Frank Anemaet

Linux Server Security

Best Practices

Linux Secure VPS

Best Practices

Frank Anemaet

This book is for sale at http://leanpub.com/linux-secure-vps

This version was published on 2020-12-22

Contents

Introduction

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Who is this book for?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

What is Linux?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Chapter 1: Updates and SSH

OpenSSH

Unless you are physically connected, you need to have an SSH server running. To access the server remotely.
By default on any cloud service, if you create a new server, SSH is running. This is often the case if you run the server in your room too.

You can connect to your server with the command below, where ip_address is the address of your server. The username is a user that exists on that server. On Windows you can use *putty* to connect to your ssh server.

```
$ ssh username@ip_address
```

You can use one of these commands to find your server ip:

```
$ ip a
$ ifconfig
```

You can check your server status with this command:

```
sudo service ssh status
```

This requires your root password.

If it's not running, you need to install the OpenSSH server. Because Linux only refers to the kernel, any Linux based operating system has a different software maintenance program.

Ubuntu

On Ubuntu/Debian/Linux Mint

```
$ sudo apt-get install openssh-server openssh-client
```

To enable/disable you can use these commands

```
$ sudo systemctl status ssh
$ sudo service ssh status
$ sudo systemctl enable ssh
$ sudo systemctl start ssh
$ sudo systemctl stop ssh
```

Make sure your **firewall** doesn't block your ssh server.

```
$ sudo ufw allow ssh
$ sudo ufw enable
$ sudo ufw status
```

If you want to change your ssh config, you can do it like this:

```
$ sudo nano /etc/ssh/sshd_config
$ /etc/init.d/sshd restart
```

Redhat

On RHEL/Centos/Fedora

```
# yum -y install openssh-server openssh-clients
```

To enable/disable it on Redhat Linux, use these commands:

```
$ dnf install openssh-server
$ yum install openssh-server
$ systemctl start sshd
$ systemctl status sshd
$ systemctl enable sshd
firewall-cmd --zone=public --permanent --add-service=ssh
```

To enable/disable it on Fedora Linux, use these commands:

```
$ rpm -qa | grep openssh-server
$ sudo dnf install -y openssh-server;
$ sudo systemctl status sshd
$ sudo ss -lt
$ sudo systemctl start sshd.service;
$ sudo systemctl stop sshd.service;
$ sudo systemctl disable sshd.service;
```

Update and upgrade

One of the first things to do after installation, is to update the system. You don't want to run old software, because there may be known vulnerabilities in it. You will need an internet connection when updating and upgrading.

On any Debian based system (Debian, Ubuntu) you can use the program **apt**

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

That will install the latest updates for your server. Press the *y* character when asked.

Automatic upgrades

You can enable automatic upgrades. This will do security updates even when you are sleeping or not around.

Ubuntu and Debian have a package for automatic upgrades named **unattended-upgrades**

```
sudo apt-get install unattended-upgrades
```

After install, you need to configure it:

```
sudo dpkg-reconfigure unattended-upgrades
```

Then you get a screen that allows you to automatically install and upgrade automatic updates. Press enter to enable.

Even though the software is upgraded automatically, you sometimes need to reboot the system. If that's required, it will write a file named *reboot-required*.

```
cd /var/run
cat reboot-required
```

If it is, then you see

```
*** System restart required ***
```

You can do manual rebooting. To check why you need to reboot, you'll see why you need to reboot

```
cat /var/run/reboot-required.pkgs
```

If you do not want to reboot manually, you can automate it.

```
sudo nano /etc/apt/apt.conf.d/50unattended-upgrades
```

Then scroll down and you'll have an option for automatic reboot. Set the option *Automatic-Reboot* to true. You can also configure the time to reboot. You may want to inform your customers about these reboots.

Summary

SSH

You need to connect to your server to configure it. If you do not have physical access, you need ssh access. To get ssh access, an ssh server needs to be enabled. The most commonly used one is openssh-server.

If you have your server in an online cloud service like Vultr or Digital Ocean, you most likely already have an ssh server running.

```
sudo service ssh status
```

Then install the openssh server.

For Debian/Ubuntu server:

```
sudo apt-get install openssh-server
```

Update the system

In time, vulnerabilities are always discovered in software. It seems simply impossible for programmers to write correct software. When vulnerabilities are known, an attacker may try to abuse them in online servers. That's why you want to update your software, those vulnerabilities get fixed.

Because Linux only refers to the kernel and not the operating system, every Linux-based operating system has a different update mechanism. On Debian/Linux the program to manage software is called **apt**.

On Debian/Ubuntu Linux you can run:

```
sudo apt update
sudo apt upgrade
```

Automatic Updates

Ubuntu Linux and Debian Linux support automatic updates.

To enable automatic updates, install the package unattended-upgrades.

```
sudo apt-get install unattended-upgrades
```

To configure

```
sudo dpkg-reconfigure unattended-upgrades
```

Then you get a menu where you can configure

Its still required to reboot manually. The status is stored in the file /var/run/reboot-required

If you want automatic rebooting, change the value in the file

```
sudo nano /etc/apt/apt.conf.d/50unattended-upgrades
```

Chapter 2: SSH Connectivity

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

SSH key pairs

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Secure sshd_config

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

What is 2FA?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Google 2FA with password

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Google 2FA with SSH Keys

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Chapter 3: Access

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Limit Root login

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

NTP client

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Chapter 4: Firewalls

What is a Firewall?

iptables

Example iptables config

UFW firewall

Block all traffic

Allow web traffic

Enable firewall

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

psad

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Chapter 5: Blocking bad traffic

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

fail2ban

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

psad

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Chapter 6: Monitoring

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Syslog

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

what is syslog?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

Syslog on Linux

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.

tcpdump

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/linux-secure-vps.