**Progress test 3-1**

**Helix**

**Dump Window's Physical Memory to Netcat**

**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>
* In this lab, you will learn how to make a copy the memory of a Window Server's over the network to another server running netcat.

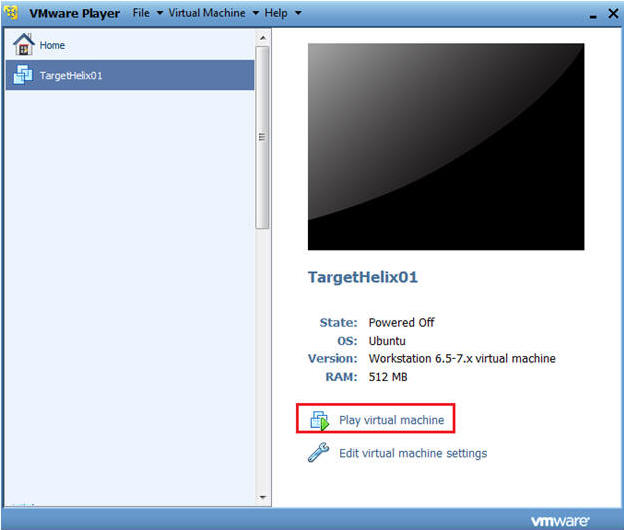
**Section 1. Pre-requisites**

Lab 1 - Helix: Getting Started

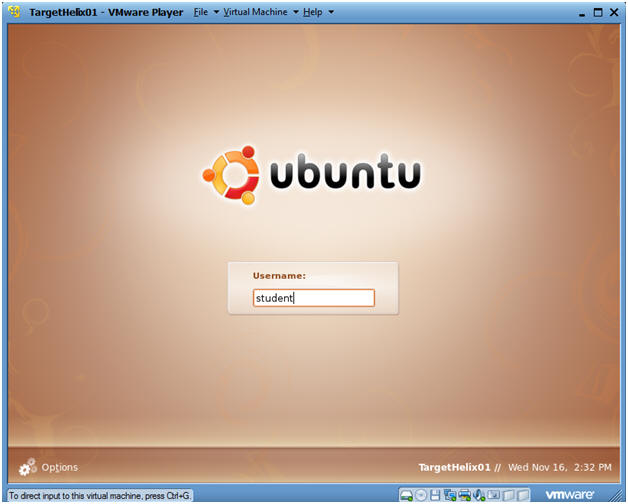
Lab 2 - Create a Helix Independent Server

**Section 2. Logging Into TargetHelix01**

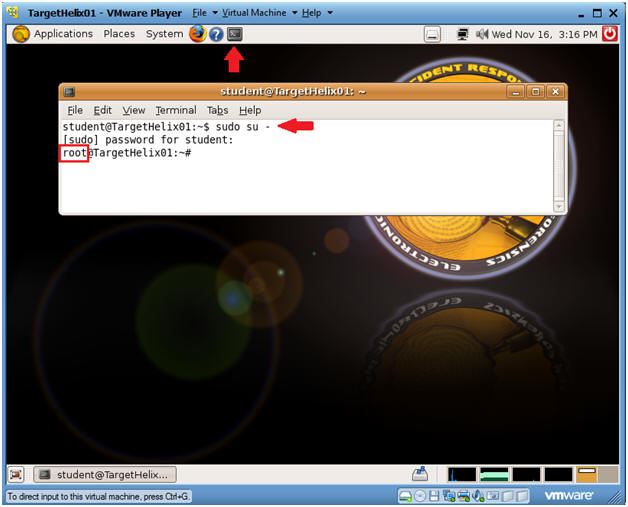
1. Booting up Helix
   * **Instructions**:
     1. Select TargetHelix01
     2. Play Virtual Machine



1. Logging into Helix
   * **Command**:
     1. Login with your the username and password you created earlier.
     2. In my case, I create a username called "student".



