ECE4112 Internetwork Security
Lab 1: OS Installation and Introduction to security tools

Date Assigned: January 12, 2009
Date Due: January 19, 2009
Last Edited: October 31, 2007

Please read the entire lab and any extra materials carefully before starting. Be sure to start early enough so that you will have time to complete the lab. Answer ALL questions in the provided Answer Sheet and be sure you turn in to the TAs ALL materials listed in the Turn-in Checklist on or before the Date Due.

Goal: This lab is designed to help you setup your hard drive with the OS’s and programs you will be using throughout the semester.

Summary: This lab consists of two parts. In the first part, you will install RedHat Workstation 4.0 on your hard disk and create virtual machines with different operating systems. In the second part, you will install and use various security tools.

Background:
- Read “Hacking Exposed” Chapters 1, 2, 3
- Try running “nslookup” in a windows command prompt followed by the site whose IP you’d like to know (while you are on a machine connected to the Internet outside our isolated lab) (for example nslookup www.google.com)
- Read about the tool “Dig” at http://www.kloth.net/services/dig.php
- Read about Bridged Networks for VMware at:

1. If you are not familiar with Linux, please look at the Appendix “General Linux Tips” and also please go to the following website to learn some basic commands. The best way to learn is to experiment on your machine.
   http://www.reallylinux.com/docs/basic.shtml

Section 1 Prelab
Glance at the Appendices now so that you know what information is at the back of this lab.

Read the Georgia Tech Computer and Network Usage Policy
http://www.oit.gatech.edu/inside_oit/policies_and_plans/policies/CNUSP.pdf
Section 2 Prelab:
Turn in this pre-lab part to the TAs with your completed answer sheet at the completion of the lab.

At home or on a school computer which is connected to the Internet (our security lab machines are not connected to the Internet):
Use the whois databases (for example www.internic.net/whois.html); a registry whois lookup (for example http://www.networksolutions.com/en_US/whois/index.jhtml); and the American Registry for Internet Numbers (ARIN) (for example http://ww2.arin.net/whois/) to find out everything you can about the company Internet Security Systems (www.iss.net). Attach a printout or hand written SUMMARY (not every single IP address required!) of that information to your lab answer sheet turn in.

Prelab Q 2.1. How do you defend your own network against this type of information gathering?

Lab Scenario: You will set up a RedHat Workstation 4.0 host machine with a base IP address, VMware, a RedHat 7.2 virtual machine, and an XP virtual machine. You will have three computers in one box all connected together in a bridged network which can communicate through one single network interface card. This one card will connect your multiple virtual computers to any network the host machine’s physical interface card is connected to.

Introduction and General Information
Working in groups of two, follow the attached lab and install Linux on your removable hard drive. During TA hours, you will need to obtain from the TA a removable hard drive, a key for the hard drive, Red Hat Workstation 4.0 installation CDs, and a floppy with the Ethernet card driver software on it.

You are to keep the hard drive and the key; however, all the CDs have to be returned before you leave the lab. You will need to get the TA to enter a VMware license number. So, make sure you are working when a TA can assist you in those steps. You may work in the lab anytime by using your buzzcard to enter, however, TA support hours are much more limited. Check off on labs must be done during the TA’s lab hours. CDs must be returned to the TAs before the TA hours end for that period.

Do not drop or roughly handle the hard drives. If you break it you will be asked to replace it and you will find they cost about $65. If you loose a hard drive frame key, it costs $25 because you have to buy an entire removable hard disk frame kit just to get the key.

To insert your hard drive into the machine:
Slide your drive into the docking bay. Push with your thumb to make sure the contacts are connected, push down the locking handle. Use your key to lock the drive into the bay. If the drive is not locked into the bay, you will not get power to your hard drive.

**General Warning for the entire quarter:**

Warnings on: 1) removing your hard disk from the machine while it is running Linux or 2) turning the power off while the machine is running Linux: do not do it!

Do not try to remove your hard drive from the Linux machine while Linux is running. Here is the procedure to shut down

In a graphical X window:

Click on the actions icon in the upper left of the screen. Select logout and then shutdown, yes.

( or if not in a graphical X window): In a text terminal:

```
shutdown -h now
```

after the machine halts use your key to remove the hard drive. DO NOT FORCE THE HANDLE UP WHEN REMOVING THE HARD DRIVE. IF YOU HAVE NOT UNLOCKED THE DRIVE AND YOU PULL HARD YOU CAN BREAK THE PLASTIC RELEASE HANDLE. Unix stores some file states in memory and this stuff needs to be written to the disk before the disk is removed otherwise you may corrupt your disk and have to reinstall LINUX. Be sure to shutdown before you remove the hard drive or before your power off the computer.

Do not use cntl alt del to reboot the machine unless you have no choice. There is a chance you will corrupt your hard drive if you do it this way.

What to do if you ever have a corrupted operating system:

In the event you try to boot and get the message that you have a corrupt file system you may try to recover by using the command fsck /dev/hda1 and repeat this for each had# your machine uses (this will be hda1, hda2, and hda3 . fsck attempts to find and repair corrupted file systems. Answer yes to all repairs. This may or may not work.

**SECTION 1**

Turn in the answer sheet with your answers. You should not turn in the lab instructions, only the answer sheet section. The first part will take approximately 2.5 hrs to complete. The second part should take approximately another 1.5 hours.

**1.1 Installing RedHat Linux Enterprise Work Station 4.0**

The main focus of this section is to ensure you properly install RedHat Linux with the correct packages. The following section will go through the necessary steps of installing RedHat Linux.

To boot from the Red Hat CD#1:

With no HD in the computer, turn on the power and insert a RH CD #1 into the CD. Turn the power off. Put your HD in, turning the key to lock it in, and then turn the power on.
This will boot the computer from the CD. Do not add or remove a HD with power turned on.

- Just hit enter to get past the main menu.
- Use tab to move to skip media test. (If you find that either the keyboard or the mouse do not work upon boot, unplug the USB mouse and keyboard and plug back in using different USB ports).
- Next at welcome screen
  - The language that will be used is **English**. Just select next.
  - The keyboard being used is **U.S. English**. Just select next.
  - IF you are asked, you want to do Install Red Hat Enterprise WS (Fresh) as opposed to modifying a detected already installed version. (This happens when you have a HD with an OS already on it).
  - If you see the mouse selection screen, the mouse is **Wheel Mouse USB**
  - Remove all partitions on this system
  - Are you sure answer YES
  - Select next on the partitioning screen

- Boot Loader Screen Select Next.
- Manually configure your machine’s name to **groupx.4112-xxx.mininet.org**, but first see the table of machine names later in this lab (approximately page 6) to see your correct name.
- Choose no firewall and then next
- Select next on language screen
- Leave Eastern time selected
- Enter root password as “password” and confirm password is “password” (This makes it easier for TA help throughout the semester, not a good idea in a real network connected to the Internet!)
- Select Customize the set of packages to be installed

In the package Group Selection Window many items are already selected. Add the following to what is already selected:

- **Servers:** Windows File Server
  - Legacy Network Server
- **Development:** Development Tools
  - Gnome Software Development
  - Legacy Software Development
- **System:** System Tools:
  - Nmap Frontend
  - Ethereal – gnome
- **Servers:** MySQL Database
  - PHP-MySQL
  - MYSQL Server
  - MYODBC
  - MYSQLDevel
• Click next
• About to Install Screen is next, select next
• Installation takes about 7 minutes and requires you to insert CD#2. After 16 more minutes you will be asked for CD #3. After 9 more minutes you will be asked for CD#4. After 3 more minutes you will be asked for CD#1 again.
• Remove CD and select exit

The first boot will stop at a Kudzu hardware detection screen. Let it time out, it will continue automatically

• Select next at the welcome screen
• Yes I agree
• Enter date and time
• enter a user name of ece and a password of password
• No I do not want to register my system with red hat.
• Next on Additional CDs screen
• Next on Finish Set Up

Congratulations. You have just finished installing the Linux operating system.

• Logon as root and password is password

In order to get the BCM5700 network interface card on the motherboard of the lab computers to work, we need to install the software driver. We got the driver from http://broadcom.com/drivers/downloaddrivers.php and on that web page selected the Linux (i386/IA64/x86-64) driver and have it for you on a floppy disk. Ask the TA for a copy if you were not given this with the installation CDs.

Put the floppy in the computer

```
mount /mnt/floppy
```

(this allows you to access the floppy graphically or with the name /media/floppy)

```
 rpm –ivh /media/floppy/bcm5700-8.3.14-1.src.rpm
```

```
umount /mnt/floppy
```

remove the floppy (careful it wants to fly when you push the floppy release button)

```
 cd /usr/src/redhat
 rpmbuild –bb SPECS/bcm5700.spec
```
rpm –ivh RPMS/i386/bcm5700-8.3.14-1.rpm
modprobe bcm5700

Now you have added the needed Ethernet card driver software. Back to the networking:

- Click RedHat icon on taskbar->system settings->network, and then select devices tab (and select new if you do not see an eth0, then select Ethernet connection and forward, then Select generic bcm5700 device and forward
- Select eth0 and edit
- Select statically set IP address
- Use the address for your group number (see table below)
- Subnet mask 255.255.255.0
- Default gateway 57.35.6.1
- Click the “Hardware Device” tab and uncheck ‘Bind to MAC Address’
- Click OK
- Close the Network Configuration window
- Yes you want to save your changes, and OK
- In a terminal window type service network stop
- Then type service network start
- Test your Ethernet by typing ping 57.35.6.10 (This is the NAS machine) It may take up to 30 seconds before it starts working.

**IP Addresses:** Each group will be assigned a range of five IP addresses. You will only need one for now, but will use more in later labs. Use the FIRST IP address for the one on the operating system you just installed. Your group number will be the Hard Drive number you are assigned by the TAs and the host name will include three digits in the place of xxx where the three digits are the value in the last octet of your assigned IP addresses. For example, group 1 will assign their first machine host name as group1-4112-86.mininet.org, the second hostname as group1-4112-87.mininet.org, and so on. Group 2 will make their first machine host name group2-4112-91.mininet.org, etc. This allows each group to have the future ability to have five different IP addresses with five well-defined unique host names.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>57.35.6.86 – 57.35.6.90</td>
<td>group1-4112-xxx.mininet.org</td>
</tr>
<tr>
<td>57.35.6.91 – 57.35.6.95</td>
<td>group2-4112-xxx.mininet.org</td>
</tr>
<tr>
<td>57.35.6.96 – 57.35.6.100</td>
<td>group3-4112-xxx.mininet.org</td>
</tr>
<tr>
<td>57.35.6.101 – 57.35.6.105</td>
<td>group4-4112-xxx.mininet.org</td>
</tr>
<tr>
<td>57.35.6.106 – 57.35.6.110</td>
<td>group5-4112-xxx.mininet.org</td>
</tr>
<tr>
<td>57.35.6.111 – 57.35.6.115</td>
<td>group6-4112-xxx.mininet.org</td>
</tr>
<tr>
<td>57.35.6.116 – 57.35.6.120</td>
<td>group7-4112-xxx.mininet.org</td>
</tr>
<tr>
<td>57.35.6.121 – 57.35.6.125</td>
<td>group8-4112-xxx.mininet.org</td>
</tr>
</tbody>
</table>
NAS configuration

For this class we will be using a Network Attached Storage device (NAS). This is a windows based server with half a terabyte of memory. The tools and documents required for this and other labs will be placed on the NAS. To connect to this machine, we will use SAMBA file transfer utilities. Once connected to samba you can access it just like you would a floppy or CDROM drive. To setup follow these steps.

• Open /etc/fstab in a text editor. You can use a graphical editor provided in RH or text based on like vi or emacs. To open either, type vi or emacs at the prompt.
• Add the following line (spaces in line are tab characters):

```
//NAS/secure_class /mnt/nas4112 smbfs noauto,username=secure_class,uid=500,gid=500 1 0
```
• Then type

```
# mkdir /mnt/nas4112
```

Since the NAS server is on a different subnet, your local machine doesn’t know how to find the NAS machine. So, edit /etc/hosts file to add the following line:

```
57.35.6.10 nas.storagerus.com nas
```

You need to do these only once. Now to mount the NAS, every time, you can just type

```
# mount /mnt/nas4112
```

The password is “secure_class”. After this, the NAS will be loaded just like a floppy or CD.
Printer Configuration

Now you will setup the lab printer, so that you can print directly from your machine. Follow these steps to set it up.

Go to the Red Hat icon -> System Settings -> Printing
On the GUI, click New
  Name: printer_4112 (type in)
Forward
  Queue Type: select JetDirect (radio button)
  Printer: 57.35.6.9 (type in)
  Port: 9100 (typed in, but should be default)
Forward (to Model select)
  Click HP->LaserJet4000T/TN (drop down arrow)
    Select Omni if asked for driver
  Click Finish

To print from a root prompt, just type:
# lpr <filename>

You can also print from gedit.

Aside 1:

While on the subject of printing, to capture a screen shot of your computer in Red Hat Linux Workstation 4.0 select “Actions” and then select “Take Screen Shot”.

NOTE: When asked to record data from the program ‘Ethereal’, take a screenshot rather than print from ‘Ethereal’ itself. Unless you select the proper print settings, printing from ‘Ethereal’ will produce a lot of extra pages. Taking a screen shot and printing this screen shot will prevent you from printing 30 or 40 pages of garbage.

