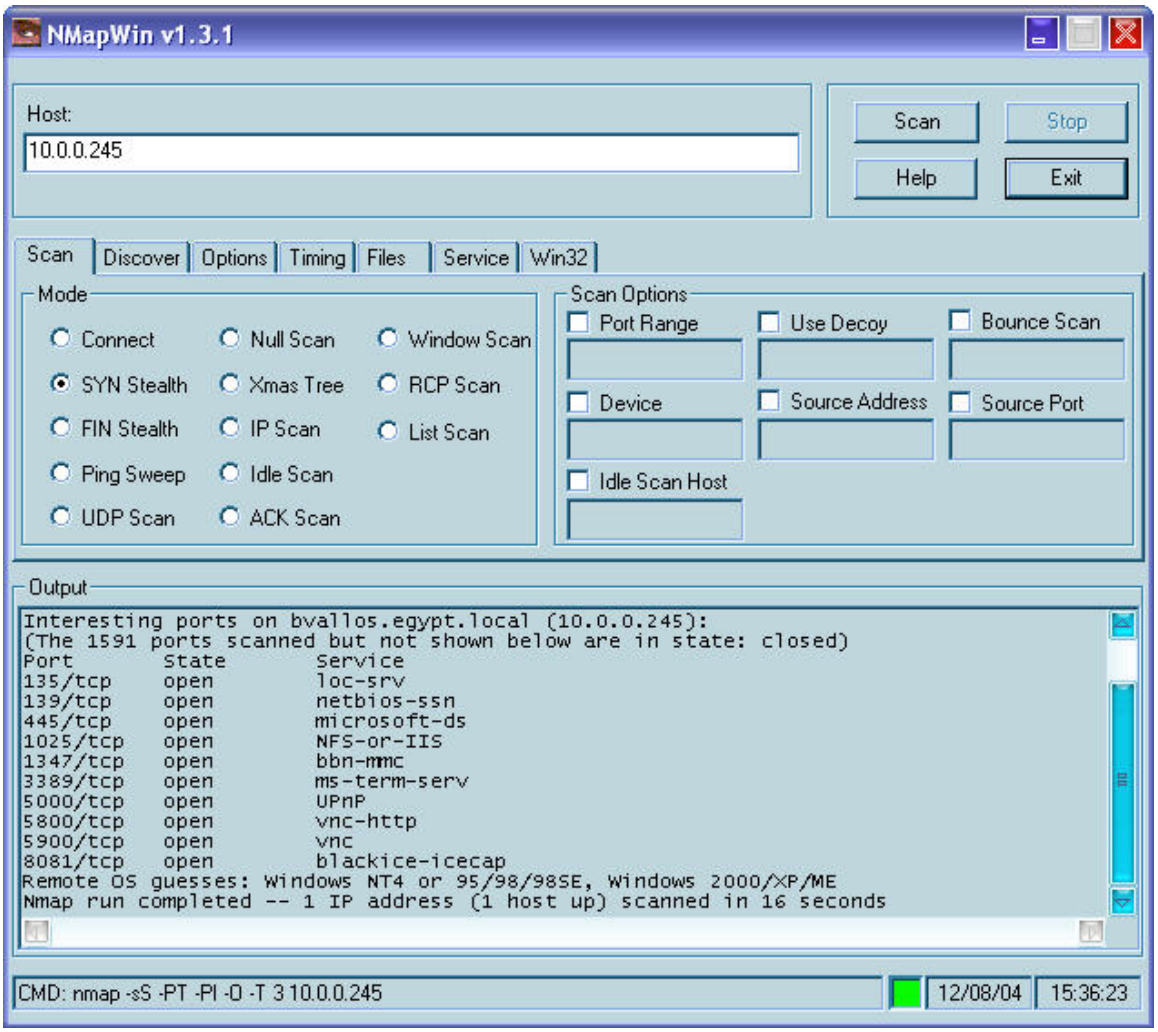
9.8.1

NMap for Windows Port Scanning

with Windows XP Firewall



Laboratory Overview

Objective

At the end of this lab students will be able to enable Windows XP built in Firewall. Students will be able to use NMapWin to scan for open ports.

Information for Laboratory

A. Students will utilize the built in Firewall capabilities of Microsoft Windows XP
B. Students will utilize NMap for Windows, a TCP/IP port scanner with a Windows graphic user interface.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Warning

The Windows XP Firewall can disrupt network connectivity. Students should make sure that the Firewall is disabled at the end of the lab.

Estimated Completion Time

60 Minutes

TCP/IP Port scanning

Port scanning is similar to a thief going through your neighborhood and checking every door and window on each house to see which ones are open and which ones are locked.

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two of the protocols that make up the TCP/IP protocol suite which is used universally to communicate on the Internet. Each of these has ports 0 through 65535 available so essentially there are more than 65,000 doors to lock.

The first 1024 TCP ports are called the Well-Known Ports and are associated with standard services such as FTP, HTTP, SMTP or DNS. Some of the addresses over 1023 also have commonly associated services, but the majority of these ports are not associated with any service and are available for a program or application to use to communicate on.

Port scanning software, in its most basic state, simply sends out a request to connect to the target computer on each port sequentially and makes a note of which ports responded or seem open to more in-depth probing.

NMAP for Windows

Nmap ("Network Mapper") is a free 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 (application name and version) those hosts are offering, what operating systems (and OS versions) 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.

Windows XP Firewall

Microsoft Windows Internet Connection Firewall is a software based Firewall that you can use to set restrictions on the information that is communicated between your home or small office network and the Internet. Internet Connection Firewall

can also help protect a single computer that is connected to the Internet. If you have a single computer that is connected to the Internet with a cable modem, a DSL modem, or a dial-up modem, Internet Connection Firewall helps protect your Internet connection.

