Assignment 2.

1) File permissions in linux:
   (a) Read: gives user the authority to - open and read a file, list contents in a directory.
   (b) Write: on a file - gives authority to modify content
   on a directory - gives authority to remove and rename files.
   (c) Execute: gives user the permission to execute/run a program.

2) (a) PING - this command is used to test connectivity b/w 2 hosts.
   (b) TRACERT - (or trace route) used to trace the path that an IP packet takes to its destination.
   (c) IP CONFIG - used to display details of the device's IP address configuration
   (d) ROUTE - this command returns the routing table (used to direct packets).
   Changes can be made to the routing table using:- Route ADD, ROUTE DELETE, ROUTE CHANGE.

3)

HTTP (Hyper Text Transfer Protocol)	HTTPS (Hyper Text Transfer Protocol Secure)
- Lacks security	- Provides secure connection b/w server and client.
- Transfers data in plain text	- Transfered data in encrypted form
- operates on port 80	- operates on port 443
- faster than https	- Slower, since it consumes computational power to encrypt the communication channel.

4) Firewall acts as a filter between the device and the internet. Based on predefined parameters / rules, it can control the passage of data (both inflow and outflow) from the system.

Firewall configuration:-

Step 1: Secure the firewall.

(a) update firewall to latest firmware.

(b) Delete, disable, or rename any default user accounts. Change all default passwords (use only complex and secure passwords).

(c) Never use shared user accounts.
In case of multiple admins managing the firewall, create additional administrator accounts with limited privileges.

(d) disable simple network management protocol or configure it to use secure community string.

Step 2:- Architect firewall zones and IP Addresses.

- Identify & value the valuable assets on your network and plan out your network structure so that the assets can be grouped and placed into networks based on similar sensitivity level and function.

- The more time zones you create, more secure is the network.
- Managing more zones requires additional time and resources.

Step 3: Configure access control lists
- to determine which traffic needs to be able to flow into and out of each zone.
- Access control lists permit traffic thro' the firewall are applied to each interface or subinterface of the firewall.
- Make ACLs specific to the exact source and/or destination IP address and port numbers.
- Make sure to have a "deny all" rule at the end of every ACL list
- Apply both inbound and outbound ACLs to each interface and subinterface on the firewall.

Step 4 :- Configure other firewall services & logging
- configure any other services that the firewall may provide Eg:- network time protocol, intrusion prevention system etc.
- configure the firewall to report to logging server.

Step 5 : Test firewall configuration.
- Testing should include both vulnerability scanning and penetration testing.

5) Prerequisites for server configuration :-

(a) User configuration
- must make sure to change the root password incase it was not part of the OS setup.

(b) Network configuration : enable network connectivity by assigning server an IP address and hostname.

(c) Package management :
- make sure to install the packages you need (incase they are not part of the distribution being used)

(d) Update installation and configuration :
- once installed, make sure everything is updated. to patch any vulnerabilities.

(e) NTP configuration :
- configure your server to sync its time to NTP servers.

(f) Secure SSH :
- SSH is the main remote access method for Linux distributors
- Disable root's ability to SSH it remotely.

(g) Daemon configuration
- set the right applications to autostart on reboot
- turn off any unwanted daemons.

(h) SELinux and further Hardening
- Test your configuration with SELinux enabled.

(i) Logging.