Practical Workbook

**Network & Information Security (CT-460)**

****

Name: **Musadique Hussain**

Roll no: **SE-21031**

Batch: **2021**

Department: **Software Engineering**

**Department of Software Engineering NED University of Engineering & Technology**

Practical Workbook

**Network & Information Security (CT-460)**

****

**Prepared By**

**Approved By**

Dr. Shariq Mehmood Khan

Prof. Dr. Najmi Ghani Haider

Associate Professor,

Chairman, SoftwareEngineering

Computer Science and

Information Technology

**Department of Software Engineering NED University of Engineering & Technology**

**C O N T E N T S**

|  |  |  |
| --- | --- | --- |
| **Lab**  **Session No.** | **Object** | **Signature** |
| 1 | Analysis of some Network Tools |  |
| 2 | Implementation of Caesar Cipher and Rot-13. |  |
| 3 | Implementation of Vigenere Cipher and Atbash |  |
| 4 | Implementation of Hill Cipher |  |
| 5 | Implementation of Playfair Cipher |  |
| 6 | Hash Function – Demonstration MD5 |  |
| 7 | Data Encryption Standard (DES) |  |
| 8 | Diffie-Hellman Key Exchange Method |  |
| 9 | RSA (Rivest–Shamir–Adleman) |  |
| 10 | Attack on RSA encryption with short RSA modulus |  |
| 11 | Network Packet Capturing & Analysis through Ethereal. |  |
| 12 | Folder Security Implementation Through BATCH Programming |  |
| 13 | Network Traffic Processing and Analysis |  |
| 14 | NMAP - A Stealth Port Scanner |  |

**Network &Information Security (CT-460) \_\_ Lab Session 01**

|  |
| --- |
| **Lab Session 01** |

**OBJECT: Analysis of some Network Tools**

**THEORY**

∙ **Ping**

ping [-t] [-a] [-n count] [-l length] [-w]

A utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections.

It is often believed that "Ping" is an abbreviation for Packet Internet Groper, but Ping's author has stated that the names comes from the sound that a sonar makes. o **Ping –t**

-t Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop – type Control-C.

Continuously ping the local host, until you press **Ctrl+C**.

This function has no special skills, but can be used in coordination with other parameters o **Ping -a**

Resolve addresses to hostnames. Resolve the NetBios name of PC.

Example: C:\>ping -a 192.168.1.21

Pinging neduet.edu.pk [192.168.1.21] with 32 bytes of data:

Reply from 192.168.1.21: bytes=32 time<10ms TTL=254

Reply from 192.168.1.21: bytes=32 time<10ms TTL=254

Reply from 192.168.1.21: bytes=32 time<10ms TTL=254

Reply from 192.168.1.21: bytes=32 time<10ms TTL=254

Ping statistics for 192.168.1.21:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

The above shows that the NetBios name of the PC with its IP being 192.168.1.21 is **neduet.edu.pk**

Department of Software Engineering

NED University of Engineering & Technology

Page **1** of **75**

**Network &Information Security (CT-460) \_\_ Lab Session 01**

o **Ping –n**

-n count Number of echo requests to send. Send the number of echo packets specified by **count**. Four packets are sent by default. You can use this command to customize the sending count, which is helpful for measuring the network speed. For example, perform the following operation to test the average/maximum/minimum time when 50 packets are returned:

C:\>ping -n 50 202.103.96.68

Pinging 202.103.96.68 with 32 bytes of data:

Reply from 202.103.96.68: bytes=32 time=50ms TTL=241

Reply from 202.103.96.68: bytes=32 time=50ms TTL=241

Reply from 202.103.96.68: bytes=32 time=50ms TTL=241

Request timed out.

………………

Reply from 202.103.96.68: bytes=32 time=50ms TTL=241

Reply from 202.103.96.68: bytes=32 time=50ms TTL=241

Ping statistics for 202.103.96.68:

Packets: Sent = 50, Received = 48, Lost = 2 (4% loss),

Approximate round trip times in milli-seconds:

Minimum = 40ms, Maximum = 51ms, Average = 46ms

The above shows that 48 packets are returned among 50 packets sent to 202.103.96.68, and two packets are lost due to unknown reasons. For the return of 48 packets, the minimum time is 40ms, the maximum time is 51ms, and the average time is 46ms.

o **Ping –l**

-l size Send buffer size.Define the size of echo packet.

