

This homework is due 10/17. Students need to work in pairs to successfully complete this lab.

- Please use a word processor for your solutions and submit your solutions to the TA gmuisa666@gmail.com with “ISA 666 HW#2” as the subject in your email as well as bring a hard copy of the homework with you to class.
- Include both names and G-numbers at the beginning of this lab submission.

Introduction

The purpose of this Lab assignment is for you to become comfortable using Nessus. In the process, you will also learn how to network 2 computers together, as well as become familiar with using VMware and Redhat.

Step 1

After finding a class partner, network your computers together, either wirelessly, using a crossover cable, a hub/switch, or any other way you that works for you. Make sure to statically setup your IP addresses or use DHCP if you have a DHCP server running. Verify you can ping each other, if not, modify your firewall rules or temporarily turn it off.

Step 2

Start by reading more about Nessus from their website: <http://www.nessus.org> as well as <http://www.securityfocus.com/infocus/1741> to get an understanding of what it is and how it is used.

Download and install the VMware free player from:

<http://www.vmware.com/download/player/> (or the free vmware server)

Now you will need to download the VMware image that has Redhat and Nessus already installed, configured, and ready to go:

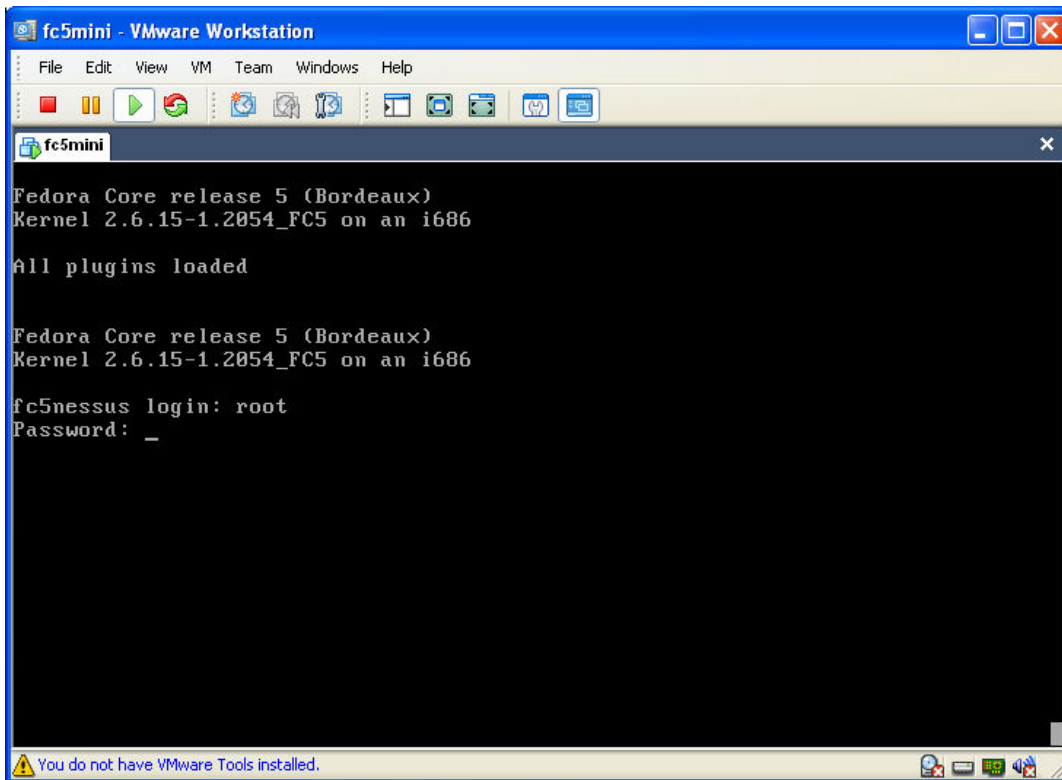
<http://www.ise.gmu.edu/~duminda/classes/fall06/isa666/downloads/fc5nessus.zip>

