ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE SISTEMAS

APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES DE LA RED INALÁMBRICA DE UNA INSTITUCIÓN

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

JÉSSICA ELIZABETH MORALES BONILLA
jelita_8891@yahoo.es

Directora: MSc. Ing. Gabriela Suntaxi
gabriela.suntaxi@gmail.com

Quito, Julio 2015

DECLARACIÓN

Yo, Jéssica Elizabeth Morales Bonilla, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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

Jéssica Elizabeth Morales Bonilla

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Jéssica Elizabeth Morales Bonilla bajo mi supervisión.

GABRIELA SUNTAXI

DIRECTORA

AGRADECIMIENTOS

A mí papi y mami! Luis Humberto, Susana, mis hermanos y hermanas Fernando, Cristian, Betito, Nayeli y Alison que sin ellos no estaría aquí para contarlo. Mis primas, primos, tías y tíos que con su apoyo, hoy es un fruto de todo nuestro ayllu.

No me dejé por las adversidades, fui con miedo, fui desconociendo el camino, fui lento pero fui; estuve ahí, me caí y continué caminando.

En mi historia, mi camino, mi pena, mi dolor, mi amor, mi trabajo, mi yo, estuvieron mujeres y hombres imperfectos de los cuales aprendí y son hoy mi motor de vida y fuente de inspiración, mis familiares, amigos, amigas y ese feo.

Estoy felizmente agradecida a la vida (Pachamama) por tenerme en tus barrios rondando, cantando mis ideas sin-vergüenzas, saltando de aquí y allá, y permitirme abrazar con todo mi yo al encanto de la magia presente en la vida.

Y otra vez gracias a la vida, a mi familia por haberme dado la oportunidad de marcar mi camino, mi nombre, con este trabajo en la poli y en la facultad que amo. Este es uno de los otros trabajos que quiero compartir y serán más los que vendrán como runa luchadora de Cotacachi, que marca camino!

“Ñami runakuna rikcharinashpa, ñukanchik kawsayta sinchiyachina kanchik.
Cuando no sabíamos escribir, escribieron por nosotros.
Cuando no sabíamos leer, leyeron por nosotros.
Cuando no sabíamos hablar la lengua del opresor, hablaban por nosotros.
Ahora que sabemos leer, escribir y hablar la lengua del opresor, es hora de contar nuestras propias historias.”
YACHAKWAYRA
Runa, kichwa, Otavalo.

DEDICATORIA

Este trabajo dedico a toda los RUNAs que con ese ñeque luchamos porque la educación de nuestro país este completa desde la cosmovisión RUNA, aquellos RUNAs donde les corre por la sangre el amor a la Pachamama y nos despertamos disfrutando de sus bondades y compartimos en ayllu.

A nuestros taitas y mamas que con su sabiduría y lucha se han mantenido en pie y hoy les digo, como persona en mi posición privilegiada de la educación no permitiré que muera nuestra historia ni el sentido de compartir con amor con los demás.

“La vida no es sólo recibir, es dar.
Por muy jodido que estés siempre tienes algo para dar.
*-**José Mujica**”*

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

El propósito del presente proyecto de titulación es aplicar un procedimiento formal y controlado de hacking ético a la red inalámbrica de una institución, con el objetivo de identificar qué posibles amenazas, vulnerabilidades y riesgos generan un impacto negativo al negocio.

Para formar el procedimiento de hacking ético para la red inalámbrica, se ha utilizado como framework las metodologías correspondientes para la evaluación de la red inalámbrica: OSSTMM Wireless (Wireless Security Testing Section Open-Source Security Testing Methodology Manual) versión 2.9.1 y 3, ISSAF draft 0.2 (Manual Information System Security Assessment Framework y OWISAM (Open Wireless Security Assessment Methodology) aplicándolas a la institución.

Con la utilización de herramientas de software libre como resultado se presentará un plan de mitigación a la alta dirección junto al administrador de la red.

Este documento está dividido en cuatro capítulos:

El CAPÍTULO 1 explica las hipótesis iniciales de los problemas encontrados en la institución, se selecciona y forma el procedimiento formal de hacking ético que permite realizar la evaluación de riesgos de la red inalámbrica, utilizando software libre.

El CAPÍTULO 2 describe el Análisis de la Evaluación de Riesgos. Se empieza con la aplicación de pruebas intrusivas y no intrusivas, lo que permitirá la búsqueda de amenazas, vulnerabilidades y riesgos presentes. Todo este procedimiento se llevará a acabo de acuerdo a los lineamientos propuestos por la metodología ISSAF y complementándola por las metodologías OSSTMM y OWISAM.

El CAPÍTULO 3 detalla el plan de mitigación y el análisis de qué tan factible es la propuesta presentada por la autora. La planificación y presentación de resultados para la alta dirección y al administrador de la red de la institución. Dentro de las recomendaciones técnicas se toma como referencia los lineamientos sugeridos por las metodologías ISSAF, norma NTE INEN-ISO/IEC 27002 y OWISAM versión 3.

En el CAPÍTULO 4 se concluye finalmente este proyecto de titulación estableciendo las conclusiones y recomendaciones, en base a la experiencia al trabajo realizado.

YACHANAMI KANCHIK

Ñukami shinakuni shuk alli proyectuta kai yachakui tukuchimanta tesista rurakuni kai red inalambricamanta, ama imallakipi urmanakunkapa, shinamanta shuk maskarikina ama tiachun, shinaka ama shuk empresa ukukunawan amalla watarichun.

Kaitami sumak yachana rurayjuni. Kai killka katishpa tarishkani hacking etico red inalambrica metodologiasta kuni OSSTMM Wireless (Wireless Security Testing Section Open-Source Security Testing Methodology Manual) versión 2.9.1 y 3, ISSAF draft 0.2 (Manual Information System Security Assessment Framework y OWISAM (Open Wireless Security Assessment Methodology)

Kai yachaykuna tiachun rikuni chusku kike:

SHUK NIKI, ñuka shinakuni imatalla ñaupaman apanata muskurin shuk institucion, shinallata mashani imañan alli rurarichun hacking eticota, chai yachay programas librekuna rurarichun.

ISHKAI NIKI, ama imallakikuna rikurichun yahaikunata mascashkani tukui red inalambrica, chai yachay ruraikuna ama shuk, shuk llakikuni yaikuchun, ama rikurichun. Kai llankaita shinakupi.
Chai proyectokuna shinarichun charinchi kimsa metodologias OSSTMM Wireless (Wireless Security Testing Section Open-Source Security Testing Methodology Manual) versión 2.9.1 y 3, ISSAF draft 0.2 (Manual Information System Security

Assessment Framework y OWISAM (Open Wireless Security Assessment Methodology).

KIMSA NIKI, ai tukui proyecto ruraruchun ñika yuyaita churani plan mitigación tukui ñawpana apak apukuna (administrador de la red, alta dirección) aki ñawpaman katichun kai tukui proyecto. Kai tukui yuyaikuna paktachun charin ishkai normas NTE INEN-ISO/IEC 27002 y OWISAM versión 3.

CHUSKU NIKI, kaipi tukuchinkapa ñuka rikuchikrini tauka paktachikuna, llakikuna, paktachina sumak ñawpaman katichun kai seguridad de la red inalambrica.

INTRODUCCIÓN

La mayoría de vulnerabilidades encontradas no se refiere en si al mal funcionamiento de equipos tecnológicos sino a la incorrecta configuración de los dispositivos inalámbricos. Actividades como no contar con políticas donde se explique el buen uso/manejo de dispositivos y la red inalámbrica o sobre la configuración del dispositivo inalámbrico, indican que existe un cierto desconocimiento del personal interno de la institución en cuanto a seguridad informática y los riesgos que en la red inalámbrica pueden estar expuestos al no contar con estos reglamentos.

Cada día aparecen noticias y publicaciones en la web sobre las nuevas vulnerabilidades en la red inalámbrica, que logran los hackers encontrar. Toda la institución que presta servicios y que cuenta con una alta cantidad de clientes, tiene como responsabilidad social y profesional asegurar que su información no sea manipulada por personal que no esté autorizado.

Para dar un acercamiento y concientización al personal de la institución sobre la seguridad de la red inalámbrica la autora ha propuesto un taller práctico de hacking ético con lineamientos basados en la metodología ISSAF draft 0.2 donde se presenta los riesgos encontrados en el caso de estudio y un plan para mitigarlos. Toda esta experiencia está documentada en este proyecto de titulación y ha sido presentada a la alta dirección de la institución y administrador de la red para que se tomen las medidas que consideren necesarias.

CAPÍTULO 1.

1. PLANTEAMIENTO DEL PROBLEMA

La seguridad de la información de cualquier persona o institución no solo protegiendo físicamente los equipos tecnológicos es suficiente, sino que, además es necesario crear un ambiente planificado donde permita analizar si el personal técnico y administrativo está preparado para reaccionar ante posibles situaciones de que pasaría si ocurre alguna falla en el sistema o robo de información no solo por un hacker sino de un usuario interno de la red.

El capítulo 1 define las hipótesis de problemas encontrados en la institución, la selección y justificación de las metodologías OSSTMM[1], ISSAF[2] y OWISAM[3] esto va a permitir definir un procedimiento de hacking ético para la evaluación de riesgos de la red inalámbrica.
Además de la selección y justificación de las herramientas de software libre a ser utilizadas, sujetas a los requerimientos encontrados.

---

[1] OSSTMM, Open Source Security Testing Methodology Manual, (Manual de la Metodología Abierta de Testeo de Seguridad)

[2] ISSAF, Information System Security Assessment Framework, (Marco de Evaluación de Seguridad de Sistemas de Información)

3 OWISAM, Open Wireless Security Assessment Methodology, (Metodología de evaluación de seguridad wireless abierta),

1.1DEFINICIÓN DEL PROBLEMA

El escenario para el ejercicio de hacking ético con fines académicos propuesto, se aplicará en la red inalámbrica de una empresa dedicada a la venta de cerámicas y porcelanato tanto nacional como internacionalmente. Para hacer referencia a la empresa, utilizaremos el término “la institución” dentro del presente proyecto, por temas de confidencialidad.

1.1.1 CARACTERIZACIÓN DE LA RED DE LA INSTITUCIÓN[l]

La institución cuenta con 4 sedes en Ambato, Cuenca y Quito Guayaquil. La sede principal está ubicada en Cuenca, cuenta con 3 proveedores de datos e internet, PuntoNet, Movistar y CNT (Corporación Nacional de Telecomunicaciones) respectivamente.

El caso de estudio se realizará a la sede ubicada en Quito, que cuenta con 6 sucursales de las cuales para el caso de se analizarán en 3 sucursales. Su infraestructura de red diseñada, provee a sus usuarios servicios de comunicaciones e interacción de aplicaciones propios para la organización.

A continuación se detalla las características que tiene esta infraestructura de red:

1.1.1.1 Usuarios

Aproximadamente a la red de la institución acceden 100 usuarios internos, entre ellos diariamente acceden a la red inalámbrica alrededor de 25 a 30 usuarios; el personal es de tipo: administrativo, ventas y clientes.

1.1.1.2 Servicios y Aplicaciones

Los servicios que acceden a través de la red inalámbrica son: Internet, Correo Electrónico empresarial y JD EDWARDS ENTERPRISEONE.

JD EDWARDS ENTERPRISEONE es un ERP (Enterprise resource planning) Sistema de Planificación de Recursos Empresariales, donde acceden los usuarios para realizar operaciones financieras, inventario, ventas, seguimiento de pedidos, facturación, adquisición, manufactura, reportes entre otros.

Las aplicaciones web que acceden a través de la red inalámbrica son:

- Portal del Ministerio de Relaciones Laborales

- IESS
- SRI
- Bancos
- Correo personal
- Facturación electrónica
- Red socio empleo y Salarios, Utilidades
- Sistema de Actas de Finiquito
- Sistemas de Contratación.

1.1.1.3 IT, Comunicaciones y demás equipamiento

En la Tabla 1-1 [m] describe los equipos y dispositivos de la infraestructura de red de la institución tanto de la red alámbrica como la inalámbrica en la cual ha sido clasificada en equipos de cliente y equipos de red:

Equipos de los Clientes				
Cantidad	**Activo**	**Características**	**Funcionalidades**	**Observaciones**
67	Ordenadores	N/A	Terminales fijos con acceso a la red cableada	Computadores de escritorio
30	Portátiles	N/A	Para la capa de acceso, terminales móviles que pueden tener acceso tanto para la red cableada como la red inalámbrica.	
8	Impresoras		Dispositivo de salida de información que nos permite visualizar la información mediante la impresión de documentos.	No cuentan con impresoras inalámbricas
7	Lectores biométricos	N/A	Forma de control de acceso al personal que labora en la institución, para registrar la hora de entrada y salida a las instalaciones.	No funcionan actualmente
10	Dispositivos móviles		Permite la comunicación interna entre el personal administrativo para objetivos de negocio.	Teléfonos empresariales

Equipos de la Red				
Cantidad	**Activo**	**Modelos**	**Funcionalidades**	**Observaciones**
1	Microtick	RouterBoard RB750GL	Este dispositivo está en la capa Core del modelo jerárquico de la red	
0	Servidores / Firewall	N/A	N/A	No cuentan con un dispositivo Firewall o servidores en la sede de Quito.
3	Switches	Conmutador 3Com Baseline Switch 2016/2024 “un dispositivo no administrado versátil y de uso simple...No necesita configuración alguna, el modo dúplex del equipo conectado y brinda una conexión conmutada adecuada.”[4]	Para la capa de distribución del modelo jerárquico de red	

[4] Fuente: http://bizsupport2.austin.hp.com/docs/support/SupportManual/c02581578/c02581578.pdf, último acceso: 14/02/2015].

Equipos de la Red				
7	DVR	La mayoría tiene esta marca Dvr Hikvision Turbo Hd 8 Canales 720p. "HIKvision, DVR Turbo HD-TVI 8CH, H.264, Soporta cámaras análogas multimarca y cámaras turbo HD propias, full channel @ 720P, grabación en tiempo real, HDMI, VGA, full 720P, salida Iphone y android"[5]	Este dispositivo almacena video en un disco duro que proviene de una o varias cámaras de video por seguridad física y del personal dentro de la institución	Ubicados en cada sucursal.
0	Antenas	N/A	Difundir ondas radioeléctricas.	No cuentan con antenas
0	Tarjeta de red inalámbrica	N/A	Permite compartir recursos entre 2 o más computadoras inalámbricamente	No cuentan con tarjetas de red inalámbricas.

[5] Fuente: http://recursos-tecnologicos.com/dvr/135-dvr-turbo-hd-8-canales-hikvision-720p-alta-definicion.html, último acceso: 22/02/2015

Equipos de la Red				
5	Router	Marca: Belkin, D-Link, TP-LINK 11N provenientes de un proveedor externo.	Interconectar redes inalámbricas y proveerlas de internet.	Había como mínimo un router o Access point en cada una de las sucursales.
3	Access point	Marca: HOME GATEWAY para Access points de CNT.	Dependiendo la configuración acceden a la red usuarios autorizados.	

Tabla 1-1 Activos de la red de la institución[6]

[6] Elaborado por: La autora en base a la información obtenida de la institución

La institución tiene servidores y firewall ubicados en Ambato, el análisis de dichos dispositivos no se encuentran en el alcance del proyecto de titulación presentado. El análisis propuesto para este proyecto de titulación corresponde a los dispositivos pertenecientes a la red inalámbrica ubicados en la sede Quito.

1.1.1.4 Esquema de red

Como se puede ver en la Figura 1-1 la infraestructura de la red de la institución, posee una topología estrella; cuentan con dos tipos de medios de transmisión: para el cableado horizontal utilizan cable UTP Categoría 6A y para el cableado vertical utilizan Fibra Óptica (enlace de datos de CNT).

Como mecanismo de autenticación a la red inalámbrica en su mayoría es WPA 2 Personal y Enterprise, pero existen otros dispositivos configurados con WEP.

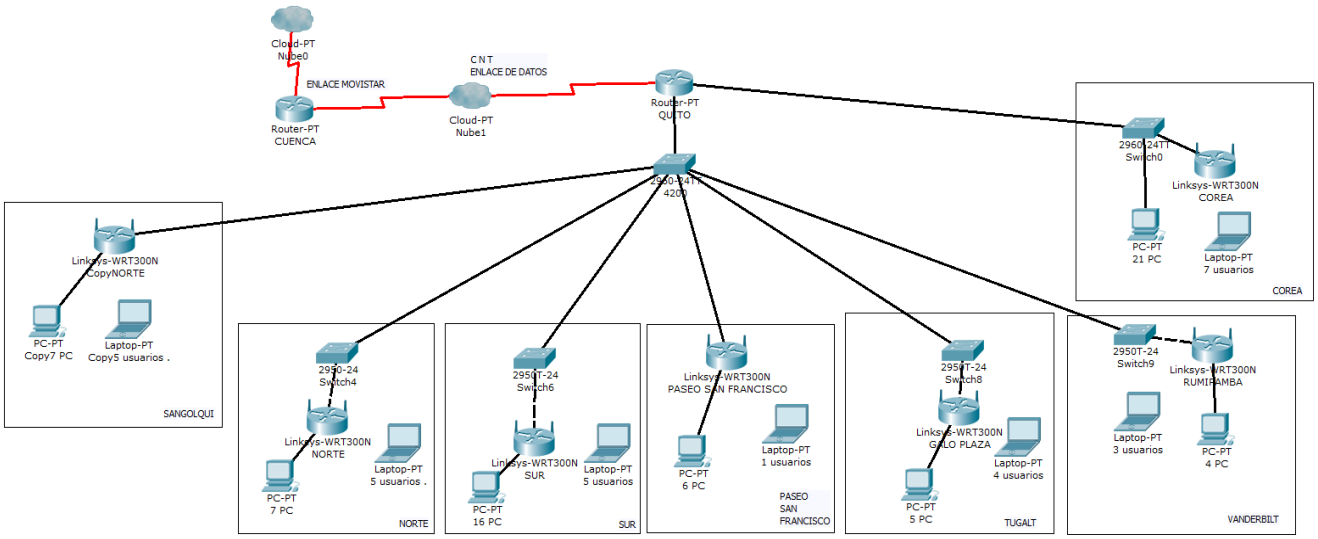


Figura 1-1. Topología de la red[7]

1.1.2 DEFINICIÓN DEL PROBLEMA

Las hipótesis de problemas de la red inalámbrica en la institución fueron definidas en función a la observación, elaboración de entrevistas con el administrador de la red (ver Anexo A, Anexo B) y la revisión de manuales técnicos.

[7] Elaborado por: La autora en base a información obtenida de la institución.

Para cada una de las entrevistas se generaron Actas de Reunión entregadas al administrador de la red, el formato se encuentra en el Anexo C.

El resumen de los problemas encontrados relacionados con la red inalámbrica se detalla a continuación:

1. **Políticas de seguridad**

La institución no cuenta con políticas de usuarios o un conjunto de buenas prácticas para el uso de la red inalámbrica. Es decir que no puede garantizar el buen manejo de servicios y recursos de la red, ni que las operaciones las realicen solo usuarios autorizados.
No cuentan con pistas de auditoría a la red inalámbrica. No se realizan capacitaciones periódicas al personal de tecnología; debido a esto existe un desconocimiento en cuanto a metodologías o herramientas que un hacker podría utilizar para tener acceso a la información sensible de la empresa a través de la red inalámbrica.

2. **Administración de los dispositivos**

La institución no cuenta con un inventario completo de todos los dispositivos inalámbricos y no realizan actualizaciones de los últimos parches. Tampoco se conoce de las limitaciones en el hardware y software que pueden tener los equipos. Es decir, los dispositivos no se encuentran dentro de un marco planificado por lo que su configuración pone en peligro la seguridad.

3. **Control de acceso**

Los controles de acceso físico a los equipos inalámbricos que tiene la institución no garantizan seguridad perimetral. Se desconoce si es que existe interferencia con otros dispositivos electrónicos en frecuencias similares y si la comunicación inalámbrica se extiende más de los límites físicos de la institución.
Para los usuarios que ya están dentro de la red inalámbrica, no presenta ninguna distinción de parámetros o accesos diferenciados entre grupos de usuarios propios de la institución versus clientes y visitantes. Es decir, no se otorgan

privilegios especiales, ni se puede brindar soporte a los diferentes usuarios de la red (calidad de servicio).

4. **Configuración de los dispositivos**

A continuación se detallan los controles que hacen falta:

- ✓ La robustez en las contraseñas administrativas, el cambio periódico, la caducidad y el manejo de las mismas.
- ✓ Implementación de SNMP (Simple Network Management Protocol); éste protocolo permite la gestión y monitoreo del tráfico, detección de errores en la red o accesos inadecuados de la red. Al momento cuenta con el dispositivo **microtick RouterBoard RB750GL** en la capa Core del modelo jerárquico de la red, en dicho dispositivo soporta la implementación del protocolo. Sin embargo, no lo tienen implementado.
- ✓ Los clientes inalámbricos cuentan con Firewall instalado pero no con el software antivirus instalado en su última versión, por lo tanto no garantiza seguridad a la red inalámbrica.
- ✓ No todos los parámetros de configuración fueron cambiados y se encuentran ciertas configuraciones con los predeterminados que vienen en el dispositivo. Eso indica que están habilitados protocolos de gestión insegura e innecesaria en los dispositivos inalámbricos.

1.2 SELECCIÓN Y JUSTIFICACIÓN DE LAS METODOLOGÍAS

Como fundamento teórico y procedimental enfocado al hacking ético de la red inalámbrica, la autora ha elegido tres metodologías para su comparación y estas son: OSSTMM WIRELESS 2.9.1 (Wireless Security Testing Section Open-Source Security Testing Methodology Manual), ISSAF draft 0.2.1 (Information Systems Security Assessment Framework (ISSAF) draft 0.2.1) y OWISAM OWISAM (Open Wireless Security Assessment Methodology).

1.2.1 DESCRIPCIÓN DE LA METODOLOGÍA OSSTMM

ISECOM presenta un método estandarizado llamado Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM), con la finalidad de realizar pruebas, para las seis diferentes secciones de seguridad de la organización. En la Figura 1-2 se puede observar el mapa de seguridad presentado por la metodología; la parte coloreada de verde corresponde a la sección de Seguridad Inalámbrica.

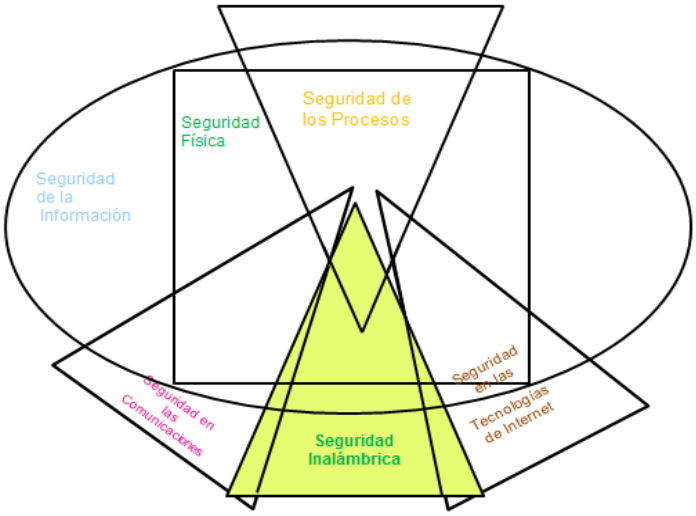


Figura 1-2. Mapa de Seguridad[8]

Cada una de las secciones del mapa de seguridad presenta una lista de módulos con sus respectivas tareas. “Cada módulo debe incluir todas las Dimensiones de Seguridad que están integradas con tareas a ser desarrolladas.

Para desarrollar un análisis de seguridad OSSTMM de una sección particular, todos los módulos de la sección deben ser desarrollados y aquellos para los que no exista infraestructura y no pueda ser verificada, debe definirse como NO APLICABLE en la hoja de datos OSSTMM anexado al informe final.”[9] En el Anexo E se encuentra la lista de todos los Módulos.

El flujo de la metodología, ver la Figura 1-3, se puede observar que cada módulo tiene una entrada y una salida; esta entrada corresponde a la información que va a utilizarse en la tarea, y la salida corresponde al resultado de dicha tarea que fue completada. Por esta razón realiza la separación entre la recolección de datos y

[8] Fuente: OSSTMM Wireless versión 2.9, página 20
[9] Fuente: OSSTMM Wireless versión 2.9, página 21.

las pruebas de verificación. Cada módulo está relacionado al módulo inmediatamente anterior y con el módulo inmediatamente posterior. A la vez que algunos módulos están interrelacionados con otras secciones.

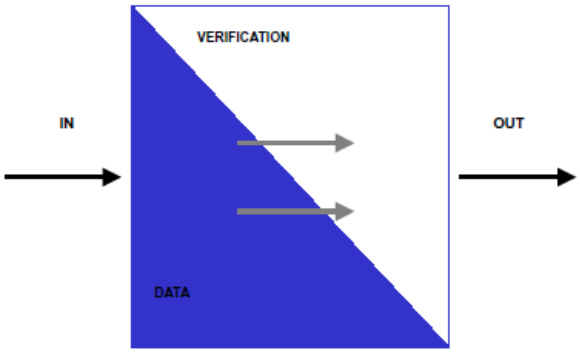


Figura 1-3. Metodología OSSTMM[10]

1.2.1.1 Estructura de las pruebas OSSTMM

"Identificar las tareas que puedan ser vistas como innecesarias y por lo tanto retiradas tranquilamente del análisis es vital, cuando se definen los módulos a analizar para un sistema objetivo, donde el ámbito del proyecto o restricciones así lo requieran. Estas tareas omitidas, sin embargo, deben documentarse claramente y deben ser aceptadas previo al proceso de análisis"[11]. En la Figura 1-4 presenta una propuesta ejemplo de la estructura de pruebas y tareas de OSSTMM.

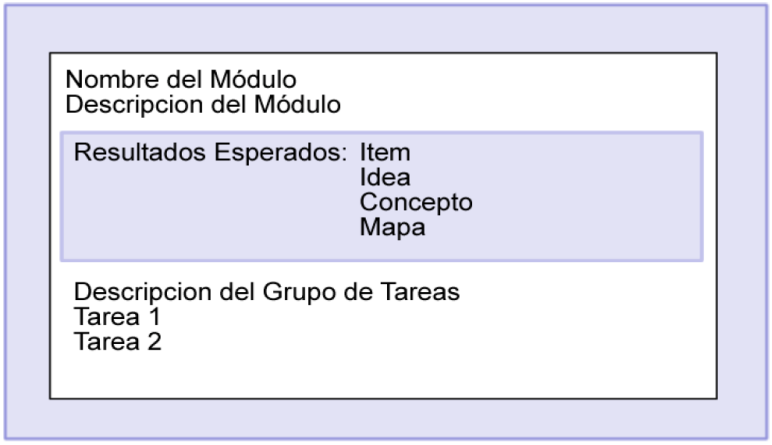


Figura 1-4. Estructura de pruebas OSSTMM[12]

[10] Fuente: OSSTMM Wireless versión 2.9, página 29
[11] Fuente: OSSTMM Wireless versión 2.9, página 30.
[12] Fuente: OSSTMM Wireless versión 2.9, página 31.

1.2.1.2 Aplicación de la metodología OSSTMM en la sección Seguridad Inalámbrica

De acuerdo al alcance definido dentro de este proyecto de titulación se elegirá de la metodología OSSTMM, solo la sección que corresponde a la red inalámbrica. En la Figura 1-5, se muestra la aplicación de las fases de la metodología sobre la sección de Seguridad Inalámbrica, con sus respectivos módulos y tareas:

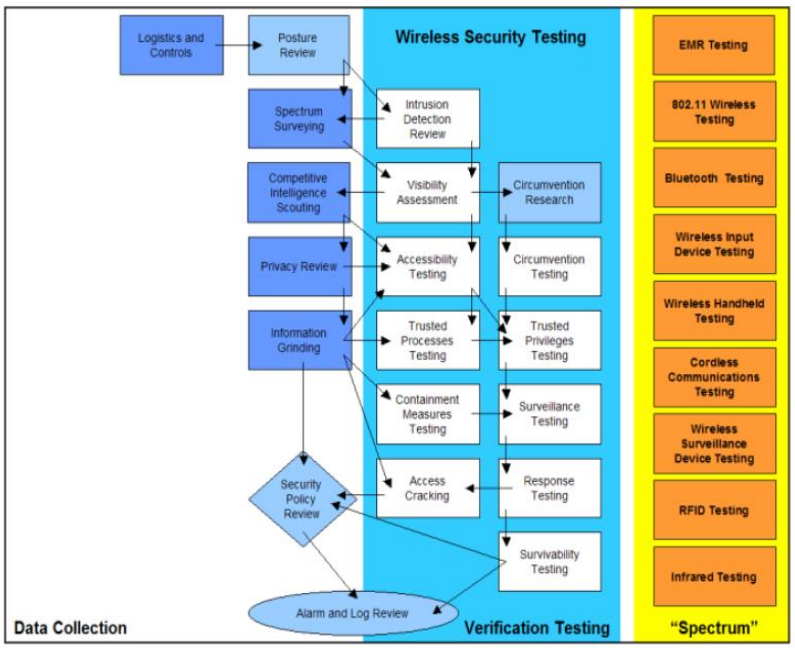


Figura 1-5. Seguridad Inalámbrica de OSSTMM[13]

Para analizar la Seguridad Inalámbrica, OSSTMM divide en módulos de acuerdo al espectro electromagnético de comunicaciones digitales y análogas.

De acuerdo a las entrevistas e inspecciones realizadas a la red de la institución se puede apreciar los componentes de su infraestructura de red. El administrador de la red tuvo que elegir el tipo de dispositivos inalámbricos son necesarios realizar la evaluación de Seguridad Inalámbrica.

En la Tabla 1-2, explica los tipos de dispositivos inalámbricos presentes en la institución, donde cuenta con los siguientes parámetros la tabla:

- Tipos de dispositivos inalámbricos, descripción del tipo.
- Número, de dispositivos que cuenta en las sedes de Quito.
- Nivel de importancia, con valor 0 indica no es de importancia para ser analizado y 1 es de importancia para ser analizado.

[13] Fuente: OSSTMM Wireless versión 2.9, página 20

Tipos de dispositivos inalámbricos	Número	Nivel de importacia
Radiación electromagnética (ej.: lcds)	15	0
Redes Inalámbricas 802.11 (ej.: Opera en el rango de frecuencias de 5Ghz o 2.5Ghz)	36	1
Dispositivos bluetooth	0	0
Dispositivos de Entrada Inalámbricos (ej.: ratones y teclados)	10	0
Dispositivos de Mano Inalámbricos (ej: celulares)	10	0
Dispositivos de Vigilancia Inalámbricos (ej.: micrófonos, cámaras)	10	0
Dispositivos de Transacción Inalámbricos (ej.: escáneres, cerrojos, lectores de tarjetas, cámaras)	15	0
Infrarrojos	0	0

Tabla 1-2. Dispositivos inalámbricos a ser analizados[14]

Por el número de dispositivos que cuentan en las sedes y el nivel de importancia se seleccionará el módulo 2 que corresponde a la "Verificación de Redes Inalámbricas [802.11]". Dicho módulo como resultados esperados y sus tareas o actividades son:

- ✓ Evaluar las necesidades de Negocio, prácticas y políticas.
- ✓ Evaluar equipamiento, firmware y actualizaciones.
- ✓ Evaluar el control de acceso, seguridad perimetral y la habilidad para interceptar o interferir con la Comunicación.
- ✓ Evaluar el acceso administrativo a los dispositivos inalámbricos.
- ✓ Evaluar la configuración, autenticación y cifrado de redes inalámbricas.

1.2.2 DESCRIPCIÓN DE LA METODOLOGÍA ISSAF DRAFT 0.2.1

ISSAF 0.2.1 es un framework estructurado de análisis de seguridad de la información, el cual proporciona información acerca de cómo llevar a cabo una prueba. Su objetivo es proporcionar entradas de campo sobre la evaluación de la seguridad que reflejan situaciones de la vida real.

[14] Elaborado por: La autora en base de la metodología OSSTMM.

“La metodología de pruebas de intrusión ISSAF está diseñada para evaluar la red, sistemas y aplicaciones. Éste se enfoca en 3 fases y 9 pasos de evaluación.
Fase I: Planeación y preparación
Fase 2: Evaluación
Fase 3: Presentación de informes “[15]

Fase I: Planificación y Preparación

En esta fase contiene los pasos iniciales de intercambio de información, para planificar y preparar al organismo de las prueba de evaluación. Antes que nada se debe firmar un acuerdo por ambas partes (Empresa y auditor de seguridad), indicando la mutua protección jurídica, los integrantes del equipo de trabajo, las fechas en las que serán realizadas, el tiempo de la prueba y otras evaluaciones.

Actividades:

- Identificación de los contactos de ambas partes
- Apertura de la reunión para identificar el alcance, enfoque y metodología.
- Acuerdo a los casos de pruebas y rutas de escalamiento.

Fase 2: Evaluación

En esta fase se lleva acabo las pruebas. Está dividido en capas, cada una indica un mayor nivel de acceso a los activos de la información y estas son:

1. Recolección de la Información, se realiza un análisis pasivo de dispositivos.
2. Mapeo de la red, se realiza un escaneo pasivo a la red para identificar los dispositivos que se encuentran relacionados.
3. Identificación de vulnerabilidades, luego de la identificación relevante a la infraestructura de los dispositivos se procede al análisis de debilidades.
4. Penetración, con las herramientas escogidas se procede con el análisis de debilidades de la red en medio de diferentes escenarios.
5. Obtener Acceso y escalada de privilegios, para asegurarnos de tener control de acceso se puede empezar con el usuario root y probar hasta lo máximo posible.

[15] Fuente: ISSAF versión 0.2.1, página 136

6. Enumeración, enumerar otros objetivos, ataque de contraseñas, analizar el tráfico de la red.
7. Comprometer usuarios/sitios remotos, se refiere a tratar de controlar ocultamente otros dispositivos.
8. Mantener Acceso, de manera oculta controlar los dispositivos.
9. Cubrir los rastros, descubrir formas de ocultamiento de pruebas.

Fase 3: Reportes, Limpieza y Destrucción de Objetos

Esta fase es de carácter crítico; se deben discutir y buscar contramedidas para resolver los problemas identificados. En los reportes constar las recomendaciones bien estructuradas. Además se deben limpiar en el sistema todas las pruebas realizadas. En la Figura 1-6, muestra la metodología ISSAF y las capas que corresponden a cada fase:

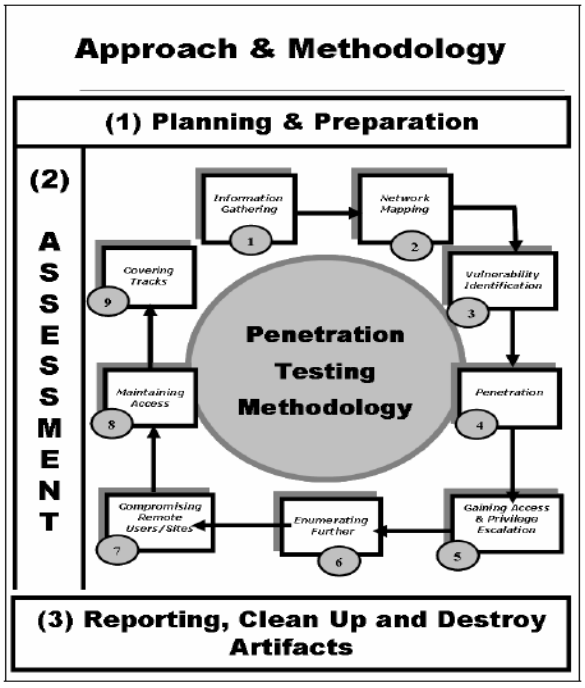


Figura 1-6. Metodología ISSAF[16]

1.2.2.1 Estructura de pruebas ISSAF

ISSAF presenta una plantilla para las pruebas, donde indica el procedimiento de la prueba cuáles son los controles técnicos dentro de la fase de Evaluación, ver la Figura 1-7:

[16] Fuente: ISSAF versión 0.2.1, página 137.

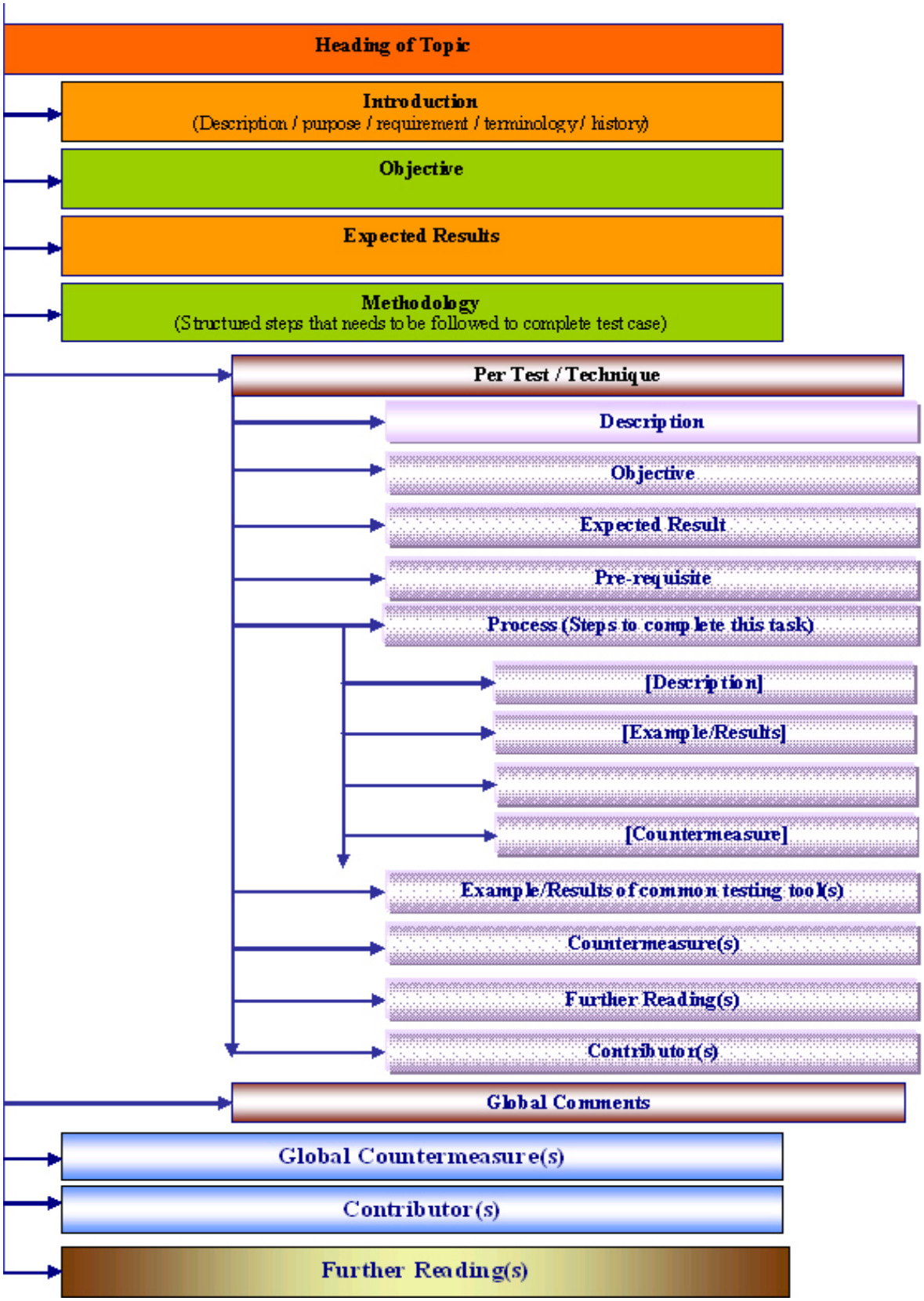


Figura 1-7. Estructura de las pruebas ISSAF[17]

[17] Fuente: ISSAF versión 0.2.1, página 23.

1.2.2.2 Aplicación de la metodología ISSAF en la sección Seguridad Inalámbrica

De acuerdo al alcance definido dentro de este proyecto de titulación de la metodología ISSAF, se elegirá la sección M llamada Evaluación de seguridad de WLAN. Ver en la Figura 1-8, muestra la aplicación de la metodología ISSAF para Seguridad Inalámbrica con las siguientes etapas de hacking ético:

- Recolección de Información.
- Escaneo y Auditoria.
- Análisis e Investigación.
- Explotación y Ataque.
- Reportes y Presentación.

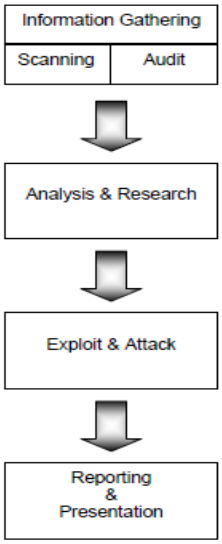


Figura 1-8. Mapa de la Metodología de la Evaluación de Seguridad WLAN[18]

Además presenta material de apoyo como lecturas adicionales, herramientas libres o con licencia con link de descarga, descripción y la razón de ser utilizadas.

1.2.3 DESCRIPCIÓN DE LA METODOLOGÍA OWISAM

OWISAM es una propuesta de metodología ágil para la revisión de la seguridad inalámbrica, con licencia Creative Commons Attribution ShareAlike 3.0 license (CC-BY-SA) donde permite la participación de toda la comunidad para la modificación y reproducción de la misma.

---

[18] Fuente: ISSAF versión 0.2.1, página 539.

Controles OWISAM

En la Tabla 1-3 detalla las verificaciones técnicas a las comunicaciones inalámbricas, esto con el fin de analizar el riesgo de seguridad que se expone una institución.

#	Código	Tipo de control	Descripción de los controles
1	OWISAM-DI	Descubrimiento de dispositivos	Recopilación de información sobre las redes inalámbricas.
2	OWISAM-FP	Fingerprinting	Análisis de las funcionalidades de los dispositivos de comunicaciones.
3	OWISAM-AU	Pruebas sobre la autenticación	Análisis de los mecanismos de autenticación.
4	OWISAM-CP	Cifrado de las comunicaciones	Análisis de los mecanismos de cifrado de información.
5	OWISAM-CF	Configuración de la plataforma	Verificación de la configuración de las redes.
6	OWISAM-IF	Pruebas de infraestructura	Controles de seguridad sobre la infraestructura Wireless
7	OWISAM-DS	Pruebas de denegación de servicio	Controles orientados a verificar la disponibilidad del entorno
8	OWISAM-GD	Pruebas sobre directivas y normativa	Análisis de aspectos normativos que aplican al uso de las redes de Wi-Fi
9	OWISAM-CT	Pruebas sobre los clientes inalámbricos	Ataques contra clientes inalámbricos
10	OWISAM-HS	Pruebas sobre hostspots y portales cautivos	Debilidades que afectan al uso de portales cautivos

Tabla 1-3. Lista de Controles OWISAM[19]

[19] Fuente: OWISAM, https://www.owisam.org/es/Controles_OWISAM, último acceso: 22/07/2014

Cada uno de estos controles explica el cómo realizar la prueba (entre 6 a 8 actividades definidas), la vulnerabilidad que afecta, recomendaciones y referencias. Es importante mencionar que no todos las pruebas están completas.

1.2.3.1 Estructura de pruebas OWISAM

OWISAM no presenta una estructura definida de cómo llevar a cabo las pruebas, pero en la mayoría de las pruebas presenta una propuesta de cómo llevarlas a cabo mientras que otras no están documentadas como fue mencionado anteriormente.

Presenta una lista de controles y dentro de cada lista se encuentran un listado de verificaciones técnicas. “Los controles de seguridad definidos por la metodología de seguridad wireless OWISAM son todas aquellas verificaciones técnicas que deben ser llevadas a cabo para analizar el riesgo de seguridad al que está expuesta una organización debido al uso de infraestructuras de comunicaciones Wi-Fi dentro de su perímetro.” [20]

Toda lista de controles de verificación técnicas que presenta la metodología OWISAM se encuentra en el Anexo D.

1.2.3.2 Aplicación de la metodología OWISAM en la sección Seguridad Inalámbrica

Al ser OWISAM una metodología orientada directamente para el área de Auditoría en la Red Inalámbrica, se procede a la selección de todas las fases que contiene la metodología.

Dentro de la metodología de análisis indica los siguientes aspectos:

- Tipos de análisis: como son caja negra, blanca y gris.
- Restricciones: correspondiente al área geográfica, ESSID, BSSID, pruebas de fuerza bruta, ataques de Denegación de servicio, ventana horaria, análisis activo, análisis del perímetro, visibilidad de las pruebas.

[20] Fuente: OWISAM, https://www.owisam.org/es/Controles_OWISAM, último acceso: 22/07/2014

- Consideraciones al inicio de la auditoria: recomienda tomar en cuenta la autorización del trabajo, el almacenamiento de información, Interacción con los dispositivos, ganancia y antenas, potencia de transmisión y frecuencias utilizadas, emisión de interferencias y duración de las pruebas.

OWISAM cuenta con 7 fases, ver en la Figura 1-9:

- ✓ **Planificación:** esta proyección debe abarcar el alcance que fue definido al inicio.
- ✓ **Recopilación de la Información:** consiste en descubrir el inventario de activos (dispositivos) que van a ser analizados.
- ✓ **Identificación de dispositivos:** caracterización de información principal de la infraestructura.
- ✓ **Ataques:** consiste en realizar pruebas a los dispositivos, como por ejemplo denegación de servicio así determinar qué debilidades puedan tener.
- ✓ **Acceso a la red:** luego del ataque mantener el acceso con la infraestructura.
- ✓ **Pruebas sobre normativa y directivas:** Comprobar el cumplimiento o no de controles normativos definidos por la institución.
- ✓ **Generación de resultados:** análisis de los resultados y presentación de informes.

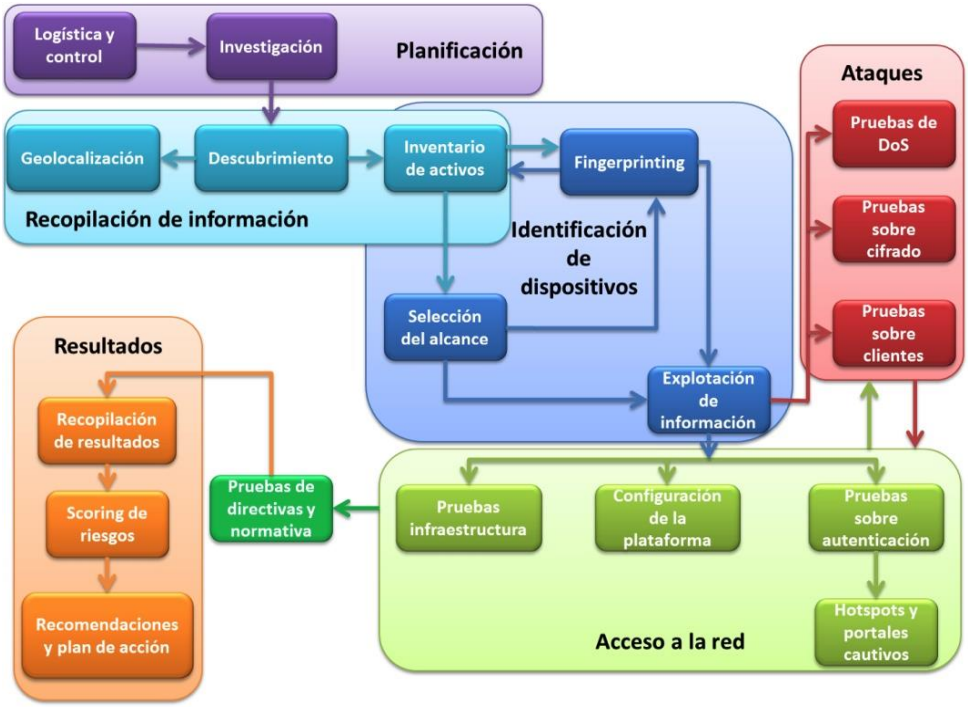


Figura 1-9. Metodología OWISAM[21]

1.2.4 SELECCIÓN DE LA METODOLOGÍA

En esta sección se realiza la comparación entre las metodologías, luego elegir por medio de parámetros que serán asignados una calificación cuantitativamente y la que tenga mayor valoración será elegida para tomar como referencia en el procedimiento de ejecución del caso de estudio.