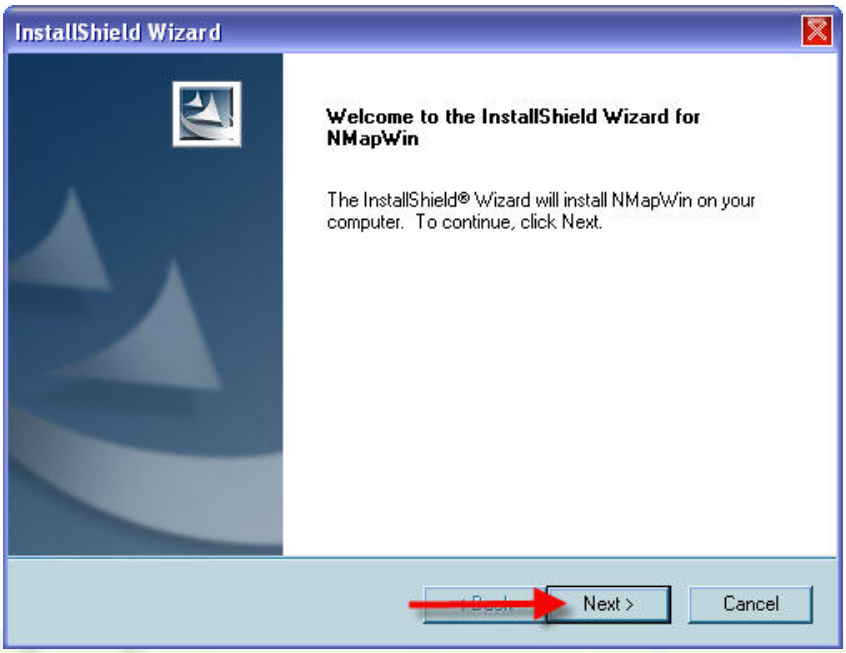
Internet Connection Firewall is a "stateful" firewall. A stateful firewall is one that monitors all aspects of the communications that cross its path and examines the source and the destination address of each message that the firewall handles. To prevent unsolicited traffic from the public side of the connection from entering the private side, Internet Connection Firewall keeps a table of all the communications that have originated from the computer that is running Internet Connection Firewall. For a single computer, Internet Connection Firewall tracks traffic that originates from the computer. Internet Connection Firewall compares all inbound traffic from the Internet to the entries in the table. Inbound Internet traffic is permitted to reach the computers in your network only if there is a matching entry in the table that shows that the communication exchange began in your computer or private network.

Communications that originate from a source outside the computer that is running Internet Connection Firewall, such as from the Internet, are dropped by the firewall unless you create an entry on the Services tab to permit passage. Instead of sending you notifications about activity, Internet Connection Firewall silently discards unsolicited communications. **This stops common hacking attempts such as port scanning**. Such notifications might be sent frequently enough to become a distraction. Instead, Internet Connection Firewall can create a security log so that you can view the activity that is tracked by the firewall.

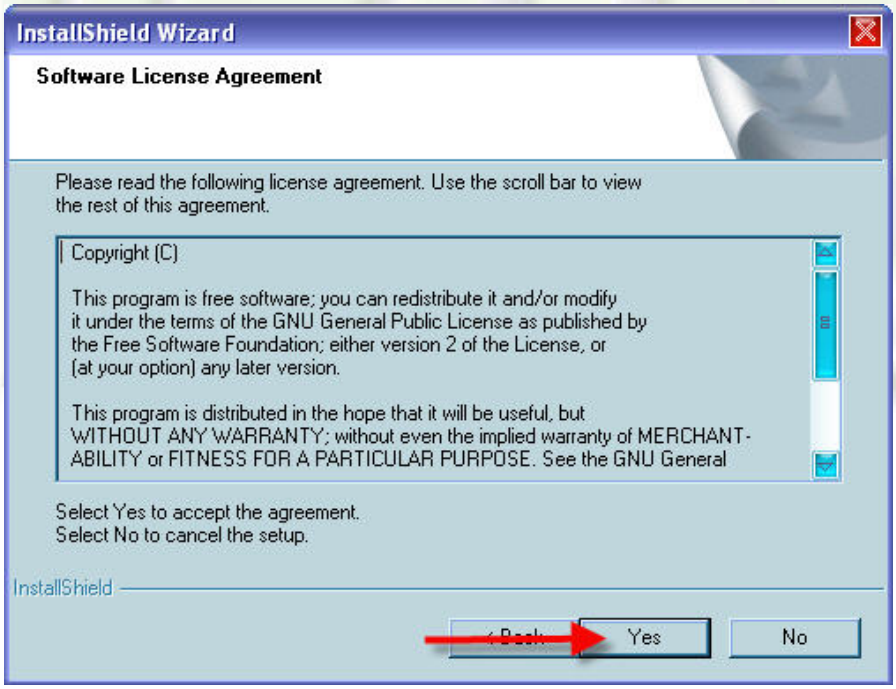
Step 1: Install NMAP for Windows with Graphic User Interface

Locate the executable installation file for Nmap nmapwin_1.3.1.exe, and double click the file to start the setup.

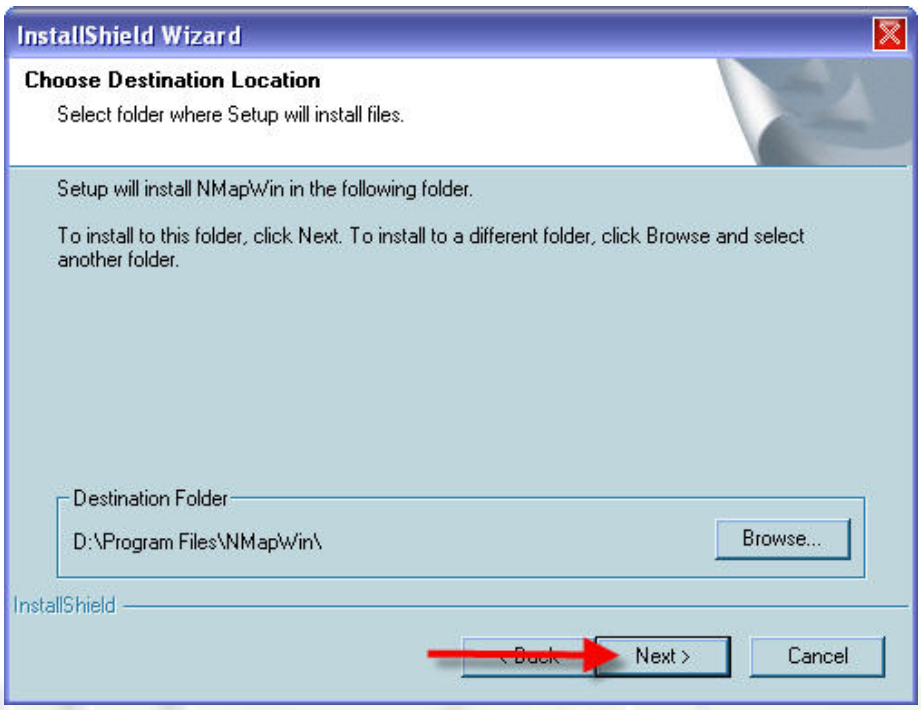
Click next to continue the installation as below.



