

L'esercizio di oggi consiste nel fare una sessione di hacking usando telnet verso la macchina metasploitable.

Quindi la prima cosa da fare è cambiare l'ip di kali a 192.168.1.25.

```
config
Flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
RX packets 135 bytes 9552 (9.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 32 bytes 3640 (3.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Poi cambiare l'ip di metasploitable a 192.168.1.40, per riuscire a pingare le due macchine.

```
[ Wrote 13 lines ]

in@metasploitable:~$ sudo /etc/init.d/networking restart
configuring network interfaces... [ OK ]
in@metasploitable:~$ ifconfig
Link encap:Ethernet HWaddr 08:00:27:a6:72:76
inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea6:7276/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:133 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:7650 (7.4 KB)
Base address:0xd020 Memory:f0200000-f0220000
```

Poi ritorniamo su kali e avviamo msfconsole e usiamo (auxiliary /scanner /telnet /telnet _version) come in foto, e usiamo (show options) per farci mostrare le opzioni eseguibili.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  no               no        The password for the specified username
  RHOSTS    yes              yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit
             /basics/using-metasploit.html
  RPORT     23               yes        The target port (TCP)
  THREADS   1                 yes        The number of concurrent threads (max one per host)
  TIMEOUT   30               yes        Timeout for the Telnet probe
  USERNAME  no               no        The username to authenticate as

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

Dopo aver controllato le opzioni eseguibili, settiamo RHOSTS a l'ip di metasploitable e di nuovo mostrare le opzioni eseguibili.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  no               no        The password for the specified username
  RHOSTS    192.168.1.40    yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit
             /basics/using-metasploit.html
  RPORT     23               yes        The target port (TCP)
  THREADS   1                 yes        The number of concurrent threads (max one per host)
  TIMEOUT   30               yes        Timeout for the Telnet probe
  USERNAME  no               no        The username to authenticate as

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

Usando il comando exploit come in foto msfconsole ci dà l'username e la password di metasploitable per accedere.

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Dopo aver trovato l'username e password usiamo il comando (telnet) per accedere a metasploitable come in foto.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Mar 5 08:31:17 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Per controllare che è tutto andato bene basta fare (ifconfig) se ci restituisce l'ip di metasploitable come in foto allora è tutto giusto.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a6:72:76
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea6:7276/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:74 errors:0 dropped:0 overruns:0 frame:0
          TX packets:261 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5480 (5.3 KB)  TX bytes:21200 (20.7 KB)
          Base address:0xd020  Memory:f0200000-f0220000
```