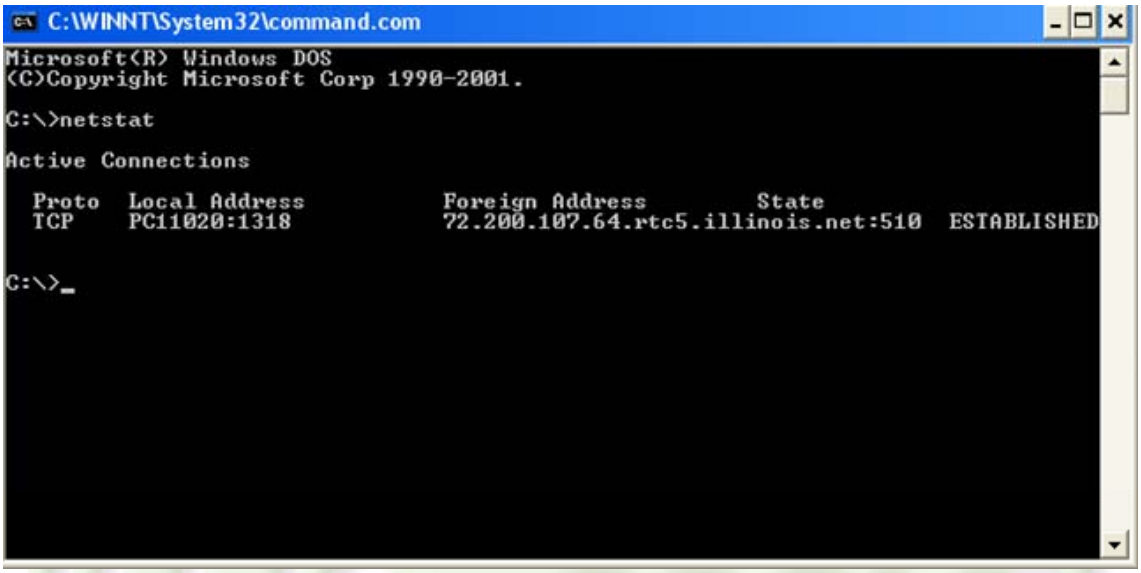
1.3.1

NETWORK UTILITIES

(NETSTAT & NBTSTAT)



Laboratory Overview

Objective

At the end of this lab students will be able to use NETSTAT and NBTSTAT for enumeration purposes. By gathering this information, you can gain a much clearer understanding of the LAN (either local or remote).

Information for Laboratory

A. Students will utilize both NETSTAT and NBTSTAT programs to scan the laboratory Windows XP computers.
B. Students will list any vulnerabilities and make recommendations to resolve the problems.

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.

Instructor Preparation

Before class, the instructor or a lab assistant will ensure that the Lab PCs have LAN connectivity with each other

Estimated Completion Time

30 Minutes

Enumeration

Enumeration is an information gathering technique. It probes systems for open, listening connections and tries to spot weaknesses.

NETSTAT & NBTSTAT

NETSTAT and NBTSTAT are utilities found in the Windows operating system. NETSTAT identifies listening, open ports on your PC, while NBTSTAT can list NetBIOS information on remote PCs as well as your own.

