Universidad de las Ciencias Informáticas
Facultad 2

Título: PLANIFICACIÓN Y EJECUCIÓN DE PRUEBAS DE PENETRACIÓN (PENTEST) A REDES DE CENTROS DE DATOS.

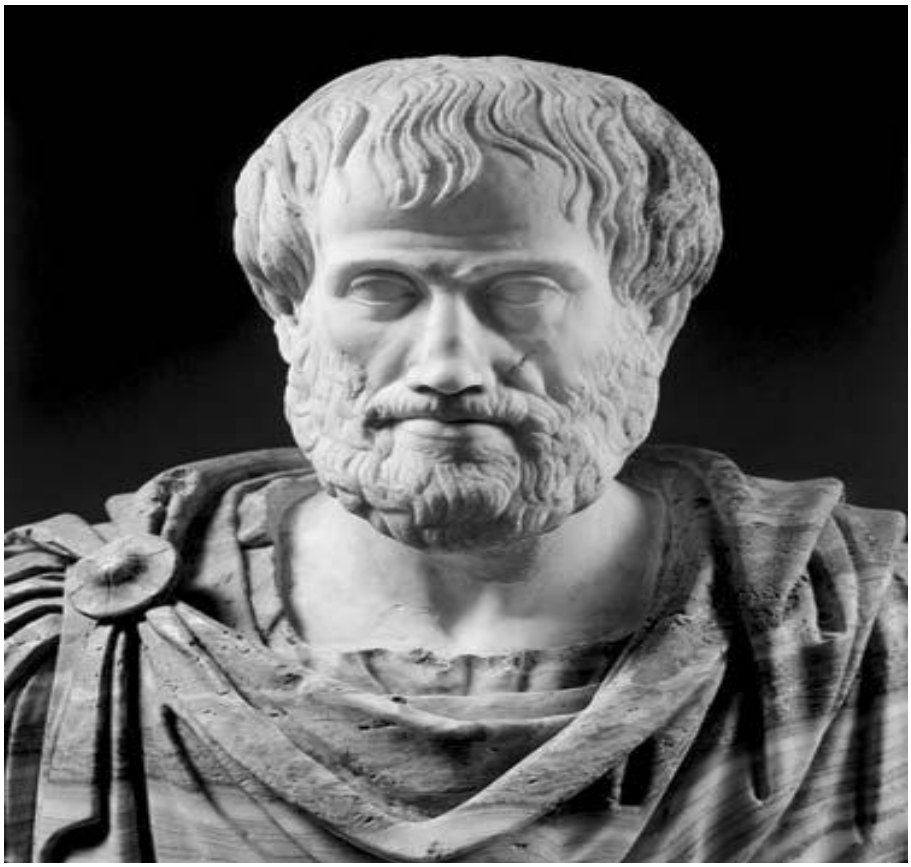
TRABAJO DE DIPLOMA PARA OPTAR POR EL TÍTULO DE INGENIERO EN CIENCIAS INFORMÁTICAS.

Autor: Yannier Valero Rosabal

Tutor: Ing. Miguel Castro-Palomino Ruiz

Ciudad de La Habana, 29 de junio de 2011
"Año 54 de la Revolución"

Frase



¨El ignorante afirma, el sabio duda y reflexiona.¨

Aristóteles

Declaración de Autoría

DECLARACIÓN DE AUTORÍA

Declaro que soy el único autor de este trabajo y autorizo al Centro de Telemática de la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

Para que así conste se firma la presente a los ____ días del mes de _____ del año _____.

Yannier Valero Rosabal

_____

Firma del Autor

Miguel Castro-Palomino Ruiz

_____

Firma del Tutor

DATOS DE CONTACTO

Nombre y Apellidos: Miguel Castro-Palomino Ruiz
Edad: 28
Ciudadanía: Cubano
Institución: Universidad de las Ciencias Informáticas.
Título: Ingeniero en Ciencias Informáticas.
Categoría: Trabajador Docente.
E-mail: miguelcp@uci.cu

- Especialista General del Departamento de Seguridad Informática del Centro Telemática.

Nombre y Apellidos: Yannier Valero Rosabal
Edad: 24
Ciudadanía: Cubana
Institución: Universidad de las Ciencias Informáticas.
E-mail: yvrosabal@estudiantes.uci.cu

Agradecimientos

AGRADECIMIENTOS

Agradecerle a toda mi familia por el apoyo que siempre me han dado, a todas mis amistades que han sido parte de mi familia durante estos 5 años, y a todos mis compañeros que estuvimos juntos en la misión en Venezuela. Agradecimiento especial a mi tía Rosarito, a mi tía Yamili, a mi tío Danilo y a mi abuelo Ricardo por su apoyo incondicional. Por último agradecer de forma muy especial a mi tutor y a todos los compañeros del Centro de Datos por toda la atención y la ayuda que me dieron para el desarrollo de este trabajo.

Dedicatoria

DEDICATORIA

Esta tesis va dedicada especialmente a mi madre que es la persona que más quiero en la vida y la que siempre me ha dado todo su apoyo y su amor. Dedicársela además a mi novia Yeni, a mis dos hermanas, a mis dos sobrinas, a mi hermanito, a mi papá y a mi cuñado, que son las personas que siempre me han ayudado y que siempre han estado ahí para lo que me hiciera falta, a todos ellos que son las personas que más quiero va dedicado este trabajo.

RESUMEN

El ámbito del presente trabajo, se centra en una propuesta para la planificación y ejecución de pruebas de penetración a las redes del Centro de Datos; para ello se realizó el análisis de varios estándares involucrados con las pruebas de penetración así como de un conjunto de herramientas de penetración especializadas en la recolección de información, la detección de vulnerabilidades en la red, en la explotación de vulnerabilidades y elaboración de informes sobre las vulnerabilidades encontradas. Inicialmente, se hace una revisión de las diferentes pruebas de intrusión existentes a nivel mundial, para determinar las actividades y herramientas que más se ajusten al entorno. Durante el trabajo, se lleva a cabo la implementación parcial de una prueba en la cual se demuestra, a través de pruebas de seguridad, cómo se logran reconocer irregularidades en los entornos que se aplican. Las herramientas utilizadas, en gran parte son multiplataforma y de distribución libre. La información recopilada durante las pruebas, muestra una visión del estado en que se encuentra el entorno informático que se ha analizado. A partir de esta información se puede reformular completa o parcialmente las políticas de seguridad del centro que lo solicite, permitiendo tener mayor seguridad frente a incidentes o mejor respuesta a estos si llegan a ocurrir.

Palabras Claves

pruebas de penetración, vulnerabilidades, Centros de Datos, herramientas de seguridad.

Contenido

Índice

INTRODUCCIÓN

El avance de la informática, los sistemas, las telecomunicaciones y otras aplicaciones de tecnología, han permitido a la sociedad desarrollarse rápidamente en todos los ámbitos. La información crece a ritmo vertiginoso y gracias a las nuevas tecnologías existen herramientas para su transmisión y los nuevos soportes facilitan su registro, almacenamiento, procesamiento y recuperación. La información, es el activo más importante en las organizaciones. En consecuencia, la seguridad de la información con la que se trabaja es uno de los aspectos más importantes para toda organización. Continuamente aparecen nuevas amenazas que explotan vulnerabilidades en los activos, entre los que sobresalen por sus impactos: virus, sabotajes informáticos, robos de información, accesos no autorizados, entre otras, que atentan contra la confidencialidad, integridad, disponibilidad e irrefutabilidad de la información. En el mundo, proyectos de seguridad como OWASP (Proyecto de Seguridad de Aplicaciones Web Abiertas, Open Web Application Security Project), entre otros, promueven el uso de medidas de seguridad, existen además variedad de herramientas de seguridad tales como: herramientas de monitoreo del tráfico de la red, escáner de vulnerabilidades, detectores de anomalías, antivirus, entre otros, todos con el objetivo de minimizar ataques a los activos informáticos.

De primera instancia, los administradores del área de sistemas establecen planes de prevención en los cuales indican a los usuarios de qué manera utilizar las herramientas y recomiendan medidas de seguridad generales. Eventualmente, la prevención no basta y las medidas no siempre ofrecen toda la seguridad necesaria; es por eso que una simulación de intrusiones bajo un ambiente controlado proporciona conocimiento adicional de los posibles fallos en la red. Dicha simulación permite identificar las vulnerabilidades dentro de una red, que cualquier atacante podría aprovechar para infiltrarse en una organización y de esta forma poder manipular información de vital importancia o hasta suplantar la identidad de alguna autoridad. Estas intrusiones de manera controladas son conocidas como pruebas de penetración y es una de las maneras de detectar vulnerabilidades en los Centros de Datos, pero a pesar que en dichos centros se toman una serie de medidas para el aseguramiento de la información con la que se trabaja y a pesar de que se utilizan una serie de herramientas y combinaciones de estas para el control de la información, existen algunos inconvenientes, entre ellos:

- Ya no es suficiente con utilizar soluciones basadas en una combinación de software, hardware y recursos humanos especializados; se hace necesario validar el estado real de la infraestructura.

- En la actualidad en el proyecto Centro de Datos no está definido un procedimiento para realizar pruebas de penetración y así validar proactivamente la seguridad de la infraestructura informática.
- A pesar de que las herramientas que se utilizan recomiendan medidas de seguridad, en la mayoría de los casos estas recomendaciones no son implementadas o no se realiza una correcta aplicación de ellas o solo se le da solución a las vulnerabilidades que implican un alto riesgo.
- Existe un desconocimiento general sobre la calidad de un PenTest y sobre cómo medir un PenTest (no si fue exitoso o no, sino, si realmente se realizaron las tareas que corresponden y no quedaron falsos negativos).
- Las recomendaciones que se obtienen a partir de las vulnerabilidades encontradas muchas veces son redactadas sin tener en cuenta el entorno operativo, esto provoca que incluso muchas recomendaciones sean técnicamente inviables.

A partir de la problemática existente en los Centro de Procesamiento de Datos, el **problema a resolve**r es el siguiente: ¿Cómo implementar una planificación y ejecución adecuada de pruebas de penetración en redes de Centros de Datos?

Por tanto el **objeto de estudio** está enfocado en los procedimientos para realizar pruebas de penetración y el **campo de acción** es el proceso de planificación y ejecución de pruebas de penetración en redes de Centros de Datos.

El **objetivo general** es elaborar una propuesta para la planificación y ejecución de pruebas de penetración (PenTest) en redes de Centros de Datos.

Las **tareas investigativas** para el cumplimiento de dicho objetivo son:

- ✓ Realizar un estudio sobre las pruebas de penetración para conocer su evolución y desarrollo así como el nivel de madurez de las mismas.
- ✓ Realizar un estudio acerca de los estándares existentes a nivel mundial para realizar pruebas de penetración y seleccionar las actividades que pudieran tributar a la propuesta de solución.
- ✓ Realizar un estudio en cuanto a características y resultados sobre las herramientas más utilizadas en el mundo para PenTest.

- ✓ Seleccionar las herramientas y distribuciones para PenTest utilizadas mundialmente e identificar en ellas características y necesidad de uso.
- ✓ Seleccionar la documentación más completa que se deriva de un PenTest para que se convierta en el documento entregable y final de proposición de medidas correctivas.
- ✓ Determinar los aspectos legales y éticos sobre los que se sustentan las pruebas de penetración.

Se utilizaron como **métodos de investigación científica:**

Teóricos

Histórico-Lógico: Para conocer cómo ha sido la evolución y el desarrollo de las pruebas de penetración a nivel mundial, así como las tendencias más novedosas que pudieran tener éxito en la solución del problema.

Analítico-Sintético: Para conocer a profundidad las características de las pruebas de penetración, cómo funcionan, cuáles son sus ventajas y desventajas. De igual manera para conocer las características de las herramientas, técnicas y procedimientos existentes para realizar este tipo de pruebas.

Empíricos

Observación: Se usó para la formulación y entendimiento del problema a investigar y fue de gran utilidad en el diseño de la investigación. Se usa para recolectar la información de cada uno de los conceptos que se utilizarán permitiendo identificar características, procesos y necesidades dentro del campo.

Experimentación:

Este método ha sido empleado durante la identificación y pruebas de las herramientas existentes, lo cual permite una mejor comprensión de los procesos que tienen lugar durante las pruebas de penetración en el proyecto Centro de Datos. Además juega un papel fundamental en la selección de aquellas soluciones idóneas al centro y constituye el factor decisivo en la definición del procedimiento a desarrollar.

El documento se encuentra estructurado en 3 capítulos:

En el **Capítulo 1** Fundamentación Teórica

Está enfocado a las soluciones existentes al problema en cuestión, así como las tendencias más revolucionarias, conceptos fundamentales, herramientas y estándares escogidos para brindar una solución a la problemática existente.

En el **Capítulo 2** Características de la Solución Propuesta

Está enfocado a la presentación de la solución propuesta, se definen etapas, roles, actividades, herramientas y artefactos dirigidos a la solución de la problemática.

En el **Capítulo 3** Validación de la Propuesta

Está dedicado a la aplicación del procedimiento definido como solución propuesta. Se mostrarán casos de pruebas realizados para validar la solución propuesta.

CAPÍTULO 1 FUNDAMENTACIÓN TEÓRICA

1.1 Introducción

En el presente capítulo se presenta el resultado de una investigación sobre el estado de arte de las pruebas de penetración, reflejándose así la evolución que han tenido las mismas. Además se realizará un análisis de los estándares, procedimientos y técnicas existentes a nivel mundial para realizar pruebas de intrusión así como también se presentará un estudio acerca de las herramientas de penetración más utilizadas por los profesionales de la seguridad informática en todo el mundo. Por último, se realizará una descripción y valoración de los distintos procedimientos y herramientas que se pueden utilizar durante la planificación y ejecución de pruebas de penetración.

1.2 Conceptos fundamentales

1.2.1 Vulnerabilidad

Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático (1).

1.2.2 Pruebas de Seguridad

Las Pruebas de Seguridad pretenden medir la confidencialidad, integridad y disponibilidad de los datos, cuantifican los riesgos a los cuales se ven expuestas las aplicaciones tanto en la infraestructura interna como externa. Simulan un ataque informático desde cualquier perspectiva (Internet, red interna, redes asociadas, acceso remoto, etc.) para establecer qué tan posible sería para un atacante, comprometer la seguridad de la información y validar la posible ocurrencia de un fraude (2).

1.2.3 Herramientas de Seguridad Informática

Dispositivo de hardware o software diseñado para proporcionar o comprobar la seguridad en un sistema informático (1). Son las herramientas informáticas basadas en estándares, protocolos, métodos, reglas, leyes entre otras y están concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

A nivel mundial existen muchas herramientas y sistemas encargados de la seguridad informática, pudiéndose citar herramientas y plataformas como IDS (Sistemas de Detección de Intrusos), IPS (Sistemas de Prevención de Intrusos), firewalls, así como los sistemas SIM (Gestión de Seguridad de la Información).

1.2.4 Seguridad Informática

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida) (3). La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

1.2.5 PenTest

Es un conjunto de métodos y técnicas para realizar una evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso no autorizado a cualquier entorno informático de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como externos (4).

1.3 Estado del arte

Saber qué está pasando en los sistemas que pueda ser relevante para la seguridad de la información de las organizaciones y en consecuencia, poder tomar decisiones de prevención y defensa, constituye hoy el objetivo principal de los responsables de seguridad de la información y obviamente de la dirección de sistemas de información de cualquier entidad pública o privada.

1.3.1 Evolución de los PenTest

Inicialmente los ataques o intrusiones eran medianamente benignos, pues en el peor de los escenarios solo se lograba poner lento el equipo; pronto pasaron a dañar sistemas completos, a borrar archivos o extraer información confidencial sobre las empresas. Después de varios intentos de proteger los sistemas, los administradores restringían más el acceso a las computadoras pero en consecuencia los crackers [1]comenzaron con ataques cada vez más destructivos y estructurados. Muchas entidades tanto civiles como militares, al notar un ambiente de inseguridad informática en sus instalaciones, optan por contratar a hackers [2](se hace referencia a los hackers blancos o white hats) expertos que ataquen el o los sistemas de la empresa con el fin de conocer cómo se puede infiltrar un verdadero atacante. Una vez que se saben

[1] Intruso; individuo que intenta penetrar en un ordenador o sistema informático ilegalmente con intenciones nocivas.

[2] Persona experta en alguna rama de la informática que se dedica a intervenir y/o realizar alteraciones técnicas con buenas (“hackers blancos” o “white hats”) o malas (“hackers negros” o “black hats”) intenciones sobre un producto o dispositivo.

las vulnerabilidades de un sistema, se pueden hacer mejoras en la configuración, en el acceso e incluso rediseño de éste para reparar dichas fallas. La frecuencia de estas actividades delictivas por parte de los intrusos y la defensa por parte de los administradores provoca el surgimiento de una nueva categoría: el hacking ético, que utiliza como procedimiento fundamental las pruebas de penetración.

En la década de los 70 se utilizaba para la evaluación de la seguridad al sistema MULTICS, Fuerza Central de Servicios de Datos de la Fuerza Aérea de los Estados Unidos. En la actualidad los PenTest evolucionan con el desarrollo de herramientas y estándares para su puesta en práctica, las cuales deben considerarse en cualquier estudio de seguridad.

1.3.2 Los PenTest

1.3.2.1 Justificación del PenTest

Una vez que la dirección de sistemas de una empresa ve la necesidad de que se le aplique una prueba de intrusión, la misma tiene que comunicarlo a la dirección general de la empresa o institución, justificando su solicitud a pruebas de penetración. Algunas de sus argumentaciones son:

- Conocer la situación real de un sistema y mejorarlo.
- Demostrar los riesgos existentes.
- Verificar que los mecanismos de seguridad se encuentren funcionando correctamente.
- Por regulaciones y/o obligación.
- Como un seguro para poder cubrirse ante auditorías.

1.3.2.2 Objetivos de un PenTest

El principal objetivo de un PenTest es determinar las debilidades de seguridad de la infraestructura y servicios de red de una organización. Dentro de sus objetivos secundarios se encuentran los de probar la capacidad de identificación y respuesta a incidentes, probar el conocimiento y conciencia de los usuarios desde el punto de vista de la seguridad y comprobar el cumplimiento de las políticas de seguridad (5).

De manera general:

- El PenTest ayuda a comprender la situación actual de la seguridad identificando los huecos de seguridad.
- Permite desarrollar planes de acción a partir de los informes de vulnerabilidades salientes de las herramientas, para remediar los problemas.

- Permite ubicar los recursos dedicados a la seguridad donde sean más necesarios.
- Ayuda a encontrar los enlaces débiles con otras entidades, empresas y otros dentro de las complejas estructuras de comunicaciones.
- Una vez que las políticas y la infraestructura de seguridad están aplicadas, un PenTest permite obtener una validación crítica que realimente el sistema.

