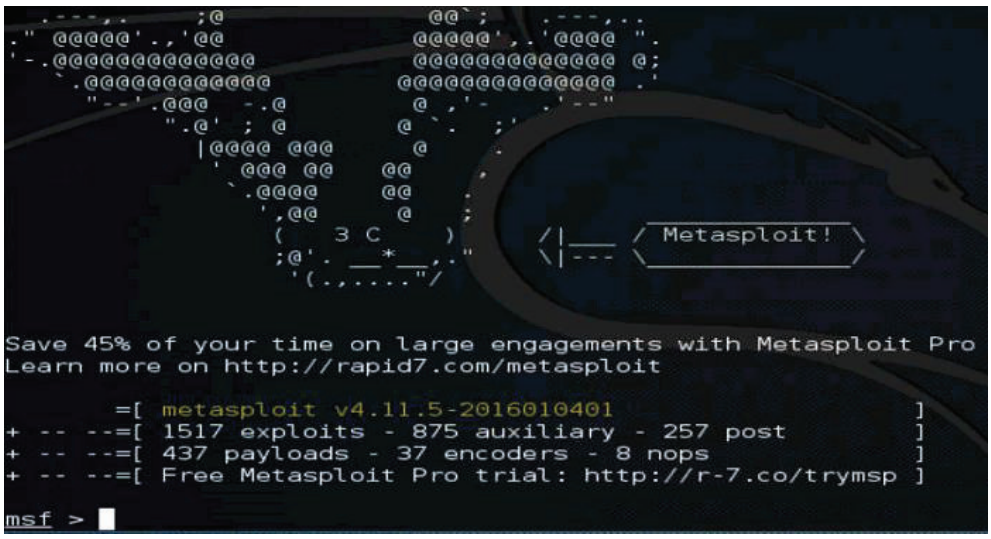


Figura 4.25 Inicio de metasploit framework. (b)

b. Búsqueda del exploit que indica la vulnerabilidad → shellshock.

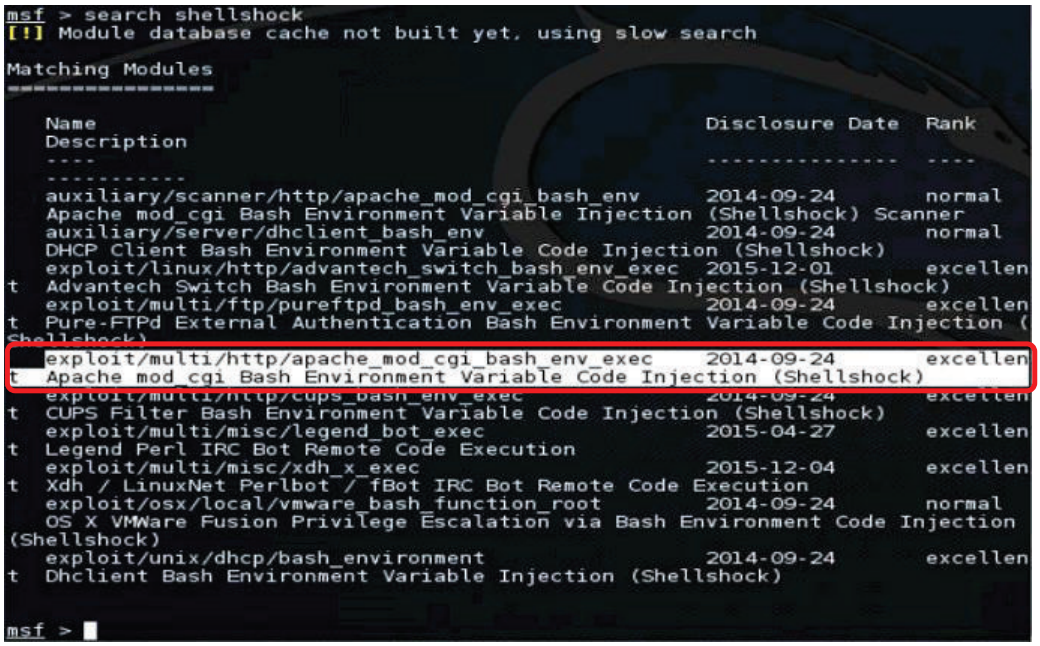


Figura 4.26 Búsqueda del exploit.

c. Después de haber buscado el exploit y saber la ruta donde se encuentra lo usamos con el comando **use** y le pasamos la ruta que nos dió la búsqueda realizada anteriormente (figura 4.26).

Figura 4.27 Uso del exploit.

d. Antes de usar el exploit es necesario saber que parámetros necesita para ser ejecutado y esto lo podemos visualizar con el comando **show options** que lo que hará es mostrarnos detalladamente los parámetros obligatorios que debe tener el exploit antes de ser ejecutado, lo cual lo podemos ver en la columna Required de la figura 4.28. Los parámetros varían de acuerdo al exploit que utilicemos.

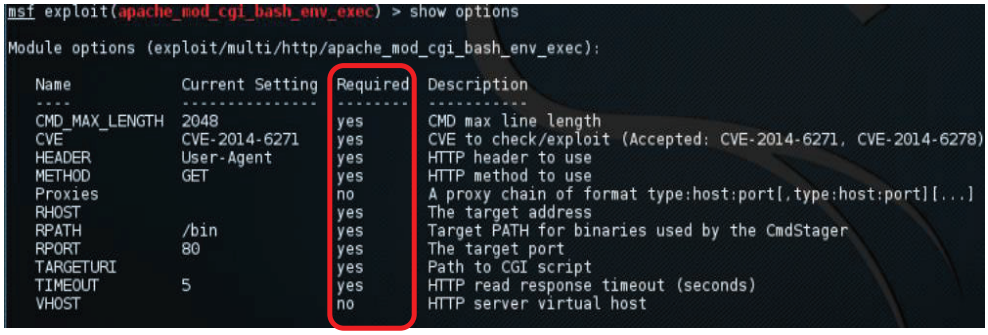


Figura 4.28 Configuración de parámetros.

e. Para emplear el exploit en nuestro objetivo, se usará la opción > set RHOST 186.47.XX.C

f. También es posible asignar un payload, este nos permite realizar una acción después de haber explotado un fallo exitosamente. Mediante el comando **show payload** se puede ver las opciones que se puede usar. (Figura 4.29).

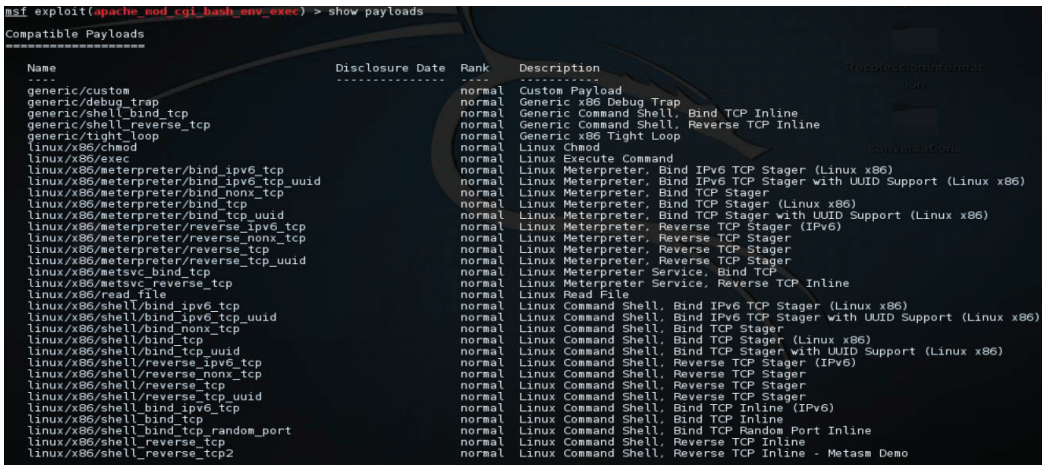


Figura 4.29 Lista de payloads a usar.

Después de ejecutar el comando show payloads nos arroja una lista de los posibles payloads que podemos usar, además cómo podemos observar en el inicio de la ruta se identifica que sistema operativo es funcional a este payload, podemos ver que hay opciones para Linux, si la vulnerabilidad ha sido explotada exitosamente creara una sesión con el usuario meterpreter de forma reversa, que quiere decir esto que la computadora vulnerada se conectara hacia nosotros y tendremos acceso a ella por medio de este usuario (meterpreter).

Asignamos el payload con el comando set payload **linux/x86/netsvc/reverse_tcp**

g. Para finalizar, se ejecuta el comando exploit, con lo cual ya estaremos dentro del sistema.

CAPÍTULO V

5. REPORTE DEL ANÁLISIS DE VULNERABILIDADES Y PLAN DE CORRECCIONES

En este capítulo se realizará el reporte de toda la información obtenida, convirtiendo todos los datos conseguidos en información que permita tomar medidas correctivas.

Además se presenta un plan de correcciones, en el cual se indica las actividades a realizar para mitigar las vulnerabilidades encontradas.

5.1.RESUMEN EJECUTIVO

Con el objetivo de analizar la postura de seguridad de la Organización evaluada y mejorar o potenciar su infraestructura, se llevaron a cabo prácticas de hacking ético con las debidas recomendaciones para reducir el riesgo de pérdida, intervención o adulteración de la información sensible que la empresa maneja.

En el periodo de evaluación se ha efectuado un conjunto de pruebas constantes a cada uno de los servicios, sin comprometer o perjudicar el desempeño de los servidores, para detectar errores en la seguridad, basándonos en metodologías de pruebas de penetración.

Como resultado de las pruebas efectuadas, se han localizado fallas considerables como: contraseñas por defecto, falta de actualizaciones en los servicios, visibilidad de equipos críticos, entre otros, lo cual demuestra que la postura de seguridad de la red perimetral no es la adecuada y que las contramedidas recomendadas para administración de redes no han sido consideradas.

