NPI000040_SNA_FinalExam_Sandesh Subedi 'A'

by Sandesh Subedi

System and Network Administration

Final Exam

Name : Sandesh Subedi 'A'

Student ID : NPI000040

Intake : BSc. IT (Semester III)

Intake Code : NPI2F1909IT

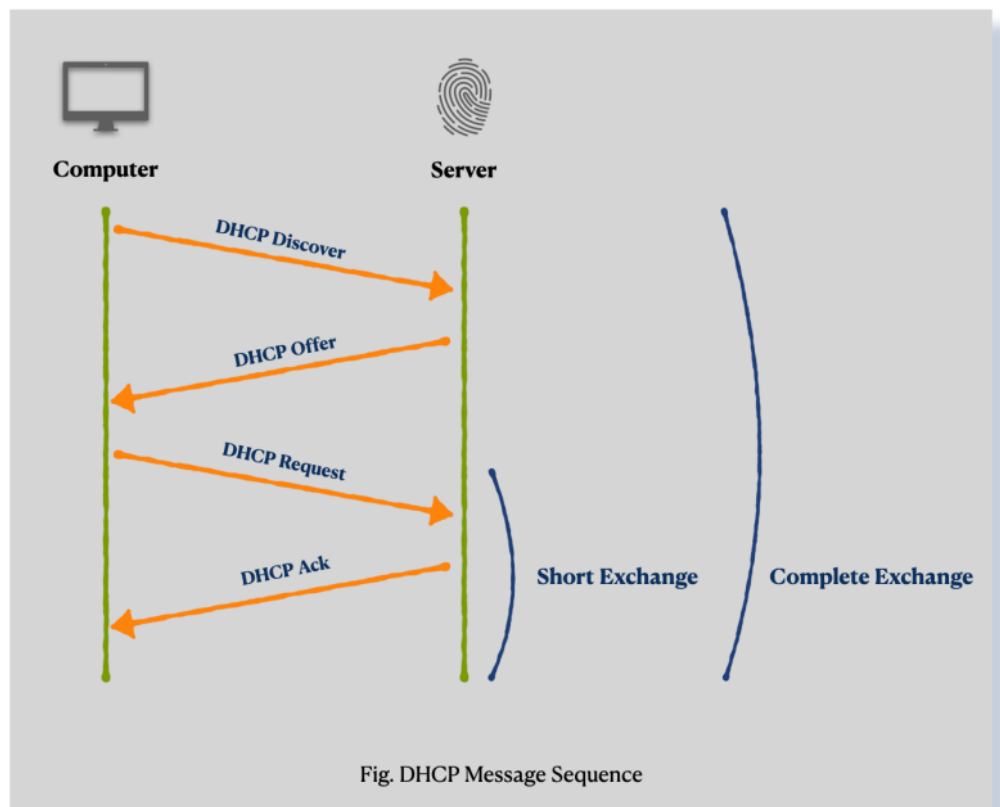**Subject Name : System and Network Administration**

Subject Code : CT106-3-2

Date : 10th September, 2021

Q no. 1) a)

Ans.

The interlinkage between DHCP servers and clients is done with the purpose of issuing distinct networking parameters such as IP addresses, default gateways, etc. The first course of action for this process is done by requesting an IP address, through client's DHCPDISCOVER message transmission. This specific message on local subnet determines configuration having distinctive identifier. Prior to the configuration of protocol software for client section, there is a blockage that disallows unicast datagrams to reach clients server. This is why the message is transmitted as a broadcast so that BOOTP relay and more importantly DHCP server can be given indications in order to broadcast multiple information to client and DHCP server.

