

CS0424IT — ESERCITAZIONE S7L2  
EXPLOIT VULNERABILITÀ TELNET CON METASPLOIT

*Simone La Porta*



---

TRACCIA

Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo `auxiliary_telnet_version` sulla macchina Metasploitable.

Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40.

---

## SERVIZIO TELNET

Telnet è un protocollo di rete utilizzato per fornire una comunicazione bidirezionale, orientata al testo, tra due macchine attraverso una rete IP. Storicamente è stato uno dei primi protocolli utilizzati per accedere remotamente ai sistemi, ma la mancanza di crittografia rende Telnet insicuro rispetto agli standard attuali e presenta oggi gravi problemi di sicurezza, principalmente perché trasmette i dati, incluse le credenziali di login, in chiaro senza cifratura.

### *Descrizione della vulnerabilità*

La vulnerabilità sfruttata in questo esercizio è la possibilità di ottenere informazioni di banner e credenziali di accesso tramite il modulo `auxiliary/scanner/telnet/telnet_version` di Metasploit. Questa vulnerabilità permette a un attaccante di ottenere accesso non autorizzato al sistema remoto se il servizio Telnet è configurato con credenziali di default o deboli.

## METASPLOIT

Metasploit è una piattaforma utilizzata per sviluppare, testare e utilizzare exploit su vulnerabilità conosciute in vari software e sistemi. Metasploit contiene codice di exploit e payload ed altre funzionalità contenute nei suoi moduli. Ogni modulo mette a disposizione un vettore di attacco diverso. È possibile cercare un determinato modulo utilizzando il comando `search`; in questo caso si cerca il modulo `vsftpd` che sfrutta una vulnerabilità nota nel server FTP.

### *Exploit*

Un exploit è un pezzo di software, un frammento di dati o una sequenza di comandi che sfrutta una vulnerabilità in un sistema informatico per causare un comportamento imprevisto o non desiderato. Nel contesto di Metasploit, un exploit è utilizzato per prendere il controllo di una macchina vulnerabile.

Le principali caratteristiche di un exploit includono:

- **Identificazione della vulnerabilità:** gli exploit sono progettati per sfruttare specifiche vulnerabilità nei software o nei sistemi.
- **Esecuzione di comandi:** permettono l'esecuzione di comandi non autorizzati sul sistema target.

- 
- **Accesso non autorizzato:** possono fornire accesso non autorizzato a dati o funzionalità del sistema target.

### *Payload*

Un payload è il codice che viene eseguito sul sistema target una volta che l'exploit ha avuto successo. Il payload può avere vari obiettivi, come aprire una shell di comando, creare una backdoor o raccogliere informazioni sensibili.

Le principali caratteristiche di un payload includono:

- **Tipo di attività:** i payload possono eseguire una varietà di attività, come l'apertura di una shell, il download di file o la raccolta di informazioni.
- **Compatibilità:** devono essere compatibili con l'exploit utilizzato per penetrare nel sistema target.
- **Obiettivo specifico:** sono progettati per raggiungere specifici obiettivi post-exploit.

### *La vulnerabilità Telnet*

La vulnerabilità sfruttata nell'esercizio riguarda la configurazione di Telnet su Metasploitable, che permette di ottenere accesso non autorizzato utilizzando credenziali di default deboli. Questa è una comune vulnerabilità presente in sistemi legacy o mal configurati.

Il sistema Metasploitable viene distribuito con credenziali di default che sono ben conosciute:

- Username: msfadmin
- Password: msfadmin

Queste credenziali non sono modificate, permettendo a un attaccante di ottenere facilmente l'accesso al sistema.

Il modulo `auxiliary/scanner/telnet/telnet_version` di Metasploit viene utilizzato per rilevare e interagire con il servizio Telnet. Se l'ausiliare ha successo, si ottengono le credenziali di login del servizio Telnet.