Los parámetros[22] para la elección de la metodología fueron tomados como referencia del proyecto de titulación llamado "Análisis de Riesgos y Vulnerabilidades de la infraestructura de la secretaria nacional de gestión de riesgos utilizando metodologías de hacking ético" y se describen a continuación:

Parámetro 1. Explica lineamientos para aplicación de hacking ético enfocado a la red inalámbrica

---

[21] Fuente: OWISAM, https://www.owisam.org/es/Controles_OWISAM, último acceso: 22/07/2014

[22] Fuente: Acosta, O. Proyecto de titulación llamado "Análisis de Riesgos y Vulnerabilidades de la infraestructura de la secretaria nacional de gestión de riesgos utilizando metodologías de hacking ético", página 26 [Marzo, 2013].

Debe explicar el procedimiento detallado de hacking ético para las redes inalámbricas, es decir cubrir las fases:

- Recolección de Información.
- Escaneo y Auditoria.
- Análisis e Investigación.
- Explotación y Ataque.
- Reportes y Presentación.

Parámetro 2. Explica tipos de análisis de hacking ético

Debe explicar qué restricciones del alcance se debe tomar en cuenta para el análisis de hacking ético y cuáles son los tipos de análisis que es posible ejecutarlos.

Parámetro 3. Explica lineamientos para recolectar Información

Debe explicar el cómo realizar la obtención de información antes, durante y al final de la información.

Parámetro 4. Explica pruebas de intrusión a redes inalámbricas

Debe explicar el modo de ejecución de las pruebas antes, durante y después de las pruebas intrusivas. La propuesta de pruebas intrusivas debe estar relacionado a: políticas, hardware y firmware, control de acceso, seguridad perimetral, control de configuración y mecanismos de autenticación en un marco de la red inalámbrica.

Parámetro 5. Recomendación de herramientas

Debe proponer herramientas para el hacking ético para la red inalámbrica, es decir un conjunto de exploits y kit de herramientas de ingeniería social.

Parámetro 6. Licenciamiento de las herramientas

Debe proveer opciones de software tanto con licencia como sin licencia.

Parámetro 7. Plantillas de los informes y reportes

Deben mostrar plantillas de cómo se debe elaborar y presentar los informes y reportes al cliente al finalizar la evaluación.

Parámetro 8. Explica el procedimiento para la Evaluación de Riesgos

Debe explicar cuáles son los parámetros necesarios para la realización de una Evaluación de la red, es decir la identificación de vulnerabilidades, amenazas.

Parámetro 9. Diseño y construcción de un Plan de Mitigación

Debe constatar un conjunto de recomendaciones para la implementación de controles que mitiguen los riesgos relacionados con la red inalámbrica. Además de que deben ser aplicables en toda la institución independiente del tipo, tamaño debido a que contamos con varias sedes.

Parámetro 10. Metodología completa

Para el caso de estudio se considera una metodología completa cuando cuente con los siguientes parámetros:

- Fases con su respectiva explicación.
- Estructura de pruebas.
- Recomendación y manejo de herramientas (con y sin licencia).
- Lecturas de referencia.
- Metodología de renombre (con más de 3 años de vigencia).

La calificación cuantitativa de cada parámetro cuenta con la siguiente valoración:

- 2 indica que está disponible.
- 0 indica que no está disponible.

#	Parámetros	Metodología		
		OSSTMM	ISSAF	OWISAM
1	Explica lineamientos para aplicación de hacking ético enfocado a la red inalámbrica	2	2	2
2	Explica tipos de análisis para el hacking ético	0	2	2
3	Explica lineamientos para recolectar Información	0	2	2
4	Explica pruebas de intrusión a redes inalámbricas	2	2	2
5	Recomendación de herramientas	0	2	2
6	Licenciamiento de las herramientas	0	2	2
7	Plantillas de los informes y reportes	2	2	0
8	Explica el procedimiento para la Evaluación de Riesgos	2	2	0

9	Diseño y construcción de un Plan de Mitigación	0	2	0
10	Metodología completa	0	2	0
	SUMATORIA	8	20	14

Tabla 1-4. Comparativa de Metodologías[23]

Como se puede observar en la tabla anterior el framework ISSAF tiene mayor puntuación, entonces se procede a la selección de dicha metodología.
Además a esto, se completarán con las tareas y herramientas sugeridas por las otras dos metodologías, para el desarrollo del presente proyecto de titulación.

1.3 SELECCIÓN Y JUSTIFICACIÓN DE LAS HERRAMIENTAS

Para la selección de las herramientas[e][q] para las pruebas de intrusión se tomó en cuenta los siguientes aspectos:

- "Herramientas que permitan escanear vulnerabilidades, dentro de cada una de las fases del hacking ético a la red inalámbrica es decir que presente un conjunto de exploits y kit de herramientas de ingeniería social."[h]
- Que sean de distribución libre, debido a que debe cumplir con los objetivos del alcance definido en el proyecto de titulación.
- Experiencia de la auditora, en el uso o manejo de la misma.
- Herramienta que permita ser instalados en ambientes virtuales.

Las herramientas para el análisis de la seguridad de la red inalámbrica, que serán utilizados de acuerdo las fases que propone ISSAF:

- Recolección de Información (Acrylic Wi-Fi Free complementándose con la distribución WifiSlax 4.9).
- Escaneo y Auditoria (Acrylic Wi-Fi Free complementándose con WifiSlax 4.9).
- Análisis e Investigación (De las distribuciones WifiSlax 4.9 complementándose con Backtrack 5).

[23] Elaborado por: La autora en base a las metodologías a ser comparadas.

- Explotación y Ataque (De las distribuciones WifiSlax 4.9 complementándose con Backtrack 5).
- Reportes y Presentación (de todas las herramientas anteriormente mencionadas)

1.3.1 ACRYLIC WI-FI FREE

Es un sniffer gratuito, su funcionalidad de capturar el tráfico de las redes inalámbricas, está disponible para sistemas operativos de Windows como Vista, 7 y 8. En su instalación también integra herramientas como Wireshark para capturar paquetes.

Objetivos:

- Detectar e identificar las redes inalámbricas
- Determinar qué canales y ESSID
- Coleccionar de direcciones IP y MAC de AP
- Determinar qué método de encriptación tiene AP

1.3.2 WIFISLAX 4.9

Está basado en la distribución Slackware Linux, es un sistema operativo que incorpora varias herramientas orientadas a la auditoria de redes inalámbricas. La distribución de WifiSlax maneja un entorno gráfico.

1.3.3 SUITE AIRCRACK-NG

Es una suite que permite desencriptar los paquetes capturados y luego obtiene las claves estáticas WEP y WPA-PSK, por fuerza bruta analizar paquetes de la red inalámbrica. Las herramientas de la suite que serán utilizadas:

- airmon-ng: rastrea y captura paquetes de las redes wireless aunque no esté destinado para el dispositivo, poniendo la tarjeta inalámbrica en modo monitor.
- airodump-ng: captura de paquetes mandados por los router más cercanos
- aireplay-ng: programa que permite inyectar tráfico en la red y conseguir paquetes con datos más rápidamente.

Objetivos:

- Detectar e identificar las redes inalámbricas

- Crackear las redes que tengan método de encriptación WEP WPA /WPA2-PSK.

1.3.4 BACKTRACK 5 [c]

Toda su distribución es en GNU/Linux diseñada con la finalidad de auditoria de seguridad informática en general. Contiene herramientas de escaneo, análisis forense y herramientas para auditoria Wireless.

Objetivos:

- Recopilación de Información
- Mapeo de Puertos
- Identificación de Vulnerabilidades
- Análisis de aplicaciones Web
- Penetración (Exploits y Kit de herramientas de ingeniería social)
- Escalada de privilegios
- Mantenimiento de Acceso

1.3.5 NMAP (NETWORK MAPPER)

Es una herramienta para exploración y auditoria de redes.

Objetivos:

- Analizar e identificar los puertos, servicios y el sistema operativo de los routers.
- Detección de AP piratas.
- Determinar los tipos de métodos de autenticación.

1.3.6 WIRESHARK

Esta herramienta con entorno gráfico donde es posible ver el tráfico que pasa a través de la red. “Permite examinar más de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, los protocolos y servicios. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión TCP”[24].

Objetivos:

- Capturar paquetes
- Revisar el tráfico de la red de clientes conectados.

---

[24] Fuente: OWISAM, http://es.wikipedia.org/wiki/Wireshark, último acceso: 22/07/2014

1.3.7 TECHNITIUM MAC ADDRESS CHANGER

Compatible con cualquier Windows y es software libre. Permite generar una MAC aleatoria y renovar IP, deshabilitar el protocolo DHCP entre otras.

Objetivos:

- Cambiar la MAC para acceder a la red institucional, es decir identificar los clientes relacionados para cambiar de MAC con Technitum, luego ingresar a la red y constatar si es posible acceder a la red.

CAPÍTULO 2.
2. EVALUACIÓN DE RIESGOS

La manera de combatir ataques informáticos tanto internos como externos a la institución, es encontrando un modelo de seguridad que permita medir la seguridad y determinar el análisis cuantitativo de los riesgos que puede estar expuesta la red inalámbrica.

Esta deducción debe estar sustentada por medio de la ejecución de pruebas a los equipos inalámbricos de la red sin dañarlos y debidamente informadas con días de antelación al administrador de la red.

El CAPÍTULO 2 describe el Análisis de la Evaluación de Riesgos. Se empieza con la aplicación de pruebas intrusivas y no intrusivas a la institución, lo que permitirá la búsqueda de vulnerabilidades, amenazas y riesgos presentes. Todo este procedimiento se llevará a acabo de acuerdo a los lineamientos propuestos por la metodología ISSAF y complementándola por las metodologías OSSTMM y OWISAM.

Esta información recolectada antes, durante y al finalizar las pruebas serán documentadas y será de utilidad para finalmente en el capítulo 3, la presentación de un informe de Análisis de Riesgos y un Plan de Mitigación de la red inalámbrica a la alta dirección.

2.1 APLICACIÓN DE PRUEBAS DE PENETRACIÓN

Las pruebas de penetración pueden tener los siguientes enfoques:

- Caja Negra, es cuando no tiene conocimiento de la infraestructura a ser evaluada por parte de auditor e intenta realizar ataques externos.
- Caja Blanca, es cuando tiene conocimiento sobre la infraestructura y define claramente el alcance (ESSIDs, BSSIDs,..) y está enfocado a dispositivos concretos o para analizar la evolución relacionado a la seguridad inalámbrica.
- Caja Gris, es una mezcla entre los anteriores pero actúa como usuario interno no-autorizado. Ej.: personal de la empresa o un asesor externo que tiene acceso físico a la red de la organización.

Para el caso de estudio se aplicarán pruebas de penetración de tipo caja gris debido a que en entrevistas con el administrador de la red se decidió cubrir los dos escenarios.

El procedimiento de hacking ético de la red inalámbrica se realizarán de acuerdo a los lineamientos dirigidos por la metodología ISSAF (su justificación explica en el acápite 1.2.3.1). Las fases de la metodología se muestran en la Figura 2-1.

Figura 2-1. Metodología ISSAF[25]

[25] Elaborado por: La autora en base a las fases propuestas por la metodologia ISSAF.

Fase 1: **Planificación y Preparación,** el objetivo de esta etapa es realizar la proyección de tareas y actividades en orden cronológico, conforme el alcance definido y la ejecución del procedimiento de hacking ético.

En esta etapa se realizaron tareas como: la definición del alcance, los límites, la planificación de actividades y el acuerdo de confidencialidad necesario, el cual se presenta como un requisito previo para el hacking ético y la ejecución de las pruebas. Esta fase se ejecutará en el acápite 2.1.1.

Fase 2: **Evaluación,** el objetivo de esta etapa es ejecutar las pruebas intrusivas y no intrusivas a la red inalámbrica. Para ello el procedimiento de las pruebas realizadas serán: Recolección de Información, Escaneo - Auditoría, Análisis de la seguridad - Búsqueda y Explotación – Ataque (ver el procedimiento en la Figura 2-1). La ejecución de las pruebas se explica en el acápite 2.1.2.
El Reporte y Presentación se explicarán en la fase 3 de la metodología en el acápite 3.3.5.

Fase 3: **Reportes, Limpieza y Destrucción de Objetos**, el objetivo de esta etapa es presentar un reporte de los resultados al administrador(a) de la red inalámbrica de la institución, por medio del Informe Ejecutivo.
Además se realizará la limpieza y destrucción de todos los objetos obtenidos durante este análisis. Para la explicación y su ejecución de esta fase referirse a los acápites 3.3.3, 3.3.4 y 3.3.5.

2.1.1 EJECUCIÓN DE LA FASE DE PLANEACIÓN Y PREPARACIÓN

En la sección sombreada de la Figura 2-2 muestra la fase de la metodología que se explicará a continuación.

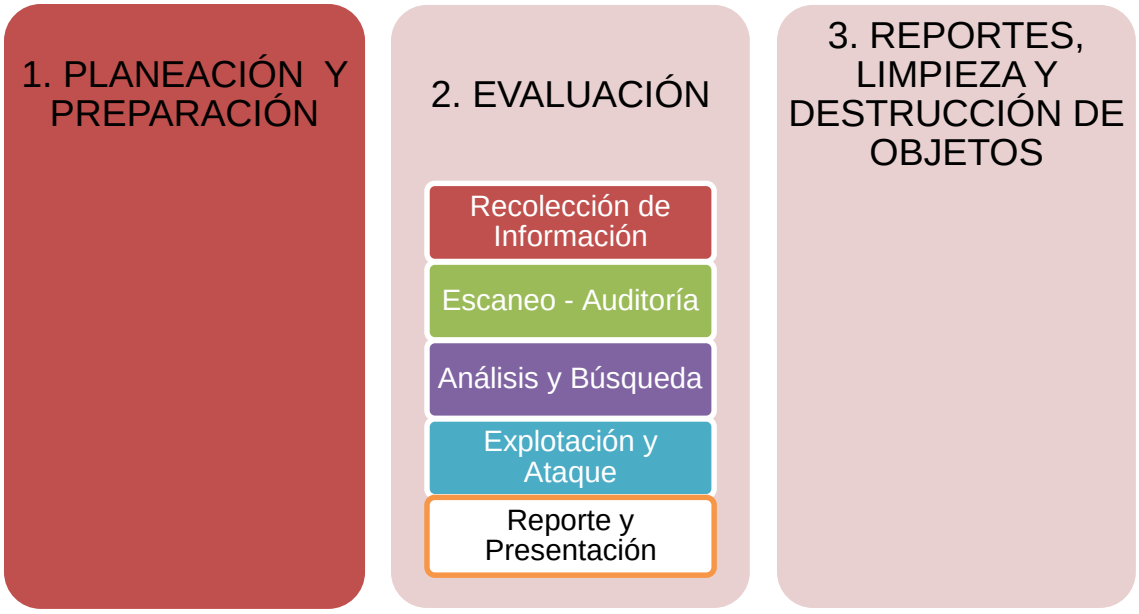


Figura 2-2. Fase de preparación y planificación[26]

En esta fase se presentaron dos documentos:

1. El Acuerdo de Confidencialidad, es una acreditación u orden de trabajo firmado entre la autora y la institución de no divulgación de información sobre los resultados obtenidos.

2. El Plan de Compromiso[27], es el documento donde se delimita y detalla las actividades destinadas para el taller práctico de análisis y evaluación de la red inalámbrica. En la Tabla 2-1 representa los parámetros que recomienda la metodología ISSAF:

Parámetros	Descripción
Nombre del proyecto	Información correspondiente los nombres de la institución y la auditor(a) que realiza el análisis.
Objetivos generales y específicos,	Corresponde parte de la descripción del alcance del procedimiento de hacking ético a la red inalámbrica. Recomienda que los objetivos sean SMART (Pequeños, medibles, auditables, realizables y basados en el tiempo). También describir las expectativas de resultados.

[26] Elaborado por: La autora en base a las fases propuestas por la metodología

[27] Fuente: ISSAF versión 0.2.1, página 40

Enfoque	Las restricciones en el alcance para el análisis propuesto. Se detalla de acuerdo a las tres fases que presenta la metodología de hacking ISSAF: ▪ **Planificación y preparación** Detalle del alcance y la logística a llevarse a cabo el taller práctico. ▪ **Evaluación** Descripción a alto nivel sobre las pruebas a ser llevadas a cabo ▪ **Reporte (Conclusiones / Resultados)** Luego de la consecución de las pruebas intrusivas y no intrusivas determinar qué tipo de entregables serán propuestos a los interesados de la institución.
Compromiso de Alcance	Describir el proceso de vida de las pruebas, la sensibilidad de los datos (financiera, ventas, empleados), los departamentos que están dentro y fuera del alcance,
Planificación de actividades,	Discutir acerca de las lecciones aprendidas. La organización de las pruebas a ser aplicadas Disponibilidad de las herramientas (comercial, freeware).

Tabla 2-1. Descripción del Plan de Compromiso[28]

Este plan de compromiso debe ser enviado al cliente además de las siguientes consideraciones:

- La evaluación debe detallar el tiempo de duración
- Contactos del equipo auditor
- Tratar de completar las evaluaciones en horarios de oficina

A continuación se presenta un resumen del Plan de Compromiso entregado al administrador de la red con el fin de explicar previamente las actividades a llevarse a cabo, su versión original se encuentra en el Anexo F:

[28] Elaborado por: La autora en base a la metodología propuesta ISSAF.

Tema del proyecto de Titulación: Aplicación de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Objetivos

- Objetivo General

  Determinar amenazas, riesgos y vulnerabilidades en la red inalámbrica de una institución aplicando metodologías formales.

- Objetivos Específicos
  - Conocer la situación actual de la institución.
  - Identificar las amenazas, riesgos y vulnerabilidades presentes en la infraestructura de la red inalámbrica.
  - Emitir un plan de mitigación para los riesgos identificados.

Enfoque

Es importante clarificar el alcance con sus restricciones en una infraestructura de red inalámbrica. Las restricciones se presentarán en los siguientes ámbitos.

- **Planificación y preparación,** corresponde a definir el alcance y logística. En la Tabla 2-2 explica parámetros para la definición de alcance que recomienda la metodología ISSAF[29] y complementándolas con OWISAM[30].

Parámetros	Respuesta
Organización completa (alcance de la evaluación)	3 sedes / 6 sedes que cuenta la institución.
Ubicación específica (s)	Quito
División (es) Específica (s)	3 sedes
Naturaleza de la prueba	Intrusiva / no intrusiva
Pruebas desde Exteriores, Interior a la institución y o Ambos	Ambos

[29] Fuente: ISSAF versión 0.2.1, página 67.

[30] Fuente: Metodología OWISAM, https://www.owisam.org/es/Metodologia último acceso: [11/08/2014]

Direccionamiento IP o rangos a evaluar	Direcciones IP del departamento de TI de la institución.
Acceso remoto	No aplica
ESSID (Extended Service Set ID, es el nombre cómo se puede identificar a la red)	La red inalámbrica de c/u de las sedes perteneciente a la institución a ser analizada.
Ataques de Denegación de servicio	Si
Horario de ejecución	Horario de Oficina
Tipo de análisis de las pruebas	Caja gris

Tabla 2-2. Restricciones para el alcance[31]

- **Evaluación**, para determinar cuáles son amenazas, vulnerabilidades y riesgos existentes en la red inalámbrica, se aplicará el procedimiento recomendado de la metodología ISSAF y para la ejecución de pruebas se complementaran con las metodologías OWISAM y OSSTMM:
  - Recolección de Información
    - Descubrimiento activo de dispositivos y redes
  - Escaneo
    - Identificación de funcionalidades soportadas por el dispositivo
  - Auditoría y Revisión
    - Controles de Implementación
      - Detección de protección de acceso basado en MAC
      - Pruebas sobre WPS
      - Debilidades en el repositorio de credenciales
    - Controles Técnicos
      - Interfaces administrativas expuestas a la red.
      - Prueba Traceroute, Prueba Aps/Router.
      - Verificación el nivel de intensidad de señal o área de cobertura.
      - Análisis del solapamiento de redes en el mismo canal de comunicaciones.

[31] Elaborado por: La autora en base a la metodologia propuesta ISSAF.

        - Controles de Gestión
            - Pruebas sobre directivas y normativa.
    - Análisis y Búsqueda
        - Debilidades en el firmware del AP
        - Análisis del protocolo SNMP en la red inalámbrica
        - Análisis de protocolos de cifrado inseguro (WEP,
        - TKIP,...)

    - Explotación y Ataque
        - Captura y cracking de claves transmitidas en el proceso de autenticación.
        - Extracción de credenciales de los clientes.
        - Pruebas de deautenticación.
        - Detección de APs falsos.

- **Reporte (Conclusiones / Resultados)**

  Al finalizar la evaluación no se almacenará información relevante a la institución. Los entregables previstos para el caso de estudio son:

  - Presentación de Resultados

    Luego de la ejecución de las pruebas se emitirá un Informe Ejecutivo y Técnico donde se muestran de las conclusiones, resultados y vulnerabilidades encontradas para la alta dirección y para el administrador de la red respectivamente.

  - Plan de Mitigación

    Con la ejecución de las pruebas y su respectivo análisis de riesgos de la red inalámbrica, se emite un plan de mitigación que es un conjunto de recomendaciones con el objetivo de aumentar el nivel de seguridad de la red inalámbrica de la institución.

Planificación de las actividades

En la **Tabla 2-3**[i] se muestra los hitos de compromiso por pruebas, recomendadas por la metodología ISSAF[32]:

FASES	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5
Recolección de Información	X	X			X
Escaneo – Auditoría		X	X		X
Análisis y Búsqueda		X	X	X	X
Explotación y Ataque			X	X	X

Tabla 2-3. Cronograma de actividades

El plan de compromiso entregado al administrador de la red se encuentra en el Anexo F.

2.1.2 EJECUCIÓN DE LA FASE DE EVALUACIÓN

El procedimiento de la fase de evaluación será guiado en función a la metodología ISSAF y las pruebas de penetración se complementará de las metodologías OSSTMM y OWISAM, de esta manera asegurar que se cubran todos los posibles escenarios. La ejecución de la segunda fase del procedimiento de hacking ético de la red inalámbrica, ver Figura 2-3.

[32] Fuente: ISSAF versión 0.2.1, página 46.

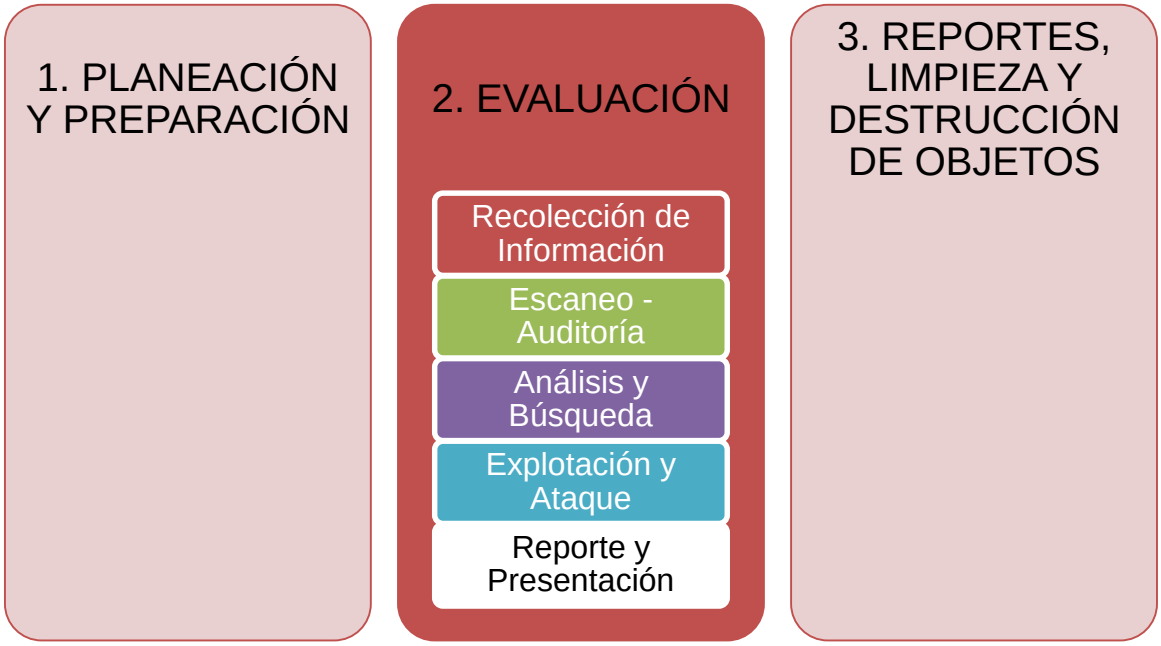


Figura 2-3. Ejecución de la fase de Evaluación[33]

La metodología ISSAF explica los dos modos de ataques que se puede ejecutar durante las pruebas y estas son:

- **Amenazas Pasivas**

  Cuando el atacante solo escucha el flujo del tráfico y hace suposiciones sobre la naturaleza del tráfico, cantidad de tráfico y la posible carga de la red. Los ataques de este tipo casi no pueden ser detectados.

  De la red a ser analizada es posible ver información como: SSID, direcciones MAC de los clientes, los posibles rangos de IP y protocolos utilizados, entre otros. Al no utilizar algún tipo de cifrado es posible capturar información más sensible como correos electrónicos y documentos, y posteriormente convertirse en una amenaza activa.

- **Amenazas Activas**

  Cuando el atacante manipula ya información y herramientas para producir diferentes tipos de resultados en la red y hosts. En cambio para estos es posible ser detectados. Los ataques activos incluyen:

  - Denegación de servicio

[33] Elaborado por: La autora en base a las fases propuestas por la metodologia.

        - Solicitar a todas las direcciones DHCP mediante paquetes falsificados
        - Configuración de AP falsos con la señal más fuerte
        - De-autenticar los clientes de la AP
    - Captura y modificación del tráfico
        - Actuar como un hombre-en-el-medio
    - Inyección del tráfico
        - Reproducción paquetes cifrados (para acelerar el agrietamiento WEP)
        - La inyección de paquetes falsificados en la red

A continuación se explican estos modos de ataque aplicados en cada una de las sub fases en la fase de Evaluación:

- Recolección de Información, OSSTMM indica para empezar con la evaluación de riesgos es necesario “identificar cuáles son las estaciones de comunicaciones y qué relación existe entre ellas”[34] y las tarea propuestas son a través de una tarjeta de interfaz de red inalámbrica ejecutar en modo monitor y descubrir dispositivos inalámbricos no autorizados, redes ocultas, relaciones no autorizadas entre otros.
- Escaneo, luego de recolectar información de los objetivos se debe realizar “pruebas en canales y ESSID, recolectar información del broadcast, identificar puntos de acceso no autorizados, las direcciones MAC las redes inalámbricas, entre otros.”[35]
- Auditoria, cuestionamiento en los controles de:
    - Implementación, se refiere al uso de mecanismos de autenticación inseguros, o elección de claves de acceso débiles o de fácil predicción, “revisar la configuración del firewall.”[36]

[34] Fuente: OSSTMM Wireless versión 2.9, páginas 76 y 77.

[35] Fuente: Metodología OWISAM, https://www.owisam.org/es/Metodologia último acceso: [11/08/2014]

[36] Fuente: ISSAF versión 0.2.1, página 220-223.

- Técnico, ej.: puertos, servicios, sistemas operativos de los dispositivos inalámbricos, determinar firmware actualizado, entre otros.[34]
- Gestión, ej.: "Determinar el uso de políticas de seguridad para contraseñas y buen uso de los dispositivos."[37]

- Análisis e Investigación, ej.: Determinar los mecanismos y protocolos de autenticación para los dispositivos.
- Explotación y Ataque, ej.: obtener las credenciales intrusivamente.
- Reportes y Presentación, esta sub fase se explicará en el acápite 3.3 del siguiente capítulo.

La Tabla 2-4, muestra la plantilla de las pruebas que se ejecutarán. Las columnas tienen la siguiente descripción:

- #, indica el número de la prueba
- Nombre de la sub fase ISSAF, corresponde dentro de la Fase de Evaluación ISSAF el nombre de la sub fase dirigido a redes inalámbricas.
- Nombre de la prueba, ejecutada.
- Objetivo y razones, explica la finalidad de la prueba y el porqué de ejecutarla.
- Herramienta que fue utilizada,
- Procedimiento, explica el modo de uso de la herramienta.
- Modo de ataque, de acuerdo al apartado explicado anteriormente puede ser en modo Activo y Pasivo.

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	MODO DE ATAQUE
1						

Tabla 2-4. Descripción de la prueba[38]

[37] Fuente: OSSTMM Wireless versión 2.9, páginas 76 y 77.

[38] Elaborado por: La autora en base al análisis de pruebas propuesto.

2.1.2.1 Pruebas aplicadas

La metodología ISSAF recomienda antes de ejecutar las pruebas previstas, se informó al administrador de la red que en caso de aparecer alguna actividad inusual durante la ejecución de las pruebas estás serán reportadas en el momento que ocurran, de forma que la institución esté informada y tome las debidas consideraciones.

Las pruebas elegidas para el fase de evaluación fueron tomadas de acuerdo a los problemas inicialmente encontrados en la institución que detallan en el acápite 1.1.2.

En la Tabla 2-5 muestra el listado de las pruebas que fueron ejecutadas en este caso de estudio utilizando las herramientas seleccionadas en el acápite 1.3 y clasificándola de acuerdo al por tipo de ataque. Se aplicó el procedimiento de hacking ético de la metodología ISSAF y para la ejecución de pruebas se complementarán con las metodologías OWISAM y OSSTMM:

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
1	Recolectar Información	Descubrimiento activo de dispositivos y redes	Descubrir los dispositivos inalámbricos que cumplen el estándar 802.11. Debido a que inicialmente se va a recolectar información de los dispositivos que están a nuestro alcance.	Suite Aircrack	Se ejecutará el comando: airodump-ng nombre_interfaz_wifi	Pasivo
2	Escaneo	Identificación de funcionalidades soportadas por el dispositivo[39]	Obtener información del dispositivo tales como: datos del fabricante, drivers, la velocidad de transmisión, tiempo de respuesta, entre otros, con la finalidad del impacto que tiene en la	Acrylic o Wireshark o Ethernet	Con la herramienta Acrylic se obtendrá información del dispositivo: datos del fabricante, la velocidad de transmisión, tiempo de respuesta, entre otros, en las secciones “Fixed Parameters” y “Tagged Parameters”, el uno identifica información más general y el otro revela	Pasivo

[39] Fuente: Metodología OWISAM, https://www.owisam.org/es/ OWISAM-FP-002 último acceso: [11/08/2014]

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
			productividad, eficacia y eficiencia de la red.		información más específica acerca del dispositivo"	
3	Auditoría y Revisión Sub fase: Controles de Implementación	Detección de protección de acceso basado en MAC[40]	Determinar la existencia de un control de dispositivos inalámbricos basados en MAC. Este mecanismo es una medida de seguridad para la red inalámbrica pero no debería considerarse como tal ya que capturando tramas es posible evadir dicha protección, de igual manera fue necesario efectuar dicha prueba.	Technitium Mac Address Changer	Con la herramienta Technitium Mac Address Changer, se identificó los clientes relacionados para luego ingresar a la red y constatar si es posible acceder a la red.	Activo

[40] Fuente: Metodología OWISAM, https://www.owisam.org/es/OWISAM-AU-001 último acceso: [11/08/2014]

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
4	Auditoría y Revisión Sub fase: Controles de Implementación	Pruebas sobre WPS[41]	Determinar que el dispositivo se encuentra habilitado el protocolo WPS. Este protocolo viene activado por defecto y al estar habilitado esta opción es susceptible a ataques de fuerza bruta.	Acrylic	Al ejecutar la herramienta Acrylic, revisar el parámetro WPS y WPS	Pasivo
5	Auditoría y Revisión Sub fase: Controles Técnicos	Interfaces administrativas expuestas a la red[42]	Identificar el acceso al dispositivo para su administración. Al estar habilitado el acceso de administración del dispositivo a partir de la web	IPScanner	IPScanner comprobar la configuración IP del gateway y acceder a través de un navegador. Entre las opciones puede ser por medio de un portal web o telnet, ssh o alguna herramienta situada en algún puerto en	Activo

[41] Fuente: Metodología OWISAM, https://www.owisam.org/es/OWISAM-AU-002 último acceso: [11/08/2014]

[42] Fuente: Metodología OWISAM, https://www.owisam.org/es/OWISAM-IF-002 último acceso: [11/08/2014]

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
			es vulnerable a que el atacante pueda acceder.		concreto.	
6	Auditoría y Revisión Sub fase: Controles Técnicos	Prueba Traceroute	Mapear los saltos de red hasta un host específico. Nos permite identificar la dirección IP del router para las siguientes pruebas.	Nmap o Consola de Windows	La herramienta Zenmap se revisó por medio de la pestaña Topology dónde permite ver gráficamente los saltos del router para salir a internet con el comando: nmap -- traceroute [IP destino] o sino en la Consola de Windows el comando: tracert [IP destino]	Activo
7	Auditoría y Revisión Sub fase: Controles Técnicos	Prueba APs/Router	Reconocer cuales son los puertos, servicios y protocolos de enrutamiento se encuentran abiertos/filtrados.	Nmap	Con los siguientes comandos: nmap -sS -sV -p 1-65535 –f –f –Pn –D [Ip router/Firewall] nmap -O -nP [Ip router] nmap –sA –p 1-65535 [Ip router/Firewall] nmap –n –vv –P0 –p256, 1080 [Ip	Activo

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
					router/Firewall] -sS: indica los servicios que se encuentran habilitados -sV: indica los versiones de los servicios habilitados - p: puertos de los servicios que utilizan 1 – 65535 son los puertos que pueden estar habilitados para la comunicación -Pn Permite ejecutar la instrucción sin realizar un ping al host (sin utilizar el protocolo ICMP) -O: Muestra el sistema operativo -sA: verifica si el Firewall contiene reglas que pueden filtrar el contenido de los puertos que están activos. -f y D: se utiliza para evadir al firewall y permita realizar el escaneo	

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
					-P0: deshabilita mensajes ICMP -vv: permite identificar la arquitectura del firewall	
8	Auditoría y Revisión Sub fase: Controles Técnicos	Análisis del solapamiento de redes en el mismo canal de comunicaciones[43]	Analizar si los rangos de frecuencia se encuentran saturados, esto sucede al configurar las redes inalámbricas en el mismo canal dentro del área de cobertura de la señal, lo puede ser el causante de interferencia y pérdida de datos en la transmisión.	Acrylic	El parámetro es Chan de la herramienta Acrylic.	Pasivo
9	Auditoría y Revisión	Verificación el nivel de	Identificar si la cobertura de la red se propaga o no	Acrylic	El parámetro es RSS de la herramienta Acrylic.	Pasivo

[43] Fuente: Metodología OWISAM, https://www.owisam.org/es/ OWISAM-CF-004 último acceso: [11/08/2014]

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
	Sub fase: Controles Técnicos	intensidad de señal o área de cobertura.[44]	dentro del perímetro de la institución, de acuerdo a los niveles de potencia. Es posible efectuar pequeñas denegaciones de servicio por un atacante y así dejar sin servicio a la institución.			
10	Auditoría y Revisión Sub fase: Controles Técnicos	Debilidades en el firmware del AP[45]	Determinar si los enrutadores inalámbricos, AP de cliente y tarjetas de red del cliente son compatibles con las versiones actuales del	N/A	Se consultó de páginas oficiales de los dispositivos para verificar si existe versiones actualizadas del firmware o si ha encontrado vulnerabilidades.	Activo

[44] Fuente: Metodología OWISAM, https://www.owisam.org/es/ OWISAM-CF-003 último acceso: [11/08/2014]

[45] Fuente: Metodología OWISAM, https://www.owisam.org/es/OWISAM-IF-001 último acceso: [11/08/2014]

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
			firmware, así los parches de seguridad se puedan implementar a medida que estén disponibles.			
11	Auditoría y Revisión Sub fase: Controles de Gestión	Pruebas sobre directivas y normativa[46]	Determinar el conjunto de buenas prácticas, que la institución destina para la seguridad de la red inalámbrica.	Encuestas	Se realizarán preguntas relacionadas con la seguridad perimetral, políticas de uso de redes inalámbricas, políticas de gestión y cambio de claves. Ver ejemplos de encuentras en los Anexos A, B y para presentación de reuniones revisar el Anexo C.	Activo
12	Análisis y Búsqueda	Análisis del protocolo SNMP en la red	Realizar el reconocimiento del uso del protocolo SNMP en la red y su respectiva versión.	Wireshark	Con la herramienta Wireshark se capturó una trama y luego se realizó el filtro snmp, para obtener información sobre la versión snmp 1 y 2 que son	Activo

[46] Fuente: Metodología OWISAM, https://www.owisam.org/es/Controles_OWISAM último acceso: [11/08/2014]

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
		inalámbrica			consideradas las más vulnerables actualmente.	
13	Análisis y Búsqueda	Análisis de protocolos de cifrado inseguro (WEP, TKIP,...)[47]	Verificar los protocolos de cifrado maneja los dispositivos, ya que dentro de cada uno de estos protocolos se manejan algoritmos con propósitos específicos.	Suite Aircrack	Con la suite aircrack-ng nos permite atacar la captura de tráfico que queremos descifrar. Los comandos que se van a utilizar son: ▪ 1: airmon-ng start wlan0 permite crear una interfaz de modo de monitor correspondiente al dispositivo wlan0. Esta nueva interfaz de modo de monitor será nombrado mon0. ▪ 2: airodump-ng mon0 permite encontrar la red inalámbrica para este caso de estudio.	Pasivo

[47]Fuente: Metodología OWISAM, https://www.owisam.org/es/OWISAM-CP-004 último acceso: [11/08/2014]

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
14	Explotación y Ataque	Captura y cracking de claves transmitidas en el proceso de autenticación [48].	Determinar si es posible realizar una captura y cracking de las contraseñas para acceder a la red inalámbrica.	WifiSlax Backtrack	Dentro del sistema operativo WifiSlax se utilizará la suite Aircrack y se procede a ejecutar los siguientes comandos:1:airodump-ng –c CANAL –bssid MACROUTER –w NOMBRE mon0. Permite observar a los usuarios conectados, los paquetes que estos envían, para capturar esos paquetes en un archivo o fichero, agregar el nombre del archivo. ▪ 2: aircrack-ng [nombreArchivo].cap permite obtener la contraseña de la red, se debe capturar el envío de algún paquete del cliente, suplantarlo y enviar varias peticiones	Activo

[48] Fuente: Metodología OWISAM, https://www.owisam.org/es/ OWISAM-AU-004 último acceso: [11/08/2014]

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
					al router para generar tráfico. ▪ 3: Aireplay-ng -0 5 -a MACROUTER –h MACCLIENTE mon0. Permite generar handshake manualmente. ▪ 4: aircrack-ng –a 2 –e WLAN_E5 –w dict.txt [nombreArchivo].cap Permite obtener la claver WPA/PSK de la red atacada.	
15	Explotación y Ataque	Detección de APs falsos[49]	Engañar al usuario y forzar su vinculación y conexión a ellos. Permite poner el escenario donde un atacante a través	Mdk3[50] Wireshark Acrylic	Dentro del sistema operativo WifiSlax se utilizó la herramienta Mdk3 y se ejecutó el siguiente comando: 1: mdk3 mon0 b –c 11 –n Prueba permite crear el nuevo AP falso con	Activo

[49] Fuente: Metodología OWISAM, https://www.owisam.org/es/OWISAM-FP-002 último acceso: [11/08/2014]

[50] Fuente: CL0UDSWXSEQURE, https://cl0udswxsequre.wordpress.com/2015/03/02/que-es-mdk3-y-para-que-sirve/último acceso: [11/08/2014]

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
			de APs falsos ataca a usuarios y gana acceso a la red interna de la institución. La detección de APs falsos al ser un ataque de forma activa realiza el análisis del inventario de los APs y encontrando su ubicación, al ser de forma pasiva realiza un análisis de comportamiento.		SSID llamado Prueba Con la herramienta Wireshark contatar que se existe tráfico del nuevo AP Con la herrameinta Acrylic confirmar la creación del AP con SSID llamado Prueba	
16	Explotación y Ataque	Pruebas de deautenticación[51]	Evitar que el cliente se pueda comunicar mientras esté enviando paquetes de	Airbase Wireshark	Dentro del sistema operativo WifiSlax se utilizó la Airbase[52] para realizar un levantamiento de red falsa para acceso	Activo

[51] Fuente: Metodología OWISAM, https://www.owisam.org/es/OWISAM-DS-001 último acceso: [11/08/2014]

#	NOMBRE DE LA SUB FASE ISSAF	NOMBRE DE LA PRUEBA	OBJETIVO Y RAZONES	HERRAMIENTA	PROCEDIMIENTO	TIPO DE ATAQUE
			comunicación, creando un AP falso.	Acrylic	a oros usuarios, libre, no necesita autenticación. Luego realizar la validación (Windows 7) Se cambió de Canales de mon0 y de wlan1 con los comandos: iwconfig wlan1 channel 6 iwconfig mon0 chanel 6 Finalmente se capturó tráfico en Wifislax con wireshark	

Tabla 2-5. Pruebas aplicadas a la institución[53]

[52] Fuente: AIRBASE-NG, https://underc0de.org/foro/wireless/airbase-ng/último acceso: [11/08/2014]

[53] Elaborado por: La autora en base a la recolección de información de las pruebas de ISSAF, OWISAM y OSSTMM.

2.1.2.2 Ejecución de las pruebas

Para la presentación de las pruebas se utiliza la plantilla propuesta por la metodología ISSAF[54], ver Tabla 2-6.

Nombre de prueba
Proceso
Pre-requisitos
Ejemplos/Resultados
Análisis/Conclusión/Observación
Contramedidas
Herramientas
Lecturas adicionales
Observaciones

Tabla 2-6. Presentación de plantilla de pruebas[55]

Desde la Tabla 2-7 hasta Tabla 2-15 se presenta una muestra (9/16) de vectores de prueba ejecutados los más relevantes con los resultados encontrados de una sola sede.

Para la ejecución de las pruebas se utilizaron las herramientas propuestas en el acápite 1.3 y no adicionales, debido a que las distribuciones WifiSlax y Backtrack cuentan con un arsenal de herramientas de penetración para red inalámbrica.

1. Descubrimiento activo de dispositivos y redes
Proceso
Descubrir los dispositivos inalámbricos que cumplen el estándar 802.11.X. Debido a que inicialmente se va a recolectar información de los dispositivos que están a nuestro

[54] Fuente: ISSAF versión 0.2.1, página 1192 -1195.

[55] Fuente: ISSAF versión 0.2.1, página 1192.

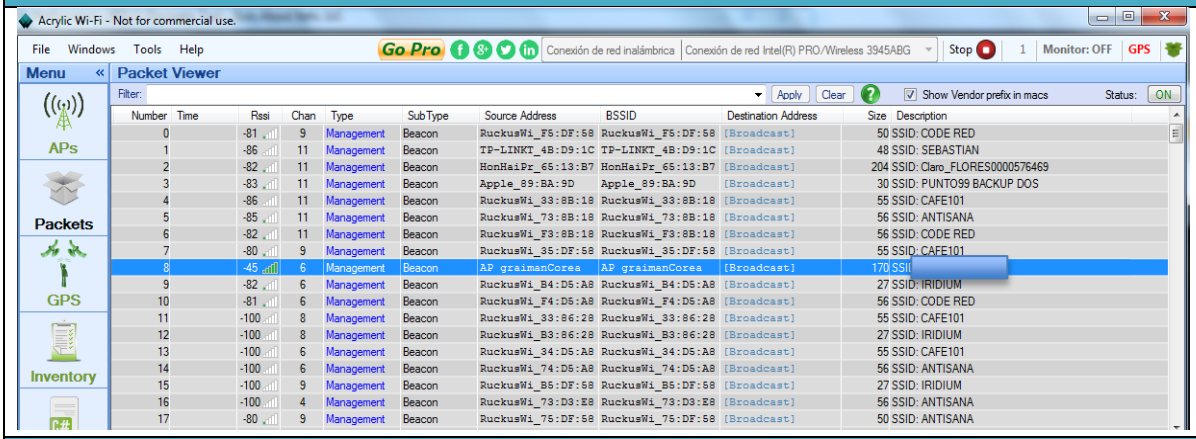
1. Descubrimiento activo de dispositivos y redes
alcance. Mostrar todas las redes inalámbricas presentes utilizando la herramienta Acrylic en la sección Packets.
Pre-requisitos
Tener instalado Acrylic.
Ejemplos/Resultados

Análisis/Conclusión/Observación
Se encuentra habilitados los beacons frames para acceder a la red inalámbrica, lo que posibilita la obtención de información del software y hardware del dispositivo.
Contramedidas
Revisar el plan de mitigación
Herramientas
Suite Aircrack 4.10 Acrylic_WiFi_Free_v2.2.5616.35860
Lecturas Adicionales
https://www.owisam.org/es/Descubrimiento_de_dispositivos_OWISAM-DI https://www.owisam.org/es/OWISAM-DI-005 https://www.owisam.org/es/OWISAM-DI-003
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Recolectar información Sub fase de la metodología ISSAF: N/A Modo de ataque: Pasivo

Tabla 2-7. Prueba Descubrimiento activo de dispositivos y redes[56]

2. Identificación de funcionalidades soportadas por el dispositivo
Proceso
Obtener información del dispositivo tales como: datos del fabricante, driver que está utilizando, la velocidad de transmisión, tiempo de respuesta, entre otros, con la herramienta Acrylic en la sección Packets.

[56] Elaborado por: La autora en base a las pruebas propuestas por la metodologia OWISAM.

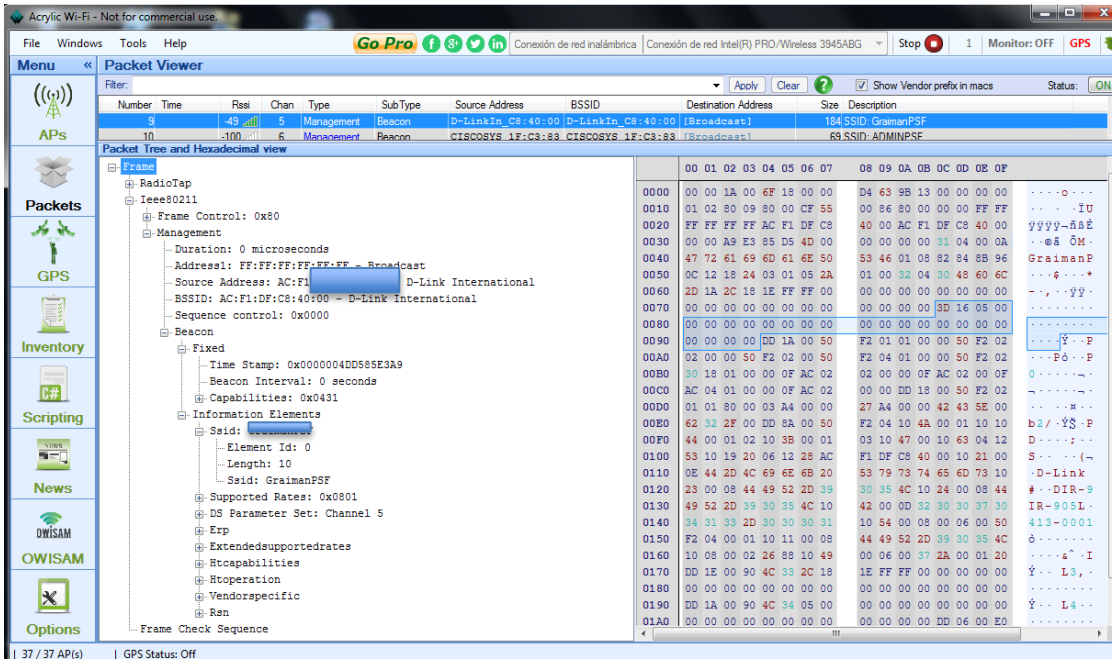
2. Identificación de funcionalidades soportadas por el dispositivo
Pre-requisitos
Tener instalado Acrylic.
Ejemplos/Resultados
SEDE 1 
Análisis/Conclusión/Observación
Por medio de la herramienta se pudo constatar información relevante al dispositivo.
Contramedidas
Revisar el plan de mitigación.
Herramientas
Acrylic_WiFi_Free_v2.2.5616.35860
Lecturas Adicionales
https://www.owisam.org/es/OWISAM-FP-002 https://www.owisam.org/es/Fingerprinting_OWISAM-FP
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Escaneo Sub fase de la metodología ISSAF: N/A Modo de ataque: Pasivo

Tabla 2-8. Prueba Identificación de funcionalidades soportadas por el dispositivo[57]

[57] Elaborado por: La autora en base a las pruebas propuestas por la metodologia OWISAM.