Fig. DHCP Message Sequence

The other three messages that are exchanged during DHCP client-server interaction are given below:

i) DHCPOFFER

Once DHCPDISCOVER message is received in subnet servers, the DHCP server might broadcasts a message, to let clients know about its availability. This particular message containing information about network parameters like subnet masks and IP addresses is known as **DHCP Offer**. These information on clients can then be configured as every servers prearrange the IP address as late as the ultimate decision of its usability.

ii) DHCPREQUEST

Considering numbers and service types, the client picks the best DHCP Offer available, while other offers are discarded. Once the server is chosen, active DHCP servers are provided with the notice of client's server selection. After the selection of DHCP Offer, a message is broadcasted with IP address packing server identifier, in order to accept the chosen offer. The message broadcasted during the meantime is known as **DHCPREQUEST**.

iii) DHCPACK

Since servers are notified with DHCPREQUEST, they search the server identifier in order to compare the IP address and hold the address as rented or prearranged. The server whose IP address is matched can assure its selection while others acknowledge their rejections. Now, the selected server broadcasts an acceptance message known as **DHCPACK**, comprising all the valuable and essential organizing information.

Q no. 1) c)

1. Ans.

In the Unix/Linux OS, /etc is a standard directory that is constructed from the origin of file system. In /etc, distinctive files relevant to configuration frameworks are expected to be found. Some of them are listed below :

- passwd that stores data of official operators/users
- inittab that demonstrates the procedures during system commencement
- group that stores data of extant groups
- plenty of .conf files agonizing runtime amenity

Similar to /etc, the /etc/rc.d is also a standard directory which sustain system files that are related to startup and shutdown. The 'rc' in /etc/rc.d stands for run commands (runcom) which executes a group of commands from a file. Inside rc.d script, the /etc/rc.d consist of scripts such as :

- /etc/rc.d/sshd **start**
- /etc/rc.d/sshd **stop**
- /etc/rc.d/sshd **restart**
- /etc/rc.d/sshd **status**

Q no. 1) c)

2. Ans.

Any three differences between /etc/passwd and /etc/shadow are shown below :

/etc/passwd	/etc/shadow
Account Details : passwd is a file that stores foremost user information such as username, directory location, etc during user creation	**Password Details** : shadow is a file that stores password information of users such as password modifications, password expirations, gid, etc.
Readable : The passwd files are world-readable i.e, can be read/viewed by any user accessing to it	**Non-readable** : The shadow file can only be read/viewed by root account unlike passwd files
Passwd files has 7 fields and exists during system installation	Shadow files has 8 fields and are not created in default during system installation

Table : Differences between /etc/passwd and /etc/shadow in tabular form

Q no. 2) a)

Ans

(I) Encapsulation :

   Encapsulation can be defined as a process where headers and trailers are append along with inclusion of some additional information. The TCP/UDP packet used in OpenVPN symbolizes top-level encapsulation, that has extent of about 16 bits. Addition of distinct header data and creation of new conventions after payload is encapsulation. Extending far down, when data is attached to packet header by a etiquette located at dispatching host, it is known as data encapsulation. This furnishes the transmission of data to either header or footer in feasible and appropriate manner. The network model is used and data is encapsulated throughout the transmission layers (from Application to Physical).

   The communication is commenced by the operator during application layer where message is sent and packets are formatted. This enables appropriate packet handling. Then, after the application layer comes Transport layer where encapsulation of data begins. Several steps such as segmentation and connection establishment happens in this step. The next layer, i.e Internet layer uses IP protocols and datagrams so that packets can be distributed with potency to accepting host. Likewise, Data-Link layer converts datagram into a frame with inclusion of header and footer. CRC (Cyclical Redundancy Check) is done with header and the frame is sent to physical layer. The physical layer now accepts the packet frame, transforms IP address into a new hardware address, then computes packet CRC.

