Mudita Gupta. ASSIGNMENT-02

Q1: There are 3 types of file permissions in Linux

1. Read: permission to read a file
2. Write: permission to write a file
3. Execute: permission to execute a file (run as a program)

The permission are denoted as rwx where r is for read, w is for write & x is for execute.

To revoke a permission a '-' is used in place of the letter

E.g. To denote read permission & execute permission, we would use r-x.

Q2 (1) ipconfig / ifconfig :-

ipconfig (Windows) / ifconfig (Linux/Unix) commands can be used to get IPv4 address, IPv6 address, MAC address, DNS server, default gateways etc. It can also be used to release & renew the IPv4 address, IPv6 address, display DNS cache, clear DNS cache etc.

(2) nslookup :-

It is used to find the IP address corresponding to a domain. We can also carry out reverse DNS look-up. nslookup stands for Name Server look-up.

(3) ping :-

used to test the reachability of the host computer. It sends packets of data to a specific IP address and displays the time taken to send the data and time taken to receive a response. It can be used to test whether our router is working properly or not, whether the network adaptor is working properly or not.

(4) netstat :- (network statistics)

It displays the ~~ports~~ statistics on network activities, routing tables, TCP and UDP ports etc.
It can be used to list all port connections, actively listening ports, ~~etc~~, statistics about the ports, routing information etc

Q3

HTTP	HTTPS
HyperText Transfer Protocol	HyperText Transfer Protocol Secure
The info. transferred b/w server & browser is NOT encrypted.	HTTPs uses SSL (secure sockets layer) certificate. This creates an encrypted connection b/w the server & browser making the connection more secure. HTTPs also use TLS to make the connection more secure.
- HTTP uses default port 80	- HTTPs uses default port 443
- HTTP works at Application Layer	- HTTPS works at Transport Layer

Q4 Firewall is a network security system that monitors the incoming & outgoing data based on some pre-determined rules.

Configuration of firewall -

1. Secure the firewall - update the firewall; change default passwords, delete or rename default accounts.
2. Set up zones - identify assets & group them in zones on the basis of sensitivity level. Once all such zones are set up, create the firewall zones & assign them to firewall interfaces
3. Configure access control list - Identify which traffic is allowed in or out of every zone. This traffic is permitted using access control lists. Deny all unnecessary traffic.
4. Configure other services & logging - Configure the extra services and disable the ones that are not going to be used
5. Test firewall configuration - In a test environment, check whether firewall works correctly, blocks all traffic that should be blocked according to access control list

Q5 Prerequisites to configure a Server

- LAN card should be connected
- Server should be configured w/ a static IP address
- The partition on which window is to be installed should be in NTFS