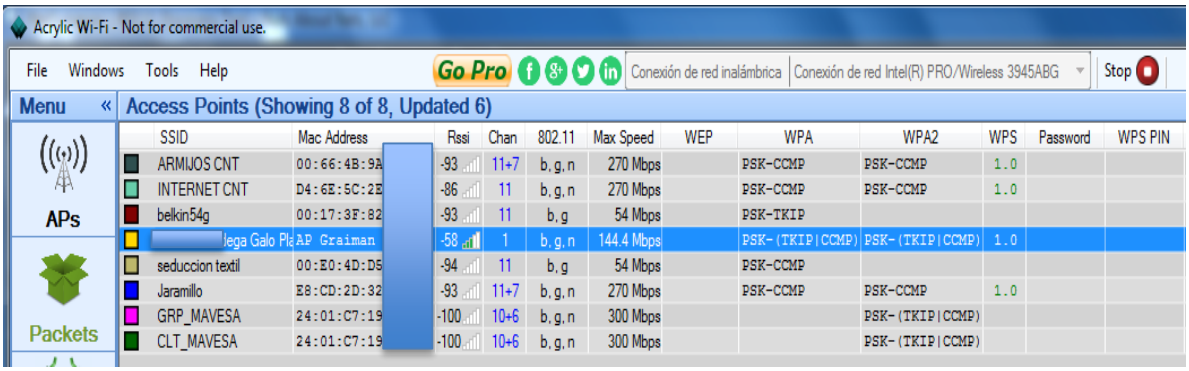
4. Pruebas sobre WPS
Proceso
Determinar que el dispositivo se encuentra habilitado el protocolo WPS. Este protocolo al estar habilitado esta opción es susceptible a ataques de fuerza bruta, viene activado por defecto. Con la herramienta Acrylic revisar el r
Pre-requisitos
Tener instalado Acrylic.
Ejemplos/Resultados

Análisis/Conclusión/Observación
En la mayoría de las sedes los APs se encuentran habilitados el protocolo WPS y WPS PIN.
Contramedidas
Revisar en el plan de mitigación
Herramientas
Acrylic_WiFi_Free_v2.2.5616.35860
Lecturas Adicionales
https://www.owisam.org/es/OWISAM-AU-002
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Auditoría y Revisión Sub fase de la metodología ISSAF: Controles de Implementación Modo de ataque: Pasivo

Tabla 2-9. Pruebas sobre WPS[58]

5. Interfaces administrativas expuestas a la red
Proceso
Identificar el mecanismo de acceso que tiene la institución para la administración del dispositivo inalámbrico. Para la realización de esta tarea se puede utilizar IPScanner comprobar la configuración IP del gateway y acceder a través de un navegador.

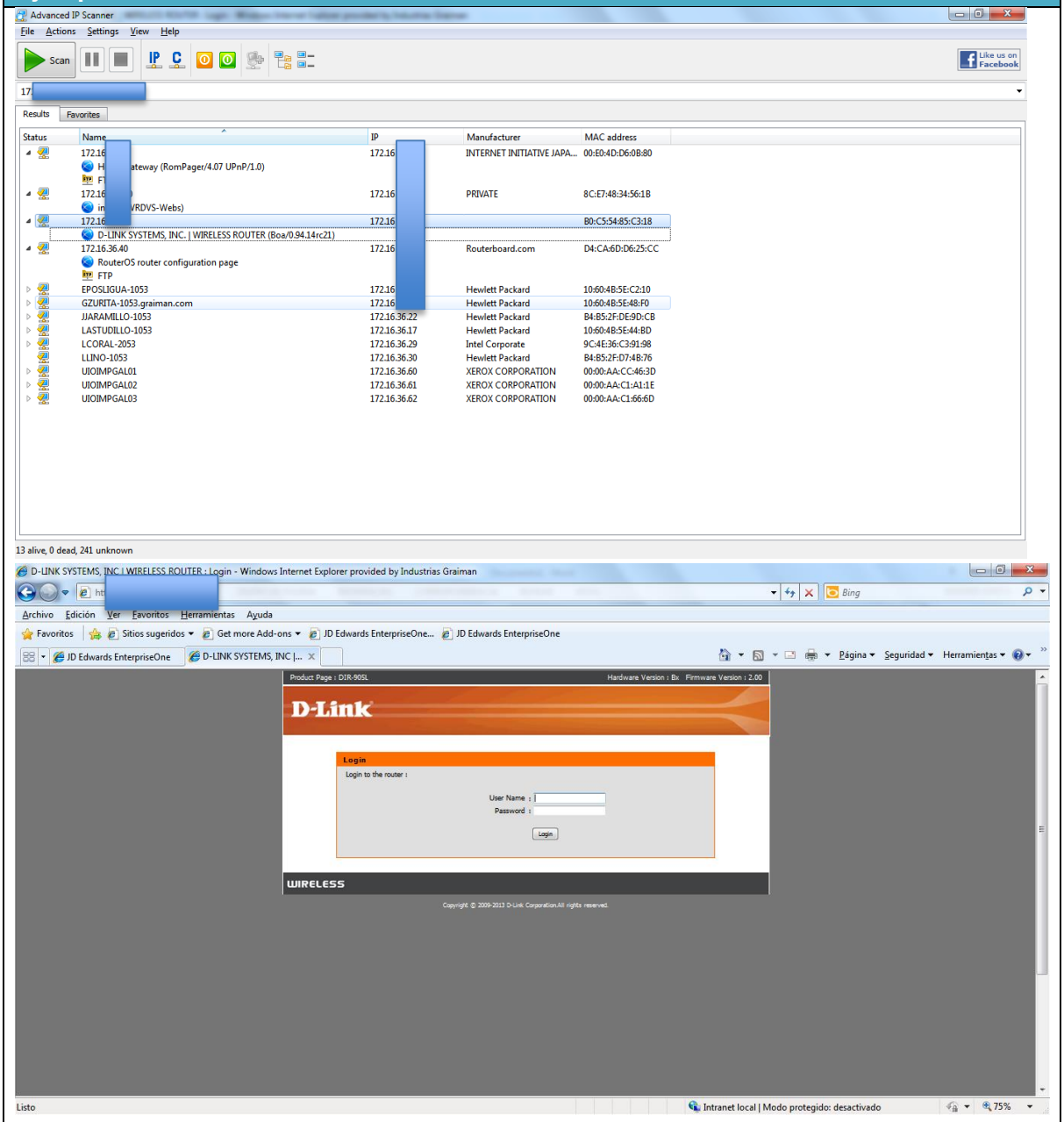
[58] Elaborado por: La autora en base a las pruebas propuestas por la metodologia OWISAM.

5. Interfaces administrativas expuestas a la red

Pre-requisitos

Tener instalado Ipscanner.

Ejemplos/Resultados



Análisis/Conclusión/Observación

En todas las sedes se pudo constatar que se encuentra habilitado el acceso para la administración del dispositivo inalámbrico al estar habilitado es vulnerable a que el atacante pueda acceder.

Contramedidas

Revisar el plan de mitigación.

Herramientas

IPscanner versión 3.34.

Lecturas Adicionales

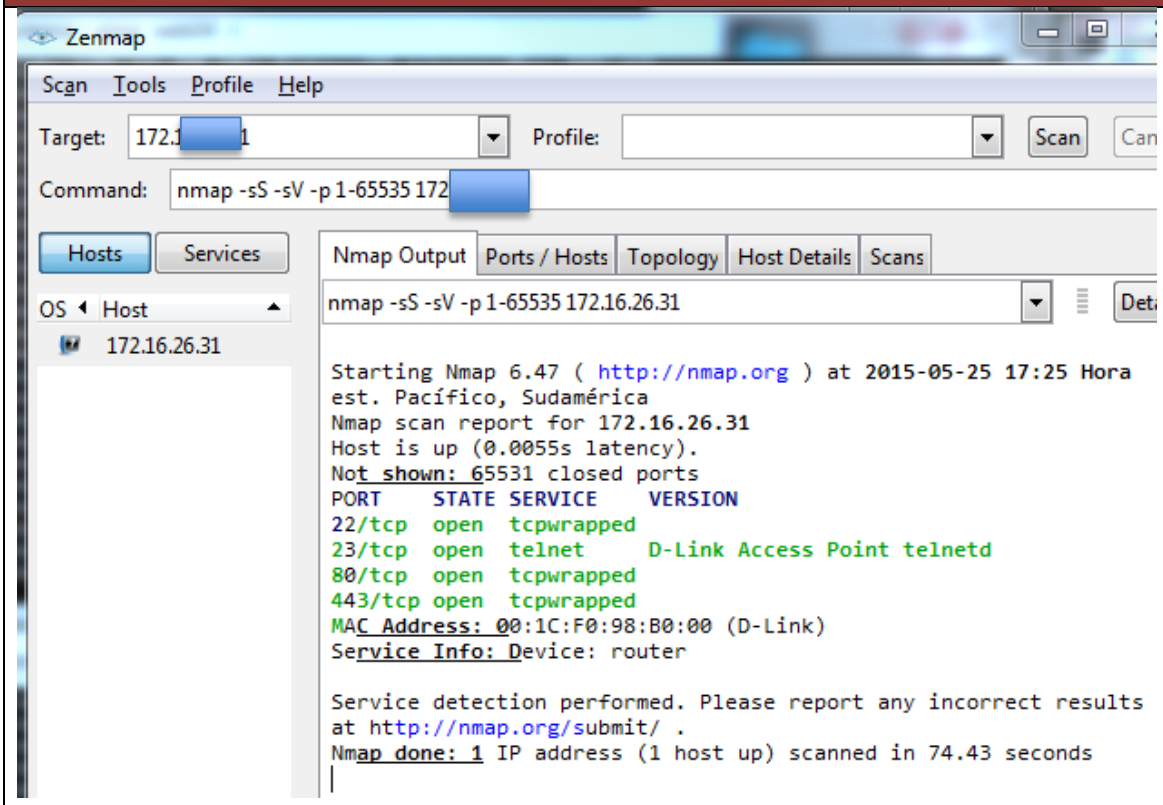
5. Interfaces administrativas expuestas a la red
https://www.owisam.org/es/OWISAM-IF-002 http://nmap.org/ http://www.routerpasswords.com/ http://www.thc.org/thc-hydra/
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Auditoria y Revisión Sub fase de la metodología ISSAF: Controles Técnicos Modo de ataque: Pasivo

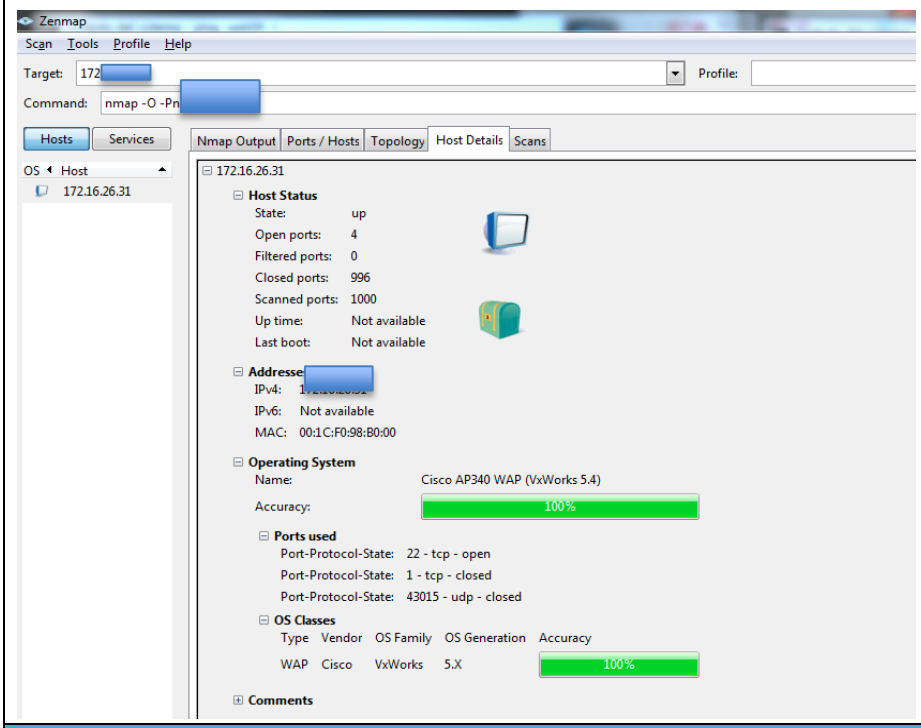
Tabla 2-10. Pruebas Interfaces administrativas expuestas a la red[59]

7. Prueba al APs/Router
Proceso
Reconocer qué puertos, servicios y protocolos de enrutamiento se encuentran abiertos/filtrados. Esta información se recolectará con la herramienta nmap. Con los siguientes comandos: nmap -sS -sV -p 1-65535 –f –Pn –D [Ip router] nmap -O -nP [Ip router] nmap –sA –p 1-65535 [Ip router] nmap –n –vv –P0 –p256, 1080 [Ip router] El significado es el siguiente - sS: indica los servicios que se encuentran habilitados - sV: indica los versiones de los servicios habilitados - p: puertos de los servicios que utilizan - 1 – 65535 son los puertos que pueden estar habilitados para la comunicación - Pn Permite ejecutar la instrucción sin realizar un ping al host (sin utilizar el protocolo ICMP) - O: Muestra el nombre del sistema operativo - sA: verifica si el Firewall contiene reglas que pueden filtrar el contenido de los puertos que están activos. - f y D: se utiliza para evadir al firewall y permita realizar el escaneo - P0: deshabilita mensajes ICMP - vv: permite identificar la arquitectura del firewall
Pre-requisitos
Obtener la dirección IP del router puede ser con la prueba traceroute. Tener instalado ZeNmap 6.47.
Ejemplos/Resultados

[59] Elaborado por: La autora en base a las pruebas propuestas por la metodologia ISSAF.

7. Prueba al APs/Router





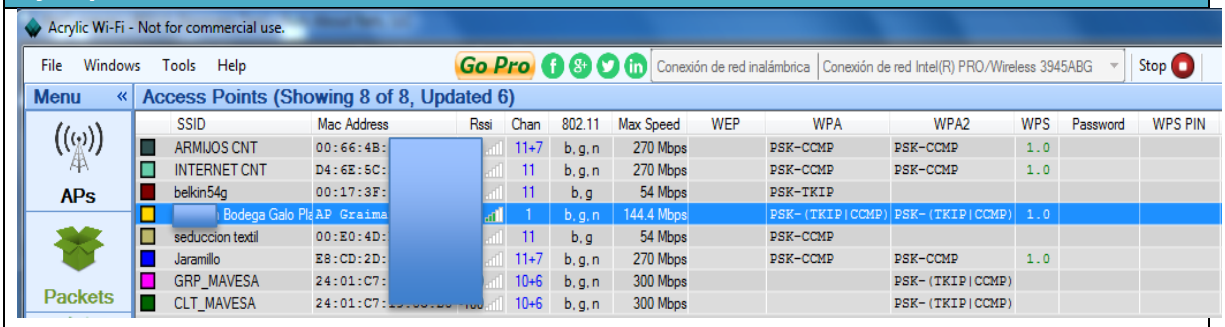
Análisis/Conclusión/Observación

"Not shown: 65531 closed protocols", esto quiere decir que se encuentran cerrados 65531 puerto lo que es beneficioso y denota que tienen precaución en este sentido.

El puerto 23 está abierto pero indican que la administración del dispositivo inalámbrico es

7. Prueba al APs/Router
a través de la web y no utilizan este puerto.
Contramedidas
Revisar el plan de mitigación
Herramientas
Tener instalado ZeNmap versión 6.47.
Lecturas Adicionales
Esta prueba fue realizada con las siguientes características: Metodología ISSAF versión 2.0.1 páginas 220, 222, 226, 235, 238, 447. Tesis de Análisis de riesgos y vulnerabilidades de la infraestructura tecnológica de la secretaría nacional de gestión de riesgos utilizando metodologías de ethical hacking
Observaciones
Fase de metodología ISSAF: Auditoria y Revisión Sub fase de la metodología ISSAF: Controles Técnicos Modo de ataque: Activo

Tabla 2-11. Pruebas al APs/Router[60]

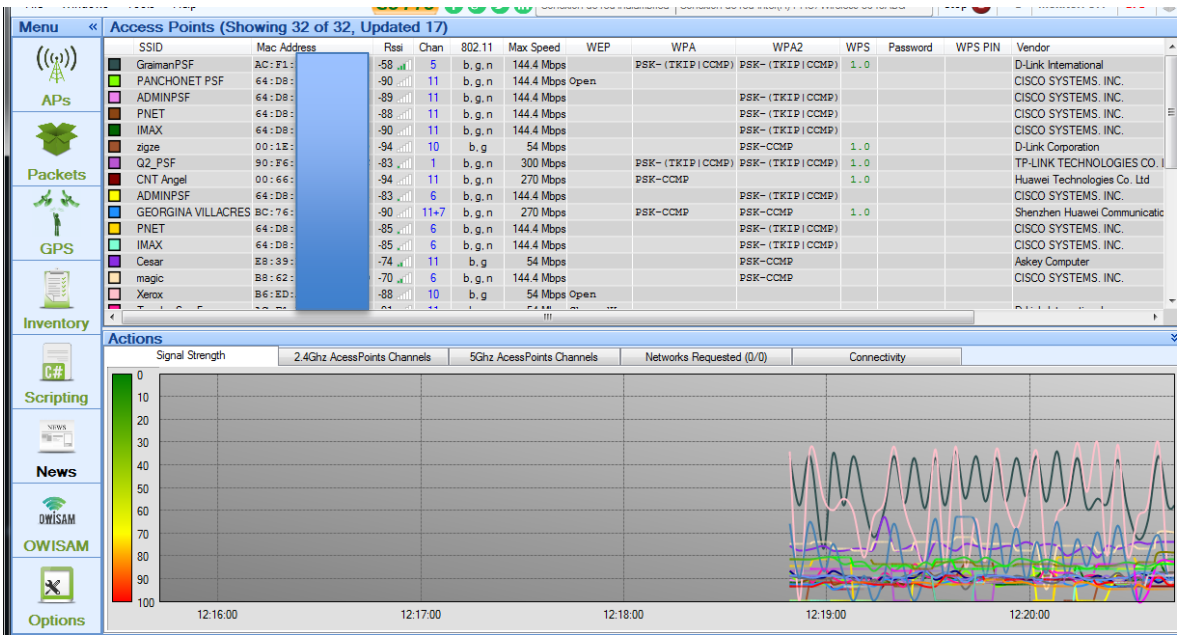
8. Análisis del solapamiento de redes en el mismo canal de comunicaciones
Proceso
Analizar si los rangos de frecuencia se encuentran saturados. La herramienta debe examinar el espectro de 2.4 GHz y 5 GHz para que examine los canales en los cuales se transmite la red inalámbrica así como el solapamiento entre ellas. Con la herramienta Acrylic revisar el parámetro Chan.
Pre-requisitos
Tener instalado Acrylic.
Ejemplos/Resultados

Análisis/Conclusión/Observación
Con el análisis realizado denota que existen varias redes vecinas a la red de la institución han se fueron configuradas las redes inalámbricas en el mismo canal dentro del área de un mismo cobertura de la señal (no en todas las redes), lo puede causar interferencia y pérdida de datos en la transmisión.
Contramedidas

[60] Elaborado por: La autora en base a las pruebas propuestas por la metodologia ISSAF.

8. Análisis del solapamiento de redes en el mismo canal de comunicaciones
Revisar el plan de mitigación
Herramientas
Tener instalado Acrylic_WiFi_Free_v2.2.5616.35860
Lecturas Adicionales
https://www.owisam.org/es/Cifrado_de_las_comunicaciones_OWISAM-CP https://www.owisam.org/es/OWISAM-CF-004 https://www.owisam.org/es/OWISAM-CF-003
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Análisis de seguridad Sub fase de la metodología ISSAF: Controles Técnicos - Pruebas de infraestructura Modo de ataque: Pasivo

Tabla 2-12. Pruebas Análisis del solapamiento de redes en el mismo canal de comunicaciones[61]

9. Verificación el nivel de intensidad de señal o área de cobertura
Proceso
Identificar si la cobertura de la red se propaga o no dentro del perímetro de la institución, de acuerdo a los niveles de potencia. El parámetro es RSS y en la sección Actions de la herramienta Acrylic.
Pre-requisitos
Tener instalado Acrylic.
Ejemplos/Resultados
SEDE 1



[61] Elaborado por: La autora en base a las pruebas propuestas por la metodologia OSSTMM y OWISAM.

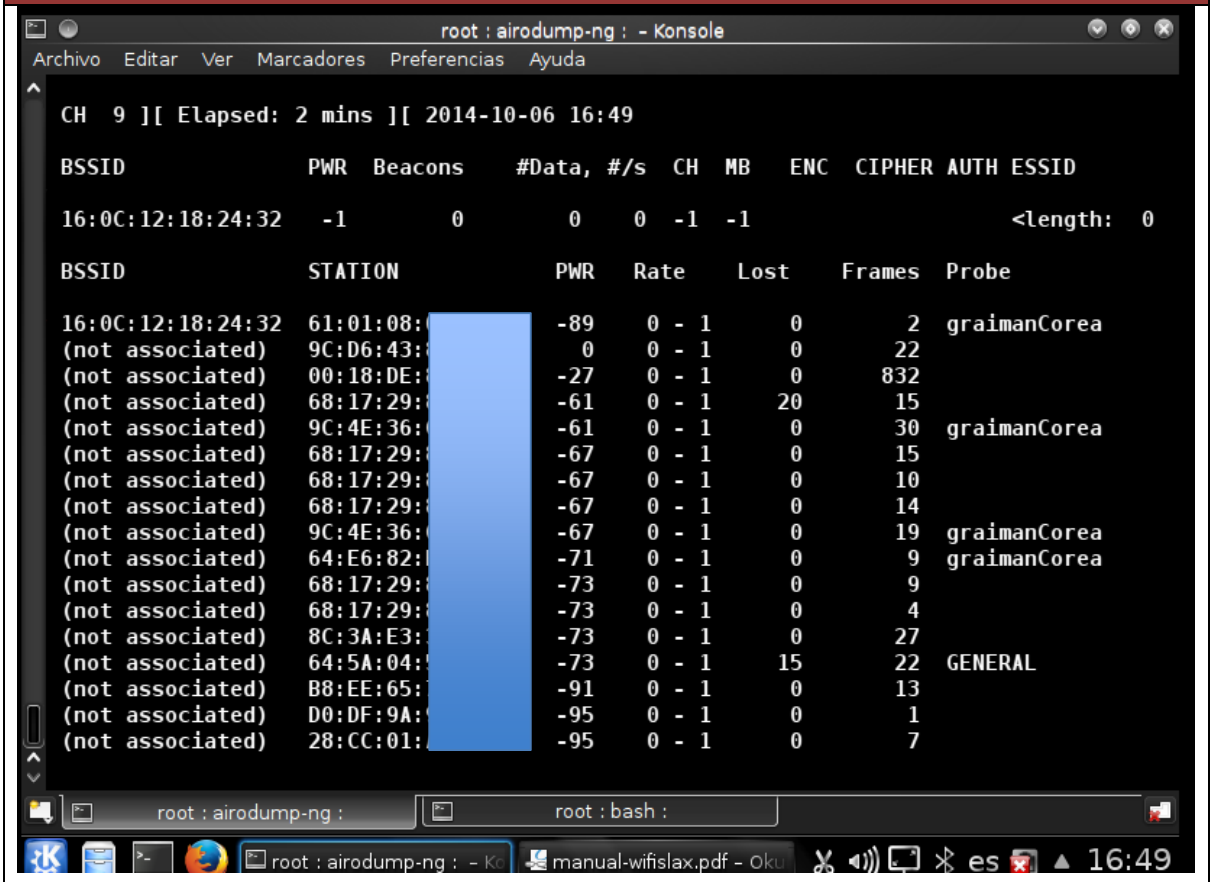
9. Verificación el nivel de intensidad de señal o área de cobertura
Análisis/Conclusión/Observación
Con el análisis realizado denota que existen varias redes vecinas a la red de la institución han se fueron configuradas las redes inalámbricas en el mismo canal dentro del área de un mismo cobertura de la señal (no en todas las redes), lo puede causar interferencia y pérdida de datos en la transmisión. Se complementa con la anterior prueba.
Contramedidas
Revisar el plan de mitigación
Herramientas
Acrylic_WiFi_Free_v2.2.5616.35860
Lecturas Adicionales
https://www.owisam.org/es/Cifrado_de_las_comunicaciones_OWISAM-CP https://www.owisam.org/es/OWISAM-CF-004 https://www.owisam.org/es/OWISAM-CF-003
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Análisis de seguridad Sub fase de la metodología ISSAF: Controles Técnicos - Pruebas de infraestructura Modo de ataque: Pasivo

Tabla 2-13. Pruebas Verificación el nivel de intensidad de señal o área de cobertura[62]

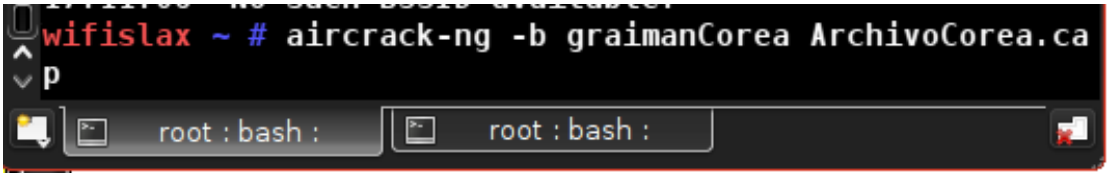
14. Captura y cracking de claves transmitidas en el proceso de autenticación
Proceso
Determinar si es posible realizar una captura y cracking de las contraseñas para acceder a la red inalámbrica. Se utilizará la suite Aircrack
Pre-requisitos
Tener el sistema operativo Wifislax versión 4.10 donde dentro de ella vienen embebidos varias herramientas destinadas para el análisis y auditoria de redes inalámbricas. Uno de ellos que fueron utilizados, es suite de Aircrack. (Wifislax es un sistema operativo que puede ser booteable como liveCD).
Ejemplos/Resultados
Dentro del sistema operativo WifiSlax se utilizará la suite Aircrack y se procede a ejecutar los siguientes comandos: 1: airodump-ng –c CANAL–w Nombre –b MACROUTER mon0. Con este comando se puede observar los usuarios conectados, los paquetes que estos envían, para capturar esos paquetes en un archivo o fichero, agregar el nombre del archivo. `wifislax ~ # airodump-ng -c 6 -w capturaCorea -b 16:[redacted]:32 mon0` resultado

[62] Elaborado por: La autora en base a las pruebas propuestas por la metodologia OSSTMM y OWISAM.

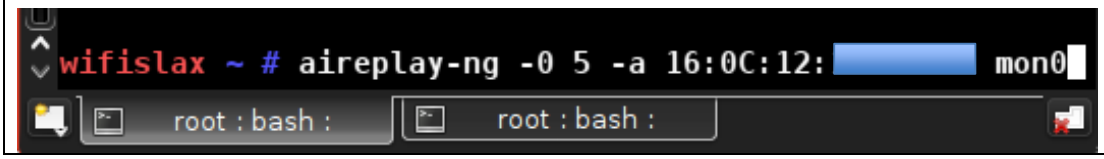
14. Captura y cracking de claves transmitidas en el proceso de autenticación



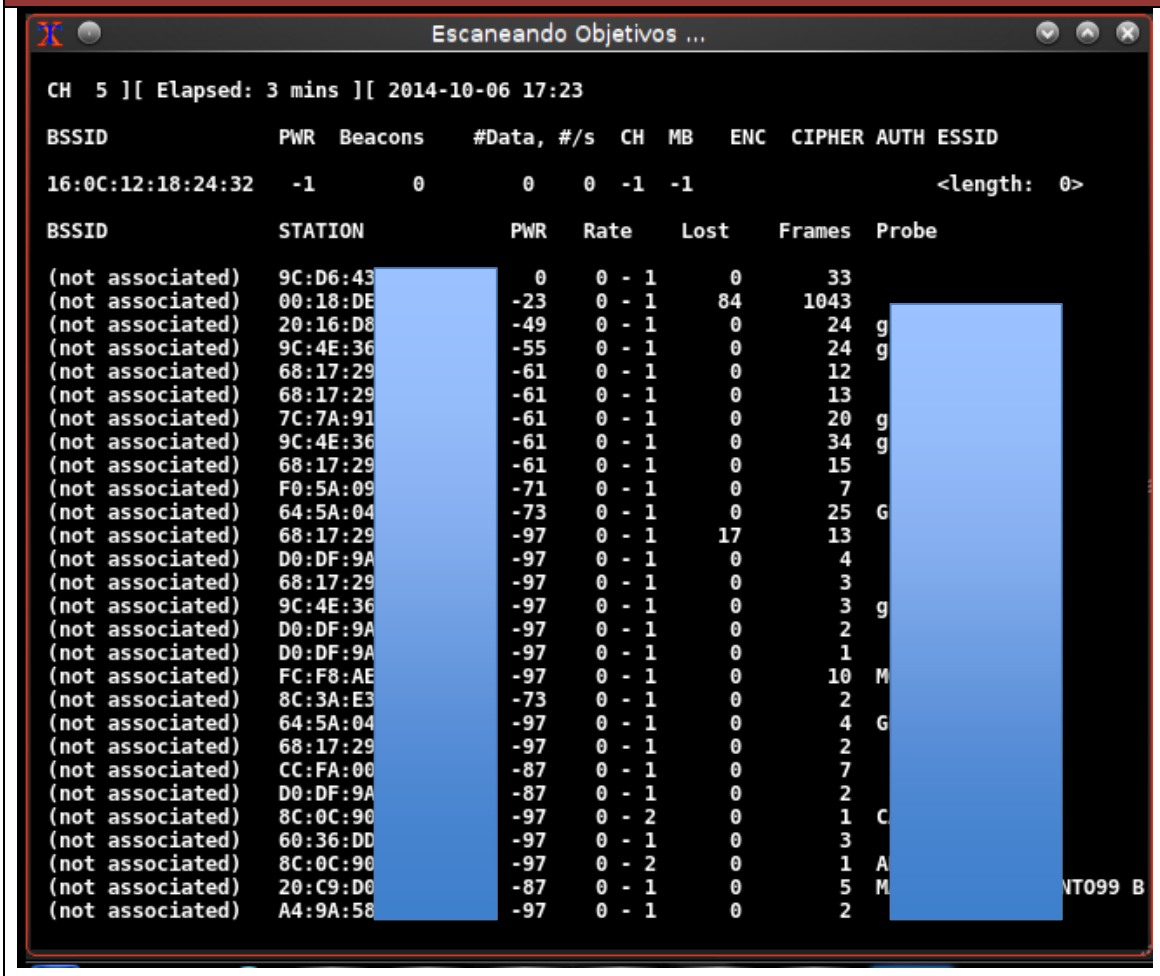
2: aircrack-ng [nombreArchivo].cap permite obtener la contraseña de la red, se debe capturar el envío de algún paquete del cliente, suplantarlo y enviar varias peticiones al router para generar tráfico.



3: Aireplay-ng -3 –b MACROUTER –h MACCLIENTE mon0. Permite generar handshake manualmente.



14. Captura y cracking de claves transmitidas en el proceso de autenticación



4: aircrack-ng –a 2 –e WLAN_E5 –w dict.txt [nombreArchivo].cap. Permite obtener la claver WPA/PSK de la red atacada

Análisis/Conclusión/Observación

Se pudo obtener las contraseñas cuando los dispositivos tenían cifrado WEP. En cambio para el cifrado WPA-WPA2, no se obtuvo el mismo resultado se utilizó diccionarios proporcionados en la red de internet, se demoró en analizar 4 horas y aún así no mostraba ningún resultado.

Contramedidas

Revisar en el plan de mitigación

Herramientas

Suite Aircrack 4.10.

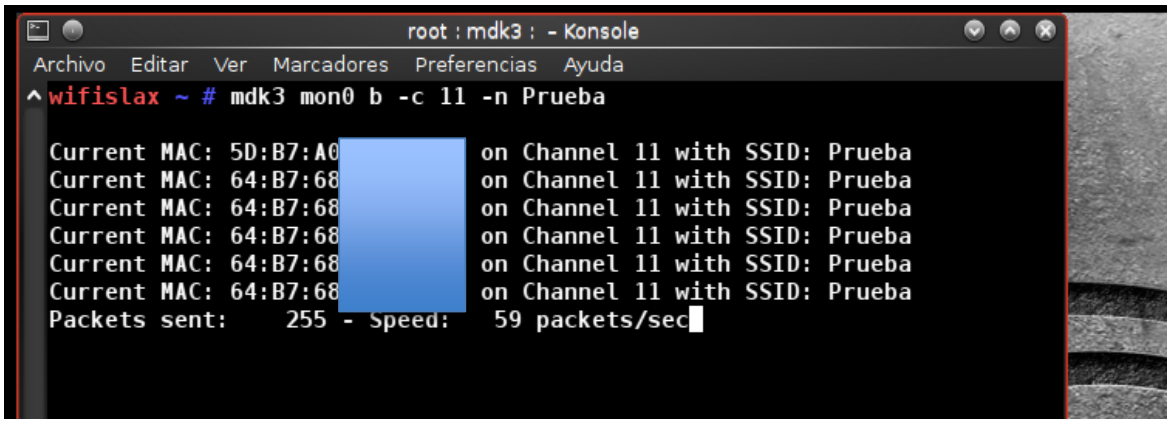
Lecturas Adicionales

https://www.owisam.org/es/OWISAM-AU-004

Observaciones

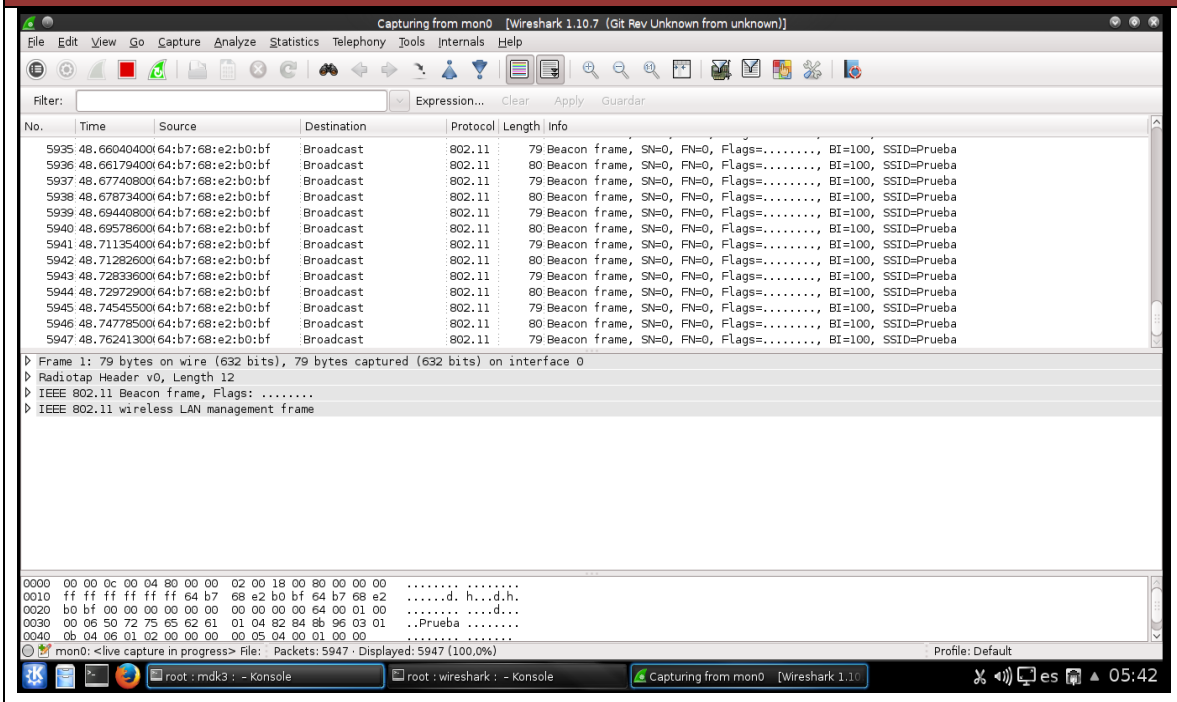
Esta prueba fue realizada con las siguientes características:
Fase de metodología ISSAF: Explotación y Ataque
Sub fase de la metodología ISSAF: N/A
Modo de ataque: Activo

Tabla 2-14. Prueba Captura y cracking de claves transmitidas en el proceso de autenticación[63]

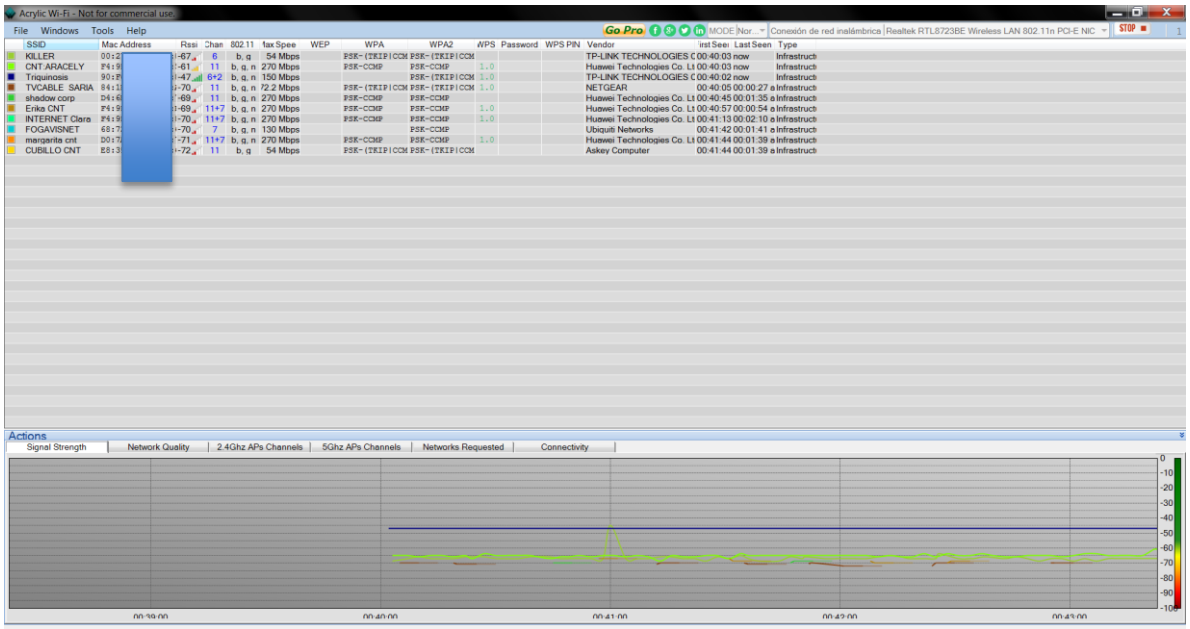
15. Detección de APs falsos
Proceso
Engañar al usuario y forzar su vinculación y conexión a ellos. Permite poner el escenario donde un atacante a través de APs falsos ataca a usuarios y gana acceso a la red interna de la institución. La detección de APs falsos al ser un ataque de forma activa realiza el análisis del inventario de los APs y encontrando su ubicación, al ser de forma pasiva realiza un análisis de comportamiento.
Pre-requisitos
Tener el sistema operativo Wifislax versión 4.10 donde dentro de ella vienen embebidos varias herramientas destinadas para el análisis y auditoria de redes inalámbricas. Uno de ellos que fueron utilizados, es suite de Aircrack. (Wifislax es un sistema operativo que puede ser booteable como liveCD). Tener instalado Wireshark para analizar los paquetes. Tener instalado Acrylic para analizar las redes inalámbricas presentes.
Ejemplos/Resultados
1: mdk3 mon0 b –c 11 –n Prueba Permite crear el AP falso con SSID llamado prueba    En la herramienta Wireshark se puede observar que está creada el AP falso ya que está enviado tramas.

[63] Elaborado por: La autora en base a las pruebas propuestas por la metodologia OSSTMM y OWISAM.

15. Detección de APs falsos



Pero en la herramienta Acrylic se puede ver que no reconoce en AP falso creado.



Análisis/Conclusión/Observación

Esta prueba consiste en captar la conexión del cliente y permitirnos tomar las claves o información que podamos obtener.

Esta prueba no tuvo éxito en la institución debido a que para la prueba, la autora no cuenta con el chipset (tarjeta para auditoría de red inalámbrica) respectiva para la ejecución de la prueba.

Contramedidas

Revisar el plan de mitigación

Herramientas

Mdk3, Wireshark, Acrylic las últimas versiones.

15. Detección de APs falsos
Lecturas Adicionales
https://www.owisam.org/es/OWISAM-FP-002 https://www.owisam.org/es/OWISAM-CT-001 https://www.owisam.org/es/Fingerprinting_OWISAM-FP
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Explotación y Ataque Sub fase de la metodología ISSAF: N/A Modo de ataque: Activo

Tabla 2-15.Prueba Detección de Aps Falsos[64]

El resultado de las pruebas ejecutadas se clasificará en las vulnerabilidades presentes y serán descritas en el acápite 2.2.4.

Para más detalle sobre los resultados encontrados, referirse al Anexo G.

2.2 ANÁLISIS DE RIESGOS DE LA RED INALÁMBRICA

Independiente de sea cual sea el negocio, los objetivos de la alta dirección es reducir costos y aumentar su rentabilidad. La información sensible y propia del negocio no puede estar al alcance de personal no autorizado. Por lo tanto las responsabilidades del departamento de TI son:

- La información viaje a través de equipos fiables.
- El mantenimiento de los sistemas de Información.
- Compra de nuevos dispositivos de la red.
- Evaluaciones de seguridad de la red periódicas.
- Plan de mitigación de posibles debilidades adquiridas.

El departamento de TI debe demostrar la justificación de costo-beneficio y el ROI (retorno de la inversión) en un nivel aceptable.

“Riesgo se puede definir como la pérdida potencial sufrida por la empresa como resultado de un evento no deseado que se traduce en una pérdida, ya sea de negocios o causa la interrupción de las operaciones comerciales…

El proceso de evaluación de riesgos aplicado al presente caso de estudio es siguiente:

- La comprensión de los objetivos de negocio estratégicos.

[64] Elaborado por: La autora en base a las pruebas propuestas por la metodologia OWISAM.

- Identificar los procesos clave del negocio que ayudan a la institución a alcanzar sus objetivos estratégicos de negocio.
- Comprender el papel del departamento de TI.
- Identificación del activo crítico dentro del negocio que puedan verse afectadas por amenazas.
- Identificación de amenazas que puede hacer frente con independencia de su probabilidad de ocurrencia.
- Identificación de vulnerabilidades.
- Priorización de riesgos.
- Un plan de tratamiento de riesgos y acción para mitigar los riesgos".[65]

Para el análisis del riesgo se definirán inicialmente los activos críticos, amenazas, probabilidad de ocurrencias y vulnerabilidades. La clasificación de la información fue elaborada en conjunto con el administrador de la red inalámbrica de la institución.

2.2.1 IDENTIFICACIÓN DEL ACTIVO CRÍTICO

La identificación de activos críticos permite reconocer cuáles son los activos que deben ser protegidos. En la caracterización de la empresa (ver el acápite 1.1.1) se determinó que el activo crítico a ser analizado es la red inalámbrica.

En función a entrevistas realizadas al administrador de la red y a la recolección de información, se pudo determinar características técnicas de la red inalámbrica, ver Tabla 2-16:

Características técnicas	Descripción
Tipo de red inalámbrica	Estándar "IEEE 802.11 a, b y g"
SSID configurado por defecto	No
Posee autenticación RADIUS	No
Mecanismo de autenticación	WPA 2 Personal y Enterprise
Tipo de encriptación	TKIP ó AES
Responsable de su administración	Administrador de la red
Longitud de clave	10 dígitos

[65] Fuente: ISSAF versión 0.2.1, página 90.

Características técnicas	Descripción
Control de acceso a la administración	Si
SSIDD Broadcast activo	Si
Cuenta con hostspots y portales cautivos	No cuenta

Tabla 2-16. Características de la red inalámbrica[66]

Cabe aclarar que no se realizará un análisis del impacto económico que conlleva la interrupción de alguno de los servicios o aplicaciones descritas en el acápite 1.1.1.2 a través de la red inalámbrica, ya que no corresponde al alcance definido en el presente proyecto de titulación.

2.2.2 IDENTIFICACIÓN DE AMENAZAS

Las amenazas consideradas se tomarán como referencia de la norma NTE INEN-ISO/IEC 27005:2012 ver el listado completo en el Anexo I.

NTE INEN-ISO/IEC 27005:2012 es igual a la ISO 27005:2008, esta norma explica cuáles serían las pautas para realizar una gestión del riesgo de la seguridad de la información, está diseñada para que facilite la implementación de la seguridad de la información desde el enfoque de gestión de riesgo.

Amenaza es un fenómeno que tiene el potencial para causar daño y poner en peligro a un grupo de personas o cosas o al ambiente. Las amenazas responden a la pregunta ¿qué puede pasar?:

- Catástrofes Naturales, fueron causados por la naturaleza, ejemplo: Inundaciones, terremotos, derrumbes, deslizamientos, avalanchas, tormentas eléctricas, contaminación y otros eventos.
- Eventos Humanos, fueron causados por seres humanos, como actos intencionales (ex empleados, crackers, hackers) o no intencionales (entrada de datos involuntaria, curiosos, personal).
- Amenazas lógicas, son programas que son utilizadas para dañar la red (puede haber puertas traseras, software incorrecto, virus, pocas herramientas de seguridad entre otros…)

Las amenazas que se ajustaron para este caso de estudio son:

---

[66] Elaborado por: La autora en base a la recolección de información de características de la red inalámbrica.

- Acceso no autorizado a la red
- Código malicioso
- Contaminación
- Denegación de Servicio
- Deterioro de soportes
- Escuchas encubiertas
- Espionaje
- Falla en los vínculos de comunicación
- Fallas en equipos
- Falta de políticas de seguridad
- Fraude
- Identidad de usuario camuflada
- Incorrecta configuración en los dispositivos inalámbricos
- Incorrecta configuración a la red inalámbrica
- Incorrecto mantenimiento a la red inalámbrica
- Ingeniería social
- Interceptación de información
- Pérdida de servicios soporte
- Robo

2.2.3 PROBABILIDAD DE OCURRENCIA

La probabilidad indica la posibilidad de que ocurra o no la amenaza. En la Tabla 2-17 presenta el nivel de posibilidad que ocurra las amenazas del acápite 2.2.2.

Valoración asignada	Probabilidad	Descripción
5	Casi seguro	Muy alta, puede ocurrir al menos varias veces al año
4	Probable	Alta, pueda surgir dos veces por año
3	Posible	Posible, pueda surgir al menos una vez en un período de 1 a 5 años
2	Casi probable	No es imposible, pero es probable que ocurra en los próximos 5 – 10 años

Valoración asignada	Probabilidad	Descripción
1	Rara vez	Muy bajo, muy poco probable durante los próximos 10 años

Tabla 2-17. Probabilidad de ocurrencia[67]

2.2.4 IDENTIFICACIÓN DE VULNERABILIDADES

La vulnerabilidad son debilidades en un sistema donde permite a cualquier atacante violar la confidencialidad, disponibilidad, integridad a la información de una empresa. Al no cumplir los objetivos de seguridad, estas serían las consecuencias:

- Integridad, se refiere a que la información será protegida contra modificaciones incorrectas.
- Disponibilidad, al no estar disponible el activo crítico de la institución para sus usuarios finales,
- Confidencialidad, se refiere a la protección de la información de divulgación no autorizada.

Las vulnerabilidades encontradas de acuerdo a las pruebas aplicadas y sus consecuencias en la institución se detalla en la Tabla 2-18:

Prueba	Vulnerabilidades
1. Descubrimiento activo de dispositivos y redes	Identificación de dispositivos mediante técnicas de descubrimiento activo
	Beacom frames habilitados
2. Identificación de funcionalidades soportadas Por el dispositivo	Obtención de información sobre el hardware y software.
	Configuración incorrecta.
	Susceptibilidad del equipamiento a la humedad y a la contaminación
3. Detección de protección de acceso basado en MAC	Autenticación contra redes inalámbricas

[67] Fuente: ISSAF versión 0.2.1, página 98.