(II) Port Forwarding :

   Port forwarding is a process that authorizes approaching internet data from one particular port to another. The port forwarding functions on private network, sending connections to programs and appliances among users associated to a VPN. The Network Address Translation

plays a vital role in portioning out sole public IP addresses, following connections to transmit to Virtual Private Network servers. Afterwards, connections are viewed with their IP and port number for further device processes. The port number is later compared and detachment of port number in any connection automatically disposes connectivity appeal. There are a lot of reasons behind increasing number of port forwarding users. Some of them are given below :

- ◉ Enhancing the download pace for torrents
- ◉ Permitting online amusement hosting
- ◉ Facilitating with remote access to personal devices

Setting port forwarding can allow VPN engaged devices to make swift and easy communications within the same private network. With port forwarding, users can select ports during distant connection, whether they want to shut down or keep ports open.

(III) Virtual Devices :

Virtual devices, also known as virtual peripheral is a file, without any linked hardwares. In Linux/Unix, virtual devices are generated using command 'mknod'. This allows us to generate a new file for writing in it. This file is called socket file. Despite existing in software version only, virtual devices imitates like a hardware that is extant physically. Primarily used for bug detection, virtual devices are just files that are perceived by the kernel as well without any hardware instances.

An example of virtual file in Unix is /dev/null, which immediately alerts the kernel when entered in the system. It notifies the kernel with a message that claims everything to be written appropriately despite being vacant. Similarly to writing, it also notifies about reaching to end of file without the actual truth. This is why it is known as virtual peripheral i.e, considered as a physical device but without hardware existence in actual.
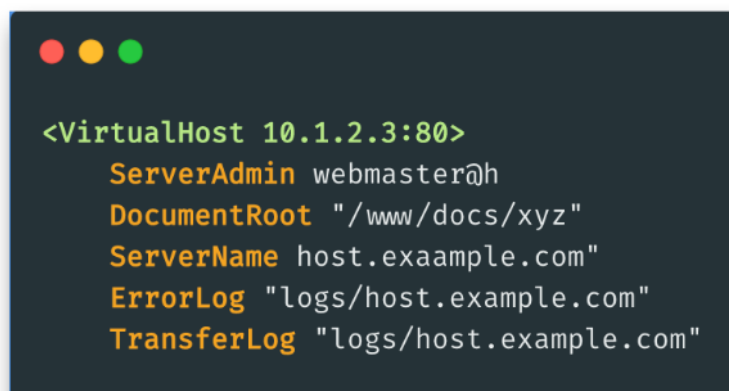
Q no. 2) b)

Ans

CNAME record, also known as Canonical Name record can be defined as a data element used in DNS, to construct a mapping portray of one domain name to the other one. Considering a site 'www.xyz.com' as an example, the prefix of displayed site (www) is known as a CNAME record while xyz.com is a domain. Handful advantages of CNAME records are demonstrated below :

◉ The Canonical Name record provides a specific hostname for a particular networks including FTPs and emails.

◉ Allowance of registration of multiple websites with same domain in different nations

◉ Subdomain for individuals and services (example : sandesh.hostname.com)

Similarly, when a user attempts operating multiple websites within one single machine and identical physical server, this practice is known as Virtual Host. The virtual host can whether be 'name-based' or 'IP-based' considering multiple number of names and IP addresses. The Virtual host directive comprise commands with unique commands, module and status.

```
<VirtualHost 10.1.2.3:80>
    ServerAdmin webmaster@h
    DocumentRoot "/www/docs/xyz"
    ServerName host.exaample.com"
    ErrorLog "logs/host.example.com"
    TransferLog "logs/host.example.com"
```

Fig. VirtualHost Directive (wrt IPV6 example)

Understanding all these distinctiveness between CNAME record and VirtualHost directive, it is evident that their common purpose is to permit multiple websites within a certain geographical location, considering the ip addresses. The hosting of domain name permits sharing of obtainable assets within the server. This further helps in significant reduction of costs and servers as well.

Q no. 2) c)
Ans

ACL stands for **Access Control List**. It is a protocol or collection of regulations that percolates the network traffic by controlling data packets.