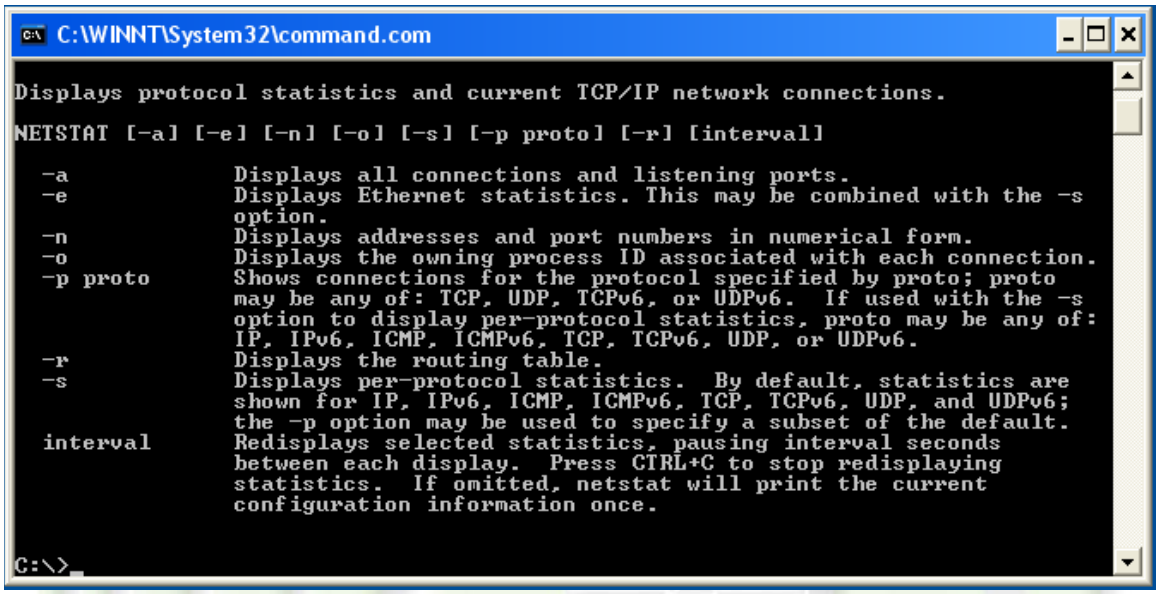
NETSTAT

Step 1:

Click on Start, Run, Command and press Enter. You will be at a DOS command shell prompt.

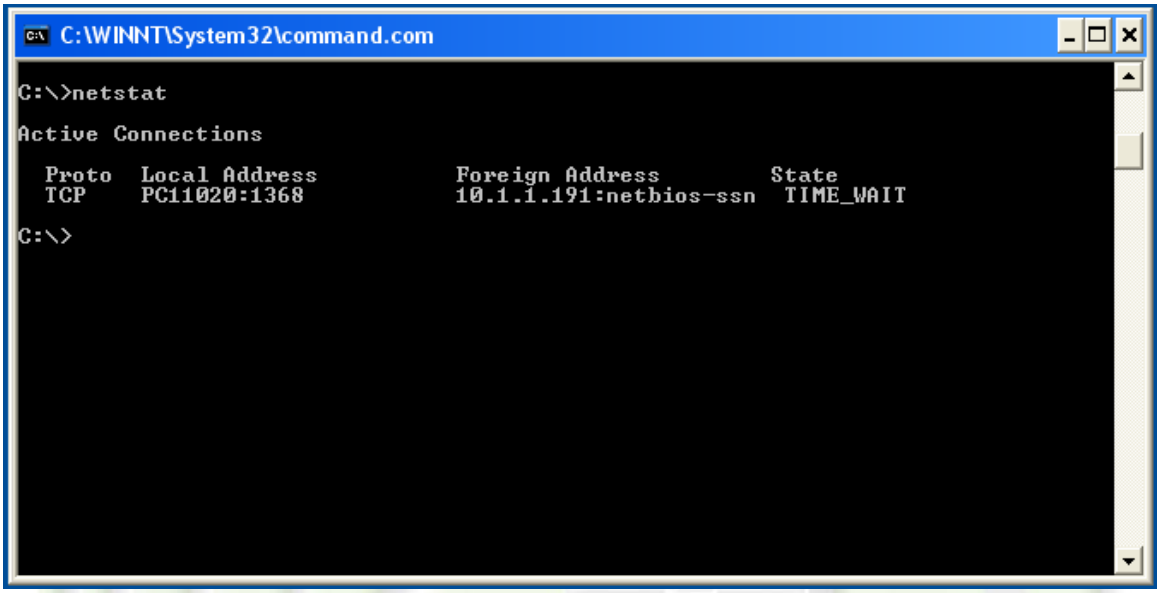
Step 2:

NETSTAT has many switches and options for you to choose from. Type in NETSTAT /? and press Enter. NOTE: You can use upper or lower case letters at the command prompt. On windows, these commands are NOT case-sensitive. You will see a screen like the one shown below.