Aside 2:

You will need this information later this semester after you have created some virtual machines. This information is presented here early because we are looking at printers now. To set up to be able to print from Virtual machines on the Windows VM:

Select “Printers & Faxes” from the Start Menu.
Select “Add a Printer”
Click “Next”
Choose “Local Printer”
Deselect “Auto Detect”
Click Next
Choose “Create a New Port” and select “Standard TCP/IP Port” from the drop down menu.
Click Next
Enter the IP address and printer name from Lab 1: 57.35.6.9 & “printer_4112”
Ensure you are connected to the Network, and click Next.
Select the correct Printer driver and follow the prompts.
   Remember: It’s a Jet Direct card on port 9100
   The printer is an HP Laserjet 4000TN

1.2. Installing VMware on your RedHat Enterprise 4.0 Host

Note: You will need a TA during this part to type in a VMware license number for you.

Now you need to install a program called VMWare. This software allows one machine to
run multiple virtual machines. This allows you to have your own virtual mini-net to do
your experiments.

Copy the VMware-workstation-5.0.0-13124.i386.rpm installation file from the
/mnt/nas4112/VMWare directory to /root.

cp -r /mnt/nas4112/VMWare/VMware-workstation-5.0.0-13124.i386.rpm /root

On your Red Hat Enterprise 4.0 host, open a terminal window. You can do this by right
clicking on the mouse and selecting new terminal.

    # rpm –Uhv VMware-workstation-5.0.0-13124.i386.rpm
    # /usr/bin/vmware-config.pl

Accept the license
Accept the default /usr/share/icons by hitting enter
Accept the default /usr/share/pixmaps by hitting enter
Yes to build vmmon
Accept the default location for C header files

Answer yes to do you want networking for your virtual machine?
Answer no to do you want to be able to use NAT networking in your virtual machines
Answer no to do you want to use host only networking in your virtual machine

... 
What this has done is set up a bridged network. We are only going to use the bridged
network which will act like a hub for all virtual machines that we wish to put on top of
our Linux host. Each of these virtual machines will be just like plugging another machine
into a hub.

Launch vmware (# vmware) and go to Help, Enter Serial Number. Have the TA come in
and enter a serial number for your VMware license.
Answer no to would you like to register now.

1.3 Installing RedHat 7.2 and Windows XP virtual machines

Note: In this section you may need to hit control and alt keys at the same time to release your mouse from a VMware window.

Now you will be installing virtual machines on your host machine. One of the ways of doing this is to create a new virtual machine in VMware and then installing the OS on it, just as you would on a normal machine. If you already have one of these machines, you can make another machine from it by just copying the right directories. This cuts the installation time by a huge amount. You can copy both images at the same time in two different terminal windows.

Copies of the virtual machines, created by the TAs, are available on the NAS server. You will be creating virtual machines out of them. Follow the steps below to do this.

- Create a vmware directory by using the command
  \texttt{# mkdir /root/vmware}
- Copy the \texttt{\slash mnt\slash nas4112\slash VMWare\slash RedHat7.2} directory to your \texttt{\slash root\slash vmware} directory by using the command
  \texttt{# cp -r /mnt/nas4112/VMWare/RedHat7.2 /root/vmware}
  This will take a long time to copy since the images are 4-6GB.
- Copy the \texttt{\slash mnt\slash nas4112\slash VMWare\slash winXPPro} directory to your \texttt{\slash root\slash vmware} directory by using the command
  \texttt{# cp -r /mnt/nas4112/VMWare/winXPPro /root/vmware}
  Again, this will take a long time to copy since the images are 4-6GB.
- Type \texttt{\textasciitilde vmware &} in a terminal window to start VMWare. The \\textasciitilde sign allows a process to run in the background, leaving the terminal open for use.
- Follow the steps below to create a RedHat 7.2 virtual machine
  - Select File->New->New Virtual machine to create a new virtual machine
  - Choose Custom machine and click Next
  - Select legacy since these images were created with an older version of VMware and click Next
  - Select Linux for operating system and click Next
  - Change the name of the machine to RedHat7.2 and set the directory to \texttt{/root/vmware/RedHat7.2}
  - You will be warned now that you already have a machine at that location, answer yes (this is what we just copied to there)
  - Leave the virtual memory setting as it is. If it gives you problems, you can increase or decrease the amount of memory for each machine, later. Then click Next.
  - Select Bridged networking and click next.
  - On the I/O adapter screen just click next
  - Choose “Use an existing virtual disk” and click Next.
• Click Browse, go into the /root/vmware/RedHat7.2 directory and choose the file called “RedHat7.2.vmdk”
• Click Finish. This will create a RedHat 7.2 virtual machine

• Follow the steps below to create a Windows XP virtual machine.
  • Select File->New->New Virtual machine to create a new virtual machine
  • Choose Custom machine and click Next
  • Select legacy since these images were created with an older version of VMware
  • Select Microsoft Windows and also select Windows XP Professional for operating system
  • Change the name of the machine to WinXP and change the directory to /root/vmware/winXPPro
  • You will be warned now that you already have a machine at that location, answer yes (this is what we just copied to there)
  • Leave the virtual memory setting as it is. If it gives you problems, you can increase or decrease the amount of memory for each machine, later.
  • Select Bridged networking and click Next.
  • Choose “Use an existing virtual disk” and click Next.
  • On the I/O adapter screen just click next
  • Click Browse, go into the /root/vmware/winXPPro directory and choose the field called “winXPPro.vmdk”
  • Click Finish. This will create a Windows XP virtual machine

### 1.3.1 Configuring the RedHat 7.2 virtual machine

Start the RedHat 7.2 virtual machine by clicking on it in the shortcuts bar and clicking “Power on this virtual machine.” Click OK to get past upgrade dialog. It will boot up like a normal system. Login with username “root” with password “password”.

The IP address for this machine has not been set yet. It will depend on what group you are in. Using the IP table given before, assign an IP address that is one more than your base Red Hat WS 4.0 installation. (e.g. If your range is 57.35.6.131 – 57.35.6.135 assign an IP of 57.35.6.132). Follow the steps below to do this.

• Click on the terminal icon to start a terminal.
• Type “ifconfig” and press Enter. It will show you the current network setup. If an IP was assigned to the original machine, of which yours is a copy, it’ll be shown on the screen. eth0 means the Ethernet interface on your computer. If you had two network cards, then it would be eth0 and eth1.
• Now type “ifconfig eth0 57.35.6.x+1” where x is the last number in your host IP address.
• Now type “route” to see the routing configuration. You need to have the default gateway set as 57.35.6.1. If there is any other entry for default, delete it by typing # route del gw x.y.z.a netmask 255.255.255.0 (where x.y.z.a is the wrong entry)
• You can now add the new gateway by typing
  
  ```
  # route add default gw 57.35.6.1
  ```

• Check your configuration by pinging your host computer (ping 57.35.6.x) and also the default gateway (ping 57.35.6.1). Press control+c to stop the ping.

However, when you restart your machine, the IP Addresses you set might be changed. To prevent this, use the following steps below to modify Linux networking configuration files.

• Click on the terminal icon to start a terminal.
• Type “vi /etc/sysconfig/network-scripts/ifcfg-eth0” and press Enter. This will open the file in the vi text editor. The text editor will start in command mode. Later we will change to insert mode to change some text. If you need to get back into command mode press Esc.
• Move the cursor to the first digit in the IP address on the line that starts with “IPADDR=”. Press “D” (Shift + d) to delete the rest of the line. If you just need to delete a single character press “x” while the cursor is on the character. Now the only text on this line should be “IPADDR=”.
• Press “a” to enter insert mode. Insert mode allows you to insert text into the file.
• Add “57.35.6.x+1” to the line after “IPADDR =”.
• Press Esc to switch back to command mode.
• Now make the necessary changes to the following lines:
  
  ```
  NETMASK=255.255.255.0
  GATEWAY=57.35.6.1
  ```

• To save the changes to the file type “:w” (colon w). You will see the command at the bottom of the window.
• Type “:q” (colon q) then Enter to quit out of vi. If you made unnecessary changes or do not wish to save the file use the command “:q!” (colon q exclamation) to exit without saving. You could also use “:wq” (colon w q) to save and quit in a single command.
• You should now be back at the terminal prompt.
• Restart this virtual machine.
• When it finishes rebooting log in and open a terminal window.
• Type “ifconfig” and press Enter. It will show you the current network setup. Make sure your IP address is correct.
• Check your configuration by pinging your host computer (ping 57.35.6.x) and also the default gateway (ping 57.35.6.1). Press control+c to stop the ping.

Now check if any unnecessary services are running. You can turn them off by typing ‘ntsysv’ in a terminal window. Scroll down to sendmail and if it is already set as on, turn it off by pressing the space bar at that line. Do this for syslog also if it set to on. Tab to OK, press return bar when OK highlighted.
NAS Configuration on Virtual machines

To be able to access the NAS server from this virtual machine you will need to the NAS configuration. It should have already been done for you in the images. Check your /etc/fstab file to make sure that it has the line

```
//NAS/secure_class /mnt/nas4112 smbfs noauto,username=secure_class,uid=500,gid=500 1 0
```

There should also be a directory called /mnt/nas4112

The /etc/hosts file needs the line

```
57.35.6.10 nas.storagerus.com nas
```

Then delete the existing line

```
57.35.10.10 NAS
```

Now to mount the NAS, every time, you can just type

```
# mount /mnt/nas4112
```

The password is “secure_class”.

After this, the NAS will be loaded just like a floppy or cd. It even has a graphical folder in /mnt.

1.4. Configuring the Windows XP virtual machine

Start your windows XP machine. Click OK to get pas upgrade screen. Then click OK to get past activation dialog. When asked to change the UUID, click Create. You will need to make some changes to it to configure it properly. Follow the steps below to do this.

Upon the first boot you may see an “Install New hardware” wizard for the SCSI drive; just click Next and then Finish.

- Choose Start->Control Panel.
- You do not need to install the SCSI driver.
- Click on Network and Internet Connections and then Network Connections.
- Right click on the LAN connection that comes up and choose properties.
- Choose TCP/IP and click properties.
- Change the IP address to two more than your host machine. E.g. 57.35.6.x+2 where x is the last number in your host IP address.
- Make sure the other settings look something like below.
  - Netmask: 255.255.255.0
  - Default Gateway: 57.35.6.1
  - DNS server: 57.35.7.254
- Click OK and then OK again. Exit the control panel window.
Your XP virtual machine is configured properly now.

Now open up a command window (type cmd in Start->Run) and ping your host machine’s IP address. Press control+c to stop it.

Summary:
At this point you have set up your Red Hat WS 4.0 host machine with a base address, a RedHat 7.2 virtual machine, and an XP virtual machine. You now have three computers in one box all connected together in a bridged network which can communicate through the single network interface card out to any network you connect you host machines physical interface card to.

General Information: The actual space for answering questions is provided at the end of the lab in the Answer sheet. You may detach it and write the answers as you go along. You may also use the original word document on the class web site to obtain an electronic copy of the answer sheet.

Q1.4.1. Draw a picture here of three machines connected together by a hub or a switch and put names on the machines as well as IP addresses on each of the three machines network connections:

Show Your Hand Drawn Diagram to the TA and also demo ping to each of the other two machines simultaneously from your Host machine Red Hat WS 4.0. Have the TA sign his/her name and enter the date in the answer sheet.

1.5 Hardening a Redhat 4.0 Virtual Machine Installation

In this section we will go through the first steps of hardening a linux system. By hardening we mean applying the ‘Principle of Least Privilege’ i.e. allowing someone to access only what he/she needs to access and nothing more. We will set up this Red Hat box only to allow traffic to 2 ports. The web server and the SSH port. Next we will disable all unnecessary services. Let’s get started.

Installing a “Hardened” Windows XP virtual machine

- Make a virtual machine of Red Hat 4.0. An image of 4.0 can be found on the NAS. Copy this machine into a directory called RedHat4.0-Hardened.
- Type ‘vmware &' in a terminal window to start VMWare. The '&' sign allows a process to run in the background, leaving the terminal open for use.
- Follow the steps above to create a Red Hat 4.0 virtual machine as you did before in section 1.3 only this time use the directory /root/vmware/RedHat4.0-Hardened instead
- Now start this virtual machine and in the terminal type
This will give us the list of open ports on the system which may/ may not be firewalled before hardening the system

- We are ready to start hardening the machine. In the terminal type
  - `#setup`

  - Using the arrow keys move down to the ‘Firewall Configuration’, hit enter. Inside here set security level to be ‘High’ and then move to the ‘Customize’ button using the ‘tab’ key. Press the spacebar when it is selected.
  - Make sure eth0 is not selected as a trusted device and select the ports WWW(HTTP) and SSH using the spacebar.
  - Select OK twice to return to the main menu.
  - Now go to ‘System Services’. You can also reach here by typing the command `#ntsysv`

- Enable only the following services
  - `anacron`
  - `autofs`
  - `crond`
  - `iptables`
  - `kudzu`
  - `netfs`
  - `network`
  - `rawdevices`
  - `xfs`
  - `xinetd`

**Note:** We have chosen to disable all other services based on the requirement for this lab box and the services disabled or enabled will depend on the requirement for the system. For more information see:

  - [www.brandonhutchinson.com/Hardening_Fedora.html](http://www.brandonhutchinson.com/Hardening_Fedora.html)
  - [www.sorgonet.com/linux/linuxdaemons/](http://www.sorgonet.com/linux/linuxdaemons/)

- OK and Quit. Now reboot the system `#reboot`
- After the system reboots run the command
  - `#netstat –an >/root/after-hardening.txt`

**Q1.5.1.** Compare the outputs before-hardening and after-hardening and list the ports that have been disabled.

### SECTION 2

**Goal:** This part of the lab will introduce you to some of the common and useful security tools. Note that one really good source for these tools is [http://sectools.org/](http://sectools.org/) which has the “top 100 Network Security Tools” available.
**Summary:** In this part you will be introduced to tools like NMAP and Nessus to learn how a network can be scanned for useful addresses and the collected addresses can then be scanned for exploitable vulnerabilities. You will also learn about some of the Windows tools that can be used to accomplish these tasks.

