

Task 17/12/24: Exploit Telnet con Metasploit

Traccia

Argomento:

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.

Obiettivo dell'Esercizio:

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**

Istruzioni:

No specifiche!

Task 17/12/24: Exploit Telnet con Metasploit

Report

Introduzione:

Questo report documenta l'analisi del servizio **Telnet** eseguita utilizzando Metasploit. L'obiettivo è stato sfruttare il modulo **auxiliary/scanner/telnet/telnet_version** per ottenere informazioni relative alla versione del servizio in esecuzione sulla macchina **Metasploitable**.

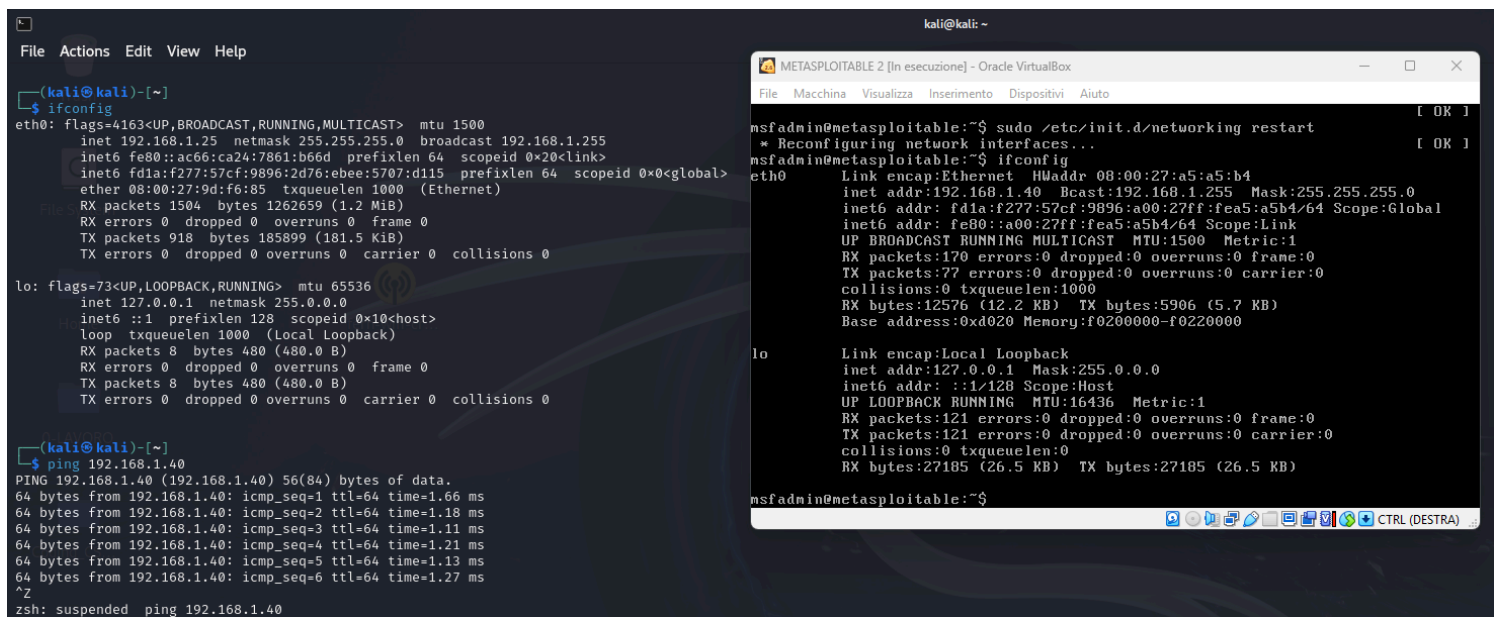
Le attività sono state eseguite da una macchina **Kali Linux** con indirizzo **IP 192.168.1.25**, mentre il target è la macchina **Metasploitable** configurata con indirizzo **IP 192.168.1.40**.

Configurazione della rete e test di connettività :

Come richiesto, ho impostato l'IP della macchina **Kali Linux** su **192.168.1.25**, l'IP della macchina **Metasploitable** su **192.168.1.40**, testando poi il funzionamento con un **ping**.

