Assignment -2 based on session-2 & session 3

Ans:1) Read, write & execute

Ans:2)
- Host command
  It is use to find domain name associated with the IP address.
  Ip-config
- It provides commands to enable or disable an interface. It is also use to view MTU.
- Nslookup
  This command queries the DNS in order to fetch the IP address or domain name from DNS record
- Traceroute
  This command is used to trace the route that packet of information takes from our computer to one that is specified.

Ans:3) http stands for hypertext transfer protocol. Communication between client computers & web servers is done by sending http Request and receiving http responses. On the other hand https is the secure version of http.

1) http is unsecured while http is secured.

2) http sends data over port 80 while https uses port 443.

3) http operates at the application layer, while https operates at the transportation layer.

4) No ssl certificates are required for http, with https it is required that you have an ssl certificate and it is signed by CA.

5) http doesn't require domain validation, whereas https requires at least domain validation and certain certificates even require legal documentation validation.

6) No encription in http, with https the data is encrypted before sending.

Ans.4) firewall is a program that surrounds the interface between a private network & the rest i.e bad network.

Configuration:- 1) Securing firewall → Updating firewall to the lastest vendor recommended firmware.
Delete, disable or rename any default user account and change all default password.

2) Architect firewall zones & ip addresses → All the servers that provide web-based service

should be organised into a dedicated zones that limits inbound traffic from the internet - often called a DMZ. Alternatively servers that are not accessed directly from the internet should be placed in internal server zones. If the IP version is 4, internal IP addresses should be used for all your internal networks. Network address translation (NAT) must be configured to allow internal devices to communicate on the internet when necessary.

3) Configure access control lists
4) Configure other firewall services & logging.

Ans-5) User configuration to protect the credential, network configuration for establishing network, package management to add what is needed & to remove what is not needed, firewalls & iptables to minimise external footprints, securing SSH to harden remote sessions, Daemons configuration to minimise the attacting surface, update installation to patch vulerabilities.