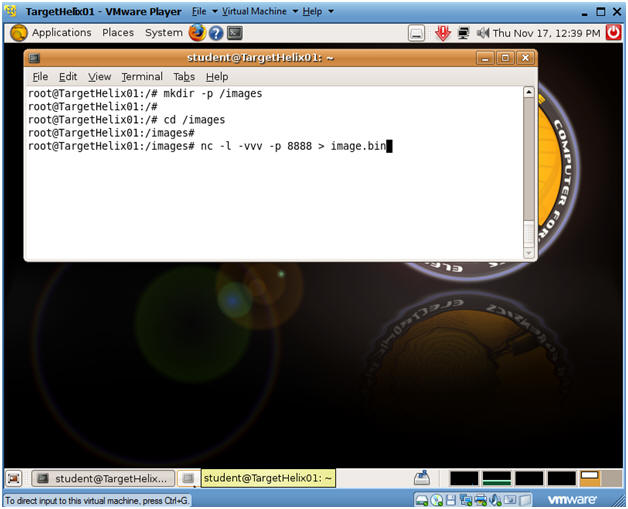
1. How to become root
   * **Command**:
     1. sudo su -
     2. Enter your current password for the account your logged in as.



1. Determine IP Address
   * **Command**:
     1. ifconfig -a
   * **Note**:
     1. In my case, my IP address is 192.168.1.116.
     2. You will use this IP address for your Netcat server.

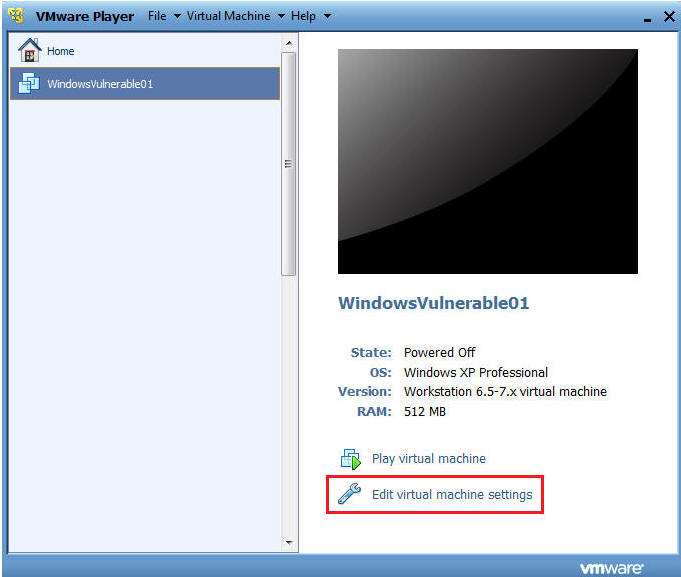


1. Setting Up Netcat
   * **Command**:
     1. mkdir -p /images
     2. cd /images
     3. nc -l -vvv -p 8888 > image.bin

