**Claudio De cicco**
**6/12/2022**

# Msfconsole telnet_version

In questo esercizio andremo ad attaccare la vulnerabilità relativa a Telnet. Per prima cosa vado a cambiare gli ip delle macchine come richiesto.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f0:63:36
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef0:6336/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:52 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4004 (3.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

```
┌──(kali㉿kali)-[~]
└─$ 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
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 177  bytes 22656 (22.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 217  bytes 136408 (133.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

A questo punto avvio **msfconsole** e vado a ricercare il modulo **telnet_version** e lo vado ad aggiungere con “use 1”

```
msf6 > search auxiliary telnet_version

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

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version                      normal  No     Lantronix Telnet Se
rvice Banner Detection
   1  auxiliary/scanner/telnet/telnet_version                                normal  No     Telnet Service Bann
er Detection


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_ve
rsion
```

Con info -d vado a vedere tutte le info complete del modulo, mi verra aperta una paggina nel browser con tutte le info.

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

msf6 auxiliary(scanner/telnet/telnet_version) > info -d
[*] Generating documentation for telnet_version, then opening /tmp/telnet_version_doc20221206-13085-n7h200.h
tml in a browser...
msf6 auxiliary(scanner/telnet/telnet_version) > Missing chrome or resource URL: resource://gre/modules/Updat
eListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs
```

## Description

This module will scan a range of machines and prints the banner, usually containing the version of any telnet servers that are running on it.

## Verification Steps

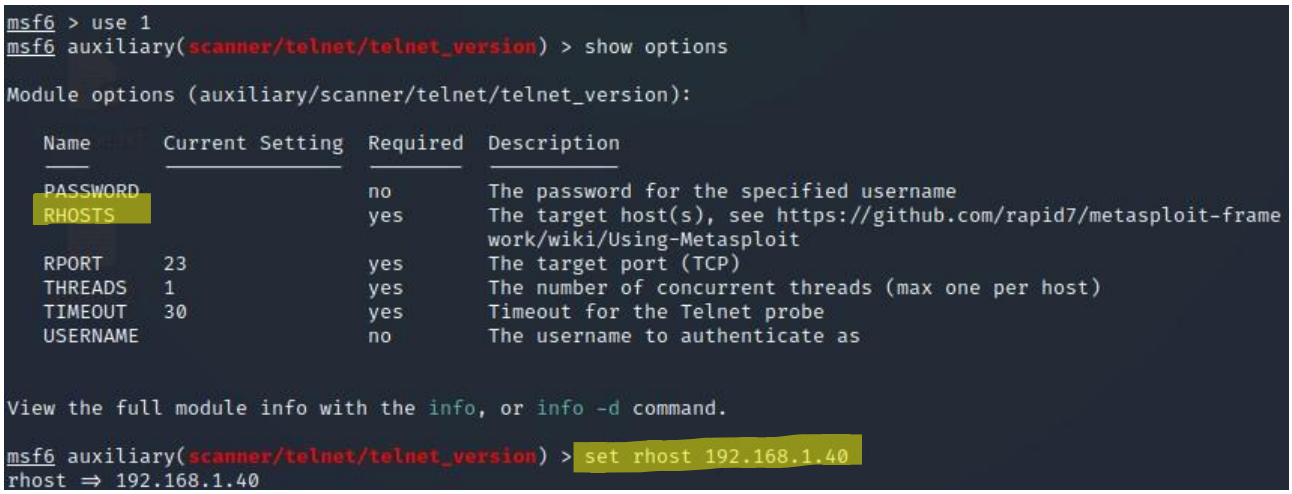
1. Do: `use auxiliary/scanner/telnet/telnet_version`
2. Do: `set RHOSTS [IP]`
3. Do: `set THREADS [number of threads]`
4. Do: `run`

## Scenarios

```
msf > use auxiliary/scanner/telnet/telnet_version
msf auxiliary(scanner/telnet/telnet_version) > set RHOSTS 1.1.1.0/24
RHOSTS => 1.1.1.0/24
msf auxiliary(scanner/telnet/telnet_version) > set THREADS 254
THREADS => 254
msf auxiliary(scanner/telnet/telnet_version) > run

[*] 1.1.1.2:23 TELNET (GSM7224) \x0aUser:
[*] 1.1.1.56:23 TELNET Ubuntu 8.04\x0ametasploitable login:
[*] 1.1.1.116:23 TELNET Welcome to GoodTech Systems Telnet Server for Windows NT/2000/XP
(Evaluation Copy)\x0a\x0a(C) Copyright 1996-2002 GoodTech Systems, Inc.\x0a\x0a\x0aLogin
username:
[*] Scanned 254 of 256 hosts (099% complete)
[*] Scanned 255 of 256 hosts (099% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_version) >
```

Con show options vado a vedere le opzioni del modulo, quini vado ad inserire l'ip di meta nella sezione RHOST.




Nelle opzioni del modulo non è presente la sezione del payload quindi vado a fare una ricerca dei payloads e ne scelgo uno. Come avevo immaginato non essendoci una sezione payloads, in questo modulo non possono essere inseriti payload.


Dopo aver settato tutto faccio partire l'exploit ricevendo come risultato le credenziali di login di metasploitable.