**Lab Scenario:** Using the laboratory equipment as set up for you

*Installation and usage of network security tools*

Start both the XP and the virtual Red Hat 7.2 virtual operating systems. Go to the 7.2 “virtual operating system”.

Now access the NAS server by typing

```
# mount /mnt/nas4112
```

The password is “secure_class”. After this, the NAS will be loaded just like a floppy or cd. It even has a graphical folder in `/mnt`.

Note: If you have problems connecting to the server, check the previous section of the lab where it discussed the NAS set up and configure your machine properly.

The tools are in the `/mnt/nas4112/Tools/Linux` folder in a tarball file called `tools.tgz`

Copy the tools file to your Linux 7.2 machine into `/home` by typing:

```
# cp tools.tgz /home
# cd /home
# tar xvfz tools.tgz
```

This creates and unpacks the tools into the `/home/tools` directory. Now, to go into the tools directory,

```
# cd tools
```

**2.1 NMAP**

Now that an attacker has gathered information about your network perhaps using the methods in the prelab for section 2, the attacker would likely use a port scanner to examine what services your network is running. The next tool we will examine is nmap. This is already installed on you Linux operating systems but you could also find it yourself at [http://www.insecure.org/nmap/](http://www.insecure.org/nmap/).

That web page says “Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers, and both console and graphical versions are available. Nmap is free software, available with full source code under the terms of the GNU GPL.”
Move to your host Red Hat WS 4.0 system by opening a new terminal window on the blue host background screen. The version of nmap there is a later version than the one on your 7.2 virtual machine. Note you may need to hit control and alt keys at the same time to release your mouse from Vmware so as to move outside a virtual machine and onto the host machine.

To start nmap, type

```
# nmapfe &
```

(The & sign makes it run in the background so you’re free to use the terminal.)

Use nmap to scan the 7.2 virtual machine by entering in its host IP address in the target(s) text field, for example 57.35.6.x+1. Select a SYN Stealth Scan using all TCP&ICMP types of pings. Leave OS detection checked. Check Version Probe. Select scan.

**Q2.1.1.** List what ports, the state of the port, and service found on the 7.2 machine.

Repeat the port scan for your Windows XP virtual machine by doing the following section:

2.1.1 Windows XP scanning and Firewall effects

The following exercise familiarizes you with Windows XP Firewall logging. In many instances, analyzing the network traffic dropped by a firewall provides insight on current attacks, which may lead to defenses against future vulnerabilities. You will scan a Windows XP machine with the firewall off, then you will repeat with the firewall on. When you are done be sure to turn the firewall back off and leave it off. Here are the detailed directions:

On your Windows XP virtual machine, open the network and dial up connections (in the control panel) and right click on Local Area Connection and select properties. Select the Advanced tab (on top) and select the option to disable the firewall (or make sure it is already disabled). Click Ok.

Scan the Windows XP machine using NMAP. Take note of which ports are open. Next turn on the firewall and turn on firewall logging.

1. From your Windows XP VMware machine, navigate to the Network Connections control panel (Start->Control Panel->Network Connections)
2. Right-click on your Ethernet interface (Local Area Connection, etc.) and go to Properties
3. Turn on the firewall
4. Go to the Advanced tab
5. Click Settings
6. Go to the Security Logging tab
7. Check both of the checkboxes (Optional, but at least check Log dropped packets)
8. Select where you want the log file to be located

9. Ping the Windows XP machine from your Red Hat workstation and take a look at the log file
Above is our log immediately after starting the firewall logging. It is empty except for the version and header information.
We set our RedHat WS4.0 machine to ping the Windows machine a bit. Above we see all of the ICMP traffic being dropped (thus making the machine unresponsive to pings).

Now that the firewall is on use nmap to scan the Windows XP virtual machine. Take note of which ports are open. Take a look at the firewall log. If a network administrator were to see traffic like this, he/she could easily assume his/her network was being port-scanned or under a more serious attack.

Turn the firewall off and repeat the scan. Compare the results you got to when you had the firewall on.

Q2.1.2. What is the difference between when you scanned the Windows XP machine before and after enabling the firewall?

Turn off the Windows XP firewall and logging once you’re done.

Q2.1.3. At a computer with Internet access, look at http://isc.incidents.org/port_details.html and type in the numbers (for the ports you found open on the Red Hat 7.2 system ) in the upper left white box (80 is the default). It will tell you what registered services are associated with that port as well as some statistics. Summarize what you found out about each running service from that web site here:
Q2.1.4. What operating system and version did nmap find on the 7.2 system? What operating system version do you see when you boot up that virtual machine? Are they the same?

Q2.1.5. Next use nmap to a range of hosts. Use for example 57.35.6.x – (x+4), select all types of ICMP pings, and select ping sweep. Did nmap see all of your three machines? This is an automated ping sweep to find machines on a network. What other machines can you find in the 57.35.6 network?

Q2.1.6. Run this again 57.35.6.x – (x+4), select ICMP ping, and select ping sweep but in the host machines terminal window also run tcpdump with the command:
```
tcpdump -nli eth0
```
Watch the output in the terminal window as nmap does the ping sweep on the range of IP addresses you request the sweep on. In other words, what do you see in the terminal window while tcpdump is running? Control C in the terminal window ends tcpdump.

Q2.1.7 – Exercise
One of the primary tasks for hackers to make their life simpler is to create a map of the network within which they’re trying to carry out their attacks. This is especially easy to do once they’re logged into one of the computers inside the target network. To do this, simple tools such as nmap and traceroute (usually found in all distributions of Linux), and no sophisticated tools need be installed.

1. On the command prompt, type `nmap –sS 57.35.*.*`
2. Machines with their open ports show up.
3. In a different terminal window, on a command prompt, for one or two machines, do
   ```bash
   #traceroute <ip address>
   ```
List one or two machines that you found, list open ports for those machines, and list the trace route results.

Q2.1.8 a) How does traceroute work? (You might need to google this)
b) What is the main difference between Unix traceroute and the Windows tracert commands (in terms of operation not in terms of syntax)? (You may want to see http://www.tech-faq.com/unix-windows-traceroute.shtml)

Now let’s say you’ve investigated the public DNS servers and determined that 138.210.230.0-138.210.240.255 is a range of IP addresses that you find very interesting. Perhaps that range contains the networks of some companies that you are interested in. Do a ping sweep of these addresses on our mininet in our lab (NOT THE REAL INTERNET) and list all the servers/IPS you could find (type `nmap –h` or `man nmap` to see nmap usage information). Also list the company or organization as you find in our
mininet in our lab (NOT THE REAL INTERNET) if you could determine it. (Hint: If it is web server, you can try opening it in a browser.) Look at the traceroute output for each computer and with the help of that, construct a diagram of what the actual network looks like. For each machine, list the open ports on your diagram as well.

Q2.1.9. How do you defend your network against a tool like NMAP?

2.2. Nessus

At this point an attacker has mapped your network, knows what services you are running, knows what operating systems you are running and now wants to see if you have any vulnerabilities open to attack. A vulnerability scanner allows an attacker to do this. This tool is also useful to a system administrator to find vulnerabilities before they are attacked. In this next section we need to have another user account besides root on the Red Hat 7.2 virtual operating system because the next tool nessus runs in a client server mode. While on the 7.2 system:

```
# adduser ece4112
# passwd ece4112
```
Enter “password”
The system will complain that is a bad password but keep going
Enter “password” again.
Now we have an account names ece4112 with password “password”.

Nessus may be found at http://www.nessus.org/
The web page says “The “Nessus” Project aims to provide to the Internet community a free, powerful, up-to-date and easy to use remote security scanner. A security scanner is a program that will audit remotely a given network and determine whether bad guys (aka ‘crackers’) may break into it, or misuse it in some way. Unlike many other security scanners, Nessus does not take anything for granted. That is, it will not consider that a given service is running on a fixed port – that is, if you run your web server on port 1234, Nessus will detect it and test its security. It will not make its security tests regarding the version number of the remote services, but will really attempt to exploit any vulnerability in its database.

To install nessus:

cd /home/tools
If not already there, copy nessus-installer.sh from the NAS to /home/tools.

```
# chmod 700 nessus-installer.sh
#/nessus-installer.sh
```

Where do you want the Nessus package to be installed?” hit ENTER

Do you want the Nessus experimental features to be enabled?” select the default [n]
Answer **YES** to library question.

Finally quit

Now create a user

```
#/usr/local/sbin/nessus-adduser
```

enter “ece4112”

ENTER to select the default cipher method
Is this a local user on this machine: answer **YES**
You may or may not see:

```
    ENTER to select anywhere
    Enter a one-time password of:  password
```

CTRL-D to end the rules creation
Is that ok? (y/n)” , **ENTER** to create the user

New Pass phrase: enter “password” and do that 3 times
Now a new user has been added.

Now to run nessus start a server:

```
#xhost +
```

to configure X Windows to allow connections to your Red Hat 7.2 host.

Start the server

```
#nessusd &
```

switch users to ece4112 by typing

```
#su ece4112
```

run Nessus with:

```
nessus &
```

Enter the passphrase: **password**

Click the Log In button
Click Ok.
If there’s a “cannot connect” error, try typing in 127.0.0.1 for localhost.

Click Target Selection tab and enter a target for example the Red Hat WS 4.0 system
```
57.35.6.x
```
Start the scan by clicking start the scan at the bottom of the page. This test takes approximately 15 minutes.

**Q2.2.1. What vulnerabilities did Nessus find with your stock Red Hat WS 4.0 System?**

List them here:

Now scan your Windows XP machine (57.35.6.x+2). Do this with the firewall disabled and again with it enabled. Remember to enable the firewall:

- Click on Start->Control Panel->Network and Internet Connections->Network Connections
- Right click Local Area Connection->Properties->Advanced tab-> Check “Internet Connection Firewall”
- Click OK

After you are done, turn the Windows XP firewall off.

**Q2.2.2. How do you defend against vulnerability scanners?**

It is important to note here that there are several network vulnerability scanners available for a network administrator to analyze, diagnose and benchmark a network. These tools allow the administrator to find security holes before attackers do. Some such tools are:

3. Google search for “network security scanner” and you will see there are more

Appendix B briefly describes the process of writing customized scripts for Nessus. These scripts would be used to increase the functionality of Nessus to check new vulnerabilities. Although important, this is probably beyond what we need to do in order for you to understand the capabilities.

**2. 3. Windows XP tools**

There are equivalent tools for Windows based machines but they are not as easy to find and many are not open source. Just to use one windows based tool, lets use a windows scanning tool named SuperScan4.

**SuperScan 4**

SuperScan 4 may be found at [http://www.foundstone.com/us/resources/proddesc/superscan4.htm](http://www.foundstone.com/us/resources/proddesc/superscan4.htm)

Note: [www.foundstone.com](http://www.foundstone.com) free tools & Resources is a good resource for tools.

That web page says:
“Powerful TCP port scanner, pinger, resolver. Copyright 2003 I by Foundstone, Inc. SuperScan 4 is a completely-rewritten update of the highly popular Windows port scanning tool, SuperScan. Here are some of the new features in this version: Superior scanning speed, Support for unlimited IP ranges, Improved host detection using multiple ICMP methods, TCP SYN scanning, UDP scanning (two methods), IP address import supporting ranges and CIDR formats, Simple HTML report generation, Source port scanning, Fast hostname resolving, Extensive banner grabbing, Massive built-in port list description database, IP and port scan order randomization, A selection of useful tools (ping, traceroute, Whois etc), Extensive Windows host enumeration capability Note that SuperScan 4 is intended for Windows 2000 and XP only. Administrator privileges are required to run the program. It will not run on Windows 95/98/ME”

Open the XP virtual machine
Change your video mode to 800 x 600 so you can see the bottom of the screens we will use
Select Start->Run
Type \57.35.6.10\secure_class
The username and password are both secure_class.
Copy the /tools/windows folder to your machine
Double click on SuperScan 4
Double click on SuperScan4 executable
This beta version has expired but you may still use it (answer no to “go to web site”?)

Select the about tab to see instructions on how to use this tool
Select the scan tab
Enter your Linux host IP address in the start IP field
Click the \rightarrow beside the IP address 57.35.6.x that you just entered
Click the blue triangle at the bottom left to start the scan

Q2.3.1. What did this tool tell you about the Linux Host?