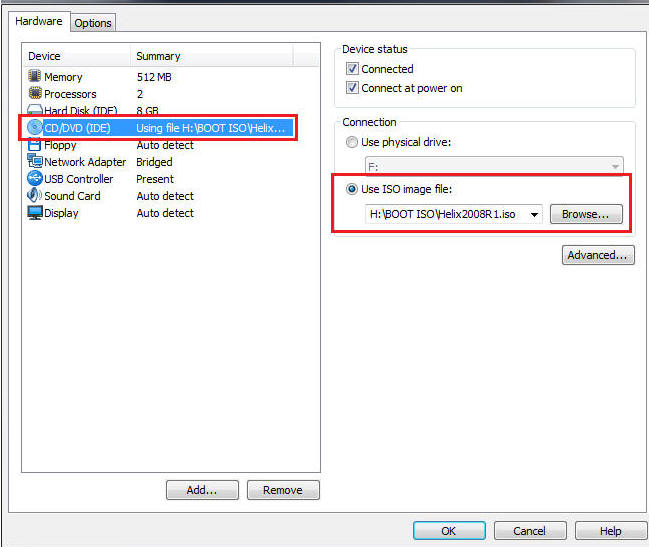


**Section 3. Logging Into TargetHelix01**

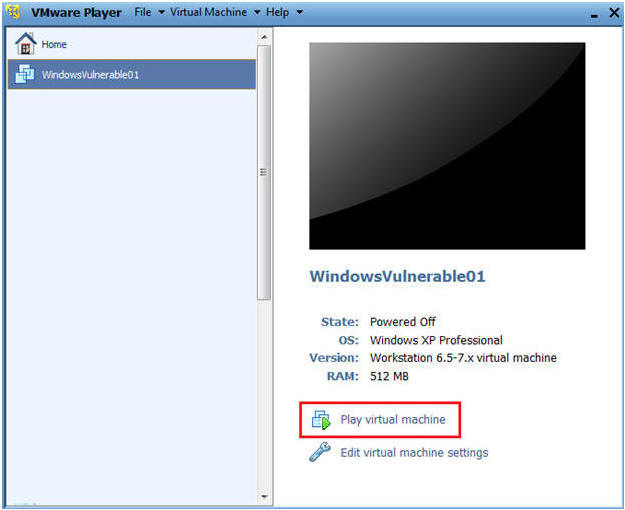
1. Edit the WindowsVulnerable01 virtual machine. (See Below)
   * **Note**: For those of you that don't have access to class material, this can be Windows XP, 2000, 2003 and 7.



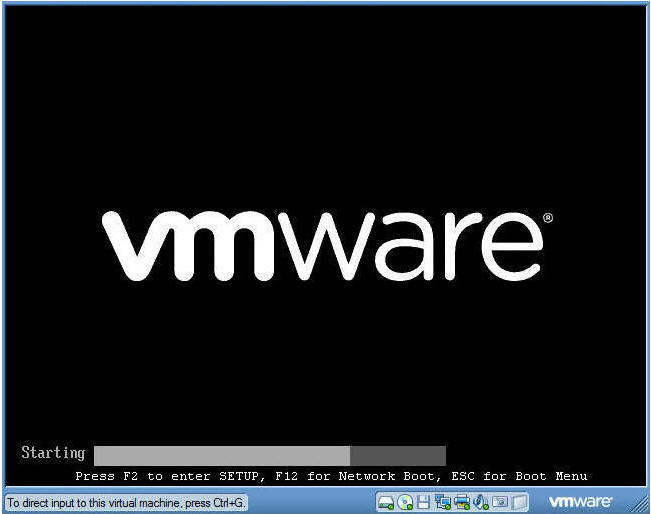
1. Configure Windows to boot off of Helix
   * **Instructions**:
     1. Select CD/DVD (IDE)
     2. Select the Use ISO image file
     3. Browse to where you saved the Helix iso.
     4. Note:  In my case, I save it in the following location:
     5. H:\BOOT ISO\Helix2008R1.iso



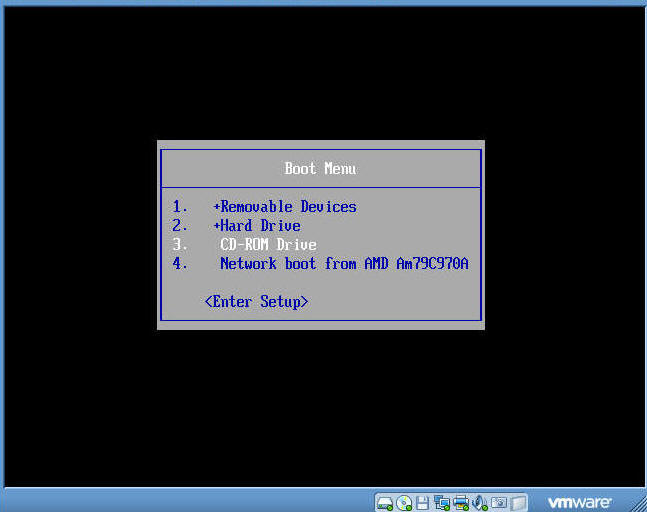
1. Play the Virtual Machine
   * Select Play Virtual Machine



1. Booting from the ISO
   * At the same time, Click the right mouse key and the press the ESC button, when the screen starts to change to the VMware screen below.
   * **Note**: This might take you a few times so be patient!!!



