

## Pratica S7/L2

Introduzione: l'obiettivo di questo esercizio era eseguire un penetration testing svolto a testare la sicurezza del servizio Telnet su una macchina virtuale Metasploitable2 e di mostrare la capacità di un attaccante di raccogliere informazioni critiche e ottenere un accesso non autorizzato sfruttando le configurazioni deboli.

### Configurazione del laboratorio:

- Kali Linux IP: 192.168.1.150 (macchina attaccante)
- Metasploitable2 IP: 192.168.1.149 (macchina bersaglio)

### Fase di attacco

Il primo passo è stato verificare la connettività tra le due macchine e eseguire una scansione nmap sulla porta 23.

```
(kali@kali)-[~]
$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data:
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.942 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.451 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.472 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.428 ms
^C
--- 192.168.1.40 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3029ms
rtt min/avg/max/mdev = 0.428/0.573/0.942/0.213 ms

(kali@kali)-[~]
$ nmap -p 23 -sV 192.168.1.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 08:32 EDT
Nmap scan report for 192.168.1.40
Host is up (0.00039s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
MAC Address: 08:00:27:34:20:AC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

La fase di attacco è iniziata avviando la console di Metasploit per utilizzare il modulo “auxiliary/scanner/telnet/telnet\_version”, ovvero un modulo progettato per scansionare e raccogliere informazioni dai servizi Telnet.

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: View a module's description using info, or the module's
version in your browser with info -d

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

https://metasploit.com

+ --=[ metasploit v6.4.69-dev ]
+ --=[ 2529 exploits - 1302 auxiliary - 432 post ]
+ --=[ 1672 payloads - 49 encoders - 13 nops ]
+ --=[ 9 evasion ]

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

```
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 configurato l'indirizzo IP del bersaglio con il comando “set RHOST”, il modulo è stato eseguito. La scansione ha avuto successo, rilevando le credenziali predefinite del servizio Telnet che erano state lasciate senza modifiche sulla macchina Metasploitable2.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.1.40
RHOST => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > run
[*] 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) > exit

(kali@kali)-[~]
$ telnet 192.168.1.40
Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is '^]'.

metasploitable2

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 Aug 26 08:29:30 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:~$
```

**Conclusioni:** l'esercizio ha dimostrato che un servizio Telnet configurato in modo debole rappresenta un grave rischio per la sicurezza. L'uso di credenziali predefinite e la mancanza di crittografia (Telnet invia i dati in chiaro) rendono il servizio un obiettivo facile per gli attaccanti.

Raccomandazioni:

- **Disattivare i servizi non necessari:** Se il servizio Telnet non fosse essenziale, dovrebbe essere disattivato per ridurre la superficie d'attacco.
- **Utilizzare protocolli sicuri:** Sostituire Telnet con alternative crittografate come SSH (Secure Shell), che cifra i dati di autenticazione e la sessione.
- **Gestione delle credenziali:** Modificare sempre le credenziali predefinite su qualsiasi servizio installato e utilizzare password complesse.
- **Principio del privilegio minimo:** Assicurarsi che i servizi di rete siano eseguiti con il minor numero di privilegi possibile.