Use the tools tab and select ping to 57.35.6.x
Use the tools tab and select traceroute to 57.35.6.x
In the windows enumeration tab, enter the IP address of the XP machine and click enumerate. Look at all the new information you get on the XP machine.

Q2.3.2. What do you think of this windows tool as compared to the Linux tools we have used previously?

2.4 General Questions

Q2.4.1. How long did it take you to complete part 1 of the lab?

Q2.4.2. How long did it take you to complete part 2 of the lab?
Q2.4.2. Was it an appropriate length lab?

Q2.4.3. What corrections and or improvements do you suggest for this lab? Please be very specific and if you add new material give the exact wording and instructions you would give to future students in the new lab handout. You may cross out and edit the text of the lab on previous pages to make minor corrections/suggestions. General suggestions like add tool xyz to do more capable scanning will not be awarded extras points even if the statement is totally true. Specific text that could be cut and pasted into this lab, completed exercises, and completed solutions may be awarded additional credit. Thus if tool xyx adds a capability or additional or better learning experience for future students here is what you need to do. You should add that tool to the lab by writing new detailed lab instructions on where to get the tool, how to install it, how to run it, what exactly to do with it in our lab, example outputs, etc. You must prove with what you turn in that you actually did the lab improvement yourself. Screen shots and output hardcopy are a good way to demonstrate that you actually completed your suggested enhancements. The lab addition section must start with the title “Lab Addition”, your addition subject title, and must start with a paragraph explaining at a high level what new concept may be learned by adding this to the existing laboratory assignment. After this introductory paragraph, add the details of your lab addition. Include the lab addition cover sheet from the class web site.
Appendix A: NAS problems

If for some reason you cannot get the NAS file system to mount, after the main steps, you might not have installed Samba during the initial installation. Samba is needed to access the Windows file sharing system with NAS. You can check whether Samba is installed by typing `man samba` at a prompt. If a man page comes up, you have samba installed.

If you skipped Samba during the initial installation follow the steps given below to install it.

While in your RedHat7.2 Virtual machine, put the RedHat ½ installation CD in the drive. Copy the following three files to your /root directory.

Samba-common-2.2.1a-4.i386.rpm
samba-2.2.1a-4-i386.rpm
samba-client-2.2.1a-4.i386.rpm

Unmount the CDROM.

Open a terminal and go to the /root directory.
Type:

```bash
rpm –Uvh samba-common-2.2.1a-4.i386.rpm
rpm –Uvh samba-2.2.1a-4-i386.rpm
rpm –Uvh samba-client-2.2.1a-4.i386.rpm
```

You should now be able to mount the NAS.
Appendix B: Writing NASL scripts

Introduction

Earlier in lab 1, you used Nessus to scan computers within the network for vulnerabilities. Nessus is really just a program that systematically executes nasl commands. Usually residing in the path, the nasl executable resides in /usr/bin/nasl. It can be used as follows:

```
#nasl -t <target_IP_address> script_file_name.nasl
```

In this supplement, you will learn how to write and test your own nasl script in the event you are interested in how to do this.

Procedure

• Make a directory for this test and a file.

```
#mkdir /root/test
#cd /root/test
#touch index_script.nasl
```

Open it in Emacs or whatever text editor.

```
#emacs ./index_script.nasl
```

• Now, we're going to walk through a sample script.

3a. Write the description of the file in the introduction.

These steps are for other people's use. They can be used for actual nessus sessions.

```
if(description)
{
    script_id(99999);
    script_version("$Revision 1.0 $");
    script_name(english: "Checks for /index.html");
    desc["english"] = "/index.html is the default homepage served by most web servers. The presence of such a file is a dead giveaway to hackers that you are running a web server.
    Solution: Configure your web server to use a file other than index.html as its homepage.
    Risk Factor: Extremely Low. Generally, if you have an index.html page, you want the web server open.
    script_description(english:desc["english"]);
```
script_summary(english:"Checks for presence of index.html");
script_category(ACT_GATHER_INFO);
script_family(english:"HTML abuses");
script_require_ports("Services/www",80);
exit(0);
}

3b. Include some files.

   include("http_func.inc");
   include("http_keepalive.inc");

3c. Select a port.

   port = 80;

3d. Write code to complete task
   o hget is a variable that contains the command “GET index.html”. this is the command your web browser sends whenever accessing a new site and you don't specify a specific html file.
   o mysoc is the socket, similar to the socket function in the UNIX networking API
   o if the port isn't open, the program closes
   o myrec is what is received from the request
   o finally, the security hole is logged if the program does not receive a 404 (file not found) error.

   url = "/index/html";
   if(get_port_state(port))
   {
      hget = http_get(item:url, port:port);
      mysoc = http_open_socket(port);
      if(!mysoc)
      {
         display("Port 80 is closed anyway\n");
         exit(0);
      }
      send(socket:mysoc, data:hget);
      myrec = recv(socket:mysoc);
      http_close_socket(mysoc);
      if (!("404" >< myrec))
      {
         display("WebServer serving index.html\n");
         security_hole(port);
      }
      if("404" >< myrec)
{ display("WebServer not detected but port 80 is open (p2p client?)\n");
}

•Copy the file to the Nessus plugin directory.

#cp /root/test/index_script.nasl /usr/lib/nessus/plugins

Execute against your own computer (55.36.6.x)

#nasl -t <ip_address> index_script.nasl

6. Try it against a computer that is a web server. It turns out that if you get a positive for port 80 being open, and there is no presence of an index.html file, you most likely are running a p2p filesharing client such as kaza or limewire.

Addendum

Valid Flags to /usr/bin/nasl

```
<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>help</td>
</tr>
<tr>
<td>-p</td>
<td>parse only</td>
</tr>
<tr>
<td>-t target</td>
<td>select target ip address</td>
</tr>
<tr>
<td>-T file</td>
<td>put results of test in file</td>
</tr>
<tr>
<td>-s</td>
<td>run script with 'safe checks' enabled</td>
</tr>
<tr>
<td>-v</td>
<td>display version number</td>
</tr>
</tbody>
</table>
```

---

nasl -- Copyright (C) Renaud Deraison <deraison@cvs.nessus.org>
nasl -- Copyright (C) Michel Arboi <arboi@alussinan.org>

All information came from Linux man pages, the above authors, and the book Hacknotes: *Linux and Unix Security Portable Reference* by Nitesh Dhanjani.
Appendix C: Search Engine Reconnaissance

Google hacking is the term used when a hacker tries to find exploitable targets and sensitive data by using search engines. The Google Hacking Database is an ongoing project that lets users save queries that have revealed sensitive information. Browse the Google Hacking Database at http://johnny.ihackstuff.com/ghdb.php to get a feel for what is possible. The Google Hacking Database (GHDB) is a database of queries that identify sensitive data. Some uses include:

- Advisories and Vulnerabilities
- Error Messages
- Files containing juicy info
- Sensitive Directories
- Footholds

Also see the google hacking mini guide at: http://www.informit.com/articles/article.asp?p=170880&seqNum=1&rl=1

The following Google commands are useful in the context of hackers looking for information:

- The **site:** operator instructs Google to restrict a search to a specific web site or domain. The web site to search must be supplied after the colon.

- The **filetype:** operator instructs Google to search only within the text of a particular type of file. The file type to search must be supplied after the colon. Don't include a period before the file extension.

- The **link:** operator instructs Google to search within hyperlinks for a search term.

- The **cache:** operator displays the version of a web page as it appeared when Google crawled the site. The URL of the site must be supplied after the colon.

- The **intitle:** operator instructs Google to search for a term within the title of a document.

- The **inurl:** operator instructs Google to search only within the URL (web address) of a document. The search term must follow the colon.

As an example of this approach, to find open directories try the search “Index of” since this will appear in all open directory pages.
The above image shows a typical open directory from Apache.

You will notice that many extraneous results are shown. To refine the results, one can use some of Google’s more advanced commands in combination with the information already known. For example the search could be made using:

```
intitle:index.of name size
```

Google can be sued to find some password information. Many people seem to have been saving the passwords in Excel spreadsheets. Hackers take advantage of this by using the search

```
"login: *" "password: *" filetype:xls
```

**What are some ways to prevent against Google Hacking?**

- Keep your sensitive data off the web!
- Googledork! your own site
- Consider removing your site from Google's index
- Check for known vulnerabilities
- Access control using robots.txt
- Blocks robots from scanning

As a further example of the power of google to hackers:

Using iss.net let us see what a search engine can dig up on this domain.

- Point your browser to [http://www.google.com](http://www.google.com) (when connected to the internet of course)
• Run the search “inurl:iss.net”

Picking up on Leads:

• Open google again and this time search for ‘Admin inurl:iss.net’
• Scroll down to find the search result “ISS Defaced”
• Click on the link and you notice that the link is dead
• Hit the back button and now click on the link that says ‘Cached’ near the search result for ‘ISS Defaced’
• Google stores information about ISS for you even if it is removed from the web.

Exercise: Have a look at the search results and identify at least 5 other servers that are also servers that belong to iss.net.

Answer:
I. blackice.iss.net
II. xforce.iss.net
III. gtoc.iss.net
IV. bvlive01.iss.net
V. documents.iss.net
VI. atla-mm1.iss.net

Exercise: Find the URL of site that was defaced and provide a small summary of what it is or was used for.

Answer: From the Cached Page:
ISS Defaced
Mon, 5 May 2003


Iss.net webdavized... where is the security?

G00db0y www.zone-h.org admin

05/05/2003

Where is the security if also a site of a big security company is hacked?

Today a very well known security company was defaced using the last webdav vulnerability. You can find more about this vulnerability here:

http://www.microsoft.com/technet/security/bulletin/ms03-007.asp

Internet Security System (www.iss.net) was not hacked in the main server but in a secondary site. Everywhere USG hacked them.

The USG team replaced the main page with these words: "ISS Hacked By ShellCode And rD of USG! FUCK BUSH, BLAIR And SHARON AND FUCK ALL WHO SUPPORT THE WAR... greetz: DKD, FBH, S4t4n1c_S0uls and all who support us".

You can see by yourself here:

http://xfiw.iss.net

Mirror here:
http://www.zone-h.org/en/defacements/view/id=258882/
Current Site that was defaced: http://xfiw.iss.net

X-Force Internet Watch Honeypot Modified by USG

As a normal course of their research, the ISS X-Force™ places servers on the Internet to monitor hacker activity, propagation of Internet worms and to serve as targets for attack. These servers are known as honeypots. In some cases, honeypots are purposely left insecure and mis-configured. Some honeypots are "visible" to the public via web servers and web pages that are placed on the servers. All of ISS’ honeypots are constantly monitored by the X-Force to better understand widely used hacking tools and techniques, but to also to identify new attack routines and vulnerabilities.

Over the weekend of May 2, 2003, content on one of the ISS X-Force's honeypot research servers was modified by USG. This server, X-Force Internet Watch (http://xfiw.iss.net/), was a publicly available web server on the Internet. The server's official and publicly promoted purpose was to make available to university students a free version of BlackICE PC Protection. The X-Force Internet Watch server was specifically selected to be a honeypot because of the association with university students and the well-known fact that students actively hack systems. The server was configured to include numerous vulnerabilities, including several well-known, older vulnerabilities.

The X-Force immediately identified the activity and initiated detailed monitoring. Once the X-Force completed this monitoring, the honeypot server was disabled to perform standard X-Force malware analysis. As is typical, this activity has resulted in the identification of new hacking tools. The X-Force is currently finalizing their investigation and working to include added protection in upcoming XPU's for our products. Once the X-Force has completed their investigation, the X-Force Internet Watch server will be made available, but will no longer serve as a honeypot.

None of Internet Security Systems production servers, including its web sites, managed protection services business, customer databases and ordering system were affected by USG's attack on the X-Force Internet Watch honeypot server.
Appendix D: Other Network Scanning Tools

Internet Security Systems Internet Scanner, Attack Tool Kit, LANspy, Cheops-NG, Etherape, Intermapper

I Internet Security Systems Internet Scanner (a commercial tool)

Internet Scanner

The vulnerability assessment tool Internet Scanner is popular commercially available audit software from Internet Security Systems (ISS). According to ISS, “Internet Scanner can identify more than 1,300 types of networked devices on your network, including desktops, servers, routers/switches, firewalls, security devices and application routers.” Internet Scanner licenses the nmap database to do OS fingerprinting and in addition to port scanning and banner grabbing, Internet Scanner can identify vulnerabilities, misconfigurations, and the absence of patches.

Internet Scanner is available from ISS’s website (www.iss.net/download) as an evaluation copy which will only work on the loop back address to your own machine. Internet Scanner is a commercial piece of software and a license is needed to scan anything other than the loopback address.

Install Internet Scanner on your Windows XP machine (note: you will need to be running Windows XP SP1):

Select Start->Run
Type \57.35.6.10\secure_class
The username and password are both secure_class.
Copy the /tools/windows/Internet Scanner folder to your machine
Double click on the Internet Scanner install executable.
Accept all the default options and select “Standard Install” when it asks you which component you wish to install.
If MSDE is not installed, the installer will recognize it and offer to install it. Go ahead and install MSDE (requires reboot) since it is required because Internet Scanner stores scan data in a MSDE database.