1.3.2.3 Principios de un PenTest

- Deben realizarse pruebas de caja negra sin privilegios, luego pruebas con privilegios en el mismo entorno (6).
- Debe existir un amplio dominio por parte de los analistas sobre la(s) herramienta(s) a utilizar.
- Debe existir un respaldo jurídico para realizar las pruebas de penetración.
- Las vulnerabilidades de alto riesgo deben ser reportadas al cliente con una solución práctica tan pronto sean encontradas.
- Prohibidas las pruebas de DoS (Denegación de Servicios o por sus siglas en inglés Denial of Services) a no ser que hayan sido permitidas en la carta de autorización.
- Los informes deben incluir soluciones prácticas orientadas a resolver los problemas descubiertos.
- Los informes deben incluir todos los hallazgos desconocidos y deben ser identificados como tales.
- Los informes deben especificar claramente todas las barreras de seguridad encontradas, no sólo las fallidas (6).

1.3.2.4 Escenarios apropiados para realizar un PenTest

- Despliegue de una nueva infraestructura de red.
- Cambios o actualizaciones de infraestructuras de red existentes.
- Puesta en marcha de nuevas aplicaciones y servicios. Se comprueba su comportamiento y problemas.
- Modificación o actualización de una aplicación o servicio.

1.3.2.5 Políticas de ejecución

- Deben realizarse PenTest internos y externos.
- La frecuencia depende de las características de la organización.
- Los auditores pueden ser internos o no a la organización.
- La corrección puede realizarse por el mismo equipo auditor o por otro equipo.

1.3.2.6 Aspectos legales y éticos

Antes de que el equipo que realiza el PenTest toque el más insignificante activo, se hace necesario que la organización que solicita las pruebas firme dos cartas a la empresa que realiza el PenTest. Se trata de un convenio de confidencialidad y una carta de autorización. El convenio de confidencialidad, básicamente un NDA (convenio de confidencialidad o por sus siglas en inglés non-disclosure agreement), donde se describen las obligaciones de la empresa que va a realizar el PenTest en relación a toda la información que conocerá, accederá y tendrá en su poder. La carta de autorización (permiso para realizar el PenTest) debe estar firmada por el responsable de la organización antes de tocarse un solo sistema.

1.3.2.7 Ventajas de un PenTest

La ejecución de un PenTest en una empresa o institución permite:

- Identificar con rapidez las vulnerabilidades del sistema.
- Generar una visión de los riesgos y su impacto en la organización.
- Identificar los problemas y darles una solución inmediata.
- Implementación de nuevos y mejores modelos de seguridad resultantes de las pruebas de intrusión.

1.3.2.8 Etapas básicas de un PenTest

- Definición del alcance (7).

Se definen a partir de las necesidades del cliente. Se establece qué pruebas se van a realizar y en qué partes del sistema, qué técnicas se pueden emplear y cuánto tiempo va a durar el proceso.

- Definición del procedimiento a utilizar.

Basada en 3 fases (Identificación, Escaneo y Explotación).

- Aplicación del procedimiento.
- Evaluación de los resultados obtenidos.
- Corrección de los problemas detectados (7).

1.3.2.9 Fases del PenTest

Formalmente no existen metodologías para realizar un PenTest, pero en la práctica existen tantos procedimientos como empresas de seguridad informática. Los procedimientos abarcan desde las tres fases mencionadas anteriormente: identificación, escaneo y explotación, hasta las múltiples fases dependiendo del procedimiento establecido, de tal forma que las pruebas sean lo más exitosas y ordenas

posibles. Generalmente las fases de un PenTest responden a (reconocimiento superficial, enumeración, ataque, consolidación, borrado de rastros y reporte).

1.3.2.10 Tipos de PenTest

En forma general y de acuerdo al alcance, los PenTest pueden categorizarse en: Externos e Internos.

Los PenTest externos apuntan a analizar el nivel de seguridad real de una organización desde el exterior. Solo se dispone de la información pública del cliente, las direcciones IP[3] (Protocolo de Internet o por sus siglas en inglés Internet Protocol) y los nombres de dominios visibles. El principal objetivo es acceder en forma remota a la organización y posicionarse como administrador del sistema. Durante este tipo de pruebas se obtendrán los antecedentes necesarios para verificar la correcta configuración de los servicios externos de la red, servidores y vulnerabilidad a ataques conocidos.

Los PenTest internos se focalizan en analizar el nivel de seguridad de una organización a nivel interno. Incluyen análisis de la infraestructura de la red, estaciones de trabajo, servidores, aplicaciones y otros. Generalmente se hacen pruebas con privilegios normales simulando ser un empleado descontento o un visitante autorizado. Este tipo de pruebas trata de demostrar hasta dónde puede llegar un usuario que posea los privilegios de un usuario común dentro de la organización.

1.3.2.11 Actividades típicas de un PenTest

- Examen de la red.
- Exploración de puertos.
- Reconocimiento de sistemas.
- Sondeo de servicios.
- Búsqueda de exploits[4].
- Verificación manual y automática de las vulnerabilidades.
- Pruebas limitadas a aplicaciones.
- Pruebas de ACL (Lista de Control de Acceso o del inglés Access Control List) y cortafuegos.

[3] Una dirección IP es una etiqueta numérica que identifica de manera lógica y jerárquica a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP.

[4] Programa o parte de un programa informático malicioso que trata de forzar alguna deficiencia o vulnerabilidad de otro programa.

- Pruebas de IDS [5](Sistemas de Detección de Intrusos o por sus siglas en inglés Intrusion Detection System).

1.3.2.12 Técnicas utilizadas durante un PenTest

Ingeniería Social

Es un conjunto de trucos, engaños o artimañas que permiten confundir a una persona para que entregue información confidencial, ya sea los datos necesarios para acceder a ésta o la forma de comprometer seriamente un sistema de seguridad (8).

Escaneo de puertos TCP – UDP

Se basa en la búsqueda de puertos abiertos para enumeración de puertos y servicios remotos y medir las limitaciones del PenTest al host (9).

Esta técnica está compuesta por otras más complejas para poder escanear a través del firewall, como son la construcción de paquetes, escaneos con filtros de protocolo ICMP (Protocolo de Mensajes de Control de Internet o por sus siglas en inglés Internet Control Message Protocol), escaneos al protocolo TCP (Protocolo de Control de Transmisión o por sus siglas en inglés Transmission Control Protocol), forzar respuestas ante peticiones válidas e inválidas.

Enumeración y detección de servicios vulnerables

Todo PenTest debe llevar un registro ordenado de todos los puertos y servicios activos en el host remoto para así poder hacerse una imagen del posible escenario de ataque.

Ataques a protocolos de red

La presente técnica es uno de los primeros tipos de ataques que se realizan en un PenTest para sacar información del host remoto, unidades compartidas, nombre del servidor, dominio en el que trabaja, direcciones MAC (Control de Acceso al Medio o por sus siglas en inglés Media Acces Control), software instalado y hasta se puede conectar al host remoto mapeando todas sus unidades a la máquina atacante, logrando acceder a información confidencial en muchos casos. Este ataque se realiza si los puertos 137,138 y 139 están abiertos (9).

Ataque a las aplicaciones web

En esta parte del ataque de acuerdo a la información obtenida, se trata de vulnerar el host remoto mediante algún error o fallo en una de las aplicaciones web instaladas (9).

[5] Es un programa usado para detectar accesos no autorizados a una computadora o a una red.

Ejecución de código arbitrario

Esta técnica se puede realizar encontrando fallos tanto en las aplicaciones web como en los diferentes servicios que se ejecutan en el host remoto, y consiste en aprovechar alguno de estos fallos para hacer que dicho host realice acciones o ejecute comandos en forma arbitraria para lo cual no está programado. Pudiendo pedirle que realice un rastreo de paquetes (mediante el comando ping, del acrónimo de Packet Internet Groper) o pedirle que envíe una interfaz de línea de comandos (también conocida como shell) a un puerto específico en el equipo atacante, que liste sus directorios y archivos, que envíe cualquier archivo que se le pida, entre otras (9).

Desbordamiento de memoria (9)

Esta técnica sucede cuando los datos enviados a un determinado servicio exceden lo esperado, entonces se desborda la memoria del bufer y se pueden sobrescribir los datos de retorno. Las consecuencias de ataques de este tipo pueden ser:

- Ataques de denegación de servicio.
- Ejecución de código arbitrario remoto.
- Ganar privilegios sobre el sistema.
- Dar acceso a información crítica.
- Acciones destructivas.

Borrado de Huellas

Es el proceso de destrucción de datos, aplicaciones o código que pueda delatar o brindar información sobre la ubicación del atacante.

1.3.2.13 Necesidad de realizar PenTest de manera periódica

La seguridad de una organización es un aspecto cambiante. Una empresa puede alcanzar un nivel de seguridad óptimo en un momento determinado y ser totalmente vulnerable poco después tras cambios en la configuración de un servidor o tras la instalación de nuevos dispositivos de red. Continuamente aparecen nuevos fallos de seguridad en softwares existentes que antes se creían seguros.

Una política de realización de pruebas de penetración periódicas mitiga en gran medida el riesgo asociado a un entorno en constante cambio, tal como lo representan los sistemas informáticos de cualquier centro.

1.3.2.14 Procedimientos de un PenTest

Existen diferentes estándares para realizar pruebas de penetración, una de las más famosas por ser gratuita y abierta es la OSSTMM (Manual de Metodología Abierta de Testeo de Seguridad o por sus siglas en inglés Open Source Security Testing Methodology Manual) del Instituto para la Seguridad y las Metodologías Abiertas ISECOM. También existen otras herramientas como la guía de pruebas OWASP (Proyecto de Seguridad para Aplicaciones Web o por su siglas en inglés Open Web Application Security Project), que está enfocado a la auditoría de aplicaciones web o ISSAF (Framework de Testeo de Seguridad para Sistemas de Información o por sus siglas en inglés Information Systems Security Assessment Framework).

1.3.2.14.1 OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad

El Manual de la Metodología Abierta de Comprobación de la Seguridad (OSSTMM, Open Source Security Testing Methodology Manual) es uno de los estándares profesionales más completos y comúnmente utilizados en auditorías de seguridad para revisar la seguridad de los sistemas. Incluye un marco de trabajo que describe las fases que habría que realizar para la ejecución de pruebas de seguridad. Se ha logrado gracias a un consenso entre más de 150 expertos internacionales sobre el tema, que colaboran entre sí mediante Internet (10).

Se encuentra en constante evolución y actualmente se compone de las siguientes fases:

Sección A -Seguridad de la Información.

Sección B – Seguridad de los Procesos.

Sección C – Seguridad en las Tecnologías de Internet.

Sección D – Seguridad en las Comunicaciones.

Sección E – Seguridad Inalámbrica.

Sección F – Seguridad Física.

Mapa de seguridad

El mapa de seguridad es una imagen de la presencia de seguridad. Ésta corresponde al ambiente de un análisis de seguridad y está compuesta por seis secciones equivalentes a las fases anteriormente mencionadas. Las secciones se superponen entre si y contienen elementos de todas las otras secciones. Un análisis apropiado de cualquier sección debe incluir los elementos de todas las otras secciones, directa o indirectamente (10).

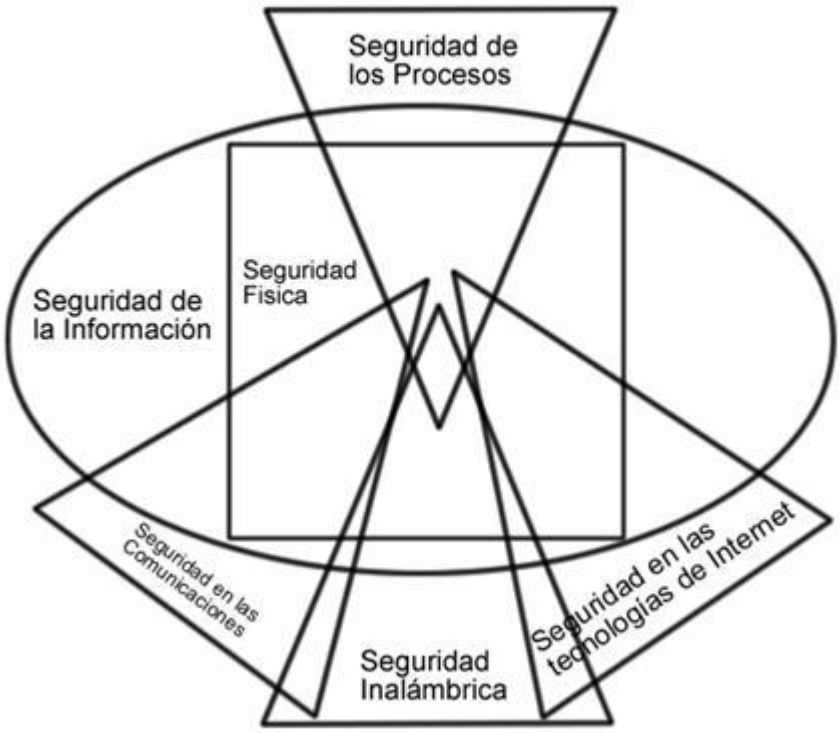


Figura 1.1 Mapa de Seguridad

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, deben definirse como no aplicable.

OSSTMM establece un conjunto de reglas y lineamientos para saber cuándo, qué y cuáles eventos son testeados. Además cubre únicamente el testeo de seguridad externo, es decir, testear la seguridad desde un entorno no privilegiado hacia un entorno privilegiado para evadir los componentes de seguridad, procesos, alarmas y ganar acceso privilegiado.

ISECOM exige que una prueba de seguridad OSSTMM solamente sea considerada como tal si es (10):

- Cuantificable.
- Consistente y que se pueda repetir.
- Válido más allá del período de tiempo actual.
- Basado en el mérito del analista de pruebas, y no en marcas comerciales.
- Exhaustivo.
- Concordante con leyes individuales y locales y el derecho humano a la privacidad.

OSSTMM representa un estándar de referencia imprescindible para todo aquel que quiera llevar a cabo un testeo de seguridad en forma ordenada y con calidad profesional. A fin de organizar su contenido, se encuentra dividida en varias secciones. Del mismo modo, es posible identificar en ella una serie de módulos de testeo específicos, a través de los cuales se observan cada una de las dimensiones de seguridad integradas con las tareas a llevar a cabo en los diferentes puntos de revisión (Seguridad de la Información, Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica y Seguridad Física). OSSTMM no solo alcanza los ámbitos técnicos y de operación de seguridad tradicionales, sino que se encarga de normar aspectos tales como: la forma en la que los resultados del mismo deben ser presentados, las normas éticas y legales que deben ser tenidas en cuenta al momento de concretar las pruebas, los tiempos que deberían ser tenidos en cuenta para cada una de las tareas, e incorpora el concepto de Valores de Evaluación de Riesgo (RAVs) y con ellos la frecuencia con la cual la prueba debe ser ejecutada a fin de proveer más que una instantánea en el momento de su ejecución (11).

1.3.2.14.2 ISSAF, Framework de Testeo de Seguridad para Sistemas de Información

ISSAF constituye un framework detallado respecto a las prácticas y conceptos relacionados con todas y cada una de las tareas a realizar al conducir un testeo de seguridad. La información contenida dentro de ISSAF, se encuentra organizada alrededor de lo que se ha llamado Criterios de Evaluación, cada uno de los cuales ha sido escrito y/o revisado por expertos en cada una de las áreas de aplicación. Estos criterios de evaluación a su vez, se componen de los siguientes elementos (11):

- Una descripción del criterio de evaluación.
- Puntos y objetivos a cubrir.
- Los pre-requisitos para conducir la evaluación.

- El proceso mismo de evaluación.
- El informe de los resultados esperados.
- Las contramedidas y recomendaciones.
- Referencias y documentación externa.

Por su parte y a fin de establecer un orden preciso y predecible, dichos criterios de evaluación se encuentran contenidos dentro de diferentes dominios entre los que es posible encontrar, desde los aspectos más generales, como son los conceptos básicos de la administración de proyectos de testeo de seguridad, hasta técnicas tan puntuales como la ejecución de pruebas de inyección de código SQL (SQL Injection) o como las estrategias del cracking de contraseñas.
A diferencia de lo que sucede con estándares más generales, si el framework no se mantiene actualizado, muchas de sus partes pueden volverse obsoletas rápidamente (específicamente aquellas que involucran técnicas directas de testeo sobre determinado producto o tecnología). Sin embargo esto no debería ser visto como una desventaja, sino como un punto a tener en cuenta a la hora de su utilización.

1.3.2.14.3 OTP, Proyecto de Testeo OWASP

OTP (OWASP Testing Project) se centra exclusivamente en pruebas de penetración para aplicaciones web, proporcionando un exhaustivo catálogo de 66 controles de seguridad a revisar en toda aplicación web (11).
OWASP es un estándar muy práctico que desde el primer momento se centra en testeos AJAX, desbordamientos de bufer, inyecciones SQL, escalado de privilegios, etc. Además explica que se hace en cada ataque, ofrece indicaciones sobre herramientas y técnicas a emplear, artículos que conviene leer así como un capítulo donde aborda el cómo redactar los informes. Esto hace a OWASP válido tanto para principiantes como para usuarios avanzados y promete convertirse en uno de los proyectos más destacados en lo que al testeo de aplicaciones web se refiere.

El proyecto consta de 2 partes, en la primera se abarcan los siguientes puntos:

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

Y en la segunda parte, se planifican todas las técnicas necesarias para testear cada paso del ciclo de vida del desarrollo de software. Incorpora en su procedimiento de testeo aspectos claves relacionados con el ciclo de vida del desarrollo de software a fin de que el ámbito del testeo a realizar comience mucho antes de que la aplicación web se encuentre en producción (11). De este modo y teniendo en cuenta que un programa efectivo de testeo de aplicaciones web debe incluir como elementos a testear: personas, procesos y tecnologías, OTP delinea en su primera parte conceptos claves, a la vez que introduce un framework específicamente diseñado para evaluar la seguridad de aplicaciones web a lo largo de su vida.

1.3.2.14.4 Comparación entre los diferentes estándares

Requisitos	OSSTMM	OWASP	ISSAF
Testeo	Utiliza el término de valores de evaluación de riesgos (RAVs).	Lista de chequeos.	Criterios de evaluación.
Generación de informes	Bien documentada	Bien documentada	Bien documentada
Aspectos legales	Bien definido.	Poco definido	Poco definido
Entorno que cubre	Entorno externo	Aplicaciones web	Externos e internos
Nivel de actualización	Actualizado	Actualizado	Actualizado
Documentación	Documentado	Documentado	Documentado
Licencia	Libre	Libre	Libre

Figura 1.2 Comparación entre los estándares

1.3.3 Diferentes tipos de ataques

1.3.3.1 Ataques por exploit

Un exploit es el nombre con el que se identifica a un programa o parte de un programa informático malicioso que trata de forzar alguna deficiencia o vulnerabilidad de otro programa (12).

