

# Step-by-step guide to Linux security

Clément Levallois

2017-04-03

# Table of Contents

Make sure you have the latest version of all packages: .....	1
Network Time Protocol .....	1
changing SSH port .....	1
enable SSH key auth .....	1
installing the undifficult firewall .....	2
denying all incoming traffic except for SSH port .....	2
install and config of Psad .....	2
disabling clear password auth .....	3
the end .....	3

last modified: 2017-04-04

## Make sure you have the latest version of all packages:

```
sudo apt-get update && sudo apt-get upgrade
```

## Network Time Protocol

```
aptitude install ntp
```

Then define your time zone (the one where your server is located):

```
dpkg-reconfigure tzdata
```

## changing SSH port

```
vi /etc/ssh/sshd_config
```

Text to change in the file: change port SSH 22 by a new port (**let's say 1234**), write the new port down somewhere

```
service sshd restart
```

## enable SSH key auth

- Generate a key with puttygen (SSH-2 RSA 1024).
- Parameters to change in `/etc/ssh/sshd_config`:

ChallengeResponseAuthentication no

X11Forwarding no

UsePAM no

LogLevel DEBUG3 (this should be added, the parameter is not listed by default)

- Save the file, then:

```
service sshd restart
```

- Add your public key to `/home/myUser/.ssh/authorized_keys`

Make sure that:

- you have put the keys in `/home/myUser/.ssh/authorized_keys` (not just in the root user folder)
- your key starts with "the "ssh-rsa" (the first "s" might be missing ...)
- the key doesn't break in several lines
- do `chmod 700 ~/.ssh` on the home folder
- use `tail -f /var/log/auth.log` for debugging

When SSH key login works, go back to `/etc/ssh/sshd_config` and do:

`PasswordAuthentication no`

then: `service sshd restart`

Things will not work the first time, useful tips: - <http://askubuntu.com/a/306832> - <http://stackoverflow.com/a/20923212/798502>

## installing the undifficult firewall

```
sudo apt-get update
```

```
apt-get install ufw
```

## denying all incoming traffic except for SSH port

```
ufw default deny incoming
```

```
sudo ufw allow 22/tcp
```

```
ufw enable
```

## install and config of Psad

First, making sure the firewall logs the traffic:

```
iptables -A INPUT -j LOG
iptables -A FORWARD -j LOG
```

```
apt-get install psad
```

Then modify some options in the config file, which is situated here:

```
vi /etc/psad/psad.conf
```

Here are some options I modified: [my psad config file](#)

Then we whitelist our own server:

```
vi /etc/psad/auto_d1
```

where I put just 2 values:

```
127.0.0.1 0; # localhost
```

```
xx.xx.xxx.xxx 0; # Server IP (replace xx.xx.xxx.xxx by your actual server IP)
```

## disabling clear password auth

```
vi /etc/ssh/sshd_config
```

Text to change in the file:

```
ChallengeResponseAuthentication no
```

```
PasswordAuthentication no
```

```
UsePAM no
```

```
service sshd restart
```

## the end

Author of this tutorial: [Clement Levallois](#)

All resources on linux security: <https://seinecle.github.io/linux-security-tutorials/>