SSH Cheatsheet

OpenSSH is a suite of secure networking tools that provide encrypted communication between computers over an unsecured network, primarily used for remote server management. It includes essential utilities like the SSH client and SSHD server, along with support for file transfers, secure copy (SCP), and secure file transfer protocol (SFTP).

📗 Definitions

SSH (Secure Shell)	A protocol for securely accessing remote machines over an encrypted connection.
OpenSSH	The most common implementation of SSH on Linux, providing client and server tools.
SSH Key Pair	A pair of cryptographic keys (private and public) used to authenticate users securely.
SSHD (SSH Daemon)	The server-side component of SSH, which listens for and manages SSH connections.
SSH Agent	A program that stores private keys in memory to simplify multiple connections.
Known Hosts File	A file listing trusted remote hosts, usually located at `~/.ssh/known_hosts`.
Authorized Keys	A file on the SSH server that stores public keys of authorized users for key-based login.
Host Key	A key unique to each SSH server, used to verify the server's identity.

🔑 Basic Commands

ssh user at host	Connect to a remote server as a specified user.
ssh-copy-id user at host	Copy a user's public key to a remote server for key-based authentication.
ssh-keygen	Generate a new SSH key pair (private and public keys).
scp file user at host:path	Securely copy files from a local machine to a remote server.
scp user at host:file path	Securely copy files from a remote server to the local machine.
ssh-add	Add a private key to the SSH agent for session persistence.
ssh-agent bash	Start a new shell session with the SSH agent for managing keys.

⚓ Configuration

Disable Root Login	Prevent root access by setting `PermitRootLogin no` in `sshd_config`.
Key-Based Authentication	Stronger authentication using SSH keys instead of passwords.
Limit Users	Restrict access with `AllowUsers` or `DenyUsers` settings in `sshd_config`.
Change Default Port	Use a custom port to avoid common port 22 scans.
Password Authentication	Disable password login with `PasswordAuthentication no` for better security.
SSH Timeout	Set `ClientAliveInterval` and `ClientAliveCountMax` to manage session timeouts.

Created by: **Trevor Smale**
Version: **1.0**