Next, give Internet Scanner a license by copying the .key file from the Internet Scanner directory to C:\Program Files\ISS\Internet Scanner\Scanner Console\Licenses.

Although we will not be doing it in this lab due to time constraints, normally you would want to run the X-Press Update Install utility to update Internet Scanner. This ensures that you are able to detect the latest vulnerabilities and patches.

Launch Internet Scanner by going to Start->All Programs-> ISS->Internet Scanner 7.0 Service Pack 2->Internet Scanner

The first time you should receive a dialog informing you of a license being installed. This is normal – click “OK”. In the next window click “Cancel”.

Add a known admin account to Internet Scanner:

From the Tools menu, select “Edit Known Accounts…”
Click “Add…”
Enter a user name and password of a local admin account on your XP machine in the appropriate fields.
Click the “Verified” and “Local Account” check boxes and then enter the Machine Name of your XP machine in the Machine Name field.
This will allow Internet Scanner to perform checks that require admin access.

Launch a scan against your Windows machine:

From the “File” menu select “New Session”. Select the “L5 Server” policy and click “Derive New Policy….” Name it whatever you like and click OK. The policy opens. Explore the policy, observing the capabilities of Internet Scanner. Note that you can click on the Categorize button (the blue stair step looking icon) and change the hierarchy of the way the checks are displayed (helpful for sorting through 1400+ checks).

Click Next, Next, and in the “Enter the Host Range to Scan” window, enter the IP of your XP machine. Click Finish.

To start the scan, select “Scan Now” from the Scan menu.

What vulnerabilities did Internet Scanner find? Did scanner correctly identify the OS?

Generate a report:

From the “Reports” menu, select “Generate Report”.
Choose Technician->Vulnerability Assessment->Vulnerability Assessment Sorted by IP Address and click “Next”.
Select the session for the scan you just ran and click “Next”.
Click “Preview Report” to look at it immediately.
Click “Print Report” to print a copy to turn in with the lab.

Here are some example outputs:
**Session Information**

**Session 20060903_134056.npy**

**Source:**

**Name:** Session

**Policy:**

4865727704-7002-4271-74528f3ea320b02711401

**License:**

Copy of XML Server

**Host Scans:**

1

**Host Specific:**

**Scan Start:** 8/31/2006 1:09:34 PM

**Scan End:** 8/31/2006 1:40:55 PM

**Comment:**

**Operating System**

Microsoft Windows XP Professional

57356.128 (group=9112-128)

**Admin Access:**

No

**WinAsn1 BoNdtmDetected:** Microsoft Windows ASN.1 buffer overflow packet using NTLM has been detected

(CAN-2003-0818)

**Additional Information**

**More Information:**

A specially-crafted ASN.1 packet containing an invalid length that has been sent to an smtp port has been detected. Microsoft Windows NT, Windows 2000, Windows XP, and Windows Server 2003 are vulnerable to a buffer overflow in Microsoft's implementation of the Abstract Syntax Notation 1 (ASN.1) library. ASN.1 is the language used to standardize data across multiple platforms. A remote attacker could exploit this vulnerability to overflow a buffer and execute arbitrary code on the system with system privileges.

**Remedies:**

Apply the appropriate patch for your system, as listed in the Microsoft Security Bulletin MS04-007. See References.

**References:**

II Introduction Attack Tool Kit

Earlier in this lab, you tested a couple port scanning and vulnerability tools such as NMAP, Nessus, and Superscan.

The following is another vulnerability scan tool like NMAP, Nessus, and Superscan. The tool is ATK, abbreviated for Attack Tool Kit. This tool is most similar to Nessus in that it has a list of known vulnerabilities that it goes through and tries. In fact, many of the plugins are derived from Nessus and can be referenced by Nessus number. Using this tool we were able to scan our RedHat 7.3 installation and it generated a detailed vulnerability list.

Where to get it
http://www.computec.ch/projekte/atk/

What the tool does
As mentioned before, the tool is very similar to Nessus in that it performs “attacks” on a target host system to determine whether or not the system has a vulnerability. If a vulnerability is found, ATK will issue a prompt such as the one shown in Figure 1 below.

![Figure 1. Example vulnerability prompt](image-url)
The ATK tool also outputs a detailed list of all the vulnerabilities checked and which ones failed and which ones passed. An example of this report can be seen in Figure 2 shown below.

![Figure 2. Vulnerability Report](image)

**Using/Configuring ATK**

Using/configuring ATK is quite simple and straightforward. Download the latest version from the ATK website mentioned above and extract the files to a folder. Open the ATK executable and click on the config button located on the toolbar. This brings up the configuration screen and allows scan options to be set. The screen should look like Figure 3 below.

![Figure 3. Configuration window](image)
Enter the target host IP address or domain name. Then use the subsequent tabs to indicate the amount of detail you want the scan to be. For this lab, we can just use the default preferences. Close the window and save changes. Now, we can start the scan by clicking the start icon on the top toolbar.

After ATK finishes scanning, it should tell you what vulnerabilities were found. Click report on the top toolbar to view a detailed report. The report window should contain three tabs. If you click on the statistics button, you should see something like Figure 4 below.

![Figure 4. Statistics of Vulnerability Scan](image)

The report data should look like Figure 2 in the previous section of the lab.

Also included is an example report which lists the vulnerabilities and gives a detailed description of each vulnerability found.
LANspy

LANspy is a good tool for windows to use for network scanning. This tool can be downloaded from [http://lantricks.com/lanspy](http://lantricks.com/lanspy). After downloading this tool install on your Windows XP virtual machine.

Open the program. It will look like this:

After tool is open go to File -> Options:

Once there go to Port scanning ->TCP

This option allows you to change what ports are scanned in your scanning. You can select the full port range or just go to add and add port 32769 and click ok then press ok again to get back to main screen:
Next, type in the host IP address in the field at the top and press the arrow to the left of the field to start the scan.

LanSpy is made for gathering the following information about a remote computer:

- Ping
- Domain name
- NetBios names
- MAC address
- Server information
- Domain (working group) information
- Domain controllers
- Remote control
- Time
- Disks
- Transports
- Users
- Logged users
- Global groups
- Local groups
• Security options
• Shared resources
• Sessions
• Open files
• Services
• Processes
• Registry
• Event log
• TCP ports
• UDP ports

This information can be important to display vulnerabilities.
The cheops-ng program is the child (or second generation offspring) of the original cheops tool listed in *Hacking Exposed 5th Edition*. Cheops-ng is a fully automated network mapping utility that its developers have dubbed “the network swiss army knife” (http://cheops-ng.sourceforge.net/). Both cheops and cheops-ng do not add any new functionality, but rather bundle a myriad of other network tools together (QueSO, halfscan, and traceroute) under one GUI-driven interface.

While cheops-ng has some difficulties running & compiling on the RH4.0 host machine (due to a myriad of RPM dependencies), it can be executed on the RH7.2 virtual machine without too many problems. However, its functionality is limited to network mapping only. Normally, OS detection, port scans, and other options would be available. The reader may want to consider using the Knoppix STD LiveCD or a Debian-based Linux distribution if they intend on using cheops-ng to its fullest extent.

Load up the RH7.2 VM, a terminal, and proceed as follows:

```bash
>> cd /usr/local/bin
Start the cheops-agent
>> ./cheops-agent
Now start cheops-ng in another terminal window
>> cd /usr/local/bin
>> ./cheops-ng
```

Type in `127.0.0.1` as the IP address of the server to connect to, if requested.

Go to **File–>Menu** and select **Add Host**. Type in your host IP address (57.35.6.x)

Go to **File–>Menu** and select **Add Network Range**. Type in 138.210.230.1 as the First IP and type in 138.210.240.254 for the Last IP.

You should see a map (albeit messy) of the network setup. Move some of the computer icons around so you can see the interconnections. **Include a screenshot which shows the connectivity between the 57.35.6.0/24 domain and 138.210.230-240.0/19 subnet.**

Look at the GTISC Mini-Net diagram on the wall of the laboratory or at http://users.ece.gatech.edu/~owen/GTISC/Dec15,%202003.jpg and see if you can identify the routers, computers, etc.

Normally, OS detection and automatic map placement is a feature in cheops-ng, but as we mentioned before, support is buggy even in RH7.2. One could use the Knoppix STD LiveCD, but the Broadcom Ethernet card presents some problems.

One of the disadvantages of the cheops-ng tool is its lack of SNMP sniffing. The original cheops tool included SNMP sniffing, which allowed for automatic network detection. As mentioned before, cheops-ng only bundles tools together, and does not present anything new.
Cheops Example Output
V. EtherApe

EtherApe combines packet sniffing and a GUI interface together (again, nothing new is introduced). Traffic type, direction, and activity are depicted in an easy-to-under interface. EtherApe requires physical access to the network to sniff packets, but can also read in a tcpdump file that has been previously recorded.

We will use the Knoppix STD LiveCD in order to run EtherApe. To get around the problems associated with the broadcom Ethernet adapter, we will be running the ISO under VMWare.

Steps:
Obtain a copy of the Knoppix STD LiveCD from the TA.
Pop it in the CD-ROM drive
Open up VMware
Go to File->New->Virtual Machine
Select Typical
Next
Linux as Guest Operating System
Other Linux as Version
Next
(If asked about Network connection, select Next)
(If asked about Disk Space connection, just select Next)

Type in KnoppixSTD as the name.
Power on the Virtual Machine

Once the KnoppixSTD Logo appears (a somewhat evil-looking cat with a watch), hit Enter.

Wait one or two minutes. Once you see the KnoppixSTD logo again:
Right-click (this should bring up the fluxbox menu)
Go to Network Utilities->etherApe

Right-click again (this should bring up the fluxbox menu)
Go to XShells->Root Aterm
Type ifconfig

If eth0 shows up (and has an IP address identical to your RH7.2 VM):
Type ifconfig eth0 57.35.6.x+4, where x is the last octet of your RH4.0 host machine IP address

If eth0 does not show up
Type ifconfig eth0 57.35.6.x+4, where x is the last octet of your RH4.0 host machine IP address. If this produced error, see a TA.

Go back to the etherApe window. You will notice capturing is started automatically.

Go to the terminal window and perform a ping on some machine in the network (say NAS, which is located at 57.35.6.10).
Example etherape output
**VII Intermapper**

**Intermapper is a commercial tool that may be used under Linux, Windows, and Mac OS X (a UNIX-port) for graphical network mapping. Again, discovery is mostly done with well-established methods (i.e. pinging or tracerouting).**

InterMapper employs a variety of highly reliable methods for discovering and reporting on your networked equipment.

- Any device with an IP address can be pinged
- Traffic on Routers and switches can be monitored using versions SNMPv1, SNMPv2c, or SNMPv3
- Nearly 100 built-in probes can test the health and performance of various kinds of servers, routers, switches, UPSs, environmental monitors and other networked equipment.
- Synthetic transactions test mail, web, and directory servers from over 50 vendors
- Windows NT services are monitored directly
- Host resource probe monitors CPU and disk activity as well as free space on drives.
- LDAP and LDAP-SSL probes support an optional password when binding, allow you to specify an alternate search field, and can trigger an alarm if an insufficient number of records are returned
- Custom probes can be created to test TCP or SNMP-speaking devices
- Command line probes test devices using a program or script. Pre-written Nagios™ and Big Brother™ plug-ins/scripts can be used as command line probes.

1. Go to java.sun.com/javase/downloads and download the Java Runtime Environment (JRE) to a removable disk to take into the lab.
2. Go to http://dartware.com/downloads/binaries/ and download the Windows binary file of Intermapper to a removable disk to take into the lab

**Installation**

- Transfer files from removable disk to the host machine and then into the Windows virtual machine. This can be done using samba on the host machine and enabling sharing in Windows virtual machine.

**JAVA Installation**

- Double-click on the Java Runtime Environment binary to begin installation of JAVA.
- Click Continue
- Click Accept to accept the software license
- Click Finish to return to the computer

**Intermapper Installation**

- Double-click on the Intermapper installation binary.
- Click Next
- Accept the terms of the license agreement and click Next.
- Select Complete and click Next
- Click Install

Using Intermapper
Intermapper will start automatically after install: if you need to open do one of the following:
- Right-click the Intermapper System tray icon and select start intermapper service.
- Click Start->All Programs->Intermapper-Intermapper

Creating a Network Map

- Once the program has started click “Try it!” to use the trial period.
- You may close the example.com map that may appear.
- (Ctrl+N) From the Map List, select the file tab and then “New Map”
- Name the map ECE4112 Lab
- Select Autodiscovery and click Next.
- Leave the default hostname, but unselect the “stay within x hops” option.
- Click Start Discovery.

Icon View (Ctrl+1)

- The network map should now display the 57.35.6.0/24 subnet.
- This mode provides a graphical overview of how devices are connected and the traffic flow between devices that it can see.
- You will probably see dashed lines representing traffic between NAS and the main subnet router. If not pull some data from NAS and it will appear.

List View (Ctrl+2)

- This mode displays network node information in the form of a list.
- By clicking View from the menu bar and then List the viewing mode will switch to List mode.
- This mode provides easy methods to sort through the data in the menu under View->Sort and View->Filter options.