Prueba	Vulnerabilidades
4. Pruebas sobre WPS	Acceso no autorizado a redes inalámbricas
	Debilidad de seguridad en la red inalámbrica
5. Interfaces administrativas expuestas a la red	Acceso no autorizado e interceptación de tráfico.
	Ausencia de validación de certificados.
6. Prueba Traceroute	Direcciónes Ips visibles
7. Prueba al APs/Router/Firewall	Acceso a segmentos de red restringidos.
8. Análisis del solapamiento de redes en el mismo Canal de comunicaciones	Degradación de la calidad del servicio.
9. Verificación el nivel de intensidad de señal O área de cobertura	Área de cobertura excesiva.
	Emisión de señal de clientes no autorizados
10. Debilidades en el firmware del AP	Robo de credenciales y acceso no autorizado.
	Debilidades en elementos de arquitectura o software.
11. Pruebas sobre directivas y normativa	Dispositivos que no cumplen el estándar / propietarios
	Detección de dispositivos emitiendo en frecuencias restringidas.
	No cuentan con política de uso/restricción de uso de redes inalámbricas
	No cuentan con política de configuración de dispositivos.
	No cuentan con política de gestión y cambio de claves
	No cuentan con una verificación de inventario de dispositivos autorizados
	Ausencia de sistemas de monitorización.

Prueba	Vulnerabilidades
12. Análisis del protocolo SNMP en la red inalámbrica	Permite la inyección de código malicioso
13. Análisis de protocolos de cifrado inseguro (WEP, TKIP,...)	Debilidad de seguridad en la red inalámbrica.
	Interceptación de comunicaciones
	Obtención de información sensible.
14. Captura y cracking de claves transmitidas en el Proceso de autenticación	Credenciales débiles.
15. Detección de APs falsos	Intrusos en redes Wi-Fi.
16. Pruebas de deautenticación	Interceptación de credenciales de autenticación.
	Ataques a la disponibilidad del servicio.
	Bloqueo de cuentas.
	Suplantación de punto de acceso y DOS.
	Degradación del servicio.

Tabla 2-18. Vulnerabilidades presentes[68]

"Pero una cosa sí que es cierta, que exista una vulnerabilidad no significa que se produzca un daño en el equipo de forma automática. Es decir, la computadora tiene un punto flaco, pero no por eso va a fallar, lo único que ocurre es que es posible que alguien ataque el equipo aprovechando ese punto débil"[69]

2.2.5 ANÁLISIS DEL RIESGOS

Luego de identificado los posibles problemas, la siguiente etapa es determinar el impacto que éstas producen en la institución. Para ello se realiza el análisis del impacto en función a los tres objetivos de seguridad: Integridad, Disponibilidad y Confidencialidad.

---

[68] Elaborado por: La autora en base a la metodologia OWISAM.

[69] Fuente: http://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo#sthash.pJ8hiIHr.LEi5HB2N.dpuf último acceso: 22/08/2014

2.2.5.1 Análisis del impacto

"Impacto" describe pérdida o degradación de cualquiera de los siguientes tres objetivos de seguridad: integridad, disponibilidad y confidencialidad. Al no cumplir los objetivos de seguridad, estas serían las consecuencias:

- Pérdida de integridad, la integridad se pierde si se realizan cambios no autorizados en el sistema de datos o por cualquier acto intencional o accidental. Si la pérdida de sistema o integridad de los datos no se corrige o datos dañados podría causar inexactitud, fraude o decisiones erróneas.
- Pérdida de disponibilidad, al no estar disponible el activo crítico de la institución para sus usuarios finales, la misión de la organización puede verse afectada, en el rendimiento de los usuarios finales de sus funciones.
- Pérdida de confidencialidad, se refiere a la protección de la información de su divulgación no autorizada.

En la Tabla 2-19 indica la valoración del impacto de una vulnerabilidad en cualquiera de los tres tipos de impacto:

Valoración del impacto	Valor asignado
Afecta	2
No afecta	0

Tabla 2-19. Valoración del impacto[70]

2.2.5.2 Estimación del Riesgo

Riesgo, es la materialización de una amenaza. En la Tabla 2-20 indica el color que será representado y la valoración del riesgo recomendada por la metodología OWISAM:

Valor asignado	Nivel de riesgo	Impacto
0-2	Mínimo	Mínimo riesgo de acceso no autorizado. Un ataque exitoso requeriría de una ventana temporal mayor al

[70] Elaborado por: La autora en base a la metodologia ISSAF.

Valor asignado	Nivel de riesgo	Impacto
		definido en el alcance de esta revisión así como un nivel de especialización alto.
3-4	Bajo	Riesgo muy reducido de que un usuario no asociado a la organización sea capaz de acceder a la infraestructura inalámbrica existente. El impacto que puede tener sobre la infraestructura es limitado.
5-6	Medio	Existe la posibilidad no despreciable de modificación de información, robo de credenciales o modificación del comportamiento normal del sistema, aunque las consecuencias para el sistema son limitadas. Este ataque es viable dentro de un marco temporal inferior a 1 mes.
7-9	Alto	La probabilidad de que ocurra un acceso no autorizado a los activos de la Organización es alta, debido principalmente a la existencia de debilidades en las redes inalámbricas existentes. Un atacante podrá impactar significativamente en la operación normal de los sistemas.
10	Crítico	La probabilidad de que ocurra un acceso no autorizado en los activos de la organización es muy elevada, debido a la existencia de redes inalámbricas que tienen visibilidad de sistemas internos y que pueden ser accedidas por usuarios externos.

Tabla 2-20. Valoración del riesgo[71]

[71] Fuente: Metodología OWISAM, https://www.owisam.org/es/CWSS último acceso: [11/08/2014]

2.2.5.3 Evaluación del Riesgo

Con la recopilación de información en base a las entrevistas, documentación, pruebas, y observación realizada por la autora se determinaron las vulnerabilidades existentes en la institución (ver acápite 2.2.4).

El activo crítico estudiado dentro del caso de estudio es la red inalámbrica y la persona responsable del correcto funcionamiento y buen uso del mismo es el administrador de la red.

Lo siguiente es la clasificación de riesgos, para ello se aplicará la matriz de Evaluación de Riesgo (ver en la Tabla 2-21). Cada celda tienen una valoración numérica dependiendo el parámetro y este está descrito en los acápites anteriores.

Los parámetros que contiene la matriz son los siguientes:

- #.- indica el número de fila.
- Amenaza, es un evento o acontecimiento que tiene el poder suficiente para causar daño o pérdida al sistema o a la institución. Los valores correspondientes a esta celda se tomarán del acápite 2.2.2.
- Probabilidad, indica con qué frecuencia o periodicidad se ejecuta este evento. Los valores correspondientes a esta celda se tomarán del acápite 2.2.3.
- Vulnerabilidad, es la debilidad de un activo que puede ser aprovechada por una amenaza. Los valores correspondientes a esta celda se tomarán del acápite 2.2.4.
- Impacto, es la consecuencia al negocio que produce en caso de que se materialice el riesgo. Los valores correspondientes a esta celda se tomarán del acápite 2.2.5.1.
- Riesgo, es la materialización de una amenaza, y está estrechamente relacionado con el impacto y la probabilidad. Dentro de la matriz esta columna se calcula automáticamente (impacto x probabilidad). La valoración se tomarán del acápite 2.2.5.2.

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo
1	Incorrecta configuración a la red inalámbrica	Acceso a segmentos de red restringidos.	2,00	5	10,00
2	Acceso no autorizado a la red	Acceso no autorizado a redes inalámbricas	2,00	3	6,00
3	Ingeniería social	Acceso no autorizado e interceptación de tráfico.	2,00	3	6,00
4	Incorrecta configuración a la red inalámbrica	Área de cobertura excesiva.	2,00	5	10,00
5	Espionaje	Ataques a la disponibilidad del servicio.	2,00	4	8,00
6	Incorrecta configuración a la red inalámbrica	Ausencia de sistemas de monitorización.	2,00	5	10,00
7	Incorrecta configuración a la red inalámbrica	Ausencia de validación de certificados.	2,00	5	10,00
8	Incorrecta configuración a la red inalámbrica	Autenticación contra redes inalámbricas	2,00	5	10,00
9	Incorrecta configuración a la red inalámbrica	Beacom frames habilitados	2,00	5	10,00
10	Denegación de Servicio	Bloqueo de cuentas.	2,00	2	4,00
11	Falta de políticas de seguridad	Configuración incorrecta.	2,00	4	8,00
12	Falta de políticas de	Credenciales débiles.	2,00	4	8,00

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo
	seguridad				
13	Fraude	Debilidad de seguridad en la red inalámbrica	2,00	4	8,00
14	Pérdida de servicios soporte	Debilidades en elementos de arquitectura o software.	2,00	5	10,00
15	Código malicioso	Degradación de la calidad del servicio.	2,00	4	8,00
16	Código malicioso	Degradación del servicio.	2,00	3	6,00
17	Falta de políticas de seguridad	Detección de dispositivos emitiendo en frecuencias restringidas.	2,00	4	8,00
18	Incorrecta configuración a la red inalámbrica	Direcciónes Ips visibles	2,00	2	4,00
19	Falta de políticas de seguridad	Dispositivos que no cumplen el estándar / propietarios	2,00	3	6,00
20	Escuchas encubiertas	Emisión de señal de clientes no autorizados	2,00	3	6,00
21	Espionaje	Identificación de dispositivos mediante técnicas de descubrimiento activo	2,00	3	6,00
22	Espionaje	Interceptación de comunicaciones	2,00	3	6,00
23	Interceptación de información	Interceptación de credenciales de autenticación.	2,00	3	6,00

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo
24	Identidad de usuario camuflada	Intrusos en redes inalámbrica	2,00	4	8,00
25	Falta de políticas de seguridad	No cuentan con política de configuración de dispositivos.	2,00	4	8,00
26	Falta de políticas de seguridad	No cuentan con política de gestión y cambio de claves	2,00	4	8,00
27	Falta de políticas de seguridad	No cuentan con política de uso/restricción de uso de redes inalámbricas	2,00	4	8,00
28	Falta de políticas de seguridad	No cuentan con una verificación de inventario de dispositivos autorizados	2,00	4	8,00
29	Falla en los vínculos de comunicación	Obtención de información sensible.	2,00	4	8,00
30	Deterioro de soportes	Obtención de información sobre el hardware y software.	2,00	3	6,00
31	Deterioro de soportes	Permite la inyección de código malicioso	2,00	3	6,00
32	Falta de políticas de seguridad	Robo de credenciales y acceso no autorizado.	2,00	4	8,00
33	Falta de políticas de seguridad	Suplantación de punto de acceso y DOS.	2,00	4	8,00
34	Incorrecto mantenimiento a la red inalámbrica	Susceptibilidad del equipamiento a la humedad y a la contaminación	2,00	1	2,00

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo
35	Identidad de usuario camuflada	Suplantación de identidad.	2,00	3	6,00
36	Fallas en equipos	Susceptibilidad del equipamiento a alteraciones en el voltaje	2,00	2	4,00
37	Espionaje	Suplantación de punto de acceso y DOS (Denegación de servicios).	2,00	3	6,00
38	Contaminación	Susceptibilidad del equipamiento a la humedad y a la contaminación	0,00	2	0,00
39	Robo	Acceso a las instalaciones donde están los equipos inalámbricos	2,00	4	8,00
40	Incorrecto mantenimiento a la red inalámbrica	Inadecuado control de cambios	2	2	4,00

Tabla 2-21. Evaluación del riesgo[72]

En el análisis de la red inalámbrica se encontraron 40 vulnerabilidades con riesgos clasificados como 7 en estado crítico, 15 son altos, 12 son medios, 4 son bajos y 2 son mínimos cada uno está sombreado con el color que le corresponde, ver Figura 2-4 y Tabla 2-22.

[72] Elaborado por: La autora en base al análisis realizado en la institución sobre los riesgos

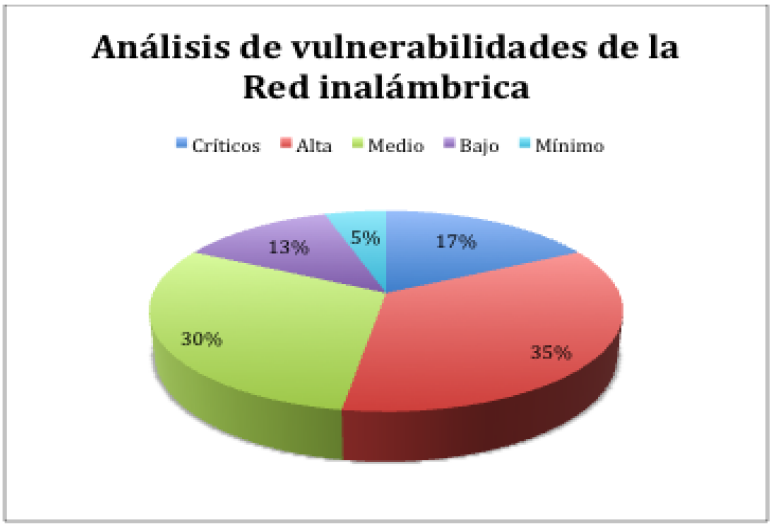


Figura 2-4. Resultados del análisis de riesgos[73]

Activo crítico analizado	Número de vulnerabilidades encontrados				
	Críticos	Alta	Medio	Bajo	Mínimo
La red inalámbrica	7	15	12	4	2
	17%	35%	30%	13%	5%

Tabla 2-22. Resultados del análisis de vulnerabilidades[74]

2.2.6 Tratamiento del Riesgo

La alta dirección junto el administrador de la red son quienes definen qué acciones tomar para los riegos encontrados descritos en el acápite 2.2.5.3, las acciones que se pueden hacer frente a los riesgos son:

1. Mitigar el riesgo, indica reducirlo, mediante la implementación de controles que disminuyan el riesgo hasta un nivel aceptable.
2. Asumir el riesgo, la alta dirección tolera el riesgo, ya que está por debajo de un valor de riesgo asumible o bien porque no se puede hacer frente razonablemente a ese riesgo, por costoso o por difícil.
3. Transferir el riesgo a un tercero, asegurando el activo que tiene el riesgo o subcontratando el servicio. Aun así, evidenciar que la responsabilidad sobre el activo permanece en manos de la organización y tener en cuenta que hay daños.

---

[73] Elaborado por la autora en base a las pruebas ejecutadas ISSAF, OWISAM y OSSTMM.

[74] Elaborado por la autora en base a la identificación de vulnerabilidades recomendada de ISSAF

4. Eliminar el riesgo. Aunque no suele ser la opción más viable, ya que puede resultar complicado o costoso.

Con el objetivo de facilitar la decisión de los involucrados de asignar un trato a los riesgos, la autora ha elegido una actividad llamada *Impacto vs. Probabilidad de ocurrencia*. La actividad consiste en:

- Explicar inicialmente a los involucrados el objetivo de esta actividad y los diferentes tratamientos que se le puede dar al riesgo
- En un papelógrafo debe estar dibujado los dos ejes, en x= impacto y en y=ocurrencia.
- En el eje x dividir en los parámetros: afecta notablemente, medianamente y no afecta. En el eje y dividir en ocurrencia: casi seguro, probable, posible, casi probable y raro.
- Escribir en pos it la descripción de los riesgos y los involucrados deben ubicar los riesgos de acuerdo a la matriz.
- El administrador junto con la alta dirección debe elegir el tratamiento deseado para dicho riesgo.
- Seleccionar los riesgos de los cuadrantes dentro de la matriz que serán tomados en cuenta para el tratamiento del riesgo.

Los resultados de la actividad se indica en la Figura 2-5.

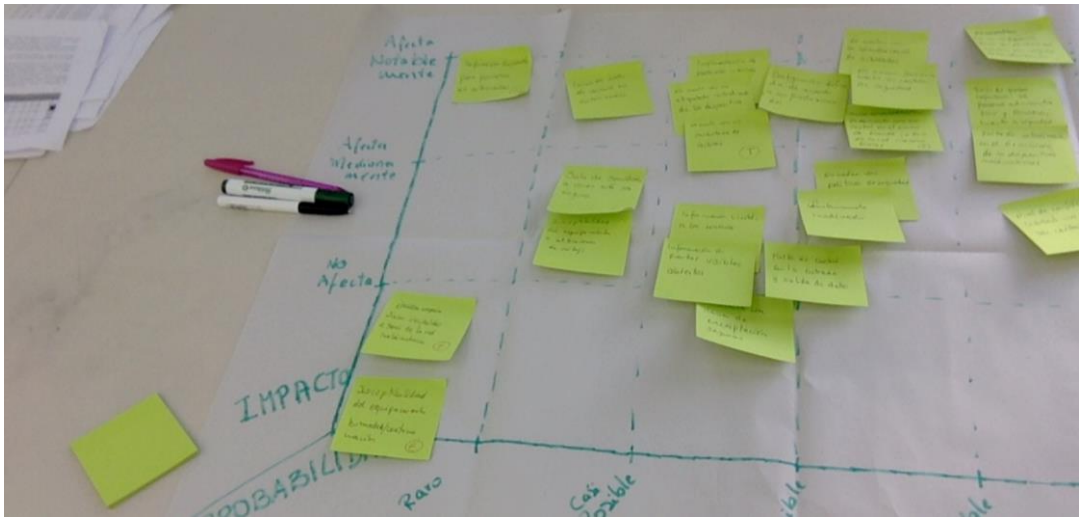


Figura 2-5. Impacto vs. Probabilidad[75]

[75] Elaborado por: La autora a la actividad realizada Impacto vs. Probabilidad.

Con la Alta dirección y el Administrador de la red con la *actividad Impacto vs. Probabilidad* se concluyó dar un tratamiento de riesgo aquellas vulnerabilidades que en su estimación esté categorizado el riesgo en: medio, alto y crítico.

El tratamiento dado a los riesgos se detalla en la Tabla 2-23.

Valor asignado	Nivel de Riesgo	Número de vulnerabilidades	Acciones
0-2	Mínimo	2	Asumir el riesgo
3-4	Bajo	5	
5-6	Medio	12	Transferir y Mitigar el riesgo
7-9	Alto	14	
10	Crítico	7	

Tabla 2-23. Clasificación del Riesgo[76]

Para el caso de estudio "transferir el riesgo" implica ver la posibilidad de asignar responsabilidades a cualquiera de los proveedores de datos e internet, PuntoNet, Movistar y CNT (Corporación Nacional de Telecomunicaciones), que tienen contrato actualmente la institución. Se "mitigarán los riesgos" aquellos que tengan el nivel de riesgo medio, alto y crítico que será descrito en el Plan de Mitigación de riesgos presentado en el acápite 3.1. Entonces se mitigaran alrededor de 34 riesgos con la estimación de riesgo promedio, ver Figura 2-6.

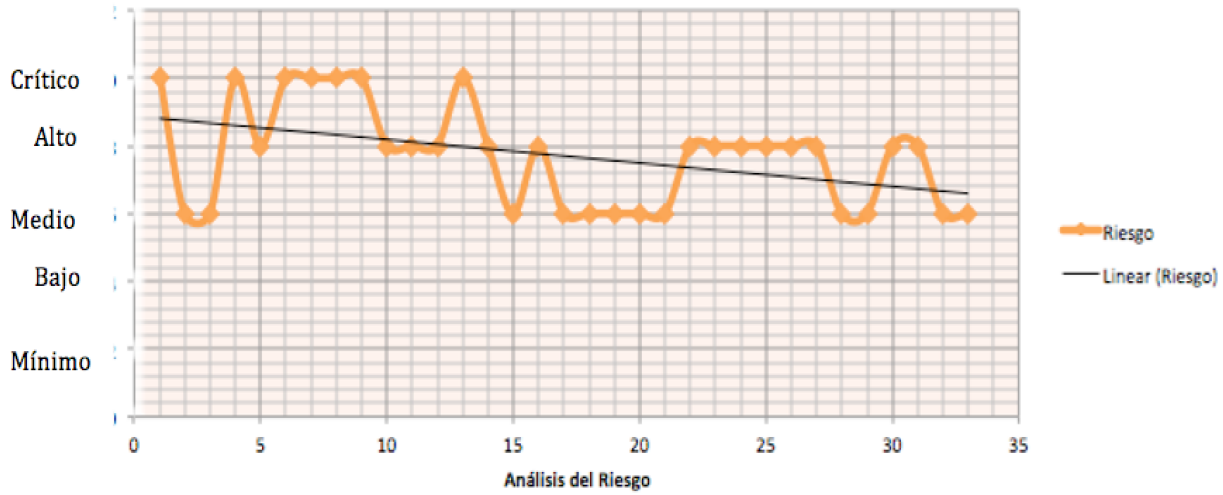


Figura 2-6. Estimación del riesgo de la institución[77]

[76] Elaborado por: La autora en base a la metodología ISO 27002.

[77] Elaborado por: La autora en base a la estimación de riesgo recomendado por ISSAF

CAPÍTULO 3.
3. PLAN DE MITIGACIÓN

La evaluación realizada sobre cualquier equipo informático no tiene mucha validez, si no se transmite al cliente en el formato adecuado sobre los resultados obtenidos y beneficios a corto plazo para la institución.

Con el objetivo de aumentar el nivel de seguridad de la red inalámbrica de la institución se entregarán los informes de resultados y el plan de mitigación a la Alta dirección junto al administrador de la red. Los informes de resultados consisten en un informe técnico y un informe ejecutivo de la evaluación realizada. El plan de mitigación explica el tratamiento que se da al riesgo, indicando cuales son las acciones que se deben tomar frente al análisis de riesgos que fue sometido la red inalámbrica.

El capítulo 3 detalla el plan de mitigación y un análisis de qué tan factible es la propuesta presentada por la autora. La explicación de la planificación y presentación de resultados para el cliente, tomando como fuente los lineamientos sugeridos por las metodologías ISSAF, norma NTE INEN-ISO/IEC 27002 y OWISAM versión 3.

3.1 PLAN DE MITIGACIÓN DE RIESGOS

3.1.1 JUSTIFICACIÓN DE LA METODOLOGÍA

Para el desarrollo de este capítulo se tomaron como fuente las siguientes metodologías cada una con diferente objetivo:

- Determinar los riesgos para la red inalámbrica
  - En función a la evaluación de riesgos realizada en el acápite 2.2.
- Mitigar los riesgos encontrados de la red inalámbrica
  - ISO/IEC 27002:2013, norma que muestra lineamientos para la implementación, monitorización, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la información, contiene 14 dominios, 35 objetivos de control y 114 controles ver Anexo H. Los dominios que se elegirán son Gestión de activos, Control de accesos, Seguridad física y ambiental.
  - OWISAM, presenta recomendaciones para mejorar la seguridad enfocadas solo de la red inalámbrica[78].
- Elaborar reportes y la presentación al cliente
  - El formato y cómo redactar los resultados del reporte serán tomados los lineamientos de ISSAF y OSSTMM versión 3 respectivamente.

3.1.2 PLAN DE MITIGACIÓN

Con el análisis realizado de la evaluación de riesgos (ver acápite 2.2.5.3) se presentan unas acciones frente a ellos. En la Tabla 3-1 las columnas Recomendaciones y Normas/Estándar de Referencia se definen dichas acciones que permitan tener una hoja de ruta para la revisión de los riesgos y posterior seguimiento.

Cabe aclarar que este plan de mitigación no es un sistema de gestión de seguridad de la información (SGSI) debido a que no está incluido en el alcance de este proyecto de titulación.

[78] Fuente: Metodología OWISAM, https://www.owisam.org/es/OWISAM acceso: [11/05/2015]

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
1	Incorrecta configuración a la red inalámbrica	Acceso a segmentos de red restringidos.	2,00	5	10,00	Cambiar los parámetros de configuración por defecto en los dispositivos inalámbricos.	- ISO/IEC 27002:2013: 9.1.1 Política de control de accesos - OWISAM: Cifrado de las comunicaciones Pruebas de infraestructura
2	Acceso no autorizado a la red	Acceso no autorizado a redes inalámbricas	2,00	3	6,00	Establecer WPA2 con AES-CCMP como método de autenticación y cifrado, definiendo tiempo de renovación de claves prudencial.	-ISO/IEC 27002:2013: 9.1.1 Política de control de accesos, 9.1.2 Control de acceso a las redes y servicios asociados - OWISAM: Pruebas de re-inyección de de tráfico (replay attack, Mic,..)
3	Ingeniería social	Acceso no autorizado e interceptación de tráfico.	2,00	3	6,00	Establecer WPA2 con AES-CCMP como método de autenticación y cifrado, definiendo tiempo de renovación de claves prudencial.	- ISO/IEC 27002:2013: 9.2.5 Revisión de los derechos de acceso de los usuarios, - OWISAM: Pruebas de re-inyección de de tráfico (replay attack, Mic,..)
4	Incorrecta	Área de cobertura	2,00	5	10,00	La potencia de los APs deben ser	- ISO/IEC 27002:2013: 9.2.3

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
	configuración a la red inalámbrica	excesiva.				controlados y limitados al radio de cobertura de la institución. Revisar los parámetros Slottime, ACK y CTS Timeout para evitar que enlaces Wi-Fi sean accesibles a mayor distancia de la esperada.	Gestión de los derechos de acceso con privilegios especiales. - OWISAM: Verificación del nivel de intensidad de señal o área de cobertura.
5	Espionaje	Ataques a la disponibilidad del servicio.	2,00	4	8,00	"Se recomienda usar WPA2, si es posible. No es recomendable usar WEP. WPA o WPA2 son más seguros. Si prueba WPA o WPA2 y no funcionan, se recomienda que actualice el adaptador de red a uno que sea compatible con WPA o	- OWISAM: Pruebas de denegación de servicio

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
						WPA2."[79]	
6	Incorrecta configuración a la red inalámbrica	Ausencia de sistemas de monitorización.	2,00	5	10,00	Preparar una calendarización de actividades donde se encuentren: plan de mantenimiento de equipos, seguridad de activos de la red inalámbrica.	ISO/IEC 27002:2013: 11.2.4 Mantenimiento de los equipos, 11.2.4 Mantenimiento de los equipos, 11.2.5 Salida de activos fuera de las dependencias de la empresa, 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones,
7	Incorrecta configuración a la red inalámbrica	Ausencia de validación de certificados.	2,00	5	10,00	Mecanismo alternativo de cifrado, puede ser el envío de credenciales a través de HTTPS, túneles VPN. Las redes abiertas generan nuevos vectores de ataque que un usuario malintencionado podría aprovechar.	- OWISAM: Cifrado de las comunicaciones,o Verificación del nivel de intensidad de señal o área de cobertura.

[79] Fuente: http://windows.microsoft.com/es-419/windows/what-are-wireless-network-security-methods#1TC=windows-7, último acceso 22/02/2015

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
8	Incorrecta configuración a la red inalámbrica	Autenticación contra redes inalámbricas	2,00	5	10,00	Se deberían eliminar las redes preferidas de los dispositivos, sobretodo las que no se van a volver a utilizar (hoteles, cafeterías...) y las que pertenezcan a la entidad corporativa.	- ISO/IEC 27002:2013: 9.2.2 Gestión de los derechos de acceso asignados a usuarios, 9.2.3 Gestión de los derechos de acceso con privilegios especiales, 9.2.4 Gestión de información confidencial de autenticación de usuarios, 9.2.5 Revisión de los derechos de acceso de los usuarios - OWISAM: Descubrimiento de preferencias de redes conocidas de clientes
9	Incorrecta configuración a la red inalámbrica	Beacon frames habilitados	2,00	5	10,00	Deshabilitar los beacon frames, que no se publique, de forma que los usuarios que lo necesiten deban introducir este valor de	

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
						forma manual a la hora de encontrar la red inalámbrica.[80]	
11	Falta de políticas de seguridad	Configuración incorrecta.	2,00	4	8,00	Crear una política de recomendaciones	- ISO/IEC 27002:2013: 9.1.1 Política de control de accesos, "Tecnología inalámbrica para proteger la red Conectada por cable"
12	Falta de políticas de seguridad	Credenciales débiles.	2,00	4	8,00	Implementar un password robusto para APs, con caracteres especiales y alfanuméricos con una longitud mínima de diez caracteres y expiración de contraseña mensualmente.	- OWISAM: Cifrado de las comunicaciones
13	Fraude	Debilidad de seguridad en la red inalámbrica	2,00	4	8,00	El uso de los algoritmos de cifrado TKIP y WEP se encuentra desaconsejado por la Wi-Fi	- OWISAM: Configuración de la plataforma

[80] Fuente: Seguridad en redes inalámbricas, http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf último acceso: [29/05/2015]

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
						Alliance. Utilizar el protocol de cifrado AES-CCMP y sustituir los dispositivos que no lo soporten.	
14	Pérdida de servicios soporte	Debilidades en elementos de arquitectura o software.	2,00	5	10,00	Consultar semestralmente las nuevas actualizaciones de firmware de los dispositivos inalámbricos.	- ISO/IEC 27002:2013: 6.1.1 Asignación de responsabilidades para la SI, OWISAM-IF Pruebas de infraestructura
15	Código malicioso	Degradación de la calidad del servicio.	2,00	4	8,00	Crear una calendarización de tareas: recordatorios de actualización de antivirus.	- ISO/IEC 27002:2013: 9.4.5 Control de acceso al código fuente de los programas, 12.2.1 Controles contra el código malicioso
17	Falta de políticas de seguridad	Detección de dispositivos emitiendo en frecuencias restringidas.	2,00	4	8,00	Configurar los dispositivos inalámbricos en canales de frecuencia no saturados.	- OWISAM: Fingerprinting, Configuración de la plataforma
19	Falta de políticas de	Dispositivos que no cumplen el estándar	2,00	3	6,00	Crear políticas de seguridad donde explique la importancia y	- OWISAM: Pruebas de infraestructura

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
	seguridad	/ propietarios				el uso de las redes inalámbricas. Capacitar al personal sobre su importancia.	
20	Escuchas encubiertas	Emisión de señal de clientes no autorizados	2,00	3	6,00	Cambiar la encriptación por la más fuerte disponible en el producto. Cambiar la version del firmware del dispositivo.	- OWISAM: Pruebas de infraestructura, OWISAM-FP Fingerprinting
21	Espionaje	Identificación de dispositivos mediante técnicas de descubrimiento activo	2,00	3	6,00	Crear periódicamente recordatorios que creen este escenario de hacking ético con el fin de encontrar nuevas vulnerabilidades.	- OWISAM: Descubrimiento de dispositivos, Fingerprinting
22	Espionaje	Interceptación de comunicaciones	2,00	3	6,00	Se recomienda que los clientes que accedan a estas redes no tengan configurada la opción de “conexión automática” aunque la red no se encuentre emitiendo.	Protección contra la denegación de servicio y las Suplantaciones[81] - OWISAM: Descubrimiento de redes ocultas

[81] Fuente: Seguridad en redes inalámbricas http://www.arubanetworks.com/pdf/products/DS_WIP_SP.pdfúltimo acceso: [29/05/2015]

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
						Verificar que el firmware está actualizado y no es posible obtener el nombre oculto tras solicitar el nombre.	
23	Interceptación de información	Interceptación de credenciales de autenticación.	2,00	3	6,00	Se recomiendo utilizer el mecamismo de autenticación AES-CCMP. En las capas superiores es recomendable el uso soluciones VPN, IPSec o SSL.	OWISAM: Pruebas sobre la autenticación, Pruebas de análisis de información transmitida a través de redes
24	Identidad de usuario camuflada	Intrusos en redes inalámbrica	2,00	4	8,00	Es importante mantener un inventario de todos los dispositivos autorizados, o al menos de los puntos de acceso, para facilitar la detección de APs falsos.	- OWISAM: Descubrimiento de dispositivos
25	Falta de políticas de seguridad	No cuentan con política de configuración de	2,00	4	8,00	Crear políticas de seguridad donde explique la importancia y el uso de las redes inalámbricas.	- ISO/IEC 27002:2013: 16.1.3 Notificación de puntos débiles de la seguridad, 8.1.3 Uso aceptable

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
		dispositivos.				Capacitar al personal sobre su importancia.	de los activos, - OWISAM: Análisis de la configuración de dispositivos
26	Falta de políticas de seguridad	No cuentan con política de gestión y cambio de claves	2,00	4	8,00	Crear una política que establezca una robustez mínima y una duración temporal máxima para las contraseñas que se empleen en la organización. Definir un tiempo de vida máximo para las claves de cifrado, tras el cual se volverán a generar unas nuevas. Esta funcionalidad debería estar activada y con un valor no superior a 3600s, para evitar ataques a la red inalámbrica.	- ISO/IEC 27002:2013: 9.1.1 Política de control de accesos, 9.1.2 Control de acceso a las redes y servicios asociados - OWISAM: Análisis de la política de gestión y cambio de claves
27	Falta de políticas de seguridad	No cuentan con política de uso/restricción de	2,00	4	8,00	Se debe disponer de unas políticas claras y conocidas por todo el personal sobre el uso de	- ISO/IEC 27002:2013: 5.1.1 Políticas para la seguridad de la información, 5.1.2 Revisión de las

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
		uso de redes inalámbricas				dispositivos con capacidades inalámbricas.	políticas para la seguridad de la información, 13.1.1 Controles de red, 13.1.2 Mecanismos de seguridad asociados a servicios en red, 13.1.3 Segregación de redes, 13.2.4 Acuerdos de confidencialidad y secreto
28	Falta de políticas de seguridad	No cuentan con una verificación de inventario de dispositivos autorizados	2,00	4	8,00	Se debe disponer de unas políticas claras y conocidas por todo el personal sobre el uso de dispositivos con capacidades inalámbricas.	- ISO/IEC 27002:2013: 8.1.1 Inventario de activos, 8.1.2 Propiedad de los activos, 8.1.3 Uso aceptable de los activos, 8.1.4 Devolución de activos, 8.2.2 Etiquetado y manipulado de la información,
29	Falla en los vínculos de comunicación	Obtención de información sensible.	2,00	4	8,00	Asegurar que esté desactivada la autenticación por clave compartida.	- ISO/IEC 27002:2013: 16.1.1 Responsabilidades y procedimientos, 16.1.2 Notificación de los eventos de seguridad de la información,

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
							16.1.3 Notificación de puntos débiles de la seguridad, 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones, 16.1.5 Respuesta a los incidentes de seguridad, 16.1.6Aprendizaje de los incidentes de seguridad de la información,16.1.7 Recopilación de evidencias.
30	Deterioro de soportes	Obtención de información sobre el hardware y software.	2,00	3	6,00	Las redes de comunicaciones inalámbricas deben usar nombres que no identifiquen a la organización, evitando usar nombres genéricos de red para evitar ataques de suplantación de identidad de puntos de acceso.	- ISO/IEC 27002:2013: 5.1.1 Documento de política de seguridad de la información, 5.1.2 Revisión de la política de seguridad de la información, 8.3.1 Gestión de soportes extraíble, 15.2.1 Supervisión y revisión de los servicios prestados por terceros

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
31	Deterioro de soportes	Permite la inyección de código malicioso	2,00	3	6,00	Es deseable disponer de un sistema de detección de intrusos (WIDS, Wireless Intrusion Detection System), que detecte y notifique la aparición de nuevos dispositivos o comportamientos anómalos.	- ISO/IEC 27002:2013: 9.4.5 Control de acceso al código fuente de los programas, 12.2.1 Controles contra el código malicioso, 14.1.1 Análisis y especificación de los requisitos de seguridad,
32	Falta de políticas de seguridad	Robo de credenciales y acceso no autorizado.	2,00	4	8,00	Como primera medida, se debe hacer hincapié en usar el sistema de cifrado más robusto del que se dispone a nivel de capa de enlace (actualmente AES-CCMP). En las capas superiores es recomendable el uso soluciones VPN, IPSec o SSL.	- ISO/IEC 27002:2013: 9.2.5 Revisión de los derechos de acceso de los usuarios,
33	Falta de políticas de seguridad	Suplantación de punto de acceso y DOS.	2,00	4	8,00	Es importante mantener un inventario de todos los dispositivos autorizados, o al menos de los puntos de acceso,	- ISO/IEC 27002:2013: 9.2.2 Gestión de los derechos de acceso asignados a usuario, OWISAM-DS Pruebas de

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
						para facilitar la detección de APs falsos.	denegación de servicio
35	Identidad de usuario camuflada	Suplantación de identidad.	2,00	3	6,00	Es importante mantener un inventario de todos los dispositivos autorizados, o al menos de los puntos de acceso, para facilitar la detección de APs falsos.	- ISO/IEC 27002:2013: 9.2.2 Gestión de los derechos de acceso asignados a usuario.,
37	Espionaje	Suplantación de punto de acceso y DOS.	2,00	3	6,00	Como primera medida, se debe hacer hincapié en usar el sistema de cifrado más robusto del que se dispone a nivel de capa de enlace (actualmente AES-CCMP). En las capas superiores es recomendable el uso soluciones VPN, IPSec o SSL.	- ISO/IEC 27002:2013: 9.2.2 Gestión de los derechos de acceso asignados a usuario, OWISAM-DS Pruebas de denegación de servicio
39	Robo	Acceso a las instalaciones donde están los equipos	2,00	4	8,00	Es importante mantener un inventario de todos los dispositivos autorizados, o al	- ISO/IEC 27002:2013: 11.1.1 Perímetro de seguridad física, 11.1.2 Controles físicos de

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
		inalámbricos				menos de los puntos de acceso, para facilitar la detección de APs falsos.	entrada, 11.1.3 Seguridad de oficinas, despachos y recurso, 11.1.4 Protección contra las amenazas externas y ambientales, 11.1.5 El trabajo en áreas seguras

Tabla 3-1. Plan de Mitigación[82]

[82] Fuente: ISSAF versión 0.2.1 página 80.

3.2 PLAN DE FACTIBILIDAD

El análisis de factibilidad es parte de las actividades de las auditoras o evaluadoras realizar el cálculo en cuanto a costo-beneficio, tiempo y recursos que serán necesarios para verificar este tipo de actividades adicionales propuestas en el plan de mitigación, ver acápite 3.1.2.

Para la definición de este estudio es asignando porcentajes estimados relativos o por rangos por cada fase dentro de un proyecto. Por ejemplo: “para un proyecto con estimación por encima del 15% para la verificación en todas las actividades (análisis de puertos, la enumeración, la identificación de la vulnerabilidad y la explotación de la vulnerabilidad), el aumento estimado en el costo para hacer la evaluación es del 5%.”[83]

Este análisis debe tiene que ser visto por la evaluadora y la institución evaluada para validar la propuesta. Este análisis implica la correcta ejecución de las pruebas y la entrega de los resultados de las pruebas, para lo cual se han realizado los controles, debe estar muy cerca de 100%.

“Con este supuesto, el cálculo de la fiabilidad de la evaluación se puede hacer por medio de fórmulas de muestreo estadístico. Es decir, para cada actividad de evaluación, la suma de los controles obligatorios, más el número de controles de la muestra se puede incluir en una fórmula fiabilidad similar a los utilizados en las encuestas, junto con el número total de objetos (puertos, servicios de red, sistemas, etc.) evaluados, para conseguir una precisión estimada de las actividades realizadas.”[77]

Esta implementación de controles añadido tiene un impacto y la ganancia se puede apreciar en los siguientes análisis de factibilidad:

- Factibilidad Técnica
- Factibilidad Operativa
- Factibilidad Económica

---

[83] Fuente: ISSAF versión 0.2.1, página 1196

3.2.1 FACTIBILIDAD TÉCNICA

En este análisis se refiere a los recursos tangibles que es necesario considerarse para la ejecución de este plan de mitigación propuesto en el acápite 3.1. Los parámetros que contiene la matriz de la Tabla 3-2 son los siguientes:

- Tareas, son las actividades que implica ejecutar el plan de mitigación.
- # Riesgos, se refiere al número de riesgos identificados en la institución. Son 7 en estado crítico, 15 en estado alto y 12 en estado medio.
- Tiempo, está estimación es en base al tiempo y esfuerzo que implica ejecutar el control. Los valores son *Horas Hombre* que es el trabajo realizado por una persona en el lapso de una hora o *Semanas hombre* indica la cantidad de trabajo que una persona puede realizar en una semana de trabajo (40 horas).

Tareas	# Riesgos	Tiempo
Implementar los controles con valoración de Riesgo 10.00 equivalente a una estimación Crítica (ver acápite 2.2.5.2)	7	6 semanas hombre
Implementar los controles con valoración de Riesgo 9.00-7.00 equivalente a una estimación Alto (ver acápite 2.2.5.2)	15	11 semanas hombre
Implementar los controles con valoración de Riesgo 6.00-5.00 equivalente a una estimación Alto (ver acápite 2.2.5.2)	12	11 semanas hombre
Rediseñar el esquema de la red.	N/A	6 semana hombre
	TOTAL	34 semanas hombre

Tabla 3-2. Análisis de factibilidad Técnica[84]

Ejecutar este plan de mitigación al administrador de la red le tomará 34 semanas hombre, lo que en sueldo se refiere alrededor de *7650*$ (mensualmente percibe un sueldo de 850$).

[84] Elaborado por: La autora.

3.2.2 FACTIBILIDAD OPERATIVA

En esta sección se debe analizar si el personal cuenta con la experiencia técnica necesaria para ejecutar este plan de mitigación propuesto descrito en el acápite 3.1.

El administrador de la red se muestra abierto con actitud positiva al cambio, esta de acuerdo en capacitarse sobre el tema de seguridad informática y luego reproducirla internamente en la institución.

Dentro de las capacitaciones que son necesarias:

- Capacitación sobre las nuevas tendencias de infraestructura inalámbrica.
- Capacitación sobre metodologías de hacking ético.
    - Capacitación sobre seguridad informática aplicado redes inalámbricas "*ISO/IEC 27033-7 , Inalámbrica,* para definir los riesgos específicos, técnicas de diseño y problemas de control de seguridad orientadas solo a las redes inalámbricas y de radio."
    - Capacitación sobre herramientas de evaluación y monitoreo.
- Capacitación sobre las normas *ISO/IEC 27002:2013 guías de buenas prácticas, Sistema de Gestión de Seguridad de la Información.*
- Luego, capacitación a los usuarios funcionales de la institución.

3.2.3 FACTIBILIDAD ECONÓMICA

En este análisis se refiere a los recursos económicos y financieros necesarios para invertir en el plan de mitigación luego de la recolección en conjunto de la factibilidad técnica y operativa.

Para este análisis se tomó como referencia del proyecto de titulación "Diseño de un plan de gestión de seguridades de la Información para instituciones públicas ecuatorianas"[f].

Partiendo del anterior tabla podemos indicar la inversión necesaria para el plan, se describe en la Tabla 3-3. Los recursos económicos son los siguientes:

Activo	Características	Costo	Comentarios
Servidor	Disco: 250 GB Memoria RAM: 1GB Procesador :Dual Core 2.5 GHz.	550$	Una manera de mitigar el riesgo 5 del plan de mitigación (ver Tabla 3-1) es por medio de la implementación de un portal cautivo.
Sistema Operativo	Cualquier Software Libre	0$	
Firewall		N/A	
Dispositivo inalámbrico		N/A	
	TOTAL	**550$**	

Tabla 3-3. Características de equipo[85]

En entrevistas al administrador de la red indicó que cuenta con una máquina servidor para la sede Quito sin utilizar entonces el recurso mostrado anterior no incluye dentro de los gastos destinados para la implementación de este plan.

El presupuesto destinado se muestra en la Tabla 3-4:

RECURSO	COSTO (c/u)
Capacitación de la Norma ISO/IEC 27002:2013	1890$
Capacitación de la Norma 27033-7 inalámbrica	1890$
Capacitación sobre herramientas de evaluación y monitoreo.	520$
Capacitación a los usuario funcionales (durante 1 semana hombre)	500$
Costo de implementación de controles	*7650$*
TOTAL	12450$

Tabla 3-4. Inversión en el plan de mitigación[86]

[85] Elaborado por: La autora

[86] Elaborado por: La autora

El presupuesto económico esperado es *12450$* en el plan propuesto para aumentar el nivel de seguridad de la red inalámbrica (dentro de este rubro no está considerado la Consultoría externa y ni el costo del equipo del servidor).
La alta dirección y el administrador de la red consideran con la capacitación interna es suficiente. La consultoría externa tiene un valor de *10000$* aproximadamente.
Considerar además que en presente análisis propuesto económico que conlleva la interrupción de alguno de los servicios o aplicaciones descritas en el acápite 1.1.1.2 a través de la red inalámbrica, ya que no corresponde al alcance definido en el presente proyecto de titulación.

3.3 REPORTES, LIMPIEZA Y DESTRUCCIÓN DE OBJETOS

En esta sección se utilizó las metodologías ISSAF y OSSTMM con el fin organizar adecuadamente el documento que será presentado a los tomadores de decisión de la institución. ISSAF en cuanto a la organización y planificación para la elaboración del documento y OSSTMM para las sugerencias o buenas prácticas en cuanto a la redacción.

ISSAF recomienda que "reportes y presentación de resultados"[87] debe estar sometido a una etapa de planificación la entrega de resultados que muestra a continuación:

- Reporte:
  - Planificación y Preparación
  - Análisis
  - Creación del Reporte, Comparación y Formato
- Presentación:
  - Presentación con el Equipo Técnico y Gerente de funcional
  - Presentación con gestión
- Limpieza y destrucción de artefactos

[87] Fuente: ISSAF versión 0.2.1, página 82-88.

3.3.1 REPORTE

3.3.1.1 Planificación y Preparación

La evaluación realizada sobre cualquier bien informático no tiene mucha validez, si no se transmite al cliente en el formato adecuado sobre los resultados obtenidos. Incluso se recomienda dirigir esta tarea a aquella persona interesada y que tenga habilidades en realizar la redacción. El resumen se debe presentar en el siguiente orden:

- Organizar la documentación de acuerdo a la entrega predefinida.
- Asegúrese que la documentación del reporte estén clasificados los datos.
- Asegúrese que se siguen los procedimientos de control del documento.
- Preparar una vista previa del reporte al cliente antes de la presentación del documento final.
    - Reunión con el equipo
    - Responsabilidades de los miembros del equipo
        - a. Jefe del Equipo
        - b. Los evaluadores
        - c. Los escritores técnicos
    - Dar información adecuada a los apropiados miembros del equipo

3.3.1.2 Análisis

Para el análisis de resultados se deben centrar en las vulnerabilidades y riesgos identificados. El análisis consiste en nuevamente identificar más vulnerabilidades y las recomendaciones y remover las inapropiadas.

Si el trabajo fue en equipo, el análisis puede ser individual y compartir con demás miembros del equipo. Luego de este análisis realizar la revisión final por un experto en la materia para precisión en las recomendaciones.

3.3.1.3 Creación del Reporte, Comparación y Formato

ISSAF recomienda la siguiente estructura del Informe:

- Resumen ejecutivo
- Alcance del trabajo

- Naturaleza de la evaluación (determinar si es interna/externa)
- Resumir lo que está fuera del alcance
- Objetivos
- Tiempo o periodo realizado
- Resumen de resultados en forma gráfica
    - Número de host/sistemas analizados,
    - Total de host/sistemas vulnerables
    - Número de vulnerabilidades de muy alto, alto, medio y bajo riesgo
- Resumen de vulnerabilidades

  Debe incluir el nombre, descripción, gravedad de la vulnerabilidad y estar clasificados como alto, medio, bajo e informativo riesgo o ninguno.
- Plan de acción (todas las soluciones y recomendaciones deben ser válidas y prácticas, resumidas en una tabla) con prioridades asignadas.
- Los resultados de las prueba detalladas con sus respectivas contramedidas

  Debe incluir cuales fueron las herramientas utilizadas, fecha y descripción de la prueba, dirección IP / Nombre de Dominio / Nombre del Ordenador (según corresponda), análisis/Conclusión/Observación y recomendaciones.

OSSTMM versión 3 recomienda para los informes lo siguiente[88]:

- Los resultados que involucren a personal sin formación en seguridad informática sólo pueden ser reportados a través de medios estadísticos.
- El/La analista no puede firmar pruebas o informes de auditoria que no haya estado directamente involucrado(a)
- El/La analista debe respetar y mantener la privacidad de todas las personas y los resultados.
- El/La analista debe notificar previamente al cliente cada vez que el analista cambia el plan de pruebas o el lugar de las pruebas de origen o si se produjo algún problema en la prueba o sin son pruebas altas de tráfico.
- Los informes deben ser objetivos y sin falsedad o malicia.
- Los informes deben indicar claramente los hallazgos que tuvieron éxito y fracaso, las medidas de seguridad y controles de pérdida.

