Chapter – 8 CONFIGURING AND SECURING SSH

Objectives:

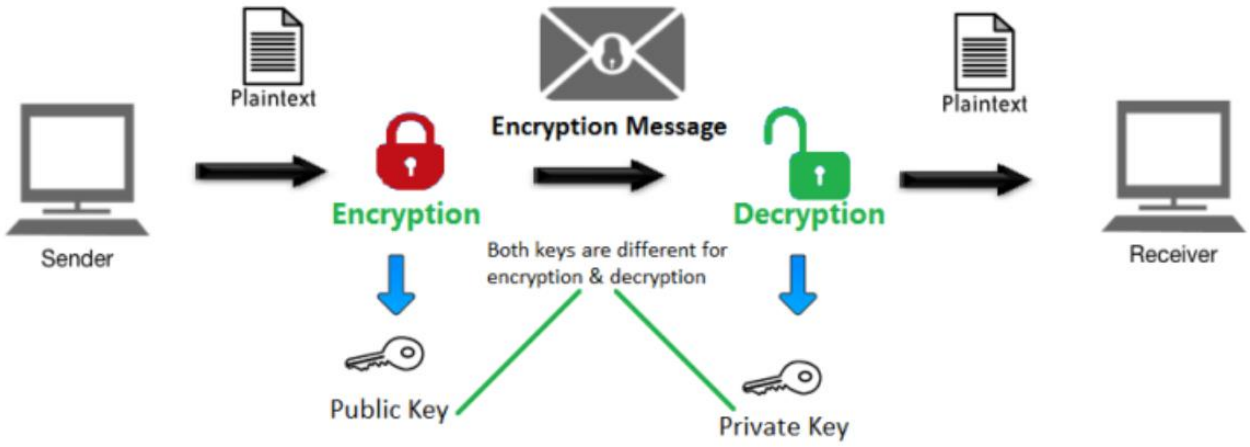
- Log in to a remote system and run commands using ssh.
- Configure key-based authentication for a user account to log in to remote systems securely without a password.
- Restrict direct logins as root authentication for the OpenSSH service.

ACCESSING THE REMOTE COMMAND LINE WITH SSH

WHAT IS OPENSSH?

OpenSSH implements the Secure Shell or SSH protocol. The SSH protocol enables systems to communicate in an encrypted and secure fashion over an insecure network.

Command: ssh user@remotehost



CONFIGURING SSH KEY-BASED AUTHENTICATION

SSH KEY-BASED AUTHENTICATION

Generating SSH Keys

Command: ssh-keygen

Your private and public keys are saved in your ~/.ssh/id_rsa and ~/.ssh/id_rsa.pub files, respectively.

Sharing the Public Key

Command: ssh-copy-id user@remotehost

CUSTOMIZING OPENSSH SERVICE CONFIGURATION

CONFIGURING THE OPENSSH SERVER

OpenSSH service is provided by a daemon called sshd. Its main configuration file is /etc/ssh/sshd_config.

PROHIBIT THE SUPERUSER FROM LOGGING IN USING SSH

Some of the risks of allowing direct login as root include:

- The user name root exists on every Linux system by default, so a potential attacker only has to guess the password, instead of a valid user name and password combination. This reduces complexity for an attacker.
- The root user has unrestricted privileges, so its compromise can lead to maximum damage to the system.
- From an auditing perspective, it can be hard to track which authorized user logged in as root and made changes. If users have to log in as a regular user and switch to the root account, this generates a log event that can be used to help provide accountability.

Value in file: PermitRootLogin yes