Cybersecurity
Assignment-2.

Name :- Aayushi Bansal

Ans 1 There are 3 owners in Linux system namely owner, group and others.
All the 3 owners have 3 types of Permissions defined.
Nine characters denotes the three types of Permissions.

1. **Read (r) :**
It allows us to open & read the content of a file. But we can't do any editing or modification in file.

2. **Write (w):**
the write Permission allows us to edit, remove or rename a file.

3. **Execute (x) :** In unix type system, we can't run or execute a Program unless execute Permissions is set. But in windows, there is no such Permission available.

File Permissions for (-rw-rw-r--)

1st Position denotes the file type, Position from 2-4 is for user, from 5-7 is owned by group and Position from 8-10 is owned by others.

Ans 2.

1. PING

- This command is used to ensure that a computer can communicate to a specified device over the network.
- It send ICMP Echo request messages in the form of packets to destination comp. & waits in order to get the response back.

eg- Your system IP address is 10.10.10.10
Your network server's IP address is 10.10.10.1
You can check connectivity with server by using the Ping command in following format.

At Dos Prompt type Ping 10.10.10.1 & Press enter, If you get the reply from the server then the connectivity is ok.

2. IPCONFIG

It shows the IP address of comp. and DNS, DHCP, Gateway addresses of the network & subnet mask.

At Dos prompt type ipconfig & press enter to see the IP adress of your computer.

3. NSLOOKUP

It's a TCP/IP based command and it checks domain name aliases, DNS records, OS info by sending query to Internet Domain Name Servers. You can resolve the errors with DNS of your network server.

4. TRACEROUTE

It's a very useful network debugging command and it is used in locating the server that is slowing down the transmission on the internet and it also shows the route between the two systems.

This command prints to the console, a list of hosts through which the packet travels in order to reach the destination.

Ans 3. HTTP

Full form - Hypertext Transfer Protocol.

- HTTP offers set of rules and standards which govern how any info can be transmitted on www.
- HTTP provides standard rules for web browsers & servers to communicate.
- It's an application layer network protocol which is built on top of TCP.
- It uses Hypertext + Structured text which establishes the logical link btw nodes containing text.

HTTPS

Full form - Hyper Text Transfer Protocol Secure.

- It is highly advanced and secure version of HTTP.
- It uses port no. 443 for Data communication.
- It allows the secure transactions by encrypting the entire communication with SSL.

Difference btw the two :

- HTTP lacks security mechanism to encrypt the data whereas HTTPS provides SSL or TLS Digital Certificate to secure the communication btw server and client.

- HTTP operates at Application layer whereas HTTPS operates at Transport layer.

- HTTP by default operates on Port 80 whereas HTTPS by default operates on port 443.

- HTTP transfers data in plain text while HTTPS transfers data in cipher text.

- HTTP is fast as compared to HTTPS.

Ans 4. **Firewall**

- A firewall is a system designed to prevent unauthorized access to or from a network.
- Firewalls can be implemented in both hardware and software.
- The Primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through.

Types of firewalls

1. **Packet Filtering firewalls**
they create a check point at a traffic router or switch.
The firewalls performs a simple check of the data packets coming through the router- inspecting info such as the destination & origination of IP address, packet type, port number, and other surface level info.

2. **Circuit-level Gateways**
It is meant to quickly and easily approve or deny traffic without consuming significant computing resources.
It work by verifying the transmission control protocol handshake.

3. **Stateful Inspection Firewalls**
These firewalls combine both packet inspection technology and TCP handshake verification to create a level of protection greater than either of the previous two architectures could provide alone.

Ans 5.

The following are the Prerequisites to configure a server :

1. LAN card should be connected
2. Root (Partition on which window is installed) should be in NTFS.
3. Server should be configured with a static IP addres.