---

[88] Fuente: OSSTMM versión 3, página 40-41.

- Los informes deben utilizar métricas cuantitativas para medir la seguridad. Estas métricas deben basarse en hechos y no en interpretaciones subjetivas.
- Todos los canales de comunicación para la entrega del informe deben ser en ambos sentidos confidencial.
- Los resultados e informes no pueden ser utilizados con fines comerciales más allá de la interacción con el cliente "
- Al finalizar, con la finalidad de garantizar la calidad del proyecto se recomienda previamente enviarle al experto en la materia antes de enviarle al cliente o administrador de la red.

3.3.2 PRESENTACIÓN

3.3.2.1 Presentación con el Equipo Técnico y Gerente de funcional

Enviar con días de antelación el resumen inicial de vulnerabilidades, para la reunión debe existir un acuerdo mutuo entre los involucrados del hacking ético en un ambiente cómodo.

El/La facilitador(a) de esta reunión debe ser quién haya realizado las pruebas y tenga buenas habilidades de comunicación tanto para el equipo técnico como para el equipo empresarial, discutir sobre los hallazgos y si es necesario apoyarse sobre las herramientas que fueron utilizadas.

Comentar que en el transcurso de las pruebas de penetración fueron reportados los temas críticos que fueron identificados para garantizar que la organización fue consciente de aquello.

3.3.2.2 Presentación con gestión

Debe llevar un resumen principal de la evaluación que respondan a las preguntas por qué, qué, cuándo, que, dónde y cómo. Incluir puntos de acción claves. La presentación debe incluir gráficos y tablas resumida de información cuantitativa. Esta información puede coincidir con la sección del informe del resumen ejecutivo (ver acápite 3.3.1.3).

S

S

3.3.3 LIMPIEZA Y DESTRUIR ARTEFACTOS

Toda la información generada por las pruebas debe ser removido de los sistemas. Si en caso por alguna razón no es posible desde un sistema remoto, todos estos archivos (de su localización) deben ser comentados en el informe técnico para que el personal técnico por parte del cliente tomen las medidas necesarias después de recibido el informe.

Esta sección se puede garantizar debido a que inicialmente se ha definido cadena de custodia de las pruebas por medio del acuerdo de confidencialidad, donde explica que se han presentado resultados exclusivamente al cliente, manteniendo la confidencialidad adecuada de la información mas relevante.

Las pruebas se realizaron mediante la creación de ambientes virtuales, los cuales después de presentar la debida documentación serán eliminadas sin mantener copias en disco. Y si el cliente lo desea la autora permite realizar la auditoria a tu máquina con el objetivo de que se muestre que no se posee información de la institución de dichos ambientes virtuales.

3.3.4 EJECUCIÓN DE LA FASE DE REPORTES, LIMPIEZA Y DESTRUCCIÓN DE OBJETOS

En la sección resaltada de la Figura 3-1 muestra la fase final de la metodología que se explicará en el presente capítulo.

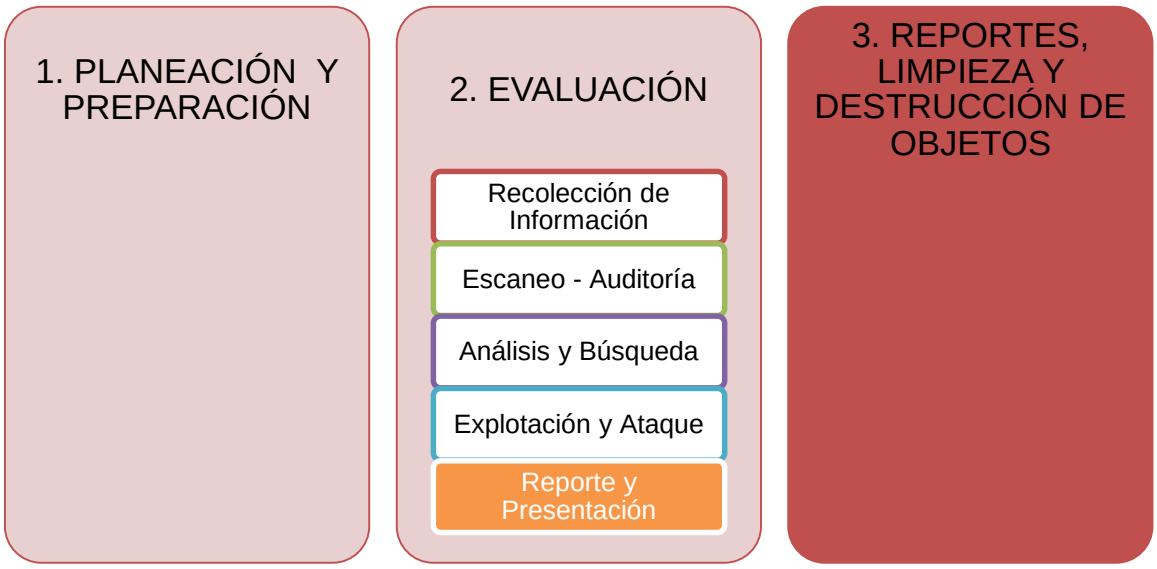


Figura 3-1. Ejecución de la última fase de ISSAF[89]

3.3.5 INFORMES PRESENTADOS

En esta fase se presenta un reporte de los resultados que son el Informe Ejecutivo orientado para la Alta Dirección y el Informe Técnico para el administrador de la red, en conjunto con el Plan de Mitigación se puede observar en Anexo K.

[89] Elaborado por: La autora en base a las fases propuestas por la metodología ISSAF.

CAPÍTULO 4

4. CONCLUSIONES Y RECOMENDACIONES

En el CAPÍTULO 4 se concluye este proyecto de titulación estableciendo las conclusiones y recomendaciones, de la experiencia en la ejecución del proyecto de titulación.

4.1 CONCLUSIONES

A continuación se muestran las conclusiones con respecto al procedimiento de hacking ético:

- La metodología ISSAF permitió llevar a cabo el procedimiento de hacking y evaluación de riesgos ético debido a que presenta un dominio orientado para la red inalámbrica.
- Decir que una sola metodología (ISSAF draf 0.2.1) va a guiar el procedimiento de hacking ético es incorrecto, se puede complementar de otras metodologías propuestas (OSSTMM versiones 2.1 y 3 y OWISAM) con el objetivo de cubrir la mayoría de escenarios posibles.
- Con la metodología ISSAF permitió a la auditora visualizar en un esquema ordenado a nivel macro para selección de las fases y en cambio la metodología OWISAM permitió aprovechar los controles a una escala pequeña.
- Con la metodología OSSTMM fue de aporte para la elaboración de los Informes Ejecutivo y Técnico.
- El procedimiento de hacking ético realizado en la institución la mayoría de veces fue realizado en horario de oficina lo que provoco que ciertas pruebas no fueron ejecutadas.
- Dentro del procedimiento de hacking ético ciertas pruebas intrusivas no se pudo ganar acceso en la institución ya que cuenta con medidas de seguridad que protegen la información a través de la red inalámbrica.
- Los controles propuestos en el plan de mitigación no van a ser asertivas al cien por ciento debido a la inexperiencia de la autora y los resultados encontrados están limitados a las herramientas en su versión software en su versión gratis.
- La metodología ISSAF indica que a veces la evaluación realizada sobre cualquier bien informático no tiene validez, si no se transmite al cliente en el formato adecuado sobre los resultados obtenidos. Incluso recomienda dirigir esta tarea a aquella persona interesada y que tenga ciertas habilidades en realizar la redacción.
- Para la explicación sobre los 34 riesgos encontrados y facilitar la decisión del tipo de tratamiento que se le debe dar al riesgo, la auditora presentó

una dinámica Impacto vs. Probabilidad hubo mayor involucramiento por parte de los interesados al visibilizar en pos it los riesgos.

- Dentro de este procedimiento de hacking ético se destruyó todos los artefactos generados ya que fueron utilizados máquinas virtuales.

4.2 RECOMENDACIONES

- Se recomienda a los siguientes profesionales relacionados con carreras de Ingeniería de Redes de la información, Sistemas continuar sus estudios en certificaciones internacionales que certifiquen la capacidad, conocimiento en seguridad informática.
- Se recomienda antes de la ejecución del taller de hacking ético dar una presentación al personal involucrado, donde se explique el alcance, objetivos y entregables para alinear las esperanzas y temores que conlleva dicho taller tanto para la auditora como para la institución.
- Se recomienda para los siguientes evaluaciones de seguridad de la red inalámbrica de hacking ético considerar también el impacto económico al materializarse alguna vulnerabilidad, ya que eso no está considerado en el presente análisis.
- Se recomienda para los siguientes evaluaciones de seguridad de la red inalámbrica de hacking ético, realizar un Sistema de gestión de seguridad de la información (SGSI) para monitorear, examinar, proteger y mejorar la seguridad de los activos de información.
- Al momento de realizar el informe de resultados al cliente, tomarse un tiempo prudente de análisis y guiarse de las recomendaciones mostradas por ISSAF.
- Las recomendaciones propuestas para aumentar el nivel de seguridad de cualquier informático, revisarlo previamente con un consultor experimentado para afinar los controles a ser propuestos.
- Se recomienda utilizar herramientas propietarias para profundizar esta evaluación de análisis de amenazas, vulnerabilidades y riesgos de la red inalámbrica.

- Para la aplicación de pruebas intrusivas de la red inalámbrica se recomienda con el equipamiento necesario, como son antenas inalámbricas, tarjetas de red inalámbricas compatibles con los sistemas operativos orientados para el hackeo, software propietario o libre destinado exclusivamente para hacking ético.
- Considerar que la traducción del resumen del presente proyecto de titulación es a Kichwa de Otavalo y no es al Kichwa unificado.
- Se recomienda al finalizar cualquier tarea, reunión con cualquier persona pedir feedback o retroalimentación, de esta manera se hacen los ajustes y mejoras necesarias en el procedimiento o actitud. El feedback corresponde a hablar sobre puntos positivos, negativos y de mejora.

GLOSARIO

A

AP, Access Point se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico.

Ancho de banda, indica la velocidad de conexión al acceso de Internet que le brinda el ISP (Proveedor de Servicio de Internet).

B

Beacon frames, es un paquete que contiene información sobre el AP.

BSSID, Basic Service Set Identifier (Identificador de la MAC)

C

Cableado Horizontal, es el cableado que se extiende desde el Rack hasta la estación de trabajo.

Cableado Vertical, es el cableado que se extiende desde distintos cuartos de comunicaciones hasta el cuarto de comunicaciones principal.

Cable UTP Categoría 6ª, es un estándar de cables para Gigabit Ethernet y otros protocolos de redes.

Capa de Acceso, su objetivo es que los datos lleguen desde el origen al destino aunque no tengan conexión directa.

Capa Core, desvía el tráfico lo más rápidamente posible hacia los servicios apropiados.

Capa de Distribución, es punto medio entre la capa de acceso y los servicios principales de la red. Realiza funciones de enrutamiento, filtrado.

Creative Commons, ayuda a compartir sus conocimientos y creatividad con el mundo.

D

DVR: Dispositivo que almacena video en un disco duro que proviene de una o varias cámaras de video.

E

Entorno gráfico, es una página web.
ESSID, Extended Service Set ID (Identificable de la red)

F

Firmware, es un programa que es grabado en una memoria ROM y establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo.
Firewall, es un sistema que protege a una red contra intrusiones provenientes de redes de la red de internet.
Framework, es un área de trabajo.

H

Hacker, es la persona que busca debilidades de un bien informático o de una red informática.
Hacking ético, es la acción de actuar proactivamente dentro de una red encontrar las cuales son vulnerables y corregirlo antes que ocurra hurto de información, para luego reportarlas y que se tomen medidas, sin hacer daño.

I

Intrusiva (o), suceden al momento de encontrar una debilidad en un sistema manipula datos y funcionalidad, genera un riesgo sin consultar al operador.

ISECOM, Institute for Security and Open Methodologies (Instituto para la Seguridad y las metodologías Abiertas) es la autoridad oficial para las certificaciones OPST y OPSA.

L

La cadena de custodia de la prueba, es el proceso de la ejecución de pruebas controladas que se aplica a los peritos, y que tiene fin no corromper el manejo que de ellos evitando alteraciones, sustituciones o destrucciones.

Lectores Biométricos, identificación basada en el reconocimiento de una característica física e intransferible de las personas.

M

MAC, es un identificador hexadecimal de 48 bits que esta asignada de forma única a una tarjeta o interfaz de red.

Medios de Transmisión, son las vías por las cuales se comunican los datos. Dependiendo de la forma de conducir la señal a través del medio o soporte físico

Microtick, provee comunicaciones, también llamado Routers.

N

No intrusiva, suceden cuando se encuentra vulnerabilidades, pero no ingresa al sistema, pero es necesario reportarlo.

P

Penetración, pueden ser intrusivas y no intrusivas permite encontrar vulnerabilidades que un atacante podría explotar.

Pistas de Auditoría, La serie de documentos, archivos informáticos, y otros elementos de información que muestran cómo las transacciones son manejadas por una empresa de principio a fin.

Protocolo, es el método por el cual dos ordenadores acuerdan comunicarse, una especificación que describe cómo los ordenadores hablan el uno al otro en una red.

S

SGSI, “Sistema de Gestión de seguridad de la información, permite establecer, monitorear, revisar, mantener y mejorar la seguridad de los activos de información, mediante la implementación de controles de seguridad seleccionados en base a un proceso de gestión del riesgo y considerando el nivel de aceptación del riesgo establecido por la organización para lograr los objetivos del negocio.
Seguridad Perimetral, es un método de defensa de red”.[d]
Slax, es un Live CD de Linux.
Snmp, se compone de un conjunto de normas para la gestión de la red.
Switches, dispositivo que examina la información y evalúa la dirección de destino, para actuar como filtros y evitar el paso de tramas de datos dañadas.

T

TCP, (Protocolo de Control de Transmisión/Protocolo de Internet).
Tarjeta wireless, son tarjetas para expansión de capacidades que sirven para enviar y recibir datos sin la necesidad de cables en las redes inalámbricas de área local.

BIBLIOGRAFÍA

[a.] ACOSTA NARANJO, Oswaldo Andrés, Análisis de riesgos y vulnerabilidades de la infraestructura tecnológica de la secretaria nacional de gestión de riesgos utilizando metodologías de ethical hacking. Proyecto de Titulación EPN 2013.

[b.] Auditoria Wireless WifiSlax 2.0. Juan Esparta Torregoza, Andrea Cascant, Diana Aparisini 2011.

[c.] BackTrack 5 Wireless Penetration Testing Beginner's Guide, Vivek Ramachandran, 2011.

[d.] Caimi Ñucanchik Shimi Yuc-Panca, Ponticifia Universidad Católica del Ecuador, 1982

[e.] CARLO, Herramientas para redes inalámbricas, 2011.

[f.] CHICAIZA JAMI, Paola Elizabeth y DÍAZ VILLAFUERTE Alex Vinicio, Diseño de un plan de gestión de seguridades de la información para instituciones públicas ecuatorianas. Proyecto de Titulación EPN 2014.

[g.] D-link, Manual de usuario DIR-615, 2006.

[h.] ESPINOZA APRÁEZ, MARÍA CRISTINA, Análisis de vulnerabilidades de la red inalámbrica para evitar la inseguridad de la información de los usuarios de la FISEI de la UTA, 2011.

[i.] GÓMEZ, LUIS CHRISTIAM, Propuesta de Plan de Proyecto para el diseño e implementación de una red inalámbrica para el Banco Popular 2012.

[j.] INEN-ISO/IEC, INEN-ISO/IEC 27002, INEN, 2009.

[k.] INEN-ISO/IEC, NTE INEN-ISO/IEC 27005, INEN, 2012.

[l.] INSTITUCIÓN, Caracterización de la empresa, 2006.

[m.] INSTITUCIÓN, Listado de equipos, 2006.

[n.] ISSAF, Information System Security Assessment Framework, (Marco de Evaluación de Seguridad de Sistemas de Información), ISECOM

[o.] OWISAM, Open Wireless Security Assessment Methodology, (Metodología de evaluación de seguridad wireless abierta),

[p.] OSSTMM, Open Source Security Testing Methodology Manual, (Manual de la Metodología Abierta de Testeo de Seguridad)

[q.] Redes Inalámbricas en los Países en Desarrollo, cuarta edición 2013. [En línea] Available: http://wndw.net/pdf/wndw3-es/wndw3-es-ebook.pdf [Último acceso: 14 de mayo del 2015]

[r.] Seguridad en redes inalámbricas, Panda Sofware International , SL. 2005.

[s.] VILLACRES MACHADO, Danny Napoleón, Propuesta metodológica para asegurar redes inalámbricas y su aplicación en la ESPOCH. Proyecto de Titulación ESPOCH 2011.

ANEXOS

ANEXO A: Preguntas para la entrevista

ANEXO B: Preguntas para la entrevista 2

ANEXO C: Acta de reuniones

ANEXO D: Lista de los controles técnicos propuesto por la metodología OWISAM

ANEXO E: Lista de Módulos del Mapa de Seguridad de OSSTMM

ANEXO F: Plan de compromiso

ANEXO G: Presentación de las pruebas

ANEXO H: Controles ISO 27002:2013

ANEXO I: Listado de Amenazas

ANEXO J: Plan de Mitigación

ANEXO K: Informes presentados

ANEXO A: PREGUNTAS PARA LA ENTREVISTA

Completar la siguiente información:

¿Posee la organización un documento de políticas de seguridad y es aprobado por la dirección Ejecutiva de la institución?

1. Si
2. No

Marque con una x los planes que cuente la institución

Planes	SI	NO	Tiempo de actualización	Es de conocimiento de los empleados
Plan Gestión Tecnológica				
Plan de Contingencia				
Plan de Capacitación				
Plan Gestión Administrativa				
Plan que hace frente al robo de los dispositivos inalámbricos				
Plan Operativo Anual				
Otro ……				

¿Cuántos usuarios diariamente acceden a la red WLAN?

1. De 10 a 50
2. De 50 a 100
3. Más de 100

¿Por favor indicar las marcas de dispositivos utilizados en la intranet?

3Com CISCO Alcatel Nortel Sonicwall

Extreme Networks Lucent

Otros, indicar: _____

¿Qué estándares o protocolos de configuración tienen los equipos, es decir para que los equipos estén configurados de manera segura?

Filtrado De Direcciones Mac.

Wep (wired Equivalent Privacy)

Las Vpn.

El 802.1x

Wpa (wi-fi Protected Access).

Otros. Explique _____

¿Para la administración de los Access Point son manejados a base de consola o el portal web?

Qué elementos de seguridad se tienen en la red inalámbrica:

Firewall

- Stateful
- Proxy
- Packet filtering

IPS o IDS Mail security Control de contenido

Gateway Antivirus Antispyware VPN

Inspección profunda de paquetes Antivirus PC

Los AP proveen el DHCP o tienen un Servidor de DHCP principal?

¿Cuáles son los procedimientos, que utiliza la red inalámbrica para realizar algunas actividades críticas (respaldo y envío de información, etc.)?

¿Cuándo fue el último estudio referente a planes de continuidad del negocio, recuperación ante desastres o planes de contingencia o análisis de riesgos sobre IT? El análisis lo han realizado auditores externos, internos o ambos.

¿Se ha generado en el último año pérdidas de información? Y la perdida ha sido por la infiltración no autorizada a la red inalámbrica? ¿Qué tipo de acciones han tomado frente a esto?

¿Qué tipo de mantenimiento se le da a la red inalámbrica?

Preventivo: _____ Correctivo: _____ Ambos: _____

¿Con qué periodicidad?_____

¿Existen controles preventivos para evitar causas de riesgos dentro de las instalaciones de la empresa?

¿La institución está preparada para ataques como:

Robo de información.

Daño a máquinas.

Ataques de intrusión.

Usar la red para realizar otros ataques.

Otros. Explique los problemas encontrados en la red inalámbrica _____

¿Se mide el impacto de implantar y aplicar tecnologías informáticas en los procesos de negocios?

¿Se han realizado estudios de seguridad física sobre la red? En caso de ser si la respuesta, cada cuánto se realizan y si cuentan con personal para dicho estudio.

1. Si
2. No

¿Se ha realizado capacitaciones en la importancia de la seguridad de la información al personal de TI?

1. Si
2. No

ANEXO B: PREGUNTAS PARA ENTREVISTA 2

Completar la siguiente información:

La institución cuenta con:

Unidad de Tecnología Departamento de TI Otro nombre: _____

Configuración de los equipos:

Identificador de red inalámbrica (ssid):_____

La cobertura de ___ metros y protocolo _____

La contraseña red inalámbrica está compuesta de __ caracteres

Sistema de encriptación:

WEP WPA WPA2

Banda de radio de red inalámbrica es:

2,4 GHz 5,0 GHz

La antena es: Bidireccional omnidireccional

Se encuentran habilitados los beacon frames

Si

No

Administración el ancho de banda:

Usuarios grupo de usuarios tipo de tráfico horarios

Todas las configuraciones detalladas anteriormente están configuradas en todos los equipos (En caso de ser no la respuesta detallar su configuración)

Si

No

Cuenta la WLAN con las últimas actualizaciones y parches de seguridad

Si

No

Los usuarios se autentican con nombre de usuario y contraseña para redes WLAN y qué tipo de autenticación se utiliza:

Local RADIUS Kerberos.

ANEXO C: ACTA DE REUNIÓN

General		
Organización y Departamento:		
Fecha y hora de la Reunión:	Fecha, hora de Inicio	Fecha, hora de finalización
Minutos preparados para:		
Lugar:		
Metas:	Razones(Metas de la Reunión):	
Preparación:	Preparación de instrucciones (OPCIONAL):	

Propósito de la Reunión

Asistentes a la Reunión				
Nombre	Departamento	e-mail	teléfono	Presencia
				Inicio/Fin
				Inicio/Fin
				Inicio/Fin
				Inicio/Fin
				Inicio/Fin
No asistencia a la reunión				

Ideas de la Reunión (Discusión, Problemas, Apuntes)
1.
2.
3.
4.

Elemento de Acción			
Acción	Asignado a	Fecha de vencimiento	Estatus

Siguiente Reunión:					
Fecha: (MM/DD/YYYY)		Hora:		Lugar:	
Agenda:					

ANEXO D: LISTADO DE LOS CONTROLES TÉCNICOS PROPUESTO POR OWISAM

Controles OWISAM 2013			
Sección	**Referencia**	**Control**	**Vulnerabilidad**
OWISAM Discovery (OWISAM-DI)	OWISAM-DI-001	Descubrimiento de puntos de acceso.	Existencia de rogue Aps.
	OWISAM-DI-002	Descubrimiento de redes ocultas.	debilidades en el firmware y seguridad por oscuridad.
	OWISAM-DI-003	Identificación pasiva de direcciones MAC de dispositivos.	Dispositivos no autorizados.
	OWISAM-DI-004	Descubrimiento de preferencias de redes conocidas de clientes.	Conexión automática a redes inseguras.
	OWISAM-DI-005	Descubrimiento activo de dispositivos y redes.	Descubrimiento de información.
	OWISAM-DI-006	Identificación de relaciones entre dispositivos.	Descubrimiento de información.
OWISAM Fingerprinting (OWISAM-FP)	OWISAM-FP-001	Identificación del dispositivo.	Obtención de información sobre el hardware y software.
	OWISAM-FP-002	Identificación de funcionalidades soportadas por el dispositivo.	Obtención de información sobre el hardware y software.

	OWISAM-FP-003	Enumeración de mecanismos de autenticación radius (802.1x)	Mecanismos de autenticación inseguros
	OWISAM-FP-004	Detección de Rogue APs	Intrusos en redes Wi-Fi.
	OWISAM-FP-005	Pruebas de client isolation	Ataques a clientes.
	OWISAM-FP-006	Detección de ataques por parte de dispositivos Wi-Fi.	Intrusos en redes Wi-Fi.
Pruebas sobre la autenticación (OWISAM-AU)	OWISAM-AU-001	Detección de protección de acceso basado en MAC.	Autenticación contra redes Wi-Fi.
	OWISAM-AU-002	Pruebas sobre WPS	Acceso no autorizado a redes Wi-Fi.
	OWISAM-AU-003	Pruebas de downgrade del método de autenticación	Inseguridad en mecanismos de autenticación.
	OWISAM-AU-004	Captura y cracking de claves transmitidas en el proceso de autenticación.	Credenciales débiles.
	OWISAM-AU-005	Uso de protocolos de autenticación inseguros (FAST-EAP,LEAP,EAP-MD5,...)	Interceptación y descifrado de credenciales.
	OWISAM-AU-006	Pruebas de fuerza bruta de usuarios contraseñas de radius (802.1x)	Credenciales débiles.
	OWISAM-AU-007	Pruebas de fuerza bruta de contraseñas contra el	Posibilidad de descifrar

		proceso de autenticación (PSK)	contraseñas débiles offline.
	OWISAM-AU-008	Debilidades en repositorio de credenciales	Acceso no autorizado y robo de credenciales.
Pruebas de cifrado de comunicaciones (OWISAM-CP)	OWISAM-CP-001	Captura y análisis de tráfico en red abierta.	Transmisión de información sensible.
	OWISAM-CP-002	Descifrado de trafico cifrado	Transmisión de información insegura.
	OWISAM-CP-003	Pruebas de análisis de información transmitida a través de Wireless	Obtención de información sensible.
	OWISAM-CP-004	Análisis de protocolos de cifrado inseguro (WEP, TKIP,...)	Debilidad de seguridad en la red.
	OWISAM-CP-005	Pruebas de renovación de claves de cifrado	Tiempo de vida de claves criptográficas elevado.
	OWISAM-CP-006	Pruebas de re-inyección de tráfico (replay attack, Mic,..)	Suplantación de identidad.
Pruebas de configuración de la plataforma (OWISAM-CF)	OWISAM-CF-001	Identificación de redes wireless con ESSID genérico.	Suplantación de identidad y ataques basados en memory trading.
	OWISAM-CF-002	Contraseñas genéricas en interfaz administrativa del	Credenciales débiles y acceso no

		punto de acceso	autorizado.
	OWISAM-CF-003	Verificación del nivel de intensidad de señal o área de cobertura.	área de cobertura excesiva.
	OWISAM-CF-004	Análisis del solapamiento de redes en el mismo canal de comunicaciones	Degradación de la calidad del servicio.
	OWISAM-CF-005	Generación de claves en base a algoritmos conocidos	Algoritmos de claves PSK o WPS débiles.
	OWISAM-CF-006	Pruebas sobre Upnp	Redirección de puertos.
Análisis de Infraestructura (OWISAM-IF)	OWISAM-IF-001	Debilidades en el firmware del AP.	Robo de credenciales y acceso no autorizado.
	OWISAM-IF-002	Interfaces administrativas expuestas a la red	Acceso no autorizado e interceptación de tráfico.
	OWISAM-IF-003	Política de firewall incorrecta	Acceso a segmentos de red restringidos.
	OWISAM-IF-004	Controles sobre mecanismos de detección de intrusos.	Ausencia de sistemas de monitorización.
	OWISAM-IF-005	Pruebas de verificación de túneles VPN (sobre redes abiertas...)	Interceptación de comunicaciones
	OWISAM-	Debilidades en servidor	Ejecución remota

	IF-006	radius	de código o denegación de servicio.
	OWISAM-IF-007	Vulnerabilidades incubadas	Debilidades en elementos de arquitectura o software.
	OWISAM-IF-008	Gestión (Alta/baja/modificación) de claves y certificados.	Gestión incorrecta de claves de acceso.
	OWISAM-IF-009	Dispositivos de comunicaciones accesible/expuestos físicamente	Acceso no autorizado y modificación de firmware.
	OWISAM-IF-010	Detección y análisis de sistemas Scada.	Acceso a sistemas de control industrial.
Denegación de servicio (OWISAM-DS)	OWISAM-DS-001	Pruebas de deautenticación	Interceptación de credenciales de autenticación.
	OWISAM-DS-002	Saturación del canal de comunicaciones (CTS/RTS,ruido, jammering, ...)	Ataques a la disponibilidad del servicio.
	OWISAM-DS-003	Bloqueo de cuentas de usuario	Bloqueo de cuentas.
	OWISAM-DS-004	Bloqueo de dispositivo de comunicaciones	Suplantación de punto de acceso y DOS.
	OWISAM-DS-005	Pruebas de degradación del canal de comunicaciones	Degradación del servicio.

Pruebas sobre directivas y normativa (OWISAM-GD)	OWISAM-GD-001	Identificación de dispositivos que no cumplen el estándar / propietarios	n/a
	OWISAM-GD-002	Detección de dispositivos emitiendo en frecuencias restringidas.	Emisión de señal no autorizada.
	OWISAM-GD-003	Análisis de la política de uso/restricción de uso de redes inalámbricas	Accesos indebidos.
	OWISAM-GD-004	Análisis de la configuración de dispositivos.	Configuración incorrecta.
	OWISAM-GD-005	Análisis de la política de gestión y cambio de claves	Tiempo de vida de contraseñas elevado.
	OWISAM-GD-006	Verificación de inventario de dispositivos autorizados	Inventario no actualizado.
Pruebas sobre clientes inalámbricos (OWISAM-CT)	OWISAM-CT-001	Pruebas de Rogue Ap y asociación automática	Suplantación de identidad y robo de credenciales.
	OWISAM-CT-002	Analisis de APTs (Advanced Persistent Threats) sobre Wireless.	Existencia de ataques persistentes.
	OWISAM-CT-003	Desbordamiento de buffer en cliente.	Ausencia de parches de seguridad y ejecución remota de código.
	OWISAM-CT-004	Extracción de identificadores de usuarios	Recopilación de información y

		(802.1x)	configuración insegura.
	OWISAM-CT-005	Pruebas sobre suplicant débil o inseguro.	Ausencia de validación de certificados.
	OWISAM-CT-006	Ataques contra clientes	Modificación de respuestas DNS,..
	OWISAM-CT-007	Extracción de credenciales de los clientes	Suplantación de identidad.
Pruebas sobre Hotspots / portales cautivos (OWISAM-HS)	OWISAM-HS-001	Acceso a otros segmentos de red sin autenticación	Segmentación o política de cortafuegos incorrecta
	OWISAM-HS-002	Debilidades en el mecanismo de autenticación.	Acceso no autorizado.
	OWISAM-HS-003	Pruebas de encapsulación de tráfico con el exterior	Evasión del mecanismo de autenticación.
	OWISAM-HS-004	Debilidades en portal captivo	Acceso no autorizado.

ANEXO E: LISTA DE MÓDULOS DEL MAPA DE SEGURIDAD

1. Seguridad de la Información
1.1. Revisión de la Inteligencia Competitiva
1.2. Revisión de Privacidad
1.3. Recolección de Documentos

2. Seguridad de los Procesos
2.1. Testeo de Solicitud
2.2. Testeo de Sugerencia Dirigida
2.3. Testeo de las Personas Confiables

3. Seguridad en las tecnologías de Internet
3.1. Logística y Controles
3.2. Sondeo de Red
3.3. Identificación de los Servicios de Sistemas
3.4. Búsqueda de Información Competitiva
3.5. Revisión de Privacidad
3.6. Obtención de Documentos
3.7. Búsqueda y Verificación de Vulnerabilidades
3.8. Testeo de Aplicaciones de Internet
3.9. Enrutamiento
3.10. Testeo de Sistemas Confiados
3.11. Testeo de Control de Acceso
3.12. Testeo de Sistema de Detección de Intrusos
3.13. Testeo de Medidas de Contingencia
3.14. Descifrado de Contraseña
3.15. Testeo de Denegación de Servicios
3.16. Evaluación de Políticas de Seguridad

4. Seguridad en las Comunicaciones
4.1. Testeo de PBX
4.2. Testeo del Correo de Voz
4.3. Revisión del FAX
4.4. Testeo del Modem

5. Seguridad Inalámbrica
5.1. Verificación de Radiación Electromagnética (EMR)
5.2. Verificación de Redes Inalámbricas [802.11]

5.3. Verificación de Redes Bluetooth
5.4. Verificación de Dispositivos de Entrada Inalámbricos
5.5. Verificación de Dispositivos de Mano Inalámbricos
5.6. Verificación de Comunicaciones sin Cable
5.7. Verificación de Dispositivos de Vigilancia Inalámbricos
5.8. Verificación de Dispositivos de Transacción Inalámbricos
5.9. Verificación de RFID
5.10. Verificación de Sistemas Infrarrojos
5.11. Revisión de Privacidad

6. Seguridad Física
6.1. Revisión de Perímetro
6.2. Revisión de monitoreo
6.3. Evaluación de Controles de Acceso
6.4. Revisión de Respuesta de Alarmas
6.5. Revisión de Ubicación
6.6. Revisión de Entorno

ANEXO F: PRESENTACIÓN DEL PLAN DE COMPROMISO

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Plan de Compromiso
Fecha:	2015/05/02		

Nombre de la institución: Anónimo

Auditora: Jessica Morales Bonilla

Objetivo del presente documento

Dar a conocer al administrador de la red sobre la planificación de actividades destinadas para el taller práctico de hacking ético a la red inalámbrica a efectuarse alrededor de 2 meses.

Tema del proyecto de Titulación: Aplicación de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Objetivos

- Objetivo General

  Determinar amenazas, riesgos y vulnerabilidades en la red inalámbrica de una institución aplicando metodologías formales.

- Objetivos Específicos
  - Conocer la situación actual de la institución.
  - Identificar las amenazas, riesgos y vulnerabilidades presentes en la infraestructura de la red inalámbrica.

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Plan de Compromiso
Fecha:	2015/05/02		

- Emitir un plan de mitigación para los riesgos identificados.

Enfoque

Es importante clarificar el alcance con sus restricciones en una infraestructura de red inalámbrica. Las restricciones se presentarán en los siguientes ámbitos.

- **Planificación y preparación,** corresponde a definir el alcance y logística. En la Tabla 1 explica parámetros para la definición de alcance que recomienda la metodología ISSAF[90] y complementándolas con OWISAM[91].

Parámetros	Respuesta
Organización completa (alcance de la evaluación)	3 sedes / 6 sedes que cuenta la institución.
Ubicación específica (s)	Quito
División (es) Específica (s)	3 sedes
Naturaleza de la prueba	Intrusiva / no intrusiva
Pruebas desde Exteriores, Interior a la institución y o Ambos	Ambos
Direccionamiento IP o rangos a evaluar	Direcciones IP del departamento de TI de la institución.
Acceso remoto	No aplica

[90] Fuente: ISSAF versión 0.2.1, página 67.

[91] Fuente: Metodología OWISAM, https://www.owisam.org/es/Metodologia último acceso: [11/08/2014]

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Plan de Compromiso
Fecha:	2015/05/02		

ESSID (Extended Service Set ID, es el nombre cómo se puede identificar a la red)	La red inalámbrica de c/u de las sedes perteneciente a la institución a ser analizada.
Ataques de Denegación de servicio	Si
Horario de ejecución	Horario de Oficina
Tipo de análisis de las pruebas	Caja gris

Tabla 1. Restricciones para el alcance[92]

- **Evaluación**, para determinar cuáles son amenazas, vulnerabilidades y riesgos existentes en la red inalámbrica, se aplicará el procedimiento recomendado de la metodología ISSAF y para la ejecución de pruebas se complementaran con las metodologías OWISAM y OSSTMM:
  - Recolección de Información
    - Descubrimiento activo de dispositivos y redes
  - Escaneo
    - Identificación de funcionalidades soportadas por el dispositivo
  - Auditoría y Revisión
    - Controles de Implementación
      - Detección de protección de acceso basado en MAC
      - Pruebas sobre WPS

[92] Elaborado por: La autora en base a la metodologia propuesta ISSAF.

- Debilidades en el repositorio de credenciales

- Controles Técnicos
  - Interfaces administrativas expuestas a la red.
  - Prueba Traceroute, Prueba Aps/Router.
  - Verificación el nivel de intensidad de señal o área de cobertura.
  - Análisis del solapamiento de redes en el mismo canal de comunicaciones.
- Controles de Gestión
  - Pruebas sobre directivas y normativa.

- Análisis y Búsqueda
  - Debilidades en el firmware del AP
  - Análisis del protocolo SNMP en la red inalámbrica
  - Análisis de protocolos de cifrado inseguro (WEP,
  - TKIP,...)

- Explotación y Ataque
  - Captura y cracking de claves transmitidas en el proceso de autenticación.
  - Extracción de credenciales de los clientes.
  - Pruebas de deautenticación.
  - Detección de APs falsos.

- **Reporte (Conclusiones / Resultados)**

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Plan de Compromiso
Fecha:	2015/05/02		

Al finalizar la evaluación no se almacenará información relevante a la institución. Los entregables previstos para el caso de estudio son:

- Presentación de Resultados

  Luego de la ejecución de las pruebas se emitirá un Informe Ejecutivo y Técnico donde se muestran de las conclusiones, resultados y vulnerabilidades encontradas para la alta dirección y para el administrador de la red respectivamente.

- Plan de Mitigación

  Con la ejecución de las pruebas y su respectivo análisis de riesgos de la red inalámbrica, se emite un plan de mitigación que es un conjunto de recomendaciones con el objetivo de aumentar el nivel de seguridad de la red inalámbrica de la institución.

Planificación de las actividades

En la Tabla 2 se muestra los hitos de compromiso por pruebas, recomendadas por la metodología ISSAF[93]:

FASES	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5
Recolección de Información	X	X			X
Escaneo – Auditoría		X	X		X
Análisis y Búsqueda		X	X	X	X
Explotación y Ataque			X	X	X

Tabla 2. Cronograma de actividades

Definir en cualquier día en la semana un tiempo de 30 minutos para discutir acerca de las lecciones aprendidas en cuanto a la evaluación realizada.

[93] Fuente: ISSAF versión 0.2.1, página 46.

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Plan de Compromiso
Fecha:	2015/05/02		

Compromiso de alcance

El departamento analizado dentro de la organización es ventas y administración.

Datos de contactos:

Auditora: Jéssica Morales Bonilla

Mail: jelita@yahoo.es

Telf.: 0979082610

Nombre de contacto de la institución: Anónimo

Mail:XXXX@XXX.XX

Telf.: XXXXXXXX

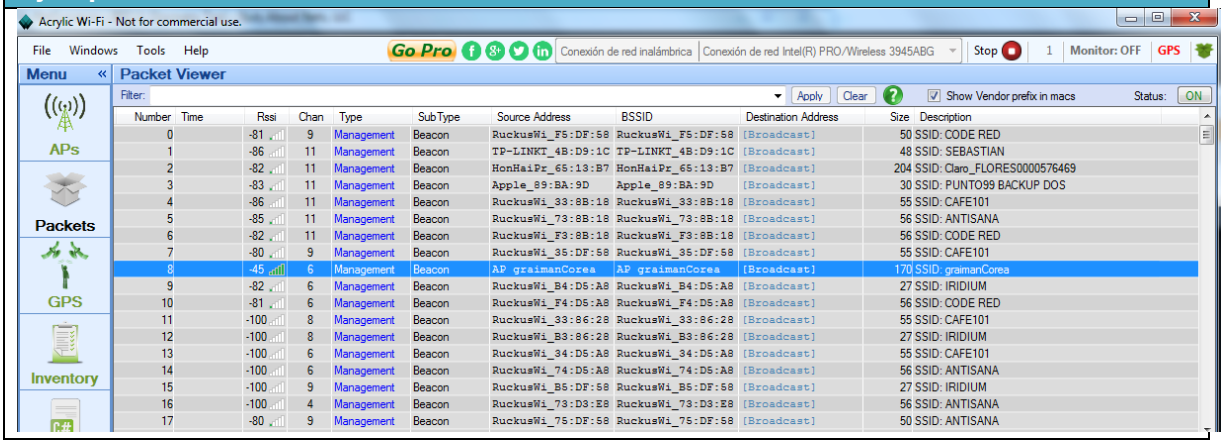
Firma de responsables:

Firma de la Auditora

Firma Administrador(a) de la red

ANEXO G: PRESENTACIÓN DE LAS PRUEBAS

El resultado de las pruebas intrusivas y no intrusivas fueron ejecutadas en las 5 sedes pertenecientes a la institución, a continuación se describen como fueron ejecutadas y se presenta una muestra de 3 sedes:

1. Descubrimiento activo de dispositivos y redes
Proceso
Descubrir los dispositivos inalámbricos que cumplen el estándar 802.11.X. Debido a que inicialmente se va a recolectar información de los dispositivos que están a nuestro alcance. Mostrar todas las redes inalámbricas presentes utilizando la herramienta Acrylic.
Pre-requisitos
Tener instalado Acrylic.
Ejemplos/Resultados

Análisis/Conclusión/Observación
Se encuentra habilitados los beacons frames para acceder a la red inalámbrica, lo que posibilita la obtención de información del software y hardware del dispositivo.
Contramedidas
Revisar el plan de mitigación
Herramientas
Suite Aircrack 4.10 Acrylic_WiFi_Free_v2.2.5616.35860
Lecturas Adicionales
https://www.owisam.org/es/Descubrimiento_de_dispositivos_OWISAM-DI https://www.owisam.org/es/OWISAM-DI-005 https://www.owisam.org/es/OWISAM-DI-003
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Recolectar información Sub fase de la metodología ISSAF: N/A Modo de ataque: Pasivo

2. Identificación de funcionalidades soportadas por el dispositivo

Proceso

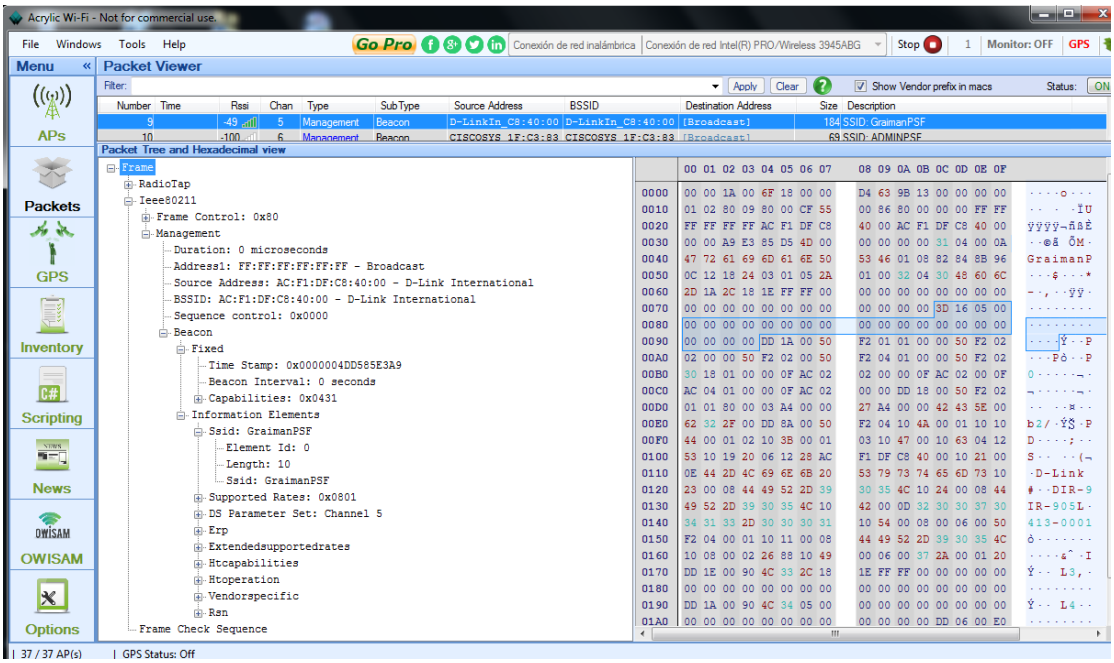
Obtener información del dispositivo tales como: datos del fabricante, driver que está utilizando, la velocidad de transmisión, tiempo de respuesta, entre otros, con la herramienta Acrylic.

Pre-requisitos

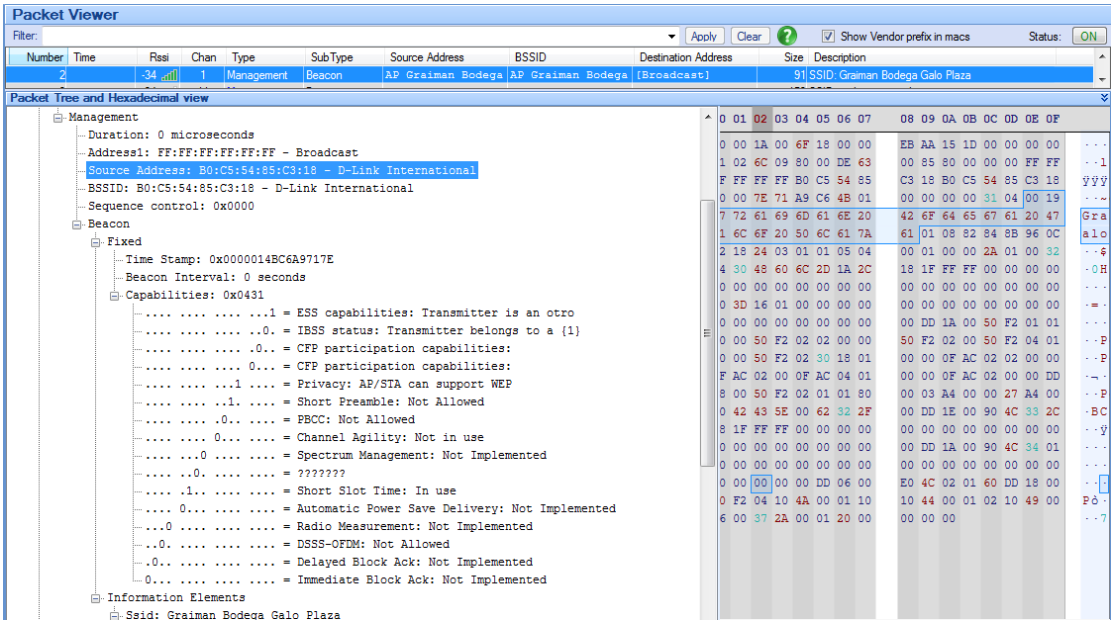
Tener instalado Acrylic.

Ejemplos/Resultados

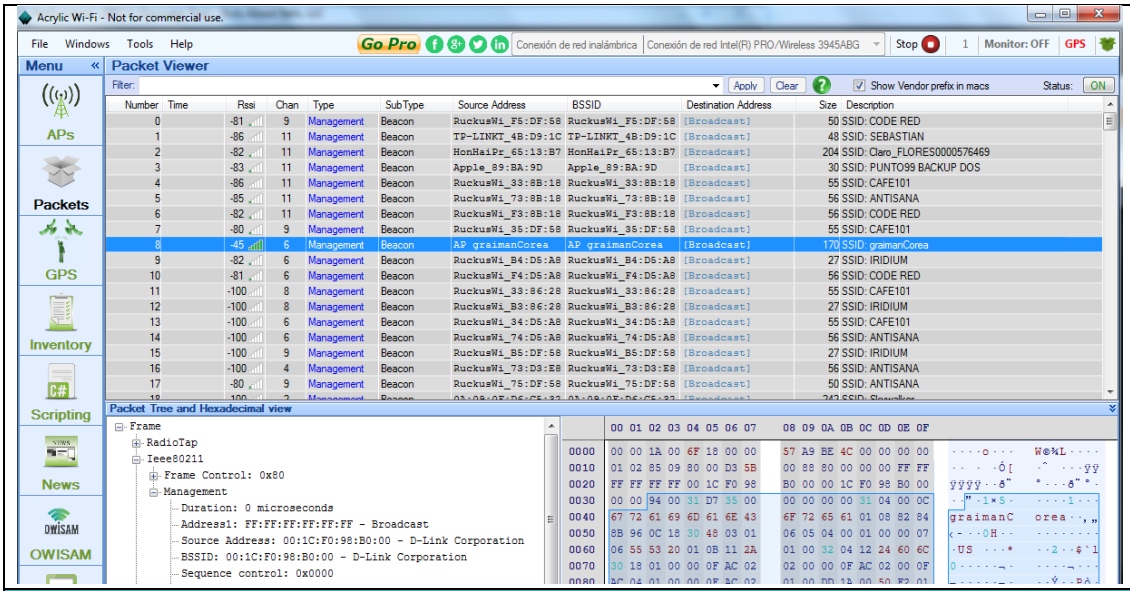
SEDE 1



SEDE 2



SEDE 3



Análisis/Conclusión/Observación

Por medio de la herramienta se pudo constatar información relevante al dispositivo.

Contramedidas

Revisar el plan de mitigación.