La vulnerabilità sfruttata risiede nella configurazione predefinita del servizio Telnet, che accetta credenziali di default senza richiedere ulteriori misure di sicurezza. Telnet, essendo un

---

protocollo non criptato, trasmette le credenziali in chiaro, rendendo facile per un attaccante intercettare e utilizzare queste credenziali, utilizzando ad esempio strumenti di sniffing come Wireshark. Inoltre, l'uso di credenziali di default è una pratica insicura che espone il sistema a rischi significativi.

Le credenziali di default sono un target facile per gli attaccanti. Molti amministratori non modificano queste credenziali dopo l'installazione del sistema, rendendo possibile l'accesso non autorizzato semplicemente conoscendo le credenziali di default comuni.

### Implicazioni di sicurezza

Questa vulnerabilità è critica poiché permette accesso non autorizzato alla macchina. Una volta ottenuto l'accesso, un attaccante può eseguire una varietà di operazioni malevole, come:

- Modificare o cancellare file.
- Installare malware.
- Accedere ad altre risorse della rete.
- Compromettere ulteriormente il sistema.

Per mitigare questa vulnerabilità, è fondamentale disabilitare Telnet e utilizzare protocolli sicuri come SSH. Inoltre, si consiglia di seguire le migliori pratiche di sicurezza, come:

- Modificare le credenziali di default.
- Utilizzare firewall per limitare l'accesso alle porte sensibili.
- Monitorare i log di sistema per rilevare tentativi di accesso non autorizzato.
- Implementare misure di rilevamento delle intrusioni.

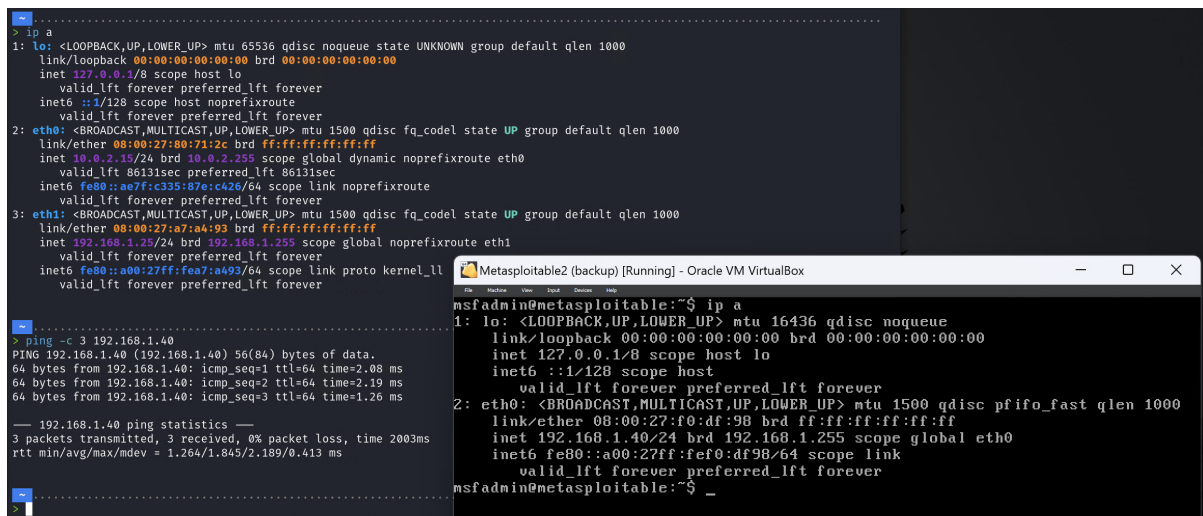
La vulnerabilità presente nel servizio Telnet su Metasploitable rappresenta un serio rischio per la sicurezza delle macchine che eseguono questo servizio con credenziali di default. È essenziale essere consapevoli delle minacce e mantenere aggiornati i propri sistemi per prevenire exploit simili.

