ITEC345 2013spring-ibarland

**Network security**

Project created by Prem Uppuluri

**Objectives:** In completing this homework, you will learn:

Section 1: how to use basic tools to troubleshoot a network.

Section 2: perform basic operations to identify potential vulnerabilities in a network.

For this homework, use the same windows workstation you [used for hw07](http://www.radford.edu/~itec345/2013spring-ibarland/Homeworks/hw07/hw07-windows-VM-login.html). You may work with the same partner, or a different partner, in teams of two. As with hw07, you will put your answers into [hw08-answer-sheet.docx](http://www.radford.edu/itec345/Homeworks/hw08/hw08-answer-sheet.docx) (including some screenshots), and submit it on D2L.

**instructions**

1. Log in to Windows machine using an administrator account.
	* You can use the account “Security Student”, if it is shown on your machine. (It won’t be, if you disabled accounts-without-passwords in hw07).
	* You can also log in to the account “Administrator” with password: “security1#”. Since “Administrator” isn’t displayed at the login window, you’ll have to issue a Ctrl+Alt+del (in vSphere, choose *Inventory > Virtual Machine > Guest > Send Ctrl+Alt+del*).
2. For the rest of the assignment you will need to use a few programs that you need to search for on the disk**. I strongly suggest that you find these programs and create shortcuts on the Desktop for the rest of the homework.** Using the search option, search for:
	* zenmap.exe (you will find this in C:\Program Files\Nmap)
	* Secunia PSI (you will find this in C:\Documents and Settings\Security Student\Desktop\Security Tools)
3. **Most of the tools that we will use in the rest of the homework require to be executed via the command prompt. To get a command prompt: *Start > Run*, and type cmd.**
4. Casing the network: Attackers use various tools to case a network. Their goal is to find out where the domain name server is located, where the firewall is located (usually on the gateway server) and where other network services are located. Here are a list of tools that can help:
	* **Identify IP address:** use the program ipconfig (from a cmd shell). Since this is a virtual machine, the IP address will listed as being for the “Ethernet adaptor”.
	* **Get the IP address of Radford University’s DNS server.**
		1. **Open the command prompt.**
		2. **Use nslookup** [**www.radford.edu**](http://www.radford.edu)

Note that nslookupreports both the domain-name server it is using, as well as the requested IP address.

* + **Ping:** using ping you can check if a specific computer on your network is active/alive as follows: ping *an-ip-address*
		1. If a response is received to the ping request then the server is alive, otherwise it isn’t.
		2. You can type Control-C in the command-window, to terminate a program.
	+ **Traceroute:**  This tool allows you to trace the path between two systems. It is used as follows from the command prompt:
		1. tracert *an-ip-address*
		This traces the path from the current computer to *an-ip-address*.

You may get (slow) lines of the form “\* \* \* request timed out.”; that is okay. (It means there *is* an intermediate computer, but it is configured to not send back its IP address info on packet timeout. That happens to be how tracert works: it sends packets contrived to time out, and then looks at the failure notices it receives back.)

* + **Nmap/Zenmap: nmap (**[**www.nmap.org**](http://www.nmap.org)**)** is a *port scanner*: it can be used to identify services, open ports and the operating system on remote systems. It simply issues requests to all ports at a given address, and reports which ones respond.
		1. Startup zenmap
		2. nmap -O *an-ip-address* specifies the OS on the specific IP address.
		3. nmap -sS *an-ip-address* specifies the list of open ports on any IP address.
		4. A range of IP addresses can also be used with the above commands. E.g., range of IP addresses from 169.1.1.1 to 169.1.1.254 can be specified as follows: 169.1.1.1-254.
			1. E.g., nmap –O 169.1.1.1-254 will scan all the computers within the network 169.1.1
1. **Checking for out-of-date software:**
	* There are several software programs available to check if all network services and other programs on your workstation are up-to-date. For this project, we will use the free trial version of Secunia PSI. This program connects to a remote database to determine if the programs on a workstation are up-to-date.
	* Find and launch Secunia PSI (will take time) – skip the first screen by selecting “Maybe later”.
2. **Packet sniffing:**
	* Packet sniffing software allows you to inspect network packets that are passing your computer’s Network Interface Controller. **Wireshark** is perhaps the most well-known packet sniffer. There are several modes to use Wireshark in.
		1. To use Wireshark:
			1. **Startup wireshark (Start🡪All Programs🡪Wireshark)**
	* **Select the interface (see figure) and press start**

Select the network card (here: “VMware Accelerated AMD …”) first and then press start.

**There are lots of options in wireshark. You can enter filters to filter the traffic based on protocols, IP addresses, ports etc. See the next two pictures to familiarize yourself with some basic Wireshark functionality.**

****

Filter traffic by typing the protocol name here.

****

This screen shows you the **raw** packet data.

Once you select a packet, you can see the packet headers and data in the screen below. Clicking on the + sign next to each layer, gives you the header information.

Once you select a packet, you can see the packet headers and data in the screen below

Network traffic. Each row represents a packet. For each packet, you can see the: source IP, destination IP , the protocol name, and brief description.