El objetivo del mismo es lograr la destrucción o inhabilitación del sistema atacado, aunque normalmente se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearse en beneficio del atacante para originar otros ataques a terceros. Algunos agujeros de seguridad permiten que al ser explotados se pueda acceder a mayores permisos dentro de un sistema o que

directamente se pueda ejecutar acciones que en realidad no se debería poder hacer a través del software explotado.

En lo que respecta a la ejecución de código de forma arbitraria, se tienen dos modalidades de exploit:
Exploit Local: Es ejecutado de forma local y uno de sus principales objetivos es escalar privilegios cuando un exploit remoto ha tenido éxito en el equipo objetivo.
Exploit Remoto: Es ejecutado desde un equipo atacante hacia el equipo víctima, muy comúnmente ejecutado vía internet. De forma remota el atacante se posiciona en el equipo objetivo y posiblemente desde este, pueda atacar a los equipos que tenga visibilidad desde el mismo (13).

En lo que respecta al lugar del impacto del ataque, se pueden tener dos modalidades:
Server Side: Es el tipo de explotación más utilizado y consiste en aprovecharse de una debilidad de una aplicación servicio, es accesible de forma directa y no requiere de la intervención de un tercero.
Cliente Side: Tiene como objetivo explotar la vulnerabilidad en el lado del cliente, aprovechándose de las debilidades de uno de los eslabones más débil en la cadena de la seguridad de la información como lo es el usuario final (13).

1.3.3.1.1 Tipos de exploit

Los exploits se pueden clasificar según las categorías de vulnerabilidades utilizadas en (12):

- De desbordamiento de bufer.
- De condición de carrera (race condition).
- De error de formato de cadena (format string bugs).
- De Cross Site Scripting (XSS).
- De Inyección SQL.
- De Inyección de Caracteres.
- De denegación del servicio (DoS).
- De inyección múltiple HTML (Multiple HTML Injection).
- De ventanas engañosas o mistificación de ventanas (Windows Spoofing).

1.3.3.2 Ataques de DoS y Buffer Overflows

Un ataque de Denegación de Servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Generalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima (14).

Este tipo de ataque se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, de ahí que se le llame denegación, pues hace que el servidor no de abasto con respecto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

El ataque por DoS viene definido porque un servicio no está disponible a una persona o proceso (aplicación) cuando es necesario (disponibilidad), entonces existen tres tipos básicos:

- Consumo de recursos escasos.
- Destrucción o alteración de la información sobre la configuración.
- Destrucción o alteración física de los componentes de la red.

Un desbordamiento de bufer (del inglés buffer overflow) es un error de software que se produce cuando se copia una cantidad más grande de datos sobre un área más pequeña sin interrumpir la operación, sobrescribiendo otras zonas de memoria. El desbordamiento del bufer es un problema de código defectuoso. La única solución es estar informado de los programas que sufren esta vulnerabilidad y tener el software actualizado o con el parche correspondiente (14).

1.3.3.3 Ataques de inyección de código

Este tipo de errores puede permitir a usuarios malintencionados acceder a datos a los que de otro modo no tendrían acceso y en el peor de los casos, modificar el comportamiento de las aplicaciones.

La inyección SQL consiste principalmente en la modificación del comportamiento de las consultas mediante la introducción de parámetros no deseados en los campos a los que tiene acceso el usuario. Esta vulnerabilidad afecta a cualquier aplicación que utilice bases de datos. Cuando se realiza una consulta sin haber tratado correctamente los datos que forman parte de ella, se puede lograr que la consulta produzca resultados no previstos. Dependiendo de diversos factores, el problema puede

autorizar un acceso no permitido, como obtener la base de datos o modificar los datos de la misma hasta ejecutar códigos no previstos en el servidor (14).

1.3.3.4 Cross Site Scripting

Son vulnerabilidades relacionadas con servidores Web suele ser errores de programación en los CGIs ubicados en el servidor. Un CGI (Common Gateway Interface) es un código capaz de comunicarse con aplicaciones del servidor, de forma que desde una página se invoque a dichas aplicaciones pasándoles argumentos y el resultado se muestre en el navegador del cliente (14).

El CGI puede ser engañoso para la entrada de un atacante en donde éste ejecute comandos imprevistos, pudiendo llegar a causar graves daños en el servidor. Además puede revelar información acerca del servidor, que permita al atacante conocer mejor la configuración del sistema y así buscar posibles agujeros.

1.3.4 Herramientas utilizadas durante un PenTest

Un PenTest no es tarea fácil y requiere de un conocimiento sólido y profundo de las tecnologías involucradas en los sistemas, aplicaciones y servicios, además de una óptica y amplia experiencia en el comportamiento de varios sistemas operativos.

Las herramientas disponibles para efectuar las penetraciones pasan por varios grados de complejidad y el manejo de algunas de ellas puede ser todo un reto a la inteligencia del atacante o pentester. Entre ellas se incluyen desde escáner de puertos, complejos algoritmos para descifrar claves, sistemas de intrusión por fuerza bruta, herramientas de captura de paquetes en las redes y penetración de firewalls, así como también herramientas de escaneo de vulnerabilidades de aplicaciones web y mucho más. Estas herramientas suelen estar agrupadas en lo que se conoce como juegos de herramientas o Toolkits. Se identificaron en primer lugar, aquellas herramientas que son utilizadas actualmente y que por su funcionalidad se han ganado un lugar en la lista de elección de los analistas de seguridad.

1.3.4.1 Herramientas de reconocimiento

Maltego

Es una aplicación forense de código abierto, la cual permite la minería y obtención de datos e información, así como la representación de dicha información en una forma significativa. Complementada con sus librerías gráficas, permite identificar la relación entre claves de información e identificar previamente las

relaciones desconocidas entre ellas. Es una herramienta que se debe tener en el campo de la inteligencia, seguridad y aplicaciones forenses (15).

Esta herramienta es utilizada para la obtención de información que permite visualizar las relaciones. Permite enumerar la información referente a la red y al dominio, como son nombres de dominio, bloques de red, direcciones IP entre otras. Maltego también permite enumerar la información de personas como dirección de correo electrónico asociada con un nombre de persona, sitios web asociados con un nombre de persona, números telefónicos asociados con un nombre de persona, grupos sociales que están asociados con un nombre de persona, empresas y organizaciones asociadas con un nombre de persona. Maltego permite también hacer una verificación simple de las direcciones de correo electrónico, búsqueda de blogs y referencias por frases, identificar vínculos entrantes para sitios web y extraer metadatos desde archivos y fuentes de dominios (15).

Foca

Es una herramienta para encontrar metadatos e información oculta en documentos de Microsoft Office, Open Office y documentos PDF/PS/EPS, extrae todos los datos de ellos, exprimiendo los ficheros al máximo y una vez extraídos cruza toda esta información para obtener datos relevantes de una empresa u organización.

Foca hace Google Hacking[6] para descubrir los archivos ofimáticos que tiene un dominio, los descarga masivamente, les extrae los metadatos, organiza los datos y muestra la siguiente información: nombres de usuarios del sistema, rutas de archivos, versión del software utilizado, correos electrónicos encontrados, fechas de creación, modificación e impresión de los documentos, sistema operativo desde donde crearon el documento, nombre de las impresoras utilizadas. Esta aplicación permite descubrir subdominios y mapear la red de la organización, muestra nombres e IPs descubiertos en metadatos, realiza búsqueda de nombres comunes en servidor DNS (Sistemas de Nombres de Dominio o por sus siglas en inglés Domain Name System) y búsqueda de IPs con resolución DNS.

Foca además realiza transferencia de zonas, detección automática de DNS Cache, vista de roles, filtro de criticidad en el log entre otras muchas cosas. Foca es especialmente útil en la tarea previa a un PenTest,

[6] Google Hacking consiste en explotar la gran capacidad de almacenamiento de información de Google, buscando información específica que ha sido añadida a las bases de datos del buscador. Google Hacking es buscar en Google información sensible, generalmente, con fines maliciosos.

donde se debe recolectar toda la información posible sobre el objetivo para que la tarea se realice de la mejor forma (16).

1.3.4.2 Herramientas de escaneo

Nmap

Nmap (Network Mapper) es una fuente libre y abierta de utilidad para la exploración de la red o la auditoría de seguridad. Nmap utiliza paquetes IP en nuevas formas para determinar qué equipos están disponibles en la red, qué servicios (nombre de la aplicación y versión) ofrecen, qué sistemas operativos (y versiones del sistema operativo) se están ejecutando, qué tipo de paquete de filtros o cortafuegos están en uso, y otras varias características (17).

La información más importante que brinda Nmap es la tabla de puertos interesantes. Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio y su estado. El estado puede ser abierto (open), filtrado (filtered), cerrado (closed), o no filtrado (unfiltered). Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. Filtrado indica que un cortafuego, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra abierto o cerrado. Los puertos cerrados indican que no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento.

Los puertos que Nmap clasifica como no filtrados son aquellos que responden a sus sondeos, pero para los que Nmap no puede determinar si se encuentran abiertos o cerrados. Nmap puede informar también acerca de las combinaciones de estado abierto/filtrado (open/filtered) y cerrado/filtrado (closed/filtered) cuando no puede determinar en cuál de los dos estados está un puerto. La tabla de puertos también puede incluir detalles de la versión de la aplicación cuando se ha solicitado detección de versiones. Nmap además ofrece información de los protocolos IP soportados. Además de la tabla de puertos interesantes, Nmap puede dar información adicional sobre los objetivos, incluyendo el nombre de DNS según la resolución inversa de la IP, un listado de sistemas operativos posibles, los tipos de dispositivo, y direcciones MAC.

Nmap es (18):

Flexible: Soporta docenas de técnicas avanzadas para el mapeo de las redes llenas de filtros IP, firewalls, routers y otros obstáculos. Esto incluye mecanismos de escaneo de puertos (tanto TCP y UDP), detección de sistema operativo, detección de versión, barridos de IP entre otros.

Potente: Nmap ha sido utilizado para escanear grandes redes de cientos de miles de máquinas.
Portable: Compatible con la mayoría de los sistemas operativos, incluyendo Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, OS Sun, Amiga, y más.
Además es fácil, libre y muy bien documentado (18).

OpenVas

Es una de las herramientas de evaluación de seguridad Open Source de mayor renombre. Es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plugin, tiene una interfaz basada en GTK (biblioteca la cual contiene los objetos y funciones para crear la interfaz de usuario), y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad (19).
Además de ser analizador de vulnerabilidades, OpenVas también se utiliza para auditar el software antivirus instalado en los servidores Windows. Actualmente es capaz de detectar soluciones antivirus de BitDefender, Kaspersky, McAfee, NOD32, Norton, Sophos, Panda, Symantec, Trend Micro y Windows Live OneCare. También es muy útil para analizar servidores supuestamente infectados y comprometidos por algún tipo de virus o troyano de los que tiene reportados.

OpenVas es una herramienta basada en un modelo cliente-servidor que cuenta con su propio protocolo de comunicación. De forma similar a otros escáneres de vulnerabilidades existentes, el trabajo correspondiente para explorar y probar ataques contra objetivos es realizado por el servidor, mientras que las tareas de control, generación de informes y presentación de los datos son gestionadas por el cliente (20).

Características principales (21):

- Utiliza arquitectura cliente/servidor. El servidor corre bajo Unix o Linux y los clientes en Windows, Java, Unix, por lo tanto es multiplataforma.
- Basa su arquitectura a través de plugin.
- Cuenta con su propio lenguaje llamado NASL (Nessus Attack Scripting language) para programar los plugin.
- Escaneo de puertos e identificación de servicios a través de Nmap.

- Una base de conocimiento muy extensa con las vulnerabilidades descritas en CVE (Common Vulnerabilities and Exposures), con la opción de configurar los parámetros de éstas.
- Genera informes en diferentes formatos como pdf, xml, html. Como parte del informe permite conocer la vulnerabilidad y da un link a la descripción de ésta, a su vez propone una solución.
- Comunicación segura entre cliente y servidor a través de PKI (Public Key Infrastructure).
- Para versiones anteriores a la tercera la licencia es GPL (General Public License), permite obtener el código fuente.
- Ideal para el escaneo de máquinas con Sistemas Operativos Unix (21).

Nikto

Un escáner web de mayor amplitud. Nikto es un escáner de servidores web que busca más de 2000 archivos/CGIs potencialmente peligrosos y problemas en más de 200 servidores. Utiliza la biblioteca LibWhisker pero generalmente es actualizado más frecuentemente que el propio Whisker (escáner de vulnerabilidades web) (19).

Basado en la funcionalidad de HTTP, este analizador busca malas configuraciones, softwares que no están al día con las actualizaciones, archivos y scripts que están inseguros, los cuales colocan en alto riesgo al servidor. La herramienta se compone de un paquete de pruebas básicas, pero también permite la escritura de pruebas adicionales para necesidades específicas.

Características Principales (21):

- Busca en diferentes aplicaciones autenticaciones genéricas.
- Compara las versiones del software que están en el servidor con las que tiene en el archivo de la base de datos, para detectar versiones obsoletas.
- Revisa la versión del servidor web y revisa en la base de datos server_msgs.db si encuentra alguna vulnerabilidad específica.
- Intenta hacer una enumeración de usuarios al servidor. Hace una petición HTTP GET para diferentes usuarios y mira el código de error que retorna el servidor web para los usuarios que existen y para los que no.
- Busca los archivos de las contraseñas en diferentes sitios.
- Este plugin trata de enumerar todos los usuarios y directorios del sistema.

- Hace un ataque de fuerza bruta que está limitado por rangos dados, en este caso la longitud del nombre de usuario.
- También trata de enumerar los usuarios del sistema con base a los códigos de error que devuelva el servidor (21).

1.3.4.3 Herramientas de explotación de vulnerabilidades

Metasploit

La herramienta es utilizada por profesionales de la seguridad de red para realizar pruebas de penetración, los administradores de sistemas la utilizan para verificar la instalación de parches. Está escrito en el lenguaje de programación Ruby e incluye componentes escritos en C y ensamblador. Además consta de herramientas, bibliotecas, módulos e interfaces de usuario. La función básica de la estructura es un lanzador de módulo, que permite al usuario configurar un módulo de explotación y lanzarlo a un sistema de destino. Si el exploit tiene éxito, la carga se ejecuta en el objetivo y el usuario dispone de una consola de comandos para interactuar con la carga útil.

Características principales (21):

Herramienta usada para la detección y explotación de vulnerabilidades. Es una utilidad para ayudar en las pruebas de penetración de múltiples sistemas operativos.

- Metasploit fue desarrollado en 2004.
- Es multiplataforma, open-source tanto en el desarrollo, en las pruebas y uso.
- Escrito en Perl.
- Existe la posibilidad de ejecutar scripts en Perl.
- Puede extenderse con módulos diseñados por terceros.
- Uso mediante línea de comandos o mediante una interfaz gráfica.
- Extensible mediante payloads, encoders, generadores y exploits.
- Dispone de una base de datos con cientos de exploits que pueden ser utilizados para explotar vulnerabilidades.
- Posibilidad de conexión al servidor de Metasploit para obtener más actualizaciones y exploits.
- Una de las mayores bases de datos de exploit en el mundo del software libre (21).

BackTrack

BackTrack es una distribución Linux en formato Live-CD enfocada a la seguridad. BackTrack es una de las herramientas de pruebas de penetración con más votos en la distribución de Linux. Sin necesidad de instalación alguna, la plataforma de análisis se inicia directamente desde el CD-ROM y es totalmente accesible en cuestión de minutos. Actualmente BackTrack integra más de 300 herramientas diferentes que están lógicamente estructuradas de acuerdo con el flujo de trabajo de los profesionales de la seguridad. Esta estructura permite que incluso los recién llegados puedan encontrar las herramientas relacionadas con una determinada tarea a cumplir. Las nuevas tecnologías y técnicas de prueba se fusionan en BackTrack tan pronto como sea posible para mantenerla al día. BackTrack tiene una gran variedad de herramientas como son escáner de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless. (21)

BackTrack ofrece al usuario una extensa colección de herramientas usables desde un Live CD o un Live USB por lo que no requiere una instalación para poder usarse. Ofrece una lista de herramientas que se agrupan en 11 familias.

- Recopilación de información.
- Mapeo de puertos.
- Identificación de vulnerabilidades.
- Análisis de aplicaciones web.
- Análisis de redes de radio (WiFi, Bluetooth, RFID).
- Penetración (exploits y kit de herramientas de ingeniería social).
- Escalada de privilegios.
- Mantenimiento de acceso.
- Forenses.
- Ingeniería inversa.
- Voz sobre IP.

Cabe destacar que siempre se le pueden añadir más herramientas de software libre para desarrolladores de programación, herramientas de oficina, etc.

Core Impact

Es una herramienta automatizada de PenTest. Posee una amplia y regularmente actualizada base de datos de exploits profesionales. A través de sus funcionalidades es posible explotar vulnerabilidades en un equipo remoto y aprovecharse de estas para establecer un túnel cifrado a través de esa máquina y así poder pivotear en otros equipos. Es una de las soluciones de software más completas para la evaluación y comprobación de las vulnerabilidades de seguridad y cuenta con el respaldo de más de 15 años de investigación sobre la seguridad y el desarrollo de calidad comercial.

Combina el reconocimiento con la explotación y elaboración de informes en un solo punto. Su objetivo principal es el de identificar posibles vulnerabilidades en un programa, explotar las vulnerabilidades sin causar interrupciones de sistema y documentar claramente cada paso del camino para que todo el procedimiento se pueda verificar por otra parte. Core Impact hace que sea fácil para un administrador de redes, ejecutar pruebas de penetración sin tener un conjunto completo de utilidades. Una característica relevante de esta herramienta es la posibilidad de instalar un agente en un equipo comprometido y luego lanzar más ataques desde ese equipo. Está demostrado ser útil en una prueba de penetración real (22).

1.3.4.4 Otras herramientas

Ethereal

Ethereal es un analizador de protocolos de red para Unix y Windows y es libre. Permite examinar datos de una red viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Ethereal tiene varias características poderosas, incluyendo un completo lenguaje para filtrar lo que se quiere ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. Incluye una versión basada en texto llamada tethereal (19).

Netcat

Una utilidad simple para Unix que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP. Está diseñada para ser una utilidad confiable que pueda ser usada directamente o fácilmente manejada por otros programas y scripts. Al mismo tiempo, es una herramienta para depurar y explorar, ya que puede crear casi cualquier tipo de conexión que se pueda necesitar (19).

TCPDump / WinDump

Es un sniffer para monitoreo de redes y adquisición de información. TCPDump es un analizador de paquetes de red basado en texto. Puede ser utilizado para mostrar los encabezados de los paquetes en una interfaz de red que concuerden con cierta expresión de búsqueda. Se puede utilizar esta herramienta para rastrear problemas en la red o para monitorear actividades de la misma. Hay una versión para Windows llamada WinDump. TCPDump es también la fuente de las bibliotecas de captura de paquetes Libpcap y WinPcap que son utilizadas por Nmap y muchas otras utilidades (19).

