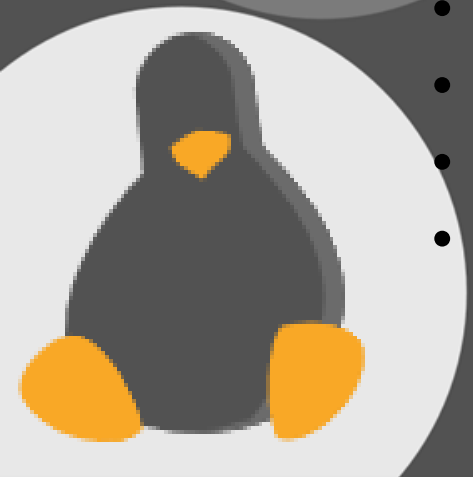
Open Source Community

SSH → Secure Shell

Agenda;

- What Is SSH
- What can SSH Do for me
- Server/Client communication
- Authentication Methods
- Installing SSH
- OpenSSH
- How to SSH a Server
- Network command
- Network Configuration File



What is SSH

- SSH is a network protocol that provides secure transport between two devices
- Gives system and network administrators a secure way to access a device over an unsecured network
- Replaces old remote login programs that transmitted user passwords in clear text and data unencrypted (Telnet)

What Can SSH Do For Me

- Provides authentication and encryption .
- Performs checks on data being transferred throughout a session to ensure integrity .

Server/Client Communication

- The device you want to remotely connect to is called the server
- The device you are trying to connect from is the client
- Both the server and client need to have their respective SSH programs installed
    - client will need to have ssh command available
    - server will need to be running the sshd daemon

Authentication Methods

- Password based authentication
  - server prompts the user to enter their passwords
  - it checks the password against the entry in the passwd file

- Key based authentication
  - Bypasses the password prompt all together
  - Uses Private/public keys to authenticate the user

- Hot based authentication
  - Allows a single user , or group of users on the client to be authenticated on the server
  - File is configured to allow specific hosts to connect to the server

Installing SSH

Debian :

$ sudo apt install openssh-server openssh-client

Fedora :

$ sudo dnf install openssh-server openssh-client

OpenSSH

- Is a free and open source implementation of SSH
- Has 3 packages :

  - openssh → porivdes the ssh-keygen command

  - openssh-clients → includes commands like ssh , scp,scftp,slogin and a comes with config file /etc/ssh/ssh_config

  - openssh-server → contains the sshd daemon and config file /etc/ssh/shd_config

How to SSH a Server

$ ssh username@ip -p [port] (by default 22)

Key Based Authentication

- On the client, ssh keys need to be generated
  $ ssh-keygen
- Private key will be located in ~/.shh/id_rsa
- Public key will be located in ~/.ssh/id_rsa.pub
- Once keys are generated, the clients public key will need to be copied over to the servers authorized_keys file

Copying Keys to Server

- $ ssh-copy-id username@ip
- $ scp .ssh/id_rsa.pub username@ip:/home/username/.ssh/authorized_keys

Network command

- Ifconfig
- Ip add
- Ping
- Traceroute
- NSLOOKUP
- NMAP

Network configuration File

- **/etc/resolve.conf**
- **/etc/hosts** → It has ips of the local hosts
- **/etc/NetworkManager/system-connections/** → This directory has all information about network you have logged in before.
- **/etc/services** → It has tcp/udp services and their ports
- **/etc/protocols** →It has protocols and their usage

Thank you

#Stay_Safe