Cyber Security

Assignment - 2.

1.) There are three user types on a LINUX System, User, Group and Other. These owners have 3 types of permissions defined:-

(i) Read. ⇒ Allows you to open & read a file.

(ii) Write ⇒ Allows you to edit, remove, rename a file

(iii) Execute ⇒ Allows you to execute a program.

~~2)~~ In LINUX, in order to execute a program, you need permission. In windows, no such permission is required.

2) (i) PING

Ping command is used to ensure if a host is alive. That is, it helps you to check the Status of a host or a network segement. Ping command sends internet control message protocol echo request messages in the form of packets to the destination computer and waits in order to get the response back. This Command keeps executing until it is interrupted.

(ii) NSLOOKUP

Nslookup is a program to query domain name servers and resolving IP.

(iii) IFCONFIG

Interface configuration (Ifconfig) is used to set or display the IPaddresses and netmask of a network interface. It also provides commands to enable or disable an interface.

(iv) HOST

Host is used to find the domain name associated with IP address or vice versa.

5)

HTTP	HTTPS.
(i) It stands for Hyper Text Transfer Protocol	(i) It stands for Hyper text transfer protocol secure.
(ii) Hyper text exchanged using HTTp goes as plain text. It can be read easily if the exchange of data b/w the browser and server is intercepted.	(ii) HTTPS means hyper text with cryptographic protocols. The data being tranferred between the browser and the server is encrypted.
(iii) It is not secure	(iii) It is secure
(iv) It uses port 80 for data transfer	(iv) It uses port 443 for data transfer.
(v) HTTP opperates at application layer	(v) HTTPS operates at transport layer.
(vi) It requires no SSL certificates	(vi) It requires SSL certificates.
(vii) HTTP does not require domain validation.	(vii) HTTPS requires domain validation and certain certificates even require legal document validation.

4. A firewall monitors and controls incoming and outgoing network traffic based on some security rules. It is a network security system and it establishes a barrier between a trusted and an untrusted network.

Following are the steps to configure a firewall:-

(i) Secure your firewall

- Update firewall
- Change all default passwords. Rename, delete or disable any default user accounts.
- Use complex and secure passwords.
- Create additional administrator accounts with limited privileges in case multiple administrator will manage the firewall.
- Disable simple network management protocol.

(ii) Architect firewall zones and IP addresses

- To protect valuable assets on your network, first they must be identified.
- Once identified, they need to be grouped together and placed into zones based on similar sensitivity level & func^{n}.
- The more the zones, higher the security.

(iii) Configure access control lists

- Now it should be determined exactly which traffic needs to be able to flow into and out of each zone.
- Make your access control lists (ACL) specific to the exact source and destination IP addresses & port numbers whenever possible.
- Disable your firewall administration interface from

public access whenever possible

- Make sure to disable all unencrypted protocols for firewall management

(iv) Configure other firewall services and logging

- Disable all the extra services that you don't intend to use

(v) Test firewall configuration

- In a test environment, verify that your firewall works as intended.

5) The pre-requisites to configure a server are:-

→ User configuration

- One must change the root password, if it wasn't a part of OS set up. The password should be complex.

→ Network configuration

- You must enable network conectivity by assigning the server an IP address and hostname.
- Set the hostname, domain and DNS server info.
- Use 2 or more DNS servers for redundancy.
- Use nslookup to ensure name resolution is working correctley.

→ ~~Re~~Package Management

- Make sure you install packages that you might need eg) PHP, nginx etc.
- Any extraneous packages that are installed on your system should be removed to shrink server footprint

→ Update Installation and Configuration

○ Make sure everything is up-to-date.

→ NTP configuration

○ Configure your server to sync its time to NTP servers

○ It's important to prevent clock drift.

→ Firewalls and iptables.

• Remember to always use the principle of least priveleges and only open those ports you absolutely need.

→ Securing SSH.

° SSH is the main remote access method for Linux distributions and should be properly secured.

→ Daemon Configuration

○ Be sure to turn off any daemons you don't need.

○ Reduce the active footprint as much as possible so the only surface areas available for attack are those required by the applications. This makes the server more secure.

→ SELinux and further hardening.

○ SElinux is a kernel hardening tool and is great at protecting against unauthorized use and access of system resources.

→ Logging.

○ Make sure of the level of logging you need is enabled and that you have sufficient resources for it.