Unit 2
SSH

What is SSH?

- SSH is a protocol for secure remote access to a machine over untrusted networks
- SSH is a replacement for telnet, rsh, rlogin and can replace ftp
- Uses encryption
- SSH is not a shell.

Features

- Transmission is secure
- Transmission can be compressed
- No login password required

- **Drawbacks of using telnet**
  - Sends data in clear text
  - Host between sender and receiver can see what the traffic is
- **Why should we encrypt data?**
  - Use the same password in more than one place
  - Data in the network is secured
- **Functions of Secure Shell**
  - Secure Command Shell
  - Port Forwarding
  - Secure file transfer

Secure command Shell

- Allows you to edit files
- View the contents of directories
- Custom based applications
- Create user accounts
- Change permissions

Port Forwarding

- Powerful tool
- Provide security to TCP/IP applications including e-mail , databases and applications
- Allows data from normally unsecured TCP/IP applications to be secured

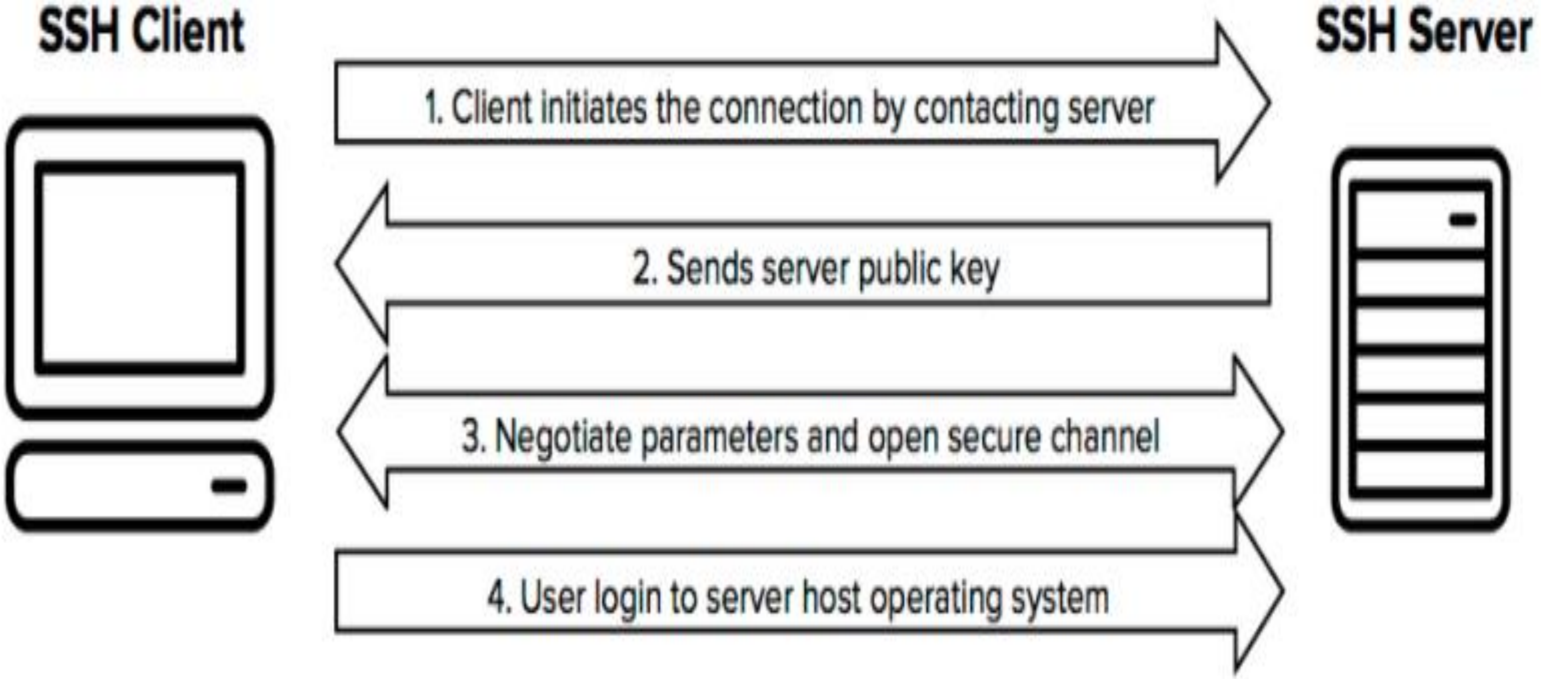
Secure File Transfer

- Secure File Transfer Protocol is a subsystem of the secure shell protocol
- Separate protocol layered over the secure shell protocol to handle file transfers
- SFTP encrypts both username/password and the data being transferred
- Uses the same port as the secure shell server

Components of secure shell

- **SSHD server**: a Program that allows incoming SSH connections to a machine, handling authentication, authorization
- **Clients:** A Program that connects to SSH servers and makes requests for service
- **Session:** An on-going connection between a client and a server. It begins after the client authenticates to a server and ends when the connection terminates

How does SSH Work


SSH Client
SSH Server
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system

How secure shell works?

- When SSHD is started, it starts listening to port22 for a socket.
- When a socket get connected the secure shell daemon spawns a child process. Which in turn generates an host key eg: RSA.
- After key is generated the secure shell daemon is ready for the local client to connect to another secure shell daemon or waits for a connection from remote host

Security Benefits

- User Authentication
- Host Authentication
- Data encryption
- Data Integrity

Public Key authentication

- Public Key authentication uses a pair of computer generated keys – one public and one private. Each key is usually between 1024 and 2048 bits in length
- To access an account on a secure shell server, the client initiates the request through a particular port. When the server get the request, at the destination port, the server start a session and sends the server public key. When the client connects to the server it proves that it has the public, key of that server, and access is granted
- Encryption – data is protected and sent on the wire

Authentication with SSH keys

- The idea is to have a cryptographic key pair - public key and private key . The public key is shared with everyone and is used for encryption. The private key is a secret key and can used by itself for decryption. The keys used for authentication are called SSH keys.
- The main use of key-based authentication is to enable secure automation.
- Once a connection has been established between the SSH client and server, the data that is transmitted is encrypted according to the parameters negotiated in the setup.
- During the negotiation the client and server agree on the symmetric encryption algorithm to be used and generate the encryption key that will be used.