nano /etc/ssh/sshd/sshd_config

https://www.youtube.com /watch?v=s8F_YWGHeDM

https://www.digitalocean.com /community/tutorials/how-to-harden-openssh-on-ubuntu-18-04

https://engineering.nordeus.com /managing-iptables-with-ansible-the-easy-way/

Iptables command:
https://www.hashbangcode.com /article/adding-iptables-rules-ansible

roles --> ssh --> templates --> sshd_config _centOS.j2

```
#   $ OpenBSD: sshd_config ,v 1.89 2013/02/06 00:20:42 dtucker Exp $

# This is the  sshd server system-wide configuration file.  See
# sshd_config (5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config  shipped with
# OpenSSH  is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Port {{ ssh_port   }}
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

# The default requires explicit activation of protocol 1
#Protocol 2

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
MaxAuthTries {{  max_auth_tries   }}
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile     .ssh/authorized_keys

#AuthorizedPrincipalsFile  none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the  ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via  ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and  ChallengeResponseAuthentication to 'no'.
UsePAM  yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
PrintMotd  no # pam  does that
#PrintLastLog  yes
#TCPKeepAlive yes
#UseLogin no
UsePrivilegeSeparation sandbox        # Default for new installations.
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS yes
#PidFile  /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum   none

# no default banner path
#Banner none

# override default of no subsystems
Subsystem     sftp     /usr/lib/ssh/sftp -server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#     X11Forwarding no
#     AllowTcpForwarding no
#     ForceCommand cvs server

AllowUsers {{allow_users}}
```

roles --> ssh --> tasks --> main.yml

```
- name: Harden ssh via  sshd_config file
  hosts:
  vars_files:
  - vars/main.yml
  template:
      src: sshd_config _centOS.j2
      dest /etc/ssh/sshd_config
      owner: root
      group: root
      mode: 0600
  become: true
  notify: restart_ sshd

- name: Restart sshd
  service:
      name: sshd
      state: restarted


- name: Harden ssh via  hosts.allow
  hosts:
  tasks:
  vars_files:
  - vars/main.yml
  template:
      src: hosts.allow.j2
      dest /etc/hosts.allow
      owner: root
      group: root
      mode: 0600
   become: true


- name: Harden ssh via  deny.deny
  hosts:
  tasks:
  vars_files:
  - vars/main.yml
  template:
      src: hosts.deny.j2
      dest /etc/hosts.deny
      owner: root
      group: root
      mode: 0600
   become: true


- name: Harden CentOS via   Iptables firewall
  hosts:
  tasks:
  vars_files:
   - vars/main.yml
```

vars --> main.yml

```
# ssh settings

ssh_port: 3345
max_auth_tries: 3
allow_users: admin@123.123.123.10 admin@10.88.88.* yurisk

# host.allow &  host.deny settings

allow_ssh_ip : sshd,sshdfwd-X11: 192.168.2. 217.40.111.121
deny_ssh_ip : sshd,sshdfwd-X11:ALL


# iptables firewall settings
```

playbook --> sshd_config.yml

```
import_roles:
    roles:
        ssh
```

roles --> ssh --> templates --> hosts.allow.j2

```
{{allow_ssh_IP }}
```

roles --> ssh --> templates --> hosts.deny.j2

```
{{deny_ssh_IP }}
```