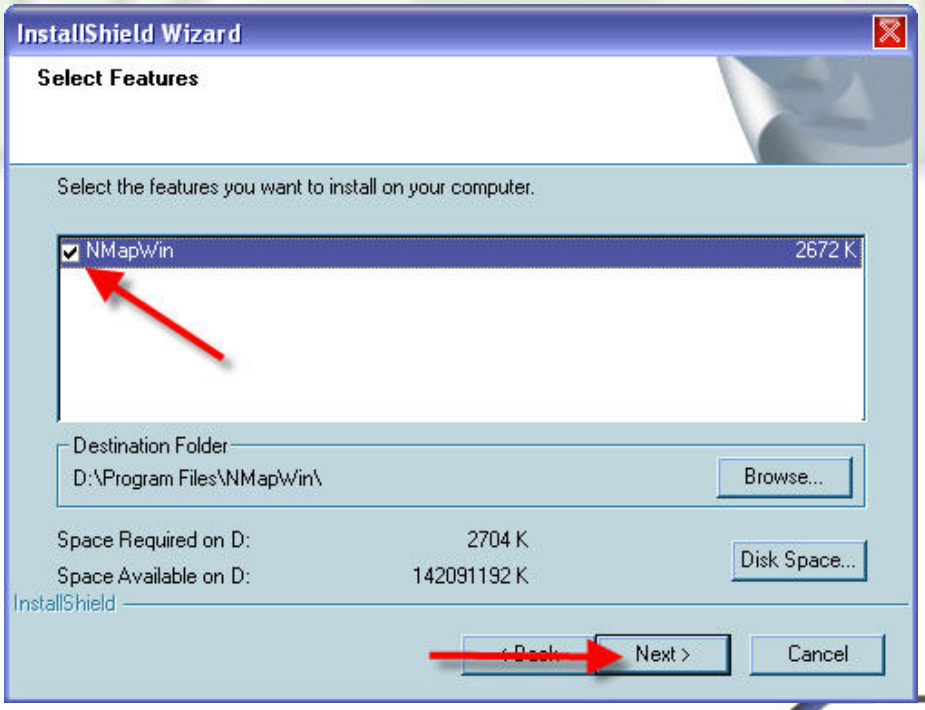
Click Yes to agree to the software license agreement as below.



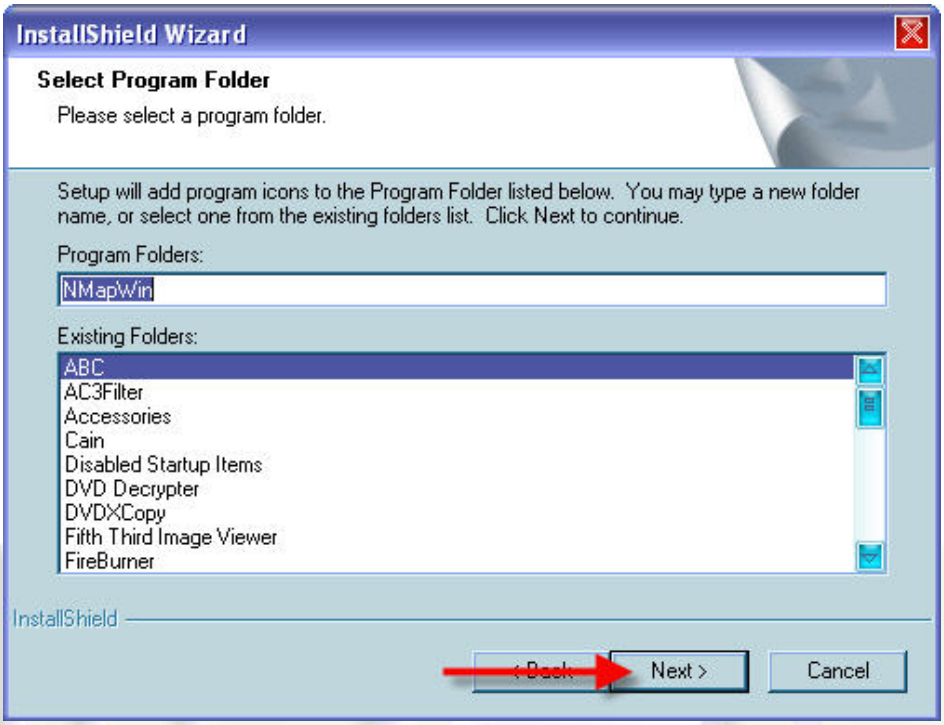
Click Next to accept the default installation directory as below.



