PRUEBAS DE PENETRACIÓN O PENT TEST

Jorge Luis Ramos Ramos
Universidad Mayor de San Andrés
Facultad de Ciencias Puras y Naturales
Carrera de Informática
Análisis y Diseño de Sistemas de Información
jorge.infobo@gmail.com

RESUMEN

En este artículo se muestra que los *ethical hackers* son personas o redes de computadoras que se dedican a analizar/evaluar las debilidades o vulnerabilidades de los sistemas informáticos, atacándolos con autorización de sus propietarios, para así poder encontrar alguna falla que los hackers o piratas puedan utilizarlos, es por eso que surge la necesidad de desarrollar esto que se conoce comopruebas de penetración *o Pent Test*.

Las pruebas de penetración o *Pent Test*son un conjunto de metodologías y técnicas que permiten realizar una evaluación integral de las debilidades de los sistemas informáticos.

Estas pruebas son realizadas con el consentimiento del o los propietarios de los sistemas, y es obligatorio y aconsejable que esto lo realicen personas ajenas a la empresa, ya que si lo hiciera alguien de la empresa se cometería el error de ser juez y parte.

Palabras Clave

Ethical Hacker, test de penetración, *Black-box, White-box, Gray-box*.

1. INTRODUCCIÓN

El termino ***Pent Test*** es como comúnmente se denomina a los "**Test de penetración**" o en inglés "***Penetration Tests"***, y es un procedimiento que se realiza atravez de un conjunto de técnicas y métodos que simulan el ataque a un sistema esto nos sirve para evaluar la seguridad de los sistemas informáticos, redes y aplicaciones.

Es necesario realizar un pent test ya que no importa que tan bien este protegido el sistema, siempre existe la posibilidad de ser blanco de ataques es por eso importante descubrir las fallas mediante el uso de las herramientas, así se podrá defender de posibles ataques.

Entre las diferentes herramientas se incluyen desde scanners de puertos, complejos algoritmos para descifrar claves, sistemas de intrusión por fuerza bruta, herramientas de *sniffing* de redes y penetración de *firewalls*, así como también herramientas de escaneo de vulnerabilidades de aplicaciones web y mucho más.

Las herramientas suelen estar agrupadas en lo que se conoce como "*Toolkits"* o juegos de herramientas, existen algunos *Toolkits* que son famosos por su eficiencia y por haber sido utilizados en penetraciones de alto nivel, existen algunos que ya están instaladas en un CD de arranque del sistema operativo con el que trabajan y son portátiles.

2. TIPOS DE PENT TESTS

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

- Pruebas de penetración con objetivo: se buscan las vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización.
- Pruebas de penetración sin objetivo: consisten en examinar la totalidad de los componentes de los sistemas informáticos pertenecientes a la organización. Estas pruebas suelen ser las más laboriosas.
- Pruebas de penetración a ciegas: en estas pruebas sólo se emplea la información pública disponible sobre la organización.
- Pruebas de penetración informadas: aquí se utiliza la información privada, otorgada por la organización acerca de sus sistemas informáticos. En este tipo de pruebas se trata de simular ataques realizados por individuos internos de la organización que tienen determinado acceso a información privilegiada.
- Pruebas de penetración externas: son realizas desde lugares externos a las instalaciones de la organización. Su objetivo es evaluar los mecanismos perimetrales de seguridad informática de la organización.
- Pruebas de penetración internas: son realizadas dentro de las instalaciones de la organización con el objetivo de evaluar las políticas y mecanismos internos de seguridad de la organización.

A su vez, cada tipo de pruebas descrito anteriormente se puede ubicar en tres modalidades.

Black-box:El pentester no tiene conocimiento del sistema. En general se utiliza cuando se contrata una empresa para que realice el trabajo desde el punto de vista de un posible atacante externo.

White-box:El pentester tiene conocimiento del funcionamiento del sistema, arquitectura de la red, sistemas operativos utilizados.etc. Si bien no representa la visión de un atacante externo, si representa el peor escenario ya que es el caso en el que un atacante ya cuenta con información antes de accesar al sistema.

Gray-box:Este es el caso en el cual el pentester simula un empleado interno, para esto se le da un usuario y clave de los sistemas. La idea es encontrar posibles problemas que puedan ser

aprovechados por usuarios internos.