A continuación un resumen de las vulnerabilidades encontradas:

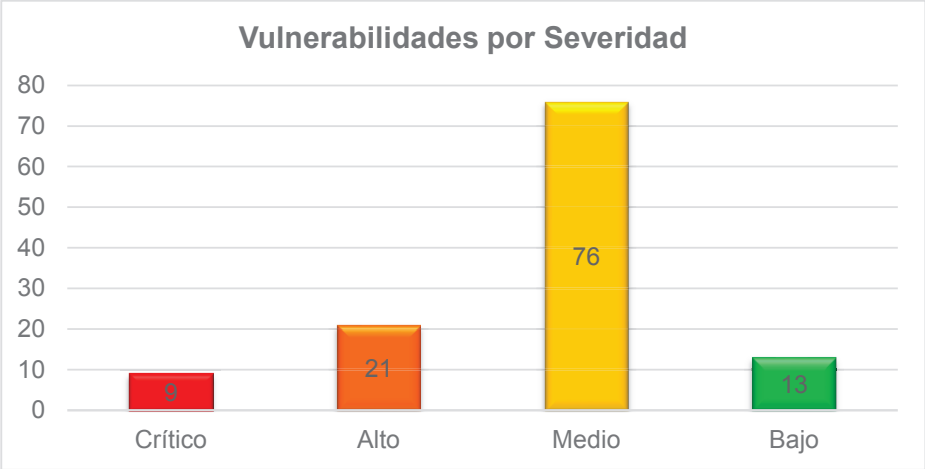


Figura 5.1 Evaluación de riegos en base a la gravedad.

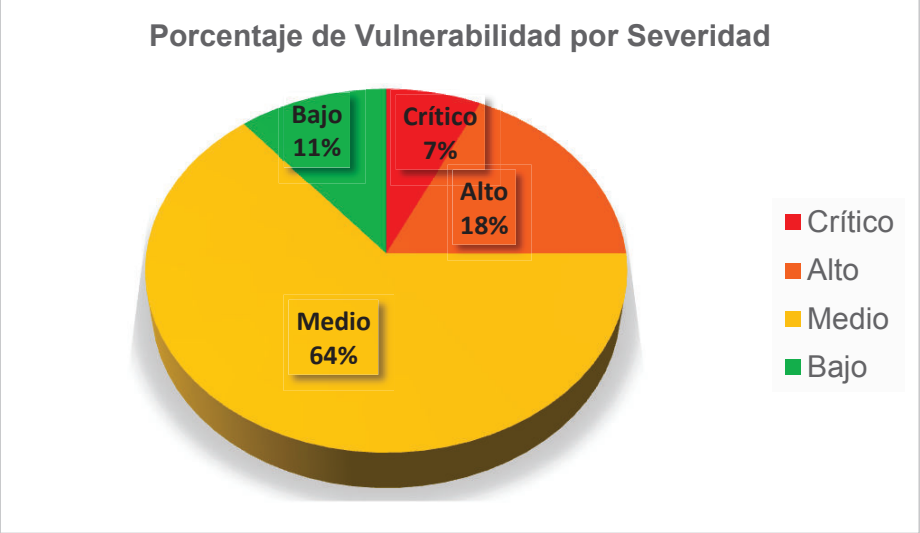


Figura 5.2 Evaluación de riesgos en base al porcentaje.

En las siguientes secciones se detallarán las vulnerabilidades encontradas, una descripción de ellas y contramedidas para mitigar las mismas.

5.2.REPORTE DE REMEDIACIÓN

Se ha evaluado la seguridad informática de la red perimetral a los servicios que presta o brinda la organización, mediante el mismo se ha identificado ciertas irregularidades que podrían desencadenar en acciones perjudiciales, motivo por el cual se sugieren ciertas medidas que brindarán un ambiente más robusto y controlado ante posibles sucesos delictivos.

- Al inicio del análisis se identificó información referente a la organización, como son registros whois, nombres del personal técnico encargado, direcciones de correo, direcciones IPs, dominios, subdominios, algunos posibles servicios y sistemas en repositorios públicos. Si bien todos estos datos se obtuvieron a través de internet de manera pasiva, es decir sin interacción directa con los servidores de la organización, es de mucha importancia que el personal encargado de la seguridad conozca de qué manera la información publicada expone a la empresa y en lo posible disminuir huellas innecesarias que va dejando a través de internet.
- Se detectó host activos pertenecientes al objetivo analizado, a través de barridos constantes a rangos de direcciones IPs, de esta manera se pudo identificar que ciertos servicios estaban activos momentáneamente. Se recomienda configuración en los equipos de seguridad perimetral, como son firewalls, IPS, IDS, de tal manera que no se responda las peticiones de PING, o en su defecto las herramientas detecten actividades sospechosas como: barrido de direcciones, consultas de banners, consulta de puertos abiertos, etc.
- El firewall es un equipo muy importante para la seguridad de una empresa, por lo tanto, es el objetivo más propenso a ser vulnerado. En el análisis realizado se encontró que el equipo responde a peticiones ICMP al realizar una traza de ruta hacia alguna dirección IP, además se identifica como un servidor de la organización, lo cual pone en evidencia que es un equipo de borde, además se detectaron ciertos puertos abiertos entre ellos ssh. Es recomendable evaluar los puertos abiertos en el firewall y de no ser necesario, cerrarlos, de igual manera se debe verificar los logs en busca de posibles actividades sospechosas.
- El uso de herramientas que interaccionan directamente con los servidores para extracción de datos relevantes acerca de los servicios, ha sido una de las actividades muy importantes en el marco de nuestro proyecto, sin embargo no hemos recibido un reporte de actividad sospechosa, o tráfico de consultas constantes hacia los sistemas, lo cual ha facilitado realizar pruebas periódicamente, esto en condiciones reales, expone a la empresa a ser investigada constantemente en busca

de fallos y buscar posibles vulnerabilidades, por parte de agentes no necesariamente éticos, se recomienda nuevamente reforzar la seguridad perimetral para evitar este tipo de eventos, al igual que configurar la seguridad en cada sistema.

- Dentro de nuestro análisis y consultas constantes a las direcciones IPs públicas, registradas por la organización, se han encontrado ciertos servicios que los identificamos como, servicios de prueba (DEMOS) debido a su corta duración o publicación, a pesar de no ser servicios en producción, se deben tomar todas las medidas necesarias como si lo fueran, en nuestro análisis se identificaron contraseñas por defecto las mismas que nos dieron acceso a la configuración y administración del servicio, de la cual también se pudo obtener información como lista de usuarios, direcciones IP internas, ciertos DNS.

5.3.RESUMEN DE LA EVALUACIÓN DE VULNERABILIDAD

Para el inicio de este proyecto se han establecido condiciones de mutuo acuerdo en el cual se establecen los objetivos y alcance, tomando en cuenta los requisitos de la organización, una vez definidos los entornos bajo las cuales se regirán las pruebas se inicia el análisis de vulnerabilidades.

Basándonos en las diferentes metodologías como osstmm issaf y owasp, se ha dividido el análisis de la siguiente manera; recolección de información, enumeración, análisis de vulnerabilidades, y métodos de explotación.

Como primer punto dentro del análisis, es muy importante conocer a que se dedica la empresa en evaluación, para lo cual hacemos uso de los motores de búsqueda de internet, observando claramente datos que puedan servir para conocer el objetivo, como es muy común hoy en día la organización tiene una página web en la cual se resaltan sus objetivos, su misión y visión. También se han encontrado datos acerca de los servicios que ofrecen, tales como: servicio de correo electrónico, servicio de sistema integrado de trasporte y obras públicas, etc.

Los motores de búsqueda son de gran utilidad para identificar información relevante, pero el número de resultados puede ser muy grande, por lo cual se

han optimizado las búsquedas con una técnica denominada *google hacking*, lo cual ha permitido mediante el uso de filtros realizar consultas específicas.

Una de las maneras más eficaces de recolectar información es hacer consultas directas a los servidores activos de la organización, pero se debe considerar que este tipo de interacción compromete con rastros para ser detectados.

Para la recolección de información de manera activa hemos utilizado un gran número de herramientas, como son: dnsenum, fierce, dmitry, maltego, etc., las cuales han permitido obtener información de la empresa, como son direcciones de dominio y subdominio, direcciones IP, identificando el servidor de correo, el firewall, el SITOP, entre otros.

No solo se han utilizado herramientas para que entregue información sino también, para realizar una análisis automático, como son whatweb, robtex, análisis de cabeceras online.

Dentro del marco de pruebas establecidas se ha realizado un barrido de IPs constante, en el cual se ha constatado y verificado los servicios activos y adicionalmente servicios temporales, los cuales se han identificado como servicios de demo, y han presentado errores en la configuración, los mismos que podrían comprometer la seguridad de la entidad evaluada.

Finalizando la recolección de información, sin dejar de lado ningún parámetro obtenido en esta fase, procedemos a enumerar los objetivos de análisis y ataque, reconociendo todos los host activos y permanentes al igual que puertos, servicios y sistemas de cada uno de los objetivos encontrados.

Con toda la información recolectada e identificando los respectivos vectores de ataque, se configuraron las herramientas OpenVAS y Nessus para realizar un análisis de vulnerabilidades, encontrando como resultado que ciertos servicios de la organización presentan vulnerabilidades de diferente severidad.