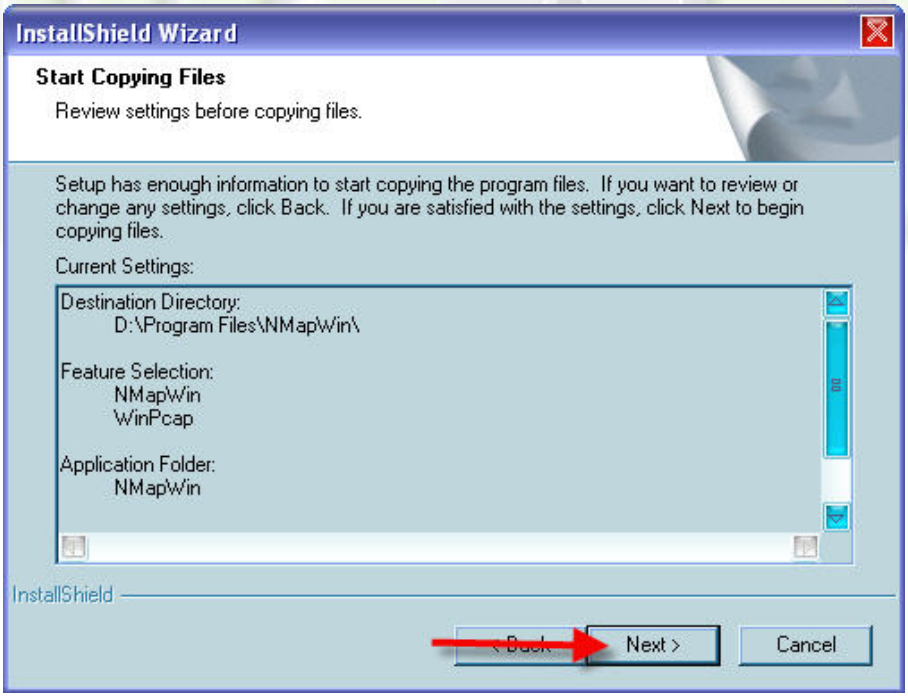
Check to make sure that NMapWin is the selected feature to be installed and click next as below.



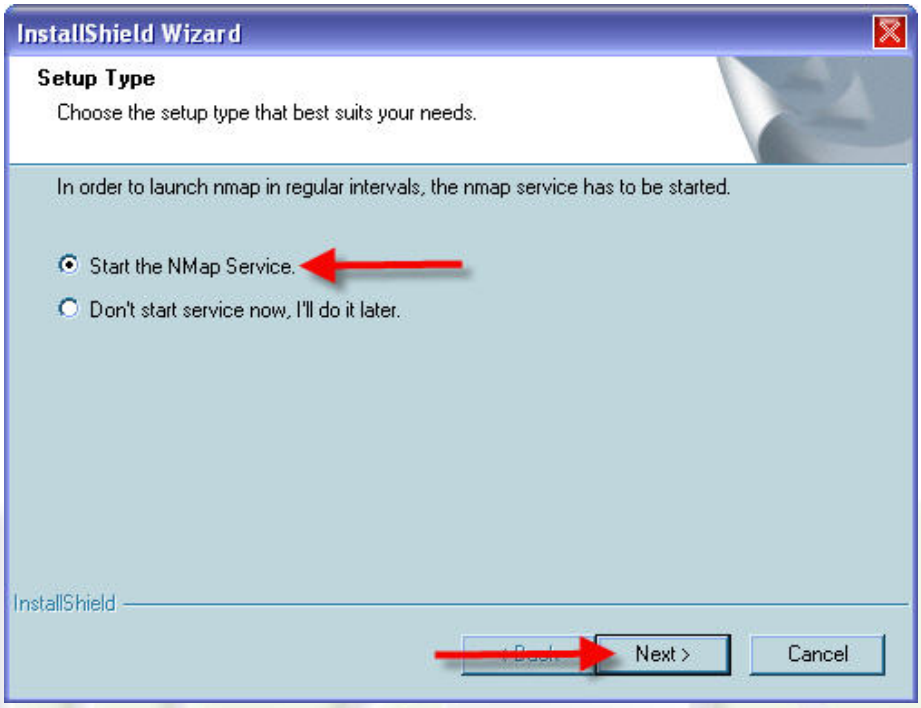
Click Next to select the program folder as below.



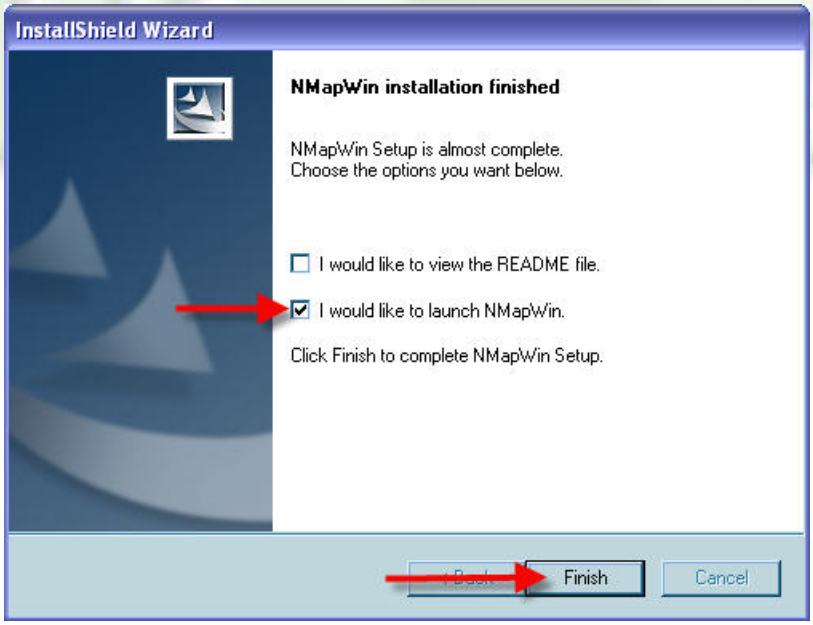
Click Next to start the file copy as below.