Hping2

Hping2 ensambla y envía paquetes de ICMP/UDP/TCP hechos a medida y muestra las respuestas. Fue inspirado por el comando ping, pero ofrece mucho más control sobre lo enviado. Esta herramienta es particularmente útil al tratar de utilizar funciones como las de traceroute/ping o analizar hosts detrás de un firewall que bloquea los intentos que utilizan las herramientas estándar (19).

1.4 Conclusiones

En el presente capítulo, luego de realizar una breve introducción al tema, se abordó de manera general el enfoque al que están dirigidos los servicios de pruebas de penetración. Se profundizó en las llamadas pruebas de intrusión y se abordaron los diferentes tipos que existen, su definición, la importancia y los beneficios que pueden aportar. Además se analizaron los principales procedimientos que existen en la actualidad para desarrollar estas tareas, capaces de garantizar una correcta ejecución y elevados niveles de calidad así como también se proporcionó una breve descripción de cada una de ellos. Finalmente se realizó una caracterización de las diferentes herramientas de penetración que existen en la actualidad y se abordó de manera general las funcionalidades para las cuales fueron creadas.

Capítulo 2 Características de la Solución Propuesta

CAPÍTULO 2 CARACTERÍSTICAS DE LA SOLUCIÓN PROPUESTA

2.1 Introducción

En el presente capítulo se realizará una descripción y valoración de las características de la solución que se propone, se destacará la utilidad, aportes, pertinencia, beneficios que se derivan de la realización de la investigación. De manera general se describirá la estrategia para la planificación y ejecución de pruebas de penetración a Redes de Centros de Datos.

2.2 Prueba de penetración

Como se ha explicado en el capítulo anterior una prueba de penetración consiste en realizar un intento de intrusión controlado a los sistemas de información, en este caso a las redes de Centros de Datos, con el objetivo de identificar las vulnerabilidades a las que están expuestas las redes y definir los planes para mitigar los riesgos.

2.3 Etapas Básicas de un PenTest

Figura 2.1 Etapas de un PenTest

2.3.1 Definición del Alcance

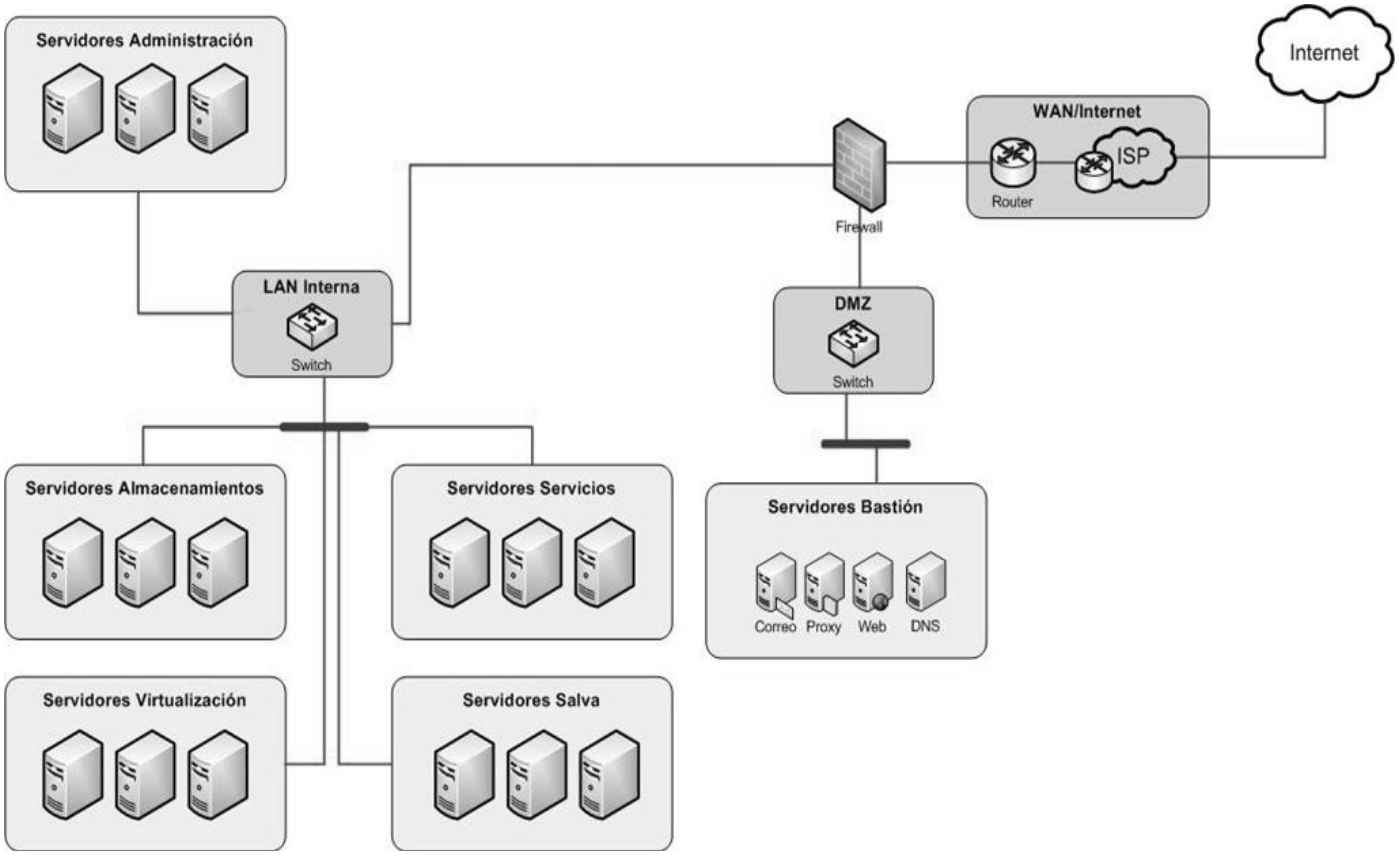


Figura 2.2 Diagrama Centro de Datos Genérico

En esta etapa se realizarán una serie de actividades que tributan a la planificación de las pruebas y a la configuración del ambiente de pruebas. En esta etapa durante la planificación de las pruebas se define el alcance de las mismas así como sus objetivos, además de tener en cuenta los recursos humanos y materiales necesarios para su realización. Como parte de la planificación se define la duración de las pruebas, factor muy relacionados con el alcance y que se concreta a partir de las necesidades del centro de datos, en esta etapa se establecen qué pruebas se van a realizar y en qué partes del sistema, qué técnicas se pueden emplear y cuánto tiempo va a durar el proceso.

Durante la configuración del ambiente de pruebas se garantiza el aseguramiento de todas las condiciones de software y hardware que sean necesarias para la ejecución de las pruebas, así como que se cuente

con un equipo de especialistas capacitados, seleccionados previamente. Este equipo debe contar con experiencia en el campo de la seguridad informática, un elevado nivel de conocimiento en redes, protocolos, sistemas operativos, aplicaciones y programación. Debe ser un equipo con perspectiva donde cada miembro puede aportar su visión del problema. El personal seleccionado debe mantener un alto sentido ético y profesional.

2.3.1.1 Equipo de Penetración: Roles

Jefe de Pruebas: Es el encargado de definir todas las políticas de seguridad mientras se ejecutan las pruebas, es el jefe del equipo y es el máximo responsable del resultado de las pruebas jugando un papel decisivo en la toma de decisiones ante cualquier situación que se presente durante el PenTest.

Especialista en Planificación de Pruebas: Junto al jefe de pruebas define el alcance, los objetivos y la duración de las pruebas. Define qué pruebas se van a realizar y en qué partes del sistema, qué técnicas se pueden emplear y cuánto tiempo va a durar el proceso.

Especialista en Diseño de Pruebas: Es el encargado de identificar, describir y diseñar los tipos de prueba. Selecciona el tipo de software a utilizar dependiendo de las técnicas que definió el planificador de pruebas.

Especialista en la Configuración del Ambiente de Pruebas: Garantiza el aseguramiento del Software y el Hardware para la realización de las pruebas, garantiza que se cuente con las herramientas necesarias ya definidas por el diseñador de pruebas.

Especialista en Pruebas: Es el encargado de realizar las pruebas de penetración según las políticas, procedimientos y reglas establecidas durante todo el ciclo de vida del PenTest. Obtiene toda la evidencia resultante de cada prueba que realiza y es el encargado junto a todo el equipo de pruebas generar el informe final de resultados.

2.3.2 Definición del Procedimiento a Utilizar

Luego del estudio de los distintos estándares y procedimientos utilizados a nivel mundial, se identificaron una serie de actividades que independientemente del estándar utilizado, son genéricas para desarrollar un satisfactorio proceso de pruebas de penetración.

Capítulo 2 Características de la Solución Propuesta

Partiendo de que existen dos tipos de diagnósticos, el interno y el externo, y según las necesidades y la problemática existente en el Centro de Datos de conocer el nivel real de amenaza o riesgo al que están expuestos, tanto desde el interior como desde el exterior, se propone la realización de las dos variantes.

Para la propuesta de procedimiento se tomaron una serie de elementos de los diferentes estándares estudiados, a continuación se presentan diferentes aspectos que se tuvieron en cuenta para la propuesta de solución.

OSSTMM

Cubre únicamente el análisis de seguridad externo, analiza la seguridad desde un entorno no privilegiado hacia un entorno privilegiado.

- Exploración de red.
- Escaneo de puertos.
- Identificación de servicios.
- Identificación de sistemas.
- Búsqueda y verificación de vulnerabilidades.
- Seguridad en las aplicaciones.

OWASP

Cubre el análisis completo para aplicaciones Web. Dentro de sus procedimientos cabe destacar:

- Explicación de las técnicas de testeo.
- Técnicas de testeo a personas, procesos y tecnologías.
- Testeo de Penetración sobre las aplicaciones.
- Testeo sobre la administración y configuración de las aplicaciones.

ISSAF

Constituye un framework detallado respecto de las prácticas y conceptos relacionados con todas y cada una de las tareas a realizar al conducir un testeo de seguridad. Utiliza el término de criterios de evaluación.

- Puntos y objetivos a cubrir.
- El informe de los resultados esperados.

- Las contramedidas y recomendaciones.

2.3.2.1 Prueba de Penetración Externa

Durante una prueba de penetración externa se dispone solamente de la información pública del cliente, las direcciones IP y los nombres de dominios visibles y el principal objetivo es acceder en forma remota a la organización y posicionarse como administrador del sistema. Se realiza desde afuera del firewall y consiste en penetrar la Zona Desmilitarizada [7](DMZ) para luego entrar a la red interna (4).

Se compone de un gran número de pruebas que se mencionan a continuación entre otras.

- Pruebas de usuario y la fuerza de sus password.
- Captura de tráfico.
- Detección de conexiones externas y sus rangos de direcciones.
- Detección de protocolos utilizados.
- Escaneo de puertos TCP, UDP e ICMP.
- Intentos de acceso vía accesos remotos, módem, Internet etc.
- Análisis de la seguridad de las conexiones con los proveedores, trabajadores remotos o entidades externas a la organización.
- Pruebas de vulnerabilidades existentes y conocidas en el momento de la realización del PenTest.
- Pruebas de ataques de negación de servicios.

En este diagnóstico durante el reconocimiento se deben obtener los antecedentes necesarios para verificar la correcta configuración de los servicios externos de la red, servidores y vulnerabilidad a ataques conocidos. Luego, durante el ataque controlado se ejecutan un conjunto de procesos y pruebas de penetración, siguiendo un estándar y procedimientos definidos. Luego de realizadas las pruebas se comienza con un estudio detallado de cada una de las vulnerabilidades detectadas en las etapas anteriores. Finalmente se conforma un informe de pruebas, indicando cada una de las debilidades encontradas y las recomendaciones para cerrar estas brechas.

[7] Zona entre el router interno y externo que aisla físicamente los servicios internos, separándolos de los servicios públicos.

2.3.2.2 Prueba de Penetración Interna

Durante una prueba de penetración interna el equipo se focaliza en analizar el nivel de seguridad de una organización a nivel interno. Este diagnóstico incluye análisis de la infraestructura de la red, estaciones de trabajo, servidores, aplicaciones y otros. Generalmente, se hacen pruebas con privilegios normales simulando ser un empleado descontento o un visitante autorizado. Se trata demostrar hasta dónde puede llegar un usuario que posea los privilegios de un usuario común dentro del centro. Esta prueba requiere que la organización provea una computadora típica, un nombre de usuario y una clave de acceso de un usuario común (4).

Dentro de las pruebas que se realizan durante un PenTest interno son:

- Análisis de protocolos internos y sus vulnerabilidades.
- Autenticación de usuarios.
- Verificación de permisos y recursos compartidos.
- Pruebas a servidores principales (www, DNS, FTP, SMTP, entre otros).
- Nivel de detección de intrusión en los sistemas.
- Análisis de seguridad en las estaciones de trabajo.
- Seguridad de la red.
- Verificación de las reglas de acceso.
- Ataques de Negación de Servicios.

Algunas de las actividades típicas de este ataque controlado son las pruebas del nivel de seguridad en los dispositivos de red, las pruebas de seguridad de los principales servidores, las prueba de seguridad de las estaciones de trabajo y las prueba a la seguridad de las aplicaciones.

Durante este tipo de prueba de penetración se realiza un levantamiento inicial de infraestructura donde se persigue obtener el diagrama de la red, la identificación de las máquinas críticas, las distintas direcciones IP internas y los servicios mínimos empleados para la normal operación del Centro de Datos. Luego se comienza con un análisis de máquinas críticas y mediante software especializado se revisa la configuración y vulnerabilidades de los servidores y computadoras identificadas como sensibles.

Posteriormente se inicia el análisis de la red, que tiene como objetivo analizar los distintos protocolos que existen en la red y compararlos con los identificados en la etapa de levantamiento. Finalmente y de manera igual a una prueba de penetración externa se realiza un informe final de pruebas donde se indican cada una de las debilidades encontradas y las recomendaciones para cerrar estas brechas.

2.3.3 Aplicación del Procedimiento

2.3.3.1 Aspectos legales antes de comenzar el PenTest

Antes de realizar el PenTest se debe de firmar dos cartas a quien realiza el trabajo, el convenio de confidencialidad (Ver Anexo # 1) que es la parte donde se describe las obligaciones de la parte que realiza la prueba en relación con toda la información que conocerá, accederá y tendrá en su poder durante la ejecución de las pruebas y la carta de autorización (Ver Anexo # 2), que es el permiso legal para realizar las pruebas de penetración. Como mínimo la carta de autorización debe tener, quién va a realizar el PenTest, cuándo será realizado, por qué será realizado, qué tipo de actividades son autorizadas y cuáles no, cuál es el alcance del PenTest y los contactos en el cliente ante cualquier emergencia.

Una vez definido el alcance y el objetivo de las pruebas y una vez firmadas el convenio de confidencialidad y la carta de autorización, está todo listo para comenzar las pruebas de penetración según todas las normas, parámetros, procedimientos y requisitos que se definieron entre el equipo que realiza el PenTest y el Centro de Datos. Ya definido el alcance y el modelo de aplicación, se han pasado dos fases importantes del PenTest, dándole paso a la tercera fase de aplicación del procedimiento.

2.3.3.2 Propuesta de Procedimiento

A partir del estudio realizado acerca de los procedimientos para realizar pruebas de penetración se propone como proceder una guía basada en fases con el objetivo de lograr una mayor organización en el trabajo y lograr un mayor entendimiento entre la empresa y el equipo PenTest. Las pruebas de penetración van a estar guiadas por las siguientes fases durante todo el ciclo de vida del mismo.

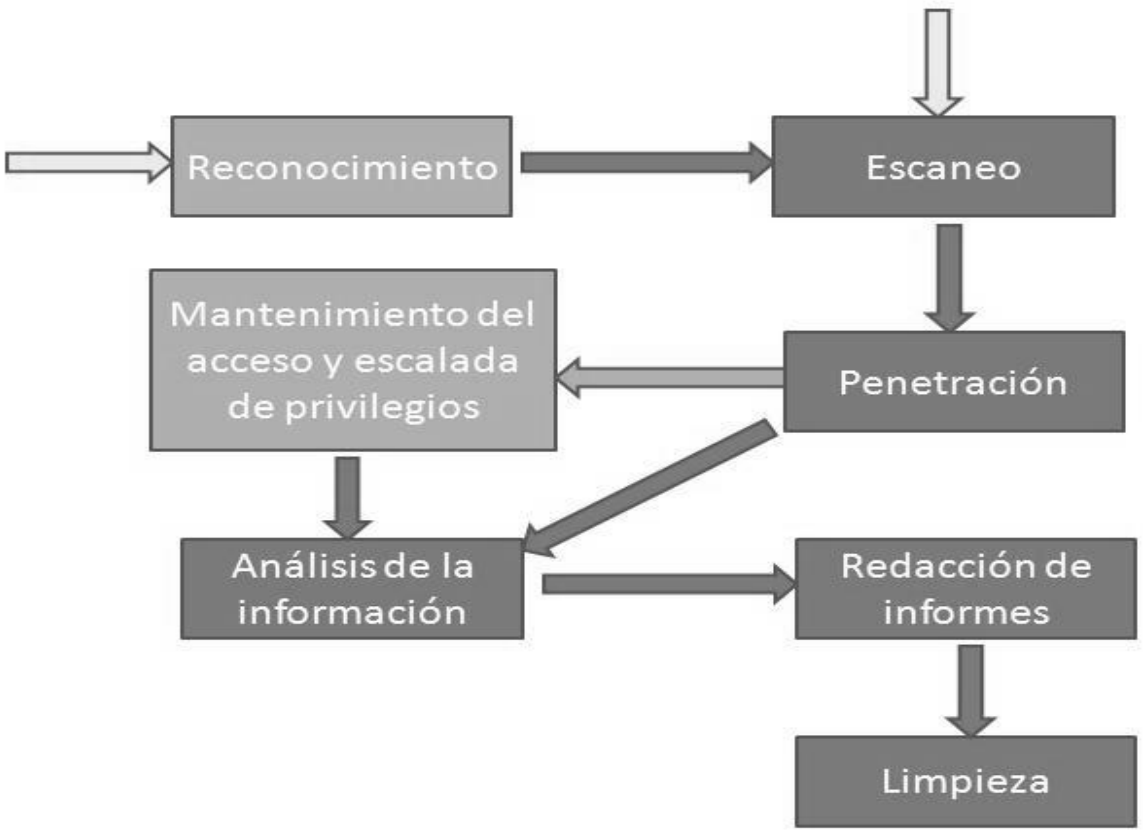


Figura 2.3 Fases de un PenTest

Simbología:

Indican las dos fases por las que puede empezar una prueba de penetración.

Indican flujo obligatorio.

Indican flujo opcional.

Fases de obligatorio cumplimiento.

Fases opcionales.

2.3.3.2.1 Reconocimiento

Esta fase se centra en entender los riesgos del negocio asociado al uso de los activos informáticos involucrados. Se realizan investigaciones tratando de recolectar información pública sobre la plataforma tecnológica del cliente. Incluye todas las pruebas para detectar las conexiones de la empresa a Internet, la

evaluación de servicios de DNS externos, la determinación de rangos de direcciones IP y sitios web, y la identificación de instalaciones físicas.