The size of ping packets in Windows is 32 bytes by default. You can customize the size and limit it to 65500 bytes. Such limit is set because of a security hole of Windows system. That is, when 65532 bytes or more are sent to the remote end for once, the remote end probably becomes down. Therefore, Microsoft limits the size of ping packets. However, this parameter is

Department of Software Engineering

NED University of Engineering & Technology

Page **2** of **75**

**Network &Information Security (CT-460) \_\_ Lab Session 01**

still harmful in coordination with other parameters. For example, the following is an attacking command by coordinating **-l** with **–t**.

C:\>ping -l 65500 -t 192.168.1.21

Pinging 192.168.1.21 with 65500 bytes of data:

Reply from 192.168.1.21: bytes=65500 time<10ms TTL=254

Reply from 192.168.1.21: bytes=65500 time<10ms TTL=254

………………

In this case, your PC will continuously send packets of 65500 bytes to 192.168.1.21. Sending such packets from several PCs at the same time can make the remote end crash.

o **Ping –w**

-w timeout Timeout in milliseconds to wait for each reply. Specify the timeout, in milliseconds.

By default ,ping waits 1,000ms (1 second) for each response to be returned before displaying the "Request Timed Out" message.if the remote system being pinged is across a high-delay link, such as a satellite link,responses may take longer to be returned. You can use the –w (wait) option to specify a longer time-out.

∙ **IPconfig**

Ipconfig is a DOS utility which can be used from MS-DOS and a MS-DOS shell to display the network settings currently assigned and given by a network. This command can be utilized to verify a network connection as well as to verify your network settings.

ipconfig [/? | /all | /release | /renew| /flushdns | /displaydns ]

|  |  |
| --- | --- |
| /all | Display full configuration information. |
| /release | Release the IP address for the specified adapter. |
| /renew | Renew the IP address for the specified adapter. |
| /flushdns | Purges the DNS Resolver cache. |
|  | /displaydns Display the contents of the DNS Resolver Cache. |

Department of Software Engineering

NED University of Engineering & Technology

Page **3** of **75**

**Network &Information Security (CT-460) \_\_ Lab Session 01**

o I**pconfig /renew**

When you use ipconfig/renew, all network adapters on the computer that uses DHCP (except those are manually configures) try to contact a DHCP server and renew their existing configuration and obtain the new configuration.

o **Ipconfig /release**

You can use the ipconfig command with the /release option to immediate release the current DHCP configuration for a host.

∙ **Traceroute**

The traceroute command traces the network path of Internet *routers* that *packets* take as they are forwarded from your computer to a destination address. The "length" of the network connection is indicated by the number of Internet routers in the traceroute path.

Traceroutes can be useful to diagnose slow network connections. For example, if you can usually reach an Internet site but it is slow today, then a traceroute to that site should show you one or more hops with either long times or marked with "\*" indicating the time was *really* long. If so, the blockage could be anywhere from your Internet service provider to a *backbone provider*, and there is likely little you can do except wait with the infinite patience.

**Syntax**

There are several command-line switches that can be used with TRACERT, but they are usually not needed for standard troubleshooting.

TRACERT syntax:

**tracert [-d] [-h maximum\_hops] [-w timeout] target\_name**

Parameters:

-d Specifies to not resolve addresses to host names.

-h maximum\_hops Specifies the maximum number of hops to search for target. -w timeout Waits the number of milliseconds specified by timeout for each reply. Target\_name Name or IP address of the target host.

∙ **Pathping**

This command combines functions of *Ping* and *Tracert*. *Pathping* will first list the number of hops required to reach the address you are testing and then send multiple pings to each router between you and the destination. After that, it computes results based on the packets returned from each router. Because pathping displays the degree of packet loss at any given router or

Department of Software Engineering

NED University of Engineering & Technology

Page **4** of **75**

**Network &Information Security (CT-460) \_\_ Lab Session 01**

link, you can determine which routers or subnets might be having network problems. Note that the whole process may consume 5-10 minutes because many pings are being sent. There are switches to modify the process and these can be seen by entering "pathping /?" in the command prompt.

∙ **Netstat**

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, **netstat** displays active TCP connections.

**Syntax**

**netstat** [**-a**] [**-e**] [**-n**] [**-o**] [**-p** *Protocol*] [**-r**] [**-s**] [*Interval*]

**Parameters**

**-a :** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

**-e :** Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with **-s**.

**-n :** Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.

**-o :** Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the **Processes** tab in Windows Task Manager. This parameter can be combined with **-a**, **-n**, and **-p**.

**-p Protocol :** Shows connections for the protocol specified by *Protocol*. In this case, the Protocol can be **tcp**, **udp**, **tcpv6**, or **udpv6**. If this parameter is used with **-s** to display statistics by protocol, Protocol can be **tcp**, **udp**, **icmp**, **ip**, **tcpv6**, **udpv6**, **icmpv6**, or **ipv6**.