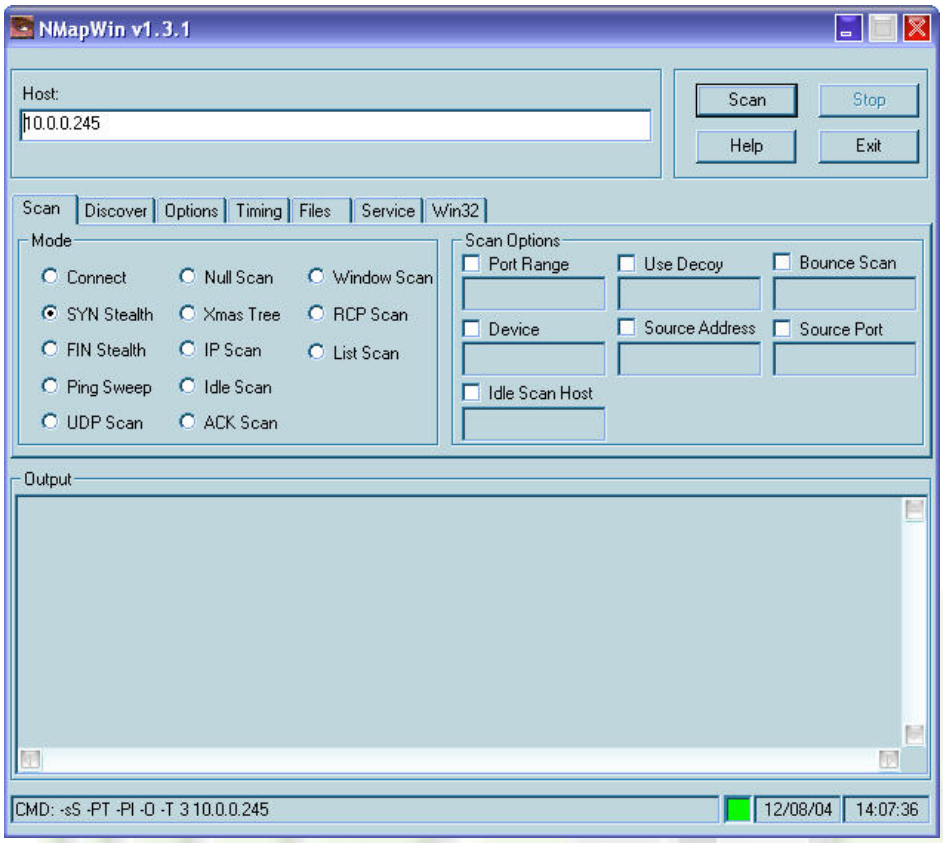
When the file copy has finished, the installation program will prompt you to choose a setup type. Choose to Start the NMap Service and click next as below.



Choose the option to launch NMapWin and click Finish to end the installation as below.

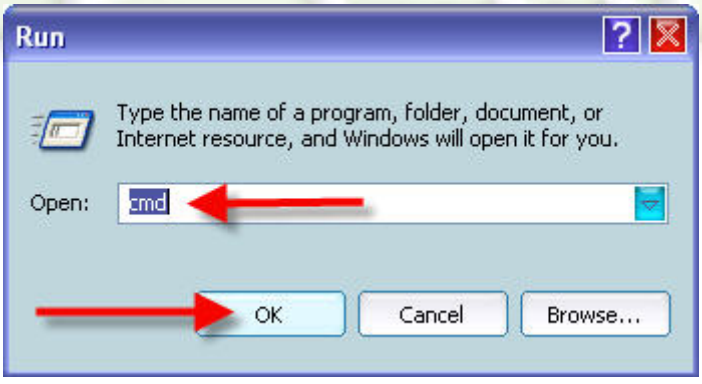


NMapWin v1.3.1 should open as below.

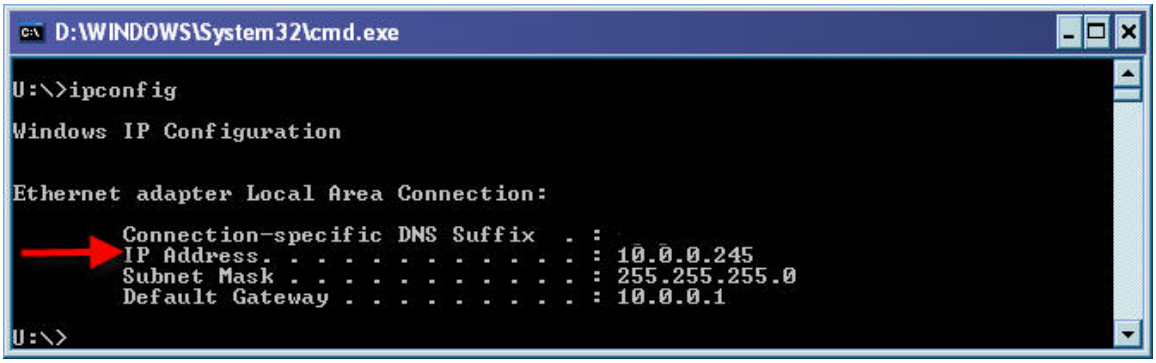


Step 2: Scan your computer for open ports

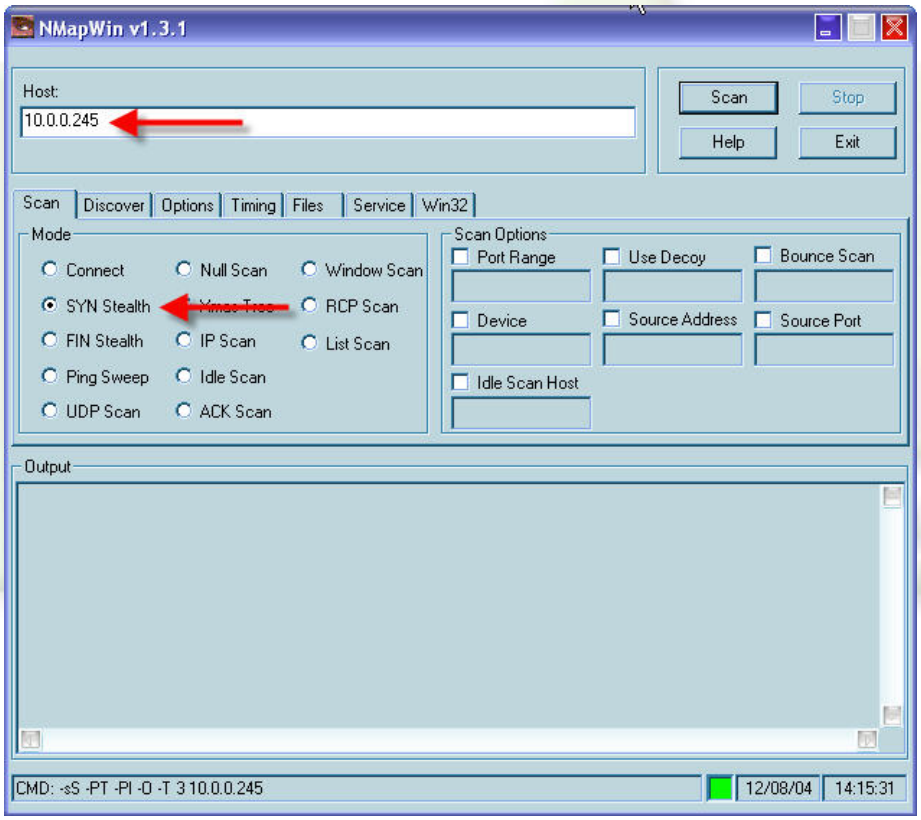
From START, Run, type ‘cmd’ in the Open box and click OK as below.