Se presenta un resumen de todas las vulnerabilidades encontradas:

- 186.47.XX.A

RESUMEN					
Crítico	**Alto**	**Medio**	**Bajo**	**Info**	**Total**
0	0	9	3	47	59

DETALLES	
Severidad	**Nombre**
Medio (6.4)	SSL Certificate Cannot Be Trusted
Medio (6.4)	SSL Self-Signed Certificate
Medio (5.0)	SSL Version 2 and 3 Protocol Detection
Medio (4.3)	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
Medio (4.3)	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Medio (4.3)	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medio (4.0)	IMAP Service STARTTLS Plaintext Command Injection
Medio (4.0)	POP3 Service STLS Plaintext Command Injection
Medio (4.0)	SMTP Service STARTTLS Plaintext Command Injection
Bajo (2.8)	POP3 Cleartext Logins Permitted
Bajo (2.6)	Web Server Transmits Cleartext Credentials
Bajo (2.6)	Web Server Uses Basic Authentication Without HTTPS
Info	HTTP Server Type and Version
Info	POP Server Detection
Info	SMTP Server Detection
Info	Traceroute Information
Info	Web Server robots.txt Information Disclosure
Info	Web Server No 404 Error Code Check
Info	Web mirroring
Info	SSL Certificate Information
Info	Open Port Re-check
Info	Web Server Directory Enumeration
Info	Nessus SYN scanner

Severidad	Nombre
Info	IMAP Service Banner Retrieval
Info	OS Identification
Info	Host Fully Qualified Domain Name (FQDN) Resolution
Info	Service Detection: 3 ASCII Digit Code Responses
Info	Service Detection (GET request)
Info	Nessus Scan Information
Info	SSL Cipher Suites Supported
Info	Service Detection
Info	HyperText Transfer Protocol (HTTP) Information
Info	TCP/IP Timestamps Supported
Info	XMPP Server Detection
Info	CGI Generic Tests Load Estimation (all tests)
Info	CGI Generic Tests Timeout
Info	Web Application Potentially Sensitive CGI Parameter Detection
Info	POP3 Service STLS Command Support
Info	SMTP Service STARTTLS Command Support
Info	XMPP Service STARTTLS Command Support
Info	HTTP Methods Allowed (per directory)
Info	Common Platform Enumeration (CPE)
Info	CGI Generic Injectable Parameter
Info	External URLs
Info	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	OpenSSL Detection
Info	Web Server Uses Basic Authentication over HTTPS
Info	SSL Session Resume Supported
Info	SMTP Authentication Methods
Info	Device Type
Info	SSL Certificate Chain Not Sorted
Info	SSL Certificate Chain Contains Unnecessary Certificates
Info	SSL / TLS Versions Supported

Severidad	Nombre
Info	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	SSL Cipher Block Chaining Cipher Suites Supported
Info	Zimbra Collaboration Server Web Detection
Info	HSTS Missing From HTTPS Server
Info	Web Application Cookies Not Marked HttpOnly
Info	Web Application Cookies Not Marked Secure

Tabla 5.1 Resumen de vulnerabilidades de IP 186.47.XX.A

- 186.47.XX.B

RESUMEN					
Crítico	Alto	Medio	Bajo	Info	Total
0	0	6	3	27	36
DETALLES					
Severidad	**Nombre**				
Medio (6.4)	SSL Certificate Cannot Be Trusted				
Medio (6.4)	SSL Self-Signed Certificate				
Medio (5.0)	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key				
Medio (4.3)	SSL/TLS Protocol Initialization Vector Implementation Information				
Medio (4.0)	SSH Protocol Version 1 Session Key Retrieval				
Medio (4.0)	SSL Certificate Signed Using Weak Hashing Algorithm				
Bajo (2.6)	SSH Server CBC Mode Ciphers Enabled				
Bajo (2.6)	SSH Weak MAC Algorithms Enabled				
Bajo (0.0)	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits				
Info	SSH Server Type and Version Information				
Info	Traceroute Information				
Info	Web mirroring				
Info	SSL Certificate Information				
Info	SSH Protocol Versions Supported				
Info	Nessus SYN scanner				

Severidad	Nombre
Info	IMAP Service Banner Retrieval
Info	IPSEC Internet Key Exchange (IKE) Version 1 Detection
Info	OS Identification
Info	Host Fully Qualified Domain Name (FQDN) Resolution
Info	Nessus Scan Information
Info	Service Detection
Info	TCP/IP Timestamps Supported
Info	CGI Generic Tests Load Estimation (all tests)
Info	Nessus UDP Scanner
Info	CGI Generic Tests Timeout
Info	CGI Generic Tests HTTP Errors
Info	Web Application Potentially Sensitive CGI Parameter Detection
Info	CISCO ASA SSL VPN Detection
Info	HTTP Methods Allowed (per directory)
Info	SSL Certificate commonName Mismatch
Info	CGI Generic Injectable Parameter
Info	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	Device Type
Info	SSL / TLS Versions Supported
Info	SSH Algorithms and Languages Supported
Info	Web Application Cookies Not Marked HttpOnly

Tabla 5.2 Resumen de vulnerabilidades de IP 186.47.XX.B

- 186.47.XX.C

RESUMEN					
Crítico	**Alto**	**Medio**	**Bajo**	**Info**	**Total**
1	0	2	0	21	24
DETALLES					
Severidad	**Nombre**				
Crítico (10.0)	GNU Bash Environment Variable Handling Code Injection (Shellshock)				
Medio (5.0)	HTTP TRACE / TRACK Methods Allowed				
Medio (5.0)	Apache Server ETag Header Information Disclosure				
Info	HTTP Server Type and Version				
Info	Traceroute Information				
Info	Web Server Directory Enumeration				
Info	Nessus SYN scanner				
Info	WebDAV Detection				
Info	OS Identification				
Info	Host Fully Qualified Domain Name (FQDN) Resolution				
Info	Nessus Scan Information				
Info	Service Detection				
Info	HyperText Transfer Protocol (HTTP) Information				
Info	TCP/IP Timestamps Supported				
Info	Nessus UDP Scanner				
Info	Backported Security Patch Detection (WWW)				
Info	HTTP Methods Allowed (per directory)				
Info	Common Platform Enumeration (CPE)				
Info	Inconsistent Hostname and IP Address				
Info	Missing or Permissive Content-Security-Policy HTTP Response Header				
Info	Missing or Permissive X-Frame-Options HTTP Response Header				
Info	Device Type				
Info	OpenSSL Version Detection				
Info	Patch Report				

Tabla 5.3 Resumen de vulnerabilidades de IP 186.47.XX.C

- 186.47.XX.D

RESUMEN					
Crítico	Alto	Medio	Bajo	Info	Total
1	2	12	2	31	48

DETALLES	
Severidad	Nombre
Crítico (10.0)	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution
Alto (9.3)	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code
Alto (9.3)	Apache Tomcat 6.0.x < 6.0.43 Multiple Vulnerabilities (POODLE)
Medio (6.4)	SSL Certificate Cannot Be Trusted
Medio (6.4)	SSL Self-Signed Certificate
Medio (5.8)	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
Medio (5.1)	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medio (5.0)	SSL Version 2 and 3 Protocol Detection
Medio (4.3)	SSL Medium Strength Cipher Suites Supported
Medio (4.3)	Terminal Services Encryption Level is Medium or Low
Medio (4.3)	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Medio (4.3)	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Medio (4.3)	SSL Null Cipher Suites Supported
Medio (4.3)	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medio (4.0)	SSL Certificate Signed Using Weak Hashing Algorithm
Bajo (2.6)	Terminal Services Encryption Level is not FIPS-140 Compliant
Bajo (0.0)	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	HTTP Server Type and Version

Severidad	Nombre
Info	Web Server robots.txt Information Disclosure
Info	SSL Certificate Information
Info	Windows Terminal Services Enabled
Info	Nessus SYN scanner
Info	OS Identification
Info	Host Fully Qualified Domain Name (FQDN) Resolution
Info	Nessus Scan Information
Info	SSL Cipher Suites Supported
Info	Service Detection
Info	HyperText Transfer Protocol (HTTP) Information
Info	TCP/IP Timestamps Supported
Info	Nessus UDP Scanner
Info	Apache Tomcat Default Error Page Version Detection
Info	HTTP Methods Allowed (per directory)
Info	SSL Certificate commonName Mismatch
Info	Common Platform Enumeration (CPE)
Info	Inconsistent Hostname and IP Address
Info	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	Missing or Permissive X-Frame-Options HTTP Response Header
Info	SSL Session Resume Supported
Info	Device Type
Info	SSL / TLS Versions Supported
Info	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	Terminal Services Use SSL/TLS
Info	RDP Screenshot
Info	Patch Report
Info	SSL Cipher Block Chaining Cipher Suites Supported
Info	Web Application Cookies Not Marked HttpOnly
Info	Web Application Cookies Not Marked Secure
Info	SSL Certificate Signed Using SHA-1 Algorithm

Tabla 5.4 Resumen de vulnerabilidades de IP 186.47.XX.D

- 186.47.XX.E

RESUMEN					
Crítico	**Alto**	**Medio**	**Bajo**	**Info**	**Total**
1	6	29	0	37	73

DETALLES	
Severidad	**Nombre**
Crítico (10.0)	OpenSSL Unsupported
Alto (9.3)	OpenSSL < 0.9.8s Multiple Vulnerabilities
Alto (9.3)	OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities
Alto (7.6)	OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow
Alto (7.5)	Unsupported Web Server Detection
Alto (7.5)	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption
Alto (7.1)	OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities
Medio (6.8)	OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities
Medio (6.8)	OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities
Medio (6.4)	SSL Certificate Cannot Be Trusted
Medio (6.4)	SSL Self-Signed Certificate
Medio (5.8)	OpenSSL < 0.9.8j Signature Spoofing
Medio (5.1)	OpenSSL < 0.9.8l Multiple Vulnerabilities
Medio (5.0)	HTTP TRACE / TRACK Methods Allowed
Medio (5.0)	SSL Certificate Expiry
Medio (5.0)	OpenSSL < 0.9.8i Denial of Service
Medio (5.0)	OpenSSL < 0.9.8k Denial of Service
Medio (5.0)	SSL Version 2 and 3 Protocol Detection
Medio (5.0)	Browsable Web Directories
Medio (5.0)	OpenSSL < 0.9.8u Multiple Vulnerabilities
Medio (5.0)	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service
Medio (5.0)	OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities (FREAK)
Medio (5.0)	OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS
Medio (4.3)	OpenSSL < 0.9.8p / 1.0.0e Double Free Vulnerability
Medio (4.3)	CGI Generic XSS (quick test)

Severidad	Nombre
Medio (4.3)	CGI Generic Cookie Injection Scripting
Medio (4.3)	CGI Generic XSS (comprehensive test)
Medio (4.3)	CGI Generic HTML Injections (quick test)
Medio (4.3)	OpenSSL < 0.9.8h Multiple Vulnerabilities
Medio (4.3)	Apache HTTP Server httpOnly Cookie Information Disclosure
Medio (4.3)	Transport Layer Security (TLS) Protocol CRIME Vulnerability
Medio (4.3)	OpenSSL < 0.9.8y Multiple Vulnerabilities
Medio (4.3)	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Medio (4.3)	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medio (4.3)	OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE)
Medio (4.3)	Web Application Potentially Vulnerable to Clickjacking
Info	HTTP Server Type and Version
Info	Traceroute Information
Info	Web mirroring
Info	SSL Certificate Information
Info	Web Server Directory Enumeration
Info	Nessus SYN scanner
Info	WebDAV Detection
Info	OS Identification
Info	Host Fully Qualified Domain Name (FQDN) Resolution
Info	Nessus Scan Information
Info	SSL Cipher Suites Supported
Info	Service Detection
Info	HyperText Transfer Protocol (HTTP) Information
Info	TCP/IP Timestamps Supported
Info	CGI Generic Tests Load Estimation (all tests)
Info	CGI Generic Tests Timeout
Info	CGI Generic Tests HTTP Errors
Info	Web Server Allows Password Auto-Completion