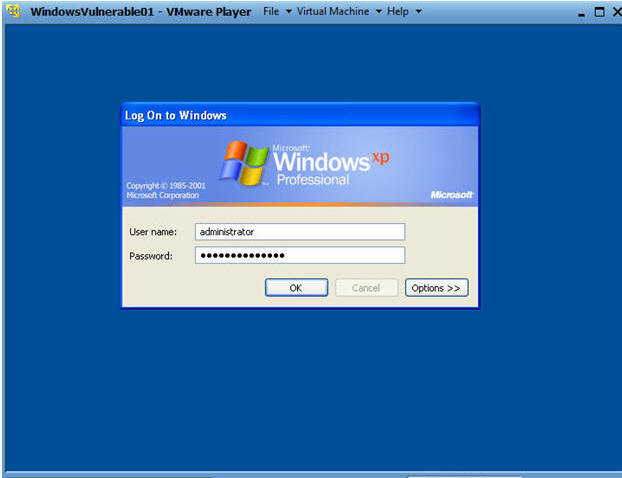
1. Boot Menu Selection
   * **Command**:
     1. Select CD-ROW Drive
     2. Press Enter



1. Booting from Helix Options
   * **Instructions**:
     1. Boot into the Helix Live CD
        + This will take you into a knoppix/linux operating systems.
        + Unfortunately, VMware seems to not allow mouse clicks.
        + In the future, I will experiment with VirtualBox to see if the same issue is present.
     2. Boot from first hard disk
        + Select this option.
        + This will allow you to run the Helix CD from Windows.



1. Log into your Windows Machine
   * **Instructions**:
     1. Its probably a good idea to long in with an administrator account to ensure you can run the Helix CD.

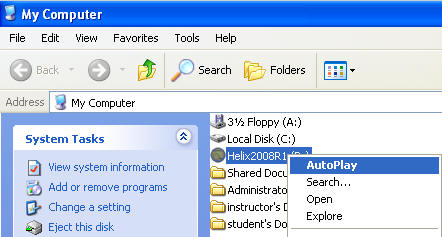


**Section 4. Starting Helix and Acquire Image on WindowsVulnerable01**

1. Open Up My Computer
   * **Command**:  Start --> My Computer



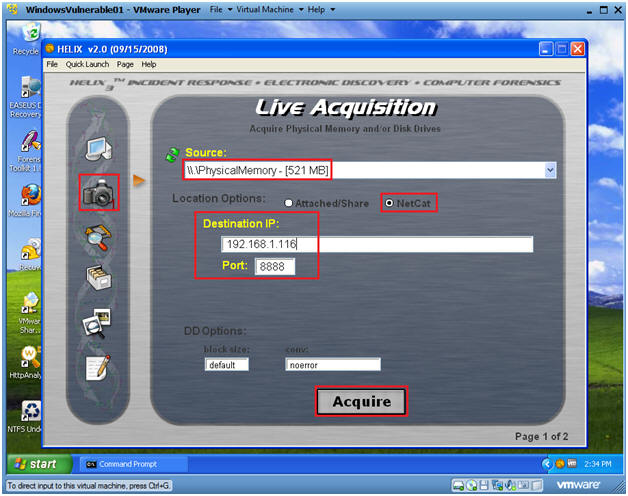
1. Starting Up Helix
   * **Command**:
     + Right Click on Helix2008R1
     + Click on AutoPlay



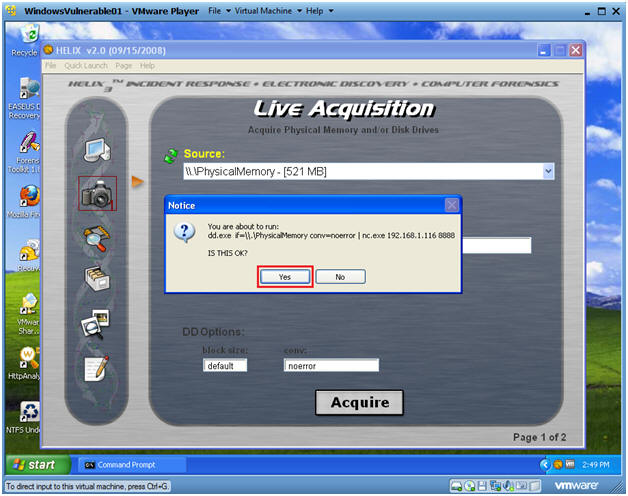
1. Select Language
   * **Command**:
     + Select English
     + Click Accept