Herramientas

Acrylic_WiFi_Free_v2.2.5616.35860

Lecturas Adicionales

https://www.owisam.org/es/OWISAM-FP-002
https://www.owisam.org/es/Fingerprinting_OWISAM-FP

Observaciones

Esta prueba fue realizada con las siguientes características:
Fase de metodología ISSAF: Escaneo
Sub fase de la metodología ISSAF: N/A
Modo de ataque: Pasivo

3. Detección de protección de acceso basado en MAC

Proceso

Determinar la existencia de un control de dispositivos inalámbricos basados en MAC. Identificar los clientes relacionados cambiar de MAC con Technitum, luego ingresar a la red y constatar si es posible acceder a la red.

Pre-requisitos

Tener el sistema operativo Wifislax versión 4.10 donde dentro de ella vienen embebidos varias herramientas destinadas para el análisis y auditoria de redes inalámbricas. Uno de ellos que fueron utilizados, es suite de Aircrack. (Wifislax es un sistema operativo que puede ser booteable como liveCD) e instalado Technitum última versión.

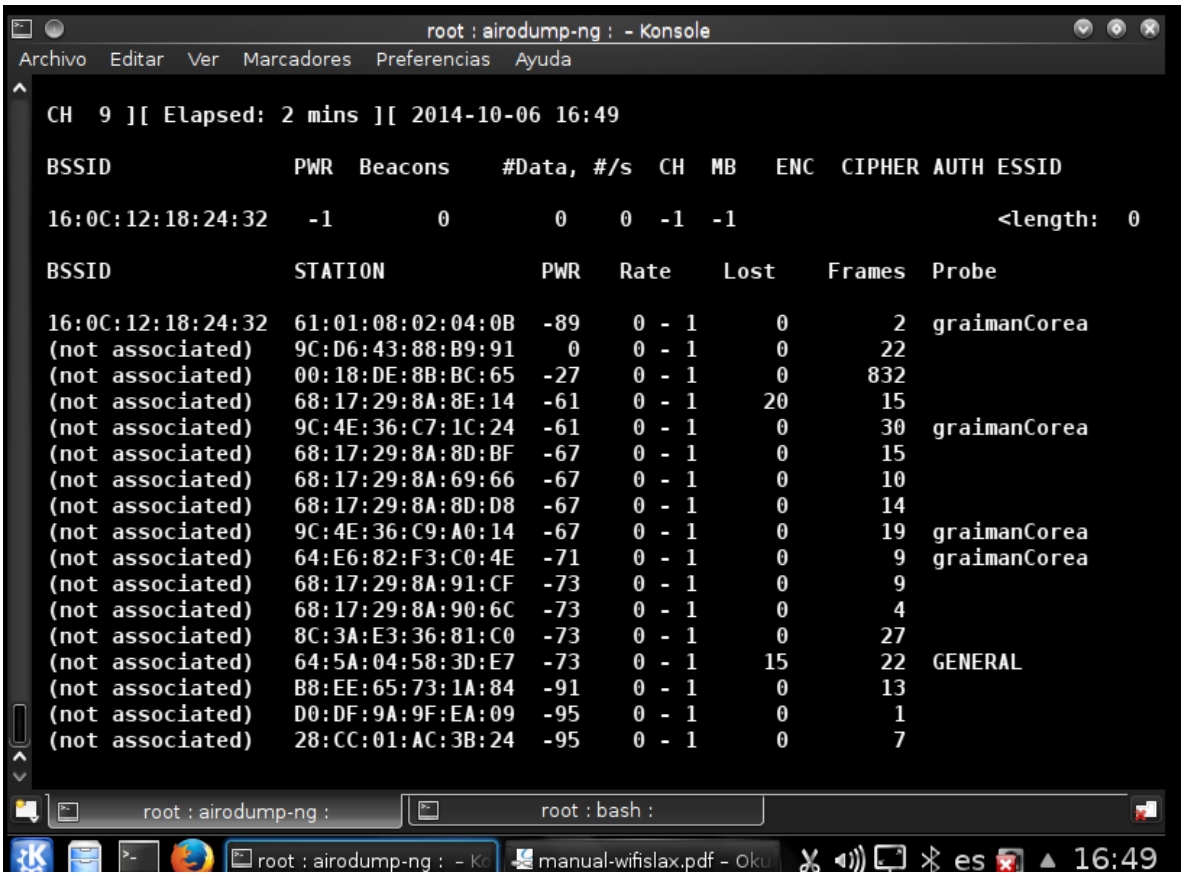
Ejemplos/Resultados

Con la herramienta WifiSlax se procede a ejecutar los siguientes comandos:

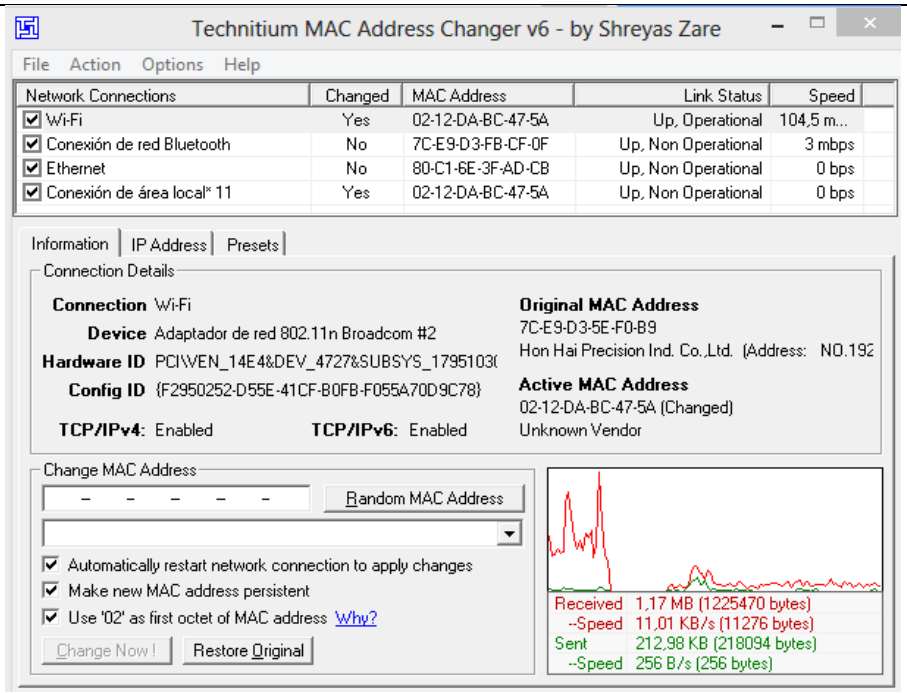
1: airodump-ng –c CANAL–w Nombre –b MACROUTER mon0. Con este comando se puede observar los usuarios conectados, los paquetes que estos envían, para capturar esos paquetes en un archivo o fichero, agregar el nombre del archivo.

```
wifislax ~ # airodump-ng -c 6 -w capturaCorea -b 16:0C:12:18:24:32 mon0
```

Resultado



Cambiar la MAC con Technitum.



Análisis/Conclusión/Observación

Al cambiar de dirección MAC de un usuario interno de la red se pudo constatar que es posible acceder a la red de internet pero no a la red interna de la empresa.

Contramedidas

Revisar el plan de mitigación

Herramientas

TECHNITIUM MAC ADDRESS CHANGER v6.

Lecturas Adicionales

https://www.owisam.org/es/Pruebas_sobre_la_autenticaci%C3%B3n_OWISAM-AU
https://www.owisam.org/es/OWISAM-AU-001

Observaciones

Esta prueba fue realizada con las siguientes características:
Fase de metodología ISSAF: Auditoría y Revisión
Sub fase de la metodología ISSAF: Controles de Implementación
Modo de ataque: Activo

4. Pruebas sobre WPS

Proceso

Determinar que el dispositivo se encuentra habilitado el protocolo WPS. Este protocolo al estar habilitado esta opción es susceptible a ataques de fuerza bruta, viene activado por defecto.

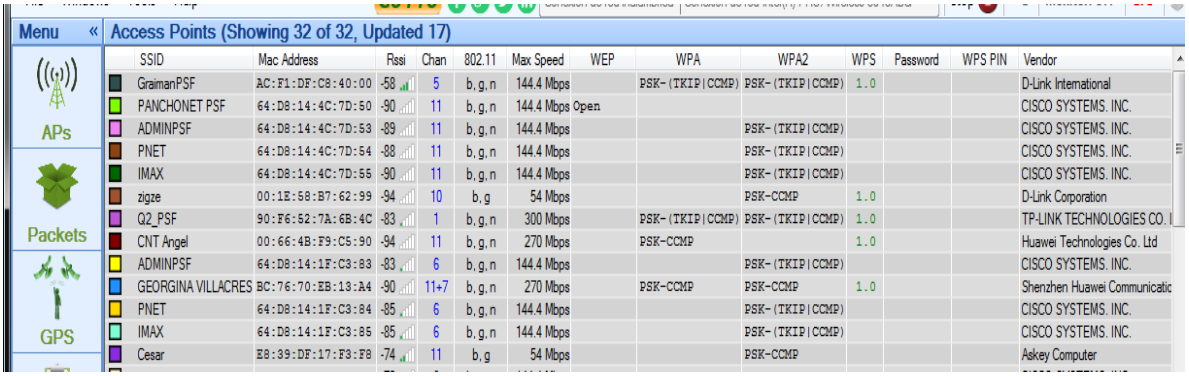
Con la herramienta Acrylic revisar el parámetro WPS y WPS PIN y confirmar la presencia de este protocolo.

Pre-requisitos

Tener instalado Acrylic.

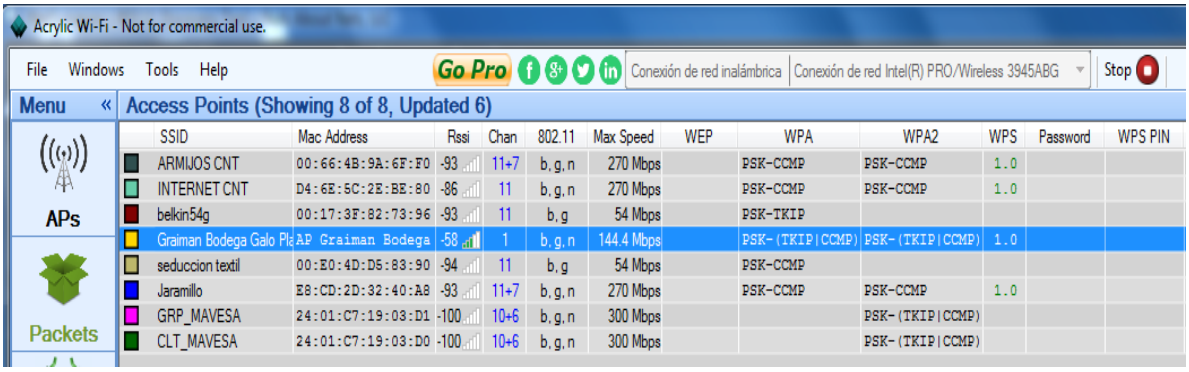
Ejemplos/Resultados

SEDE 1



SSID	Mac Address	Rssi	Chan	802.11	Max Speed	WEP	WPA	WPA2	WPS	Password	WPS PIN	Vendor
GraimanPSF	AC:F1:DF:C8:40:00	-58	5	b,g,n	144.4 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0			D-Link International
PANCHONET PSF	64:D8:14:4C:7D:50	-90	11	b,g,n	144.4 Mbps	Open						CISCO SYSTEMS. INC.
ADMINPSF	64:D8:14:4C:7D:53	-89	11	b,g,n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS. INC.
PNET	64:D8:14:4C:7D:54	-88	11	b,g,n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS. INC.
IMAX	64:D8:14:4C:7D:55	-90	11	b,g,n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS. INC.
zigze	00:1E:58:B7:62:99	-94	10	b,g	54 Mbps			PSK-CCMP	1.0			D-Link Corporation
Q2_PSF	90:F6:52:7A:6B:4C	-83	1	b,g,n	300 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0			TP-LINK TECHNOLOGIES CO.
CNT Angel	00:66:4B:F9:C5:90	-94	11	b,g,n	270 Mbps		PSK-CCMP		1.0			Huawei Technologies Co. Ltd
ADMINPSF	64:D8:14:1F:C3:83	-83	6	b,g,n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS. INC.
GEORGINA VILLACRES	BC:76:70:EB:13:A4	-90	11+7	b,g,n	270 Mbps		PSK-CCMP	PSK-CCMP	1.0			Shenzhen Huawei Communicatio
PNET	64:D8:14:1F:C3:84	-85	6	b,g,n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS. INC.
IMAX	64:D8:14:1F:C3:85	-85	6	b,g,n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS. INC.
Cesar	E8:39:DF:17:F3:F8	-74	11	b,g	54 Mbps			PSK-CCMP				Askey Computer

SEDE 2



SSID	Mac Address	Rssi	Chan	802.11	Max Speed	WEP	WPA	WPA2	WPS	Password	WPS PIN
ARMIJOS CNT	00:66:4B:9A:6F:F0	-93	11+7	b,g,n	270 Mbps		PSK-CCMP	PSK-CCMP	1.0		
INTERNET CNT	D4:6E:5C:2E:BE:80	-86	11	b,g,n	270 Mbps		PSK-CCMP	PSK-CCMP	1.0		
belkin54g	00:17:3F:82:73:96	-93	11	b,g	54 Mbps		PSK-TKIP				
Graiman Bodega Galo Pla	AP Graiman Bodega	-58	1	b,g,n	144.4 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0		
seduccion textil	00:E0:4D:D5:83:90	-94	11	b,g	54 Mbps		PSK-CCMP				
Jaramillo	E8:CD:2D:32:40:A8	-93	11+7	b,g,n	270 Mbps		PSK-CCMP	PSK-CCMP	1.0		
GRP_MAVESA	24:01:C7:19:03:D1	-100	10+6	b,g,n	300 Mbps			PSK-(TKIP|CCMP)			
CLT_MAVESA	24:01:C7:19:03:D0	-100	10+6	b,g,n	300 Mbps			PSK-(TKIP|CCMP)			

SEDE 3

	Rssi	Chan	802.11	Max Speed	WEP	WPA	WPA2	WPS	Password	WPS PIN	Vendor	First Seen	Last Seen	Type
D6:B6:EE	-78	2	b,g,n	144.4 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0			D-Link International	15:00:56	00:00:11 ago	Infrastructure
F5:DF:58	-100	9	b,g,n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:56	now	Infrastructure
33:D3:E8	-80	4	b,g,n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:56	00:00:47 ago	Infrastructure
73:D3:E8	-80	4	b,g,n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:56	00:00:11 ago	Infrastructure
65:13:B7	-80	11	b,g,n	72.2 Mbps	SharedKey						Hon Hai Precision Ind. Co.Ltd.	15:00:56	now	Infrastructure
F3:D3:E8	-77	4	b,g,n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:56	00:00:11 ago	Infrastructure
98:B0:00	-61	6	b,g	54 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				D-Link Corporation	15:00:56	now	Infrastructure
B9:BA:9D	-83	11	b,g,n	216.7 Mbps		PSK-TKIP	PSK-(TKIP|CCMP)				Apple	15:00:54	now	Infrastructure
34:D4:E8	-84	11	b,g,n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:59	now	Infrastructure
34:D5:28	-81	1	b,g,n	130 Mbps			PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:59	00:00:11 ago	Infrastructure
A6:EE:C2	-88	11	b,g,n	144.4 Mbps		PSK-TKIP	PSK-(TKIP|CCMP)				Apple	15:00:59	now	Infrastructure
35:DF:58	-100	9	b,g,n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:59	now	Infrastructure

Análisis/Conclusión/Observación

En la mayoría de las sedes los APs se encuentran habilitados el protocolo WPS y WPS PIN.
Contramedidas
Revisar en el plan de mitigación
Herramientas
Acrylic_WiFi_Free_v2.2.5616.35860
Lecturas Adicionales
https://www.owisam.org/es/OWISAM-AU-002
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Auditoría y Revisión Sub fase de la metodología ISSAF: Controles de Implementación Modo de ataque: Pasivo

5. Interfaces administrativas expuestas a la red

Proceso

Identificar el mecanismo de acceso que tiene la institución para la administración del dispositivo inalámbrico.

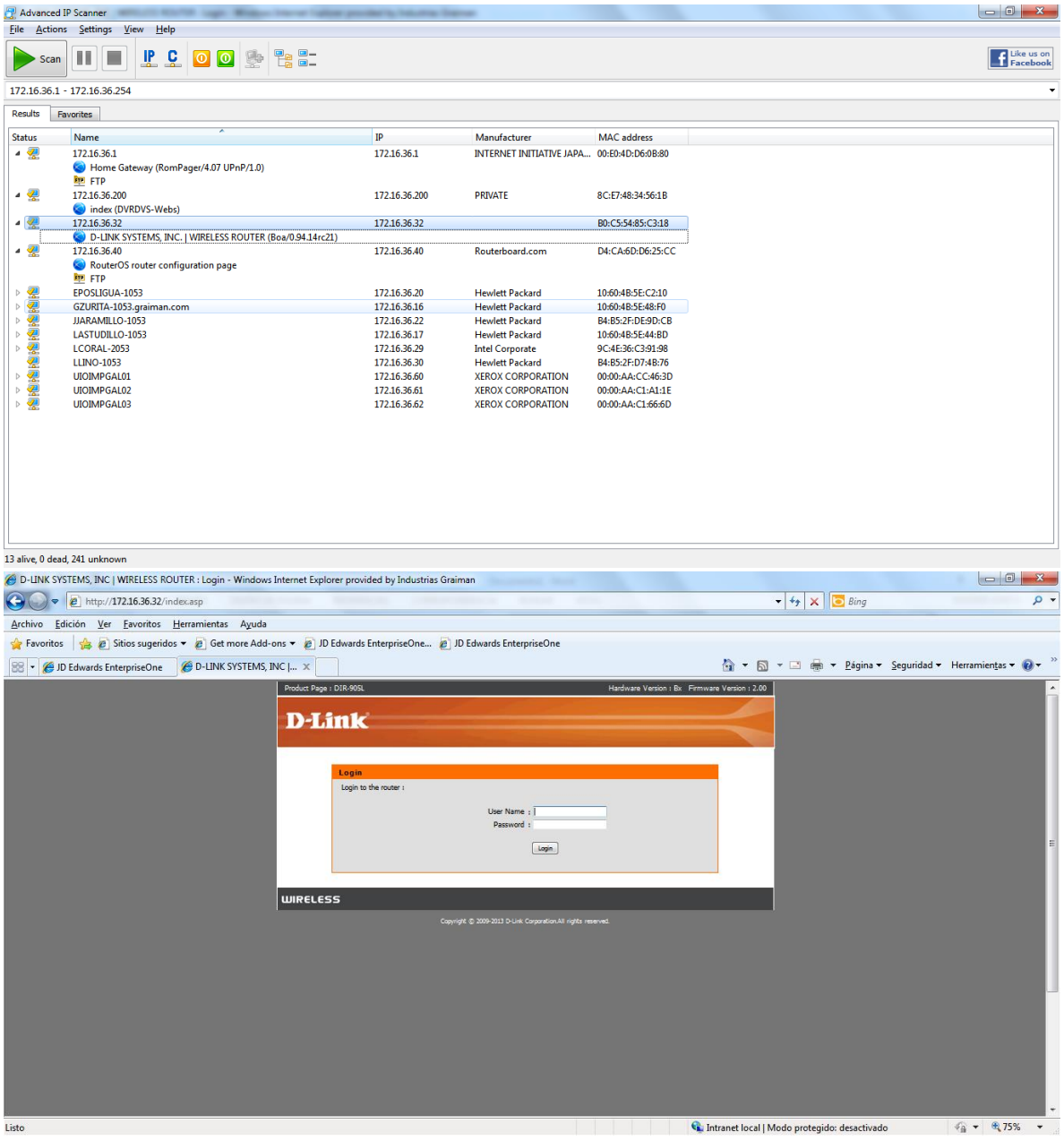
Para la realización de esta tarea se puede utilizar IPScanner comprobar la configuración IP del gateway y acceder a través de un navegador.

Pre-requisitos

Tener instalado Ipscanner.

Ejemplos/Resultados

SEDE 1



Análisis/Conclusión/Observación

En todas las sedes se pudo constatar que se encuentra habilitado el acceso para la administración del dispositivo inalámbrico al estar habilitado es vulnerable a que el

atacante pueda acceder.
Contramedidas
Revisar el plan de mitigación.
Herramientas
IPscanner versión 3.34.
Lecturas Adicionales
https://www.owisam.org/es/OWISAM-IF-002 http://nmap.org/ http://www.routerpasswords.com/ http://www.thc.org/thc-hydra/
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Auditoria y Revisión Sub fase de la metodología ISSAF: Controles Técnicos Modo de ataque: Pasivo

6. Prueba Traceroute

Proceso

Mapear los saltos de red hasta un host específico.
La herramienta nmap tiene una pestaña ue permite ver gráficamente los resultados obtenidos.
Comando: nmap -- traceroute [IP destino]
O sino con la consola de Windows
Comando: tracert [IP destino]

Pre-requisitos

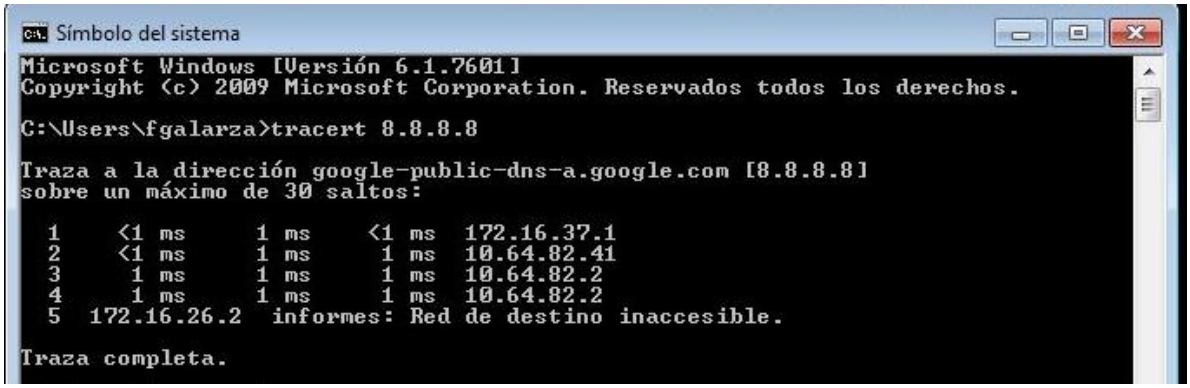
Tener instalado nmap

Ejemplos/Resultados

SEDE 1

SEDE 2

SEDE 3

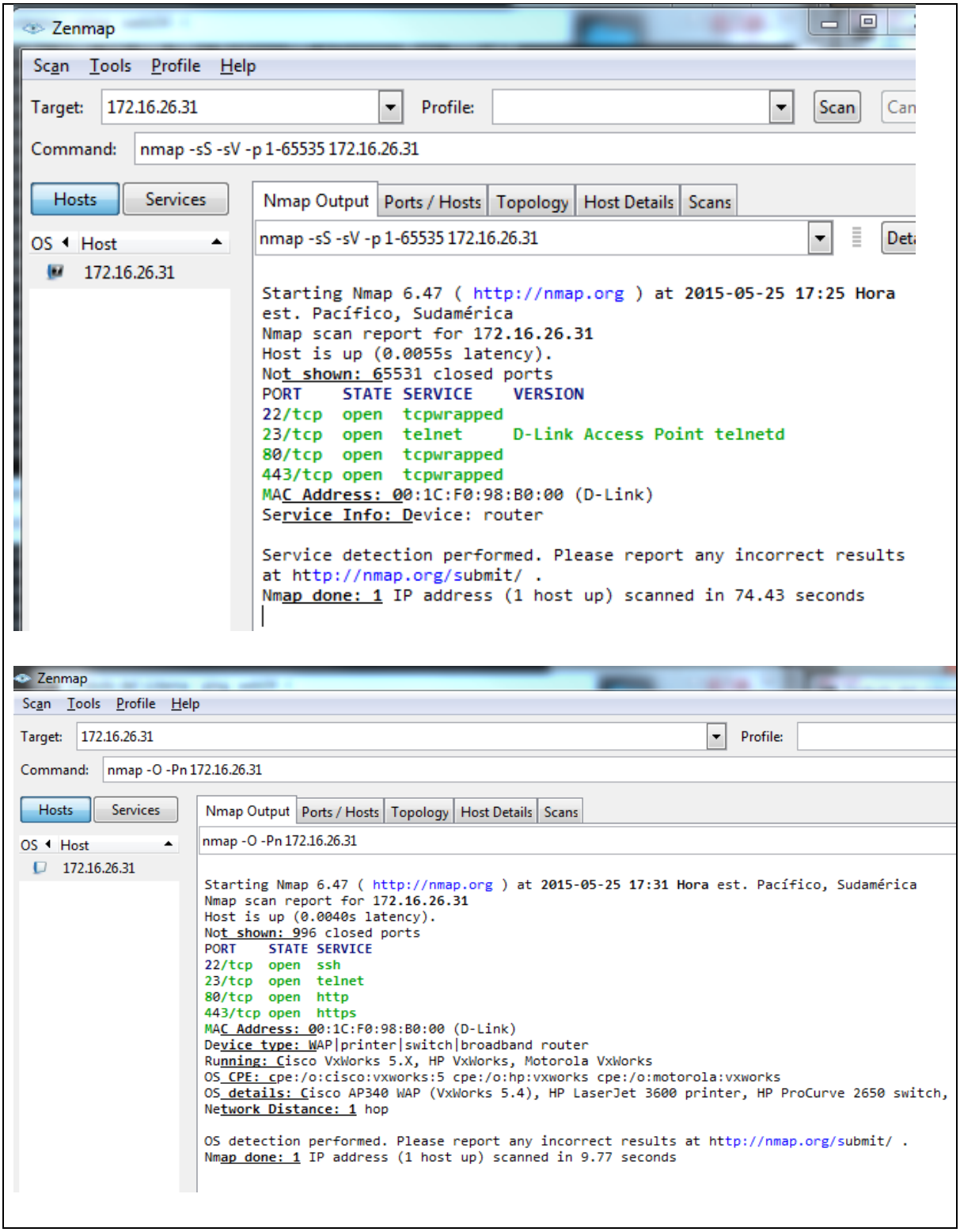


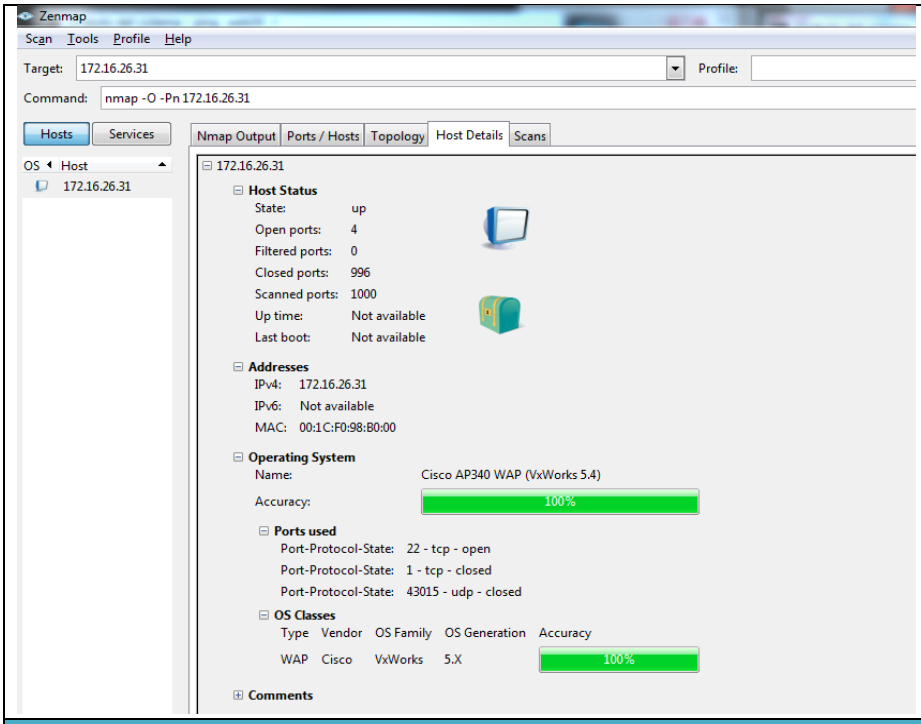
Análisis/Conclusión/Observación

Al mapear los saltos como usuario interno de la red se pudo constatar la dirección IP del router a ser analizado en la siguiente prueba.

Contramedidas
Revisar el plan de mitigación
Herramientas
Tener isntalado ZeNmap 6.47 Utilizar Consola de Windows .
Lecturas Adicionales
Metodología ISSAF versión 2.0.1 páginas 220, 222 226 235 238
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Auditoria y Revisión Sub fase de la metodología ISSAF: Controles Técnicos Modo de ataque: Activo

7. Prueba al APs/Router/Firewall
Proceso
Reconocer qué puertos, servicios y protocolos de enrutamiento se encuentran abiertos/filtrados. Esta información se recolectará con la herramienta nmap. Con los siguientes comandos: nmap -sS -sV -p 1-65535 –f –Pn –D [Ip router/Firewall] nmap -O -nP [Ip router/Firewall] nmap –sA –p 1-65535 [Ip router/Firewall] nmap –n –vv –P0 –p256, 1080 [Ip router/Firewall] El significado es el siguiente - sS: indica los servicios que se encuentran habilitados - sV: indica los versiones de los servicios habilitados - p: puertos de los servicios que utilizan - 1 – 65535 son los puertos que pueden estar habilitados para la comunicación - Pn Permite ejecutar la instrucción sin realizar un ping al host (sin utilizar el protocolo ICMP) - O: Muestra el nombre del sistema operativo - sA: verifica si el Firewall contiene reglas que pueden filtrar el contenido de los puertos que están activos. - f y D: se utiliza para evadir al firewall y permita realizar el escaneo - P0: deshabilita mensajes ICMP - vv: permite identificar la arquitectura del firewall
Pre-requisitos
Obtener la dirección IP del router puede ser con la prueba traceroute. Tener instalado ZeNmap 6.47.
Ejemplos/Resultados


Zenmap
Scan Tools Profile Help
Target: 172.16.26.31
Profile:
Scan
Command: nmap -sS -sV -p 1-65535 172.16.26.31
Hosts
Services
OS Host
172.16.26.31
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sS -sV -p 1-65535 172.16.26.31
Starting Nmap 6.47 (http://nmap.org) at 2015-05-25 17:25 Hora est. Pacífico, Sudamérica
Nmap scan report for 172.16.26.31
Host is up (0.0055s latency).
Not shown: 65531 closed ports
PORT STATE SERVICE VERSION
22/tcp open tcpwrapped
23/tcp open telnet D-Link Access Point telnetd
80/tcp open tcpwrapped
443/tcp open tcpwrapped
MAC Address: 00:1C:F0:98:B0:00 (D-Link)
Service Info: Device: router
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.43 seconds
Zenmap
Scan Tools Profile Help
Target: 172.16.26.31
Profile:
Command: nmap -O -Pn 172.16.26.31
Hosts
Services
OS Host
172.16.26.31
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -O -Pn 172.16.26.31
Starting Nmap 6.47 (http://nmap.org) at 2015-05-25 17:31 Hora est. Pacífico, Sudamérica
Nmap scan report for 172.16.26.31
Host is up (0.0040s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
80/tcp open http
443/tcp open https
MAC Address: 00:1C:F0:98:B0:00 (D-Link)
Device type: WAP|printer|switch|broadband router
Running: Cisco VxWorks 5.X, HP VxWorks, Motorola VxWorks
OS CPE: cpe:/o:cisco:vxworks:5 cpe:/o:hp:vxworks cpe:/o:motorola:vxworks
OS details: Cisco AP340 WAP (VxWorks 5.4), HP LaserJet 3600 printer, HP ProCurve 2650 switch,
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.77 seconds



Análisis/Conclusión/Observación

"Not shown: 65531 closed protocols", esto quiere decir que se encuentran cerrados 65531 puerto lo que es beneficioso y denota que tienen precaución en este sentido.
El puerto 23 esta abierto pero indican que la administración del dispositivo inalámbrico es a través de la web y no utilizan este puerto.

Contramedidas

Revisar el plan de mitigación

Herramientas

Tener instalado ZeNmap versión 6.47.

Lecturas Adicionales

Esta prueba fue realizada con las siguientes características:
Metodología ISSAF versión 2.0.1 páginas 220, 222, 226, 235, 238, 447.
Tesis de Análisis de riesgos y vulnerabilidades de la infraestructura tecnológica de la secretaría nacional de gestión de riesgos utilizando metodologías de ethical hacking

Observaciones

Fase de metodología ISSAF: Auditoria y Revisión
Sub fase de la metodología ISSAF: Controles Técnicos
Modo de ataque: Activo

8. Análisis del solapamiento de redes en el mismo canal de comunicaciones

Proceso

Analizar si los rangos de frecuencia se encuentran saturados.

La herramienta debe examinar el espectro de 2.4 GHz y 5 GHz para que examine los canales en los cuales se transmite la red inalámbrica así como el solapamiento entre ellas.

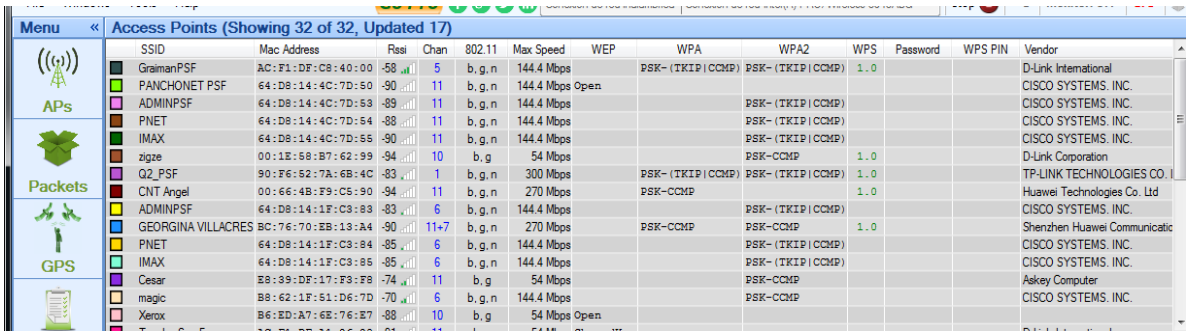
Con la herramienta Acrylic revisar el parámetro Chan.

Pre-requisitos

Tener instalado Acrylic.

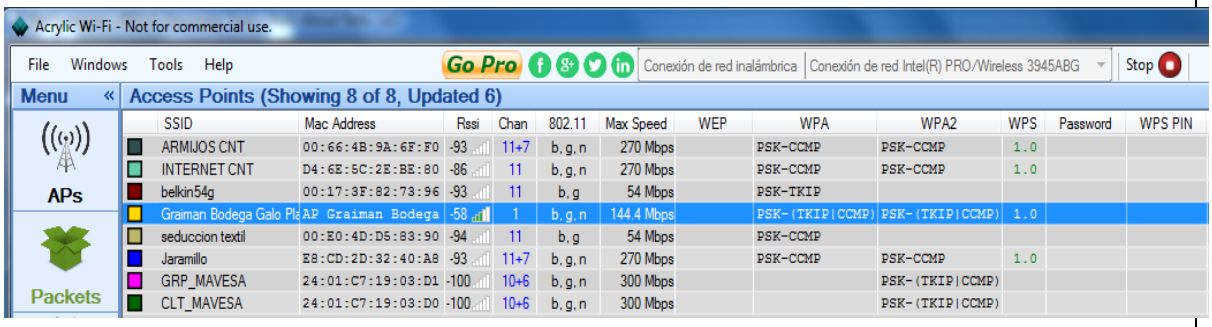
Ejemplos/Resultados

SEDE 1



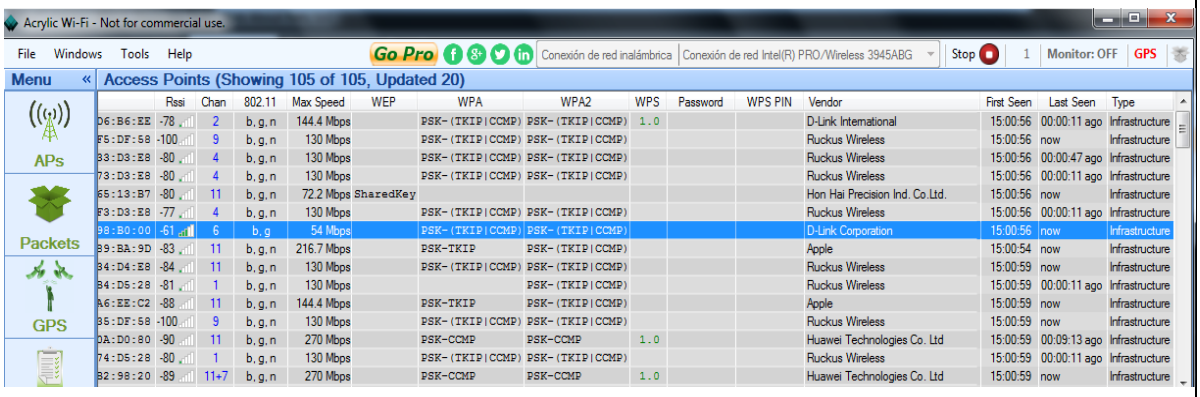
SSID	Mac Address	Rssi	Chan	802.11	Max Speed	WEP	WPA	WPA2	WPS	Password	WPS PIN	Vendor
GraimanPSF	AC:F1:DF:C8:40:00	-58	5	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0			D-Link International
PANCHONET PSF	64:D8:14:4C:7D:50	-90	11	b, g, n	144.4 Mbps	Open						CISCO SYSTEMS, INC.
ADMINPSF	64:D8:14:4C:7D:53	-89	11	b, g, n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS, INC.
PNET	64:D8:14:4C:7D:54	-88	11	b, g, n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS, INC.
IMAX	64:D8:14:4C:7D:55	-90	11	b, g, n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS, INC.
zigze	00:1E:58:B7:62:99	-94	10	b, g	54 Mbps			PSK-CCMP	1.0			D-Link Corporation
Q2_PSF	90:F6:52:7A:6B:4C	-83	1	b, g, n	300 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0			TP-LINK TECHNOLOGIES CO.
CNT Angel	00:66:4B:F9:C5:90	-94	11	b, g, n	270 Mbps		PSK-CCMP		1.0			Huawei Technologies Co. Ltd
ADMINPSF	64:D8:14:1F:C3:83	-83	6	b, g, n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS, INC.
GEORGINA VILLACRES	BC:76:70:EB:13:A4	-90	11+7	b, g, n	270 Mbps		PSK-CCMP	PSK-CCMP	1.0			Shenzhen Huawei Communicatio
PNET	64:D8:14:1F:C3:84	-85	6	b, g, n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS, INC.
IMAX	64:D8:14:1F:C3:85	-85	6	b, g, n	144.4 Mbps			PSK-(TKIP|CCMP)				CISCO SYSTEMS, INC.
Cesar	E8:39:DF:17:F3:F8	-74	11	b, g	54 Mbps			PSK-CCMP				Askey Computer
magic	B8:62:1F:51:D6:7D	-70	6	b, g, n	144.4 Mbps			PSK-CCMP				CISCO SYSTEMS, INC.
Xerox	B6:ED:A7:6E:76:E7	-88	10	b, g	54 Mbps	Open						

SEDE 2



SSID	Mac Address	Rssi	Chan	802.11	Max Speed	WEP	WPA	WPA2	WPS	Password	WPS PIN
ARMIJOS CNT	00:66:4B:9A:6F:F0	-93	11+7	b, g, n	270 Mbps		PSK-CCMP	PSK-CCMP	1.0		
INTERNET CNT	D4:6E:5C:2E:BE:80	-86	11	b, g, n	270 Mbps		PSK-CCMP	PSK-CCMP	1.0		
belkin54g	00:17:3F:82:73:96	-93	11	b, g	54 Mbps		PSK-TKIP				
Graiman Bodega Galo Pl	AP Graiman Bodega	-58	1	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0		
seduccion textil	00:E0:4D:D5:83:90	-94	11	b, g	54 Mbps		PSK-CCMP				
Jaramillo	E8:CD:2D:32:40:A8	-93	11+7	b, g, n	270 Mbps		PSK-CCMP	PSK-CCMP	1.0		
GRP_MAVESA	24:01:C7:19:03:D1	-100	10+6	b, g, n	300 Mbps			PSK-(TKIP|CCMP)			
CLT_MAVESA	24:01:C7:19:03:D0	-100	10+6	b, g, n	300 Mbps			PSK-(TKIP|CCMP)			

SEDE 3



	Rssi	Chan	802.11	Max Speed	WEP	WPA	WPA2	WPS	Password	WPS PIN	Vendor	First Seen	Last Seen	Type
D6:B6:EE	-78	2	b, g, n	144.4 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0			D-Link International	15:00:56	00:00:11 ago	Infrastructure
F5:DF:58	-100	9	b, g, n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:56	now	Infrastructure
B3:D3:E8	-80	4	b, g, n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:56	00:00:47 ago	Infrastructure
73:D3:E8	-80	4	b, g, n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:56	00:00:11 ago	Infrastructure
55:13:B7	-80	11	b, g, n	72.2 Mbps	SharedKey						Hon Hai Precision Ind. Co.Ltd.	15:00:56	now	Infrastructure
F3:D3:E8	-77	4	b, g, n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:56	00:00:11 ago	Infrastructure
98:B0:00	-61	6	b, g	54 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				D-Link Corporation	15:00:56	now	Infrastructure
39:BA:9D	-83	11	b, g, n	216.7 Mbps		PSK-TKIP	PSK-(TKIP|CCMP)				Apple	15:00:54	now	Infrastructure
34:D4:E8	-84	11	b, g, n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:59	now	Infrastructure
84:D5:28	-81	1	b, g, n	130 Mbps			PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:59	00:00:11 ago	Infrastructure
A6:EE:C2	-88	11	b, g, n	144.4 Mbps		PSK-TKIP	PSK-(TKIP|CCMP)				Apple	15:00:59	now	Infrastructure
35:DF:58	-100	9	b, g, n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:59	now	Infrastructure
DA:D0:80	-90	11	b, g, n	270 Mbps		PSK-CCMP	PSK-CCMP	1.0			Huawei Technologies Co. Ltd	15:00:59	00:09:13 ago	Infrastructure
74:D5:28	-80	1	b, g, n	130 Mbps		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Ruckus Wireless	15:00:59	00:00:11 ago	Infrastructure
82:98:20	-89	11+7	b, g, n	270 Mbps		PSK-CCMP	PSK-CCMP	1.0			Huawei Technologies Co. Ltd	15:00:59	now	Infrastructure

Análisis/Conclusión/Observación

Con el análisis realizado denota que existen varias redes vecinas a la red de la institución han se fueron configuradas las redes inalámbricas en el mismo canal dentro del área de un mismo cobertura de la señal (no en todas las redes), lo puede causar interferencia y pérdida de datos en la transmisión.

Contramedidas

Revisar el plan de mitigación
Herramientas
Tener instalado Acrylic_WiFi_Free_v2.2.5616.35860
Lecturas Adicionales
https://www.owisam.org/es/Cifrado_de_las_comunicaciones_OWISAM-CP https://www.owisam.org/es/OWISAM-CF-004 https://www.owisam.org/es/OWISAM-CF-003
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Análisis de seguridad Sub fase de la metodología ISSAF: Controles Técnicos - Pruebas de infraestructura Modo de ataque: Pasivo

9. Verificación el nivel de intensidad de señal o área de cobertura

Proceso

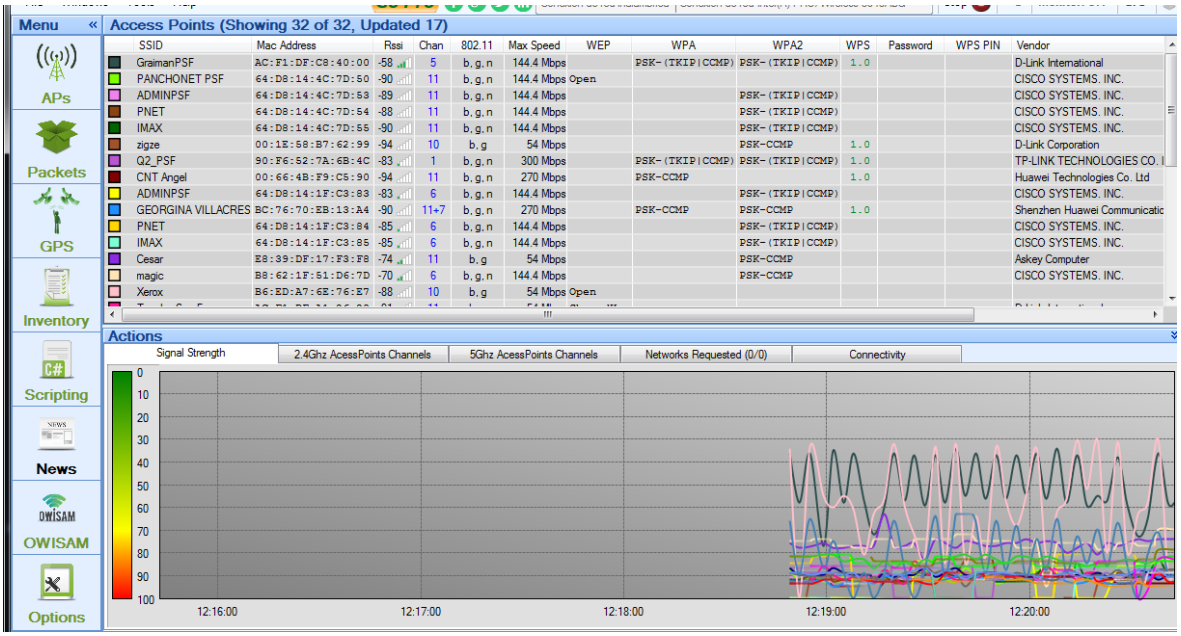
Identificar si la cobertura de la red se propaga o no dentro del perímetro de la institución, de acuerdo a los niveles de potencia.
El parámetro es RSS y en la sección Actions de la herramienta Acrylic.

Pre-requisitos

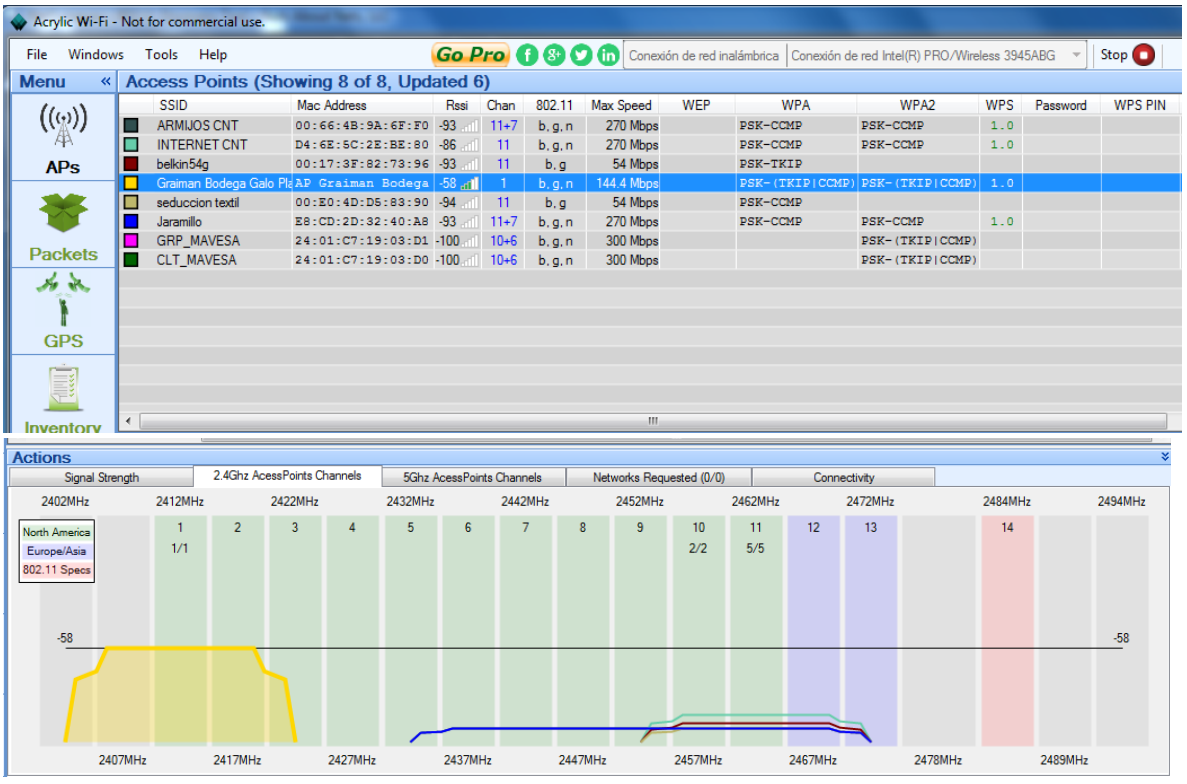
Tener instalado Acrylic.