Severidad	Nombre
Info	HTTP Methods Allowed (per directory)
Info	SSL Certificate commonName Mismatch
Info	Common Platform Enumeration (CPE)
Info	Inconsistent Hostname and IP Address
Info	CGI Generic Injectable Parameter
Info	External URLs
Info	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	Missing or Permissive X-Frame-Options HTTP Response Header
Info	OpenSSL Detection
Info	Device Type
Info	SSL / TLS Versions Supported
Info	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	OpenSSL Version Detection
Info	SSL Compression Methods Supported
Info	Patch Report
Info	SSL Cipher Block Chaining Cipher Suites Supported
Info	HSTS Missing From HTTPS Server
Info	Web Application Cookies Not Marked HttpOnly
Info	Web Application Cookies Not Marked Secure

Tabla 5.5 Resumen de vulnerabilidades de IP 186.47.XX.E

- 186.47.XX.F

RESUMEN					
Crítico	Alto	Medio	Bajo	Info	Total
6	13	8	1	30	58
DETALLES					
Severidad	Nombre				
Crítico (10.0)	PHP 5.5.x < 5.5.14 Multiple Vulnerabilities				
Crítico (10.0)	PHP 5.5.x < 5.5.29 Multiple Vulnerabilities				

Severidad	Nombre
Crítico (10.0)	PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilities
Crítico (10.0)	PHP 5.5.x < 5.5.32 Multiple Vulnerabilities
Crítico (10.0)	PHP 5.5.x < 5.5.33 Multiple Vulnerabilities
Crítico (10.0)	PHP 5.5.x < 5.5.34 Multiple Vulnerabilities
Alto (9.3)	PHP 5.5.x < 5.5.18 Multiple Vulnerabilities
Alto (9.3)	PHP 5.5.x < 5.5.26 Multiple Vulnerabilities
Alto (9.3)	PHP 5.5.x < 5.5.28 Multiple Vulnerabilities
Alto (8.5)	PHP 5.5.x < 5.5.30 Multiple Vulnerabilities
Alto (7.8)	PHP 5.5.x < 5.5.19 'donote' DoS
Alto (7.8)	PHP 5.5.x < 5.5.25 Multiple Vulnerabilities
Alto (7.8)	PHP 5.5.x < 5.5.22 Multiple Vulnerabilities (GHOST)
Alto (7.5)	Apache 2.4.x < 2.4.10 Multiple Vulnerabilities
Alto (7.5)	PHP 5.5.x < 5.5.16 Multiple Vulnerabilities
Alto (7.5)	PHP 5.5.x < 5.5.20 'process_nested_data' RCE
Alto (7.5)	PHP 5.5.x < 5.5.21 Multiple Vulnerabilities
Alto (7.5)	PHP 5.5.x < 5.5.23 Multiple Vulnerabilities
Alto (7.5)	PHP 5.5.x < 5.5.24 Multiple Vulnerabilities
Medio (6.8)	PHP 5.5.x < 5.5.27 Multiple Vulnerabilities (BACKRONYM)
Medio (5.0)	HTTP TRACE / TRACK Methods Allowed
Medio (5.0)	Browsable Web Directories
Medio (5.0)	PHP 5.5.x < 5.5.13 'src/cdf.c' Multiple Vulnerabilities
Medio (5.0)	Apache 2.4.x < 2.4.12 Multiple Vulnerabilities
Medio (5.0)	Apache 2.4.x < 2.4.16 Multiple Vulnerabilities
Medio (4.3)	PHP 5.5.x < 5.5.15 Multiple Vulnerabilities
Medio (4.3)	Web Application Potentially Vulnerable to Clickjacking
Bajo (2.6)	Web Server Transmits Cleartext Credentials
Info	HTTP Server Type and Version
Info	Traceroute Information
Info	Web mirroring
Info	Web Server Directory Enumeration
Info	Nessus SYN scanner

Severidad	Nombre
Info	OS Identification
Info	Host Fully Qualified Domain Name (FQDN) Resolution
Info	Nessus Scan Information
Info	Service Detection
Info	HyperText Transfer Protocol (HTTP) Information
Info	TCP/IP Timestamps Supported
Info	PostgreSQL Server Detection
Info	Web Site Cross-Domain Policy File Detection
Info	CGI Generic Tests Load Estimation (all tests)
Info	Nessus UDP Scanner
Info	CGI Generic Tests Timeout
Info	Web Application Potentially Sensitive CGI Parameter Detection
Info	Web Server Allows Password Auto-Completion
Info	HTTP Methods Allowed (per directory)
Info	Common Platform Enumeration (CPE)
Info	Inconsistent Hostname and IP Address
Info	CGI Generic Injectable Parameter
Info	PHP Version
Info	External URLs
Info	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	Missing or Permissive X-Frame-Options HTTP Response Header
Info	Device Type
Info	Patch Report
Info	Web Site Client Access Policy File Detection
Info	Web Application Cookies Not Marked Secure

Tabla 5.6 Resumen de vulnerabilidades de IP 186.47.XX.F

- 186.47.XX.I

RESUMEN					
Crítico	Alto	Medio	Bajo	Info	Total
0	0	1	2	18	21
DETALLES					
Severidad	**Nombre**				
Medio (4.3)	SSH Weak Algorithms Supported				
Bajo (2.6)	SSH Server CBC Mode Ciphers Enabled				
Bajo (2.6)	SSH Weak MAC Algorithms Enabled				
Info	SSH Server Type and Version Information				
Info	Traceroute Information				
Info	VNC Software Detection				
Info	SSH Protocol Versions Supported				
Info	Nessus SYN scanner				
Info	OS Identification				
Info	Host Fully Qualified Domain Name (FQDN) Resolution				
Info	VNC Server Security Type Detection				
Info	Nessus Scan Information				
Info	Service Detection				
Info	TCP/IP Timestamps Supported				
Info	Nessus UDP Scanner				
Info	Backported Security Patch Detection (SSH)				
Info	Common Platform Enumeration (CPE)				
Info	Inconsistent Hostname and IP Address				
Info	Device Type				
Info	VNC Server Unencrypted Communication Detection				
Info	SSH Algorithms and Languages Supported				

Tabla 5.7 Resumen de vulnerabilidades de IP 186.47.XX.I

- 186.47.XX.J

RESUMEN					
Crítico	**Alto**	**Medio**	**Bajo**	**Info**	**Total**
0	0	8	2	31	41

DETALLES	
Severidad	**Nombre**
Medio (6.4)	SSL Certificate Cannot Be Trusted
Medio (5.8)	Unencrypted Telnet Server
Medio (5.8)	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
Medio (5.8)	SSL Version 2 and 3 Protocol Detection
Medio (4.3)	SSL Weak Cipher Suites Supported
Medio (4.3)	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Medio (4.3)	Web Application Potentially Vulnerable to Clickjacking
Medio (4.0)	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
Bajo (2.6)	Web Server Transmits Cleartext Credentials
Bajo	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	Telnet Server Detection
Info	Traceroute Information
Info	Web Server No 404 Error Code Check
Info	Web mirroring
Info	RTSP Server Type / Version Detection
Info	SSL Certificate Information
Info	Network Time Protocol (NTP) Server Detection
Info	Open Port Re-check
Info	Nessus SYN scanner
Info	OS Identification
Info	Host Fully Qualified Domain Name (FQDN) Resolution
Info	Nessus Scan Information
Info	SSL Cipher Suites Supported
Info	Service Detection

Severidad	Nombre
Info	HyperText Transfer Protocol (HTTP) Information
Info	CGI Generic Tests Load Estimation (all tests)
Info	CGI Generic Tests HTTP Errors
Info	Web Server Allows Password Auto-Completion
Info	SSL Certificate Expiry - Future Expiry
Info	SSL Certificate commonName Mismatch
Info	Common Platform Enumeration (CPE)
Info	Inconsistent Hostname and IP Address
Info	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	Missing or Permissive X-Frame-Options HTTP Response Header
Info	OpenSSL Detection
Info	Device Type
Info	SSL / TLS Versions Supported
Info	SSL Cipher Block Chaining Cipher Suites Supported
Info	SSL Certificate Chain Contains Certificates Expiring Soon
Info	HSTS Missing From HTTPS Server
Info	SSL Certificate Signed Using SHA-1 Algorithm

Tabla 5.8 Resumen de vulnerabilidades de IP 186.47.XX.J

- 186.47.XX.K

RESUMEN					
Crítico	**Alto**	**Medio**	**Bajo**	**Info**	**Total**
0	0	1	0	13	14
DETALLES					
Severidad	**Nombre**				
Medio (4.3)	Web Application Potentially Vulnerable to Clickjacking				
Info	HTTP Server Type and Version				
Info	Traceroute Information				
Info	Nessus SYN scanner				
Info	Host Fully Qualified Domain Name (FQDN) Resolution				
Info	Nessus Scan Information				
Info	Service Detection				
Info	HyperText Transfer Protocol (HTTP) Information				
Info	TCP/IP Timestamps Supported				
Info	Nessus UDP Scanner				
Info	HTTP Methods Allowed (per directory)				
Info	Inconsistent Hostname and IP Address				
Info	Missing or Permissive Content-Security-Policy HTTP Response Header				
Info	Missing or Permissive X-Frame-Options HTTP Response Header				

Tabla 5.9 Resumen de vulnerabilidades de IP 186.47.XX.K

- 186.47.XX.L

RESUMEN					
Crítico	**Alto**	**Medio**	**Bajo**	**Info**	**Total**
0	0	0	0	16	16
DETALLES					
Severidad	**Nombre**				
Info	HTTP Server Type and Version				
Info	Nessus SYN scanner				
Info	OS Identification				

Severidad	Nombre
	Host Fully Qualified Domain Name (FQDN) Resolution
Info	Nessus Scan Information
	Service Detection
Info	HyperText Transfer Protocol (HTTP) Information
Info	TCP/IP Timestamps Supported
Info	Nessus UDP Scanner
Info	HTTP Methods Allowed (per directory)
Info	Common Platform Enumeration (CPE)
Info	Inconsistent Hostname and IP Address
Info	External URLs
Info	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	Missing or Permissive X-Frame-Options HTTP Response Header
Info	Device Type

Tabla 5.10 Resumen de vulnerabilidades de IP 186.47.XX.L

Finalmente mediante un plan de ataques aprobado por la organización, se realizan pruebas para verificar las vulnerabilidades encontradas, detectando las siguientes fallas:

- Falta de uso de cifrado en transmisión de credenciales, lo que podría permitir a un atacante robar las mismas para cometer actos delictivos.
- Uso de protocolos no seguros como es http.
- Aplicaciones sin ningún parámetro de seguridad, en los cuales se puede ingresar como administrador y ver información confidencial.
- Mediante la búsqueda de directorios web se pudieron identificar páginas de autenticación para sistemas críticos.

