

EPICODE

CYBERSECURITY COURSE

BY MAX ALDROVANDI

17/05/2024

Web-site: <https://epicode.com/it>

Locality:

Via dei Magazzini Generali,
6 Roma, Lazio 00154, IT

PRACTICE EXERCISE S7/L2

Track:

Based on the exercise seen in theory class, use Metasploit to exploit the Telnet-related vulnerability with the auxiliary telnet_version module on the Metasploitable machine.

Requisite: Follow the steps seen in the theory lesson.

First, configure the ip of your **Kali** with **192.168.1.25** and the ip of your **Metasploitable** with **192.168.1.40**.

Change IP addresses:

As first we changed the IP addresses of Kali and Metasploitable.

```
GNU nano 2.0.7      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1

[ Read 15 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

KALI

```
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1

[ Cancelled ]

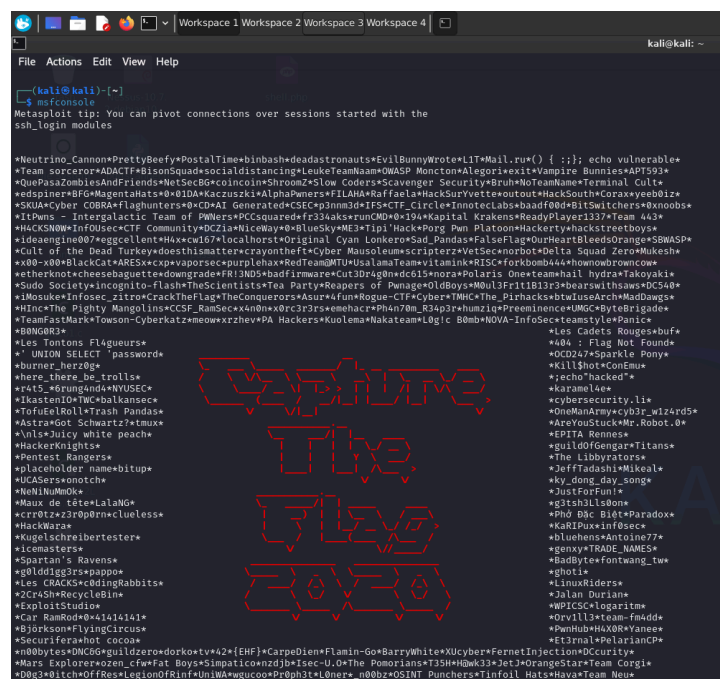
^G Get Help      ^O WriteOut      ^R Read File      ^Y Prev Page      ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is       ^V Next Page      ^U UnCut Text    ^T To Spell
```

METASPLOTABLE

MSF console:

We then proceeded by starting msf console from the terminal using the command:

msfconsole



```
kali@kali: ~
File Actions Edit View Help

(kali@kali)~$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

#Neutrino_Cannon*PrettyBeefy*PostalTime+binbash+deadastronauts*EvilBunnyWrote*LiT*Mail.ru() { ;; } echo vulnerable+
#Team sorcerer*ADACTF*BisonSquad+socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593*
#QuePasaZombiesAndFriends*NetSecB*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult+
#redspine*DFG*RegentAmes*0*JIDA*Wacouski*AlghaPwners*FLAHA*Reffaele*HackSurfVette*outout*HackSouth*Corax*yee80iz+
#SKUA*Cyber COBRA*Flaghunters*0*CD*AI Generated*CSCE*p3nm3d*TF5*CTF_Circle*Innoteclabs*baadf00d*BitSwitchers*0*noobs+
#ITPwns - Intergalactic Team of PWNers*PCCsquared*fr33k4ks*runCMD*0*194*Kapital Krakens*ReadyPlayer1337*Team 443*
#HACKSNOW*InfoSec*CTF Community*DC21a*NiceWay*0*BlueSky*ME3*Tipi*Hack*Porg Pm Platoon*Hackerty*hackstreetboys*
#idaengine07*eggcellent*H4x*c0d37*localhost*Original Cyan Lonkers*Sad_Pandas*FalseFlag*0*Heartbleed*Orange*SBWASP+
#Cult of the Dead Turkey+doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squad Zero*Mukesh+
#x00*x00*BlackCat*ARES*cxp*vaporsec*purplehax*RedTeam*MTU*UsalamaTeam*vitamink*RIS*forkbomb444*hownowbrowncow+
#etherknot*cheesebagutte*downgrade*FR1ND0*badfirmware*cut3d4g*hw*dc65*noop*Polaris One*examhall hydra*Akoyaki+
#Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*Mbui3*Fr1t1B13r3*bearswithsaws*DC540+
#iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*TMHC*The_Pirhacks*btwLuseArch*MadDaags+
#Tinc*The Pightly Mangolins*CCSF_RamSec*x4n0n*x0rc3p3rse*emehacr*Ph4n70m_R34p3r*humziq*Preeminence*UMG*ByteBrigade+
#TeamFastMark*Towson-Cyberkatzeow*arzhew*PA Hackers*Kuolema*Hakateam*Legic B0mb*NOVA-InfoSec*teamstyle*Panice+
#BANG0R3+
#Les Tontons Flagueurs+
# UNION SELECT password+
#burner_her0ge+
#where_there_be_trolls+
#r4t5_*grung4nd4*NVUSEC+
#listen10*WUChalkansce+
#TofuEleRoll*Trash Pandas+
#Astra*Got Schwartz*tmux+
#Unl*Juicy white peach+
#HackerKnights+
#Pentest Rangers+
#placeholder_name=bitup+
#UCASeas*onotch+
#NeN1nuMe0ke+
#Maux de tête*LalaNo+
#cr0r0z*23r0p0rn*clueless+
#Hack0r4r+
#Kugelschreibertester+
#icemasters+
#Spartan's Ravens+
#g0lddigg3r*pappo+
#Les CRACKS*c0dingRabbits+
#Z0c4sh*Recyclablin+
#ExploitStudio+
#Car RamRod*0*414141+
#Bjorkson*FlyingCircus+
#Securifer*ahot cocos+
#n00bytes*DMCG*guidzero*dork*ty42*[EHF]*CarpeDiem*Flamin-Go*BarryWhite*XUcyber*FernetInjection*0ccurity+
#Mars Explorer*ozen_cf*Fat Boys*Simpatico*nzdb*Isac-U.O*The Pomorians*T3SH*H0wk33*Jet3*OrangeStar*Team Corgi+
#00g3*itchhoffRes*LegionOfRIn*UnlNA*Wgucoc*Pr0ph3t*L0n0r*_n00bz*0SINT_Punchers*TInfoil_Hats*Hava*Team Neu+
```

We looked for the exploit we were interested in in this case the 'auxiliary scanner/telnet/telnet_version'

