Read “Counter Hack” Chapter 5 Phase 1 Reconnaissance, and Chapter 6 Phase 2: Scanning.

Turn in this lab to the TAs with your answers.

All the tools you need for this lab are available on CDs that are in the lab (4883 Tools CD). Check one out from the TA.

At home or on a school computer:
Use the whois databases (for example http://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 Internet Security Systems (www.iss.net). Attach a printout or handwritten SUMMARY (not every single IP address required!) of that information to your lab.

How do you protect your own network against this type of information gathering?
Start both the XP and the virtual Red Hat 7.2 virtual operating systems. Go to the 7.2 “virtual operating system”. Create a /home/tools directory. Make sure that you are in X Windows while installing and running the tools. Use the command startx to initiate x windows. Copy the tools file to your Linux 7.2 machine into /home by

```
cp tools.tgz /home
```

Then

```
tar xvfz tools.tgz
```

This unpacks the tools into /home/tools directory.

```
cd tools
```

to go into the tools directory.

### CHEOPS-NG

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. Lets look at an automated tool for network mapping that draws a nice picture of the target network. You should now have the file cheops-ng-0.1.5 from the CD in your /home/tools. You can find this tool on your own at [http://cheops-ng.sourceforge.net/](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”.

Next

```
tar xvfz cheops-ng-0.1.5.tgz
cd cheops-ng-0.1.5
./configure
gmake
gmake install
```

The way to use this tool is to first start an agent daemon running in background mode on your virtual operating system. Type:

```
cheops-agent &
```

Next start your main program which has the graphical user interface. Connect to it with cheops-ng

You will need to tell the main program you want to connect to the background program running on agent hostname 127.0.0.1 which is your own machine.

At this point select viewspace and select add network. Enter in the network your machine is connected to in the lab, for example w.x.y.0 Use 255.255.255.0 in for the netmask.

At this point you should see the three virtual machines you have running at present and anyone else on the subnetwork. Draw by had a diagram of what this Cheops tool is showing you at present. Draw your diagram by hand here or on an attached page:
With the network map displayed, right mouse click on the windows XP system. Select detailed info. List the services, port number and protocol that are running here:

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

... 

Take a few minutes to explore what else this tool will do.

**NMAP**
Now that an attacker has gathered information about your network and has mapped it, 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 your Linux operating systems but you may 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 8.0 system by opening a new terminal window on the blue host background screen. The version of nmap thee 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 &

Use nmap to scan the 7.2 virtual machine by entering in its host IP address for example w.x.y.z+1. Select a SYN Stealth Scan using TCP&ICMP. Leave OS detection checked. Select scan.
List what ports, the state of the port, and service found on the 7.2 machine.

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...

At a computer with Internet access, look at [http://isc.incidents.org/port_details](http://isc.incidents.org/port_details) 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:

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?

Next use nmap to a range of hosts. Use for example w.x.y.z-(z+5), select ICMP ping, and select ping sweep. Did nmap see all of your three machines? This is an automated ping sweep to find machines on a network.

How does what you just did differ from the cheops tool as far as finding out about what machines are on your network?
Run this again w.x.y.z-(z+5), select ICMP ping, and select ping sweep but in the host machines terminal window also run tcpdump with the command:

```
tcpdump –nl 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 words, what do you see in the terminal window while tcpdump is running? Control C in the terminal window ends tcpdump.

---

**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 available for 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 ece4883
passwd ece4883
password
```

the system will complain that is a bad password but keep going

```
password
```

now we have an account names ece4883 with password password.

Nessus may be found at [http://www.nessus.org/](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 software which 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 the vulnerability”.

To install nessus:

First copy nessus-installer.sh from the CD that the TA has to /home/tools.

```
chmod 700 nessus-installer.sh
./nessus-installer.sh
```
hit the enter key

Where do you want the Nessus package to be installed?” select 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 ece4883

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 +138.210.231.101
to configure X Windows to allow connections to your Red Hat 7.2 host.

Start the server
nessusd &

switch users to ece4883 by typing
su ece4883

run Nessus with:
nessus &
Enter the passphrase: password

Click the Log In button
Click Ok.
Click Target Selection tab and enter a target for example the Red Hat 8.0 system w.x.y.z

Start the scan by clicking start the scan at the bottom of the page. This test takes approximately 15 minutes.

What vulnerabilities did Nessus find with your stock Red Hat 7.2 System? List them here:

How do you protect against vulnerability scanners?
Part 4: 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, let's use a windows scanning tool named SuperScan4.

Supercan 4
Supercan 4 may be found at http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan4.htm
That web page says:
“Powerful TCP port scanner, pinger, resolver. Copyright 2003 (c) by Foundstone, Inc.
http://www.foundstone.com 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
Insert the tools CD
Copy the windows folder to your machine
Remove the CD
Double click on SuperScan 4
Double click on SuperScan 4 extractor
Extract all
Answer the installation wizard questions
Double click on SuperScan4 executable
This beta version has expired but you may still use it (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 - beside the IP address w.x.y.z that you just entered
Click the blue triangle at the bottom left to start the scan
What did this tool tell you about the Linux Host?

Use the tools tab and select ping to w.x.y.z
Use the tools tab and select traceroute to w.x.y.z
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.

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

How long did it take you to complete this lab? Was it an appropriate length lab?

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 corrections/suggestions.