5.4.PLAN DE MITIGACIÓN

Para mitigar el riesgo que conlleva cada una de las vulnerabilidades presentadas se proponen varias actividades, dependiendo del tipo de debilidad encontrada.

- **Vulnerabilidad: SSL Certificate Cannot Be Trusted**

  Presentada en los hosts: 186.47.XX.A, 186.47.XX.B, 186.47.XX.D y 176.47.XX.J.

  Esta debilidad indica que el certificado SSL para el servicio no es de confianza, para mitigar esta vulnerabilidad se recomienda adquirir un certificado adecuado para el servicio.

- **Vulnerabilidad: SSL Self-Signed Certificate**

  Presentada en los hosts: 186.47.XX.A, 186.47.XX.B y 186.47.XX.D.

  Esta debilidad indica que la cadena de certificados SSL para este servicio termina en un certificado auto-firmado no reconocido, para mitigar esta vulnerabilidad se recomienda adquirir un certificado adecuado para el servicio.

- **Vulnerabilidad: SSL Version 2 and 3 Protocol Detection**

  Presentada en los hosts: 186.47.XX.A, 186.47.XX.D y 186.47.XX.J.

  Esta debilidad indica que el servicio remoto encripta tráfico usando un protocolo con deficiencias conocidas, para mitigar esta vulnerabilidad se recomienda deshabilitar SSL 2.0 y 3.0 ó usar un conjunto de certificados aprobados, como TLS 1.1 o superior.

- **Vulnerabilidad: SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)**

  Presentada en los hosts: 186.47.XX.A y 186.47.XX.F.

  Esta debilidad indica que puede ser posible obtener información sensible desde el host remoto con el/los servicios habilitados para SSL/TLS, para mitigar esta vulnerabilidad se recomienda: configurar los servidores para soportar TLS 1.1 o 1.2, configurar los servidores SSL/TLS solo para admitir conjuntos de cifrados que no usen cifrado de bloque y aplicar todos los parches necesarios.

- **Vulnerabilidad: SSL RC4 Cipher Suites Supported (Bar Mitzvah)**

  Presentada en los hosts: 186.47.XX.A, 186.47.XX.D y 186.47.XX.J.

  Esta debilidad indica que el servicio remoto es compatible con el uso del sistema de cifrado RC4, para mitigar esta vulnerabilidad se recomienda evitar el uso de cifrado RC4 y usar TLS 1.2 con un conjunto de cifrado AES-GCM.

- **Vulnerabilidad: SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)**

  Presentada en los hosts: 186.47.XX.A y 186.47.XX.D.

  Esta debilidad indica que es posible obtener información sensible desde el host remoto con los servicios SSL/TLS habilitados, para mitigar esta vulnerabilidad se recomienda deshabilitar SSLv3 en caso de no poder ser desactivado se debe habilitar el mecanismo TLS Fallback SCSV.

- **Vulnerabilidad: IMAP Service STARTTLS Plaintext Command Injection**

  Presentada en el host: 186.47.XX.A.

  Esta debilidad indica que el servicio remoto de correo permite inyección de comandos en texto plano mientras negocia un canal de comunicación cifrado, para mitigar esta vulnerabilidad se recomienda actualizar la versión del servidor.

- **Vulnerabilidad: POP3 Service STLS Plaintext Command Injection**

  Presentada en el host: 186.47.XX.A.

  Esta debilidad indica que el servicio remoto de correo permite inyección de comandos en texto plano mientras negocia un canal de comunicación cifrado, para mitigar esta vulnerabilidad se recomienda actualizar la versión del servidor.

- **Vulnerabilidad: SMTP Service STARTTLS Plaintext Command Injection**

  Presentada en el host: 186.47.XX.A.

  Esta debilidad indica que el servicio remoto de correo permite inyección de comandos en texto plano mientras negocia un canal de comunicación cifrado, para mitigar esta vulnerabilidad se recomienda actualizar la versión del servidor.

- **Vulnerabilidad: POP3 Cleartext Logins Permitted**

  Presentada en el host: 186.47.XX.A.

  Esta debilidad indica que el demonio remoto POP3 permite credenciales para ser transmitidos en texto plano, para mitigar esta vulnerabilidad se recomienda cifrar el tráfico usando SSL/TLS usando stunnel.

- **Vulnerabilidad: Web Server Transmits Cleartext Credentials**
  Presentada en los hosts: 186.47.XX.A, 186.47.XX.F y 186.47.XX.J.
  Esta debilidad indica que el servidor web remoto puede transmitir las credenciales en texto sin cifrar, para mitigar esta vulnerabilidad se recomienda transmitir contenido sensible a través de HTTPS.
- **Vulnerabilidad: Web Server Uses Basic Authentication Without HTTPS**
  Presentada en el host: 186.47.XX.A.
  Esta debilidad indica que el servidor web remoto parece transmitir las credenciales en texto sin cifrar, para mitigar esta vulnerabilidad se recomienda verificar que las autenticaciones HTTP se transmitan sobre HTTPS.
- **Vulnerabilidad: Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key**
  Presentada en el host: 186.47.XX.A.
  Esta debilidad indica que el servicio remoto IKEv1 soporta el modo agresivo de clave pre-compartida, para mitigar esta vulnerabilidad se recomienda: deshabilitar el modo agresivo, no usar clave en modo compartido para autenticaciones, usar claves fuertes, no permitir conexiones VPN desde cualquier dirección IP.
- **Vulnerabilidad: SSH Protocol Version 1 Session Key Retrieval**
  Presentada en el host: 186.47.XX.B.
  Esta debilidad indica que el servicio remoto ofrece un protocolo de encriptación inseguro, para mitigar esta vulnerabilidad se recomienda deshabilitar la compatibilidad del protocolo con la versión 1.
- **Vulnerabilidad: SSL Certificate Signed Using Weak Hashing Algorithm**
  Presentada en los hosts: 186.47.XX.B, 186.47.XX.D.
  Esta debilidad indica que un certificado SSL en la cadena de certificados se ha firmado utilizando un algoritmo de hash débil, para mitigar esta vulnerabilidad se debe obtener un certificado reeditado mediante la Autoridad Certificadora.

- **Vulnerabilidad: SSH Server CBC Mode Ciphers Enabled**
  Presentada en los hosts: 186.47.XX.D y 186.47.XX.I.
  Esta debilidad indica que el servidor SSH está configurado para usar Cipher Block Chaining, para mitigar esta vulnerabilidad se recomienda desactivar la codificación del modo de cifrado CBC, y habilitar el modo de encriptación CTR o GCM.
- **Vulnerabilidad: SSH Weak MAC Algorithms Enabled**
  Presentada en los hosts: 186.47.XX.B y 186.47.XX.I.
  Esta debilidad indica que el servidor remoto SSH está configurado para permitir MD5 y algoritmos MAC de 96 bits, para mitigar esta vulnerabilidad se recomienda deshabilitar MD5 y algoritmos MAC de 96-bits.
- **Vulnerabilidad: SSL Certificate Chain Contains RSA Keys Less Than 2048 bits**
  Presentada en los hosts: 186.47.XX.B, 186.47.XX.D y 186.47.XX.J.
  Esta debilidad indica que la cadena de certificados X.509 utilizado para este servicio contiene los certificados con claves RSA menores que 2048 bits, para mitigar esta vulnerabilidad se recomienda aumentar la longitud de la clave del certificado y emitir el mismo nuevamente.
- **Vulnerabilidad: GNU Bash Environment Variable Handling Code Injection (Shellshock)**
  Presentada en el host: 186.47.XX.C.
  Esta debilidad indica que el servidor web remoto es afectado por una vulnerabilidad de ejecución de remota de código, para mitigar esta vulnerabilidad se recomienda aplicar el parche correspondiente al servidor.
- **Vulnerabilidad: HTTP TRACE / TRACK Methods Allowed**
  Presentes en los hosts: 186.47.XX.C y 186.47.XX.F.
  Esta debilidad indica que el servidor web tiene funciones de depuración habilitadas, para mitigar esta vulnerabilidad se recomienda deshabilitar los métodos HTTP TRACE / TRACK.

- **Vulnerabilidad: Apache Server ETag Header Information Disclosure**
  Presentada en el host: 186.47.XX.C.
  Esta debilidad indica que el servidor web remoto está afectado por una vulnerabilidad de divulgación de información, para mitigar esta vulnerabilidad se recomienda modificar el encabezado ETag HTTP del servidor web.
- **Vulnerabilidad: Vulnerability in Schannel Could Allow Remote Code Execution**
  Presentada en el host: 186.47.XX.D.
  Esta debilidad indica que el host remoto de Windows está afectado por una vulnerabilidad de ejecución de código remoto, para mitigar esta vulnerabilidad se recomienda aplicar los parches de Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, y 2012 R2, que han sido publicados por Microsoft.
- **Vulnerabilidad: Vulnerabilities in Remote Desktop Could Allow Remote Code**
  Presentada en el host: 186.47.XX.D.
  Esta debilidad indica que el host remoto de Windows está afectado por una vulnerabilidad de ejecución de código remoto, para mitigar esta vulnerabilidad se recomienda aplicar los parches de Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, y 2012 R2, que han sido publicados por Microsoft.
- **Apache Tomcat 6.0.x < 6.0.43 Multiple Vulnerabilities (POODLE)**
  Presentada en el host: 186.47.76.12.
  Esta debilidad indica que el servicio remoto Tomcat Apache está afectado por múltiples vulnerabilidades, para mitigar esto es necesario actualizar la versión del servidor a 6.0.43 o superior.
- **SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection**
  Presentada en los hosts: 186.47.XX.D, 186.47.XX.J.
  Esta debilidad indica que el servicio remoto permite renegociación insegura de conexiones TLS/SSL, para mitigar esta vulnerabilidad se recomienda contactar con el proveedor para obtener información específica del parche.

