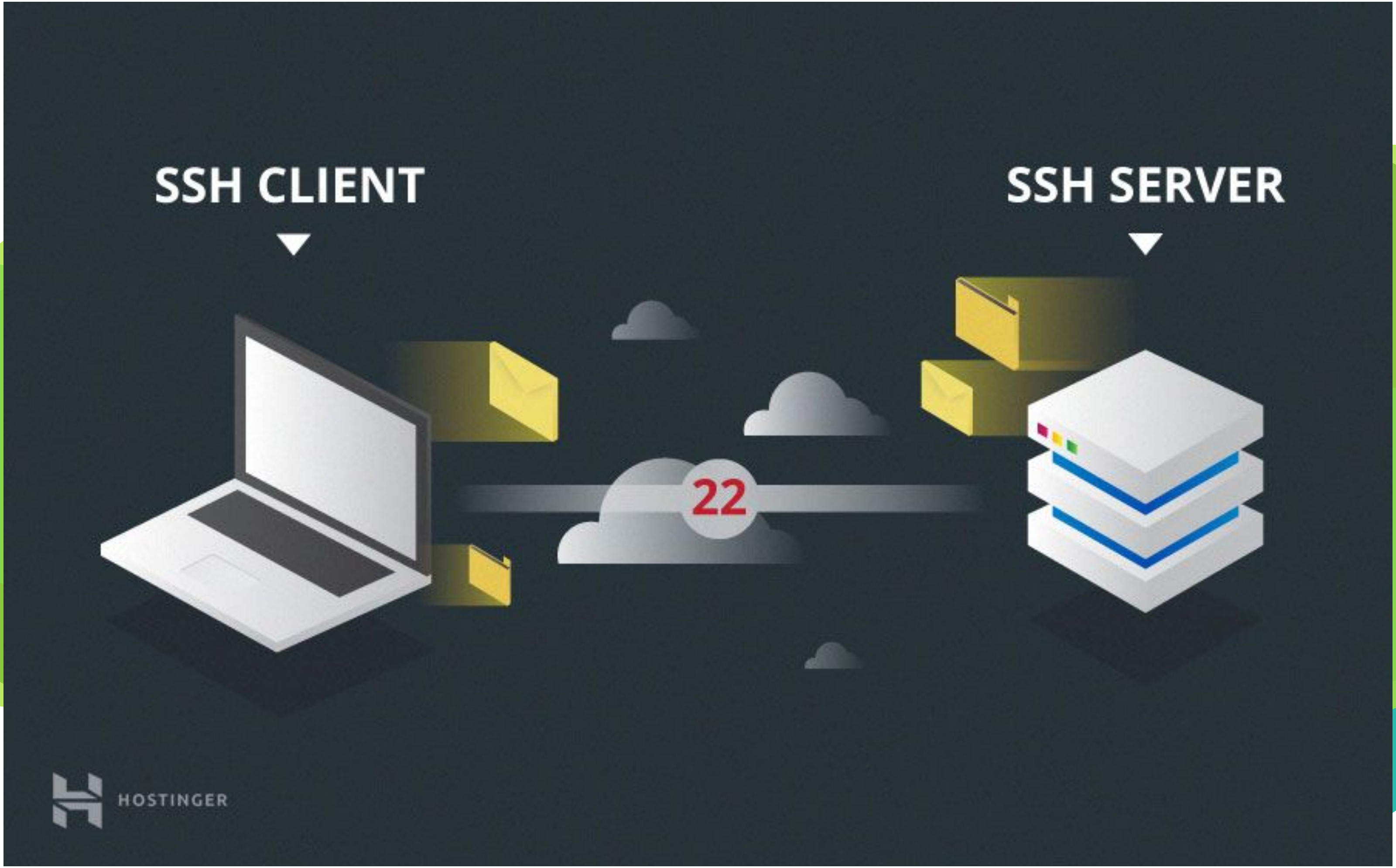
SSH

What is SSH?

SSH stands for **S**ecure **Sh**ell

It is a package that allows you to remotely create a terminal connection to another computer system.


SSH CLIENT
SSH SERVER
22
HOSTINGER

How does SSH work?

SSH provides a protocol for establishing an encrypted connection (hence the “secure”) between a server and client.

Uses keys and symmetric/asymmetric encryption to ensure only authenticated users are accessing the system.

After access is granted, a remote terminal (hence the “shell”) is opened to the server.

SSH on Linux

To use ssh, install the following package with apt.

- openssh-server
- openssh-client

- Clients only need openssh-client
- Servers need both

/etc/ssh/sshd_config

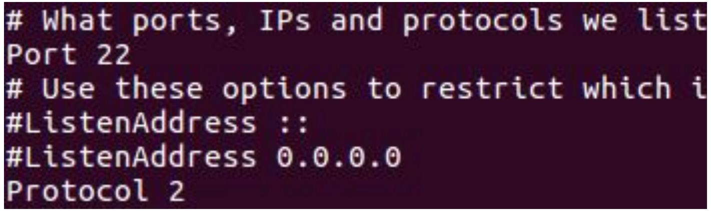
This file is our main configuration file. There is another file named ssh_config, but this is for client connections.