From the command prompt, type ‘ipconfig’ to view you current IP address, as below.



From MapWin enter your IP address in the Host box as below. Do not modify any of the NMap settings, the scan should be setup as an SYN Stealth scan. When set, click Scan in the top right corner as shown below.



The port scanning will take a few minutes to complete, when finished, the results will be displayed in the Output box on the bottom half of the NMapWin program. You should see some basic open ports such as…

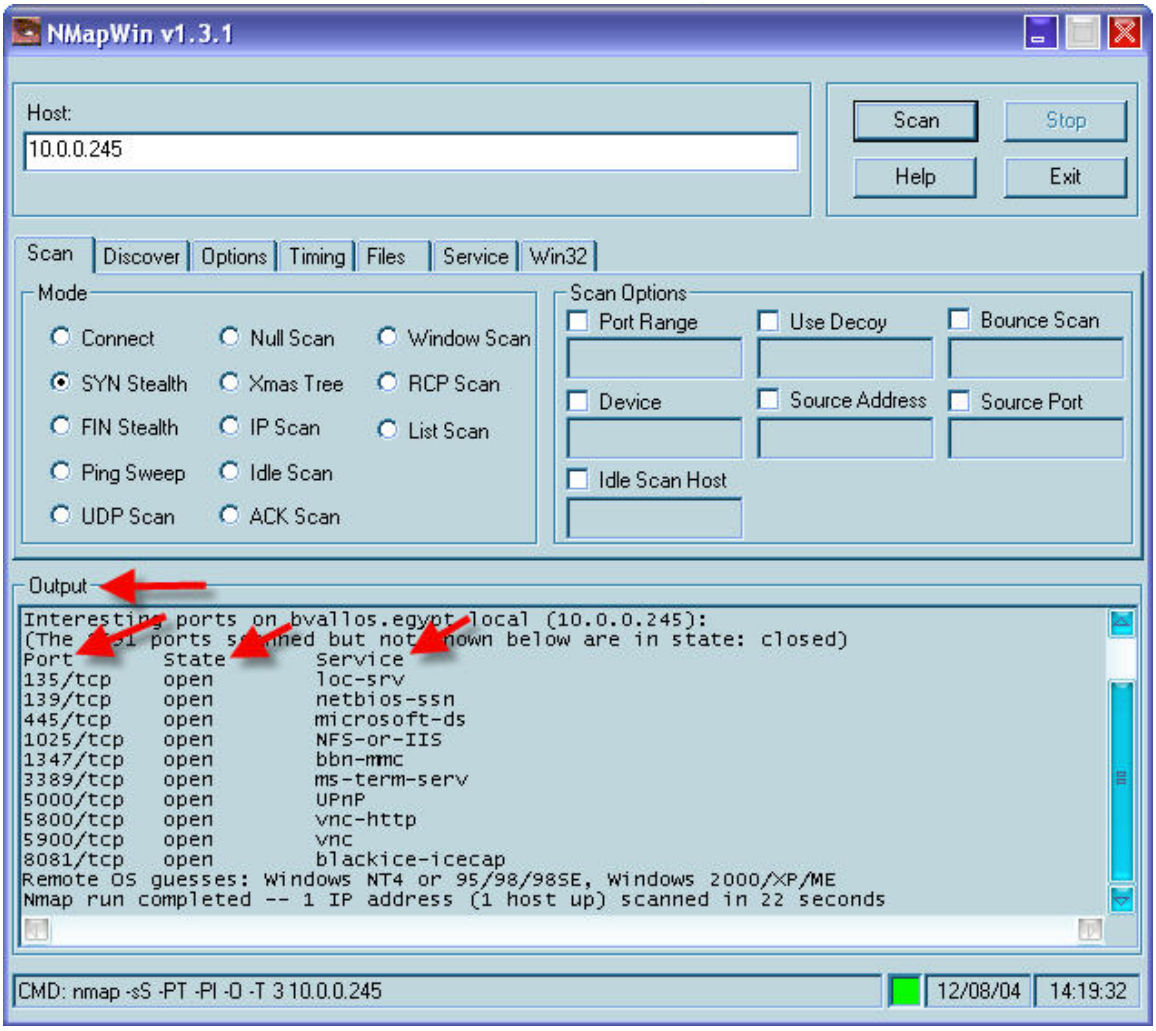
Port State Service

135/TCP OPEN LOC-SRV
139/TCP OPEN NETBIOS-SSN
445/TCP OPEN MICROSOFT-DS

3389/TCP OPEN MS-TERM-SERV – OPEN IF REMOTE DESKTOP IS ENABLED

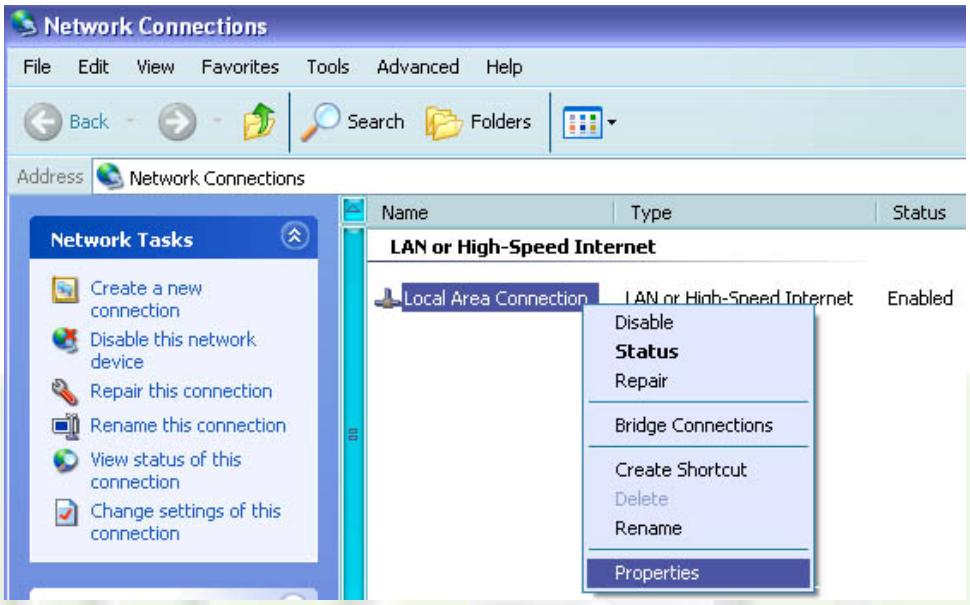
5900/TCP OPEN VNC – OPEN IF VNC SERVER IS RUNNING