3. METODOLOGIA DE EVALUACION

Se utiliza una metodología de evaluación de seguridad informática que incluye cuatro etapas:

3.1 Etapa de Descubrimiento

Esta es la etapa donde se deberá delimitar las áreas donde se focalizara la evaluación, para ello se debe entender los riesgos del negocio asociado al uso de los activos informáticos involucrados. Es por eso necesario realizar la recolección de información como por ejemplo:

- Rangos de direcciones IP asignados
- Direcciones IP de servicios tercerizados
- Dirección física de la empresa
- Números telefónicos
- Nombres de personas y cuentas de correo electrónico
- Fuentes de información
- Análisis de la página WEB
- Existencia de redes inalámbricas (WiFi)

3.2 Etapa de Exploración

En esta se trazan los objetivos para las demás etapas y se aplican técnicas no invasivas para identificar todos los blancos potenciales.

Además se deberá incluir el análisis de protocolos, relevamiento de plataforma y barreras de protección, scanning telefónico, scanning de puertos TCP y UDP, detección remota de servicios y sistemas operativos, análisis de banners y búsqueda de aplicaciones web.

Las tareas que predominan en esta etapa son:

- Detección de módems activos.
- Confirmación de rangos de direcciones IP.
- Detección de equipos activos e identificación de Sistemas Operativos.
- Detección de servicios activos e identificación Software y versiones.
- Detección de barreras de protección.
- Análisis de características de configuración en redes WiFi.

3.2.1 Técnica de Scanning

Esta técnica la utilizan los intrusos para poder acceder a un conjunto de blancos potenciales buscando alguna característica.

Esta técnica se la utiliza en la detección de equipos, servicios y módems activos.

3.3 Etapa de Evaluación

Se basa en el análisis de todos los datos encontrados para la detección y determinación de vulnerabilidades de seguridad informática que afectan a los sistemas evaluados.

Durante esta etapa se realizan las evaluaciones de seguridad en todos los posibles niveles, destacándose las siguientes tareas:

- Ejecución de herramientas de scanning de vulnerabilidades.
- Búsqueda manual de vulnerabilidades.

3.3.1 Herramientas de scanning de vulnerabilidades

- Buscan automáticamente vulnerabilidades “conocidas” en los Sistemas Operativos y servicios que se estén ejecutando.
- Permiten, en algunos casos, “explotar” las vulnerabilidades detectadas.
- Facilitan la actualización de las bases de datos de vulnerabilidades.

3.3.2 Búsqueda manual de vulnerabilidades

Para realizar esta búsqueda es necesario verificar la existencia de vulnerabilidades conocidas que puedan afectar a las versiones del software identificado en cada servicio.

Existen numerosos sitios con información sobre vulnerabilidades reportadas por otros pentesters.

3.4 Etapa de Intrusión

Esta es la etapa más compleja del pent test pero al mismo tiempo el emocionante para el equipo de trabajo, ya que es donde se ve reflejado en mayor medida el conocimiento y profesionalismo del mismo.

Aquí se utiliza el conocimiento adquirido en etapas previas para buscar alternativas que permitan acceder a los sistemas y obtener el control de los mismos.

4. PLANEAMIENTO

La realización de un pent test requiere una planificación previa que tiene mínimamente los siguientes pasos:

- Reunión de alineamiento

En esta reunión debe definirse el alcance del trabajo. Dentro de esto tenemos:

- ¿Que tipo de Pentest se va a realizar?
- Horario de realización del pentest (durante las horas laborales o fuera del horario laboral)
- Se permitira DOS?
- Se pueden instalar *Backdoors* ?
- Se pueden realizar *Defacement* de los sitios?
- Se pueden borrar l*ogs* ?
- Conocerá el personal la realización del pentest?
- Se puede utilizar Ingeniería Social?

Luego de esta reunión se realizara un documento en forma de contrato o de memo interno indicando el alcance del pent test y otorgando el permiso necesario para la realización.

- Realización del Pentest

La realización del pentest básicamente esta dividida en los siguientes pasos:

Reconocimiento: Que a su vez esta divido en *Footprint* y *Scanning*

Adquisición de Objetivo: Comprende Enumeración de vulnerabilidades, Acceso, estalación de privilegios y búsqueda de nuevos objetivos.

Eliminación de Huellas: Eliminación de rastros en logs.

Luego dependiendo de los acordados, se pueden realizar pruebas de Denegación de Servicios o dejar instalados Backdoors.

- Reporte

En este paso se realizara el reporte de los resultados obtenidos de la evaluación

- Presentación de resultados

En este último paso se presentan todos los resultados de la evaluación del sistema.