**-s :** Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The **-p** parameter can be used to specify a set of protocols.

**-r :** Displays the contents of the IP routing table. This is equivalent to the **route print** command.

***Interval* :** Redisplays the selected information every *Interval* seconds. Press CTRL+C to stop the redisplay. If this parameter is omitted, **netstat** prints the selected information only once.

**/? :** Displays help at the command prompt.

Department of Software Engineering

NED University of Engineering & Technology

Page **5** of **75**

**Network &Information Security (CT-460) \_\_ Lab Session 01**

Examples

To display both the Ethernet statistics and the statistics for all protocols, type the following command:

o **netstat -e -s**

To display the statistics for only the TCP and UDP protocols, type the following command: o **netstat -s -p tcp udp**

To display active TCP connections and the process IDs every 5 seconds, type the following command:

o **netstat -o 5**

To display active TCP connections and the process IDs using numerical form, type the following command:

o **netstat -n –o**

∙ **Nslookup**

Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The Nslookup command line tool is available only if you have installed the TCP/IP protocol.

Syntax

nslookup [-SubCommand ...] [{ComputerToFind| [-Server]}]

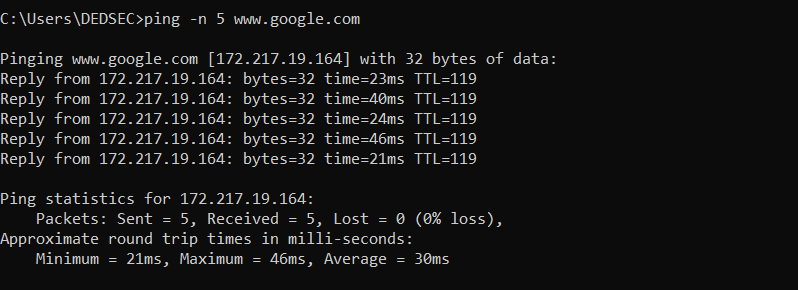
Department of Software Engineering

NED University of Engineering & Technology

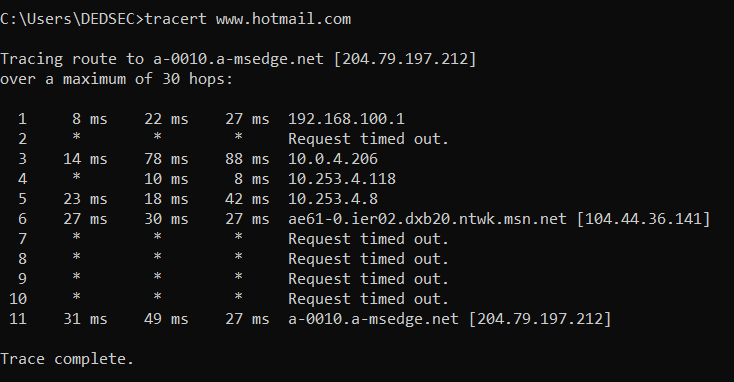
Page **6** of **75**

**EXERCISE**

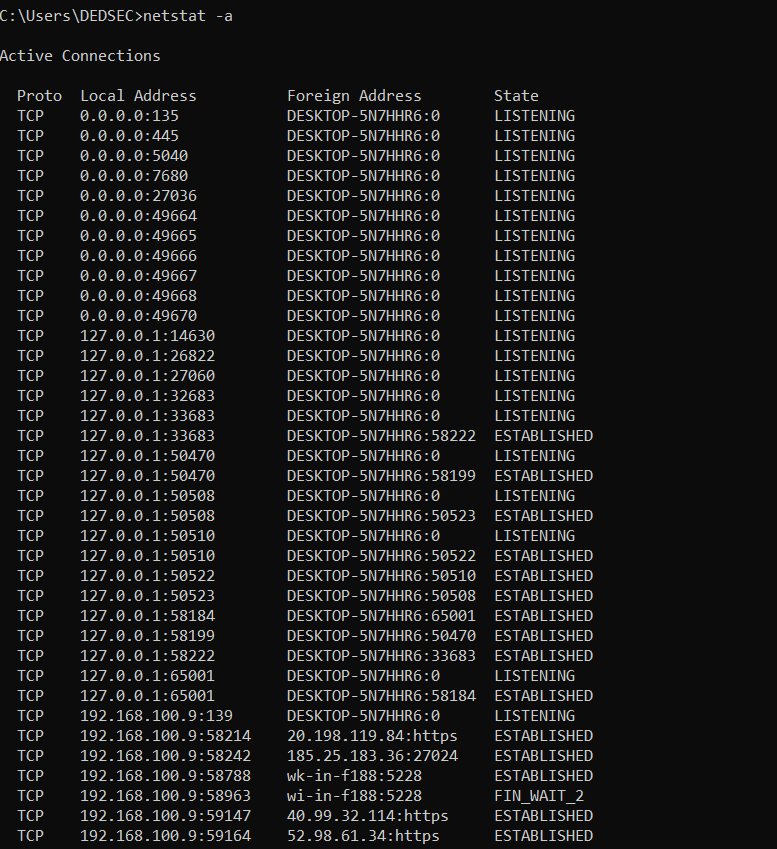
**1. Test the reach ability towards a PC [ ] and limit the number of echoes to 5**

