Praktiska övningar Säkerhet i datasystem
Del 2

LAB1
TCP/IP

The Internet was developed to provide a communication network that could function in wartime. Although the Internet has evolved from the original plan, it is still based on the TCP/IP protocol suite. The design of TCP/IP is ideal for the decentralized and robust Internet. Many common protocols were designed based on the four-layer TCP/IP model.

Any device on the Internet that wants to communicate with other Internet devices must have a unique identifier. The identifier is known as the IP address because routers use a Layer 3 protocol called the IP protocol to find the best route to that device. The current version of IP is IPv4. This was designed before there was a large demand for addresses. Explosive growth of the Internet has threatened to deplete the supply of IP addresses. Subnets, Network Address Translation (NAT), and private addresses are used to extend the supply of IP addresses. IPv6 improves on IPv4 and provides a much larger address space. Administrators can use IPv6 to integrate or eliminate the methods used to work with IPv4.

In addition to the physical MAC address, each computer needs a unique IP address to be part of the Internet. This is also called the logical address. There are several ways to assign an IP address to a device. Some devices always have a static address. Others have a temporary address assigned to them each time they connect to the network. When a dynamically assigned IP address is needed, a device can obtain it several ways.

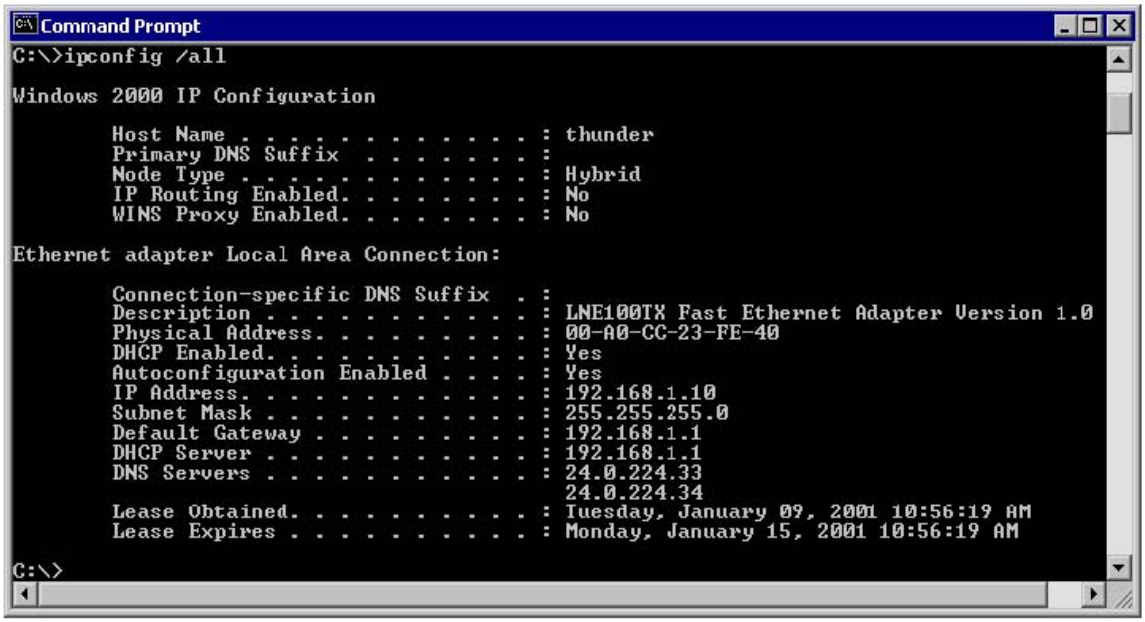
Step 1

Gather TCP/IP configuration information

Use the Start menu to open the Command Prompt, an MS-DOS-like window. Press **Start** > **Programs** > **Accessories** > **Command Prompt** or **Start** > **Programs** > **Command Prompt**.

The following figure shows the Command screen. Type **ipconfig** and press the **Enter** key. The spelling of **ipconfig or ipconfig/all.**