Ejemplos/Resultados

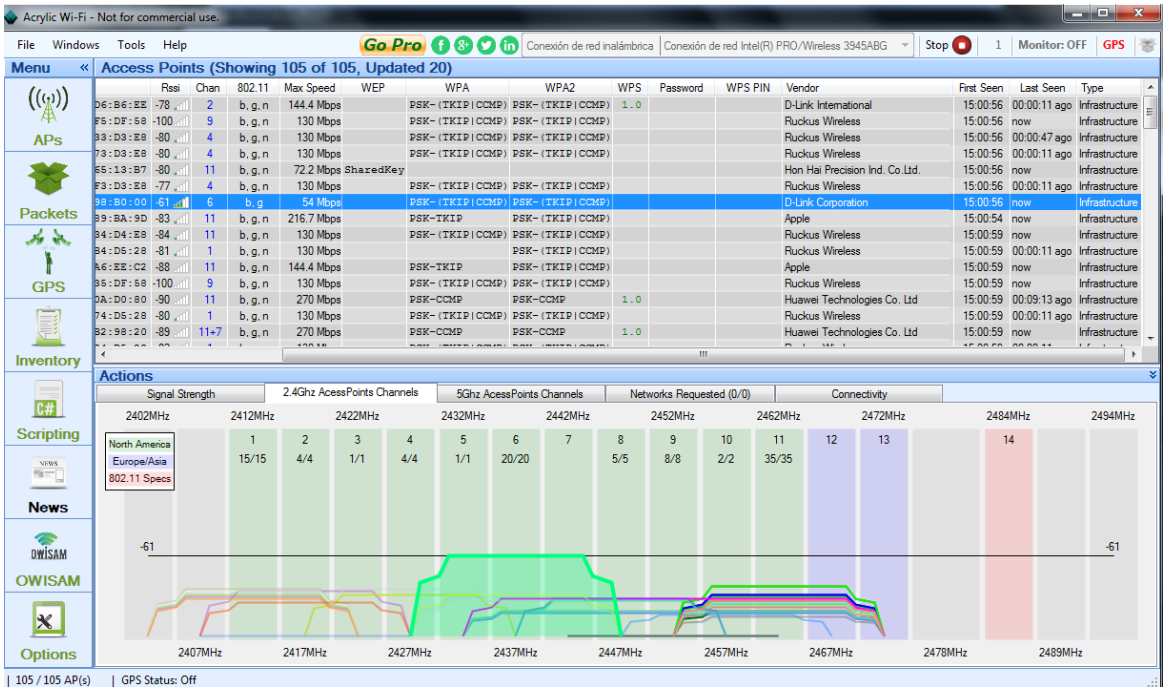
SEDE 1



SEDE 2



SEDE 3



Análisis/Conclusión/Observación

Con el análisis realizado denota que existen varias redes vecinas a la red de la institución han se fueron configuradas las redes inalámbricas en el mismo canal dentro del área de un mismo cobertura de la señal (no en todas las redes), lo puede causar interferencia y pérdida de datos en la transmisión. Se complementa con la anterior prueba.

Contramedidas

Revisar el plan de mitigación

Herramientas

Acrylic_WiFi_Free_v2.2.5616.35860

Lecturas Adicionales

https://www.owisam.org/es/Cifrado_de_las_comunicaciones_OWISAM-CP
https://www.owisam.org/es/OWISAM-CF-004
https://www.owisam.org/es/OWISAM-CF-003

Observaciones

Esta prueba fue realizada con las siguientes características:
Fase de metodología ISSAF: Análisis de seguridad
Sub fase de la metodología ISSAF: Controles Técnicos - Pruebas de infraestructura
Modo de ataque: Pasivo

10. Debilidades en el firmware del AP

Proceso

Determinar si los dispositivos inalámbricos, AP de cliente y tarjetas de red del cliente son compatibles con las versiones actuales del firmware, así los parches de seguridad se puedan implementar a medida que estén disponibles.
Consultar en las páginas oficiales de los dispositivos para verificar si se ha encontrado vulnerabilidades.

Pre-requisitos

N/A

Ejemplos/Resultados

Sede	Equipo	Marca	Modelo	Firmware	Actualizado?
Sede 1	Router	D-Link	DW-2100AP	V2.40na	No
	ADSL2+	HOME GATEWAY	HG532s	V100R001C33B016SP05 (2011)	Si
Sede 2	Router	D-Link	Dir-615	1.1	No
Sede 3	Router	D-Link	DW-2100AP	V2.30na	No
	Router	D-Link	Dir-905L	2.0	

Análisis/Conclusión/Observación

Se pudo constatar que no existe actualización de firmware del router y APs en la mayoría de las sedes.

Contramedidas

Revisar el plan de mitigación

Herramientas

N/A

Lecturas Adicionales

https://www.owisam.org/es/OWISAM-IF-001
http://web.nvd.nist.gov/view/vuln/search
http://www.exploit-db.com/
http://www.cvedetails.com/
http://www.routerpwn.com/

Observaciones

Esta prueba fue realizada con las siguientes características:
Fase de metodología ISSAF: Análisis de seguridad
Sub fase de la metodología ISSAF: Controles Técnicos - Pruebas de infraestructura
Modo de ataque: Activo

11. Pruebas sobre directivas y normativa

Proceso

Determinar el conjunto de buenas prácticas, que la institución destina para la seguridad de la red inalámbrica.

Se realizarán preguntas relacionadas con la seguridad perimetral, políticas de uso de redes inalámbricas, políticas de gestión y cambio de claves a las 3 sedes. Cada respuesta tiene una valoración de 25%.

Pre-requisitos

- Deben constar en el acta de reunión.

Ejemplos/Resultados

Preguntas	Cuenta con	
Seguridad Perimetral	**Si**	**No**
Los AP inalámbricos cuentan con medidas de seguridad como por ejemplo: cerraduras con llave, cajas de protección, cámaras o algún protector.		
La comunicación inalámbrica no se extienda más allá de los límites físicos de la organización.		
Si la intención es para restringir el acceso de red inalámbrica a ubicaciones dentro de los edificios y áreas externas, verificar que los AP están colocados en zonas internas del edificio y no cerca de las paredes exteriores y ventanas.		
Con un plan en marcha para hacer frente con el robo de todos o algún de dispositivos inalámbricos.		
Análisis de la política de uso/restricción de uso de redes inalámbricas		
La existencia de una política de seguridad donde trate el uso de la tecnología inalámbrica, incluyendo el uso de 802.11.		
Todos los usuarios esten capacitados en el uso adecuado y los peligros de la tecnología de red inalámbrica.		
Con una evaluación de riesgos de seguridad para determinar el valor de los activos de la organización que están expuestos a la red inalámbrica.		
Con auditorías de seguridad anuales esporádicas para monitorear y rastrear dispositivos.		
Análisis de la política de gestión y cambio de claves		
Con personal autorizado para cambiar las contraseñas de los AP inalámbricos.		
Todos los AP cuentan con contraseñas administrativas fuertes.		
Una regla de contraseñas para los dispositivos inalámbricos es que se cambien con regularidad y almacenen de forma segura.		
Que los routers inalámbricos, gateways y AP inalámbricos no almacenen la contraseña de administración en texto plano por defecto en Management Information Base (MIB)		

Análisis/Conclusión/Observación

Resultados

Sedes	Seguridad Perimetral		Política de uso/restricción de uso de redes inalámbricas		Política de gestión y cambio de claves		
	SI	NO	SI	NO	SI	NO	Desconoce
1	25%	75%	0%	100%	0%	75%	25%
2	25%	75%	0%	100%	0%	75%	25%
3	50%	50%	0%	100%	0%	75%	25%
4	25%	75%	0%	100%	0%	75%	25%
5	50%	50%	0%	100%	0%	75%	25%

Contramedidas

Revisar el plan de mitigación

Herramientas

Tomado de las metodologías ISSAF versión 2.1, OSSTMM versión 2.1 y 3, OSSTMM versión 2.1 orientado a redes inalámbricas.

Lecturas Adicionales

https://www.owisam.org/es/Pruebas_sobre_directivas_y_normativa_OWISAM-GD

Observaciones

Esta prueba fue realizada con las siguientes características:
Fase de metodología ISSAF: Auditoria y Revisión
Sub fase de la metodología ISSAF: Controles de Gestión
Modo de ataque: Pasivo

12. Análisis del protocolo SNMP en la red inalámbrica

Proceso

Analizar la versión del protocolo SNMP en los dispositivos inalámbricos.

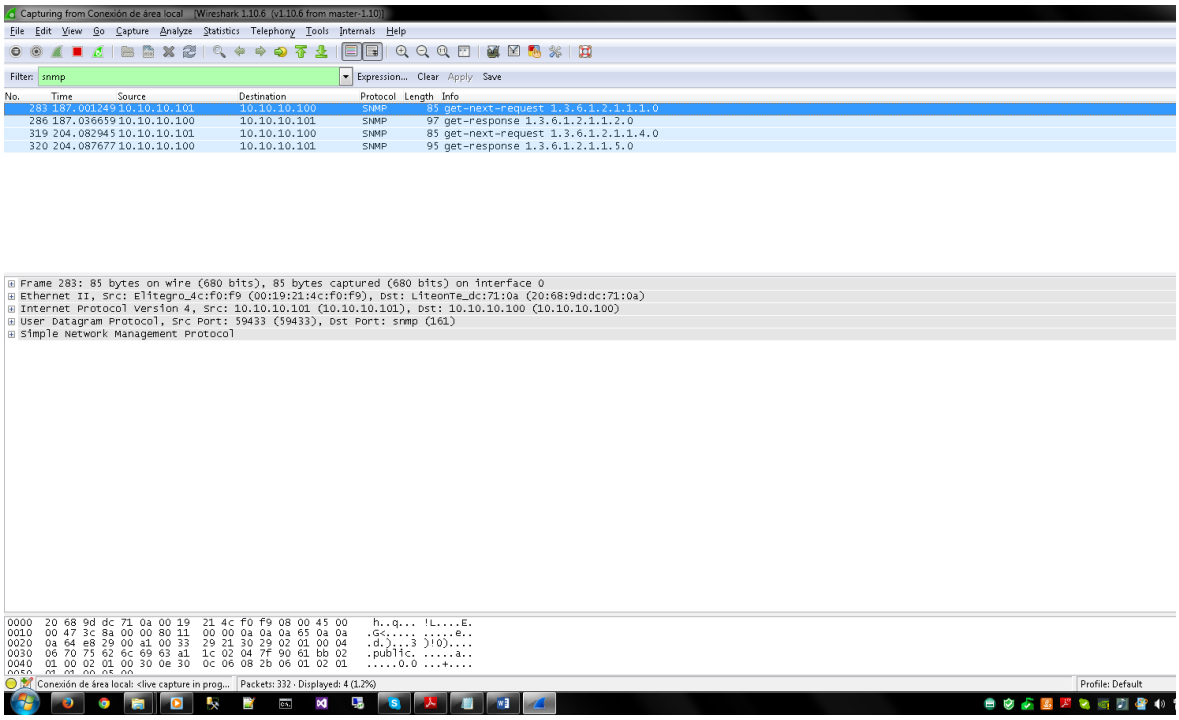
Escanear los puertos del dispositivo inalámbrico, revisar los puertos 161 y 162, estandarizados para el uso de este protocolo.

Pre-requisitos

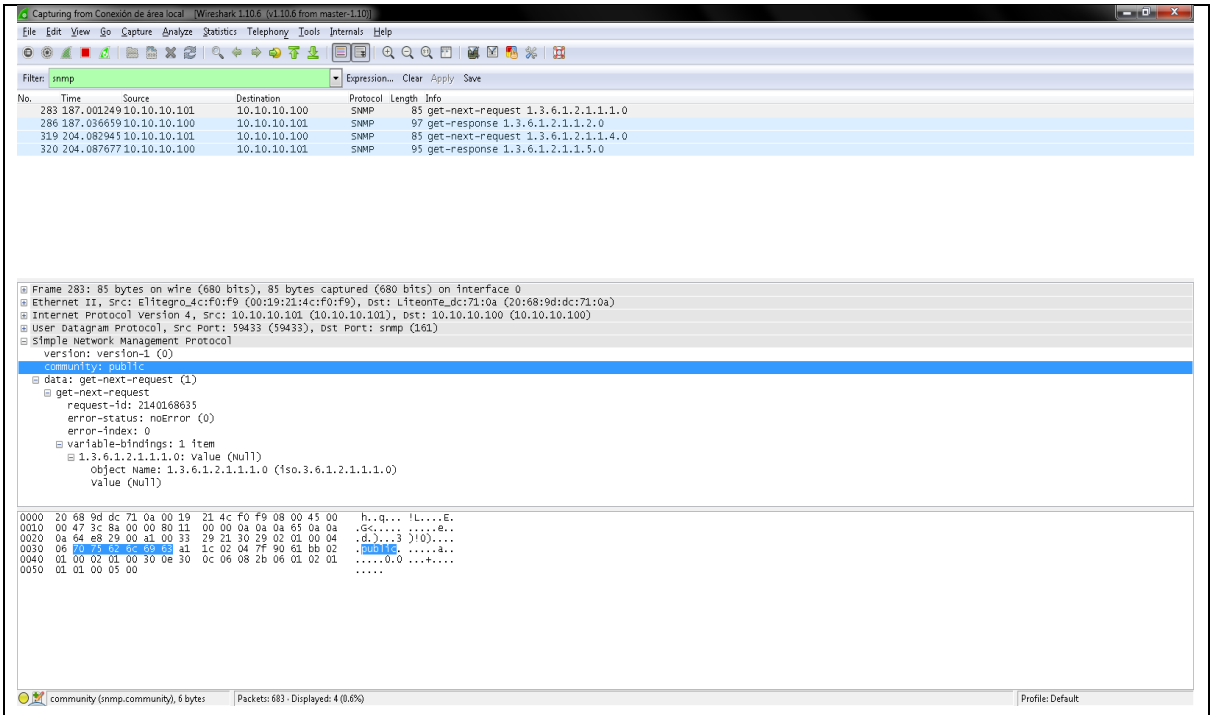
Tener instalado Wireshark y MIB Browser las últimas versiones.

Ejemplos/Resultados

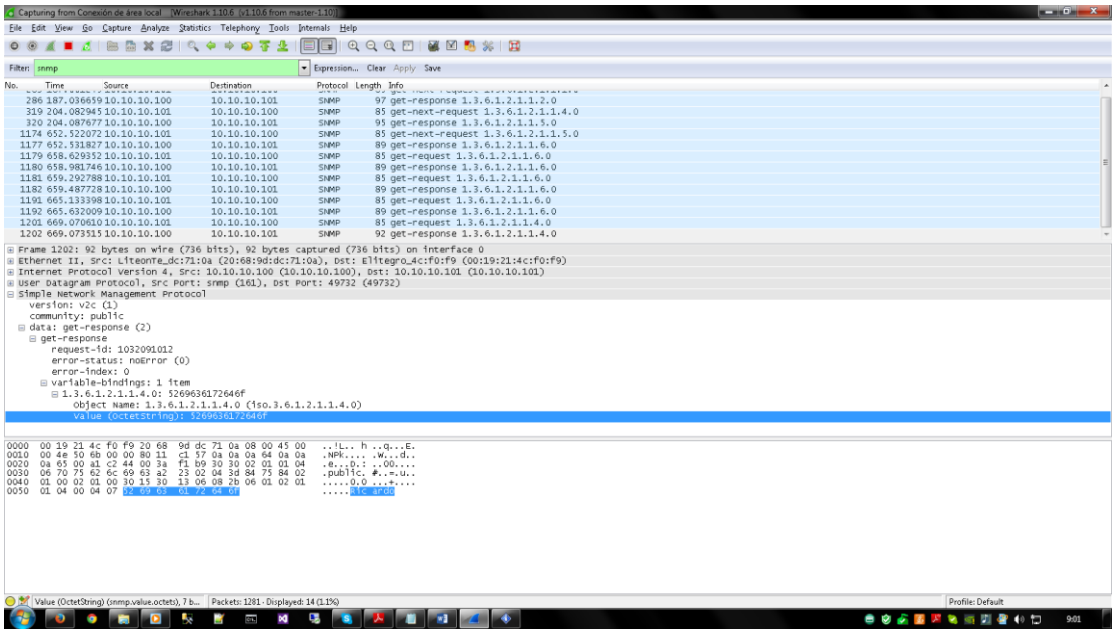
Con la herramienta WireShark, escaneamos la red, para capturar paquetes con filtrado por protocolo SNMP.



Una vez escaneadas las tramas, podemos visualizar los campos de Versión, comunidad entre otros.

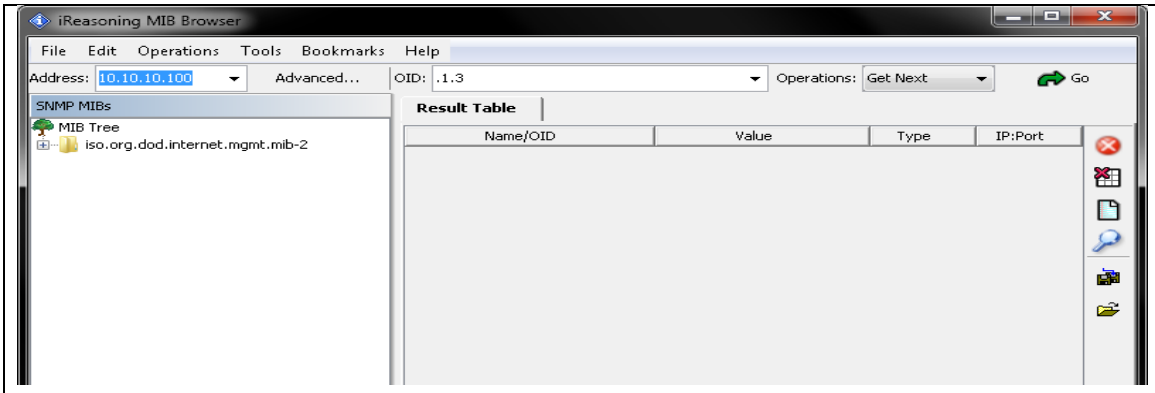


Protocolo SNMP con Versión 1 (de la sede 2).

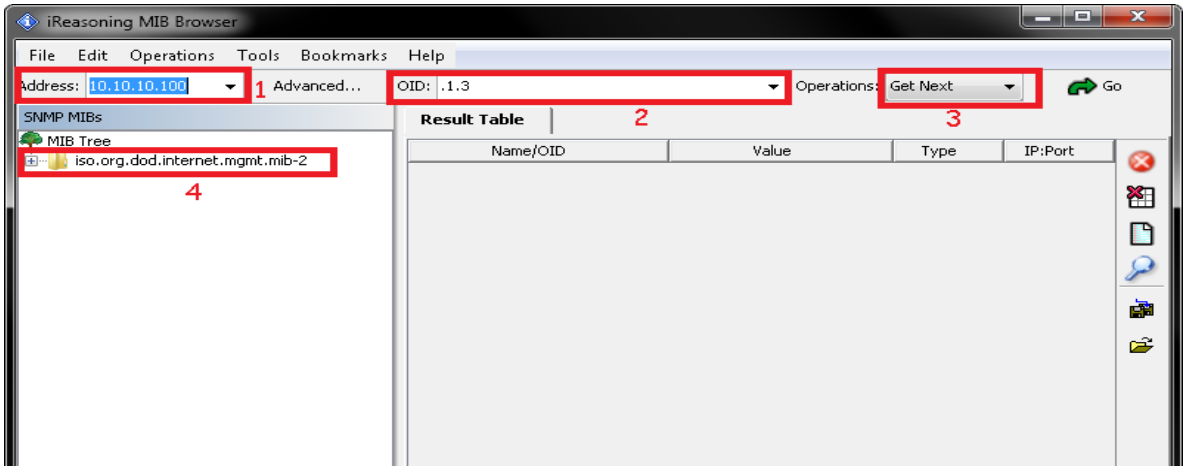


Protocolo SNMP con Versión 2c (de la sede 2).

Si la versión es 1 o 2c, se puede explotar esta vulnerabilidad, enviando peticiones a esa dirección con la herramienta MIB-Browser, la cual nos permite realizar consultas.

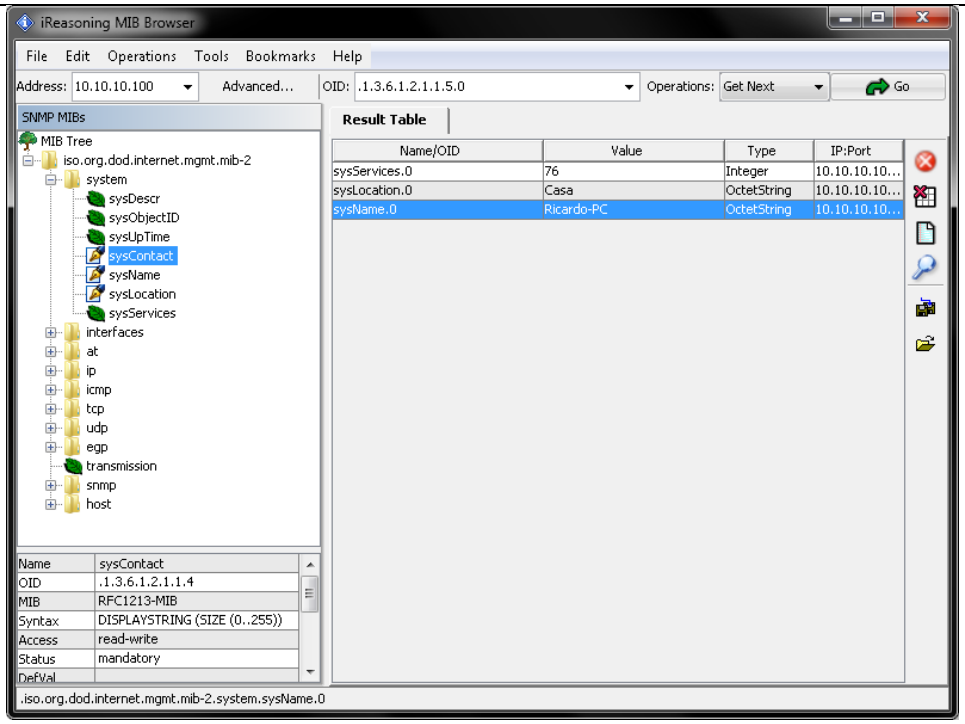


Peticiones para SNMP



Dirección IP destino de la Petición a realizar
OID: Numero de MIB, se selecciona automáticamente seleccionando en la opción 4 la MIB para la consulta.
MIB: Pequeña base de datos de los dispositivos, guarda estadísticas o información de uso o de vital importancia del sistema.
Petición que se desea realizar al dispositivo destino.
Árbol Mib: Bases o información que se puede obtener mediante la petición.

A continuación se presenta un ejemplo después de realizar algunas peticiones a la computadora con dirección IP 10.10.10.100



Análisis/Conclusión/Observación

En la sede 3 se pudo confirmar que se encuentran habilitados el protocolo SNMP dentro de 2 dispositivos con versión 1 y 2, esto es una debilidad para que un atacante pueda realizar denegación de servicio por medio de inyección de código malicioso.

Contramedidas

Revisar en el plan de mitigación

Herramientas

Wireshark
MIB Browser

Lecturas Adicionales

Observaciones

Esta prueba fue realizada con las siguientes características:
Fase de metodología ISSAF: Explotación y Ataque
Sub fase de la metodología ISSAF: N/A
Modo de ataque: Activo

13 Análisis de protocolos de cifrado inseguro (WEP, TKIP,...)

Proceso

Verificar los protocolos de cifrado maneja los dispositivos, ya que dentro de cada uno de estos protocolos se manejan algoritmos con propósitos específicos.
Con la suite aircrack-ng nos permite atacar la captura de tráfico que queremos descifrar.

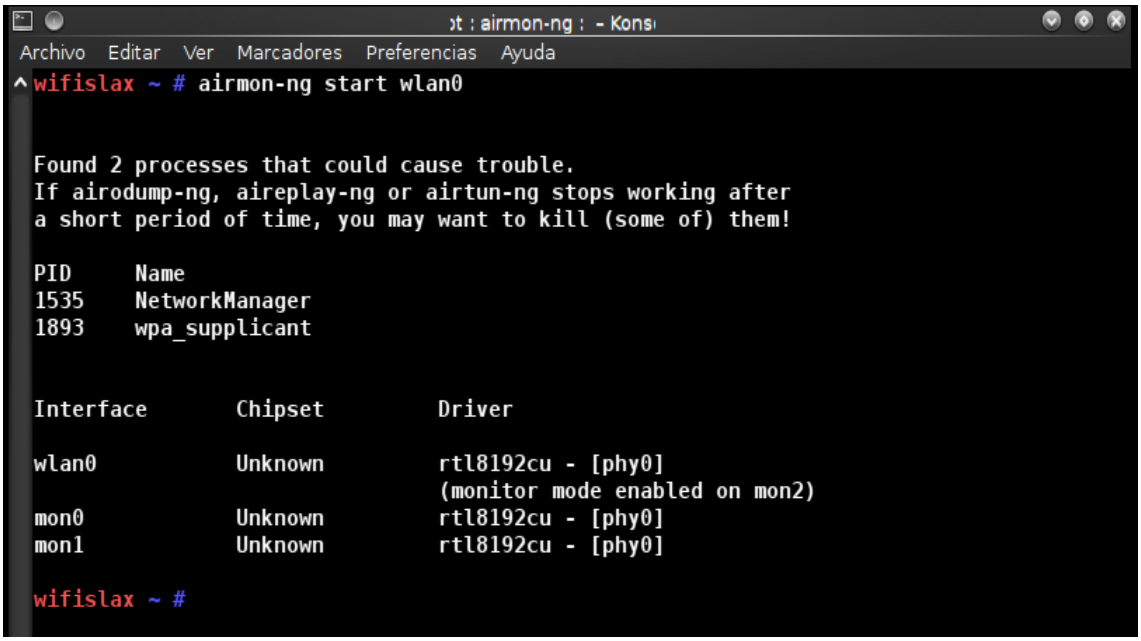
Pre-requisitos

Tener el sistema operativo Wifislax versión 4.10 donde dentro de ella vienen embebidos varias herramientas destinadas para el análisis y auditoria de redes inalámbricas. Uno de ellos que fueron utilizados, es suite de Aircrack. (Wifislax es un sistema operativo que puede ser booteable como liveCD).

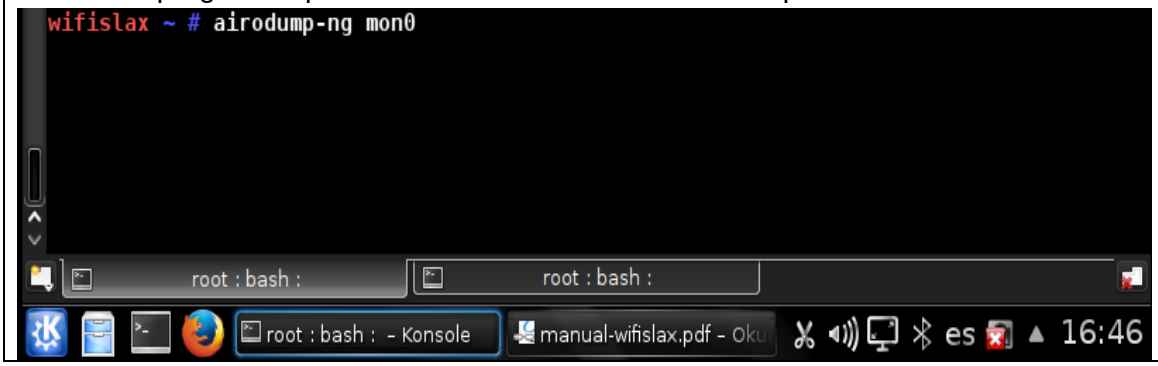
Ejemplos/Resultados

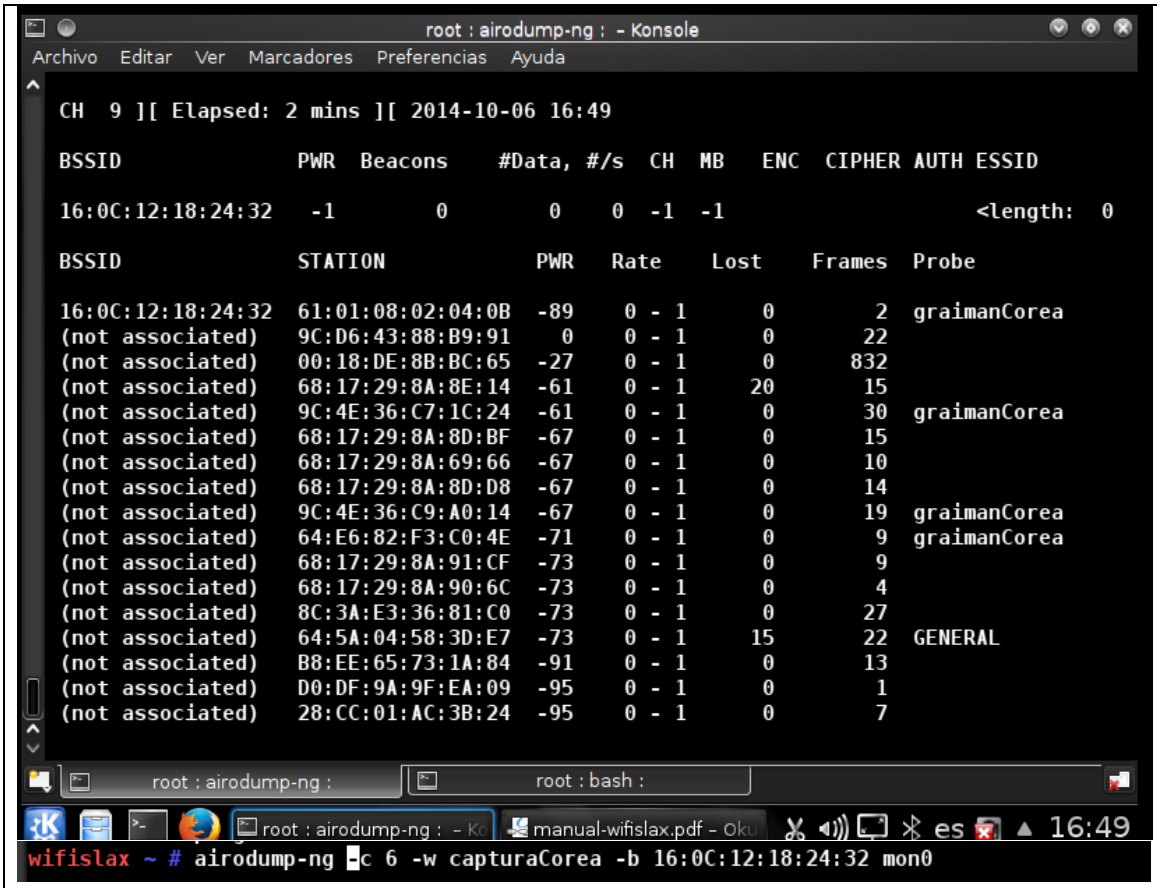
Los comandos que se van a utilizar son:

1: airmon-ng start wlan0 permite crear una interfaz de modo de monitor correspondiente al dispositivo wlan0. Esta nueva interfaz de modo de monitor será nombrado mon0.



2: airodump-ng mon0 permite encontrar la red inalámbrica para este caso de estudio.





Análisis/Conclusión/Observación
En la sede 2 se pudo constatar que se encuentra configurado uno de los dos dispositivos inalámbricos como mecanismo de cifrado WEP y en su mayoría con WPA- WPA2.
Contramedidas
Revisar en el plan de mitigación
Herramientas
Suite aircrack versión 4.10.
Lecturas Adicionales
https://www.owisam.org/es/OWISAM-CP-004
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Análisis y Búsqueda Sub fase de la metodología ISSAF: Controles de implementación Modo de ataque: Activo

14. Captura y cracking de claves transmitidas en el proceso de autenticación

Proceso

Determinar si es posible realizar una captura y cracking de las contraseñas para acceder a la red inalámbrica.
Se utilizará la suite Aircrack

Pre-requisitos

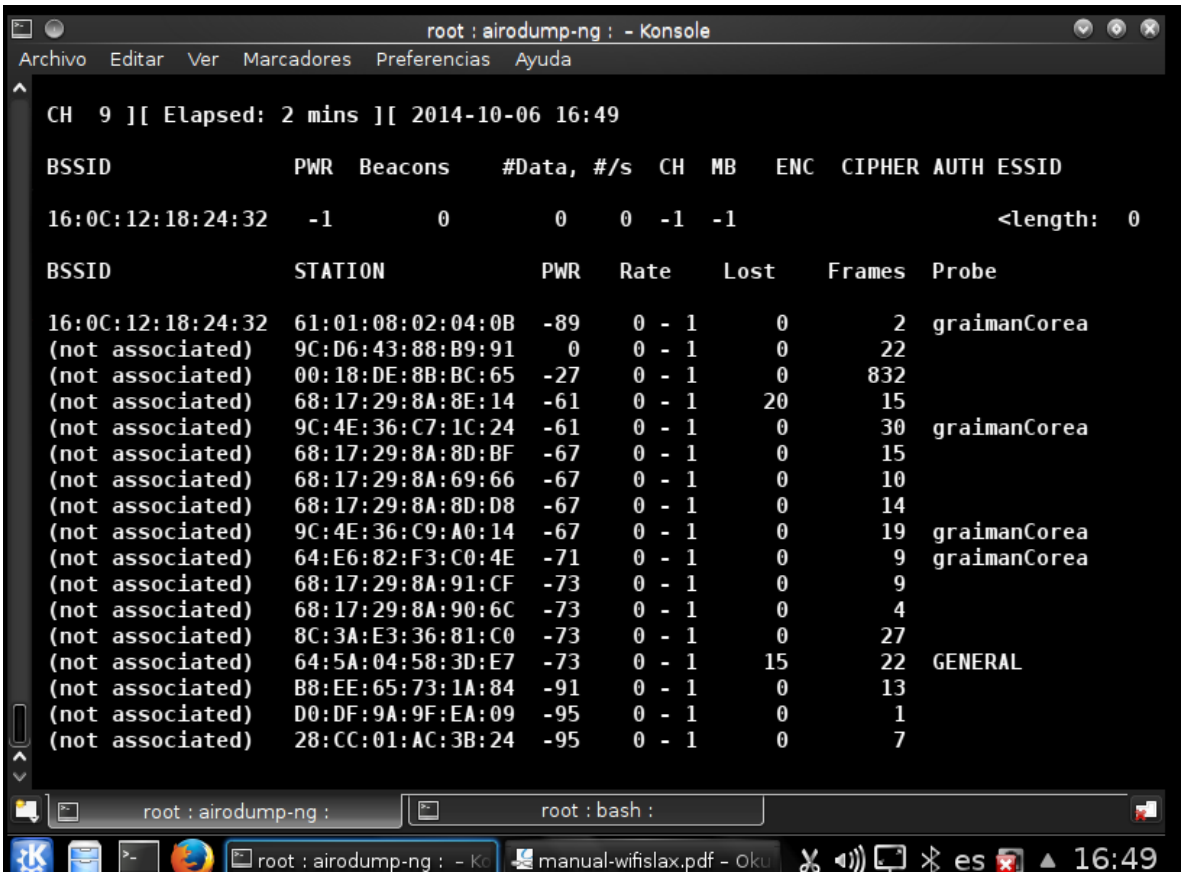
Tener el sistema operativo Wifislax versión 4.10 donde dentro de ella vienen embebidos varias herramientas destinadas para el análisis y auditoria de redes inalámbricas. Uno de ellos que fueron utilizados, es suite de Aircrack. (Wifislax es un sistema operativo que puede ser booteable como liveCD).

Ejemplos/Resultados

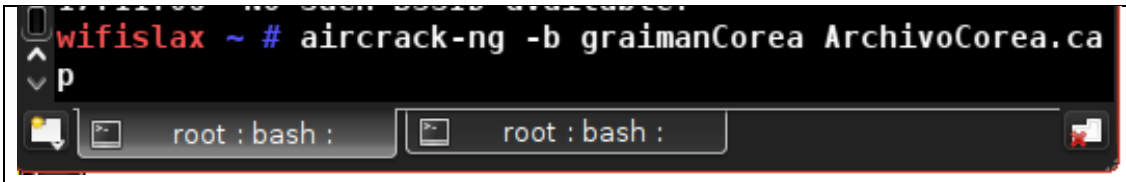
Dentro del sistema operativo WifiSlax se utilizará la suite Aircrack y se procede a ejecutar los siguientes comandos:
1: airodump-ng –c CANAL–w Nombre –b MACROUTER mon0. Con este comando se puede observar los usuarios conectados, los paquetes que estos envían, para capturar esos paquetes en un archivo o fichero, agregar el nombre del archivo.

```
wifislax ~ # airodump-ng -c 6 -w capturaCorea -b 16:0C:12:18:24:32 mon0
```

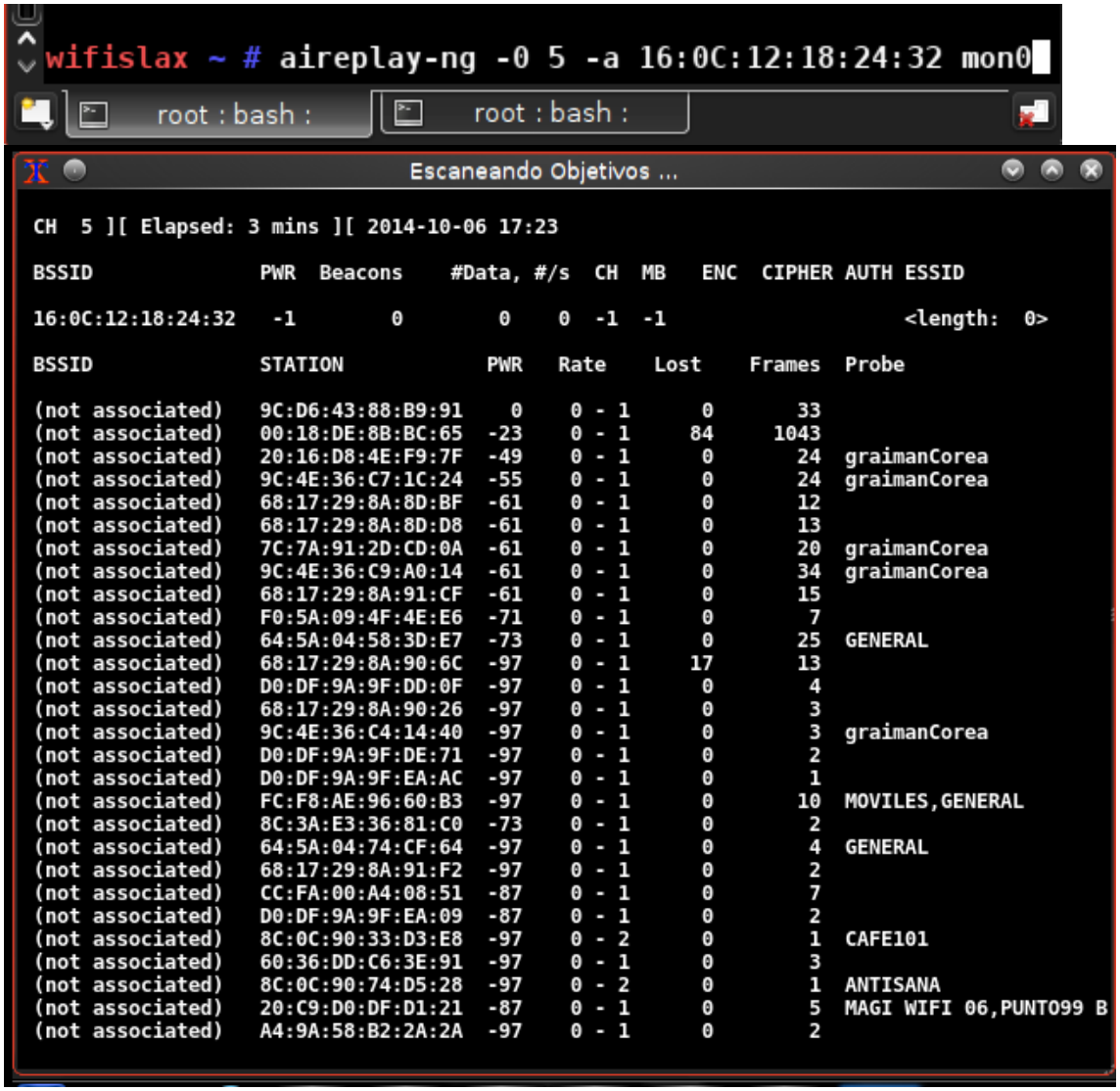
resultado



2: aircrack-ng [nombreArchivo].cap permite obtener la contraseña de la red, se debe capturar el envío de algún paquete del cliente, suplantarlo y enviar varias peticiones al router para generar tráfico.



3: Aireplay-ng -3 –b MACROUTER –h MACCLIENTE mon0. Permite generar handshake manualmente.



4: aircrack-ng –a 2 –e WLAN_E5 –w dict.txt [nombreArchivo].cap. Permite obtener la claver WPA/PSK de la red atacada

Análisis/Conclusión/Observación

Se pudo obtener las contraseñas cuando los dispositivos tenían cifrado WEP. En cambio para el cifrado WPA-WPA2, no se obtuvo el mismo resultado debido a que se utilizaron diccionarios para crackear la red inalámbrica no fueron los adecuados, se demoró en analizar 4 horas y aún así no mostraba ningún resultado.

Contramedidas

Revisar en el plan de mitigación

Herramientas

Suite Aircrack 4.10.
Lecturas Adicionales
https://www.owisam.org/es/OWISAM-AU-004
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Explotación y Ataque Sub fase de la metodología ISSAF: N/A Modo de ataque: Activo

15. Detección de APs falsos

Proceso

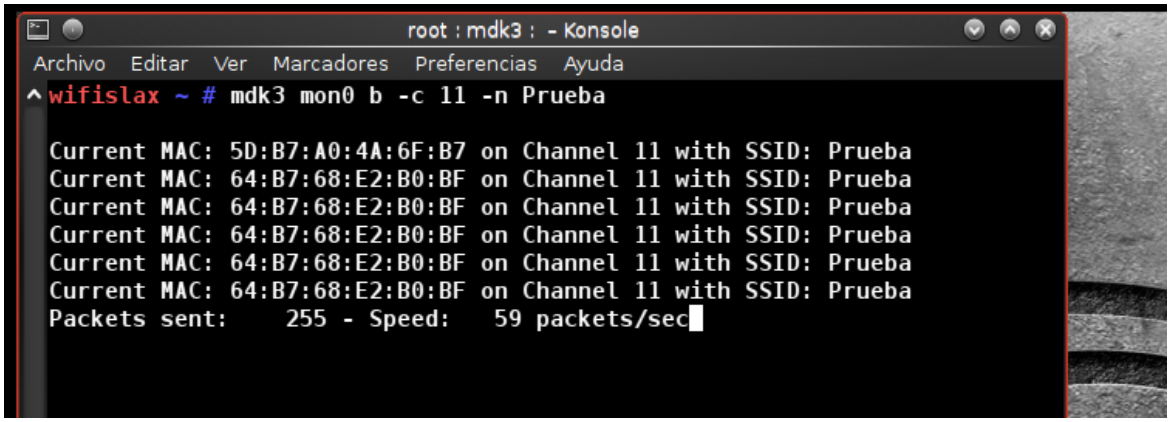
Engañar al usuario y forzar su vinculación y conexión a ellos.
Permite poner el escenario donde un atacante a través de APs falsos ataca a usuarios y gana acceso a la red interna de la institución. La detección de APs falsos al ser un ataque de forma activa realiza el análisis del inventario de los APs y encontrando su ubicación, al ser de forma pasiva realiza un análisis de comportamiento.

Pre-requisitos

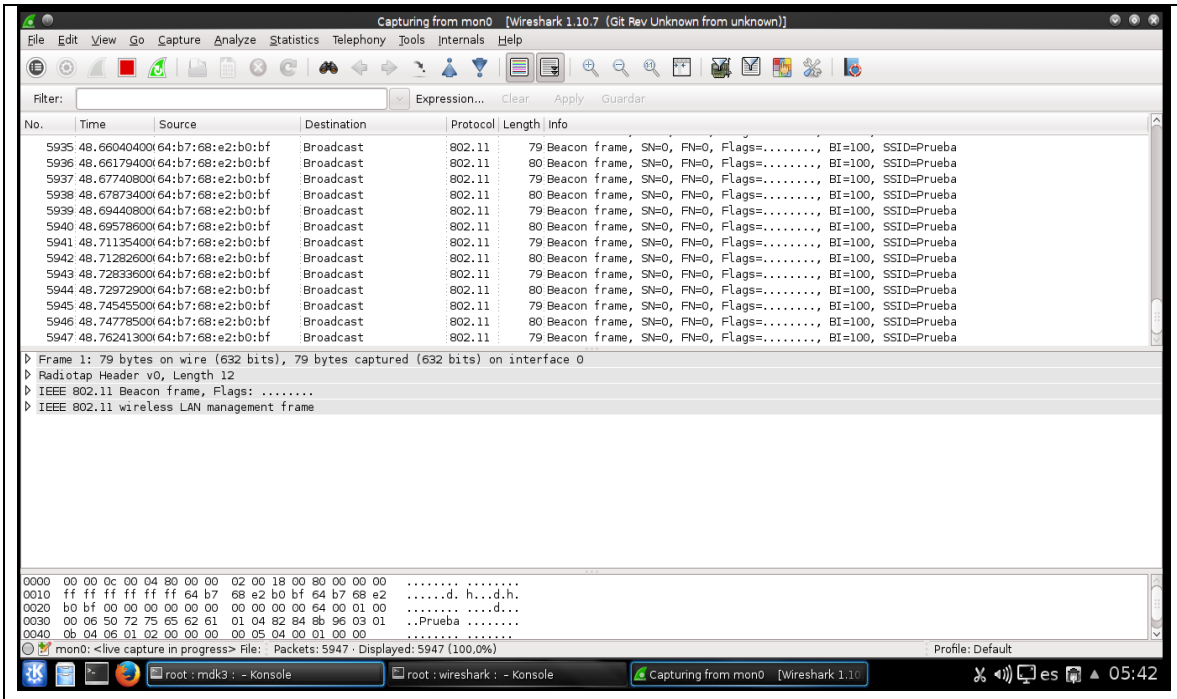
Tener el sistema operativo Wifislax versión 4.10 donde dentro de ella vienen embebidos varias herramientas destinadas para el análisis y auditoria de redes inalámbricas. Uno de ellos que fueron utilizados, es suite de Aircrack. (Wifislax es un sistema operativo que puede ser booteable como liveCD).
Tener instalado Wireshark para analizar los paquetes.
Tener instalado Acrylic para analizar las redes inalámbricas presentes.