Se identifica la topología de la red objetivo, routers, firewalls, servidores, aplicaciones Web y otros activos informáticos que hayan sido incluidos en el alcance. En esta fase el equipo que realiza las pruebas utiliza todos los medios posibles para comprometer el centro, incluyendo la ingeniería social.

Actividades:

- Validar la conectividad con un equipo remoto.
- Conocer la ubicación de la red a la que está conectada un equipo remoto.
- Conocer el trayecto de los paquetes de red al viajar desde la ubicación del especialista hasta la del equipo remoto (víctima).
- Examinar la información del registro de dominio en busca de servidores.
- Consultar los servidores de nombres primario, secundario y del ISP (Proveedor de Servicios de Internet o por sus siglas en inglés Internet Service Provider) en busca de hosts y subdominios.
- Obtener la mayor cantidad de información posible acerca del objetivo.

Posibles resultados:

Se recolecta la mayor cantidad de evidencia sobre el centro en prueba. Esta información suele ser:

- Rangos de direcciones IP asignados.
- Direcciones IP de servicios tercerizados.
- Nombres de dominios.
- Nombres de servidores.
- Información ISP / ASP (Proveedor de Servicios de Aplicaciones).
- Dirección física de la empresa.
- Números telefónicos.
- Nombres de personas y cuentas de correo electrónico.
- Fuentes de información.
- Existencia de redes inalámbricas (WiFi).
- Incidentes de Seguridad Informática reportados.

Durante la fase de Reconocimiento

- No se realiza ningún tipo de escaneo o contacto con la maquina objetivo.
- Se permite construir un mapa del objetivo, sin interactuar con él.
- Existen menos herramientas informáticas que en las otras fases.
- Se recolecta información pública (Ingeniería Social y Google Hacking).

Herramientas: MALTEGO, FOCA.

Técnicas: Ingeniería Social.

2.3.3.2.2 Escaneo

Se aplican técnicas no intrusivas para identificar todos los potenciales blancos. Incluye el análisis de protocolos, relevamiento de plataforma y barreras de protección, escaneo de puertos TCP y UDP, detección remota de servicios y sistemas operativos, análisis de banners y búsqueda de aplicaciones web. En esta fase, se realiza el barrido de las direcciones IP en busca de puertos abiertos para luego pasar a la enumeración de puertos y servicios activos en el server remoto.

Actividades:

- Descubrir servidores e identificar host activos.
- Obtener el mapa de la red objetivo.
- Identificar el estado de los puertos en los host objetivos (abierto, cerrado o filtrado).
- Determinar qué servicios se están ejecutando e identificar el estado de los servicios de comunicación.
- Obtener información que de indicios acerca del sistema operativo del equipo víctima.
- Intervenir las comunicaciones entre equipos para escuchar y transmitir información, ocultando la verdadera ubicación e identidad del atacante.

Posibles resultados:

- Puertos abiertos, cerrados y filtrados.
- Direcciones IP de los sistemas activos.
- Direccionamiento de los sistemas de la red interna.

- Lista de los protocolos descubiertos de tunelizado y encapsulado.
- Servicios activos.
- Tipos de servicios.
- Tipo y nivel de parcheado de las aplicaciones de los servicios.
- Tipo de sistema operativo.
- Nivel de parcheado.
- Tipo de sistema.
- Lista de sistemas activos.
- Mapa de la red.

Enumeración y detección de vulnerabilidades

Todo PenTest debe llevar un registro ordenado de todas las vulnerabilidades encontradas así como de los puertos y servicios activos en el host remoto, para así poder hacerse una imagen del posible escenario de ataque.

Herramientas: Nmap, OpenVas, Nikto.

2.3.3.2.3 Penetración

Una vez enumeradas y detectadas las vulnerabilidades se procede a la fase de penetración donde se utilizan una serie de herramientas y procederes ya predefinidos por el equipo que realiza el PenTest.

Es una de las fases más complejas, ya que el evaluador debe de buscar aprovecharse de las vulnerabilidades identificadas, para lograr el ingreso (intrusión) en el sistema objetivo.

Actividades:

- Interrumpir parcial o totalmente los servicios de un equipo (servidor) en una red.
- Interrumpir la comunicación entre los equipos de una red.
- Suplantar identidades de equipos dentro de una red.
- Conseguir una terminal de comandos del equipo remoto.
- Conseguir acceso al sistema de archivos del equipo remoto.
- Conseguir una contraseña de usuario.

Explotación de vulnerabilidades.

Todas las vulnerabilidades son explotadas utilizando técnicas actuales. El objetivo de esta fase es demostrar el riesgo real asociado con cada vulnerabilidad.

Herramientas: Metasploit, BackTrack.

Técnicas: Ataques a protocolos de red, ataque a aplicaciones web, evasión de firewalls, ejecución de código arbitrario, desbordamiento de memoria, escalamiento de privilegios.

2.3.3.2.4 Mantenimiento del acceso y escalada de privilegios

Se aprovecha el modo inicial de acceso para ganar privilegios adicionales en el objetivo. Generalmente es en esta fase cuando un atacante instala un canal de comunicación oculto para transferir información desde su objetivo.

Actividades:

- Garantizar la comunicación entre el atacante y el equipo víctima.
- Conseguir el mayor nivel de privilegios de usuario.
- Crear canales de comunicación ocultos para transmitir la información deseada.

Técnicas: BackDoor[8], Rootkits[9]

2.3.3.2.5 Análisis de la información

Una vez terminada la fase de explotación se procede a recolectar y a analizar toda la información obtenida. El análisis de la información es de vital importancia pues puede haberse encontrado información vieja o nada aportante. Este análisis se va a realizar a toda la información que haya sido investigada y a toda aquella que se haya arrojado de las pruebas realizadas sin importar si las pruebas fueron satisfactorias o no.

[8] Es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema.

[9] Paquetes de software que sustituyen a los troyanos por binarios utilizados por el propio sistema operativo implicando el peor escalamiento de privilegios de la máquina atacada.

2.3.3.2.6 Redacción del informe

En esta fase del PenTest es donde se ve reflejado el análisis del evaluador de seguridad, aquí se plasman todos los hallazgos, las no conformidades, las opciones para mejorar, y las conclusiones y recomendaciones. En sentido general el informe no debe tener falsos positivos, debe mostrar resultados que establezcan prioridades, debe tener secciones técnicas y ejecutivas por separado, debe establecer qué recursos son necesarios y cuáles son las recomendaciones.

Reporte Técnico: Se entregará un informe con todos los datos y detalles técnicos acerca de las pruebas realizadas, las técnicas utilizadas, software empleado, etc.

Reporte Ejecutivo: Va dirigido a la dirección del centro de pruebas y se le entregará un informe con el alcance e impacto de un ataque informático a la infraestructura.

Artefactos: Reporte Técnico, Reporte Ejecutivo.

2.3.3.2.7 Limpieza

Este es el último paso de un PenTest. Después de haber logrado acceder al host remoto, haber capturado información confidencial o sensible y haber saltado los sistemas de seguridad, viene el borrado de huellas que es el proceso de destrucción de datos, aplicaciones o código que pueda delatar o brindar información sobre la ubicación del atacante (generalmente IP). Se pretende evitar que tras un análisis forense, se descubra información comprometedora del atacante. Dentro de las actividades que se realizan en esta fase se encuentran:

Actividades:

- Eliminar los artefactos usados durante el ataque que puedan dar información sobre la identidad, presencia o ubicación del atacante.
- Eliminar o esconder los archivos copiados en el destino.
- Eliminar los logs de sucesos de seguridad.
- Parar el antivirus, firewall, etc.
- Eliminar los logs de sucesos de las aplicaciones que fueron de una forma u otra atacadas.

2.3.4 Evaluación de los resultados obtenidos

Una vez terminado el proceso de pruebas y obtenido el informe final del PenTest, se da pase al proceso de evaluación de los resultados obtenidos, aquí se evidencia si los resultados son los que el centro en prueba esperaba, se evalúan los riesgos a los que está expuesto el centro así como la calidad del PenTest.

2.3.5 Corrección de los problemas detectados

En esta etapa es donde se pone en marcha la corrección de los problemas que fueron detectados. Luego de presentado el informe técnico de los resultados obtenidos por el PenTest viene la puesta en práctica de una correcta aplicación de las recomendaciones emanadas de los informes finales entregados.

2.4 Conclusiones

En este capítulo se han abordado las características de la solución propuesta, se ha explicado paso a paso qué hacer en cada etapa de una prueba de penetración, se ha explicado qué actividades realizar, propuesta de herramientas a utilizar así como los artefactos que se generan en cada fase del PenTest.

Capítulo 3 Validación de la Propuesta

CAPÍTULO 3 VALIDACIÓN DE LA PROPUESTA

3.1 Introducción

El presente capítulo estará enfocado en la validación de la propuesta desarrollada para realizar las pruebas de penetración a las redes de Centros de Datos. Se realizarán una serie de pruebas utilizando las herramientas y técnicas más convenientes para este caso sin afectar el objetivo del PenTest. Con el uso de estas herramientas se obtendrán como resultado los datos necesarios para identificar el estado de las estructuras analizadas.

3.2 Validación de la propuesta de PenTest en las Redes de Centro de Datos

A continuación se describirá un ejemplo de cómo realizar pruebas de penetración a un escenario montado en la red del Centro de Datos. Se explicará la manera de plantearse un ataque mediante los resultados obtenidos por herramientas automatizadas como Nmap, OpenVas, Nikto entre otras.

3.2.1 Alcance de las pruebas

El objetivo principal es detectar las vulnerabilidades en los servidores de Apache y de Postgree, explotar algunas vulnerabilidades encontradas, demostrar hasta dónde se puede llegar con los privilegios de un usuario común. Se hace necesario para la realización de las pruebas, una máquina de un usuario común y como herramienta a utilizar a BackTrack que es un Toolkits que contiene todas las herramientas predefinidas en el procedimiento. El tipo de prueba que se va a realizar es una aprueba de penetración interna.

3.2.2 Validación del procedimiento

Como se ha especificado anteriormente se va a utilizar la herramienta BackTrack para realizar las pruebas al Centro de Datos. Una vez en la máquina donde se van a realizar las pruebas de penetración, se ejecuta BackTrack. (Ver Anexo 3 y 4).

3.2.2.1 Reconocimiento

Como la prueba que se va a realizar es una prueba de penetración interna y ya se ha suministrado la información necesaria, entonces se puede dar por concluida esta fase sin necesidad de utilizar la herramienta propuesta. Con esto se pretende ahorrar la fase de reconocimiento y facilitar en gran parte la tarea de intrusión.

3.2.2.2 Escaneo

En esta etapa se identificarán y enumerarán todos los servicios y aplicaciones vulnerables. Mediante un escaneo intensivo al objetivo se identificarán puertos accesibles, host accesibles, detalles de los sistemas operativos entre otros.

Herramientas: Nmap y Nikto (Vienen incluidas dentro de BackTrack).

Con toda la información suministrada durante la fase de reconocimiento, se puede realizar un escaneo intensivo a la infraestructura a partir de las direcciones IP entregadas. Para este proceso se utilizará la herramienta Nmap con el objetivo de realizar un levantamiento de la red. Uno de los objetivos principales será el de reducir un conjunto de rango de direcciones IP en una lista de equipos activos.

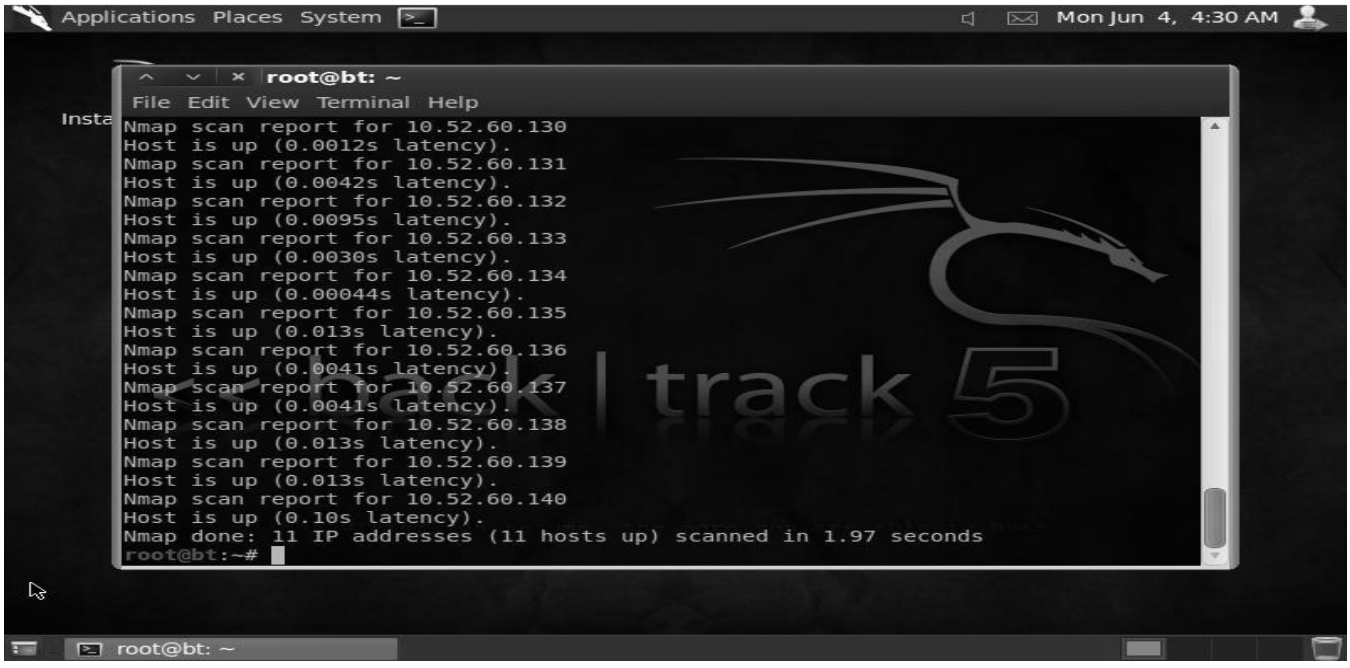
Primeramente se debería conocer qué es un escaneo de puertos y cómo establecer una conexión normal TCP, pues para realizar este tipo de conexión es necesario seguir una negociación de tres pasos. Esta negociación es iniciada con un paquete SYN en la máquina de origen, al que la máquina de destino corresponde con un paquete SYN/ACK, que es finalmente respondido por la máquina que inicia la conexión por un paquete ACK. Una vez que se han cumplido estos pasos, está hecha la conexión TCP. Un rastreador de puertos envía muchos paquetes SYN a la máquina que se está probando y detecta de qué forma regresan los paquetes para ver el estado de los puertos en el destino, interpretándolos de la siguiente forma:

Si al enviar un paquete SYN a un puerto específico, el destino devuelve un SYN/ACK, el puerto está abierto y escuchando conexiones. En otro caso, si regresa un paquete RST, el puerto está cerrado. Por último, si no regresa el paquete, o si se recibe un paquete ICMP Port Unreachable, el puerto está filtrado por algún tipo de cortafuegos (18).

Una vez ejecutado Nmap se verifican cuáles direcciones IP se encuentran activas dentro del rango de direcciones obtenidas anteriormente. Para esto se utiliza el comando siguiente:

Nmap –sP 10.32.60.130-140 (Ver Anexo 5) y el resultado es el que se muestra en el siguiente caso de prueba.

Capítulo 3 Validación de la Propuesta

Caso de Prueba 1
Nombre: Encontrar direcciones IP activas.
Descripción: Se verifica que direcciones IP se encuentran activas dentro del rango de direcciones 10.52.60.130 al 10.52.30.140
Condiciones de ejecución: Ninguna
Entrada/Pasos de ejecución: Se ejecuta la secuencia de comandos siguientes: Nmap –sP 10.32.60.130-140 Escaneo ping: A veces únicamente se necesita saber que servidores en una red se encuentran activos. Nmap puede hacer esto enviando peticiones de respuesta ICMP a cada dirección IP de la red que se especifica. Aquellos servidores que responden se encuentran activos.
Resultado esperado: Un listado de host activo.
Explicación del Resultado:    Como se puede evidenciar todos los host han respondido y por tanto se encuentran activos en la subred.
Evaluación de la prueba: Prueba satisfactoria

Las direcciones IP activas son las siguientes:

Direcciones IP o rangos de direcciones que serán testeados y detalles	
Direcciones IP	**Detalles**
Rango 10.52.60.130 al 10.52.60.140	**Todos los host están encendidos**

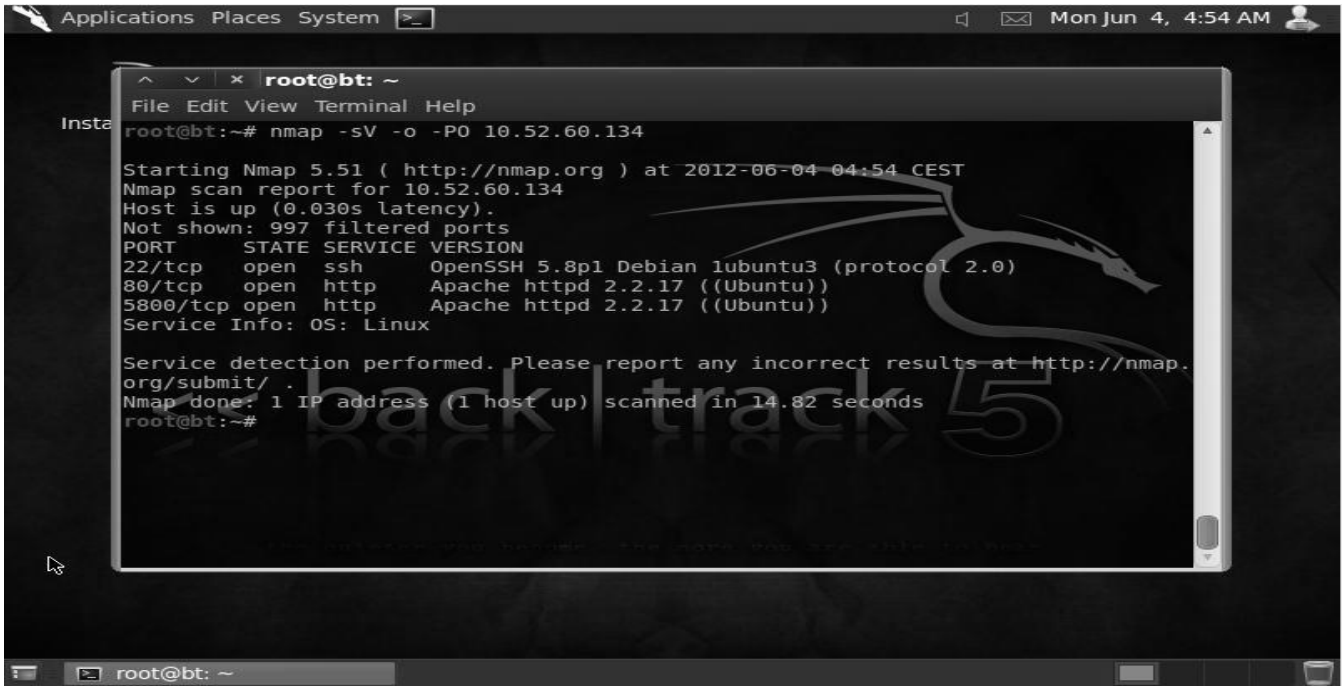
Tabla 3.1 Host activos

Una vez identificados los host activos, se comienza con el proceso de escaneo de los puertos con el objetivo de detectar los puertos abiertos, filtrados o cerrados y los servicios que corren por cada uno de ellos, por otra parte se intentará averiguar qué tipo y versión de aplicación se está corriendo en cada puertos. Se utilizará el rango completo de puertos desde 1 hasta 65535 y se revisarán los protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol). Para ello se ejecuta el comando:
nmap –sV -O –P0 –p 0-65534 para cada uno de los host activos. (Ver Anexo 6)

-sV: Modo de información ampliada, proporciona mayor cantidad de información que otro escaneo simple.
-O: Para determinar el sistema operativo que corre en un host.
-PO: No intenta hacer ping a un servidor antes de escanearlo. Esto permite el escaneo de redes que no permiten que pasen peticiones (o respuestas) de ecos ICMP a través de su firewall.
-p: Para especificar un puerto o rango de puertos a escanear.