Compare your output to the output below.

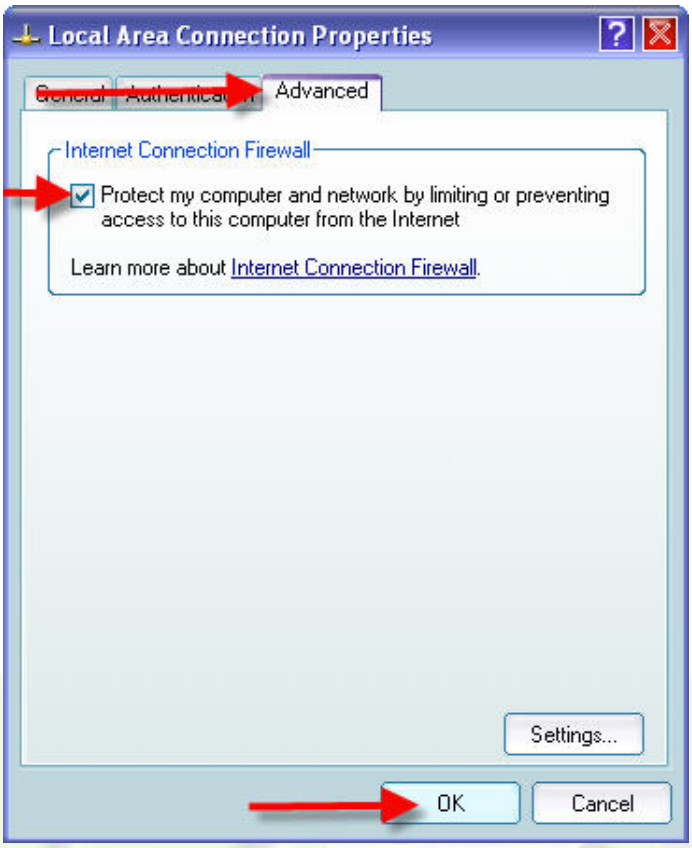


Step 3: Enable Window XP Firewall

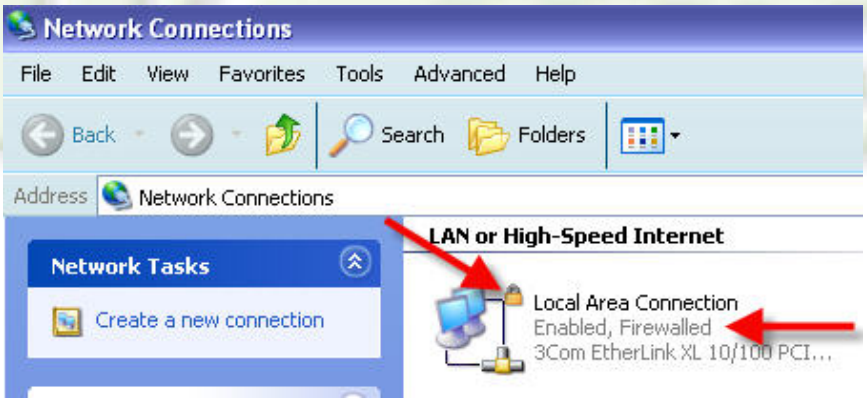
From your desktop, Right click on My Network Places, and click properties. This will open the Network Connections page. From the network connections page, you should have listed your Local Area Connection. This should be a 10/100 MB network connection to your LAN. Right click, and go to properties of your Local Area Connection, as show below.



From the properties page, click on the Advanced tab at the top. From the Advanced tab, select the check box to Protect my computer and network by limiting or preventing access to this computer from the Internet, and click OK at the bottom as shown below.