Comandi utilizzati: **ping 192.168.1.40**

Risultato: La macchina ha risposto al ping.



```
(kali@kali)~$ ifconfig
eth0: 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::ac66:ca24:7861:b66d prefixlen 64 scopeid 0<link>
    inet6 fd1a:f277:57cf:9896:2d76:ebec:5707:d115 prefixlen 64 scopeid 0<global>
    ether 08:00:27:9d:f6:85 txqueuelen 1000 (Ethernet)
    RX packets 1504 bytes 1262659 (1.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 918 bytes 185899 (181.5 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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(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=1.66 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=1.18 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=1.11 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=1.21 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=1.13 ms
64 bytes from 192.168.1.40: icmp_seq=6 ttl=64 time=1.27 ms
^Z
zsh: suspended ping 192.168.1.40

msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces...
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a5:a5:b4
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fd1a:f277:57cf:9896:a00:27ff:fea5:a5b4/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fea5:a5b4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:170 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12576 (12.2 KB)  TX bytes:5906 (5.7 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:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27185 (26.5 KB)  TX bytes:27185 (26.5 KB)

msfadmin@metasploitable:~$
```

Avvio di Metasploit:

Ho avviato **Metasploit**.

Comandi utilizzati: **msfconsole**

Risultato: Il servizio risulta avviato.

```
(kali㉿kali)-[~]
$ msfconsole

Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

      .
    .-'.
   /   \
  /     \
 /       \
/         \
(   _   _   )
(  _ 0 0 _  )
 \  o_o  /
  \     /
   \   /
    \ /
     *

      M S F
      WW
      |||
      |||

Home          fern-wifi-cr...

=[ metasploit v6.4.38-dev ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

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

msf6 > 
```

Ricerca e setup del modulo di exploit:

Ho selezionato e configurato il modulo relativo a **Telnet**.

Comandi utilizzati: **search auxiliary telnet** , **use 14** , **options** e **set RHOSTS 192.168.1.40**

Risultato: Il modulo è stato scelto e configurato correttamente con l'IP della macchina target.

```
msf6 > search auxiliary telnet

Matching Modules
=====
#    Name                                          Disclosure Date  Rank  Check  Description
-    -
0    auxiliary/server/capture/telnet              .               normal No    Authentication Capture: Telnet
1    auxiliary/scanner/telnet/brocade_enable_login .               normal No    Brocade Enable Login Check Scanner
2    auxiliary/dos/cisco/ios_telnet_rocm          2017-03-17      normal No    Cisco IOS Telnet Denial of Service
3    auxiliary/admin/http/dlink_dir_300_600_exec_noauth 2013-02-04      normal No    D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
4    auxiliary/scanner/ssh/juniper_backdoor        2015-12-20      normal No    Juniper SSH Backdoor Scanner
5    auxiliary/scanner/telnet/lantronix_telnet_password .               normal No    Lantronix Telnet Password Recovery
6    auxiliary/scanner/telnet/lantronix_telnet_version .               normal No    Lantronix Telnet Service Banner Detection
7    auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof 2010-12-21      normal No    Microsoft IIS FTP Server Encoded Response Overflow Trigger
8    auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass 2021-09-06      normal Yes   Netgear PNPX_GetShareFolderList Authentication Bypass
9    auxiliary/admin/http/netgear_r6700_pass_reset 2020-06-15      normal Yes   Netgear R6700v3 Unauthenticated LAN Admin Password Reset
10   auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce 2021-04-21      normal Yes   Netgear R7000 backup.cgi Heap Overflow RCE
11   auxiliary/scanner/telnet/telnet_ruggedcom      .               normal No    RuggedCom Telnet Password Generator
12   auxiliary/scanner/telnet/satel_cmd_exec        2017-04-07      normal No    Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
13   auxiliary/scanner/telnet/telnet_login          .               normal No    Telnet Login Check Scanner
14   auxiliary/scanner/telnet/telnet_version        .               normal No    Telnet Service Banner Detection
15   auxiliary/scanner/telnet/telnet_encrypt_overflow .               normal No    Telnet Service Encryption Key ID Overflow Detection

Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/telnet/telnet_encrypt_overflow

msf6 > use 14
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) > options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  192.168.1.40     yes       The password for the specified username
  RHOSTS    23               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.

```

Esecuzione dell'exploit:

L'exploit è stato eseguito con successo, ottenendo le credenziali in chiaro della macchina target.

Comandi utilizzati: `exploit`

Risultato: sono state ottenute le credenziali in chiaro della macchina Metasploitable.

```

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

```