1 2 3 4

10:19

kali@kali: ~

File Actions Edit View Help

```
   33  exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection  2015-12-20       excellent  No     TP-Link SC2020n Authenticated Telnet Injection
   34  auxiliary/scanner/telnet/telnet_login                                               normal     No     Telnet Login Check Scanner
   35  auxiliary/scanner/telnet/telnet_version                                             normal     No     Telnet Service Banner Detection
   36  auxiliary/scanner/telnet/telnet_encrypt_overflow                                    normal     No     Telnet Service Encryption Key ID Overflow Detection
   37  payload/cmd/unix/bind_busybox_telnetd                                               normal     No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   38  payload/cmd/unix/reverse                                                            normal     No     Unix Command Shell, Double Reverse TCP (telnet)
   39  payload/cmd/unix/reverse_ssl_double_telnet                                          normal     No     Unix Command Shell, Double Reverse TCP SSL (telnet)
   40  payload/cmd/unix/reverse_bash_telnet_ssl                                            normal     No     Unix Command Shell, Reverse TCP SSL (telnet)
   41  exploit/linux/ssh/vyos_restricted_shell_privesc                    2018-11-05       great      Yes    VyOS restricted-shell Escape and Privilege Escalation
   42  post/windows/gather/credentials/mremote                                             normal     No     Windows Gather mRemote Saved Password Extraction


Interact with a module by name or index. For example info 42, use 42 or use post/windows/gather/credentials/mremote

msf6 > search telnet_version

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

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

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 https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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
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\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

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: Tue Mar  7 11:12:26 EST 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:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:49:56:27
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe49:5627/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:52 errors:0 dropped:0 overruns:0 frame:0
          TX packets:176 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3816 (3.7 KB)  TX bytes:16747 (16.3 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:150 errors:0 dropped:0 overruns:0 frame:0
          TX packets:150 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```