- **Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness**

  Presentada en el host: 186.47.XX.D.

  Esta debilidad indica que puede ser posible conseguir el acceso al host remoto, para mitigar esta vulnerabilidad se recomienda forzar el uso de SSL en la capa de transporte.

- **SSL Medium Strength Cipher Suites Supported**

  Presentada en el host: 186.47.XX.D.

  Esta debilidad indica que el servicio remoto es compatible con el uso de sistemas de cifrado SSL de fuerza media, para mitigar esta vulnerabilidad se recomienda reconfigurar la aplicación afectada o si es posible evitar el uso de sistemas de cifrado de fuerza media.

- **Terminal Services Encryption Level is Medium or Low**

  Presentada en el host: 186.47.XX.D.

  Esta debilidad indica que el host remoto está usando criptografía débil, para mitigar esta vulnerabilidad se recomienda cambiar el nivel de cifrado RDP a uno fuerte o compatible con FIPS.

- **Terminal Services Doesn't Use Network Level Authentication (NLA) Only**

  Presentada en el host: 186.47.XX.D.

  Esta debilidad indica que los servicios de terminal remoto no utilizan autenticación a nivel de red, para mitigar esta vulnerabilidad se recomienda usar la autenticación a nivel de red.

- **SSL Null Cipher Suites Supported**

  Presentada en el host: 186.47.XX.D.

  Esta debilidad indica que el servicio remoto es compatible con el uso de sistemas de cifrado nulos, para mitigar esta vulnerabilidad se recomienda reconfigurar la aplicación afectada para evitar el uso de cifrados nulos.

- **Terminal Services Encryption Level is not FIPS-140 Compliant**
  Presentada en el host: 186.47.XX.D.
  Esta debilidad indica que el host remoto no es compatible con FIPS-140, para mitigar esta vulnerabilidad se recomienda cambiar el nivel de encriptación RDP para que sea compatible con FIPS.
- **Browsable Web Directories**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que algunos directorios del servidor web son navegables, para mitigar esta vulnerabilidad se recomienda quitar los directorios vulnerables para que no pueda ser visto por cualquier persona.
- **Web Application Potentially Vulnerable to Clickjacking**
  Presentada en los hosts: 186.47.76.21, 186.47.76.28 y 186.47.76.29.
  Esta debilidad indica que el servidor web remoto puede fallar al momento de mitigar vulnerabilidades de aplicación web, para mitigar esta vulnerabilidad se recomienda usar opciones de X-Frame en HTTP.
- **PHP 5.5.x < 5.5.14 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.14 o superior.
- **PHP 5.5.x < 5.5.29 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.29 o superior.
- **PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para

mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.31 / 5.5.17 o superior.

- **PHP 5.5.x < 5.5.32 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.32 o superior.
- **PHP 5.5.x < 5.5.33 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.33 o superior.
- **PHP 5.5.x < 5.5.34 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.34 o superior.
- **PHP 5.5.x < 5.5.18 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.18 o superior.
- **PHP 5.5.x < 5.5.26 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.26 o superior.

- **PHP 5.5.x < 5.5.28 Multiple Vulnerabilities**

  Presentada en el host: 186.47.XX.F.

  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.28 o superior.

- **PHP 5.5.x < 5.5.30 Multiple Vulnerabilities**

  Presentada en el host: 186.47.XX.F.

  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.30 o superior.

- **PHP 5.5.x < 5.5.19 'donote' DoS**

  Presentada en el host: 186.47.XX.F.

  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por una vulnerabilidad de denegación de servicio, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.19 o superior.

- **PHP 5.5.x < 5.5.25 Multiple Vulnerabilities**

  Presentada en el host: 186.47.XX.F.

  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.25 o superior.

- **PHP 5.5.x < 5.5.22 Multiple Vulnerabilities (GHOST)**

  Presentada en el host: 186.47.XX.F.

  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.22 o superior.

- **Apache 2.4.x < 2.4.10 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 2.4.10 o superior.
- **PHP 5.5.x < 5.5.16 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.16 o superior.
- **PHP 5.5.x < 5.5.20 'process_nested_data' RCE**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por una vulnerabilidad de ejecución de código arbitrario, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.20 o superior.
- **PHP 5.5.x < 5.5.21 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.21 o superior.
- **PHP 5.5.x < 5.5.23 Multiple Vulnerabilities**
  Presentada en el host: 186.47.XX.F.
  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.23 o superior.

- **PHP 5.5.x < 5.5.24 Multiple Vulnerabilities**

  Presentada en el host: 186.47.XX.F.

  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.24 o superior.

- **PHP 5.5.x < 5.5.27 Multiple Vulnerabilities (BACKRONYM)**

  Presentada en el host: 186.47.XX.F.

  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.27 o superior.

- **PHP 5.5.x < 5.5.13 'src/cdf.c' Multiple Vulnerabilities**

  Presentada en el host: 186.47.XX.F.

  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.13 o superior.

- **Apache 2.4.x < 2.4.12 Multiple Vulnerabilities**

  Presentada en el host: 186.47.XX.F.

  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 2.4.12 o superior.

- **Apache 2.4.x < 2.4.16 Multiple Vulnerabilities**

  Presentada en el host: 186.47.XX.F.

  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 2.4.16 o superior.

- **PHP 5.5.x < 5.5.15 Multiple Vulnerabilities**

  Presentada en el host: 186.47.XX.F.

  Esta debilidad indica que el servidor web remoto está ejecutando una versión de PHP que se ve afectada por múltiples vulnerabilidades, para mitigar esta vulnerabilidad se recomienda actualizar la versión de PHP a 5.5.15 o superior.

- **SSH Weak Algorithms Supported**

  Presentada en el host: 186.47.XX.I.

  Esta debilidad indica que el servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles o ningún algoritmo, para mitigar esta vulnerabilidad se recomienda mitigar cualquier tipo de cifrado débil.

- **Unencrypted Telnet Server**

  Presentada en el host: 186.47.XX.J.

  Esta debilidad indica que el servidor Telnet transmite tráfico sin encriptar, para mitigar esta vulnerabilidad se recomienda deshabilitar el servicio telnet y usar SSH.

- **SSL Weak Cipher Suites Supported**

  Presentada en el host: 186.47.XX.J.

  Esta debilidad indica que el servicio remoto es compatible con el uso de sistema de cifrado SSL débiles, para mitigar esta vulnerabilidad se recomienda reconfigurar el sistema para evitar el uso de este tipo de cifrados.

- **SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)**

  Presentada en el host: 186.47.XX.J.

  Esta debilidad indica que el host remoto se ve afectado por una vulnerabilidad que permite a un atacante potencial des-encriptar el tráfico TLS capturado, para mitigar esta vulnerabilidad se recomienda desactivar SSL y exportar conjuntos de cifrado más fuertes.

CAPÍTULO VI

6. CONCLUSIONES Y RECOMENDACIONES

Se presentan las debidas conclusiones y recomendaciones que han dado en el desarrollo del presente proyecto.

6.1.CONCLUSIONES

- El presente proyecto nos ha permitido desarrollar un hacking ético perimetral, que es una parte de las funciones que realiza un profesional en seguridad para determinar brechas de seguridad y generar un plan de mitigación.
- Todo sistema informático es vulnerable y los sistemas de la organización evaluada en este proyecto no ha sido la excepción, es cuestión de tiempo para que personas comunes o expertos en hardware y software, con conocimientos en tecnología descubran errores y quieran vulnerar los sistemas tecnológicos. Es por esto que existe personas dedicadas a evaluar vulnerabilidades con el objetivo de evidenciar, corregir y mejorar la seguridad.
- Mediante la evaluación de la seguridad perimetral de la Organización, se detectó fallos en algunos sistemas, los mismos que posibilitaron la recopilación de la información, identificación de servicios, accesos a través de autenticación por defecto, etc. La falta de una buena administración de redes conlleva a que se puedan realizar este tipo de actividades de forma periódica y sin evidencia de bloqueo de tráfico, corte de conexión o alguna respuesta de acción inmediata.
- El presente proyecto ha girado en torno a un ambiente real, en el que se puede evidenciar que existen errores considerables en relación a la administración de la red, como es el uso de contraseñas por defecto, falta de monitoreo para evidenciar actividades sospechosas, falta de actualización en servicios web, tiempos de respuesta elevados para eventos sospechosos, etc.
- El gran número de herramientas utilizadas como nmap, fierce, google hacking, netcraf, whois, entre otras, han permitido obtener información

relevante de la organización, aun tomando en cuenta que no conocíamos nada sobre nuestra empresa evaluada, hemos recopilado información que permite familiarizarnos con la misma.

- Las reglas de operación para la implementación de pruebas de penetración se han establecido en conjunto con el personal encargado de la seguridad dentro de la organización evaluada, de esta manera el equipo de hacking ético pudo trabajar en función de alcances y objetivos claros.
- Las prácticas de hacking ético permitieron medir el nivel de seguridad de la empresa frente a ataques reales, aprovecharnos de los errores o las brechas de seguridad y presentar planes de mitigación, pero al ser un aspecto cambiante es importante realizar las pruebas en períodos de tiempo definitivos y no muy prolongados, con el fin de mantener actualizados los sistemas en cuanto a seguridad.
- Una de las desventajas de usar un escáner de vulnerabilidades es que son muy ruidosos y por lo tanto muy fáciles de detectar debido a la gran cantidad de tráfico que se origina, en el proyecto se puedo notar que no existe ningún tipo de control o monitoreo debido a que no se detectaron las pruebas realizadas, por lo cual hemos aprovechado el fallo para efectuar varias veces las mismas pruebas.
- La utilización de metodologías como OSSTMM, ISSAF, OWASP, es muy importante para llevar a cabo una actividad como la que presentamos en este proyecto, sin embargo, para el desarrollo del mismo también nos hemos guiado en los pasos que siguen los diferentes autores de libros citados. Todo esto permite llevar un orden tanto en la ejecución de procesos como en la documentación obtenida.
- Nessus ha resultado ser una de las herramientas más robustas e importantes dentro del análisis, a pesar de ser similar a OpenVAS. Los resultados que presenta son más precisos, el inconveniente es que tiene una licencia de pago, sin embargo su utilización como versión de prueba ha permitido evaluar nuestro habiente real.

