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

Metasploit utilizza due tipologie di moduli:

- **Moduli normali**:
  - eseguono attacchi diretti per sfruttare falle di sicurezza note;
  - eseguono attacchi diretti per sfruttare l'accesso al sistema;
  - eseguono azioni post-attacco per il mantenimento dell'accesso al sistema;
  - Utilizzano i payload.
- **Moduli ausiliari** (Auxiliary Modules):
  - Progettati per svolgere supporto durante il test della sicurezza (scansione della rete, Information Gathering etc.);
  - Non effettuano attacchi diretti, ma forniscono informazioni aggiuntive utili per ottenere il quadro completo della sicurezza della rete o del sistema;
  - Non utilizzano, quasi mai, i payload.

Esercizio:

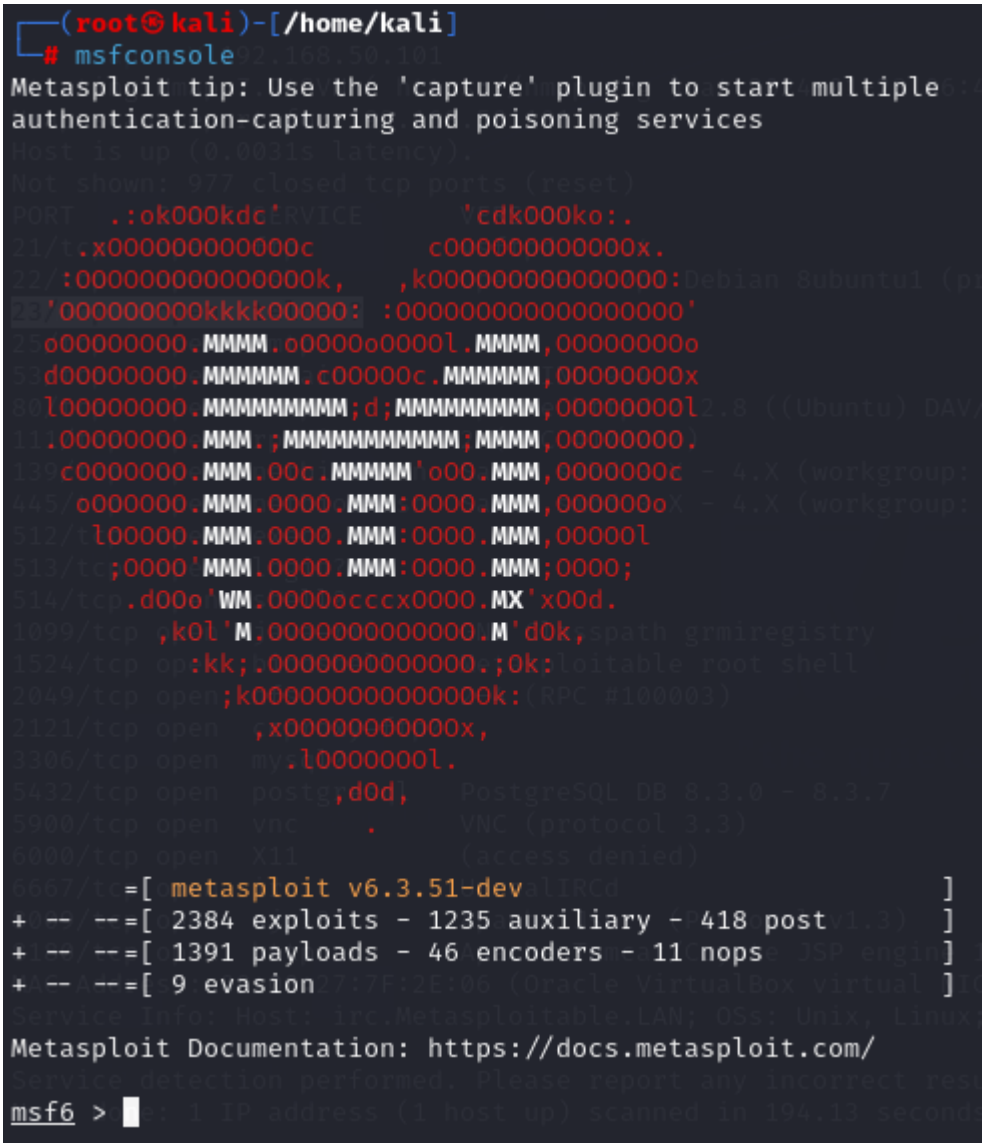
Kali Linux IP **192.168.50.100** (Macchina attaccante)
Metasploitable 2 IP **192.168.50.101** (Macchina vittima)

Eseguito il comando «**nmap –sV 192.168.50.101**» per scansionare il target e raccogliere le informazioni sulle porte aperte, i servizi collegati e le relative versioni.