Notifier View (Ctrl+3)

- By clicking View from the menu bar and then Notifiers the viewing mode will switch to Notifier mode.
- This mode provides easy information about the status of each node.

Viewing Options

- Right clicking on a node and selecting “Info Window” will display the label for the node, the IP address, the probe type, and operating system specific information.
- Right clicking on a node and selecting “Status Window” will display much of the same information, but also network availability statistics.
- Right clicking on a node and selecting “Helper Apps” will launch other tools for you using the information provided by node.

Exporting Data

- Images can be exported as a PNG file using the File->Export->Image option.
- Raw Data can be exported using the File->Export->Data option.
Appendix E: Sharing files between Virtual Machines

If a file needs to be transferred between virtual machines you may do so using the shared folders available through VMWare tools. To do this for example with two XP virtual machines (as a general example):

1. Right-click on the WinXP virtual machine tab in VMWare and click Settings. Now click on the Options tab. Click on Shared Folders and make sure that it is enabled. If it isn’t, check the Enable Shared Folders checkbox. Now click Add… near the bottom of the window and select the folder which you want to share (suggestion: you might want to create and share a directory called root/vmware/shared). Enter a name for the shared resources (“Shared Folder”).
2. Repeat the above for the XPPro Copy machine.
3. Now right click on My Computer in the XPPro machine and click Tools->Map Network Drive.
4. Use the default drive letter for “Drive:” and click Browse to locate the shared folder.
5. Expand VMWare Shared Folders and select the folder which you shared in step 1.
6. Repeat step 4 for the XP Copy machine.

Now, anything copied to the network drive will be available to both machines.

Here is another explanation:

1. Make sure that the virtual machine is “Powered Off” (not just suspended).
2. In the menu go to VM – Settings
3. Click on the Options tab
4. Select “Shared Folders”
5. Click “Add…”
6. Name it however you would like.
7. Enter the path of the folder on the host machine that you want to make available to the virtual machine. Typing in “/” will make the entire host filesystem available.
8. Make sure “Enable this share” is selected, and click OK.
9. Click OK again.
10. Power up the virtual machine.

In Linux, the share appears under /mnt/hgfs
In Windows, access it by typing //host/Shared Folders in the run box of in the explorer address bar.
Appendix F: *Sam Spade Tool (Windows XP)*

The Sam Spade software tool is actually created to track down and report spammers on the Internet. However, this is an excellent reconnaissance tool that is able to look at various whois servers at once and determine information that would be useful to a network security administrator or a hacker.

There is a Windows version of the tool available for download at [http://www.samspade.org/](http://www.samspade.org/). However do not set up this tool in our lab because there is nothing to look at if you do get the tool. Instead if you want to use this tool, use the tool from a machine connected to the Internet by going to

http://www.samspade.org/t/

An example of a whois search on ISS.net is shown below.
Figure 1 – An example of a whois search for “iss.net”.
Appendix G: Bastille Linux and Cheops

Bastille Linux is a hardening system that attempts to tighten security on Unix operating systems. The Bastille system supports the Red Hat, Debian, Gentoo, Mandrake, SuSE, TurboLinux, HP-UX and Mac OS X operating systems. Bastille Linux runs a series of scripts that address security issues related to your system’s File Permissions, Account Security, Boot Security, etc. Unlike Nessus and other vulnerability scanners, Bastille Linux identifies vulnerabilities and tries to educate the administrator about each of the security issues involved in each of its scripts tasks. Each step is optional and contains a clear description of the security issues involved.

Bastille Linux goes a step further than Nessus and other tools by providing utilities that help secure your UNIX system. For example, bundled with Bastille is the Port Scan attack Detector (PSAD) which analyzes information gathered in firewall logs to determine whether or not someone is scanning your machine. PSAD features a set of flexible thresholds (with sensible defaults provided) that are used to define what constitutes a port scan, detection for advanced port scans (syn, fin, Xmas) that are easily leveraged against a machine via nmap, email alerts that contain the source and destination ip addresses, the range of scanned ports, begin and end times, tcp flags set in the scanning packets (2.4.x kernels only), reverse dns and whois information, and more.

Bastille Linux can be found at http://www.bastille-Linux.org

We will not install Bastille Linux in our systems in the lab because of the attacks which we will run in future labs which might not be possible with Bastille Linux installed.

You have already used ping to see what systems are on your “network”. Using ping coupled with the tool traceroute (unix) tracert (windows) manually allows you to map a network. Let’s look at an automated tool for network mapping that draws a nice picture of the target network. You can find this tool on your own at http://cheops-ng.sourceforge.net/ That page says: “Cheops-ng is a Network management tool for mapping and monitoring your network. It has host/network discovery functionality as well as OS detection of hosts. Cheops-ng has the ability to probe hosts to see what services they are running. On some services, cheops-ng is actually able to see what program is running for a service and the version number of that program”.

We are no longer using Cheops in the lab because it does not work as well as it promises on the web site.
Appendix H: Firestarter firewall for Linux (similar to Win XP firewall)

This lab had explored firewalls for windows briefly and how a network administrator may be able to detect hackers. This addition would do the same for Linux. Students would learn about the concept of firewalls for Linux and how to monitor active connections to a Linux machine and a way to detect vulnerability scanning or port scanning.

This tool defends against vulnerability scanning and port scanning.

**BACKGROUND**

From the Firestarter website ([http://www.fs-security.com/docs/introduction.php](http://www.fs-security.com/docs/introduction.php)):

Firestarter is an open source visual firewall program. The software aims to combine ease of use with powerful features, therefore serving both Linux desktop users and system administrators.

We strongly believe that your job is to make the high level security policy decisions and ours is to take care of the underlying details. This is a departure from your typical Linux firewall, which has traditionally required arcane implementation specific knowledge.

**INSTRUCTIONS**

Obtain Firestarter from the Internet from [http://www.fs-security.com/](http://www.fs-security.com/)
Transfer it to your usb drive
Plug the usb drive into your host machine

From your **host**:
Double click on the rpm file you just downloaded and follow the prompts to install Firestarter
Go to Applications > System Tools > Firestarter
Click Forward, Forward, Forward, and Save
The Firestarter gui should pop up
Click on Active Connections so that any activity may be viewed

From your **Linux virtual machine**:
Start a nessus scan on your host

On your **host**:
Notice that Firestarter has logged all the packets in the Events tab as Nessus is running.

Also notice the change in the firestarter icon on the upper right hand corner of your host machine to warn you that an attack is in progress.

Before you complete this exercise, make sure to stop the firestarter firewall using the GUI.
QUESTIONS

Q. What was the difference between scanning the Windows machine with firewall and scanning Linux with firestarter?

Ans: Nessus takes a lot longer to scan Linux with firestarter. The reason for this is that firestarter drops the packets silently, instead of rejecting them like Windows.

Q. Name five services that Nessus had attempted to exploit.

Ans2: http, ftp, samba, amanda, dns, dhcp, ssh, netbust2, nntp, tempo, Ntalk, echo, tftp, kpasswd, sql.

FIGURES OF FIRESTARTER

Figure 1: Firestarter Status Tab

Figure 2: Firestarter Events Tab during Nessus vulnerability scan
<table>
<thead>
<tr>
<th>Time</th>
<th>Port</th>
<th>Source</th>
<th>Protocol</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep 3 11:25:12</td>
<td>5</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Rdp</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>3</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>2</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>7</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>1</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>40</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>HTTP</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>11</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Java</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>21</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Ftp</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>31</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>41</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>51</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>61</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>110</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Netcat</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>119</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Nmap</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>146</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>198</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>286</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>289</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>290</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>291</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>300</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>317</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>319</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>320</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>321</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>322</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>40</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>410</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>411</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>412</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>413</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>414</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>518</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>594</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>682</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sep 3 11:25:12</td>
<td>683</td>
<td>77.35.6.122</td>
<td>TCP</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
Appendix I: Microsoft Security Baseline Analyzer

Vulnerability scanning for a windows system (similar to nessus vulnerability scanning for Linux).

Search for various vulnerabilities in Windows.

BACKGROUND

Just like Nessus vulnerability scanner is used to analyze vulnerabilities in Linux, this is a windows tool to detect vulnerabilities in your OS.

From the website (http://www.microsoft.com/technet/security/tools/mbsahome.mspx):

Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed for the IT professional that helps small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. Improve your security management process by using MBSA to detect common security misconfigurations and missing security updates on your computer systems.

INSTRUCTIONS

To Install Microsoft Security Baseline Analyzer do the following on the Windows Virtual Machine:

Right click on My Computer > Tools > Folder options
Click the View tab
Uncheck use simple file sharing and click Ok
Right click on C: and select sharing and security
make sure 'share this folder' is selected
Note the share name C$
Go to start and then right click on My Computer and select Manage
Click on the + sign next to Local Users and Groups and click on the Users folder
In the right side window, right click on administrator and click set password
Click proceed on the warning, and set the password to "password"

In the Host machine, open a terminal and enter:

    mkdir /root/windowsSMB
    mount -t smbfs username=Administrator //57.35.6.x+3/C$ /root/windowsSMB

Enter the password when prompted (it may take around 30 secs to connect)
Obtain the MBSASetup-EN.msi from the Microsoft website at http://www.microsoft.com/downloads/details.aspx?familyid=b13ebd6b-e258-4625-b0a3-64a4879f7798&displaylang=en
Download the file into your usb key
Use a usb key to transfer the file to the host machine in the directory /root/windowsSMB in your host machine

In the virtual machine:
Go to C:
Install the MBSASetup-EN.msi package following the instructions
Launch the MBSA tool from the desktop
Click Scan Computer
Select your computer from the dropdown list or enter your ip address (if necessary)
Uncheck "Check for Security Updates"
Click on Start Scan
Wait for the scan to complete
For any critical errors (marked by a 'X') click the What was scanned, Result Details, and How to correct this links

To unmount the windows share, Type:
`umount /root/windowsSMB`

In the windows virtual machine:
Go to Start > My Computer > Tools Menu > Folder Options
Click the View Tab and click use simple file sharing
Click on ok.

QUESTIONS

Q: What vulnerabilities did the MBSA find?

Ans: Some user accounts have blank or simple passwords
Automatic updates has not been configured
Windows firewall is disabled
Some unnecessary services are installed
Two file shares are present

Q: What did MBSA recommend to make the system more secure?

Ans: Adopt a strong password policy, enable and configure automatic updates, enable windows firewall, disable services that should not be running on the computer, and remove shares that are not needed
Appendix J: fping

Detecting alive systems at a number of ip addresses using a file as opposed to specifying a range in nmap. The output of fping is easy to parse and can be used in scripts.

Defenses:
One can use a firewall to block incoming ICMP packets.

BACKGROUND

From http://fping.sourceforge.net/

fping is a ping(1) like program which uses the Internet Control Message Protocol (ICMP) echo request to determine if a host is up. fping is different from ping in that you can specify any number of hosts on the command line, or specify a file containing the lists of hosts to ping. Instead of trying one host until it timeouts or replies, fping will send out a ping packet and move on to the next host in a round-robin fashion. If a host replies, it is noted and removed from the list of hosts to check. If a host does not respond within a certain time limit and/or retry limit it will be considered unreachable.

Unlike ping, fping is meant to be used in scripts and its output is easy to parse.

INSTRUCTIONS

Obtain fping from the internet for redhat and transfer it to your host machine. Fping can be found at http://fping.sourceforge.net/

Double click on the rpm to install

Type fping --help in the terminal to make sure that the package is installed

In a text editor, create a list of ip addresses such as:

57.35.6.x
57.35.6.x+1
57.35.6.x+2
57.35.6.x+3

Try the command:

fping -f filename.txt

where filename.txt is the name of the file you just created

Now go to your windows XP virtual machine and turn on the firewall.
Run the fping command again from your host.

Q: What is the difference in output between the first and second fping scans?

Ans: The Windows XP destination machine status has changed from alive to unreachable.
FIGURE

[root@group6 lab1]# fping -f ips.txt
57.35.6.111 is alive
57.35.6.112 is alive
57.35.6.113 is alive
57.35.6.114 is alive
[root@group6 lab1]#
Appendix K: SNMP enumeration in windows

It may be possible for a hacker to gain useful information about the vulnerabilities of a system using default SNMP configurations on equipment.

Defense is to block the SNMP ports, disabling the SNMP service or by setting the SNMP password.

References and Attributes:

For this addition, we used SUN Java 6 (http://java.sun.com), and the Ireasoning MibBrowser (http://www.ireasoning.com/).

To get the mibbrowser running, the launch script must be modified to point to the java version installed by students using the following instructions. This should be done once for the version of the mibbrowser placed on NAS.

BACKGROUND

SNMP, or the Simple Network Management Protocol is a simple query and set protocol used for the monitor and control of various networked devices. Cisco routers, Dell and HP servers, and many other types of devices all implement SNMP so that administrators can easily configure and monitor these devices remotely over the network. When it is not properly secured or disabled however, it can just as easily be used by hackers to obtain valuable information about a network and networked devices.

INSTRUCTIONS

• Obtain the Java Linux self-extracting file from NAS and transfer to your host machine. Place the file in /root.
• Open a terminal and type the following:
  1.cd /root
  2./jre-6u2-linux-i586.bin
• Follow the prompts to extract linux to the root directory.
• Obtain the MibBrowser from NAS, and place the mibbrowser folder in /root.
• Run the MibBrowser from a terminal by typing:
  1.cd /root/mibbrowser
  2./browser.sh
• In the “Address” field, type the IP address of NAS (57.35.6.10)
• In the “Operations” pull-down menu, select “Walk”
• Click “Go” if necessary.

