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?

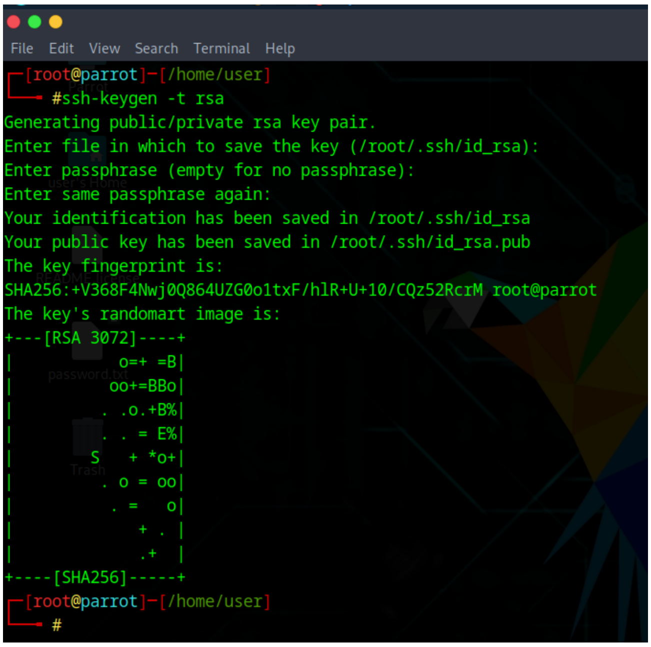
SSH keys are useful because they:

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



```
┌─[root@parrot]─[/home/user]
└──╼ #ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:+V368F4Nwj0Q864UZG0o1txF/hlR+U+10/CQz52RcrM root@parrot
The key's randomart image is:
+---[RSA 3072]----+
|           o=+ =B|
|          oo+=BBo|
|         . .o.+B%|
|         . . = E%|
|        S   + *o+|
|         . o = oo|
|          . =   o|
|             + . |
|             .+  |
+----[SHA256]-----+
┌─[root@parrot]─[/home/user]
└──╼ #
```

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