## SVOLGIMENTO

### Configurazione degli rete

Come prima cosa, sono stati configurati gli indirizzi IP di Kali Linux e Metasploitable:

- Kali Linux: 192.168.1.25
- Metasploitable: 192.168.1.40



The image shows two terminal windows. The left window is a Kali Linux terminal where the user runs 'ip a' to show network interface details for 'lo', 'eth0', and 'eth1'. It then runs 'ping -c 3 192.168.1.40' to verify connectivity to the Metasploitable machine. The right window is a Metasploitable2 (backup) terminal running in Oracle VM VirtualBox. It shows the user running 'ip a' to display the configuration for 'lo', 'eth0', and 'eth1'.

```
> ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:00:21:12c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 86131sec preferred_lft 86131sec
    inet6 fe80::ae7f:c335:87e:c426/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a7:a4:93 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe07:a493/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

> ping -c 3 192.168.1.40
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=2.08 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=2.19 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=1.26 ms

--- 192.168.1.40 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.264/1.845/2.189/0.413 ms

>
```

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:f0:df:98 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe07:df98/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Figura 1: Configurazione degli indirizzi IP

La configurazione è stata verificata tramite il comando ping.

### Avvio di Metasploit e ricerca/configurazione del modulo

Dopo aver avviato la console di Metasploit con il comando `msfconsole`, è stato cercato il modulo `auxiliary/telnet/version` con il comando `search telnet`.

Il comando `search telnet` ha restituito due moduli: `auxiliary/scanner/telnet/lantronix_telnet_version` e `auxiliary/scanner/telnet/telnet_version`. È stato scelto il secondo modulo. Individuato il modulo corretto, è stato utilizzato con il comando `use auxiliary/scanner/telnet/telnet_version`. Successivamente, sono state controllate le opzioni necessarie con il comando `show options`, notando che era necessario impostare `RHOSTS` con l'indirizzo target dove è in esecuzione il servizio Telnet.

È stata impostata l'opzione `RHOSTS` con l'indirizzo IP della macchina Metasploitable utilizzando il comando `set RHOSTS 192.168.1.40`.

```
> msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

[ ASCII art of a duck ]

= [ metasploit v6.4.15-dev ]
+ -- --[ 2433 exploits - 1251 auxiliary - 428 post ]
+ -- --[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

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

msf6 > search telnet_version

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/telnet/lantronix_telnet_version . normal No Lantronix Telnet Service Banner Detection
1 auxiliary/scanner/telnet/telnet_version . normal No Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version

msf6 > use 1
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
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.
```

Figura 2: Ricerca e configurazione del modulo Telnet Version

### *Esecuzione dell'attacco*

Non essendo necessario specificare un payload per questo modulo, l'attacco è stato eseguito con il comando `exploit`. Il modulo ha recuperato i dati di login del servizio Telnet, mostrando che le credenziali da utilizzare erano username: `msfadmin` e password: `msfadmin`.

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

Figura 3: Esecuzione dell'attacco

```
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: Sun Jul 7 12:04:20 EDT 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:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```

Figura 4: Verifica delle credenziali Telnet

---

### *Verifica delle credenziali e accesso alla macchina target*

È stata verificata la correttezza delle informazioni eseguendo il comando `telnet` seguito dall'IP della macchina Metasploitable. Una volta connessi, sono state inserite le credenziali ottenute (`msfadmin/msfadmin`), confermando che l'attacco ha avuto successo e che la vulnerabilità del servizio Telnet è stata sfruttata correttamente.

Per verificare ulteriormente l'effettività dell'attacco, sono stati eseguiti i comandi `uname -a` e `whoami` per assicurarsi di essere nella macchina target.

Di seguito, i comandi eseguiti e i risultati ottenuti:

- `uname -a`: visualizza informazioni sul kernel e sul sistema operativo
- `whoami`: visualizza l'utente attualmente loggato