Unzip the file and double click on a file called “Other Linux 2.6.x kernel.vmx”. Once the Redhat image finishes loading, press enter and use the following login:

login: root

Password: nessus

Homework #2
ISA 666 Internet Security Protocols Fall 2006



```
fc5mini - VMware Workstation
File Edit View VM Team Windows Help
fc5mini
Fedora Core release 5 (Bordeaux)
Kernel 2.6.15-1.2054_FC5 on an i686

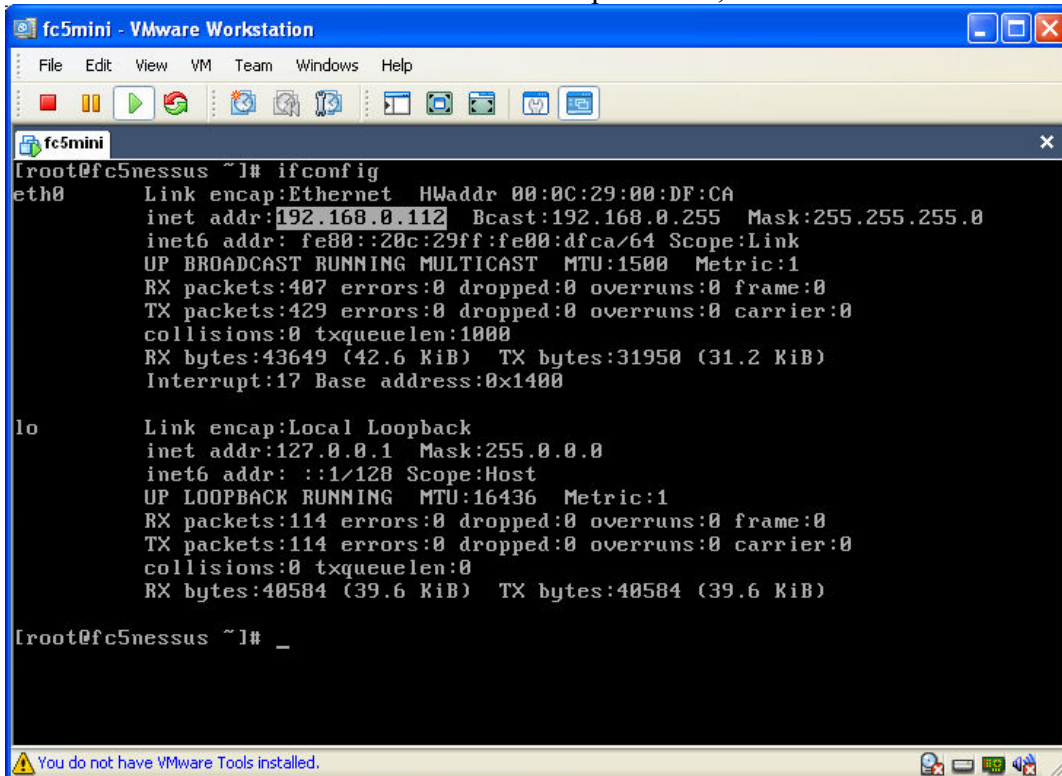
All plugins loaded

Fedora Core release 5 (Bordeaux)
Kernel 2.6.15-1.2054_FC5 on an i686

fc5nessus login: root
Password: _

You do not have VMware Tools installed.
```