QUESTIONS

Q. What kind of information could be learned from this type of tool?

ANS: Running Service Names, Share Names, User Names, NIC Addresses, IP Addresses, Operating System, Hardware Info, and Port Status
Q. How might a Hacker use this information?
ANS: A hacker could learn which services the machine has, and then exploit known vulnerabilities, try to brute force listed accounts, attack ports in listen state, etc.

Q. How could a system administrator prevent against this vulnerability? Would it be possible to make this data more secure?
ANS: A system administrator could disable the snmp service, or if snmp was needed, change the snmp key.

Security implications (www.wikipedia.org)

1. SNMP versions 1 and 2c are subject to packet sniffing of the clear text community string from the network traffic, because they do not implement encryption.
2. All versions of SNMP are subject to bruteforce and dictionary attacks for guessing the community strings/authentication strings, because they do not implement a challenge-response handshake.
3. Although SNMP works over TCP and other protocols, it is most commonly used over UDP which is connectionless and vulnerable to IP spoofing attacks. Thus, all versions are subject to bypassing device access lists that might have been implemented to restrict SNMP access, though SNMPv3's other security mechanisms should prevent a successful attack.
4. SNMP's configuration (write) capabilities can be misconfigured and used to cause much damage. These 'write' capabilities are very rarely used in practice, due to lack of security in SNMP versions before SNMPv3. This lack of security is particularly serious with SNMPv1 or v2c over UDP - clear text community strings can be intercepted and combined with IP spoofing.
5. SNMP tops the list of the SANS Institute's Common Default Configuration Issues with the issue of default SNMP community strings set to 'public' and 'private' and is number ten on the SANS The Top 10 Most Critical Internet Security Threats for the year 2000.
Appendix L: Port Scanner Python Script

Students can learn how a port scanner is made. Students can also execute the port scanner and compare the results with nmap.

This concept exploits port scanning. The defense would be to setup a firewall, or stop unwanted services.

References and Additions

We obtained the Python script from the ActiveState ASPN cookbook, which can be found online at (http://aspn.activestate.com/ASPN/Cookbook/Python/Recipe/286240).

BACKGROUND

In this lab, we've already used a port scanner, and learned about what kind of information it can tell the user, as well as how that information can be used to exploit vulnerabilities. This section is designed to show students how this kind of utility could be written using the Python programming language.

INSTRUCTIONS

Download the python script from the NAS-storager
Place it in the /root directory
Open a terminal and type:

```python /root/pyScan.py ipaddress```
where ipaddress is your target ip address, preferably 57.35.6.x+1/x+2

QUESTIONS

Q. Name the open ports at each of the machines?
Ans: x+1: 111, 139
    x+2: 139, 135, 445
    May be different based on open ports

Q. What are the services associated with each of these ports (use Google)?
Ans: Various based on open ports.

Q. Take a look at the python script, specifically the scanner class. How does this script decide if ports are open?
Ans: It makes a TCP connection to the host specified on the range of ports that were specified by the user. If the connection is successful then the port is open.

Q. How could you defend against this kind of attack?
Ans: Enable a firewall

Python Script:

```python
# a simple portscanner with multithreading
```
import socket as sk
import sys
import threading
import thread

MAX_THREADS = 1000

def usage():
    print "\npyScan 0.1"
    print "usage: pyScan <host> [start port] [end port]"

class Scanner(threading.Thread):
    def __init__(self, host, port):
        threading.Thread.__init__(self)
        # host and port
        self.host = host
        self.port = port
        # build up the socket obj
        self.sd = sk.socket(sk.AF_INET, sk.SOCK_STREAM)

    def run(self):
        try:
            # connect to the given host:port
            self.sd.connect((self.host, self.port))
            print "%s:%d OPEN" % (self.host, self.port)
            self.sd.close()
        except: pass

class pyScan:
    def __init__(self, args=[]):
        # arguments vector
        self.args = args
        # start port and end port
        self.start, self.stop = 1, 1024
        # host name
        self.host = ""

        # check the arguments
        if len(self.args) == 4:
            self.host = self.args[1]
        try:
            self.start = int(self.args[2])
            self.stop = int(self.args[3])
        except ValueError:
            usage()
            return
        if self.start > self.stop:
            usage()
            return
elif len(self.args) == 2:
    self.host = self.args[1]
else:
    usage()
    return

try:
    sk.gethostbyname(self.host)
except:
    print "hostname '%s' unknown" % self.host
    self.scan(self.host, self.start, self.stop)

def scan(self, host, start, stop):
    print "About to Scan Host: %s, Start: %s, Stop: %s" % (host, start, stop)
    self.port = start
    while self.port <= stop:
        #print "port= %s, stop= %s" % (self.port, stop)
        if threading.activeCount() < MAX_THREADS:
            Scanner(host, self.port).start()
            self.port += 1
        else:
            print "%s threads in use" % (threading.activeCount())
            print "ERROR: MAX_THREADS limit reached. Either change this value in the script, or scan less ports at a time."
            exit(1)

if __name__ == "__main__":
    pyScan(sys.argv)
FIGURE
Appendix M: VMware cloning

create a clone using the Clone Virtual Machine Wizard:

1. Select the virtual machine you want to clone.

   Click the name of a virtual machine in the Favorites list or click the tab of a virtual machine in the summary window.

2. Open the Clone Virtual Machine Wizard (VM > Clone) and click Next.

3. Select the state of the parent from which you want to create a clone, and click Next.

   You can choose to create a clone from either of two states.

   - From the parent's current state (Workstation creates a snapshot of the virtual machine before cloning it)
   - From any snapshot of the parent: select the snapshot name from a drop-down menu of existing snapshots.

4. Select the type of clone you want to create and click Next.
You can choose to make a full clone or a linked clone. See Full and Linked Clones for a description of the differences.

5. Type a name and a path for the cloned virtual machine, and click Finish.

![Clone Virtual Machine Wizard](image)

The default name and path are based on the original virtual machine name and location. You can type a new entry for name and path, or use the Browse button to locate a directory for the clone files.

After you have verified your entries, click Finish. The Clone Virtual Machine Wizard then displays a status page.

![Status page](image)

A full clone can take many minutes to create, depending on the size of the virtual disk that is being duplicated.

6. Click Done to exit the Clone Virtual Machine Wizard.
Appendix N: General Linux Tips

The purpose of this section is to give students that are new to the Linux Operating System some general tips on using Linux.

Typing Long Filenames

The student should have noticed by now that a large majority of files in Linux have very long filenames. It is however not necessary to type out the entire filename. The student can use the <TAB> key to complete filenames. For example, if you

Understanding Installation Filenames

Files ending with the extension ‘.gz’, means that it is a gnu-zipped file. This is a form of data compression not unlike WinZip. To create your own gzip files, use the command ‘gzip’.

*NOTE: Please review the Linux Commands section or the man documentation provided in Linux for the various options (sometimes referred to as switches) that can be used with this and all subsequent commands.

Files ending with the extension ‘.tar’, means that the file has been tar-red. This is also just another form of data compression.

Files ending with the extension ‘.tgz’, means that the file has been tarred and gnu-zipped. This is also just another form of data compression.

Installation Instructions

Most installation files when uncompressed have README or INSTALL files. These provide information on how to install the files.

The ‘make’ command compiles source files. The ‘make install’ command installs the compiled source to their appropriate directories.

Virtual consoles

The system's console is the monitor and keyboard connected directly to the system. (Because Linux is a multi-user operating system, you may have other terminals connected to serial ports on your system, but these would not be the console.) Linux provides access to virtual consoles (or VCs), that let you have more than one login session on the console at one time. To demonstrate this, log in to your system. Next, press <ALT>+<F2>. You should see the login: prompt again. You're looking at the second
virtual console. To switch back to the first VC, press <ALT>+<F1>. The Linux system we will be using lets you access six VCs, by pressing <ALT>+<F1> through <ALT>+<F6>. It is possible to enable up to 12 VCs—one for each function key on your keyboard. As you can see, use of VCs can be very powerful because you can work in several different sessions at the same time. While the use of VCs is somewhat limiting (after all, you can look at only one VC at a time), it should give you a feel for the multi-user capabilities of Linux. While you're working on the first VC, you can switch over to the second VC and work on something else.

**Changing your password**

The command ‘passwd’ will prompt you for your old password, and your new password. It will ask you to reenter the new password for validation. Be careful not to forget your password!!

**Getting Online Help**

Almost every UNIX system, Linux included, provides a facility known as ‘manual pages’, or ‘man pages’ for short. These man pages contain online documentation for all of the various system commands, resources, configuration files, and so on. The command used to access man pages is man. For example, if you're interested in finding out about the other options of the ‘ls’ command, you can type ‘man ls’ and the man page for ‘ls’ will be displayed. Unfortunately, most of the man pages out there are written for those who already have some idea of what the command or resource does. For this reason, man pages usually only contain the hardcore technical details of the command, without a lot of tutorial. However, man pages can be an invaluable resource for jogging your memory if you forget the syntax of a command. You'll notice some of commands won't have man pages. This could be for several reasons. For one, the man pages haven't been written yet. Secondly, the command might be an internal shell command, or an alias, in which case it would not have a man page of its own. One example is ‘cd’, which is a shell internal command. The shell actually processes the ‘cd’—there is no separate program which contains this command.

**Using the vi Editor**

You will want to use the GUI based text editors whenever they are available, however sometimes this may not be the case. In that situation, you will want to use vi. While using vi, at any one time you are in one of three modes of operation. These modes are known as command mode, insert mode, and last line mode. When you start up vi, you are in command mode. This mode allows you to use certain commands to edit files or to change to other modes. For example, typing ‘x’ while in command mode deletes the character underneath the cursor. The arrow keys move the cursor around the file, which
you're editing. Generally, the commands used in command mode are one or two characters long.

You actually insert or edit text within insert mode. When using vi, you'll probably spend most of your time within this mode. You start insert mode by using a command such as ‘i’ (for insert) from command mode. While in insert mode, you are inserting text into the document from your current cursor location. To end insert mode and return to command mode, press <ESC>.

Last line mode is a special mode used to give certain extended commands to vi. While typing these commands, they appear on the last line of the screen (hence the name). For example, when you type ‘:’ from command mode, you jump into last line mode, and can use commands such as ‘wq’ (to write the file and quit vi), or ‘q!’ (to quit vi without saving changes). Last line mode is generally used for vi commands which are longer than one character. In last line mode, you enter a single-line command and press <ENTER> to execute it.

The best way to understand these concepts is to actually fire up vi and edit a file. In the example ‘screens’ below, we're only going to show a few lines of text, as if the screen was only six lines high (instead of twenty-four). The syntax for vi is

    vi <filename>

where <filename> is the name of the file that you wish to edit.

Start up vi by typing

    vi test

which will edit the file test. You should see something like

```
|~_|
|~|
|~|
|~|
|~|
"test"_[New_file]_____________________________________________
```

The column of ‘~’ characters indicates that you are the end of the file.

**Inserting text**
You are now in command mode; in order to insert text into the file, press ‘i’ (which will place you into insert mode), and begin typing.

| Now is the time for all good people to come to the aid of the party._ |
| ~ |
| ~ |
| ~ |
| ~ |
| ~ |
| ~ ________________________________ |

While inserting text, you may type as many lines as you wish (pressing <ENTER> after each, of course), and you may correct mistakes using the backspace key. To end insert mode, and return to command mode, press <ESC>. While in command mode, you can use the arrow keys to move around the file. Here, because we only have one line of text, trying to use the up- or down-arrow keys will probably cause vi to beep at you. There are several ways to insert text, other than using the ‘i’ command. For example, the ‘a’ command inserts text beginning after the current cursor position, instead of on the current cursor position. For example, use the left arrow key to move the cursor between the words ‘good’ and ‘people’.

| Now is the time for all good_people to come to the aid of the party. |
| ~ |
| ~ |
| ~ |
| ~ |
| ~ |
| ~ ________________________________ |

Press ‘a’, to start insert mode, type ‘wo’, and then hit <ESC> to return to command mode.

| Now is the time for all good people to come to the aid of the party. |
| ~ |
| ~ |
| ~ |
| ~ |
| ~ |
| ~ ________________________________ |

To begin inserting text at the line below the current one, use the ‘o’ command. For example, press ‘o’ and type another line or two:

| Now is the time for all good people to come to the aid of the party. |
| Afterwards, we'll go out for pizza and beer._ |
Deleting text

From command mode, the x command deletes the character under the cursor. If you press <x> five times, you'll end up with:

```
|Now is the time for all good people to come to the aid of the party.
|Afterwards, we'll go out for pizza and _
|~
|~
|~
|~
```

Now press <a>, insert some text, followed by <ESC>:

```
|Now is the time for all good people to come to the aid of the party.
|Afterwards, we'll go out for pizza and Diet Coke._
|~
|~
|~
|~
```

You can delete entire lines using the command ‘dd’ (that is, press <d> twice in a row). If your cursor is on the second line, and you type ‘dd’,

