**Day 39**

**Exploitation Analyst**

**Control Remote Connections:**

**SSH Keys:**

**What are SSH keys?**

SSH keys are cryptographic keys used for secure authentication in place of passwords.

* Private key: Stays on your machine, must be kept secret.
* Public key: Stored on the server in ~/.ssh/authorized\_keys.
* During login, the server verifies the private key matches the public key → access granted.

**Why SSH keys are useful?**

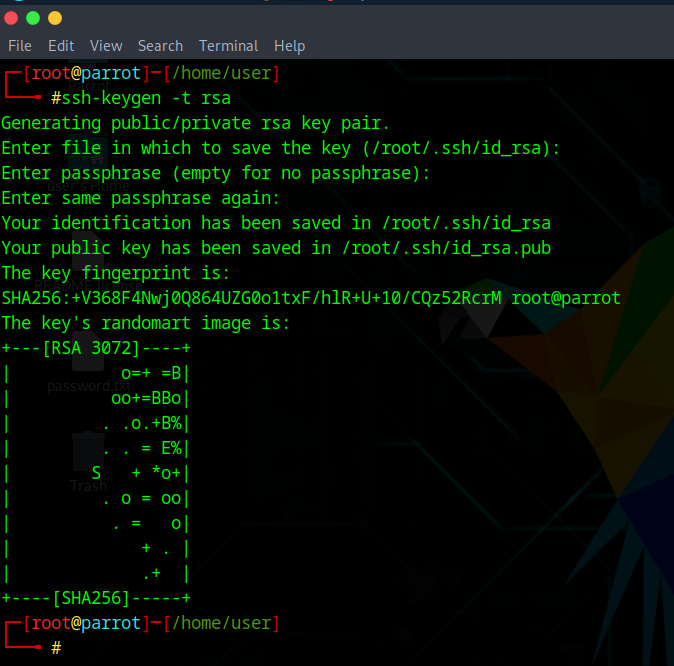
SSH keys are useful because they:

1. Increase security – harder to brute-force than passwords.
2. Enable passwordless login – faster and convenient.
3. Support automation – scripts and DevOps tools use keys.
4. Prevent credential theft – private key never leaves client.
5. Allow granular control – keys can be limited to specific users/commands.

**Setting the SSH Keys:**

Steps:

Generate SSH Key Pair on Client: using the command ssh-keygen -t rsa



Then copy the public key to the server: ssh-copy-id user@server\_ip