6.2.RECOMENDACIONES

- Es importante que los administradores de red mantengan actualizados sus conocimientos de esta forma pueden detectar o tomar medidas contra nuevas vulnerabilidades, además, deben verificar nuevos parches, versiones, licencias, etc., de cada sistema operativo, servicio o protocolo.
- Es importante verificar los datos que se publican de una Organización, de esta forma se puede evitar que los cibercriminales obtengan ventaja para explotar brechas de seguridad de los sistemas y generar accesos no autorizados a los activos.
- Se recomienda la realización de análisis de vulnerabilidades con periodos de 6 meses o un año de diferencia, a través de internet, con el objetivo de simular ataques controlados y verificar los tiempos de respuesta y los mecanismos de mitigación existentes para contra-restar este tipo de eventos en caso de producirse realmente.
- Se recomienda adquirir, en caso de no tener, equipos de seguridad perimetral, como son IDS, IPS, Firewall, etc., para proteger los servicios y los sistemas de la organización, de posibles ataques como denegación de servicio, ataque por fuerza bruta, tráfico sospechoso a través de consultas; en caso de contar con los equipos de seguridad perimetral, se recomienda tenerlos actualizados con las últimas versiones liberadas por los fabricantes, al igual que mantener la configuración con las mejores prácticas establecidas por los proveedores.
- En caso de instalar productos de prueba o soluciones de evaluación, recomendamos realizar las configuraciones de seguridad suficientes, para que no se convierta en una brecha de seguridad, como son: versiones actualizadas, contraseñas robustas, y de ser el caso que sea público a internet, colocarlo en una DMZ. De esta manera se evita un posible fallo de seguridad que a futuro se vuelva el puente para vulnerar otros sistemas.

- Las herramientas usadas en el presente proyecto, son fáciles de configurar e instalar, lo necesario es conocer cuáles son los resultados que deseamos obtener con cada una, para un mejor entendimiento.
- El uso de diferentes herramientas para un mismo propósito ayuda a descartar información que no es relevante.
- Es importante que los administradores de redes tengan conocimientos de hacking ético, para poder realizar pruebas de seguridad y de esta forma poder evitar ataques predecibles.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS Y MANUALES

[1] Jara, H., y Pacheco, F. G. (2012). Ethical hacking 2.0. (1a ed.). Buenos Aires: Fox Andina

[2] Allen, L. (2012). Advanced Penetration Testing for Highly-Secured Environments: The Utimate Security Guide. Birmingham: Packt Publishing.

[3] Baloch, R. (2015). ETHICAL HACKING AND PENETRATION TESTING GUIDE. London: Taylor & Francis Group.

[4] Beggs, R. W. (2014). Mastering Kali Linux for Advanced Penetration Testing. Birmingham: Packt Publishing.

[5] Caballero, A. (2015). Hacking con Kali Linux curso Virtual, Versión 2.5. Recuperado de: http://www.reydes.com/d/?q=node/2.

[6] Offensive Security, Penetration Testing with BackTrack, PWB Online Lab Guide.

[7] Astudillo, K. (2013). Hacking Ético 101-Cómo hackear profesionalmente en 21 días o menos. Guayaquil: el autor.

[8] Tori, C. (2008). Hacking Ético. Rosario: el autor.

[9] OSSTMM 3 Open Source Security Testing Methodology Manual, Contemporary Security Testing and analysis. Created by Pete Herzog, developed by ISECOM.

[10] OISSG (Open Information Systems Security Group), Infomation Systems Security Assessment Framework (ISSAF) Draft 0.2.1, Date: April 30, 2006

[11] OWASP Open Web Application Security Project, testing Guide 4.0, 2014 The OWASP Foundation

DIRECCIONES ELECTRÓNICAS

[12] Secure-IT, *Introducción al hacking ethico* [en linea]. [fecha de consulta: 07 Noviembre 2016]. Disponible en: <https://securitcrs.wordpress.com/hacking/terminologia-esencial/>

[13] Jorge Mieres, *Certified Ethical Hacker Review Guide* [en Linea]. Octubre 2012, [fecha de consulta 07 Noviembre 2016]. Disponible en: <http://www.it-docs.net/ddata/863.pdf>

[14] Alejandro Reyes Plata, *Ethical Hacking* [en linea]. [fecha de consulta 07 Noviembre 2016]. Disponible en: <http://www.seguridad.unam.mx/descarga.dsc?arch=2776>

[15] https://securitcrs.wordpress.com/hacking/terminologia-esencial/ [fecha de consulta 07 Nobiembre 2016].

ANEXOS

ANEXO A: Carta de Autorización

CARTA DE AUTORIZACIÓN

A QUIEN LE INTERESE,

Acorde al Memorando Nro. MTOP-CGAD-2015-57-ME, la Dirección de Tecnologías de la Información del Ministerio [redacted], autoriza a Luis Alcides Mendaño y María Elena Hurtado, a realizar Pruebas de Penetración basadas en técnicas de Hacking Ético, siempre y cuando las personas mencionadas se encarguen de precautelar la infraestructura de red e información obtenida de este análisis, garantizando que la información sea usada únicamente con fines educativos y los resultados en caso de ser publicados no contendrán la información que ponga en riesgo la infraestructura de la Institución.

Una vez realizado el análisis, el reporte será entregado a la Dirección de Tecnologías de la Información, quien se encargará de revisar que se cumpla con lo antes mencionado.

Ing. Paulina Lastra Valverde
Directora de Tecnologías de la Información

ANEXO B: Acuerdo de Confidencialidad y no divulgación de la Información

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN

En Quito a los 7 días del mes de Diciembre del 2015.

Por una parte comparece el MINISTERIO [redacted], con domicilio, en la ciudad de QUITO, representada en este acto por la Ing. Paulina Lastra, en su calidad de Directora de Tecnologías de la Información, en adelante [redacted] y por otra parte, el señor Luis Mendaño y la señora María Elena Hurtado, en adelante ANALISTAS.

EXPONEN

Que ambas partes se reconocen capacidad jurídica suficiente para suscribir el presente documento.

Que para proteger adecuadamente los activos de tecnología de la información del Ministerio [redacted] se requiere de una persona que evalúe los sistemas de seguridad mediante la realización de evaluaciones de vulnerabilidad y pruebas de penetración. Estas actividades implican escanear equipos informáticos propiedad del Ministerio de una forma regular y periódica para descubrir las vulnerabilidades presentes en estos sistemas, solo con el conocimiento de estas vulnerabilidades se podrá aplicar parches de seguridad u otros controles de compensación para mejorar la seguridad de la organización.

Que durante la mencionada relación las partes intercambiarán o crearán información que están interesadas en regular su confidencialidad y secreto, en base a las siguientes ESTIPULACIONES:

CONDICIONES

PRIMERA.- Objetivo. Con el presente contrato, las partes fijan formalmente y por escrito los términos y condiciones bajo las que las partes mantendrán la confidencialidad de la información suministrada y creada entre ellas.

Que a los efectos de este acuerdo, tendrá la consideración de información confidencial, toda la información susceptible a ser revelada por escrito, de palabra

o cualquier otro medio tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro, intercambiada como consecuencia de este acuerdo.

SEGUNDA.- Las partes se obligan a entregarse todo el material que sea necesario, y en el caso de ser este confidencial se comprometen a:

a. Utilizar dicha información de forma reservada.
b. No divulgar ni comunicar la información técnica facilitada por la otra parte.
c. Impedir la copia o revelación de esa información a terceros, salvo que gocen de aprobación escrita de la otra parte, y únicamente en términos de tal aprobación.
d. Restringir el acceso a la información a sus empleados y subcontratados, en la medida en que razonablemente puedan necesitarla para el cumplimiento de sus tareas acordadas.
e. No utilizar la información o fragmentos de ésta para fines que no sean educativos.

Las partes serán responsables entre sí, ante el incumplimiento de esta obligación, ya sea por sus empleados o por subcontratados.

Las partes mantendrán ésta confidencialidad y evitarán revelar la información a toda persona que no sea empleado o subcontratado, salvo que:

a. La parte receptora tenga evidencia de que conoce previamente la información recibida.
b. La información recibida sea de dominio público.
c. La información recibida proceda de un tercero que no exige secreto.

TERCERA.- Las partes se obligan a devolver cualquier documentación, antecedente facilitado en cualquier tipo de soporte y, en su caso, las copias obtenidas de los mismos, que constituyan información amparada por el deber de confidencialidad objeto del presente Acuerdo en el supuesto de que cese la relación entre las partes por cualquier motivo

CUARTA.- El presente Acuerdo entrará en vigor en el momento de la firma del mismo por ambas partes, extendiéndose su vigencia hasta un plazo de 4 meses después de finalizada la relación entre las partes.

QUINTA.- Las partes acuerdan que este acuerdo reviste el carácter de confidencial y por tanto se prohíbe su divulgación a terceros.

Y en señal de expresa conformidad y aceptación de los términos recogidos en el presente Acuerdo, lo firman las partes por duplicado ejemplar y a un solo efecto en el lugar y fecha al comienzo indicados.

POR EL [redacted]

Ing. Paulina Lastra.

POR LOS ANALISTAS

María Elena Hurtado

Luis Alcides Mendaño

ANEXO C: Reporte de OpenVAS

Scan Report

May 15, 2016

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "186.47.[redacted]". The scan started at Wed May 11 11:27:51 2016 UTC and ended at Wed May 11 11:49:13 2016 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
186.47.	0	1	2	9	0
Total: 1	0	1	2	9	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.

This report contains all 12 results selected by the filtering described above. Before filtering there were 24 results.

2 Results per Host

2.1 186.47.

Host scan start	Wed May 11 11:28:48 2016 UTC
Host scan end	Wed May 11 11:49:13 2016 UTC

Service (Port)	Threat Level
22/tcp	Medium
22/tcp	Low
general/tcp	Low
22/tcp	Log
general/tcp	Log
general/CPE-T	Log
5901/tcp	Log

2.1.1 Medium 22/tcp

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result
`The following weak client-to-server encryption algorithms are supported by the r`

. . . continues on next page . . .

