SSH Cheatsheet

Overview

- SSH (Secure Shell) is a protocol used for secure remote access to a machine over an unsecured network.
- It provides encrypted communication between the client and the server, preventing eavesdropping, tampering, and other security threats.
- SSH is commonly used for remote shell access, file transfers, and tunneling.

Basic Usage

- Connect to a remote machine: `ssh username@remote_host`
- Connect to a remote machine on a specific port: `ssh -p port_number username@remote_host`
- Copy a file from a remote machine to the local machine: `scp username@remote_host:/path/to/remote/file /path/to/local/directory`
- Copy a file from the local machine to a remote machine: `scp /path/to/local/file username@remote_host:/path/to/remote/directory`

Key Management

- Generate an SSH key pair: `ssh-keygen`
- Copy the public key to a remote machine: `ssh-copy-id username@remote_host`
- Add a private key to the SSH agent: `ssh-add /path/to/private/key`
- List the keys in the SSH agent: `ssh-add -l`

Security

- Disable root login: Edit `/etc/ssh/sshd_config` and set `PermitRootLogin no`
- Use key-based authentication: Edit `/etc/ssh/sshd_config` and set `PasswordAuthentication no`
- Use a strong passphrase for the private key: `ssh-keygen -p`

Resources

- OpenSSH Manual Pages
- SSH Wikipedia
- How To Use SSH to Connect to a Remote Server in Ubuntu