

Intro to Linux

2.4.1 - Secure Shell Protocol (SSH)



Secure Shell

SSH, or Secure Shell, is a robust protocol for a secure means of connecting to and managing remote machines

- Involves configuration files, commands, and tunneling capabilities that enhance the security and functionality of remote connections



SSH Configuration Files

SSH configuration relies on several key files

- `/etc/ssh/sshd_config` is for server-side settings
- `/etc/ssh/ssh_config` is for client-side configurations
- `~/.ssh/known_hosts` stores host keys
- `~/.ssh/authorized_keys` lists authorized public keys for server access
- `~/.ssh/config` serves as a personal configuration file for customizing SSH behavior



SSH Commands

The SSH suite includes essential commands for using SSH

- ssh-keygen generates secure key pairs
- ssh-copy-id facilitates logins without needing passwords by copying public keys to remote servers
- ssh-add manages private keys through the SSH authentication agent



SSH Tunneling

The SSH utility can be extended using tunneling options

- X11 Forwarding enables graphical application forwarding from a remote server to the local machine
- Port Forwarding redirects network traffic
- Dynamic Forwarding establishes a SOCKS proxy for secure browsing and traffic forwarding

