1 Mark Questions

1)SSH stands for

SSH:- Secure Shell

2)Where do you locate SSH configuration files?

etc/ssh

3)Name the SSH server package

”openssh-server” Package

4)Name the SSH client package

”open-ssh-client” Package

5)What is IP spoofing?

IP Spoofing:- Sending false package to look like right host

6)What is DNS Poisoning?

7)How to login to SSH server using SSH client?

ssh username@hostname→ ssh [User124@example.com](mailto:User124@example.com)

7 Marks questions

1)What is SSH ? What are the main features?

SSH (Secure Shell) is a protocol which facilitates secure communications between two systems using a client-server architecture and allows users to log in to server host systems remotely. Unlike other remote communication protocols, such as FTP or Telnet, SSH encrypts the login session, rendering the connection difficult for intruders to collect unencrypted passwords.

* No one can pose as the the intended server
* After an initial connection, the client can verify that it is connecting to the same server it had
* connected to previously.
* No one can capture the authentication information
* The client transmits its authentication information to the server using strong, 128-bit
* encryption.
* No one can intercept the communication
* All data sent and received during a session is transferred using 128-bit encryption, making
* intercepted transmissions extremely difficult to decrypt and read.
* Additionally, it also offers the following options:
* It provides secure means to use graphical applications over a network
* Using a technique called X11 forwarding, the client can forward X11 (X Window System)
* applications from the server.
* It provides a way to secure otherwise insecure protocols
* The SSH protocol encrypts everything it sends and receives. Using a technique called port forwarding, an SSH server can become a conduit to securing otherwise insecure protocols, like POP, and increasing overall system and data security.
* It can be used to create a secure channel
* The OpenSSH server and client can be configured to create a tunnel similar to a virtual
* private network for traffic between server and client machines.
* It supports the Kerberos authentication
* OpenSSH servers and clients can be configured to authenticate using the GSSAPI (Generic
* Security Services Application Program Interface) implementation of the Kerberos network
* authentication protocol.

2)What are the major types of attacks on Network System?Explain.

Interception of communication between two systems

The attacker can be somewhere on the network between the communicating parties,

copying any information passed between them. He may intercept and keep the information,

or alter the information and send it on to the intended recipient.

This attack is usually performed using a packet sniffer, a rather common network utility that

captures each packet flowing through the network, and analyzes its content.

Impersonation of a particular host

Attacker's system is configured to pose as the intended recipient of a transmission. If this strategy

works, the user's system remains unaware that it is communicating with the wrong host.

This attack can be performed using a technique known as DNS poisoning, or via so-called IP

spoofing. In the first case, the intruder uses a cracked DNS server to point client systems to a

maliciously duplicated host. In the second case, the intruder sends falsified network

packets that appear to be from a trusted host.

3)What are the steps involved in establishing a SSH communication between two hosts.

The primary role of the transport layer is to facilitate safe and secure communication between the two hosts

at the time of authentication and during subsequent communication. The transport layer accomplishes this by handling the encryption and decryption of data, and by providing integrity protection of data packets as they are sent and received. The transport layer also provides compression, speeding the transfer of information.

Once an SSH client contacts a server, key information is exchanged so that the two systems can correctly construct the transport layer. The following steps occur during this exchange:

* Keys are exchanged
* The public key encryption algorithm is determined
* The symmetric encryption algorithm is determined
* The message authentication algorithm is determined
* The hash algorithm is determined

To connect to an OpenSSH server from a client machine, you must have the openssh-clients Package

The ssh utility allows you to log in to a remote machine and execute commands there. It is a secure replacement for the rlo g in, rsh, and telnet programs.

To connect to server use: ssh username@hostname→ssh [sam@example.com](mailto:sam@example.com)

4)Give the procedure to start SSH service at aserver and to log in to it from a remote   
PC.

First as a server we should install openssh server package we have to get root privilege for modification

1. To start service we use: systemctl start sshd.service
2. To make the service automatically start we use: systemctl enable sshd.service
3. To log in from remote PC as user we use:ssh username@hostname→ssh [sam@example.com](mailto:sam@example.com)
4. Here openssh can also be used:

5)What is scp? Give the procedure to copy a local file remote file and also remote file to local file using scp.

SCP can be used to transfer files between machines over a secure, encrypted connection. In its design, it is very similar to rcp.

scp local file username@ hostname: remotefile

For example, if you want to transfer a tag list. vim to a remote machine named

penguin. example. co m: scp tag list. vim USER @ penguin. example. com:. vim/plugin/tag list. Vim

Multiple files can be specified at once. To transfer the contents of . vim/plug in/ to the same

directory on the remote machine penguin. example. co m→USER @ penguin. example. co m:. vim/plug in/

To transfer a remote file to the local system, use the following syntax:scp username@ hostname: remotefile localfile

eg:-scp USER @ penguin. example. co m:. vimrc . vimrc

6)What is sftp? List the different commands available in sftp

The sftp utility can be used to open a secure, interactive FTP session. In its design, it is similar to ftp except that it uses a secure, encrypted connection.

To connect to a remote system, use a command in the following form:-->sftp USER @ penguin. example. co m USER@ penguin.example.com

set of commands in sftp

● ls [directory]:-List the available files

● cd directory:-Change or switch directory

● mkdir directory:- make directory

● rmdir path:- remove directory

7)Give the different packages and their significance available with openssh package.

Red Hat Enterprise Linux includes the general OpenSSH package, openssh, as well as the

OpenSSH server, openssh-server, and client openssh-clients, packages The OpenSSH packages require the OpenSSL package openssl-libs, which installs several important cryptographic libraries

In order to run an OpenSSH server, you must have the openssh-server package installed

systemctl start sshd.service

To stop the running sshd daemon in the current session

systemctl stop sshd.service

If you want the daemon to start automatically at the boot time, type as root

systemctl enable sshd.service

To connect to an OpenSSH server from a client machine, you must have the openssh-clients package installed

The ssh utility allows you to log in to a remote machine

● Ssh It is a secure replacement for the rlogin, rsh, and telnet programs.

* To Login as User we use ssh username@hostname→ssh [sam@example.com](mailto:sam@example.com)