Gautika Singh.

03/11/2020

Assignment - 2

Cybersecurity.

(1) In linux we have three types of file permissions, that are :-

(a) Read (r) : The read permission allows us to open and read the content of a file. But we can't do any editing or modification in the file.

(b) Write (rw) : The write permission allows us to edit, remove or rename a file. For example, if a file is present in a directory, and write permission is set on the file but not on the directory, then we can edit the content of the file but can't remove, or rename it.

(c) Execute (x) : In linux-type system, we can't run a program unless execute permission is set.

(2) Networking and Troubleshooting commands :-

(a) nslookup : It queries the Domain Name System (DNS) in order to

fetch the IP address or the domain name for DNS records.

(b) traceroute: This command is used to get the route of a packet. It is used to determine the path along which a packet travels.

(c) host: This command 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.

(d) Arp (Address Resolution Protocol): It is used to display and modify ARP cache, that contains the mapping of IP address to MAC address.
(media access control)

(3) HyperText Transfer Protocol (HTTP) 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 used http isn't as secure as we would like it to be. In fact, hyper-text

exchanged using http goes as plain text i.e. anyone between the browser and server can read it relatively easy if one intercepts this exchange of data. We need the security over the web, because, as it's kinds of 'Online Shopping' at Amazon/Flipkart. In them, as soon as we click on the check-out on these online shopping portals, the address bar gets changed to use https. This is done to make the transfer secure.

Differences b/w HTTP and HTTPS :-

HTTP	HTTPS
(1) URL begins with "http://"	(1) URL begins with "https://".
(2) It uses port number 80 for communication.	(2) It uses port number 443.
(3) It is considered to be insecure.	(3) Whereas it is considered to be secure.
(4) In it, encryption is absent.	(4) In it, encryption is present.
(5) It works at application layer.	(5) It works at Transport layer.

(4) A firewall is a network security system, that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Basically, it establishes a barrier between a trusted network and an untrusted network

Configuration:-

Secure firewall

Step 1 :- → Delete, disable or rename any default user accounts and change all default passwords.

step 2 :- → Architect firewall zones and IP address

In order to protect valuable assets on the network, we should identify what assets are. Then plan out the network structure so that these assets can grouped together and placed into zones based on similar security level.

step 3 :- → Configure access control lists

Now we should determine exactly which traffic needs to be able to flow into and out of each zone.

Step 4 :- → Configure other firewall service and logging

If the firewall is also capable of acting as DHCP, NTP, etc, then we should go ahead and configure the services we wish to use.

Step 5:- Test the firewall configuration

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

5) The prerequisites to configure a server are:-

(i) Extend the active directory schema.
(ii) configure the system management container in active directory.
(iii) Adding windows roles and features on the server.