Propuesta Prevención para Ataques de Pentesting

4Geeks Academy

FELIPE ALONSO GOMEZ HENRY
ESTUDIANTE BOOTCAMP CIBERSEGURIDAD

4Geeks

Contenido

4Geeks

Información General

Autor: Felipe Gómez Henry

Fecha: 16-04-2025

Objetivo general: Plantear prácticas de prevención para evitar ataques de pentesting que exponga vulnerabilidades en un sistema vulnerable (Metasploitable).

Introducción

Este informe detalla las vulnerabilidades encontradas durante ejercicios de pentesting en laboratorios controlados. Las pruebas se realizaron sobre dos entornos conocidos: Metasploitable2 y DVWA (Damn Vulnerable Web Application). Para el presente reporte, se enfocará el análisis en el primero, en el cual se identificaron debilidades críticas en servicios críticos, se documentaron los vectores de ataque y se plantean medidas para su prevención.

4Geeks

Enfoque y Estrategia

Se realizaron fases completas de reconocimiento, enumeración, explotación y post-explotación usando herramientas automáticas para Identificar vulnerabilidades como:

- Nmap.
- Metasploit Framework.

Objetivos y metodologías de trabajo

- Identificar vulnerabilidades con herramientas automáticas.
- Explotar acceso remoto sin autenticación.
- Validar ejecución remota de comandos (RCE)
- Extraer credenciales con post-explotación

Reconocimiento

i. Escaneo de puertos con nmap con “sudo nmap -sS -sV –script=vuln <ip_atacada>.

Servicios descubiertos:

- FTP (21)
- SSH (22)
- Samba (139, 445)
- Apache Tomcat (8180)
- MySQL (3306)

4Geeks

Resultado Vulnerabilidades Expuestas

I. Nivel alto – Backdoor puerto 21 (ftp).

El servicio FTP se encuentra corriendo con la versión **vsftpd 2.3.4**, vulnerable a un backdoor intencional introducida en el código fuente.

Impacto: Permite al atacante obtener una Shell remota ejecutando :) como nombre de usuario.

II. Nivel medio – puerto 22 (OpenSSH).

Es una versión antigua de OpenSSH (4.7p1) expone la superficie a múltiples vulnerabilidades de enumeración y fuerza bruta.

Impacto: Usuarios pueden ser descubiertos por error responses distintos, potencial para explotación si este combinado con credenciales débiles.

III. Nivel alto – puerto 139/445 (Samba).

Se presenta una versión vulnerable de Samba, vulnerable a “user map script injection”, que permite ejecución remota de comandos como root.

Impacto: Shell remota con privilegios root.

IV. Nivel alto – puerto 8180 (Apache Tomcat).

Se descubrió que el puerto con el servicio Apache Tomcat Manager está expuesto sin credenciales o con credenciales por defecto.

Impacto: Subida de WAR malicioso para ejecución remota, posible Shell reversa.

V. Nivel alto – puerto 3306 (MySQL).

MySQL se encuentra expuesto sin contraseña para usuario root. Esto permite un total acceso a toda la base de datos.

Impacto: Dump completo de la base de datos, modificación o eliminación de datos.

4Geeks

Recomendaciones de prevención para Maquina vulnerable (Metasploitable)

1. Aplicar parches y actualizaciones de seguridad.
2. Limitar exposición de puerto con iptables.
3. Eliminar versiones obsoletas de servicios (vsftpd 2.3.4, Samba 3.x, OpenSSH 4.x)
4. Deshabilitar FTP si no es necesario.
5. Actualizar versión de OpenSSH.
6. Forzar autenticación por clave pública.
7. Usar fail2ban o rate limiting para evitar brute force.
8. Actualizar o eliminar servicios Samba no utilizados.
9. Aplicar configuración restrictiva a smb.conf (ej. map to guest = never).
10. Restringir acceso a puertos 139/445 por firewall.
11. Apache Tomcat: Deshabilitar manager y host-manager en producción.
12. Apache Tomcat: Cambiar credenciales por defecto.
13. Restringir acceso a la consola de administración por IP.
14. MySQL: Establecer una contraseña fuerte para root.
15. Restringir acceso a 3306 solo desde localhost.
16. Eliminar usuarios anónimos.
17. Habilitar logs de auditoría y alertas.

4Geeks

Referencias:

- Vsftpd 2.3.4 Backdoor: https://nvd.nist.gov/vuln/detail/CVE-2011-2523
- Vsftpd 2.3.4 Backdoor: https://nvd.nist.gov/vuln/detail/CVE-2011-2523
- OpenSSH 4.7p1 User Enumeration (Timing): https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=528969
- Samba usermap_script RCE: https://nvd.nist.gov/vuln/detail/CVE-2007-2447
- Apache Tomcat WAR Upload (Manager Exploit): https://www.exploit-db.com/exploits/16572
- MySQL – Root sin contraseña / Exposición: https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- Exploit DB – vsftpd 2.3.4: https://www.exploit-db.com/exploits/49757
- Exploit DB – Samba usermap_script: https://www.exploit-db.com/exploits/16320
- Exploit DB – Apache Tomcat Auth Bypass & WAR Upload: https://www.exploit-db.com/exploits/16572
- Packet Storm Security – vsftpd 2.3.4: https://packetstormsecurity.com/files/162145
- OWASP Top Ten 2021: https://owasp.org/www-project-top-ten/
- CVE Details (para búsqueda de vulnerabilidades): https://www.cvedetails.com/
- Vulners Search Engine: https://vulners.com/