Una vez vistos los resultados, se evidencia que los servidores de Apache y Postgree se encuentran en los host 10.52.60.134 y 10.52.60.136 respectivamente. En los casos de pruebas siguientes se muestran los resultados obtenidos de ambas direcciones IP.

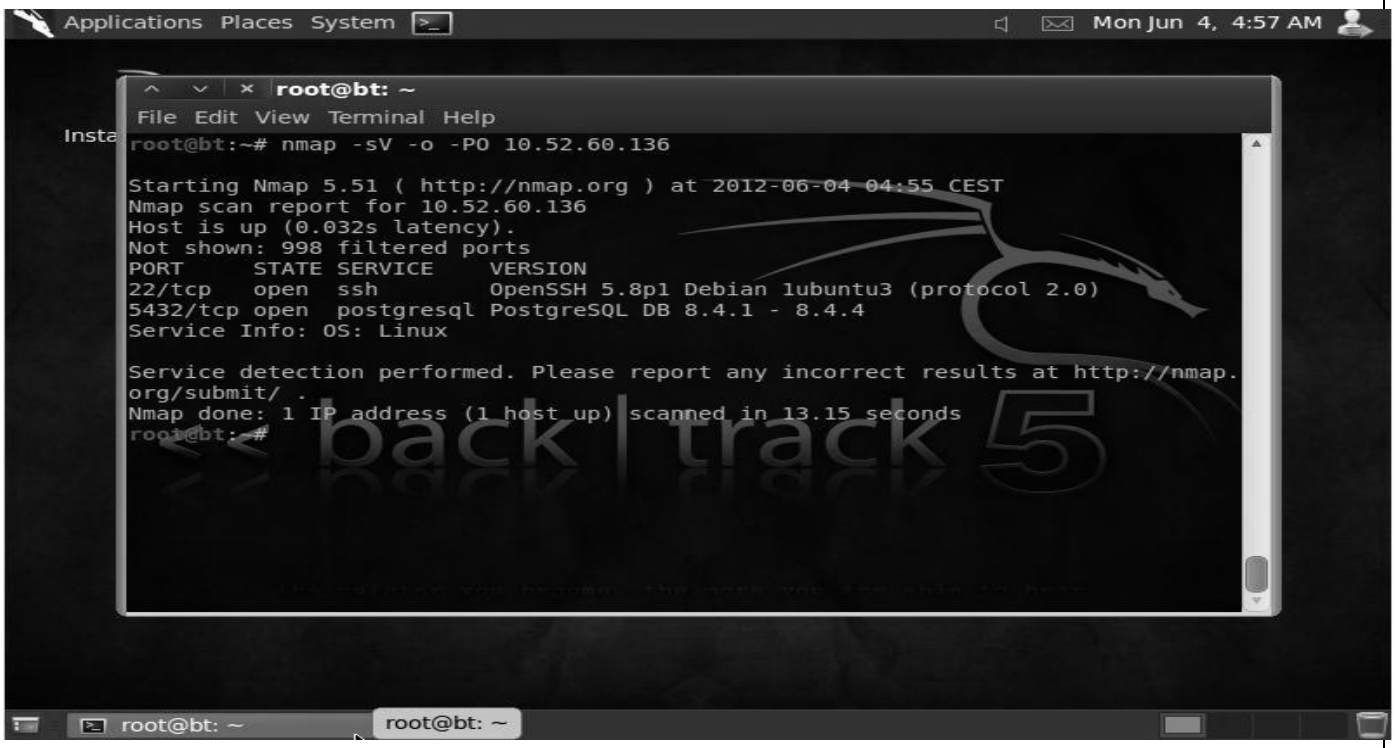
Caso de Prueba 2
Nombre: Escanear host 10.52.60.134
Descripción: Se escanean los puertos con el objetivo de detectar los puertos abiertos, filtrados o cerrados así como los servicios que corren por cada uno de ellos Se utiliza el rango completo de puertos desde 1 hasta 65535 y se revisa el protocolo TCP.
Condiciones de ejecución: Que el host objetivo se encuentre activo.
Entrada/Pasos de ejecución: Se ejecuta la secuencia de comandos siguiente: nmap –sV -O –P0 –p 0-65534 10.52.60.134
Resultado esperado: Estado de los puertos, protocolo, servicio que corre en cada puerto, versión de los servicios y sistema operativo del host objetivo.
Explicación del Resultado:



Se evidencia que el servidor de Apache se encuentra activo en esta dirección IP.

Evaluación de la prueba: Prueba satisfactoria

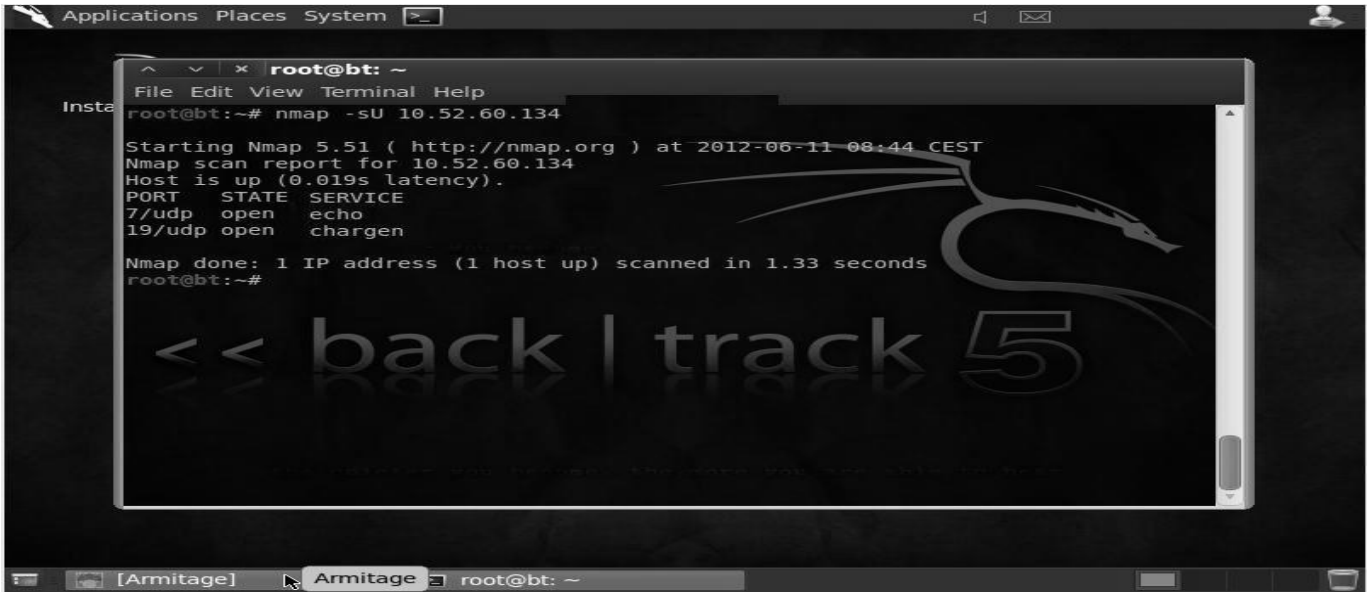
Capítulo 3 Validación de la Propuesta

Caso de Prueba 3
Nombre: Escanear host 10.52.60.136
Descripción: Se escanean los puertos con el objetivo de detectar los puertos abiertos, filtrados o cerrados así como los servicios que corren por cada uno de ellos Se utiliza el rango completo de puertos desde 1 hasta 65535 y se revisa el protocolo TCP.
Condiciones de ejecución: Que el host objetivo se encuentre activo.
Entrada/Pasos de ejecución: Se ejecuta la secuencia de comandos siguientes: nmap –sV -O –P0 –p 0-65534 10.52.60.136
Resultado esperado: Estado de los puertos, protocolo, servicio que corre en cada puerto, versión de los servicios y sistema operativo del host objetivo.
Explicación del Resultado:    Se puede evidenciar que el servidor de Postgree se encuentra activo en esta dirección IP.
Evaluación de la prueba: Prueba satisfactoria

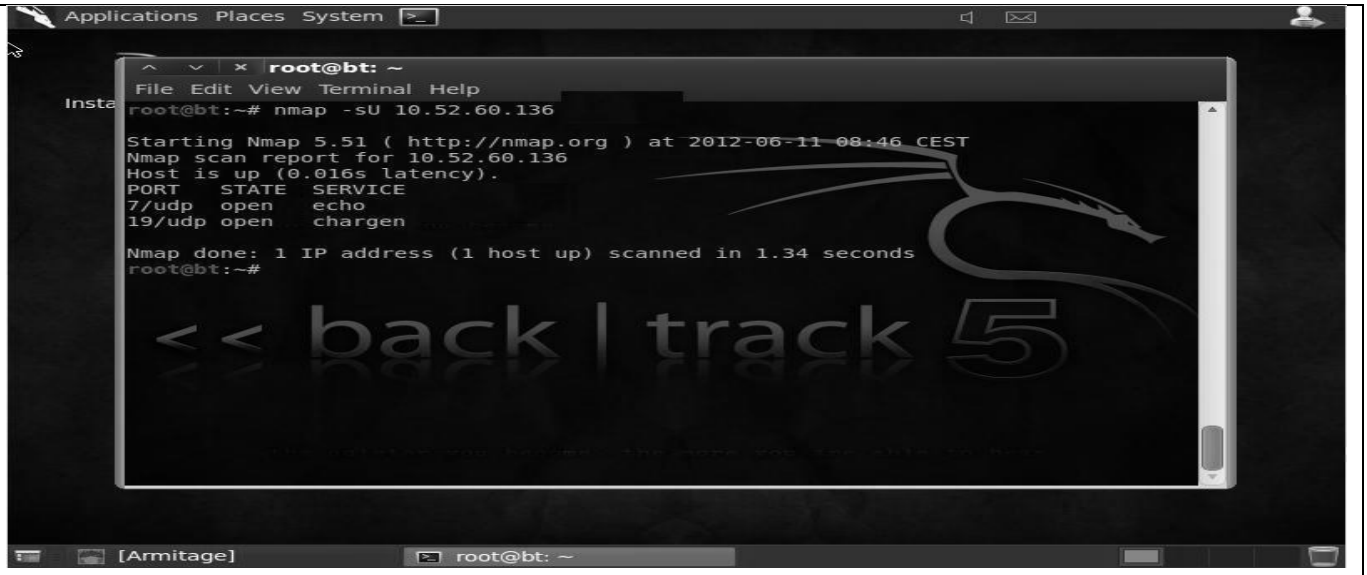
Capítulo 3 Validación de la Propuesta

Como se puede ver en los caso de pruebas anteriores, se tiene ya localizado dónde se encuentran funcionando los servidores de Apache y Postgree, el puerto por el que corren los servicios y la versión de los mismos. Una vez escaneados los puertos TCP se comienza con el escaneo en los puertos UDP como se muestra en el caso de prueba siguiente:

Caso de Prueba 4
Nombre: Escanear Protocolo UDP a Servidores Apache y Postgres
Descripción: Se escanean los puertos con el objetivo de detectar los puertos abiertos así como los servicios que corren por cada uno de ellos. Se revisan los puertos del protocolo UDP.
Condiciones de ejecución: Que el host objetivo se encuentre activo.
Entrada/Pasos de ejecución: Se ejecuta la secuencia de comandos siguientes: nmap –sU 10.52.60.134 nmap –sU 10.52.60.136
Resultado esperado: Estado de los puertos, servicio que corre en cada puerto.
Explicación del Resultado:



Capítulo 3 Validación de la Propuesta



Como se puede observar se muestran los puertos UDP abiertos así como el servicio que corre por los mismos.

Evaluación de la prueba: Prueba satisfactoria

Luego se enumeran los puertos y servicios activos en el host remoto.

Host	Puerto	Protocolo	Estado	Servicio	Versión
10.52.60.134	22	TCP	Abierto	ssh	OpenSSH 5.8p1
	80	TCP	Abierto	http	Apache httpd 2.2.17
	5800	TCP	Abierto	http	Apache httpd 2.2.17
	7	UDP	Abierto	echo	
	19	UDP	Abierto	chargen	
10.52.60.136	22	TCP	Abierto	ssh	OpenSSH 5.8p1
	5432	TCP	Abierto	postgresql	PostreSQL DB 8.4.1 - 8.4.4
	7	UDP	Abierto	echo	
	19	UDP	Abierto	chargen	

Tabla 3.2 Enumeración de puertos y servicios

Capítulo 3 Validación de la Propuesta

De los casos de prueba 2 y 3 se puede preciar también que el Sistema Operativo que se encuentra instalado en ambos objetivos es Linux. Conocer la versión de sistema operativo y del software instalado es de gran importancia para realizar las pruebas, esto se debe a que en la mayoría de los ataques, se emplean exploits que necesitan ser ajustados previamente con datos concretos, que dependen de la versión exacta del propio software o del sistema operativo.

A partir de ahora se comienza con la detección de vulnerabilidades que como su nombre lo indica, el objetivo es identificar si el sistema es débil o susceptible de ser afectado o atacado de alguna manera. Se utilizará la herramienta de escaneo Nikto. Con esta herramienta se pueden conocer descuidos de administración o vulnerabilidades previamente conocidas. Para ello se ejecuta Nikto desde BackTrack y se lanza el siguiente comando: ./Nikto.pl –h 10.52.60.134

Algunas de las pruebas más importantes realizadas por Nikto son (23):

0 - File Upload. Exploits

1 - Interesting File / Seen in logs

2 - Misconfiguration / Default File

3 - Information Disclosure

4 - Injection (XSS/Script/HTML)

5 - Remote File Retrieval - Inside Web Root

6 - Denial of Service

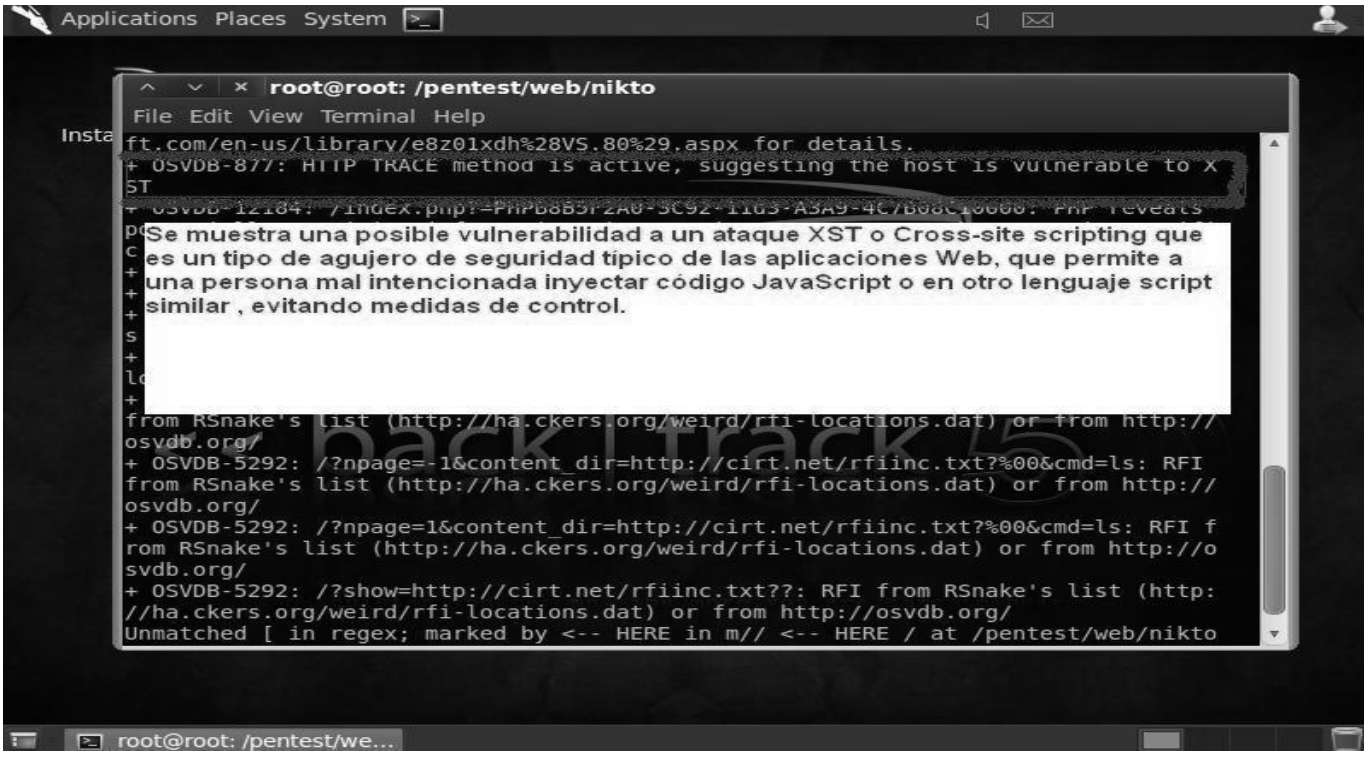
7 - Remote File

8 - Command Execution / Remote Shell

9 - SQL Injection

Por tanto dependiendo del tipo de prueba a realizar será la orden de ejecución que se le dará, por ejemplo para realizar un escaneo en busca de posibles inyecciones XSS se deberá dar la orden de escaneo tipo 4 con el comando: ./Nikto.pl –h 10.52.60.134 –T 4

Caso de Prueba 5
Nombre: Escaneo de vulnerabilidades con Nikto
Descripción: Utilizando la herramienta Nikto se realiza un escaneo del servidor Apache en busca de vulnerabilidades.
Condiciones de ejecución: Que el servidor se encuentre activo.
Entrada/Pasos de ejecución: Ejecutar Nikto desde BackTrack. Se ejecuta la secuencia de comandos siguientes: **./Nikto.pl –h 10.52.60.134**
Resultado esperado: Posibles vulnerabilidades en el servidor Apache.
Explicación del Resultado:



Se muestra una vulnerabilidad a un posible ataque XST.