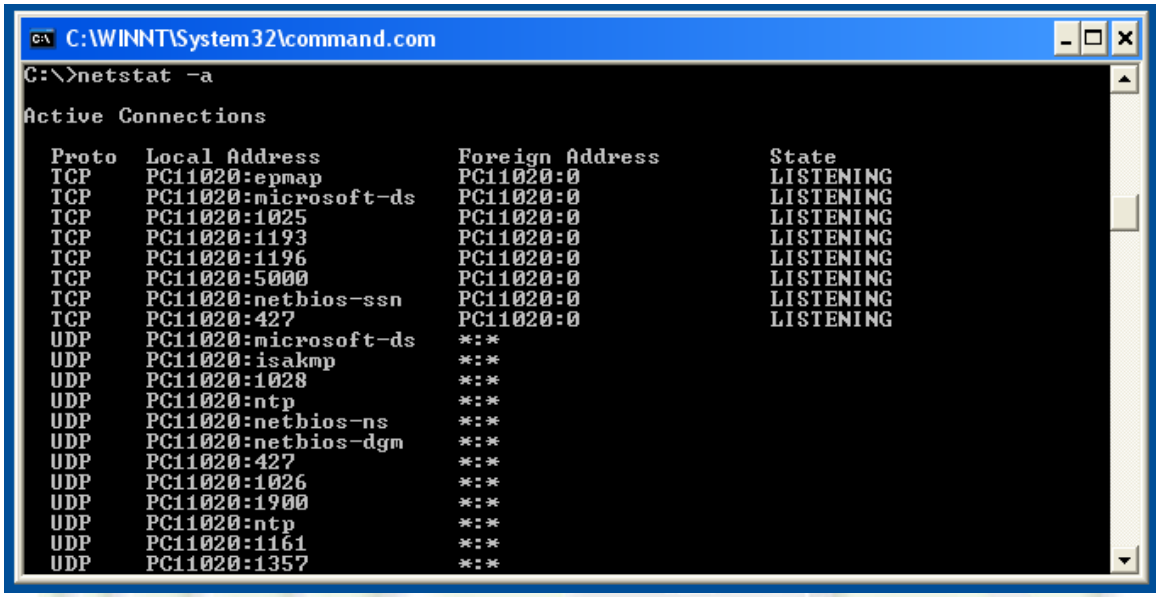


Step 3:

As you can see, it will display protocol stats and your TCP/IP connections. Let's see what your computer TCP/IP ports are doing. Type in NETSTAT and press Enter. On my computer, this is what displayed:

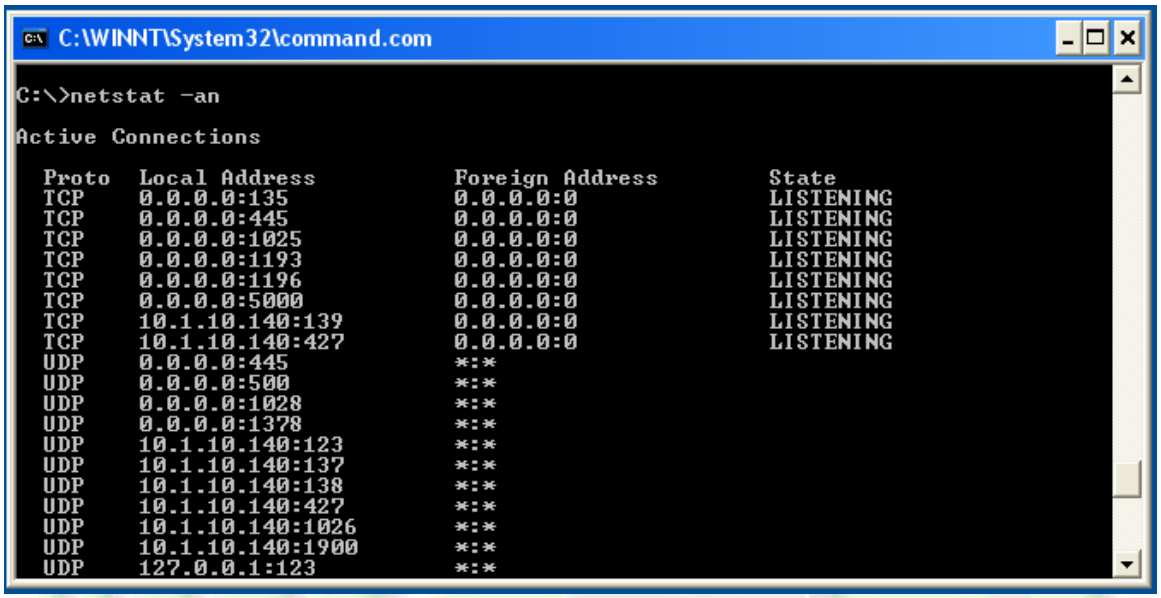


As you can see, this shows *active* connections only. Let's see all the listening and/or established connections as well. To do this type in NETSTAT –A and press Enter. You will see a screen similar to the one shown below.



Unspecified addresses and ports appear as *:*. As you can see from the screen shot shown above, this PC has many listening ports.

You can display the output in a slightly different format as well. Type in NETSTAT –AN and press Enter. You will see something like the screen shot below.



This listing shows it by IP address and port number instead of using the NetBIOS names.

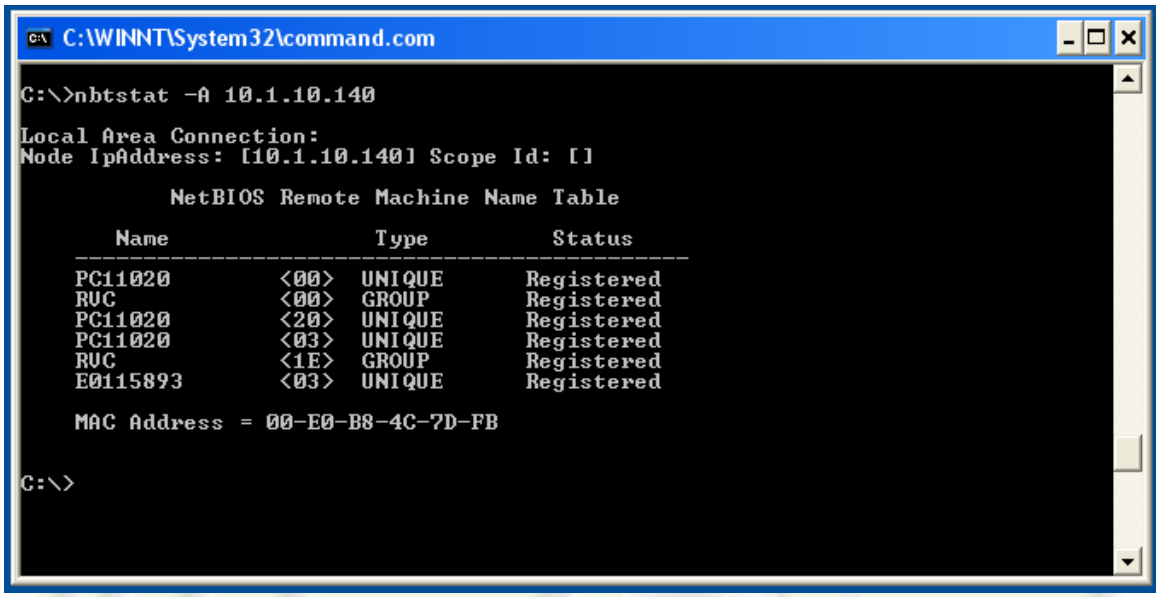
NBTSTAT

Step 4:

Now let's try the NBTSTAT tool. This tool allows you to connect to specific machines (including your own), rather than enumerating the entire network. It will call up the NetBIOS

name table after you issue the command.