5. HERAMIENTAS ÚTILES EN PENETRATION TESTING PARA APLICACIONES WEB

Estas herramientas son muy útiles para la realización de tests de penetración (Pen Testing) sobre aplicaciones web. Algunas herramientas son gratuitas y de código abierto, otras de pago y propietarias.

- **Burp Suite [6]**

Es una excelente plataforma para PenTest y seguridad en sitios web. Esta herramienta posee muy buenas características como: *Intercept Proxy*, detección automática de vulnerabilidades, herramienta de repetición, posibilidad de escribir *plugins* propios

- **Acunetix – Scaner para vulnerabilidades web [7]**

Esta es una potente herramienta para MS Windows que detecta un gran número de vulnerabilidades, entre ellas Cross-Site Scripting, SQL Injection, CRLF injection, busca vulnerabilidades en formularios de subida de archivos (*file upload*) y otros mas.
También nos permite guardar los resultados en una base de datos o exportarlos en el formato deseado para generar reportes detallados

- **SQLmap [8]**

Es una herramienta Open Source y gratuita basada en línea de comandos que automatiza la detección y explotación de vulnerabilidades SQL Injection y extracción de información de bases de datos.

- **Nessus [10]**

Está orientada a un uso mas extensivo en materia de tests (es decir, redes amplias, gran cantidad de dispositivos, etc.) también es muy útil para realizar PenTesting a aplicaciones web habilitando y configurando los módulos correctos.

6. CONSIDERACIONES LEGALES

Ante la realización de un PenTest se deben considerar las implicaciones legales que esto puede acarrear.
Ya que existen legislaciones que condenan la intrusión a sistemas y redes informáticas, formalmente hace falta que la organización firme dos cartas a la empresa que realiza el PenTest: un convenio de confidencialidad y una carta de autorización.
El convenio de confidencialidad es básicamente un reglamento, 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 durante la realización del PenTest.
La carta de autorización debe estar firmada por el responsable de la Organización (CIO, Oficial de Seguridad Informática, Abogado, etc.) antes de tocar un solo sistema. Estas cartas deberán incluir como mínimo; ¿Quién va a realizarlo?, ¿Cuándo va a ser realizado?, ¿Por qué será realizado?, ¿Qué tipo de actividad es la autorizada y cuál no?, ¿Cuál es el alcance?.
Cuando estos contratos pasan por abogados se demora el proyecto ya que el área legal de la organización se toma sus tiempos para analizar los documentos y seguramente introducirá modificaciones a favor de la organización.

7. CONCLUSIONES

Como podemos ver las técnicas y metodologías del PenTest nos permiten evaluar, y encontrar riesgos que existen en los sistemas informáticos, así poder prevenir ante cualquier amenaza que podría existir.
La seguridad en una organización es un aspecto cambiante, es por eso muy importante realizar un PenTest. Una empresa puede alcanzar un nivel de protección óptimo en un momento determinado y ser totalmente sensible poco después, tras cambios en la configuración de un servidor o tras la instalación de nuevos dispositivos de red. Al pasar del tiempo también surgen fallas en sistemas que se creían que eran seguros.
Es por eso que las compañías tienen una política de realización de PenTest periódicas para poder mitigar en gran medida los riesgos asociados a un entorno cambiante tal como lo representan los sistemas informáticos de cualquier organización.
Existen beneficios cuando se realiza un PenTest por que proporciona un conocimiento del grado de vulnerabilidad de los sistemas de información, es imprescindible para aplicar medidas correctivas, también se descubren fallas de seguridad tras cambios de configuración, también determina sistemas en peligros debido a su desactualización, identifica configuraciones erróneas que pudieran desembocar en fallos de seguridad en dispositivos de red (*switches*, *routers*, *firewalls*, etc.), entre otros mas.

8. REFERENCIAS

[1] http://www.e-securing.com/Mauro Mauini R.
[2]http://d3ny4ll.blogspot.com/2008/11/pentest-una-breve-guia.html
[3]Víctor H. Montero - Seminario “Técnicas del Penetration Testing”
[4]http://seguridadetica.wordpress.com/2012/04/11/5-heramientas-utiles-en-penetration-testing-para-aplicaciones-web/
[5]http://www.seguridad.unam.mx/descarga.dsc?arch=2776
[6]http://portswigger.net/
[7]http://acunetix.com/
[8]http://sqlmap.sourceforge.net/
[9]http://www.morningstarsecurity.com/research/whatweb
[10]http://tenable.com/
[11]MSc. Julio C. Ardita – “Del Penetration Test a la realidad”