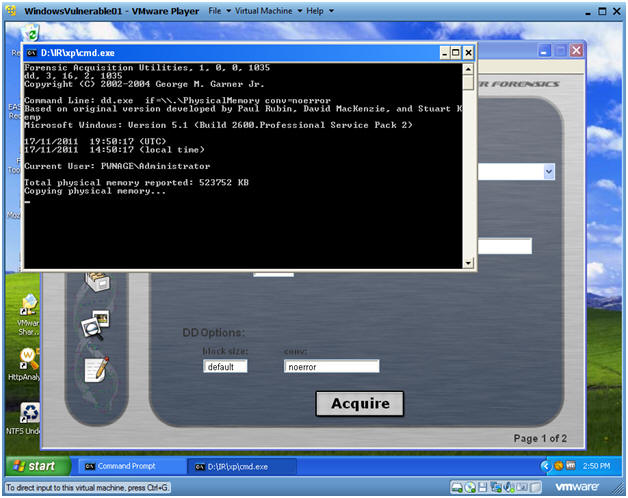
1. Live Memory Acquisition
   * **Command**:
     + Click on the Camera
     + Select \\Physical Memory
       - You have the option of acquiring the entire disk as well.
     + Location Options:  Netcat
     + Destination IP: 192.168.1.116
       - **Note**: This is the IP Address of the Helix Server found in(Section 2, Step 4)
     + Port: 8888
     + Acquire



1. Notice
   * **Command**: Yes

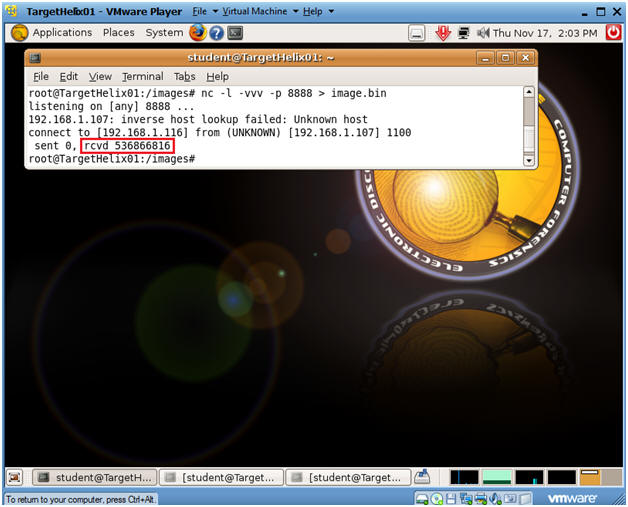


1. So what is going on?
   * **Note**:
     + Your physical memory is now being copied to the Helix server.
     + This will take between 5 to 10 minutes depending your system and network resources.
   * **Next Steps:**
     + Once the copy completes, the Black cmd.exe screen will close.
     + Once the screen closes, then move on to the next section.

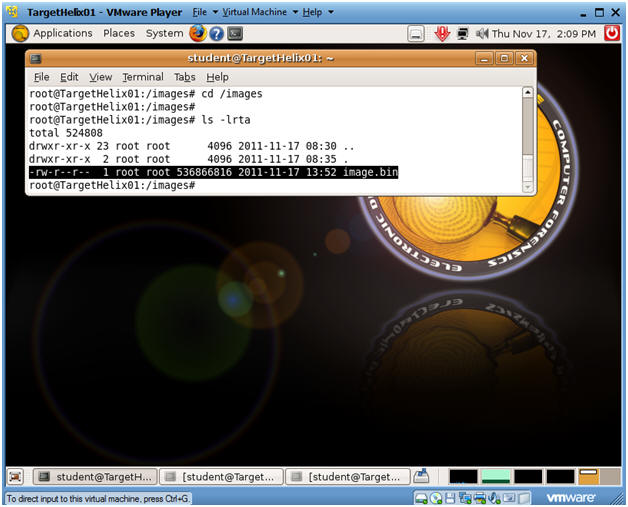


**Section 5. Verifying Image Copy on the Helix Server**

1. On your Helix Server
   * **Note**:  Once the copy completes on WindowsVulnerable01, you will see a similar received message "rcvd  536866816".



1. Verifying your Image
   * **Proof of Lab**
   * **Command**:
     1. cd /images
     2. ls -lrta
     3. Do a Print Screen, Paste into a Word Document, Upload to Moodle.



**Section: Proof of Lab**

1. Cut and Paste a screen shot found in Section 5, Step 2 in a word and upload to Moodle.