Now you must determine the IP address of the Redhat server. Type in “ifconfig” and note the IP address of the server. In the example below, it’s 192.168.0.112.



```
fc5mini - VMware Workstation
File Edit View VM Team Windows Help
fc5mini
[root@fc5nessus ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:00:DF:CA
          inet addr:192.168.0.112  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe00:dfca/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:407 errors:0 dropped:0 overruns:0 frame:0
          TX packets:429 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:43649 (42.6 KiB)  TX bytes:31950 (31.2 KiB)
          Interrupt:17 Base address:0x1400

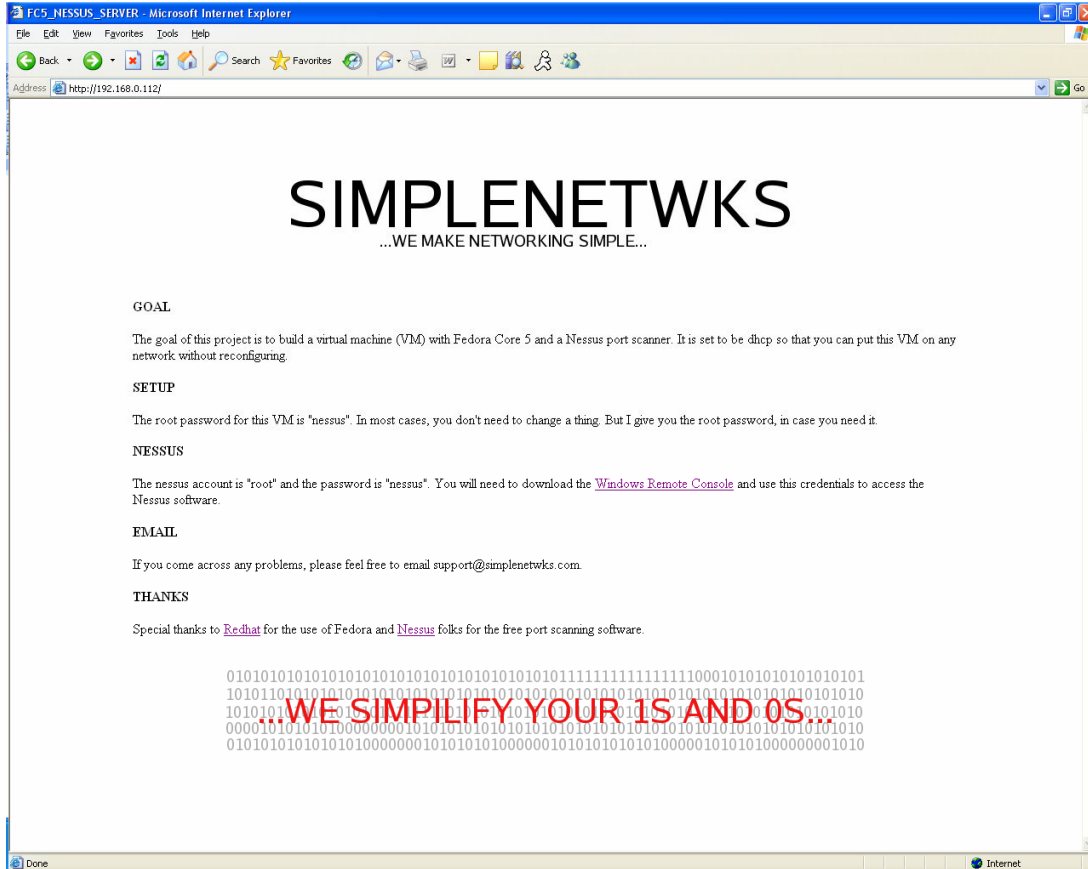
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40584 (39.6 KiB)  TX bytes:40584 (39.6 KiB)

[root@fc5nessus ~]# _

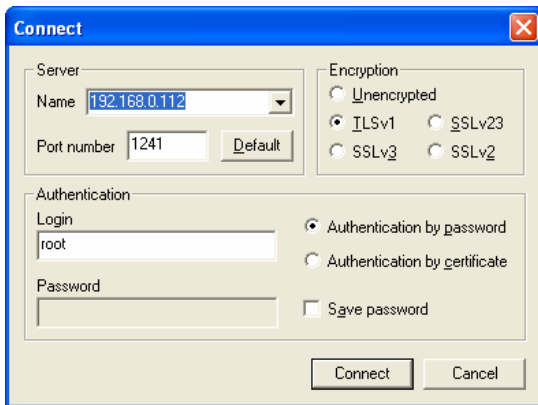
You do not have VMware Tools installed.
```

Step 3

Now that you have determined the IP address of the server, put it into your web browser and then click on the “Windows Remote Console” and download it on your computer.



Extract the files and double click the “NessusWX.exe”. It will want to create a Database directory, click yes. Click on “Communications” and then “Connect”, type in the IP address of the server.



Click “Connect”, click “Accept & Save” and then put in the password: nessus

Now you are ready to start a scan. Start a new session, click on “Add” in the “Targets” tab. Put in the IP address of your partner’s Redhat server. Click on the “Plugins” tab and click the “Use session-specific plugin set” checkmark. Now click select plugins, and click on “Disable All”, then click “No” when asked about disabling the port scanner. At this point, you are to specify which plugins to use. Expand the plugins folder and click on individual plugins, if you want more information about a plugin.

Before you start the scan, make sure your partner temporarily turns off his firewall. You are trying to find vulnerabilities on the Redhat server your partner is running. So select the plugins that are suitable for this scan.

Step 4

Your write up should be no more than 5 pages, single spaced, times new roman size font 12. It should include the following information:

Part 1

How were the computers, between you and your partner, networked together?
List the issues you encountered and how you resolved them?

Part 2

Describe what Nessus is and when you would use it.
Find and briefly compare two other programs that do the same thing.
Screenshot of Redhat’s IP address. (Similar to bottom of p.2)

Part 3

List the plugins you used for the scan and justify why chose them.
List all the open ports you found and what they are used for.

Part 4

For you and your partner:
What was the most difficult part of this lab assignment?
What was the most interesting thing you learned from this lab assignment?