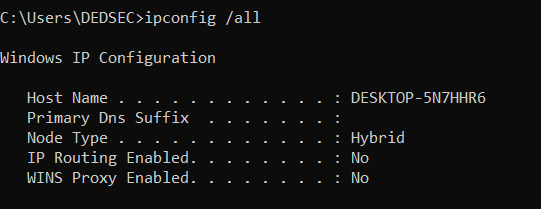
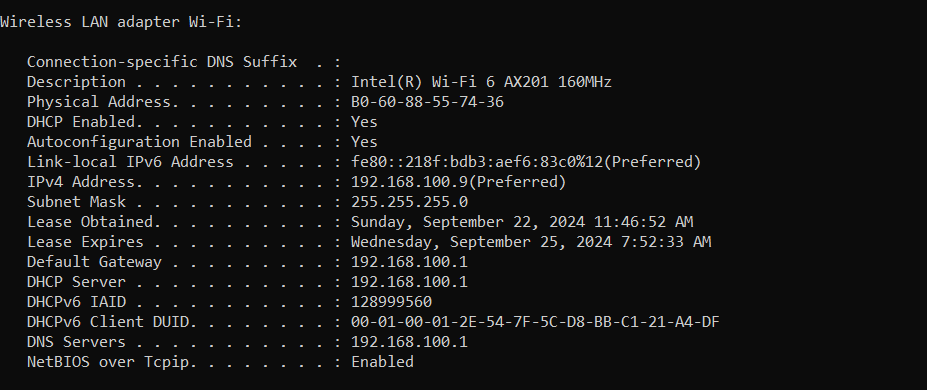
****

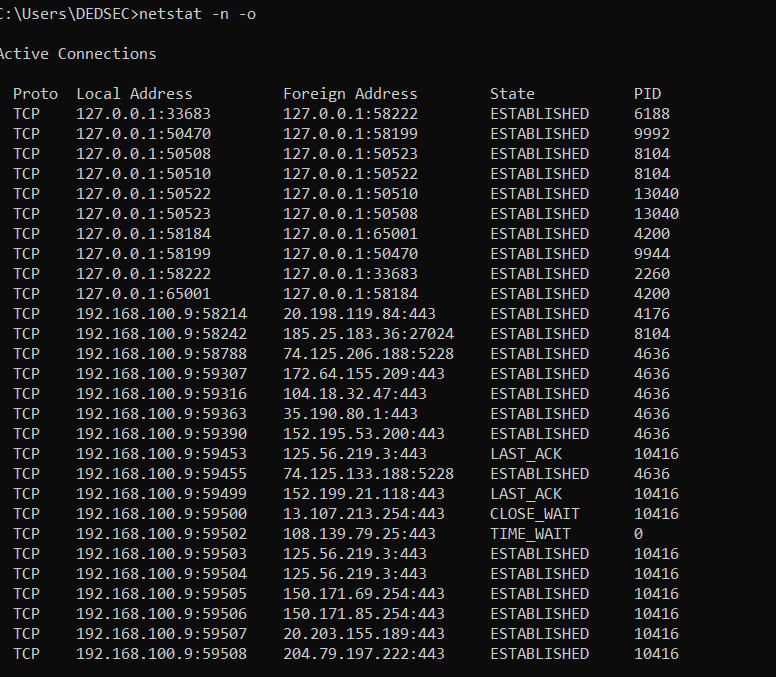
**2. Find the route from your PC to Hotmail i.e [www.hotmail.com]**

****

**3. Open a browser connection to http server [www.yahoo.com] and write down the outcome of the command 'netstat -a'**.



**4. How would you know about the TCP/IP configuration on your PC, write the command and the respective output.**

**5. Which command we use to display active TCP connections and the process IDs using numerical form.**

Department of Software Engineering

NED University of Engineering & Technology

Page 7 of 75

Department of Software Engineering

NED University of Engineering & Technology

Page **7** of **75**

Department of Software Engineering

NED University of Engineering & Technology

Page **7** of **75**