ASSIGNMENT - 2

Q 1. Explain types of file permissions in Linux.

Sol Every file and directory in our linux system has following 3 - permissions defined for all the 3 - owners [User, Group, other]

- Read - This permission give us the authority to open and read a file.
- Write - This permission gives us the authority to modify the contents of a file.
- Execute - In windows, an executable program usually has an extension ".exe" and which we can easily run. In Linux, we cannot run a program unless the execute permission is set. If the execute permission is not set, we might still be able to see/modify the program code (Provided read and write permissions are set), but not run it.

Q 2. Explain any 4 networking and troubleshooting commands.

Sol four networking and troubleshooting commands are:

1. nslookup - nslookup command queries the DNS in order to fetch the IP address or the domain name from DNS records.

2. traceroute - this command is used to get the route of a packet. In other words, traceroute command is used to determine the path along which a packet travels. it also returns the number of hops taken by the packet to reach the

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

3. host - host command is used to find domain name associated with the IP address or find IP address associated with domain name. The returned IP address is either IPv4 or IPv6.

4. netstat - netstat (Network statistics) is the command that is used to display routing table, connection information, the status of ports, etc. This command works with Linux Network Subsystem. This command basically displays the content of proc/net file defined in the Linux file system.

Q 3. What do you mean by HTTP and HTTPS ? Explain the difference between two.

Sol HTTP (Hyper Text Transfer Protocol) is a protocol using which hypertext is transferred over the web. Due to its simplicity, http has been the most widely used protocol for data transfer over the web but the data exchanged using http isn't as secure as we would like it to be. The extra 's' in https stands for "secure". and HTTPS is much more secure compared to http.

- HTTP uses port number 80 for communication while HTTPS uses port number 443 for communication.
- HTTP works at Application layer and HTTPS works at Transport layer.

- On HTTP, Encryption is absent and Encryption is present in HTTPS. ~~as~~ o
- HTTP does not require any certificates and HTTPS needs SST ~~Certifates~~. certificates.

Q 4. What is a firewall ? Explain its configuration.

Sol In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the internet.

we can configure a firewall in 5 steps. that are :

1. Secure your firewall.
   - update your firewall to the latest firmware.
   - delete, disable, or rename any default user accounts and change all default passwords. Make sure to use only complex and secure passwords.
   - if multiple administrators will manage the firewall, create additional administrator accounts with limited privileges based on responsibilities. Never use shared user accounts.
   - disable simple network management protocol (SNMP) or configure it to use a secure community string.

2. Architect your firewall zones and IP addresses.
   In order to protect the valuable assets on your network, you should first identify what the assets are. Then plan out your network structure so that these assets can be

grouped together and placed into networks or zones based on similar sensitivity level and function. The more zones you create, the more secure your network. but managing more zones requires additional time and resources.

3. Configure access control lists.
after your network zones established and assigned them to interfaces, you should determine exactly which traffic needs to be able to flow into and out of each zone.
This traffic will be permitted using firewall rules called access control lists (ACLs), which are applied to each interface or subinterface on the firewall. Make your ACLs specific to the exact source and/or destination IP addresses and port numbers whenever possible.

4. Configure your other firewall services and logging.
if your firewall is also capable of acting as a dynamic host configuration protocol (DHCP) server, network time protocol (NTP) server, intrusion prevention system (IPS) etc., then go ahead and configure the services you wish to use. Disable all the extra services that you don't intend to use.

5. Test your firewall configuration.
verify that your firewall works as intended. Don't forget to verify that your firewall is blocking traffic that should be blocked according to your ACL configurations. Testing your firewall should include both vulnerability scanning and penetrating testing.

Teacher's Signature.....

Date:
Page No.

Q 5. What are the prerequisites to configure a server?

Sol The pre-requisites to configure a server are :

1. User Configuration - The very first thing you are going to wa to do, if it was not part of your OS setup, is change the root password.
2. Network Configuration - One of the most basic configurations you'll need to make is to enable network connectivity by assigning the server an IP address and hostname.
3. Package Management - Presumably you are setting up your new server for a specific purpose, so make sure you install whatev packages you might need if they are not part of the distribution you are using.
4. Update Installation and Configuration - Once you have the right packages installed on your server, you should make sure that everything is updated.
5. NTP Configuration - Configure your server to sync its time to NTP servers.
6. Firewalls and iptables - Depending on your distribution, iptables may already be completely locked down and require you to open what you need, but regardless of the default config. you should always take a look at it and make sure its set up the way you want.
7. Securing SSH - SSH is the main remote access method for linux distributions and as such should be properly secured. You should disable root's ability to SSH in remotely, even if you disable the account.

Signature

Date :
Page No. :

8. Daemon Configuration - its important to set the right applications to autostart on reboot. Be sure to turn off any daemons you don't need.
9. SELinux and Further Hardening - SELinux is great at protecting against unauthorized use and access of system resources. make sure you test your configuration out with SELinux enabled and use the logs to make sure nothing legitimate is being blocked.
10. Logging - finally, you should make sure that the level of logging you need is enabled and that you have sufficient resources for it.

Teacher's Signature.....