Evaluación de la prueba: Prueba satisfactoria

3.2.2.3 Penetración o ataque

Con toda la información obtenida de las etapas anteriores se dirigen los ataques hacia los puertos abiertos descubiertos y los servicios donde se ejecutan las aplicaciones web o puertos donde se ejecutan servicios con altos privilegios.

Para esta fase se utiliza el entorno gráfico Armitage creado para Metasploit, donde se visualizan los equipos, exploits, payloads a usar gráficamente. Para poder conectarse a Armitage será necesario conocer el usuario y password de la base de datos de Metasploit.

Una vez en el entorno gráfico de Metasploit se añaden los host que serán objetos de intrusión como se muestra en la figura siguiente.

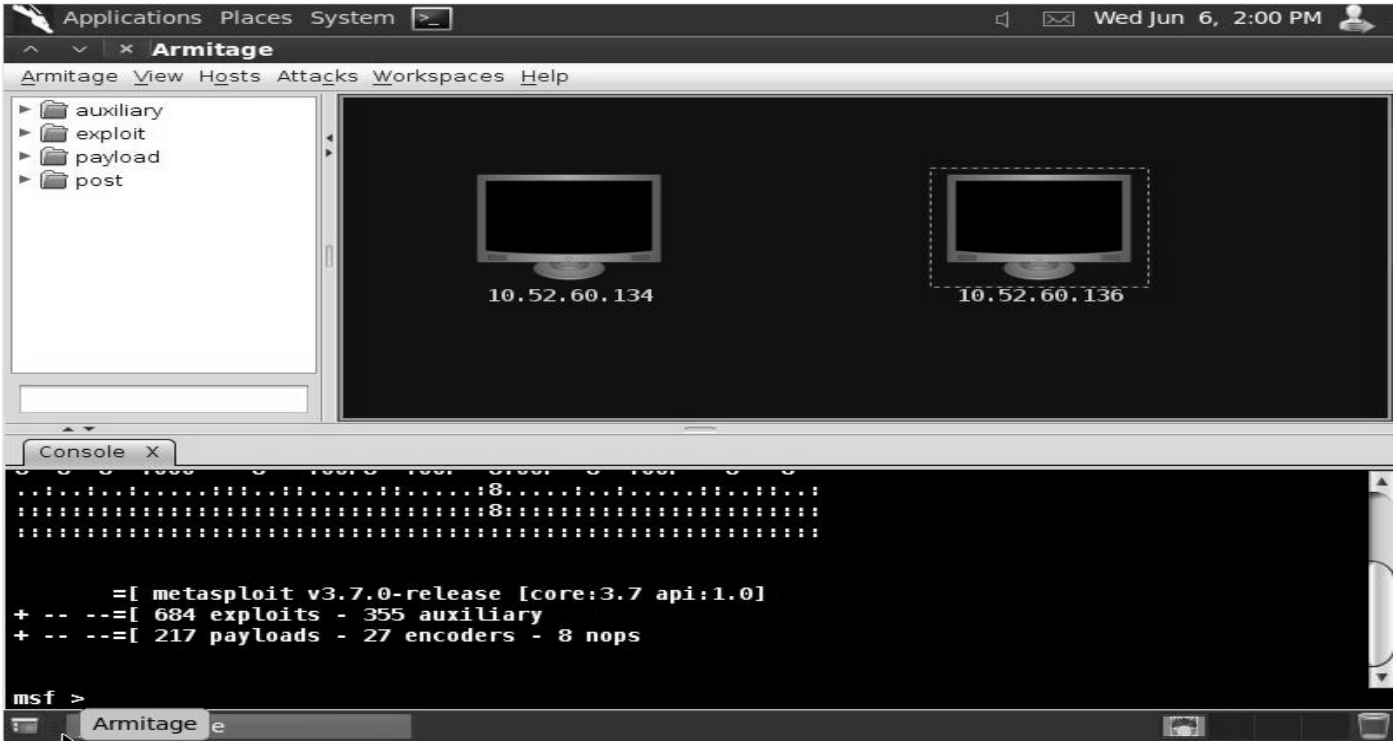
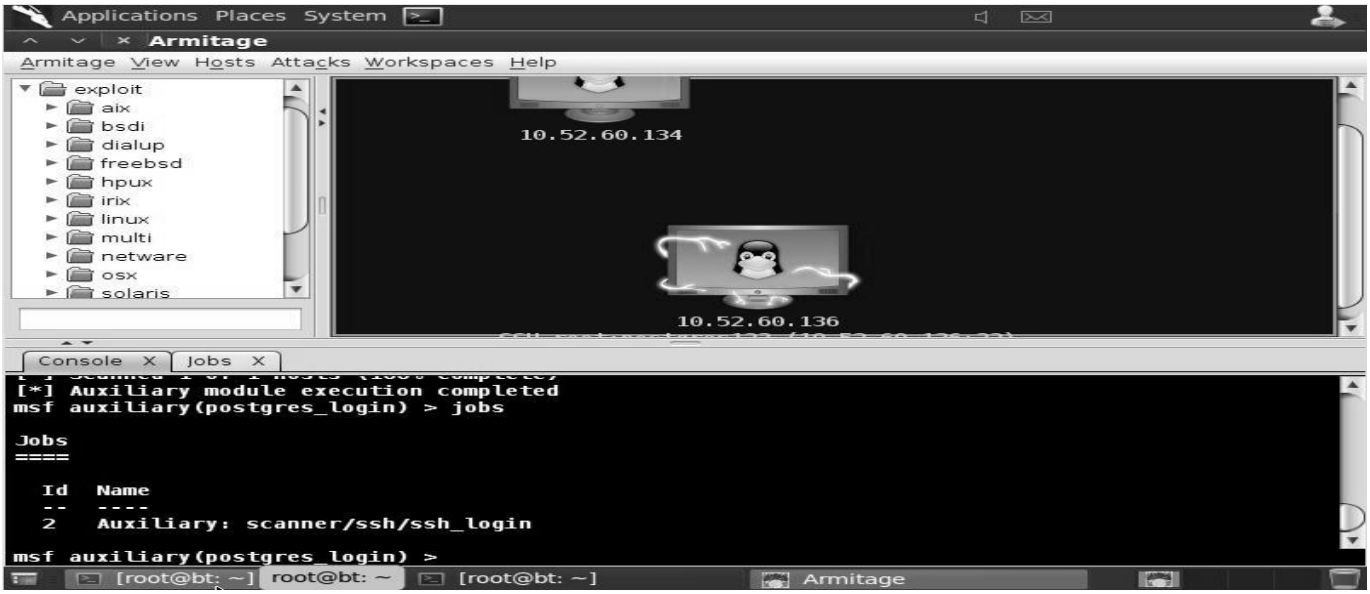
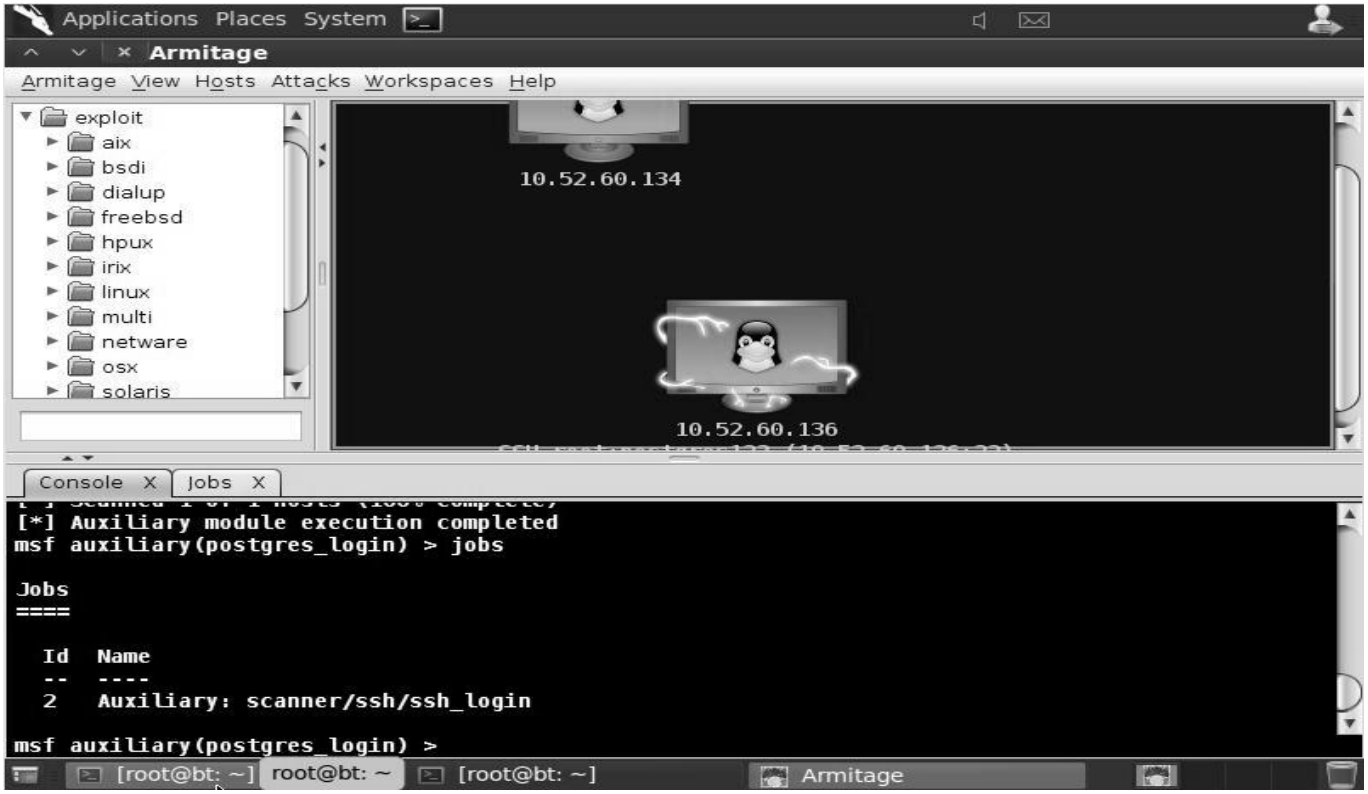


Figura 3.1 Entorno de Armitage

Caso de Prueba 6
Nombre: Vulnerar Servidor Postgres
Descripción: Utilizando la herramienta Metasploit se tratará de vulnerar el servidor de Postgres.
Condiciones de ejecución: Que el servidor se encuentre activo. Que el puerto 5432 esté abierto.
Entrada/Pasos de ejecución: Ejecutar Metasploit desde BackTrack. Se ejecuta la secuencia de comandos siguientes: **search postgres** (para buscar los módulos de Metasploit relacionados con Postgres). En este caso se selecciona **auxiliary/scanner/postgres/postgres_login.** Luego se muestran las opciones disponibles con el comando **show options.** Luego hay que cambiar la opción **RHOSTS** e indicar el IP objetivo, en este caso 10.52.60.136 que es donde se encuentra el servidor de Postgres.
Resultado esperado: Que las credenciales (usuario y contraseña) por defecto de Postgres no hayan sido cambiadas.
Explicación del Resultado:    El exploit fue lanzado con éxito y las credenciales de postgres son las de por defecto.
Evaluación de la prueba: Prueba satisfactoria

Caso de Prueba 6.1
Nombre: Vulnerar Servidor Postgres
Descripción: Utilizando la herramienta Metasploit se tratará de vulnerar el servidor de Postgres.
Condiciones de ejecución: Que el caso de prueba 6 haya sido finalizado con éxito.
Entrada/Pasos de ejecución: Ya conocidas las credenciales de acceso a Postgres, se procede al logueo desde Metasploit con el comando psql -h 10.52.60.136 -p 5432 -U postgres –W postgres
Resultado esperado: Que el usuario/grupo postgres pueda acceder a /root) para obtener el archivo que contiene la clave pública de SSH.
Explicación del Resultado:    Se obtuvo la clave pública de SSH.
Evaluación de la prueba: Prueba satisfactoria

Capítulo 3 Validación de la Propuesta

Aprovechando que los puertos 7 y 19 de UDP en los servidores objetivos se encuentran activos se puede realizar un ataque Snork enviándose un paquete UDP que genere un bucle de ciclo infinito entre los dos servidores.

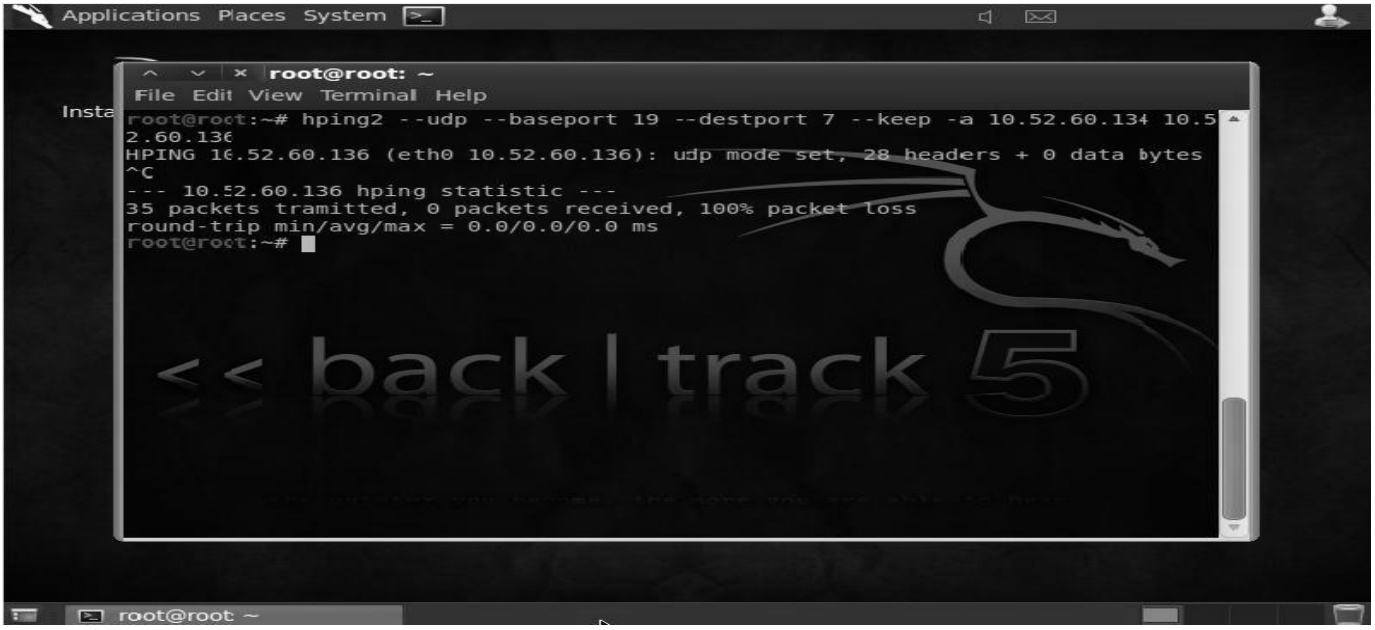
El comando a ejecutar es el siguiente:

hping2 --udp --baseport 19 --destport 7 --keep -a Victima PC_Lanzadera.

Víctima	IP de la víctima.
PC_Lanzadera	IP de la máquina que se usará de lanzadera para atacar a la víctima.
--keep –a	Permite que el puerto origen y destino se incrementen en forma numérica.
--destport	Puerto destino.
--baseport	Puerto fuente.

Caso de Prueba 7
Nombre: Ataque Snork
Descripción: Este ataque puede realizarse entre varias computadoras (consumiendo ancho de banda y degradando el rendimiento de la red) o desde un mismo computador consiguiendo consumir los recursos existentes (especialmente CPU y memoria) de la máquina atacada.
Condiciones de ejecución: Que los puertos 7 y 19 de UDP se encuentren en estado abierto (open) en los servidores de Apache y Postgres.
Entrada/Pasos de ejecución: Desde BackTrack ejecutamos el comando hping2 para enviar un paquete UDP que genere el bucle infinito entre 10.52.60.134 y 10.52.60.136. El comando a ejecutar sería el siguiente: hping2 --udp --baseport 19 --destport 7 --keep -a 10.52.60.134 10.52.60.136
Resultado esperado: Que se genere un bucle infinito de tal forma que ocurra una denegación de servicios en el servidor de Apache.

Explicación del Resultado:



No se logró el objetivo.

Evaluación de la prueba: Prueba insatisfactoria, se necesita más de una PC para lograr la denegación de servicios.

Capítulo 3 Validación de la Propuesta

3.3 Resultado de los casos de pruebas

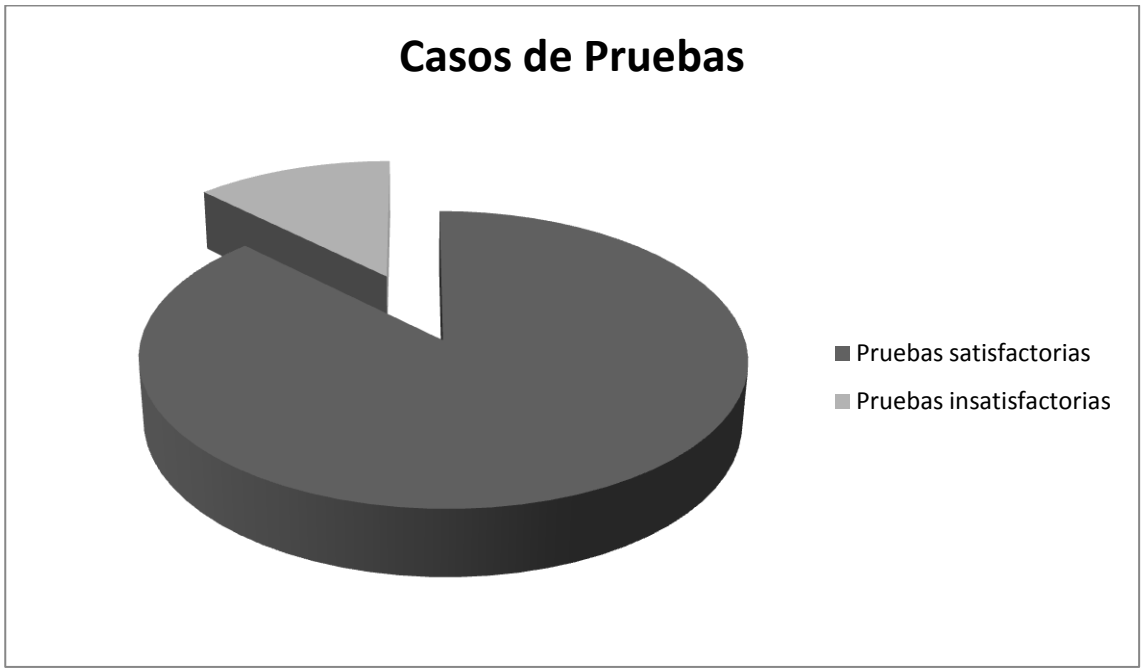


Figura 3.2 Representación gráfica de los casos de pruebas

3.4 Conclusiones

En este capítulo se ha validado la propuesta de solución, poniéndose en ejecución el procedimiento definido para realizar pruebas de penetración, durante el procedimiento se realizaron una serie de actividades identificadas por cada etapa así como también se utilizaron una serie de herramientas automatizadas contenidas en BackTrack, obteniéndose de esta manera el artefacto principal del PenTest como lo es el reporte final de las pruebas.