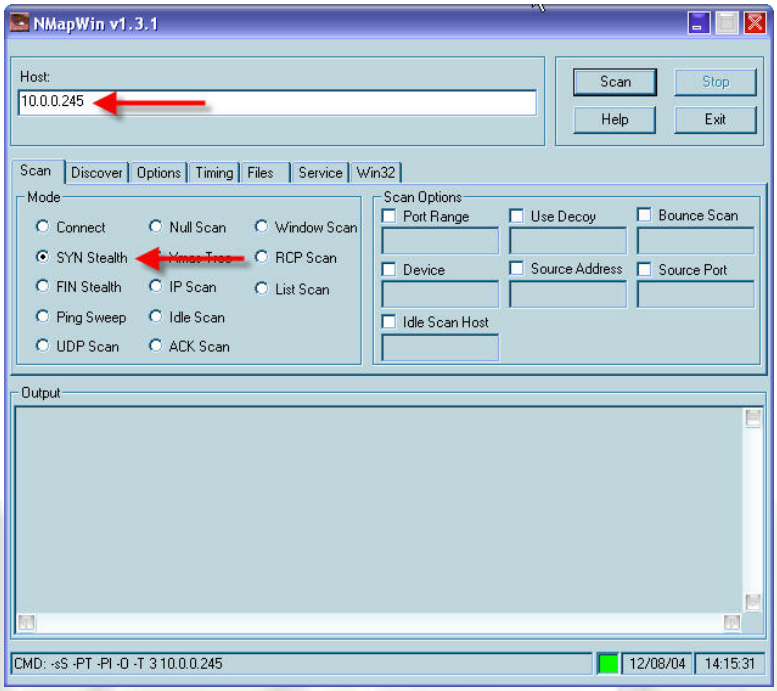
After Clicking OK, you should be back at the Network Connections page. Here you should now be able to see the Local Area Connection Icon has a lock over it, and it is listed as Enabled, Firewalled, as shown below.



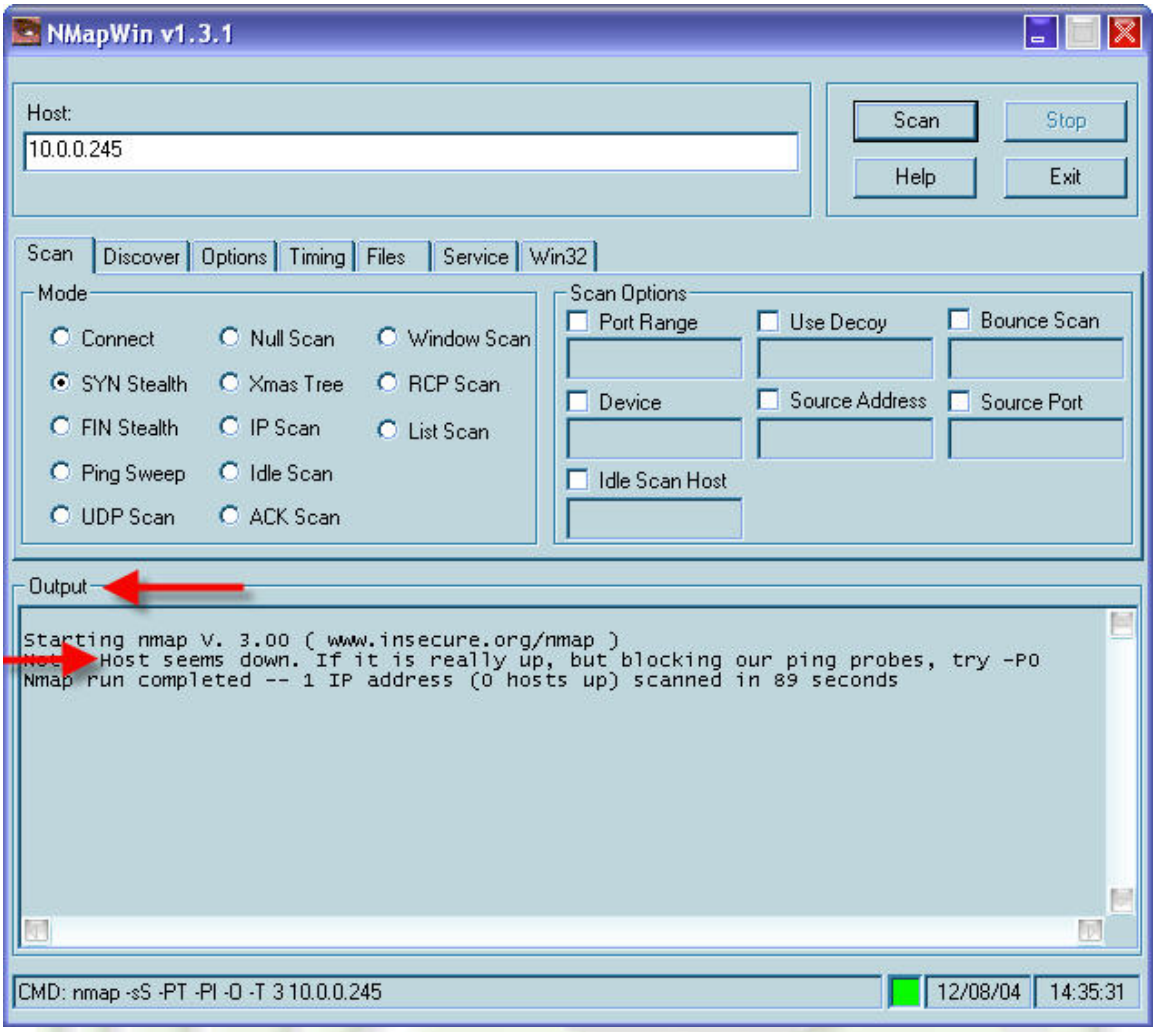
Close all open windows.

Step 4: Rescan with NMAP

With the Windows XP Firewall enabled, open NMapWin and enter your IP address in the host box. Click scan, as show below. This should be done exactly as in Step 2 above.



When the scan is finished, you should see the output has changed. NMap will report back that the Host seems down. This is because the “Statefull” Firewall has blocked all attempts at port scanning, and has also blocked all open ports. Hence, NMap returns no data and shows the Host as down.



Analysis:

1) For which applications are Firewalls best suited?

2) After working with these utilities, what about NMapWin and or Windows XP Firewall do you feel you should study

further? Why?

3) Why should you enable Windows XP Firewall if your computer is directly connected to the Internet?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

Appendix:

This lab was developed using Nmapwin Version 1.3.1.

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 1. For use of Nmapwin with XP SP2, see the www.insecure.org news link.