Relationship between **ACL** and **Firewall** :

ACL (Access Control Lists) and firewall are two crucial components of network security department. ACL is a protocol that filters arriving and departing packets. Similarly, firewall is network security device that inspects traffic progressing within network. Both ACL and firewall are brought to use, in order to observe and detect the traffic flow within the network system. Most of the functions possessed by ACL and firewall do not have huge difference in many cases. Both firewall as well as ACL wield predefined declarations to compare ingoing and outgoing data. Access Control List (ACL) is moreover used in routing as well while allocating the routing modernization in system network. ACL, despite being less powerful and innovatory than firewall, they can guard quick interfaces while firewall, in some cases, might restrict.

Although the paramount purpose of ACL and firewall is same (network security), there are handful of differences between their functionalities, performances and way of working. One of the major differences between these network security shields is their way of implementation. Firewall might be implemented just for a single purpose but ACL has plentiful of utilizations to

be made. Considering the inspection, ACL and firewall perform stateless and stateful inspection respectively. This means, stateless inspection (done by ACL) prioritizes discrete packets while stateful packets (done by firewalls) studied the whole scenario with required knowledge of TCP conversation as well. One of the major advantage of having firewall is Intrusion detection which is absent in case of ACL. This prohibits the entrance of malicious activities into the network system by strongly shielding and appropriate monitoring.

Q no. 3   b)
Ans

Considering recent studies about advantageous and hinderance impacts of password modifications, the argument between Alice and Bob is consequential and debatable. As we have been following the tradition-like protocols of undergoing password changes frequently in uniform time gap, handful of globally popular companies (eg. Microsoft), stepped forward claiming regular password changes to be a complication rather than a security measure. Most of the companies still believe changing passwords guarantees or strengthens the security like Alice, while there are experts and groups like Bob who rise against them. And understanding the perception on both sides, the outcome is evident : password alteration has both pros and cons.

Observing the scenario from Alice's point of view, she wants to change the password monthly with the intention of assuring user security. With regular password modifications, unauthorized employees in her company won't be accessible to every information. Since staffs in a company can leave or get fired, those people might access the company's data, despite not being associated with their job. Apart from this, regular password changes lessens threat from attackers, at least to some extent. Attackers who use hacking tricks like social engineering and dictionary attacks can be avoided in a lot of cases. Likewise, the password files (shadow) in Linux might have vulnerabilities files which might get cracked and leak credentials. Password
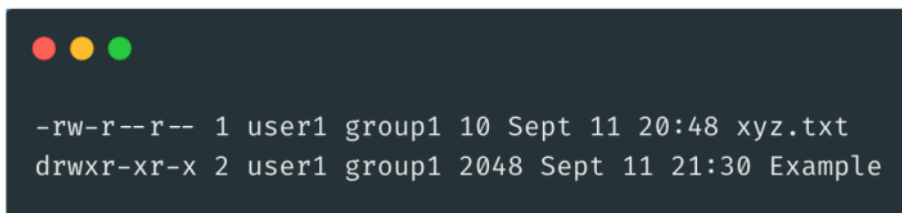
change in these sort of situations, encrypted passwords are different to each other which keeps crackers away from accessing credentials.

Now from Bob's perception, it is not sensible to change passwords every month like Alice is planning. It is difficult not to agree with Bob as there are a lot of drawbacks in password rotation. One of the simplest and foremost reason is poor hygiene because of frequent credential changes. When users are forced to change their passwords within short time period, they are expected to choose easier or less secured passwords in order to remember easily. This promotes weak passwords and hackers or crackers can easily break into their accounts. And when a unethical hacker cracks your credentials, he doesn't wait for a month to perform his activity. This way, it does not make sense to change passwords every month.