... continued from previous page ...

```
↪emote service:
rijndael-cbc@lysator.liu.se
cast128-cbc
aes256-cbc
arcfour
arcfour256
aes192-cbc
blowfish-cbc
aes128-cbc
arcfour128
3des-cbc
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
rijndael-cbc@lysator.liu.se
cast128-cbc
aes256-cbc
arcfour
arcfour256
aes192-cbc
blowfish-cbc
aes128-cbc
arcfour128
3des-cbc
```

Solution
Disable the weak encryption algorithms.

Vulnerability Insight
The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Check if remote ssh service supports Arcfour, none or CBC ciphers.
Details:`SSH Weak Encryption Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `$Revision: 3160 $`

References
`Other:`
`URL:https://tools.ietf.org/html/rfc4253#section-6.3`
`URL:https://www.kb.cert.org/vuls/id/958563`

[return to 186.47.76.27]

2.1.2 Low 22/tcp

Low (CVSS: 2.6) NVT: SSH Weak MAC Algorithms Supported
Summary The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Vulnerability Detection Result
`The following weak client-to-server MAC algorithms are supported by the remote s`
`↪ervice:`
`hmac-md5-96`
`hmac-md5`
`hmac-sha1-96`
`The following weak server-to-client MAC algorithms are supported by the remote s`
`↪ervice:`
`hmac-md5-96`
`hmac-md5`
`hmac-sha1-96`

Solution Disable the weak MAC algorithms.
Vulnerability Detection Method Details:`SSH Weak MAC Algorithms Supported` OID:1.3.6.1.4.1.25623.1.0.105610 Version used: `$Revision: 3157 $`

[return to 186.47.76.27]

2.1.3 Low general/tcp

Low (CVSS: 2.6) NVT: TCP timestamps
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
`It was detected that the host implements RFC1323.`
`The following timestamps were retrieved with a delay of 1 seconds in-between:`
`Paket 1: 679283784`
`Paket 2: 679284883`

Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.

. . . continues on next page . . .

... continued from previous page ...

Solution

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details:`TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 787 $`

References
`Other:`
`URL:http://www.ietf.org/rfc/rfc1323.txt`

[return to 186.47.76.27]

2.1.4 Log 22/tcp

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

Summary
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result
```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
```

Log Method
Details:`SSH Protocol Versions Supported`

... continues on next page ...

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.100259
Version used: $Revision: 2817 $

Log (CVSS: 0.0)
NVT: SSH Server type and version

Summary
This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result

```
Detected SSH server version: SSH-2.0-OpenSSH_5.3
Remote SSH supported authentication: password,publickey
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:5.3
Concluded from remote connection attempt with credentials:
  Login: OpenVAS
  Password: OpenVAS
```

Log Method
Details:SSH Server type and version
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: $Revision: 2902 $

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
An ssh server is running on this port
```

Log Method
Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 3210 $

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result

```
The following options are supported by the remote ssh service:
kex_algorithms:
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-h
↪ellman-group14-sha1,diffie-hellman-group1-sha1
server_host_key_algorithms:
ssh-rsa,ssh-dss
encryption_algorithms_client_to_server:
aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowf
↪ish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client:
aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowf
↪ish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
mac_algorithms_client_to_server:
hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd16
↪0,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
mac_algorithms_server_to_client:
hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd16
↪0,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Log Method
Details:`SSH Protocol Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: `$Revision: 2828 $`

[return to 186.47.76.27]

2.1.5 Log general/tcp

Log (CVSS: 7.8)
NVT: 3com switch2hub

Summary
The remote host is subject to the switch to hub flood attack.

. . . continues on next page . . .

... continued from previous page ...

Description : The remote host on the local network seems to be connected through a switch which can be turned into a hub when flooded by different mac addresses. The theory is to send a lot of packets (¿ 1000000) to the port of the switch we are connected to, with random mac addresses. This turns the switch into learning mode, where traffic goes everywhere. An attacker may use this flaw in the remote switch to sniff data going to this host
Reference : http://www.securitybugware.org/Other/2041.html

Vulnerability Detection Result
`Fake IP address not specified. Skipping this check.`

Solution
Lock Mac addresses on each port of the remote switch or buy newer switch.

Vulnerability Detection Method
Details:`3com switch2hub`
OID:1.3.6.1.4.1.25623.1.0.80103
Version used: `$Revision: 3208 $`

Log (CVSS: 0.0)
NVT: arachni (NASL wrapper)

Summary
This plugin uses arachni ruby command line to find web security issues.
See the preferences section for arachni options.
Note that OpenVAS is using limited set of arachni options. Therefore, for more complete web assessment, you should use standalone arachni tool for deeper/customized checks.

Vulnerability Detection Result
```
Arachni could not be found in your system path.
OpenVAS was unable to execute Arachni and to perform the scan you
requested.
Please make sure that Arachni is installed and that arachni is
available in the PATH variable defined for your environment.
```

Log Method
Details:`arachni (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.110001
Version used: `$Revision: 3117 $`

Log (CVSS: 0.0)
NVT: Traceroute

Summary

... continues on next page ...

... continued from previous page ...

A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 192.168.1.5 to 186.47.[redacted]:
192.168.1.5
186.42.168.18
186.42.168.17
186.46.4.70
186.46.4.126
192.168.211.1
192.168.211.2
186.47.[redacted]
186.47.[redacted]
```

Solution

Block unwanted packets from escaping your network.

Log Method

Details:Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 2837 $

[return to 186.47.76.27]

2.1.6 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary

This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result

```
186.47.[redacted]|cpe:/a:openbsd:openssh:5.3
```

Log Method

Details:CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 2837 $

[return to 186.47.76.27]

2.1.7 Log 5901/tcp

Log (CVSS: 0.0) NVT: VNC security types
Summary This script checks the remote VNC protocol version and the available 'security types'.

Vulnerability Detection Result
`The remote VNC server supports those security types:`
`+ 2 (VNC authentication)`

Log Method Details:`VNC security types` OID:1.3.6.1.4.1.25623.1.0.19288 Version used: `$Revision: 1318 $`

[return to 186.47.76.27]

ANEXO D: Reporte de Nessus

Nessus Report

Nessus Scan Report

Mon, 09 May 2016 14:05:47 GMT-0500

Table Of Contents

Vulnerabilities By Host

186.47.76.29

Scan Information

Start time: Mon May 09 14:05:47 2016

End time: Mon May 09 14:25:31 2016

Host Information

DNS Name: 29.pichincha.andinanet.net

IP: 186.47.[redacted]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	13	14

Results Details

0/tcp

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the FQDN of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2012/09/28

Ports

tcp/0

```
186.47.[redacted] resolves as 29.pichincha.andinanet.net.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

46215 - Inconsistent Hostname and IP Address

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

The name of this machine either does not resolve or resolves to a different IP address.
This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.
As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information:

Publication date: 2010/05/03, Modification date: 2015/06/02

Ports

tcp/0

```
The host name '29.pichincha.andinanet.net' does not resolve to an IP address
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2016/04/08

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.6.2
Plugin feed version : 201605051230
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.2.57
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
```

```
Web application tests : enabled
Web app tests -  Test mode : some_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2016/5/9 14:05
Scan duration : 1180 sec
```

0/udp

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2015/07/01

Ports

udp/0

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

```
For your information, here is the traceroute from 192.168.2.57 to 186.47.[redacted] :
192.168.2.57
?
192.168.1.1
186.33.166.73
?
10.201.232.5
10.201.21.18
10.201.211.237
10.201.211.238
10.201.111.149
10.201.111.62
```

```
10.201.111.53
200.110.120.4
190.152.252.178
186.46.4.6
186.46.4.185
186.46.4.70
186.46.4.126
186.46.4.126
186.47.[redacted]
186.47.[redacted]
```

80/tcp

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.
X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.
Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.
Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

http://en.wikipedia.org/wiki/Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF CWE:693

Plugin Information:

Publication date: 2015/08/22, Modification date: 2016/04/14

Ports

tcp/80

```
The following pages do not use a Clickjacking mitigation response header and contain a clickable
 event :

  - http://186.47.[redacted]/doc/page/login.asp
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

Ports

tcp/80

```
A web server is running on this port.
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.
The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

http://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/80

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:
```

```
  - http://186.47.[redacted]/doc/page/login.asp
  - http://186.47.[redacted]/index.asp
```

50344 - Missing or Permissive Content-Security-Policy HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.
The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a properly configured Content-Security-Policy header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/80

```
The following pages do not set a Content-Security-Policy response header or set a permissive
 policy:

  - http://186.47.[redacted]/doc/page/login.asp
  - http://186.47.[redacted]/index.asp
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/80

```
The remote web server type is :

Hikvision-Webs
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/80

```
Based on tests of each method :

  - HTTP methods DELETE GET HEAD POST are allowed on :

    /doc/page

  - HTTP methods DELETE GET HEAD POST PUT are allowed on :

    /
    /doc
    /doc/css
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/80

```
Protocol version : HTTP/1.0
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: Hikvision-Webs
  Date: Mon May  9 14:18:20 2016
  Pragma: no-cache
  Cache-Control: no-cache
  Content-Type: text/html
  Location: http://29.pichincha.andinanet.net/index.asp
```

ANEXO E: Plan de Explotación

PLAN DE ATAQUES

Con el fin de probar la seguridad perimetral de la red Institucional, se realizarán pruebas de explotación que no comprometan la disponibilidad de los servicios e información confidencial. Las mismas serán realizadas sin ningún cronograma específico para validar la administración y monitoreo de los sistemas.

Con este antecedente, queda prohibido realizar pruebas del tipo:

- De denegación de servicios.
- Inyección de códigos que puedan causar desbordamiento de buffer.
- Uso de exploits o scripts para explotar una vulnerabilidad, debido a que los mismos pueden comprometer la disponibilidad de los sistemas y servicios.

Se autoriza a Luis Alcides Mendaño y María Elena Hurtado, a realizar explotación de vulnerabilidades tipo:

- Escaneo de directorios web.
- Explotación de usuarios y contraseñas por defecto.
- Transmisión Vulnerable de Credenciales en una Aplicación Web.
- Ataques de autenticación por fuerza bruta.
- Autenticación web básica
- Servicio web sin método de autenticación.
- Clickjacking
- Procedimiento de uso de un exploit para explotar una vulnerabilidad

Ing. Paulina Lastra Valverde

Directora de Tecnologías de la Información