SSH (Secure Shell)

- The SSH protocol is used for:
  - Secure Remote Management of Servers, Routers, other Networking Devices
  - Network File Copy: rsync, scp, sftp, winscp
  - Tunneling, SSH Port Forwarding
- sshd is the SSH server (daemon) and ssh or putty is the client

Installation:

- **Ubuntu**: sudo apt update && sudo apt install openssh-server openssh-client
- **CentOS:** sudo dnf install openssh-server openssh-clients
- Checking its status: sudo systemctl status ssh

- Service Stop, Restart, Start: sudo systemctl [start|restart|stop] ssh
- Enable, Disable auto booting: sudo systemctl [enable|disable] ssh

Server config file: /etc/ssh/sshd_config

Client Config file: /etc/ssh/ssh_config

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:dml6c4xBSGXKOFMF9+Ge44aX7Kz6QUHbO8bI3igueN0.
Please contact your system administrator.
Add correct host key in /home/andrei/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /home/andrei/.ssh/known_hosts:3
  remove with:
  ssh-keygen -f "/home/andrei/.ssh/known_hosts" -R "192.168.0.108"
ECDSA host key for 192.168.0.108 has changed and you have requested strict checking.
Host key verification failed.
```