Secure SSH connection on your Server

Securing the SSH connection on your server (change port, fail2ban...)

Cheat Sheet by Clément G, 05 November 2022

1.delsuser X sudo

X user and 1 sudo user per server

The user must not have sudo rights

$deluser X sudo

```
Removing user `senthil' from group `sudo' ...
Done.
```

2.Change SSH default port

Change SSH port 22 (default) to one other port

$nano /etc/ssh/sshd_config

Chose port between 1024 & 65535

```
# default value.

Port 24322
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

3.PermitRootlogin NO

Disable ssh login with root user

$nano /etc/ssh/sshd_config

Replace yes with no

```
# Authentication:

LoginGraceTime 1m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
MaxSessions 1
```

4.Install fail2ban

Install fail2ban

$apt upgrade

$apt install fail2ban

5. Change fail2ban ssh listen port

Change failban shh listen port

$ nano /etc/fail2ban/jail.conf

same port you chose in stape 2

```
#
# SSH servers
#

[sshd]

# To use more aggressive sshd
# normal (default), ddos, extr
# See "tests/files/logs/sshd"
#mode   = normal
port    = 24322
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

6. Configure bantime /maxretry

choose your own banning configuration

$ nano /etc/fail2ban/jail.conf

```
# "bantime" is the number of seconds that a host is banned.
bantime  =60m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 1m

# "maxretry" is the number of failures before a host get banned.
maxretry = 3
```

Dont't forger to save your new configuration : systemctl restart fail2ban & systemctl restart sshd

information: This is a basic, non-evolved cheat sheet with simple commands.