1. What kind of information might be found ?_____



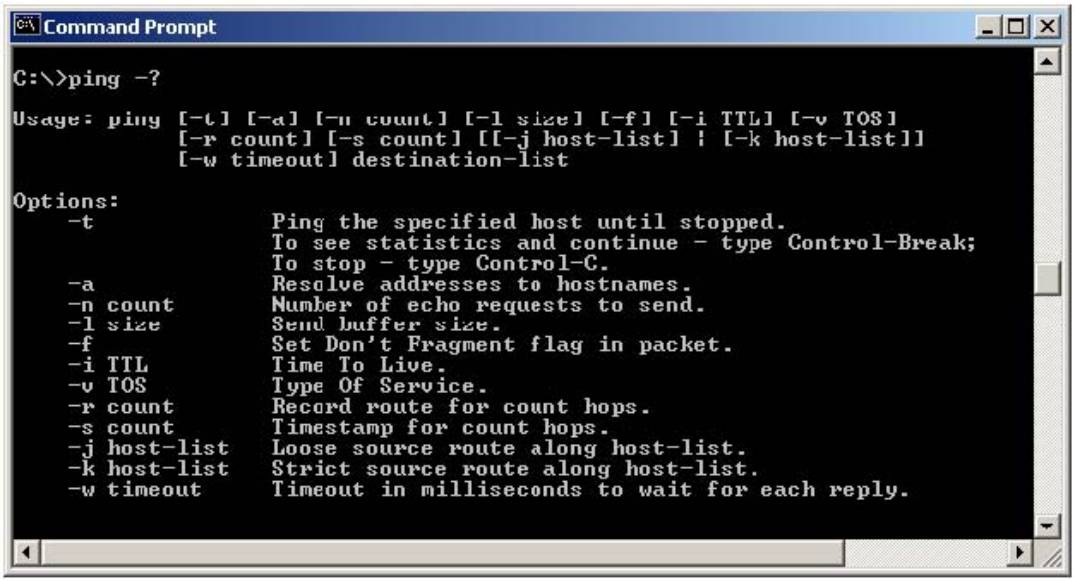
Step 2

Use tracert and ping

Try **tracert -?** and then **ping -?** to see the options available for the commands used previously.

In looking at the help for ping, notice the –t option, which will send continuous pings, not just four. More importantly, notice the two commands to stop it:

- **Control-Break**
- **Control-C**



Try **tracert www.msn.se , tracert www.yahoo.com** and then

ping www.msn.se, ping www.yahoo.com

3. Was the tracert successful? _____

4. Was the ping successful? _____

Step 4

Use Command Prompt and check commands:

nbtstat -?
nbtstat –c
nbtstat –R
nbtstat -S
nslookup
net view
netstat -n

5. What kind of information might be found? _____

6. How somebody else can use this information?_____

Step 5

Answer to the questions 1 to 5 and describe short:

Denial of Service, Ping of Death, IP spoofing, Brute Force, Sniffing packets

LAB2

Personal Software Firewall

"The **perfect personal firewall** would be inexpensive and easy to install and use, would offer clearly explained configuration options, would hide all ports to make your PC invisible to scans, would protect your system from all attacks, would track all potential and actual threats, would immediately alert you to serious attacks, and would ensure nothing unauthorized entered or left your PC." This great definition is quoted from *Make Your PC Hacker Proof*, Jeff Sengstack, PC World, July 21, 2000.

Step 1

Download, install and use one of Personal Software Firewalls :

1. The first option is Windows XP Service Pack 2 and later offers a built-in software firewall.

2. The second options is ZoneAlarm software firewall. You can download free Personal Software Firewall **ZoneAlarm**: www.zonelabs.com

Important Tips

Before installing personal firewall software on a Windows XP computer, be sure that the firewall built into Windows XP is turned off. Never use two software firewalls at the same time. Completely uninstall one before installing another. Use the vendor's uninstalling utility or if not available, use the Windows XP add/remove software tool in the control panel. Testing your firewall is the only sure way to tell that your computer is really being protected.

To find more information about firewalls, try

http://www.firewallguide.com

Step 2

Test drivning your new protektion

After your new firewall protection is up and running you can run a quick test using the port-scanning utility provided by a collection of broadband providers:
http://www.dslreports.com/scan

Click **Probe** and when it finished click **Results.**

Another similar test is provided online by a group opposed to hacking, called Hacker Watch:
http://www.hackerwatch.org/probe/

Click **Port Scan** to start the test.

Step 3

Answer to the questions:

1. How **Personal Software Firewall** works?

2. What are the main features of **Personal Software Firewall**?

3. Which results get you after port scanning? Are your network protected well?

4. How **Personal Software Firewall** can help you to protect your network?

5. What to do if you think you have been hacked?

LAB3

Digital certificate

An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

An individual wishing to send an encrypted message applies for a digital certificate from a *Certificate Authority (CA)*. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.
http://www.webopedia.com/TERM/D/digital_certificate.html

and more
http://www.verisign.com.au/repository/tutorial/digital/intro1.shtml

You look at the digital certificate on Amazon.com to determine whether it is valid and who issued it.

Step 1

Go to http://www.amazon.com

Browse through the products, pick something you would like to order, and add it to your shipping cart. *Do not worry, you are not really going to order, but you need to get to the secure part of the site!*

Step 2

Go to the area where you check out:
Click the **Proceed to checkout** button or link.
It will ask for an email address and a password if you are a returning customer.

Leave the e-mail box blank, enter any password, and press **Enter.** You will get an error about failing to provide an e-mail address, but you will be redirected to the secure page.

Step 3

Answer to the questions 1 to 3

Notice the “https” in the address bar.
Right-click anywhere on the page. On the resulting menu :

- Click **Properties.**
- Click the **Certificates** button.

- Click the **Details** tab.

1.What information does it give you ?

- Click the **Certification path** tab.

2. What information does it give you ?

3. From the information supplied, what can you determine about the certificate?

Close all windows or click the Back button on the toolbar to exit from the page.