Let’s open the **/etc/ssh/sshd\_config** file and discuss its content:

Port 22 # defines listening port for ssh

AddressFamily any # accepts IPv4 et IPv6 addresses

ListenAddress 0.0.0.0 # allows ssh to listen on all network interfaces

ListenAddress :: # listens on IPv6 addresses too

Protocol 2 # defines version of ssh (version 1 is not used any more)

SyslogFacility AUTHPRIV # stores logging attempts in /var/log/secure (see rsyslog.conf file)

LoginGraceTime 2m # sets the time to connect

PermitRootLogin yes # allows direct login as root: outside lab, this option should be set to 'no'

StrictModes yes # allows connection only if the user's home directory is not world-writable

MaxAuthTries 6 # defines the number of authentication attempts allowed

MaxSessions 10 # defines the limit of simultaneous open connections

PubKeyAuthentication yes # enables public key authentication

AuthorizedKeysFile .ssh/authorized\_keys # defines the location of the authorized-keys file

HostbasedAuthentication no # forbids the use of /etc/hosts.equiv

IgnoreUserKnownHosts no # reads the .ssh/known\_hosts at each connection

IgnoreRhosts yes # doesn't read user's ~/.rhosts file

PasswordAuthentication yes # sets password-based authentication

PermitEmptyPasswords no # doesn't allow empty passwords (hopefully!)

ChallengeResponseAuthentication no # forbids use of one-time passwords

UsePAM yes # enables the Pluggable Authentication Module interface

AllowAgentForwarding yes # allows the ssh-agent to forward private keys

AllowTCPForwarding yes # allows TCP communications to be forwarded

GatewayPorts no # prevents remote hosts from connecting to ports forwarded for the client

X11Forwarding yes # enables X11 forwarding

X11DisplayOffset 10 # limits the number of GUI display open at the same time

X11UseLocalhost yes # defines how the GUI display is bound to the SSH server

PrintMotd yes # displays the message of the day

PrintLastLog yes # displays the date of the last login

TCPKeepAlive yes # allows the system to send TCP keepalive messages

UseLogin no # specifies whether login is used for interactive login session

UsePrivilegeSeparation yes # separates incoming network traffic processing from the rest

PermitUserEnvironment no # doesn't deal with environment options

Compression delayed # specifies that compression is delayed until user authentication

ClientAliveInterval 0 # doesn't send any message before client deconnection

ClientAliveCountMax 3 # defines the number of messages before client deconnection

- # if ClientAliveInterval is different from 0

UseDNS yes # checks remote hostnames against DNS

PidFile /var/run/sshd.pid # defines the file where the SSH process ID is stored

MaxStartups 10 # defines the number of terminals simultaneously allowed

PermitTunnel no # doesn't support device forwarding

ChrootDirectory none # disables the use of chroot

Subsystem sftp /usr/libexec/openssh/sftp-server # supports the use of SSH encryption for SFTP file transfers