At the command prompt, type in NBTSTAT –A *ip-address* where *ip-address* is your own PC IP address. You will see a screen similar to the one shown below.



NBTSTAT extracts the system name, which in this case is, PC11020, and the domain it's in, which is RVC. It will also detect any services running as well as the remote machine's MAC address!

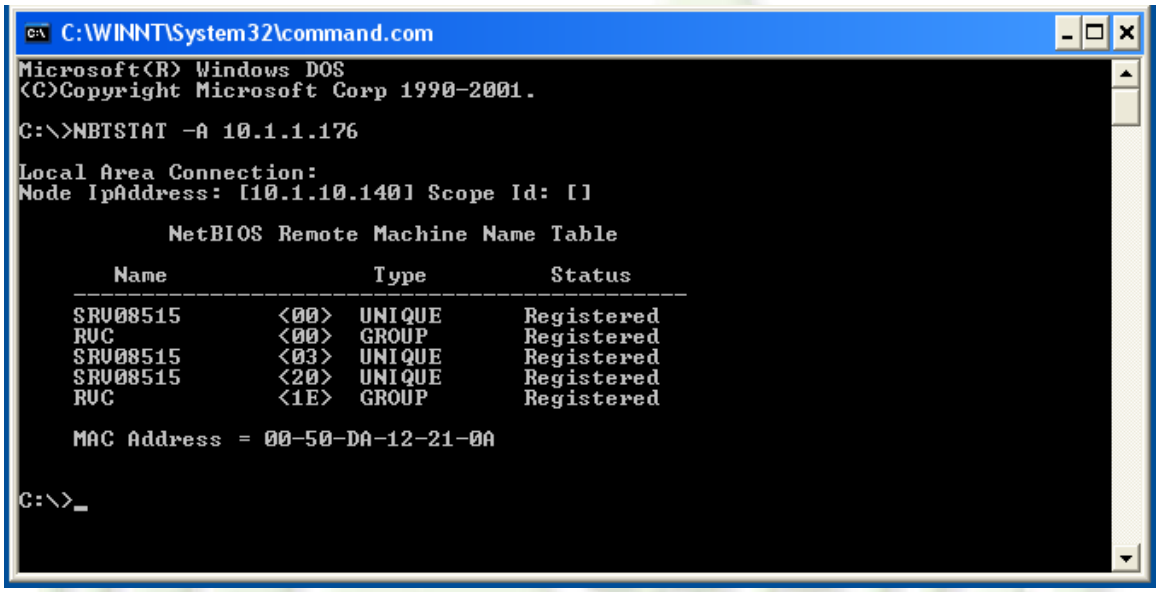
The numbers enclosed in brackets are NetBIOS service codes. A partial listing of these codes are below.

NetBIOS Code	Purpose
00	Workstation name
00	Domain Name

1E	Browser Service Elections
20	File Server Service
03	Messenger Service (for this computer)

Step 5:

Now let's use NBTSTAT to scan a remote machine. Your instructor will give you the IP address and/or name of this machine to scan. At the prompt type in NBTSTAT –A *ip-address* and press Enter, where *ip-address* is the remote address of the machine to be scanned. Sample output is shown below.



Analysis

1) Why would you use these utilities?

2) After working with NBSTAT and NBTSTAT, what about them do you feel you should study further? Why?

3) When would you use these utilities?

4) The NETSTAT command lists listening and active ports. Do some research and find out what those port #s signifiy. What services are those ports running? Would you be able to turn any of these services off?

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.

If You Want To Learn More

What other software tools (both commercial and hacker) provide the same functionality?

Go to http://www.iana.org/assignments/port-numbers to get more information on port numbers and their meanings.

Appendix:

This lab was developed using the NETSTAT and NBTSTAT

utilities in Windows XP, Version 2002, Service Pack 2 (8/04), which may be obtained from:

http://www.microsoft.com

-or-

http://www.download.com

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).