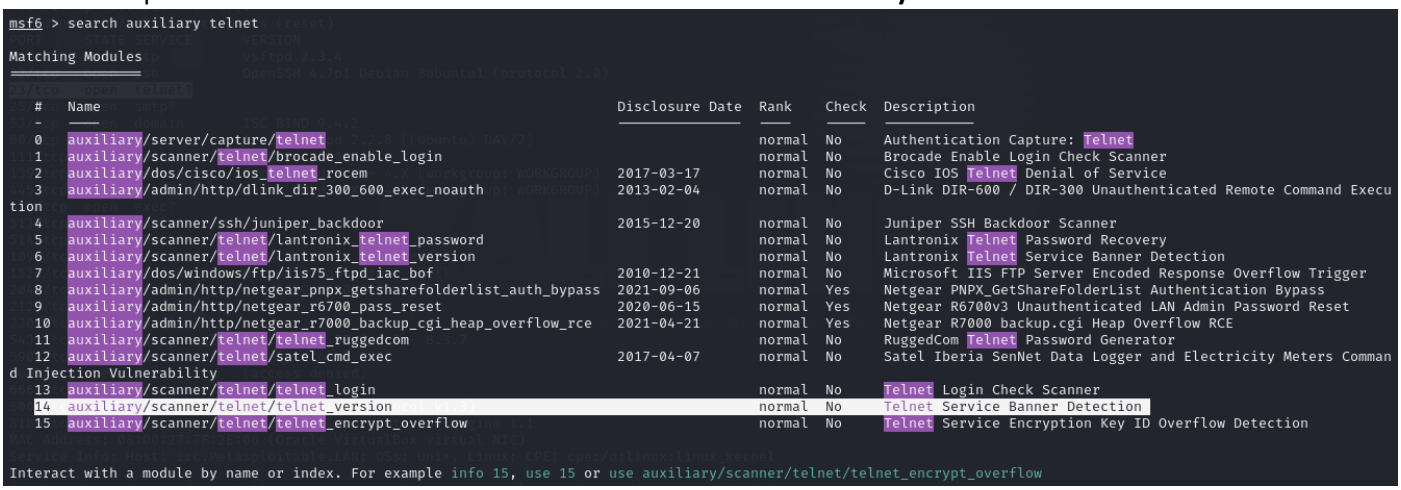
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 06:47 EST
Nmap scan report for 192.168.50.101
Host is up (0.0031s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7F:2E:06 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, 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 194.13 seconds
```

Avvviato Metasploit con il comando «**msfconsole**»



Cercato l'exploit del servizio telnet nei moduli ausiliari con «**search auxiliary telnet**»



Identificato l'exploit usarlo con «**use 14**» o, al posto del numero, il suo percorso.

```
msf6 > use 14
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 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        The username to authenticate as

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

Controllare con «**show options**» le opzioni che possono essere configurate.

Configurare rhosts (remote host) con il comando «**set rhosts 192.168.50.101**» e ricontrollare se il settaggio è andato a buon fine digitando di nuovo «**show options**»

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
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    192.168.50.101   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        The username to authenticate as

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

Lanciare l'exploit con «**exploit**»

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.50.101:23     - 192.168.50.101:23 TELNET _ _ _ _ ___ \x0a _ __ ___ ___| |_ __ _ ___ _ __ | | ___ (_) |_ __
_| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _ \ | '_ \| |/ _ \ __) |\x0a| | | | | __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |
__// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|.__/|_|\___|____/|\x0a                    |_|                                    \x0
a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0
ametasploitable login:
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Notiamo che l'exploit lanciato sul servizio telnet è andato a buon fine riuscendo a trovare la Username e Password della macchina. (Vedi figura).

Opzionale:

Configurate l'IP della vostra Kali con **192.168.1.25** e l'IP della vostra Metasploitable con **192.168.1.40**

Controllato che le due macchina comunicassero con il comando «ping»

```
┌──(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=0.759 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.449 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.411 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.493 ms
^C
── 192.168.1.40 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.411/0.528/0.759/0.136 ms
```

Eseguita una scansione con nmap

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 07:27 EST
Nmap scan report for 192.168.1.40
Host is up (0.00083s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7F:2E:06 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, 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 194.00 seconds
```

Dopo aver avviato Metasploit, cercato il modulo ausiliare del servizio telnet ed utilizzato, configuriamo il rhosts con l’indirizzo IP 192.168.1.40 e lanciamo l’exploit.

```
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 _                  _     _ _       _        _             ____    \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _|
 |__ | | ____|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __
// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                    |_|                                  \x0a\
x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0am
etasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```