

Lab 3: Introduction to our Security VM and Port Scanning

Due: 9/23/09 at the beginning of class

Objectives - to:

1. familiarize yourself with our security VM
2. using your VM to investigate ports

I. Security VM:

1. Start

All Programs

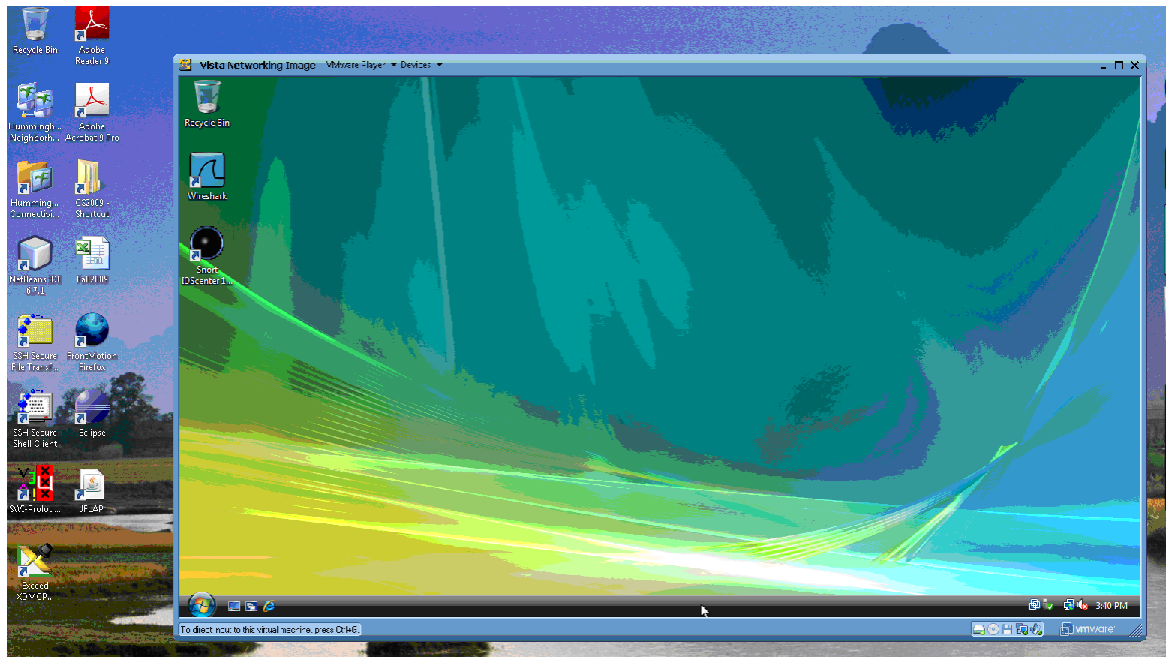
VMware

VMware Player

(cancel VM web check)

Open

C / Virtual Machines/ Vista Networking Machine – Copy 1



2. Take a look at all the security programs installed on the VM – you will use some in class and the others are there for your investigation.
3. Note that there is a second VM on your machine – open that.
4. Using the cmd prompt, determine the IP addresses of your 2 VMs
VM1_____ VM2_____
5. To return to your actual machine at any time, click *Ctrl-Alt*
6. Your VM is portable; you will need at least 5G.

II. Port Scanning

The TCP/IP suite of protocols is responsible for the reliable transmission of data from one host to another – and it is based on **port numbers**.

A **port number** indicates what service on the receiving host (the application layer) is being accessed.

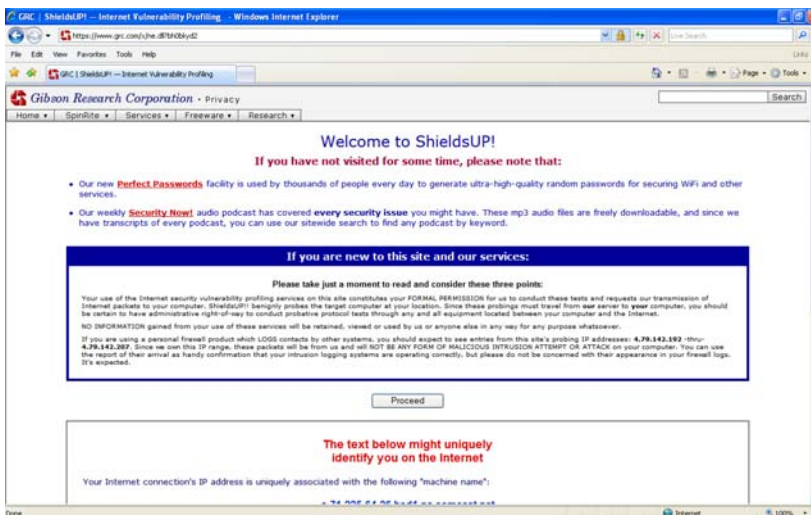
Recall that packets have headers – each header contains the source and destination IP addresses as well as the source and destination _____.

There are a total of 65, 535 available **port numbers** of which 1, 023 are considered well known port numbers – associated with particular programs or services.

Since **open ports** serve as an entry point into a computer, attackers can and do take advantage of open ports to transmit malicious code.

II a. Using Gibson Richard's 'Shields Up' to analyze port connections

1. From your VM, download 'Shields Up,'



2. Before you click 'Proceed', what 2 pieces of information about your computer has already been revealed? _____
3. How is it that this information (from number 2) is so easily available? _____

4. Given the ease at which the info (from 2 and 3) is available, what implications does that have? _____

5. Having answered 4 and 5, click 'Proceed.'

6. Click on 'File Sharing.'

7. Print Screen

8. Go back and click on 'All Service Ports.'

9. Print Screen

10. Is your IP address consistent? _____

11. How many ports are in open, closed, stealth modes? _____

12. Identify 4 protocols associated with open ports _____

13. What does stealth mode mean? _____

II b. Identifying Processes Using Open Ports

1. Open up *Command Prompt* on your VM
2. Use *netstat -ano* to see the established connections and the ports on which your computer is listening for new connections. Keep this screen open
3. Screen shot
4. Go to the *Windows Task Manager* and click on the *Processes* tab
5. On this screen, click *View* on the menu bar and then click *Select Columns* – you will probably need to check the *PID* box. Click *OK*.
6. What does PID stand for? _____
7. Click on the PID column to sort numerically by PID
8. Screen shot
9. Using this information, identify 4 port names that are in 'listening' mode

(5 points)

Total: 25 Points