{EPITECH} LEARN DIFFERENT*

DEVOPS SEMINAR

DEBIAN SECURITY KEY PARTITION

*apprendre autrement

DEVOPS SEMINAR

Slug of the day: `nsapoold01`

Task 00 - Installation

Before anything else, if you do not already have them, you have to download prerequisites:

- ✓ VirtualBox
- ✓ An ISO of Debian 11 “Bullseye”

Task 01 - Debian

Create a virtual machine with 20 Go virtual hard drive and 1024 Mo of RAM.

Install Debian, without GUI (KDE, etc), with separate partitions.
to clarify, you can install debian using the graphical install.

Debian must be installed in English

Once installation is done. You should have following partitions:

- ✓ swap
- ✓ /
- ✓ /home
- ✓ /var

You are free to choose the `root` password and create your user account.

Please be careful, logically choose the partition sizes.

About the auto-grader

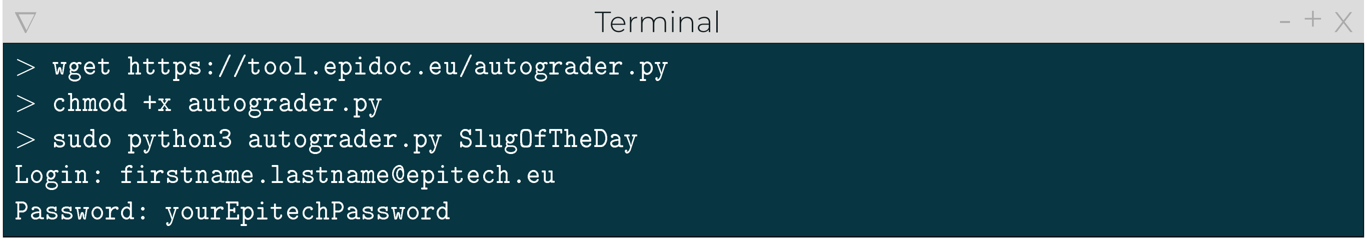
To be evaluated, you have to use our auto-grader script. It will communicate with an external server (so you must assure that your virtual machine has access to internet). Use the auto-grader to check your progression, **but beware**, the number of run each day is limited (the script will tell you how many checks you have left for the day before running).

Use the auto-grader at least once per day, otherwise your project will have no evaluations.

On your virtual machine, download the autograder.

Be sure to use the autograder with administrator rights.

You must authenticate with your school login (email address) and password.



```
> wget https://tool.epidoc.eu/autograder.py
> chmod +x autograder.py
> sudo python3 autograder.py SlugOfTheDay
Login: firstname.lastname@epitech.eu
Password: yourEpitechPassword
```

You result will be visible on my.epitech.eu.

Task 02 - User

Create a user named `marvin` with the following characteristics:

- ✓ Password: `toto42sh`
- ✓ Home directory: `/home/marvin`
- ✓ Description/Fullname: `Android Paranoid`
- ✓ UID: `4242`

The passwords used in this pool are *NOT* good passwords in the real world.

Task 03 - Group

Create a group named `H2G2` with GID `42400`.
Add `marvin` to this group then create a `zaphod` user with the following characteristics:

- ✓ Password: `ZappyBibicy`
- ✓ Home directory: `/home/zaphod`
- ✓ Description/Fullname: `Zaphod Beeblebrox`
- ✓ UID: `4200`
- ✓ GID: `42400`

Finally, create a `/home/HeartOfGold` folder that belongs to the `H2G2` group.

Task 04 - ssh

Install and configure the *ssh* service so that users can connect to it
Configure the service to only allow connection via ssh key (not via password).

- ✓ Change the default port to `4242`
- ✓ Disable ssh access for `root`.

Task 05 - ssh: you are not allowed

User `zaphod` can't be able to login via *ssh*.

> Nothing must change for other users.

Task 06 - Fail to ban

Install *fail2ban* to protect the *ssh* service.
Configure it for block IP address for 30 minutes, if more than 3 connections attempts for any user in 5 minutes.

The rules must be written in minutes

Iptables

Task 07 - Filter

Configure the firewall *iptables* with the following characteristics:

- ✓ rules have to be written in the `/etc/iptables/rules.v4`
- ✓ allow service *ssh* (input and output)
- ✓ allow HTTP protocol (output)
- ✓ allow HTTPS protocol (output)
- ✓ allow DNS protocol (output)

The other ports must be blocked and iptables configurations must not be wiped at reboot

For test, you must be able to update package (apt) after application of theses rules.

iptables-save, iptables persistent and system-config-firewall-tui is forbidden v 1.5

{EPITECH}

LEARN DIFFERENT*

*apprendre autrement