```
msf6 > search telnet/telnet_version

Matching Modules

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

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version
```

And we used it with the command:

use + 'path of the exploit'

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

with the command:

show options

We saw what the requirements were for using this exploit, and with the command:

set + RHOSTS + IP Target

we set the information that was required

```
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
-      -
PASSWORD  no              no       The password for the specified username
RHOSTS    yes            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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              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) > █
```

With the command:

run

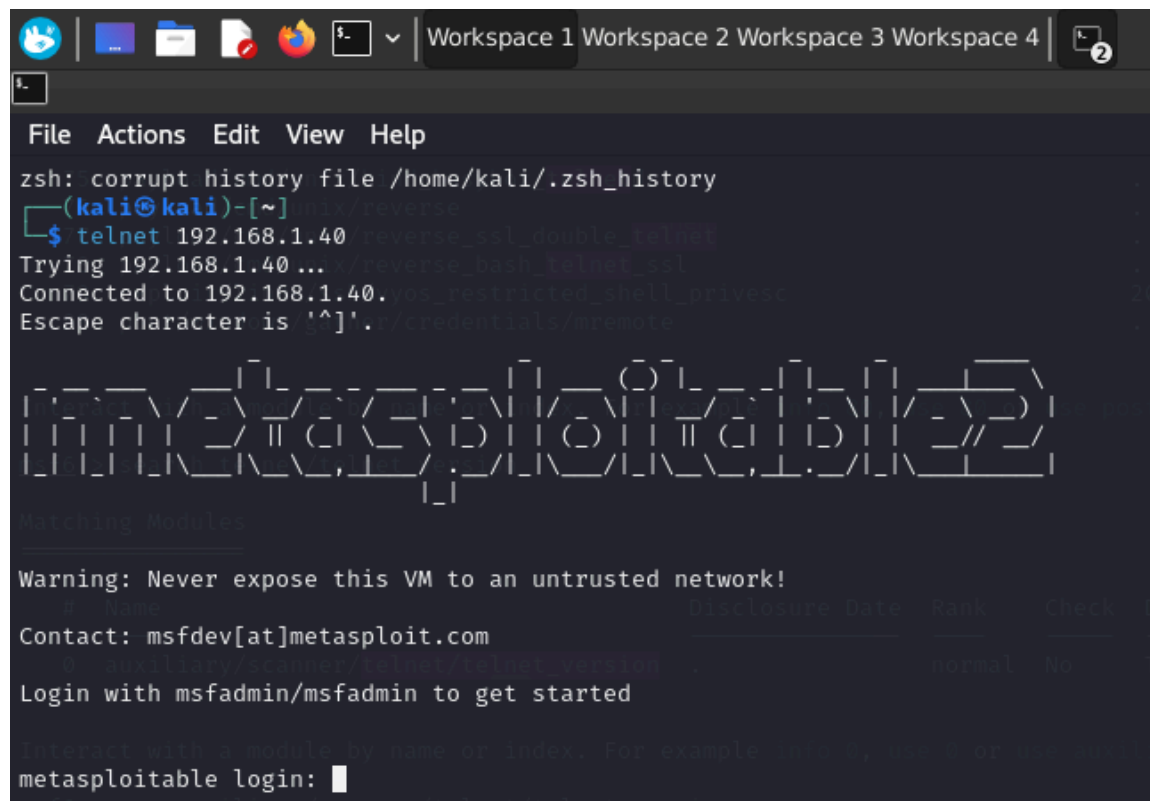
we launched the exploit

```
msf6 auxiliary(scanner/telnet/telnet_version) > run
[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
VM to an untrusted network! \x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0aWarning: Never expose this
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

With the command:

telnet + IP target machine

we verify that the credentials are correct by trying to access the service.



```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ telnet 192.168.1.40 reverse_ssl_double_telnet
Trying 192.168.1.40 ... reverse_bash_telnet_ssl
Connected to 192.168.1.40.yos_restricted_shell_privesc
Escape character is '^]'.
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
Interact with a module by name or index. For example: info, use, or use -j
metasploitable login: |
```