Ejemplos/Resultados

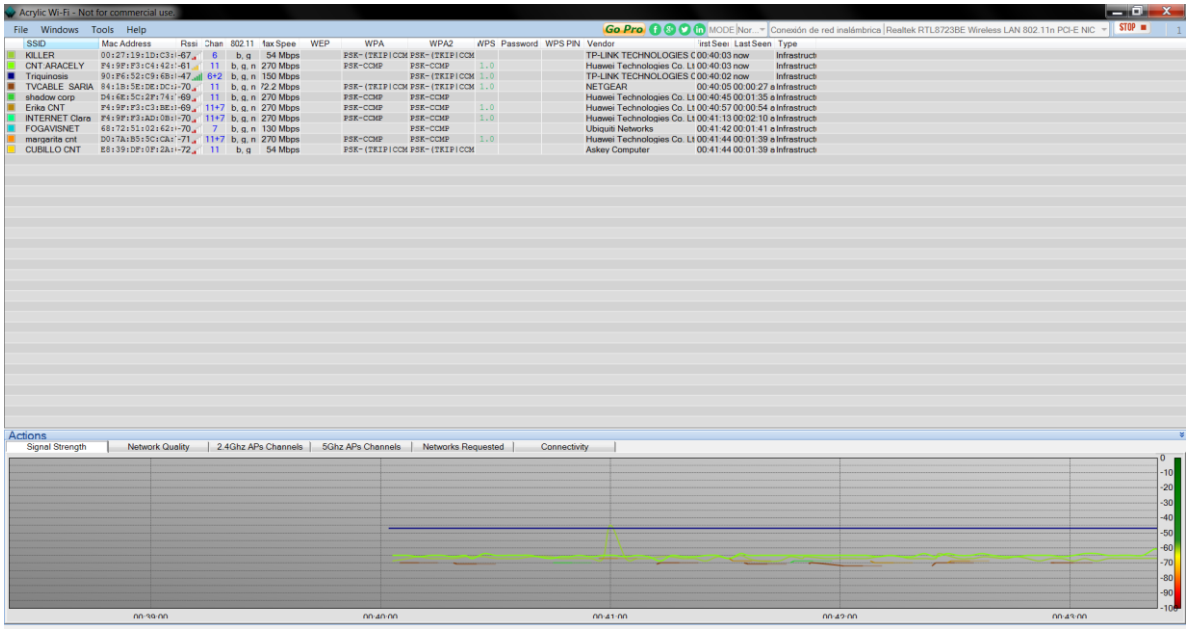
1: mdk3 mon0 b –c 11 –n Prueba
Permite crear el AP falso con SSID llamado prueba



En la herramienta Wireshark se puede observar que está creada el AP falso ya que está enviado tramas.



Pero en la herramienta Acrylic se puede ver que no reconoce en AP falso creado.



Análisis/Conclusión/Observación

Esta prueba consiste en captar la conexión del cliente y permitirnos tomar las claves o información que podamos obtener.

Esta prueba no tuvo éxito en la institución debido a que para la prueba, la autora no cuenta con el chipset (tarjeta para auditoría de red inalámbrica) respectiva para la ejecución de la prueba.

Contramedidas

Revisar el plan de mitigación

Herramientas

Mdk3, Wireshark, Acrylic las últimas versiones.

Lecturas Adicionales

https://www.owisam.org/es/OWISAM-FP-002 https://www.owisam.org/es/OWISAM-CT-001 https://www.owisam.org/es/Fingerprinting_OWISAM-FP
Observaciones
Esta prueba fue realizada con las siguientes características: Fase de metodología ISSAF: Explotación y Ataque Sub fase de la metodología ISSAF: N/A Modo de ataque: Activo

16. Pruebas de deautenticación

Proceso

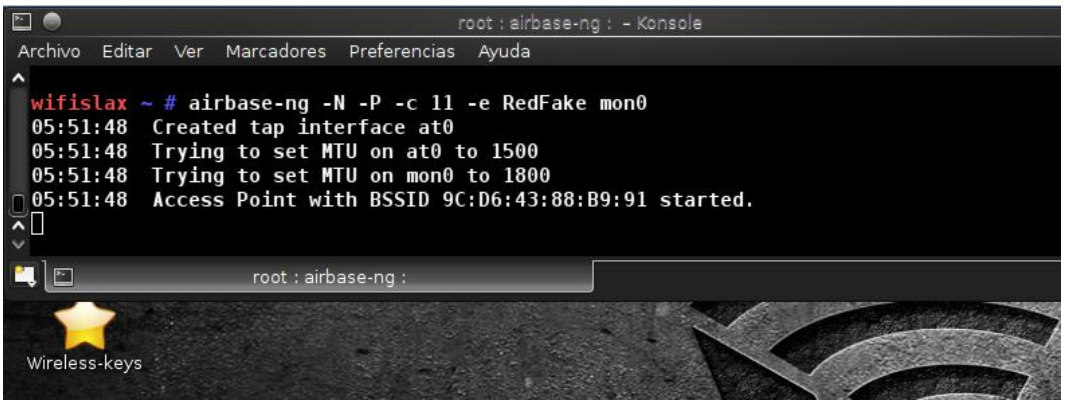
Denegar el servicio a los clientes internos de la institución.
La deautenticación hace que los usuarios conectados al AP, pierdan la conexión y da la posibilidad de que vuelvan a reconectarse.
Se puede hacer uso de una herramienta como aireplay-ng para llevar a cabo este tipo de ataques mediante el envío de frames generados de forma automática para la denegación de servicios.

Pre-requisitos

Tener el sistema operativo Wifislax versión 4.10 donde dentro de ella vienen embebidos varias herramientas destinadas para el análisis y auditoria de redes inalámbricas. Uno de ellos que fueron utilizados, es suite de Aircrack. (Wifislax es un sistema operativo que puede ser booteable como liveCD).
Tener instalado Wireshark para analizar los paquetes.

Ejemplos/Resultados

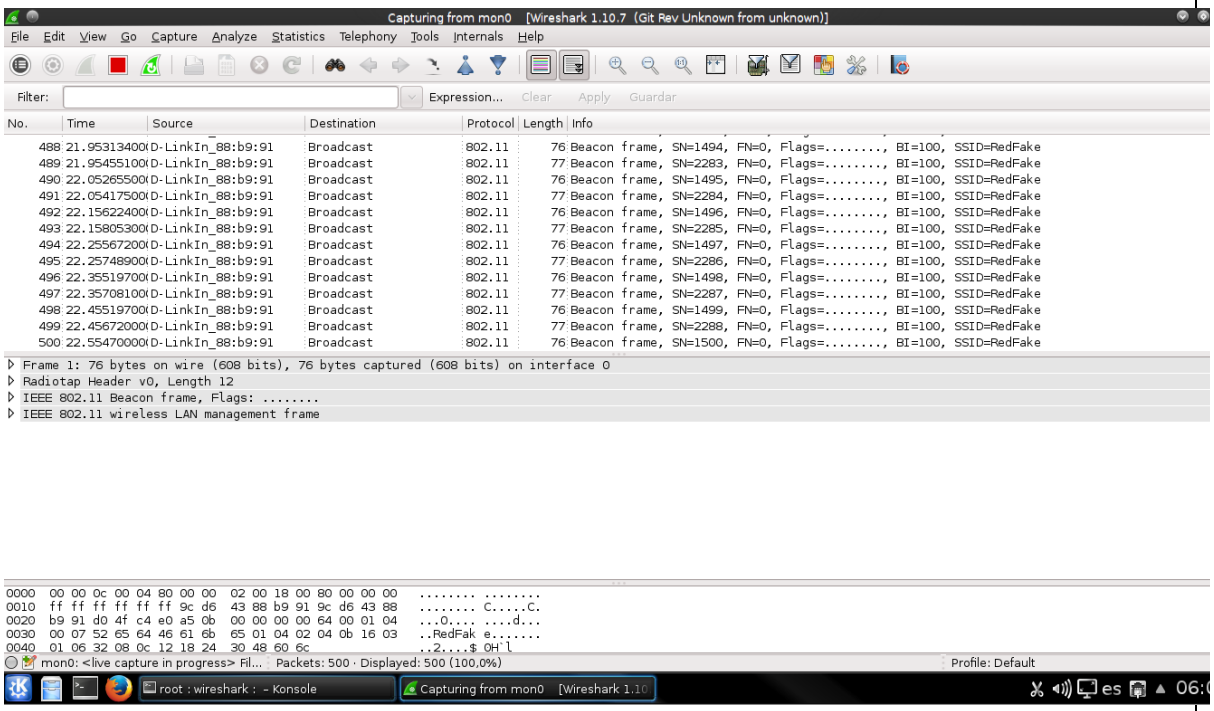
1. Levantamiento de Red Falsa para acceso a oros usuarios, libre, no necesita autenticación



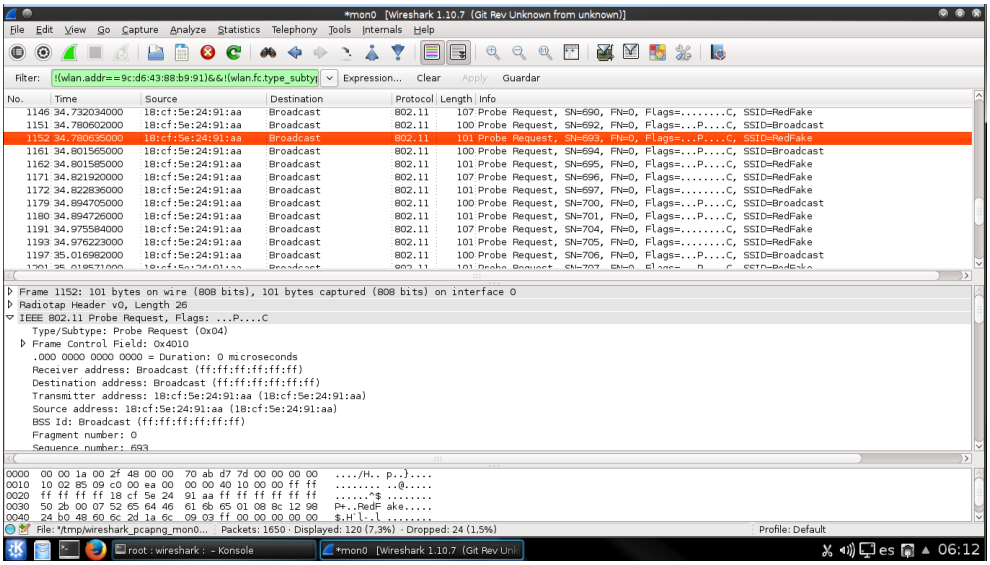
Validación (Windows 7)

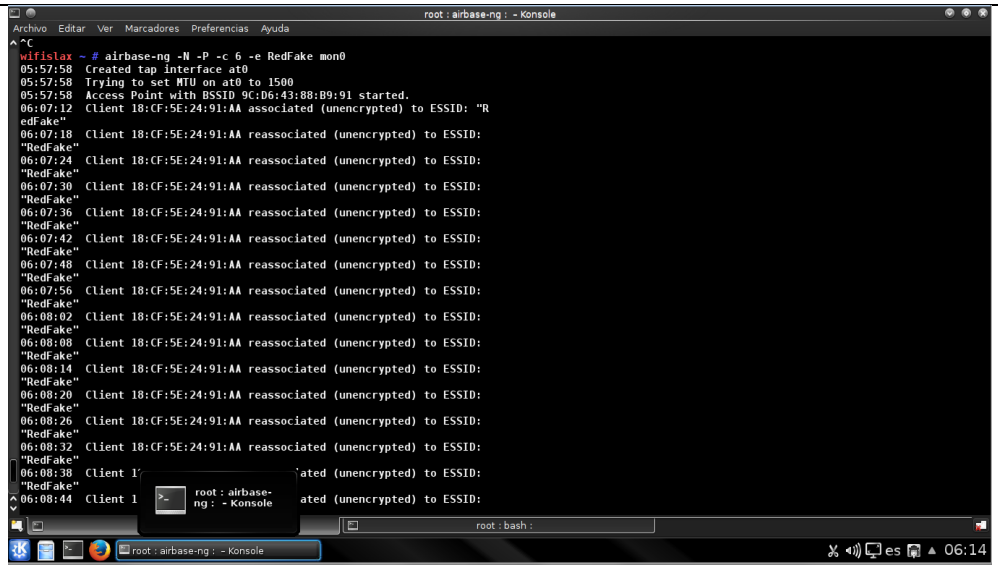
2. Cambio de Canales de mon0 y de wlan1

3. Captura de trafico en Wifislax con wireshark



El usuario intenta autenticación y se muestra su dirección IP, para poder desautenticarlo o falsear MAC, en caso de filtrado por MAC





Análisis/Conclusión/Observación

Los clientes sufrieron denegación de servicio, al enviar peticiones de un cliente indicando cierre de sesión al AP, este le desconectó lo que obligó al cliente otra vez acceder a la nueva red; se aprovechó capturando el handshake para obtener las claves de autenticación de la red.

Contramedidas

Revisar en el plan de mitigación.

Herramientas

Suite de Aircrack.
Wireshark última versión.

Lecturas Adicionales

https://www.owisam.org/es/OWISAM-DS-001
http://www.aircrack-ng.org/doku.php?id=deauthentication

Observaciones

Esta prueba fue realizada con las siguientes características:
Fase de metodología ISSAF: Explotación y Ataque
Sub fase de la metodología ISSAF: N/A
Modo de ataque: Activo

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.
- 5.1.1 Conjunto de políticas para la seguridad de la información.
- 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.
- 6.1.1 Asignación de responsabilidades para la segur. de la información.
- 6.1.2 Segregación de tareas.
- 6.1.3 Contacto con las autoridades.
- 6.1.4 Contacto con grupos de interés especial.
- 6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.
- 6.2.1 Política de uso de dispositivos para movilidad.
- 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.
- 7.1.1 Investigación de antecedentes.
- 7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.
- 7.2.1 Responsabilidades de gestión.
- 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
- 7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.
- 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.
- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 8.1.3 Uso aceptable de los activos.
- 8.1.4 Devolución de activos.

8.2 Clasificación de la información.
- 8.2.1 Directrices de clasificación.
- 8.2.2 Etiquetado y manipulado de la información.
- 8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.
- 8.3.1 Gestión de soportes extraíbles.
- 8.3.2 Eliminación de soportes.
- 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.
- 9.1.1 Política de control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.
- 9.2.1 Gestión de altas/bajas en el registro de usuarios.
- 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
- 9.2.4 Gestión de información confidencial de autenticación de usuarios.
- 9.2.5 Revisión de los derechos de acceso de los usuarios.
- 9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.
- 9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.
- 9.4.1 Restricción del acceso a la información.
- 9.4.2 Procedimientos seguros de inicio de sesión.
- 9.4.3 Gestión de contraseñas de usuario.
- 9.4.4 Uso de herramientas de administración de sistemas.
- 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

10.1 Controles criptográficos.
- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.
- 11.1.1 Perímetro de seguridad física.
- 11.1.2 Controles físicos de entrada.
- 11.1.3 Seguridad de oficinas, despachos y recursos.
- 11.1.4 Protección contra las amenazas externas y ambientales.
- 11.1.5 El trabajo en áreas seguras.
- 11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.
- 11.2.1 Emplazamiento y protección de equipos.
- 11.2.2 Instalaciones de suministro.
- 11.2.3 Seguridad del cableado.
- 11.2.4 Mantenimiento de los equipos.
- 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 11.2.8 Equipo informático de usuario desatendido.
- 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.
- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.
- 12.1.3 Gestión de capacidades.
- 12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.
- 12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.
- 12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.
- 12.4.1 Registro y gestión de eventos de actividad.
- 12.4.2 Protección de los registros de información.
- 12.4.3 Registros de actividad del administrador y operador del sistema.
- 12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.
- 12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.
- 12.6.1 Gestión de las vulnerabilidades técnicas.
- 12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.
- 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.
- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.
- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.
- 14.2.1 Política de desarrollo seguro de software.
- 14.2.2 Procedimientos de control de cambios en los sistemas.
- 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 14.2.4 Restricciones a los cambios en los paquetes de software.
- 14.2.5 Uso de principios de ingeniería en protección de sistemas.
- 14.2.6 Seguridad en entornos de desarrollo.
- 14.2.7 Externalización del desarrollo de software.
- 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- 14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.
- 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.
- 15.1.1 Política de seguridad de la información para suministradores.
- 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
- 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.
- 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
- 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras.
- 16.1.1 Responsabilidades y procedimientos.
- 16.1.2 Notificación de los eventos de seguridad de la información.
- 16.1.3 Notificación de puntos débiles de la seguridad.
- 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
- 16.1.5 Respuesta a los incidentes de seguridad.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.
- 17.1.1 Planificación de la continuidad de la seguridad de la información.
- 17.1.2 Implantación de la continuidad de la seguridad de la información.
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.
- 18.1.1 Identificación de la legislación aplicable.
- 18.1.2 Derechos de propiedad intelectual (DPI).
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.
- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento de las políticas y normas de seguridad.
- 18.2.3 Comprobación del cumplimiento.

ANEXO I: LISTADO DE AMENAZAS

Este catálogo de amenazas es tomado de la norma ISO 27002
La siguiente es una lista de amenazas. Esta no es una lista definitiva. Cada organización puede agregar amenazas por situaciones específicas.

Acceso físico no autorizado
Acceso no autorizado a la red
Acceso no autorizado al sistema de información
Amenaza de bomba
Ataques terroristas
Código malicioso
Contaminación
Daños ocasionados durante pruebas de intrusión
Daños provocado por actividades de terceros
Descarga de un rayo
Destrucción de registros
Deterioro de soportes
Error de usuario
Errores de aplicaciones
Errores de mantenimiento
Escuchas encubiertas
Espionaje industrial
Explosión de bomba
Falla en los vínculos de comunicación
Fallas en equipos
Falsificación de registros
Fraude
Fraudes
Fuga o revelación de información
Huelgas
Identidad de usuario camuflada
Incendio
Incumplimiento de leyes
Incumplimiento de relaciones contractuales
Ingeniería social
Instalación no autorizada de software

Interceptación de información
Interrupción del suministro eléctrico
Inundación
Modificación accidental de datos del sistema de información
Modificación no autorizada de registros
Otros desastres (naturales)
Otros desastres (ocasionados por el hombre)
Pérdida de servicios soporte
Revelación de contraseñas
Robo
Uso de códigos no autorizados o no probados
Uso erróneo de herramientas de auditoría
Uso erróneo de sistemas de información
Uso no autorizado de materiales patentados
Uso no autorizado de software
Vandalismo

ANEXO J: PLAN DE MITIGACIÓN

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Plan de Mitigación

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
1	Incorrecta configuración a la red inalámbrica	Acceso a segmentos de red restringidos.	2,00	5	10,00	Cambiar los parámetros de configuración por defecto en los dispositivos inalámbricos.	- ISO/IEC 27002:2013: 9.1.1 Política de control de accesos - OWISAM: Cifrado de las comunicaciones Pruebas de infraestructura
2	Acceso no autorizado o a la red	Acceso no autorizado a redes inalámbricas	2,00	3	6,00	Establecer WPA2 con AES-CCMP como método de autenticación y cifrado, definiendo tiempo de renovación de claves prudencial.	-ISO/IEC 27002:2013: 9.1.1 Política de control de accesos, 9.1.2 Control de acceso a las redes y servicios asociados - OWISAM: Pruebas de re-inyección de de tráfico (replay attack, Mic,..)
3	Ingeniería social	Acceso no autorizado e interceptación de tráfico.	2,00	3	6,00	Establecer WPA2 con AES-CCMP como método de autenticación y cifrado, definiendo tiempo de renovación de claves prudencial.	- ISO/IEC 27002:2013: 9.2.5 Revisión de los derechos de acceso de los usuarios, - OWISAM: Pruebas de re-inyección de de tráfico (replay attack, Mic,..)

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
4	Incorrecta configuración a la red inalámbrica	Área de cobertura excesiva.	2,00	5	10,00	La potencia de los APs deben ser controlados y limitados al radio de cobertura de la institución. Revisar los parámetros Slottime, ACK y CTS Timeout para evitar que enlaces Wi-Fi sean accesibles a mayor distancia de la esperada.	- ISO/IEC 27002:2013: 9.2.3 Gestión de los derechos de acceso con privilegios especiales. - OWISAM: Verificación del nivel de intensidad de señal o área de cobertura.
5	Espionaje	Ataques a la disponibilidad del servicio.	2,00	4	8,00	"Se recomienda usar WPA2, si es posible. No es recomendable usar WEP. WPA o WPA2 son más seguros. Si prueba WPA o WPA2 y no funcionan, se recomienda que actualice el adaptador de red a uno que sea compatible con WPA o WPA2."[94]	- OWISAM: Pruebas de denegación de servicio
6	Incorrecta configuración a la red inalámbrica	Ausencia de sistemas de monitorización.	2,00	5	10,00	Preparar una calendarización de actividades donde se encuentren: plan de mantenimiento de equipos, seguridad de activos de la red inalámbrica.	ISO/IEC 27002:2013: 11.2.4 Mantenimiento de los equipos, 11.2.4 Mantenimiento de los equipos, 11.2.5 Salida de activos fuera de las dependencias de la empresa, 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones,
7	Incorrecta	Ausencia de validación de	2,00	5	10,00	Mecanismo alternativo de cifrado, puede ser el	- OWISAM: Cifrado de las comunicaciones,o

[94] Fuente: http://windows.microsoft.com/es-419/windows/what-are-wireless-network-security-methods#1TC=windows-7, último acceso 22/02/2015

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
	configuración a la red inalámbrica	certificados.				envío de credenciales a través de HTTPS, túneles VPN. Las redes abiertas generan nuevos vectores de ataque que un usuario malintencionado podría aprovechar.	Verificación del nivel de intensidad de señal o área de cobertura.
8	Incorrecta configuración a la red inalámbrica	Autenticación contra redes inalámbricas	2,00	5	10,00	Se deberían eliminar las redes preferidas de los dispositivos, sobretodo las que no se van a volver a utilizar (hoteles, cafeterías...) y las que pertenezcan a la entidad corporativa.	- ISO/IEC 27002:2013: 9.2.2 Gestión de los derechos de acceso asignados a usuarios, 9.2.3 Gestión de los derechos de acceso con privilegios especiales, 9.2.4 Gestión de información confidencial de autenticación de usuarios, 9.2.5 Revisión de los derechos de acceso de los usuarios - OWISAM: Descubrimiento de preferencias de redes conocidas de clientes
9	Incorrecta configuración a la red inalámbrica	Beacon frames habilitados	2,00	5	10,00	Deshabilitar los beacon frames, que no se publique, de forma que los usuarios que lo necesiten deban introducir este valor de forma manual a la hora de encontrar la red inalámbrica.[95]	
11	Falta de políticas	Configuración incorrecta.	2,00	4	8,00	Crear una política de recomendaciones	- ISO/IEC 27002:2013: 9.1.1 Política de control

[95] Fuente: Seguridad en redes inalámbricas, http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf último acceso: [29/05/2015]

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
	de seguridad						de accesos, “Tecnología inalámbrica para proteger la red Conectada por cable”
12	Falta de políticas de seguridad	Credenciales débiles.	2,00	4	8,00	Implementar un password robusto para APs, con caracteres especiales y alfanuméricos con una longitud mínima de diez caracteres y expiración de contraseña mensualmente.	- OWISAM: Cifrado de las comunicaciones
13	Fraude	Debilidad de seguridad en la red inalámbrica	2,00	4	8,00	El uso de los algoritmos de cifrado TKIP y WEP se encuentra desaconsejado por la Wi-Fi Alliance. Utilizar el protocol de cifrado AES-CCMP y sustituir los dispositivos que no lo soporten.	- OWISAM: Configuración de la plataforma
14	Pérdida de servicios soporte	Debilidades en elementos de arquitectura o software.	2,00	5	10,00	Consultar semestralmente las nuevas actualizaciones de firmware de los dispositivos inalámbricos.	- ISO/IEC 27002:2013: 6.1.1 Asignación de responsabilidades para la SI, OWISAM-IF Pruebas de infraestructura
15	Código malicioso	Degradación de la calidad del servicio.	2,00	4	8,00	Crear una calendarización de tareas: recordatorios de actualización de antivirus.	- ISO/IEC 27002:2013: 9.4.5 Control de acceso al código fuente de los programas, 12.2.1 Controles contra el código malicioso
17	Falta de políticas de seguridad	Detección de dispositivos emitiendo en frecuencias restringidas.	2,00	4	8,00	Configurar los dispositivos inalámbricos en canales de frecuencia no saturados.	- OWISAM: Fingerprinting, Configuración de la plataforma

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
19	Falta de políticas de seguridad	Dispositivos que no cumplen el estándar / propietarios	2,00	3	6,00	Crear políticas de seguridad donde explique la importancia y el uso de las redes inalámbricas. Capacitar al personal sobre su importancia.	- OWISAM: Pruebas de infraestructura
20	Escuchas encubiertas	Emisión de señal de clientes no autorizados	2,00	3	6,00	Cambiar la encriptación por la más fuerte disponible en el producto. Cambiar la version del firmware del dispositivo.	- OWISAM: Pruebas de infraestructura, OWISAM-FP Fingerprinting
21	Espionaje	Identificación de dispositivos mediante técnicas de descubrimiento activo	2,00	3	6,00	Crear periódicamente recordatorios que creen este escenario de hacking ético con el fin de encontrar nuevas vulnerabilidades.	- OWISAM: Descubrimiento de dispositivos, Fingerprinting
22	Espionaje	Interceptación de comunicaciones	2,00	3	6,00	Se recomienda que los clientes que accedan a estas redes no tengan configurada la opción de “conexión automática” aunque la red no se encuentre emitiendo. Verificar que el firmware está actualizado y no es posible obtener el nombre oculto tras solicitar el nombre.	Protección contra la denegación de servicio y las Suplantaciones[96] - OWISAM: Descubrimiento de redes ocultas
23	Intercepteación de información	Interceptación de credenciales de autenticación.	2,00	3	6,00	Se recomiendo utilizer el mecamismo de autenticación AES-CCMP. En las capas superiores es recomendable el uso	OWISAM: Pruebas sobre la autenticación, Pruebas de análisis de información transmitida a través de redes

[96] Fuente: Seguridad en redes inalámbricas

http://www.arubanetworks.com/pdf/products/DS_WIP_SP.pdfúltimo acceso: [29/05/2015]

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
						soluciones VPN, IPSec o SSL.	
24	Identidad de usuario camuflada	Intrusos en redes inalámbrica	2,00	4	8,00	Es importante mantener un inventario de todos los dispositivos autorizados, o al menos de los puntos de acceso, para facilitar la detección de APs falsos.	- OWISAM: Descubrimiento de dispositivos
25	Falta de políticas de seguridad	No cuentan con política de configuración de dispositivos.	2,00	4	8,00	Crear políticas de seguridad donde explique la importancia y el uso de las redes inalámbricas. Capacitar al personal sobre su importancia.	- ISO/IEC 27002:2013: 16.1.3 Notificación de puntos débiles de la seguridad, 8.1.3 Uso aceptable de los activos, - OWISAM: Análisis de la configuración de dispositivos
26	Falta de políticas de seguridad	No cuentan con política de gestión y cambio de claves	2,00	4	8,00	Crear una política que establezca una robustez mínima y una duración temporal máxima para las contraseñas que se empleen en la organización. Definir un tiempo de vida máximo para las claves de cifrado, tras el cual se volverán a generar unas nuevas. Esta funcionalidad debería estar activada y con un valor no superior a 3600s, para evitar ataques a la red inalámbrica.	- ISO/IEC 27002:2013: 9.1.1 Política de control de accesos, 9.1.2 Control de acceso a las redes y servicios asociados - OWISAM: Análisis de la política de gestión y cambio de claves
27	Falta de políticas de	No cuentan con política de uso/restricción	2,00	4	8,00	Se debe disponer de unas políticas claras y conocidas por todo el	- ISO/IEC 27002:2013: 5.1.1 Políticas para la seguridad de la

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
	seguridad	de uso de redes inalámbricas				personal sobre el uso de dispositivos con capacidades inalámbricas.	información, 5.1.2 Revisión de las políticas para la seguridad de la información, 13.1.1 Controles de red, 13.1.2 Mecanismos de seguridad asociados a servicios en red, 13.1.3 Segregación de redes, 13.2.4 Acuerdos de confidencialidad y secreto
28	Falta de políticas de seguridad	No cuentan con una verificación de inventario de dispositivos autorizados	2,00	4	8,00	Se debe disponer de unas políticas claras y conocidas por todo el personal sobre el uso de dispositivos con capacidades inalámbricas.	- ISO/IEC 27002:2013: 8.1.1 Inventario de activos, 8.1.2 Propiedad de los activos, 8.1.3 Uso aceptable de los activos, 8.1.4 Devolución de activos, 8.2.2 Etiquetado y manipulado de la información,
29	Falla en los vínculos de comunicación	Obtención de información sensible.	2,00	4	8,00	Asegurar que esté desactivada la autenticación por clave compartida.	- ISO/IEC 27002:2013: 16.1.1 Responsabilidades y procedimientos, 16.1.2 Notificación de los eventos de seguridad de la información, 16.1.3 Notificación de puntos débiles de la seguridad, 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones, 16.1.5 Respuesta a los incidentes de seguridad, 16.1.6Aprendizaje de los incidentes de seguridad de la información,16.1.7

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
							Recopilación de evidencias.
30	Deterioro de soportes	Obtención de información sobre el hardware y software.	2,00	3	6,00	Las redes de comunicaciones inalámbricas deben usar nombres que no identifiquen a la organización, evitando usar nombres genéricos de red para evitar ataques de suplantación de identidad de puntos de acceso.	- ISO/IEC 27002:2013: 5.1.1 Documento de política de seguridad de la información, 5.1.2 Revisión de la política de seguridad de la información, 8.3.1 Gestión de soportes extraíble, 15.2.1 Supervisión y revisión de los servicios prestados por terceros
31	Deterioro de soportes	Permite la inyección de código malicioso	2,00	3	6,00	Es deseable disponer de un sistema de detección de intrusos (WIDS, Wireless Intrusion Detection System), que detecte y notifique la aparición de nuevos dispositivos o comportamientos anómalos.	- ISO/IEC 27002:2013: 9.4.5 Control de acceso al código fuente de los programas, 12.2.1 Controles contra el código malicioso, 14.1.1 Análisis y especificación de los requisitos de seguridad,
32	Falta de políticas de seguridad	Robo de credenciales y acceso no autorizado.	2,00	4	8,00	Como primera medida, se debe hacer hincapié en usar el sistema de cifrado más robusto del que se dispone a nivel de capa de enlace (actualmente AES-CCMP). En las capas superiores es recomendable el uso soluciones VPN, IPSec o SSL.	- ISO/IEC 27002:2013: 9.2.5 Revisión de los derechos de acceso de los usuarios,
33	Falta de políticas	Suplantación de punto de	2,00	4	8,00	Es importante mantener un inventario de todos los	- ISO/IEC 27002:2013: 9.2.2 Gestión de los

#	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Recomendaciones	Normas / Estándar de Referencia
	de seguridad	acceso y DOS.				dispositivos autorizados, o al menos de los puntos de acceso, para facilitar la detección de APs falsos.	derechos de acceso asignados a usuario, OWISAM-DS Pruebas de denegación de servicio
35	Identidad de usuario camuflada	Suplantación de identidad.	2,00	3	6,00	Es importante mantener un inventario de todos los dispositivos autorizados, o al menos de los puntos de acceso, para facilitar la detección de APs falsos.	- ISO/IEC 27002:2013: 9.2.2 Gestión de los derechos de acceso asignados a usuario.,
37	Espionaje	Suplantación de punto de acceso y DOS.	2,00	3	6,00	Como primera medida, se debe hacer hincapié en usar el sistema de cifrado más robusto del que se dispone a nivel de capa de enlace (actualmente AES-CCMP). En las capas superiores es recomendable el uso soluciones VPN, IPSec o SSL.	- ISO/IEC 27002:2013: 9.2.2 Gestión de los derechos de acceso asignados a usuario, OWISAM-DS Pruebas de denegación de servicio
39	Robo	Acceso a las instalaciones donde están los equipos inalámbricos	2,00	4	8,00	Es importante mantener un inventario de todos los dispositivos autorizados, o al menos de los puntos de acceso, para facilitar la detección de APs falsos.	- ISO/IEC 27002:2013: 11.1.1 Perímetro de seguridad física, 11.1.2 Controles físicos de entrada, 11.1.3 Seguridad de oficinas, despachos y recurso, 11.1.4 Protección contra las amenazas externas y ambientales, 11.1.5 El trabajo en áreas seguras

ANEXO K: INFORMES PRESENTADOS

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Ejecutivo
Fecha:	2015/05/02		

Resumen ejecutivo

La institución acogió la propuesta de realizar la evaluación de la red inalámbrica utilizando metodologías formales de hacking ético, por parte de la estudiante de la carrera de Ingeniería de Sistemas Informáticos y de Computación de la Escuela Politécnica Nacional.

Agradeciendo al administrador de la red ya que dio la apertura a las reuniones para la recolección de información, ejecución de pruebas y proveer información requerida; se mostró dispuesto a pesar de su carga de trabajo diaria.

El presente informe da a conocer el conjunto de observaciones y recomendaciones obtenidas luego del análisis de evaluación de la red inalámbrica. Estos resultados son brindadas por la auditora con el objetivo de poner a consideración a la Alta Dirección para que evalúe y considere las medidas que son necesarias, para aumentar el nivel de seguridad de la red inalámbrica.

Alcance

Describir los problemas y propuestas de solución a la Seguridad de la red Inalámbrica de la Unidad de Gestión de la Información de las 3 sucursales de la sede de Quito de la institución.

Objetivo

Determinar amenazas, riesgos y vulnerabilidades en la red inalámbrica de la

institución utilizando metodologías formales de hacking ético con software libre.

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Ejecutivo
Fecha:	2015/05/02		

Tiempo o periodo realizado

Durante casi dos meses con la colaboración del administrador de la red se efectuaron las pruebas en el siguiente orden:

- Recolección de Información
- Escaneo – Auditoría
- Análisis y Búsqueda
- Explotación y Ataque

Resumen de vulnerabilidades

El activo crítico estudiado dentro del caso de estudio es JD Edwards Enterpriseone y los servicios que ofrece a través de la red inalámbrica. Se encontraron 40 vulnerabilidades con riesgos clasificados en críticos, altos, medios, bajos y mínimos, ver Figura , Tabla el porcentaje y número que corresponden.

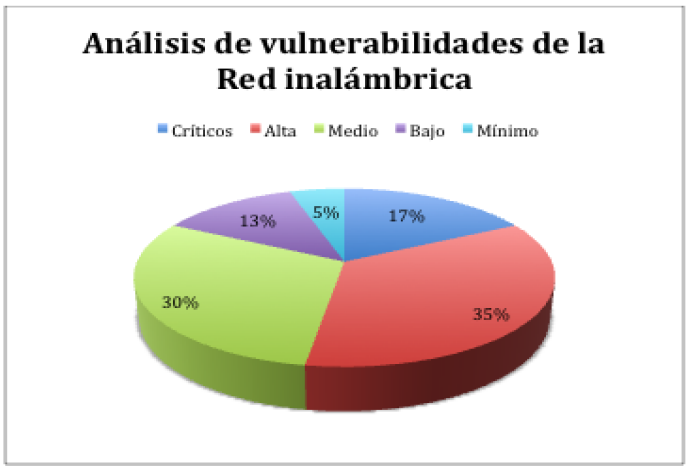


Figura 1. Resultados del análisis de riesgos

Fuente: La auditora

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Ejecutivo
Fecha:	2015/05/02		

Análisis de Activo	Número de vulnerabilidades encontrados				
	Críticos	Alta	Medio	Bajo	Mínimo
JD Edwards Enterpriseone y los servicios que ofrece a través de la red inalámbrica.	7	15	12	4	2
	17%	35%	30%	13%	5%

Tabla 1. Resultados del análisis de vulnerabilidades
Fuente: La auditora

Con la Alta dirección y el Administrador de la red se concluyó dar un tratamiento de riesgo aquellas vulnerabilidades que en su estimación esté categorizado el riesgo en: medio, alto y crítico.

Luego de identificadas las vulnerabilidades y determinar si son riesgos que pueden ser mitigados, se hizo un análisis de impacto y probabilidad de ocurrencia. Entonces se decidió que van a ser mitigados alrededor de 34 riesgos.

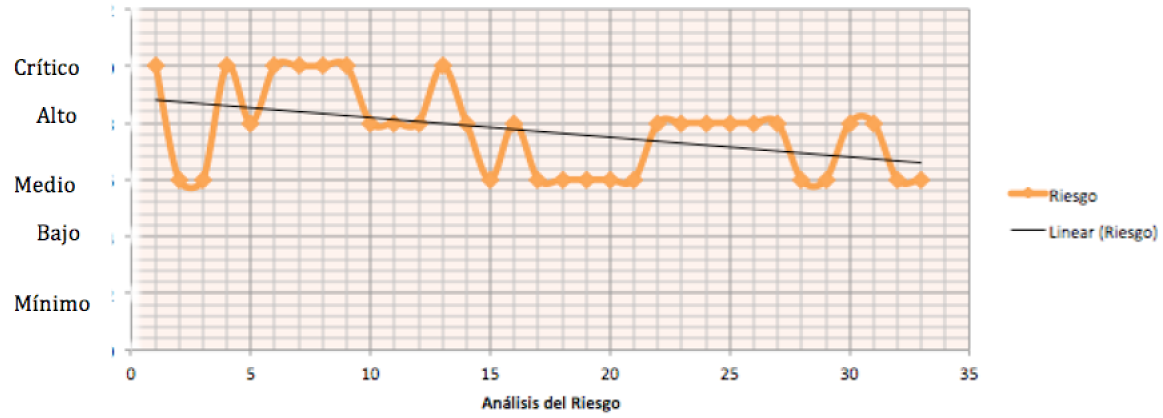


Figura 2. Estimación del riesgo

Fuente: La auditora

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Ejecutivo
Fecha:	2015/05/02		

Como se puede observar los riesgos oscilan entre alto y medio eso quiere decir que genera un impacto negativo en el negocio actualmente.

Este listado de riesgos forma parte del Plan de Mitigación y el informe técnico de los resultados fue presentado al Administrador de la red. Los controles recomendados que mitigan estos riesgos en la red inalámbrica serán descritos en el Plan de Mitigación, ver Anexo J.

Resumen del Análisis de la Factibilidad

Como involucrado directo de la ejecución de este plan para las sedes de Quito de la institución es el administrador de la red, quien se muestra abierto con actitud positiva al cambio, esta de acuerdo en capacitarse sobre el tema de seguridad informática. Dentro de las capacitaciones necesarias son:

- Capacitación sobre las nuevas tendencias de infraestructura inalámbrica.
- Capacitación sobre metodologías de hacking ético.
    - Capacitación sobre seguridad informática aplicado redes inalámbricas "*ISO/IEC 27033-7 , Inalámbrica,* para definir los riesgos específicos, técnicas de diseño y problemas de control de seguridad orientadas solo a las redes inalámbricas y de radio."
    - Capacitación sobre herramientas de evaluación y monitoreo.
- Capacitación sobre las normas *ISO/IEC 27002:2013 guías de buenas prácticas, Sistema de Gestión de Seguridad de la Información.*

- Capacitación a los usuarios funcionales de la institución.

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Ejecutivo
Fecha:	2015/05/02		

Duración en la implementación del plan propuesto

Tareas	# Riesgos	Tiempo
Implementar los controles con valoración de Riesgo 10.00 equivalente a una estimación Crítica (ver acápite 2.2.5.2)	7	6 semanas hombre
Implementar los controles con valoración de Riesgo 9.00-7.00 equivalente a una estimación Alto (ver acápite 2.2.5.2)	15	11 semanas hombre
Implementar los controles con valoración de Riesgo 6.00-5.00 equivalente a una estimación Alto (ver acápite 2.2.5.2)	12	11 semanas hombre
Rediseñar el esquema de la red.	N/A	6 semana hombre
	TOTAL	34 semanas hombre

Tabla 2. Análisis de factibilidad Técnica[97]

Ejecutar este plan de mitigación al administrador de la red le tomará 34 semanas hombre, lo que en sueldo se refiere alrededor de *7650*$ (cuando actualmente percibe un sueldo de 850$).

[97] Elaborado por: La autora en base al análisis del plan de mitigación realizado.

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Ejecutivo
Fecha:	2015/05/02		

El presupuesto destinado se muestra en la siguiente tabla:

RECURSO	COSTO (c/u)
Capacitación de la Norma ISO/IEC 27002:2013	1890$
Capacitación de la Norma 27033-7 inalámbrica	1890$
Capacitación sobre herramientas de evaluación y monitoreo.	519$
Capacitación a los usuario funcionales (durante 1 semana hombre)	500$
Costo de implementación de controles	*7650$*
TOTAL	12450$

Tabla 3. Inversión en el plan de mitigación
Fuente: La auditora

El presupuesto económico esperado es *12450$* en el plan propuesto para aumentar el nivel de seguridad de la red inalámbrica (dentro de este rubro no está considerado la Consultoría externa y ni el costo del equipo del servidor).
La consultoría externa tiene un valor de *13000$* aproximadamente.

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Ejecutivo
Fecha:	2015/05/02		

Observaciones:

- La identificación de amenazas, vulnerabilidades y riesgos se realizó por medio de entrevistas, pruebas controladas que fueron recomendadas por metodologías formales: ISSAF, OSSTMM, OSSTMM y OWISAM.
- La mayoría de vulnerabilidades encontradas no se refiere en si al mal funcionamiento de equipos tecnológicos sino a la incorrecta configuración de los dispositivos inalámbricos, facilitando una posible entrada de un atacante a la red inalámbrica.
- Por medio de herramientas de auditoria de red inalámbrica, se pudo constatar información relevante a la institución que viaja con métodos de encriptación inseguros.
- Existieron 65531 puertos cerrados lo que es beneficioso y denota que tienen precaución en este sentido.
- El personal técnico y administrativo desconoce sobre el correcto uso/manejo de la red inalámbrica, lo que implica una urgente capacitación sobre la importancia de la seguridad de la información.
- El análisis de factibilidad presentado fue el resultado de análisis de factibilidad técnica y operativa realizado en conjunto con la tutora, el administrador de red y la auditora.
- Las observaciones técnicas a mayor detalle se encuentran en el Informe Técnico y el Plan de Mitigación entregado al Administrador de la red inalámbrica.

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Ejecutivo
Fecha:	2015/05/02		

- El personal interno de la empresa se mostraron interesados (as) y abiertos en la actualización del conocimiento.
- Las herramientas utilizadas fueron limitadas ya que se utilizó software libre, en el caso de comprar la herramienta tendrían resultados asertivos.

RECOMENDACIONES

- Se recomienda que el administrador de la red conozca las configuraciones y servicios que deben ser configurados el dispositivo inalámbrico.
- Para la implementación de esta propuesta considerar si es necesario contratar a otro nuevo integrante, debido a no saturar la carga laboral al actual administrador de la red.
- Se recomienda que cualquier crecimiento físico en la infraestructura de la red de la institución sea regulado por el administrador de la red, para que se cumplan con normas de seguridad de la información.
- Se recomienda examinar periódicamente controles para aumentar el nivel de seguridad en la red inalámbrica.
- Este plan de mitigación propuesto puede ser ejecutado por el administrador de la red o sino consultar con una empresa que preste servicios de Auditoria.

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Técnico
Fecha:	2015/05/02		

Resumen ejecutivo

La institución acogió la propuesta de aplicar hacking ético a la red inalámbrica utilizando metodologías formales, por parte de la estudiante de la carrera de Ingeniería de Sistemas Informáticos y de Computación de la Escuela Politécnica Nacional.

Los días establecidos para la recolección de la información no fueron suficientes, ya que se requirió más tiempo de lo esperado debido a que no se tenía conocimiento sobre las herramientas y la dimensión de trabajo.

Alcance

Describir los problemas y propuestas de solución a la Seguridad de la red Inalámbrica de la Unidad de Gestión de la Información de las 3 sucursales de la sede de Quito de la institución.

Parámetros	Respuesta
Organización completa	No
Ubicación específica (s)	Quito
División (es) Específica (s)	5 sucursales
Naturaleza de la prueba	intrusiva / no intrusiva
Pruebas desde Exteriores, Interior a la institución y o Ambos	Ambos

Direccionamiento IP o rangos a evaluar	N/A

Tabla 4. Alcance definido
Fuente: La autora

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Técnico
Fecha:	2015/02/02		

Parámetros	Respuesta
Acceso remoto	No aplica
ESSID	La red inalámbrica perteneciente a la institución en c/u de las sedes
BSSID	Si
Ataques de Denegación de servicio	Si
Horario	Horario de Oficina
Tipo de análisis de las pruebas	Caja gris

Tabla 5. Alcance definido
Fuente: La autora

Objetivo

Determinar amenazas, riesgos y vulnerabilidades en la red inalámbrica de la institución utilizando metodologías formales de hacking ético con software libre.

Tiempo o periodo realizado

Las pruebas fueron realizadas de acuerdo al siguiente cronograma:

FASES	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6
Recolección de	X	X				X

Información						
Escaneo – Auditoría		X	X			X

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistema
Ingeniería en Informáticos y de Computación

Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Técnico
Fecha:	2015/05/02		

FASES	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6
Análisis y Búsqueda		X	X			X
Explotación y Ataque			X	X	X	X

Tabla 6. Periodo de las pruebas realizadas
Fuente: La autora

Resumen de vulnerabilidades

El activo crítico estudiado dentro del caso de estudio es JD Edwards Enterpriseone y los servicios que ofrece a través de la red inalámbrica. Se encontraron 40 vulnerabilidades con riesgos clasificados en críticos, altos, medios, bajos y mínimos. Por medio de la ejecución de entrevistas, a detalle pueden revisar Anexo A, Anexo B, Anexo C y pruebas controladas ver Anexo G.

El plan de mitigación propuesto se encuentra en el Anexo I.

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Técnico
Fecha:	2015/05/02		

CONCLUSIONES

- La mayoría de vulnerabilidades encontradas no se refiere al funcionamiento de equipos tecnológicos sino a la incorrecta configuración de los dispositivos inalámbricos, facilitando una posible entrada a un atacante.
- Se pudo obtener las contraseñas cuando los dispositivos tenían cifrado WEP. En cambio para el cifrado WPA-WPA2, no se obtuvo el mismo resultado debido a que se utilizaron diccionarios para crackear la red inalámbrica no fueron los adecuados, se demoró en analizar 4 horas y aún así no mostraba ningún resultado.
- Esta prueba de Detección de APs falsos no tuvo éxito en la institución debido a que para la prueba, la autora no cuenta con el chipset (tarjeta para auditoría de red inalámbrica) respectiva para la ejecución de la prueba.
- Los clientes sufrieron denegación de servicio, al enviar peticiones de un cliente indicando cierre de sesión al AP, este le desconectó lo que obligó al cliente otra vez acceder a la nueva red; se aprovechó capturando el handshake para obtener las claves de autenticación de la red.
- Con el análisis realizado denota que comparten varias redes inalámbricas vecinas en el mismo canal dentro de un mismo radio de cobertura de la

señal (no en todas las redes), lo puede causar interferencia y pérdida de datos en la transmisión. Se complementa con la anterior prueba.

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Técnico
Fecha:	2015/05/02		

- Se pudo constatar que en la mayoría de las sedes no existe una calendarización de actividades para la actualización de firmware del router y APs,.
- "Not shown: 65531 closed protocols", esto quiere decir que se encuentran cerrados 65531 puerto lo que es beneficioso y denota que tienen precaución en .
- La administración del dispositivo inalámbrico es a través de la web y no utilizan este puerto el puerto 23 para la administración del mismo.
- Se encuentra habilitados los beacons frames para acceder a la red inalámbrica, lo que posibilita la obtención de información del software y hardware del dispositivo.

RECOMENDACIONES

- Deshabilitar el soporte de WPS PIN y verificar que dicha funcionalidad no se encuentra activa.
- Cambiar las contraseñas por defecto para su acceso por otras más

robustas y que este cambio sea periódico.

- La forma de evitar que las credenciales de acceso a la organización se vean expuestas es verificar que estas no están siendo almacenadas en los equipos y dispositivos de los usuarios.

Realizado por:	Jéssica Morales Bonilla	Nombre del Documento	Informe Técnico
Fecha:	2015/05/02		

- Implementar el uso de mecanismos de autenticación robustos, como WPA2-CCMP, no utilizar credenciales genéricas o predecibles y habilitar la renovación automática de claves.
- Consulte en el sitio web oficial del fabricante del equipo y busque las actualizaciones del firmware del AP con los últimos parches de seguridad y mantener un log para de eventos.
- La potencia con la que los APs difunden la red debe estar controlada y limitada, evitando que el perímetro de cobertura exceda más de los límites de la organización o de los equipos.
- No debería estar accesible la administración del dispositivo inalámbrico a través de la web debido a que personal no autorizado podría llegar a modificar la configuración del dispositivo.
- Se debe monitorizar el tráfico periódicamente y esporádicamente que se produzca en la red, así como establecer un sistema de alarmas o calendarización de actividades que permitan notificar estas tareas al personal responsable.
- Se recomienda revisar el log o auditoria de eventos del AP para detectar qué usuarios tratan de ingresar a otras cuentas o intento de explotar una vulnerabilidad o pueden ser víctimas de denegación de servicios.