The sshd configuration stands for the **ssh d**aemon configuration (daemon is a background process), and thus is applied to servers, which is what we will be configuring.

SSH Configurations - Protocol

Good

- Protocol 2
- ALWAYS use protocol 2 because it is newer and more secure



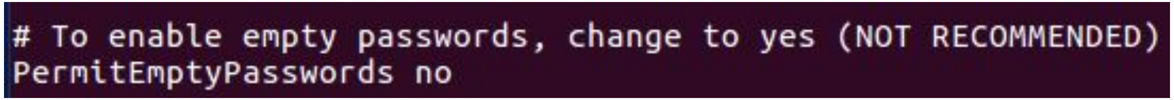
```
# What ports, IPs and protocols we list
Port 22
# Use these options to restrict which i
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
```

Bad:

- Protocol 1
- NEVER use protocol 1
- You may also see “Protocol 2, 1” in the config
  - Sets protocol 2 as priority and protocol 1 as backup
  - Make sure you remove the 1 because we do not want to use it in any case

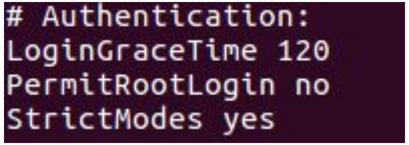
SSH Configurations - Passwords/Login

- PermitEmptyPasswords no
  - You should know why by now



```
# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no
```

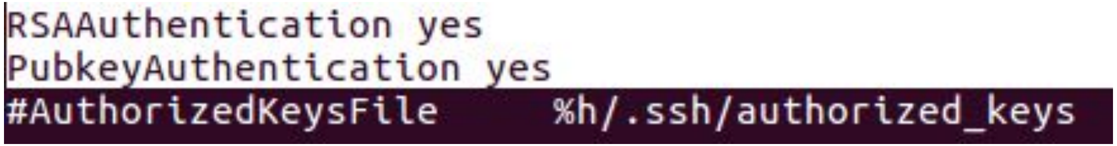
- PermitRootLogin no
  - Do not want users to login as root



```
# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes
```

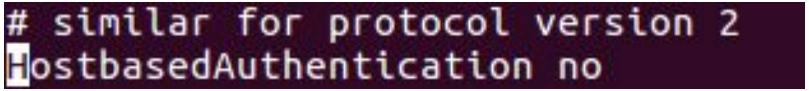
SSH Configurations - Authentication

- RSAAuthentication yes, PubkeyAuthentication yes
  - Both of these encryption methods are secure



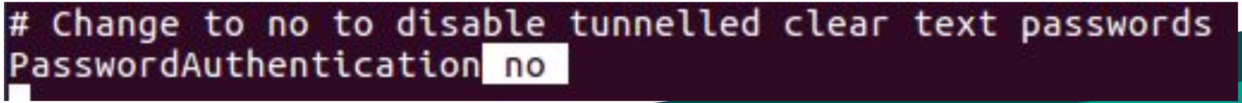
```
RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile     %h/.ssh/authorized_keys
```

- HostbasedAuthentication no



```
# similar for protocol version 2
HostbasedAuthentication no
```

- PasswordAuthentication no
  - This one is unintuitive, instructor should know why (see speaker notes if you don’t)



```
# Change to no to disable tunnelled clear text passwords
PasswordAuthentication no
```

SSH Configurations - X11

- X11Forwarding no
  - Disable transmission of GUI information
- PrintMOTD yes
  - Legal reasons, (Instructor: see speaker notes if you don’t know why)

SSH Configurations - Port Number

- Port [#]
  - The default value is 22
  - Changing it prevent hackers from knowing what port ssh is on
  - If you change it also update firewall rules

SSH Configurations - Authentication

- PubkeyAuthentication yes
  - Use public/private key pair to authenticate
  - More secure than password authentication
- HostbasedAuthentication no
  - Prevents authentication through trusted hosts
- IgnoreRhosts yes
  - Rhosts specifies which users can use what commands
  - The .rhosts file is a target for hackers, remove it from your system
- MaxAuthTries 4
  - limits number of authentication attempts
  - *this line needs to be manually added

SSH Configurations - Users

- AllowUsers [user1] [user2] [...]
    - Allows a user to access the ssh server
- DenyUsers [user1] [user2] [...]
    - Restricts a user from accessing the ssh server

Additional Information

To make sure all your configurations are applied, make sure to restart ssh (the sshd service):

- sudo service sshd restart

Although SSH involves key management, this is outside our scope. You can research on your own if you want to learn how SSH keys work, and how to set them up.