Q no. 3) c)
Ans

The use of file permissions as well as Access Control List in UNIX assists in protection or file of user data. Different kind of files require different methods and ownership to keep them secured at highest level using software like WinSCP and SSH Secure Shell, like Alice said. For instance, if a user enters   ls   -lah , the screen will display output similar to picture attached below :

```
-rw-r--r-- 1 user1 group1 10 Sept 11 20:48 xyz.txt
drwxr-xr-x 2 user1 group1 2048 Sept 11 21:30 Example
```

Fig : Sample output of command in plain picture

The output includes r, w, and x which denotes read, write and execute respectively. The letter 'd' in output means directories while file name will also be displayed (say, xyz.com). Considering the special ownership of files and commands, there are three accessible classes for ownership assignation in UNIX. They are :

◉ **User (u) :**

        User is basically the owner who created and owns the file. User has fundamental rights within the system that includes reading (rw-), writing (rw-), implementing and making modifications to the file.

◉ **Group (g) :**

        This class refers to all the members present in user group. This includes user i.e, file owners as well as other members within the ownership group. Group members can read the file but not write or make modifications as shown in output (rwx) above.

◉ **Others (o) :**

        This is the class that denotes users who do not own any file. Furthermore, they are not the group members either but have access to servers.

UNIX offers several unique commands that allows users to modify and keep information safe. Some of the commands includes :

Unix Command	Function
ls	File listing and additional file details
chmod	Alterations in file permissions
chown	Modifies file ownership

Using commands such as chmod, file permissions are set so that only selected or permitted users can access the file according to symbols (r, w, x) described above.

Once the permissions are set for files, the monitor everything functioning around the system and take necessary actions and resistance. The chmod numeric codes perform specific commands focusing system protection from various area.

chmod (numeric value)	Function
400 file	Avoids fortuitous overwriting
500 directory	Avoids fortuitous erasing and modifications
644 file	World-readable (only user/creator can modify)
700 file	Prevents unauthorized entrance

Following, understanding and implementing all these ownership and permissions, unauthorized access can be denied and Bob's user files containing his information can be kept in high level of security.

Q no. 3) a)
Ans

AAA is a standard security framework that monitors and guides permissions to available resources within the network. Comparing 3As to other three provided options, close relations can be found between :

◉ Accounting - Packet Filter

Accounting is basically used when a certain report or audit is being created. During this, data are collected and they are analyzed : from packet lists implementation. Packet

Filter basically filters network traffic flow and examines IP addresses (source and destination), flags, port numbers (source and destination) and several other ports and packets. A packet is transmitted, riddled and compared with protocols which further goes into acceptance/declination.

◉ Authentication - Username + Password

Username and passwords are considered to be one of the most ordinary, historic and yet most convincible means of authentication. These two elements are used to verify whether a user is actually authorized. Having several other factors such as biometrics and body parts scanning, passwords and usernames are still mandatory in most of the websites and applications. Most of the websites today ask users to create an account with username and password for authentication about what their users know. Then, users need to enter their credentials (username + passwords) during login which are sent to internal server for authentication. Once it is approved, user gets access to whichever applications or websites, he's trying to use.

◉ Authorization - Intrusion Detection System (IDS)

The Intrusion Detection System (IDS) monitors and alerts the system admin if any sort of confusions and unethical attempt are made to trespass the system. This intrusion system examines network traffic circulation and inspects if there's any doubtable ventures or entrances. An internal signature database is used to study attack patterns and the incoming threats are obstructed with closure of hacker's port. Moreover, activities like connectivity analysis and port matching are also performed by IDS. The only way to access confined areas in presence of IDS is with completion of identification which allows necessary steps to be taken for further authorization.

Q no. 1) b)

Ans

The reason for requirement of multiple interfaces is to have access to multiple network by an instance. With multiple network interfaces, the communication speed is strengthen and more dependable. Moreover, multiple alternatives are available in NIC card ports along with access of sharing bulk data within connected users.

The IP addresses assigned to these interfaces do not change. This is because it facilitates users with suitable remote access using programs like Virtual Private Networks. With permanent assignation of IP address, the connection is more reliable compared to that of dynamic. Despite costing higher in contrast to dynamic methodology, the permanent IP address assignation offers better DNS servers, hosting servers and geo-location facilities.