```
|Now is the time for all good people to come to the aid of the party.
|~
|~
|~
|~
```

To delete the word which the cursor is on, use the ‘dw’ command. Place the cursor on the word ‘good’, and type ‘dw’.

---

- 76 -
Now is the time for all people to come to the aid of the hungry.

Changing text

You can replace sections of text using the ‘R’ command. Place the cursor on the first letter in ‘party’, press <R>, and type the word ‘hungry’.

Using ‘R’ to edit text is much like the ‘i’ and ‘a’ commands, but ‘R’ overwrites text, instead of inserting it. The ‘r’ command replaces the single character under the cursor. For example, move the cursor to the beginning of the word ‘Now’, and type ‘r’ followed by ‘C’, you'll have:

The ‘~’ command changes the case of the letter under the cursor from upper- to lower-case, and vise versa. For example, if you place the cursor on the ‘o’ in ‘Cow’, above, and repeatedly press <~>, you'll end up with:
Moving Commands

You already know how to use the arrow keys to move around the document. In addition, you can use the ‘h’, ‘j’, ‘k’, and ‘l’ commands to move the cursor left, down, up, and right, respectively. This comes in handy when (for some reason) your arrow keys aren't working correctly. The ‘w’ command moves the cursor to the beginning of the next word; the ‘b’ moves it to the beginning of the previous word. The ‘0’ (that's a zero) command moves the cursor to the beginning of the current line, and the ‘$’ command moves it to the end of the line. When editing large files, you'll want to move forwards or backwards through the file a screenful at a time. Pressing <CTRL>+<F> moves the cursor one screenful forward, and <CNTRL>+<B> moves it a screenful back. In order to move the cursor to the end of the file, type ‘G’. You can also move to an arbitrary line; for example, typing the command ‘10G’ would move the cursor to line 10 in the file. To move to the beginning of the file, use ‘1G’. You can couple moving commands with other commands, such as deletion. For example, the command ‘dS’ will delete everything from the cursor to the end of the line; ‘dG’ will delete everything from the cursor to the end of the file, and so on.

Saving Files and Quitting vi

To quit vi without making changes to the file, use the command: ‘q!’. When you type the ‘:’, the cursor will move to the last line on the screen; you'll be in last line mode.

In last line mode, certain extended commands are available. One of them is ‘q!’, which quits vi without saving. The command ‘:.wq’ saves the file and then exits vi. The command ‘ZZ’ (from command mode, without the ‘:’) is equivalent to ‘:.wq’. Remember that you must press <ENTER> after a command entered in last line mode. To save the file without quitting vi, just use ‘:w’.
Editing another file

To edit another file, use the `:e` command. For example, to stop editing test, and edit the file foo instead, use the command

```
|COW IS THE TIME FOR ALL PEOPLE TO COME TO THE AID OF THE HUNGRY.
|~
|~
|~
|~
|~
|~
: e foo
```

If you use `:e` without saving the file first, you'll get the error message

```
|No_write_since_last_change_(":edit!"_overrides)
```

which simply means that vi doesn't want to edit another file until you save the first one. At this point, you can use `:w` to save the original file, and then use `:e`, or you can use the command

```
|COW IS THE TIME FOR ALL PEOPLE TO COME TO THE AID OF THE HUNGRY.
|~
|~
|~
|~
|~
|~
:e! foo
```

The `!` tells vi that you really mean it---edit the new file without saving changes to the first.

Including Other Files

If you use the `:r` command, you can include the contents of another file in the current file. For example, the command

```
:r foo.txt
```

would insert the contents of the file foo.txt in the text at the current cursor location.
Running shell commands

You can also run shell commands from within vi. The ‘:r!’ command works like ‘:r’, but instead of reading a file, it inserts the output of the given command into the buffer at the current cursor location. For example, if you use the command

:r!  ls -F

you'll end up with

```
|COW IS THE TIME FOR ALL PEOPLE TO COME TO THE AID OF THE |
|HUNGRY. |
|letters/ |
|misc/ |
|papers/|
|~ |
|~ |
```

You can also ‘shell out’ of vi, in other words, run a command from within vi, and return to the editor when you're done. For example, if you use the command

:`! ls -F

the ‘ls –F’ command will be executed, and the results displayed on the screen, but not inserted into the file which you're editing. If you use the command

:`shell

vi will start an instance of the shell, allowing you to temporarily put vi ‘on hold’ while you execute other commands. Just logout of the shell (using the exit command) to return to vi.

Linux Commands

Here are some of the basic commands that will help the new Linux user.

*NOTE:* Be aware that commands are case-sensitive in Linux.

`cd`  
Change the current working directory  
Syntax: cd <directory>, where <directory> is the name of the directory you wish to change to.
ls  Displays information about the named files and directories
    Syntax:  ls <files>, where <files> consists of the filenames or directories to list

cp  Copies one or more files to another file or directory
    Syntax:  cp <files> <destination>, where <files> lists the files to copy and
             <destination> is the destination file or directory

mv  Moves one or more files to another file or directory. This is the
     equivalent of the cp command followed by the deletion of
     the original file. This command can be used to rename files.
    Syntax:  mv <files> <destination>, where <files> lists the files to move
             and <destination> is the destination file or directory

rm  Deletes files.
    Syntax:  rm <files>, where <files> are the files to be deleted

mkdir  Creates new directories
    Syntax:  mkdir <directoryname>, where <directoryname> is the name of
             the directory you wish to create

rmdir  This command deletes empty directories. When using rmdir, your
       current working directory must not be within the directory to be
       deleted.
    Syntax:  rmdir <dir1> <dir2> ... <dirN>, where <dir1> through <dirN> are
             the directories to delete.

man  Displays the manual page for the given command or resource (that is,
     any system utility which isn't a command, such as a library
     function.)
    Syntax:  man <command>, where <command> is the name of the
             command or resource to get help on.

more  Displays the contents of the named files, one screenful at a time.
     Syntax:  more <file1> <file2> ... <fileN>, where <file1> through
             <fileN> are the files to display.
cat  Officially used to concatenate files, cat is also used to display the entire contents of a file at once.
Syntax:  cat <file1> <file2> ... <fileN>, where <file1> through <fileN> are the files to display.

grep  Display all of the lines in the named file(s) matching the given pattern.
Syntax:  grep <pattern> <file1> <file2> ... <fileN>, where <pattern> is a regular expression pattern, and <file1> through <fileN> are the files to search.
Example:  grep loomer /etc/hosts will display all lines in the file /etc/hosts which contain the pattern `loomer'.

shutdown  Shuts the machine down
Syntax:  shutdown –h now

shutdown  Reboots the machine.
Syntax:  shutdown –r now

startx  Starts X Windows
Syntax:  startx
Prelab:

We have read the Read the Georgia Tech Computer and Network Usage Policy at http://www.oit.gatech.edu/information_security/policy/usage/ and understand that if we run these class tools outside the class laboratory we may be in violation of these and other laws. We are aware of our responsibilities to not use these tools in an illegal or unethical manner.

Signed: _______________________________  _____________________________

Section 1.4

Q1.4.1. Draw a picture here of three machines connected together by a hub or a switch and put names on the machines as well as IP addresses on each of the three machines network connections:
Show Your Hand Drawn Diagram to the TA and also demo ping to each of the other two machines simultaneously from your Host machine Red Hat WS 4.0. Have the TA sign his name and enter the date here:

______________________________  Date: ______________________

Q1.5.1. Compare the outputs before-hardening and after-hardening and list the ports that have been disabled.

Section 2

Attach a printout or hand written SUMMARY (not every single IP address required!) of the WHOIS information, to your answer sheet.

Prelab Q 2.1. How do you defend your own network against this type of information gathering?

Section 2.1

Q2.1.1. List what ports, the state of the port, and service found on the 7.2 machine.
Q2.1.2. What is the difference between when you scanned the Windows XP machine before and after enabling the firewall?

Q2.1.3. At a computer with Internet access, look at http://isc.incidents.org/port_details.html and type in the numbers (for the ports you found open) in the upper left white box (80 is the default). It will tell you what registered services are associated with that port as well as some statistics. Summarize what you found out about each running service from that web site here:

Q2.1.4. What operating system and version did nmap find on the 7.2 system? What operating system version do you see when you boot up that virtual machine? Are they the same?

Q2.1.5. Next use nmap to a range of hosts. Use for example 57.35.6.x – (x+4), select all types of ICMP pings, and select ping sweep. Did nmap see all of your three machines? This is an automated ping sweep to find machines on a network. What other machines can you find in the 57.35.6 network?
Q2.1.6. Run this again 57.35.6.x – (x+4), select ICMP ping, and select ping sweep but in the host machines terminal window also run tcpdump with the command:

tcpdump –nli eth0

Watch the output in the terminal window as nmap does the ping sweep on the range of IP addresses you request the sweep on. In other words, what do you see in the terminal window while tcpdump is running? Control C in the terminal window ends tcpdump.

Q2.1.7 – Exercise
One of the primary tasks for hackers to make their life simpler is to create a map of the network within which they’re trying to carry out their attacks. This is especially easy to do once they’re logged into one of the computers inside the target network. To do this, simple tools such as nmap and traceroute (usually found in all distributions of Linux), and no sophisticated tools need be installed.

4. On the command prompt, type nmap –sS 57.35.*.*
5. Machines with their open ports show up.
6. In a different terminal window, on a command prompt, for one or two machines, do

   #traceroute <ip address>

List one or two machines that you found, list open ports for those machines, and list the trace route results.

Q2.1.8 a) How does traceroute work? (You might need to google this)
b) What is the main difference between Unix traceroute and the Windows tracert commands (in terms of operation not in terms of syntax)? (You may want to see http://www.tech-faq.com/unix-windows-traceroute.shtml )
Now let’s say you’ve investigated the public DNS servers and determined that 138.210.230.0-138.210.240.255 is a range of IP addresses that you find very interesting. Perhaps that range contains the networks of some companies that you are interested in. Do a ping sweep of these addresses on our mininet in our lab (NOT THE REAL INTERNET) and list all the servers/IPs you could find (type nmap –h or man nmap to see nmap usage information). Also list the company or organization as you find in our mininet in our lab (NOT THE REAL INTERNET) if you could determine it. (Hint: If it is web server, you can try opening it in a browser.) Look at the traceroute output for each computer and with the help of that, construct a diagram of what the actual network looks like. For each machine, list the open ports on your diagram as well.
Q2.1.9. How do you defend your network against a tool like NMAP?

Section 2.2

Q2.2.1. What vulnerabilities did Nessus find with your stock Red Hat WS 4.0 System? List them here:

Q2.2.2. How do you defend against vulnerability scanners?

Section 2.3

Q2.3.1. What did this tool tell you about the Linux Host?

Q2.3.2. What do you think of this windows tool as compared to the Linux tools we have used previously?
2.4 General Questions

Q2.4.1. How long did it take you to complete part 1 of the lab?

Q2.4.2. How long did it take you to complete part 2 of the lab?

Q2.4.3. What corrections and/or improvements do you suggest for this lab? Please be very specific and if you add new material give the exact wording and instructions you would give to future students in the new lab handout. You may cross out and edit the text of the lab on previous pages to make minor corrections/suggestions. General suggestions like add tool xyz to do more capable scanning will not be awarded extras points even if the statement is totally true. Specific text that could be cut and pasted into this lab, completed exercises, and completed solutions may be awarded additional credit. Thus if tool xyz adds a capability or additional or better learning experience for future students here is what you need to do. You should add that tool to the lab by writing new detailed lab instructions on where to get the tool, how to install it, how to run it, what exactly to do with it in our lab, example outputs, etc. You must prove with what you turn in that you actually did the lab improvement yourself. Screen shots and output hardcopy are a good way to demonstrate that you actually completed your suggested enhancements. The lab addition section must start with the form “laboratory Additions Cover Sheet” which may be found on the class web site and is repeated here for the first lab:
Addition Title: ___________________________________________
(Include this cover page on every laboratory addition you submit.)

What new concept may be learned by adding this to the existing laboratory assignment? (Or what existing concept is better learned with this addition as opposed to what is in the existing lab assignment):

1) What are the specific vulnerabilities this concept exploits and what are the defenses one can use against the vulnerabilities?

Completion checklist:
• Did you email an electronic copy of your laboratory addition to Henry within 24 hours after the class (and name the attachment Grx_Laby_Add.doc)?
• Did you prepare a 5 minute in class presentation (which includes enough theory and results to educate your classmates on what you did and how you did it and discuss defenses) and email that to Henry within 24 hours after the class (and name the attachment Grx_Laby_Add.ppt)?
• Did you include proof that you got this working in our laboratory with our equipment? (Screen shots, output, etc)?
• Did you include references and attributes for all materials that you used? 
• Did you write your addition so that it does not require editing to cut and paste into the lab?
• In adding your new concepts/exercises did you include detailed lab instructions on where to get any software you may need, how to install it, how to run it, what exactly to do with it in our lab, example outputs proving that you got the enhancement to work in our lab?
• Did you include any theory/background and or fundamentals of the ideas and concepts behind this addition?
Turn-in Checklist

1- A printout of information you found on ISS.net from Section 2 Prelab
2- Answer Sheet with answers and TA signature.
3- Your detailed laboratory enhancements with the required cover sheet.