

ANALISI E ACCESSO TRAMITE TELNET SU METASPLOITABLE

Prima di procedere con l'analisi, ho verificato che le due macchine fossero **correttamente connesse** alla stessa rete eseguendo un **ping** da Kali Linux verso Metasploitable:

```
ping 192.168.50.149
```

```
(kali@vbox)-[~]
$ ping 192.168.50.149
PING 192.168.50.149 (192.168.50.149) 56(84) bytes of data.
64 bytes from 192.168.50.149: icmp_seq=1 ttl=64 time=1.91 ms
64 bytes from 192.168.50.149: icmp_seq=2 ttl=64 time=3.05 ms
64 bytes from 192.168.50.149: icmp_seq=3 ttl=64 time=1.38 ms
64 bytes from 192.168.50.149: icmp_seq=4 ttl=64 time=6.26 ms
64 bytes from 192.168.50.149: icmp_seq=5 ttl=64 time=24.6 ms
^C
--- 192.168.50.149 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.383/7.445/24.628/8.756 ms
```

Dalla macchina Kali Linux, ho avviato il **Metasploit Framework** per eseguire la scansione di Telnet:

```
msfconsole
```

Dopo aver avviato **Metasploit**, ho utilizzato il modulo di **scansione della versione Telnet** per ottenere informazioni sul servizio in esecuzione su Metasploitable.

```
use auxiliary/scanner/telnet/telnet_version
```

Ho visualizzato le opzioni del modulo:

```
show options
```

```
= [ metasploit v6.4.50-dev ]
+ -- [ 2496 exploits - 1283 auxiliary - 431 post ]
+ -- [ 1610 payloads - 49 encoders - 13 nops ]
+ -- [ 9 evasion ]

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

use auxiliary/scanner/telnet/telnet_version

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 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
```

Ho impostato dell'IP **target** (Metasploitable):

```
set RHOSTS 192.168.50.149
```

run

```
telnet 192.168.50.149
```

- **Username:** msfadmin
- **Password:** msfadmin

```
msf6 auxiliary(scanner/telnet/telnet_login) > telnet 192.168.50.149
[*] exec: telnet 192.168.50.149

Trying 192.168.50.149 ...
Connected to 192.168.50.149.
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 11 09:08:35 EDT 2025 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:~$
```