CONCLUSIONES

Durante todo este trabajo se ha realizado un estudio acerca de las pruebas de penetración para adaptarlas a los Centros de Datos, se ha realizado un estudio sobre la evolución de las mismas así como de las herramientas de penetración más actuales y más utilizadas hoy en el mundo de la seguridad informática. Se analizaron los procedimientos de pruebas de penetración más actuales, identificándose una serie de actividades, que independientemente de los estándares existentes, son genéricas para desarrollar un satisfactorio proceso de pruebas de penetración. Se adaptaron las características y los estándares de las pruebas de penetración en una propuesta de solución a la problemática existente en los Centros de Datos, elaborándose así el procedimiento propuesto para realizar pruebas de intrusión en las redes de los Centros de Datos. Una vez validado este procedimiento mediante un ataque controlado en un escenario montado en dicho centro y a partir de los resultados obtenidos, se concluye (ó) que la efectividad de un ataque es proporcional a la cantidad de información que se tenga sobre el sistema objetivo, que el descuido por parte de los responsables de la seguridad sobre la publicación de determinada información puede ser utilizada de forma ofensiva para ingeniar un ataque. Lo mismo ocurre con configuraciones de servicios y sistemas que ofrecen información precisa sobre las versiones de software que están en funcionamiento pudiéndose citar banners y mensajes de error. No es necesario ser un experto para desplegar muchos de los ataques que hoy en día sufren organizaciones y empresas. La existencia de herramientas de PenTest utilizadas para llevar a cabo auditorías son también utilizadas por ciberdelicuentes para comprometer sistemas. La facilidad de uso de muchas de estas herramientas da lugar a que se incrementen los intentos de intrusión por personas que apenas tienen conocimientos básicos en seguridad informática. La mejor manera de evitar un ataque es estar preparados. Existe un abanico enorme tanto de técnicas como de herramientas para pruebas de penetración que no se han cubierto en todo el documento por no ser objeto directo del mismo pero sin lugar a dudas BackTrack recoge un buen arsenal de estas herramientas por lo que la convierte en una de las distribuciones más utilizadas para testear y auditar sistemas. Existen múltiples puntos de acceso y caminos que el atacante puede seguir para obtener información y acceso a un entorno que se considera seguro. Por lo tanto, no se debe obviar ninguna de las cuestiones relacionadas al ambiente informático por mínimas que parezcan y se deben seguir las mejores prácticas recomendadas por los profesionales de seguridad de todo el mundo.

RECOMENDACIONES

- Continuar perfeccionando el procedimiento de pruebas de penetración en la infraestructura del Centro de Datos.
- Realizar pruebas de penetración a todas las áreas existentes en la red del Centro de Datos desde las perspectivas internas y externas.
- Dar continuidad a los estudios acerca de las pruebas de penetración ya que este campo está en constante evolución y los métodos y medios para violar la seguridad en las redes son cada vez más novedoso y mejores planificados.
- Se recomienda la creación de un grupo especializado en la implementación de pruebas de penetración.
- Probar y evaluar nuevas herramientas para pruebas de penetración estableciendo comparaciones entre las mismas.
- Ampliar la estrategia de pruebas con nuevas herramientas y nuevos mecanismos.

BIBLIOGRAFÍA

Tesis:

[1]. Gómez Santiago Marco Antonio, Venegas Tamayo Carlos Daniel, Yáñez Hernández Vicente. Herramientas para Hacking Ético. Instituto Politécnico Nacional Escuela Superior de Cómputo, 2010. 99.

[2]. Cristian F. Borghello. Seguridad Informática: Sus implicancias e implementación.

[3]. Inti Jiménez Márquez. Test de Penetración en la Red de la Universidad de las Ciencias Informáticas. La Habana, 2008. 88

Fuentes electrónicas:

[1]. Jorge Mieres. Ataques Informáticos. Debilidades de seguridad comúnmente explotadas, 2009.

[2]. Ethical Hacking. Capítulo 7, 2010.

[3].Ethical Hacker Security Training – Metodologías de Penetration Testing, 2008.

[4]. Dr. Javier Areito Bertolín y Dra. Ana Areito Bertolín. Test de penetración y gestión de vulnerabilidades, estrategia clave para evaluar la seguridad de red, 2009.

[5]. Borja Merino Febrero y José Miguel Holguín. PenTest: Recolección de Información, 2012. [Disponible en: http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_information_gathering.pdf]

[6]. Bernabé Muñoz. Taller Auditoria y PenTest, 2011. [Disponible en: http://es.scribd.com/doc/61764495/Taller-Practico-de-Auditoria-y-Pentest]

[7]. Conceptos de Hacking Ético, 2010. [Disponible en:http://www.tics.org.ar/index.php?option=com_content&view=article&id=97:conceptos-de-hacking-etico&catid=14:seguridad-informca&Itemid]

[8]. María Dolores Cano Baños, Natalio López Martínez. Práctica 0: Escáneres de red. [Disponible en: http://ocw.bib.upct.es/pluginfile.php/6720/mod_resource/content/1/Practica_0.pdf]

[9]. José Rhin Salazar. Ethical Hacking, 2009.

[10]. Maikel Menéndez Méndez. Ethical hacking: Test de intrusión. Principales metodologías, 2009.

[11]. Juan David Berrio López. Hacking Ético VS Defensa en Profundidad, 2012. [Disponible en: www.dsteamseguridad.com]

[12]. Martin Vila. Ethical Hacking, Métodos Avanzados de Hacking y Protección, 2012. [Disponible en: http://www.cert.uy/archivos/ISEC_PRESENTACION_AGESIC_2009_MARTIN_VILA_JULIO_BALDERRAMA.pdf]

[13]. Gaspar Modelo Howard. Evaluación de Vulnerabilidades Informáticas. [Disponible en: http://web.ics.purdue.edu/~gmodeloh/ppt/LatinCACS05-323-GMHoward-v1.05.pdf]

[14]. OWASP Web Application Penetration Checklist. [Disponible en: http://www.owasp.org]

[15]. David Buyer. Penetration Test Manual, 2010.

[16]. Israel Rosales Marco. Hacking Labs for PenTest, 2011.

[17]. Luis Ramírez. Penetration Test, Metodologías & Usos, 2009.

[18]. Ezequiel H. Farah. Seguridad Informática. Ethical Hacking Y Herramientas, 2010.

[19]. Alejandra T. Chávez Flores. Informe de Seguridad Informática, 2009.

[20]. DrC. Walter Baluja García. Seguridad de Redes y Sistemas, 2006.

[21]. Armando Carvajal. Introducción a las técnicas de ataque e investigación forense, un enfoque pragmático.

[22]. Enrique Javier Santiago Chinchilla. Test de penetración como apoyo a la evaluación, 2009.

[23]. Álvaro Gómez Vieites. Tipos de Ataques e Intrusos en las Redes Informáticas.

[24]. Víctor H. Montero. Técnicas del Penetration Testing, 2009.

[25]. Ministerio de la Informática y las Comunicaciones. RESOLUCIÓN No. 127 /2007. [Disponible en:http://seguridad.uci.cu/sites/all/themes/arthemia/files/reglamentos/Resolucion_127_del_MIC.pdf]

[26]. M. en C. Mario Farías-Elinos. Seguridad en los Sistemas de Cómputo, 2008.

[27]¿Cómo realizar un Penetration Test?,2011.

[28]. Lic. Tomás Heredia. Seguridad Informática para Administradores de Redes y Servidores, 2008.

[29]. Sitio Web Oficial de Nmap, 2012. [Disponible en: http://insecure.org/nmap]

[30]. Sitio Oficial de OpenVas, 2012. [Disponible en: http://www.openvas.org/]

REFERENCIAS

[1]. MIC. Portal de Seguridad Informática. Resolución 127 del MIC, 2007. [Disponible en: http://seguridad.uci.cu/sites/all/themes/arthemia/files/reglamentos/Resolucion_127_del_MIC.pdf.]

[2]. Estratecgias, 2012 [Disponible en:http://www.estratecgias.com/software/calidad-de-software/pruebas-seguridad]

[3]. Seguridad de la Información, 2011. [Disponible en: http://seguridadenlainformacion81.bligoo.com.mx/.]

[4]. Borghello, Cristian F. Seguridad Informática. Sus Implicancias e Implementación, 2010. [Disponible en: http://www.segu-info.com.ar]

[5]. McBride George G. The Art of Penetration Testing, 2010. [Disponible: http://ebookbrowse.com/george-g-mcbride-rsa03-the-art-of-penetration-testing-ppt-d17644162]

[6]. Arce, Iván, 2010. The Penetration Test.

[7]. Lic. Ramírez, Luis Penetration Test Metodologías & Usos, 2009. [Disponible en:http://www.cybsec.com/upload/Ramirez_Tendencias_PenTest_v2_0.pdf]

[8].Consultoría de Seguridad de la información, 2007. [Disponible en: http://www.berriaconsultores.es/web/ingenieria]

[9].Técnicas de Security Penetration Testing, 2009. Disponible en [http://www.haxsecurity.org/documentos/presentaciones/Penetration_Testing.pps]

[10].Pete Herzog. OSSTMM 2.1, Manual de la Metodología Abierta de Testeo de Seguridad, 2003. [Disponible en: http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf]

[11].Mallelin Bolufe Chávez, Maikel Menéndez Méndez. Ethical hacking: Test de intrusión. Principales metodologías, 2009.

[12].SEGURIDAPC.NET Test, 2012. [Disponible en: http://www.seguridadpc.net/exploit.htm]

[13].Juan David Berrio López. Hacking Ético VS Defensa en Profundidad, 2012. [Disponible en: http://www.dsteamseguridad.com/museo/HACKIN%20ETICO_VS_DEFENSA_PROFUNDIDAD_JUANBERRIO.pdf]

[14].Fabián Leonardo Herrera Rico, Arnold Iván Ordóñez Ramírez. Herramienta para Detección de Vulnerabilidades en Infraestructura Tecnológica. Bogotá, 2008.

[15]. Maltego. [Disponible en: http://andres-elladooscuro.com/2012/02/maltego.html]

[16]. FOCA – Herramienta para análisis de Meta Datos [Disponible en: http://www.dragonjar.org/foca-herramienta-para-analisis-meta-datos.xhtml]

[17].Nmap. Página oficial, 2012. [Disponible en: http://nmap.org/man/es]

[18]. Carlos Tori. Hacking Ético, 2008. [Disponible en: http://seguridad.uci.cu/?q=node/15/203]

[19].Las 75 Herramientas de Seguridad Más Usadas, 2012. [Disponible en: http://insecure.org]

[20].Joaquín García Alfaro. Exploraciones de red con Nmap y Nessus,2010. [Disponible en: http://www.sw-computacion.f2s.com/Linux/012.3-Aspectos_avanzados_en_seguridad_en_redes_apendice.pdf]

[21].Fabián Leonardo Herrera Rico, Arnold Iván Ordóñez Ramírez, 2008. Herramienta para Detección de Vulnerabilidades en Infraestructura Tecnológica.

[22].Stephen Northcutt, Jerry Shenk, Dave Shackleford, Tim Rosenberg, Raúl Siles, and Steve Mancini. Penetration testing: Assessing Your Overall Security Before Attackers Do, 2006. [Disponible en: http://www.sans.org/reading_room/analysts_program/PenetrationTesting_June06.pdf]

[23]. Nikto: Documentation, 2012. [Disponible en: http://cirt.net/nikto2-docs/]

ANEXOS

Anexo # 1 Acuerdo de Confidencialidad y no Divulgación de la Información.

ACUERDO DE CONFIDENCIALIDAD
Y NO DIVULGACIÓN DE INFORMACIÓN

En _____ (ciudad), a los___ del mes de _____ de _____.
De un lado, _____ (Nombre y apellidos del DIVULGANTE), en su propio nombre y derecho / en nombre y representación de _____ (Nombre de la empresa, organización o institución que solicita el PenTest), con domicilio a efectos del presente Acuerdo en _____ (Dirección donde radica la empresa, organización o institución que solicita el servicio), en adelante "EL DIVULGANTE".
Y de otro, _____ (Nombre y apellidos del posible INVERSOR), en su propio nombre y derecho / en nombre y representación de _____ (Nombre de la empresa o institución que realizará el PenTest), con domicilio a efectos del presente Acuerdo en _____ (Dirección donde radica la empresa o institución que prestará el servicio), en adelante "EL INVERSOR".

Ambas partes suscriben el presente Acuerdo de Confidencialidad y de No Divulgación de Información en base a las siguientes ESTIPULACIONES:
PRIMERA. El presente Acuerdo se refiere a la información que EL DIVULGANTE proporcione al INVERSOR o a la información que el INVERSOR tenga acceso durante el servicio que prestará, ya sea de forma oral, gráfica o escrita y, en estos dos últimos casos, ya esté contenida o no en cualquier tipo de documento, con ocasión de las negociaciones que se están desarrollando / que se van a desarrollar a fin de realizar las pruebas de penetración.
SEGUNDA.- 1. EL INVERSOR únicamente utilizará la información facilitada por EL DIVULGANTE para el fin mencionado en la Estipulación anterior, comprometiéndose EL INVERSOR a mantener la más estricta confidencialidad respecto a dicha información, advirtiendo de dicho deber de confidencialidad y secreto al resto de su equipo y a cualquier persona que, por su relación con EL INVERSOR, deba tener acceso a dicha información para el correcto cumplimiento de las obligaciones del INVERSOR para con

EL DIVULGANTE.

2. EL INVERSOR o las personas mencionadas en el párrafo anterior no podrán reproducir, modificar, hacer pública o divulgar a terceros la información objeto del presente Acuerdo sin previa autorización escrita y expresa del DIVULGANTE.

3. De igual forma, EL INVERSOR adoptará respecto a la información objeto de este Acuerdo, las mismas medidas de seguridad que adoptaría normalmente respecto a la información confidencial de su propia empresa, evitando en la medida de lo posible su pérdida, robo o sustracción.

TERCERA.- Sin perjuicio de lo estipulado en el presente Acuerdo, ambas partes aceptan que la obligación de confidencialidad no se aplicará en los siguientes casos:

a) Cuando la información se encontrara en el dominio público en el momento de su suministro al INVERSOR o, una vez suministrada la información, ésta acceda al dominio público sin infracción de ninguna de las Estipulaciones del presente Acuerdo.

b) Cuando la información ya estuviera en el conocimiento del INVERSOR con anterioridad a la firma del presente Acuerdo y sin obligación de guardar confidencialidad.

c) Cuando la legislación vigente o un mandato judicial exija su divulgación. En ese caso, EL INVERSOR notificará al DIVULGANTE tal eventualidad y hará todo lo posible por garantizar que se dé un tratamiento confidencial a la información.

d) En caso de que EL INVERSOR pueda probar que la información fue desarrollada o recibida legítimamente de terceros, de forma totalmente independiente a su relación con EL DIVULGANTE.

CUARTA.- Los derechos de propiedad intelectual de la información objeto de este Acuerdo pertenecen al DIVULGANTE y el hecho de revelarla al INVERSOR para el fin mencionado en la Estipulación Primera no cambiará tal situación.

En caso de que la información resulte revelada o divulgada o utilizada por EL INVERSOR de cualquier forma distinta al objeto de este Acuerdo, ya sea de forma dolosa o por mera negligencia, habrá de indemnizar al DIVULGANTE los daños y perjuicios ocasionados, sin perjuicio de las acciones civiles o penales que puedan corresponder a este último (si se quiere, se puede fijar aquí mismo una cantidad determinada como indemnización).

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

relación entre las partes por cualquier motivo.

SEXTA.- El presente Acuerdo entrará en vigor en el momento de la firma del mismo por ambas partes, extendiéndose su vigencia hasta un plazo de _____ después de finalizada la relación entre las partes o, en su caso, la prestación del servicio.

SÉPTIMA.- En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, las partes se someten expresamente a los decretos y leyes existentes en la República de Cuba aplicándose la Resolución No 127 /2007 del Ministerio de la Informática y las Comunicaciones.

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

_____	_____
Nombre y apellidos del INVERSOR	Nombre y apellidos del DIVULGANTE

Anexo # 2 Carta de Autorización

CARTA DE AUTORIZACIÓN
PARA REALIZAR
PRUEBAS DE PENETRACIÓN (PenTest)

En _____ (ciudad), a los___ del mes de _____ de _____.

Para proteger adecuadamente los activos de la organización en cuanto a las tecnologías de la información se refiere, el equipo de seguridad de la información de _____ (Nombre de la empresa, organización o institución que solicita el PenTest) ve la necesidad de evaluar nuestra posición de seguridad periódicamente mediante la realización de evaluaciones de vulnerabilidad y pruebas de penetración. Estas actividades suponen pruebas de intrusión a equipos de sobremesa, portátiles, servidores, elementos de red y otros sistemas informáticos propiedad de esta organización sobre una base regular y periódica para descubrir las vulnerabilidades presentes en estos sistemas. Sólo con el conocimiento de estas vulnerabilidades nuestra organización puede aplicar parches de seguridad u otros controles de compensación para mejorar la seguridad de nuestras redes.
El propósito de esta nota es para conceder la autorización a los miembros específicos del equipo de pruebas de penetración de _____ (Nombre de la empresa o institución que realizará el PenTest) para llevar a cabo evaluaciones de vulnerabilidad y pruebas de penetración contra los bienes de esta organización. A tal fin, el firmante atestigua la siguiente:

1) [Inserte los nombres y apellidos de todos los miembros del equipo PenTest] tienen permiso para realizar pruebas de penetración a las redes del centro. Este permiso se concede a partir de [insertar fecha de inicio] hasta [insertar fecha de finalización].

2) [Insertar nombre del aprobador] tiene la autoridad para conceder este permiso para probar los activos de las Tecnologías de la Información de la organización.

3) [Inserte permisos adicionales y / o restricciones en su caso.]

_____ _____

Nombre y Apellidos de quien aprueba la carta (Director, Jefe o Gerente del centro)

Firma y Cuño