https://doc.ubuntu-fr.org/arborescence avec la norme FHS (File Hierarchy standard)

https://doc.ubuntu-fr.org/services
pw
https://doc.ubuntu-fr.org/ssh, UFW, …

To defense (Claire)
https://github.com/HEADLIGHTER/Born2BeRoot-42/blob/main/evalknwoledge.txt

Machine learning, VM, …
https://openclassrooms.com/fr/search?page=1&query=machine+

etapes

1. creer VM avec Virtual Box
2. installer OS/SE avec Debian (et non l<autre)
3. …

A SUIVRE (Tchin):
Zacharia:
https://openprojectrepo.com/project/ZakariaMahmoud-Born2beRoot_101-python-deep-learning
Guillaume : https://githubmate.com/repo/GuillaumeOz/Born2beroot
Monitoring.sh https://github.com/GuillaumeOz/Born2beroot/blob/master/monitoring.sh

+ verif chaque cmde / ex dmde dans le sujet

Baigal: https://discord.com/channels/@me/914819713434001418/933418429279522836

https://wiki.debian.org/fr/sudo

https://doc.ubuntu-fr.org/virtualbox

Machine virtuelle (VirtualBox) https://www.youtube.com/watch?v=vaA0a9L4Y3M2

https://www.youtube.com/watch?v=5kX6dmbeIX4 donne les touches pour accéder a la fenêtre Console

Yves Rougy

tutoriel SUDO :
1.
2. https://www.youtube.com/watch?v=pY3KN4J7pPw
3.
tutoriel SSH :
1.https://www.youtube.com/watch?v=QGixbJ9prEc
tuto Distributions Linux (1 noyau du Systeme d Exploitation : kernel.org) :
https://www.youtube.com/watch?v=jxStDDGDstQ

tuto : https://baigal.medium.com/born2beroot-e6e26dfb50ac
=> pour installer Debian, Get the Debian installer image :
https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/

https://githubmate.com/repo/GuillaumeOz/Born2beroot

https://fr.wikipedia.org/wiki/**Image_disque** :
Une **image disque** (ou **image ISO,** 1 des normes de codage, correspondant chacune à une extension particulière, .iso) est un (voire plusieurs) fichier(s) archive proposant la copie conforme d'un disque optique ou magnétique (tel qu'il serait écrit sur celui-ci).

Virtualisation

Avec l'arrivée des systèmes virtuels ou émulés, les images disques sont également devenues un moyen pratique de simuler un grand nombre de médias : elles permettent notamment de stocker, sur un seul disque dur physique, de nombreuses images disques virtuelles permettant d'accéder à des données qui pourraient ne pas être compatibles avec le système hôte. L'utilisation directe d'une image disque par le système de virtualisation ou d'émulation évite également de devoir refabriquer un support physique systématiquement, ce qui pourrait en plus ne plus être possible.

Par exemple, dans le cadre de l'émulation d'un ancien système, il est fort probable que ses supports physiques ne puissent même pas être adaptés sur un matériel moderne. La fabrication d'images permet ainsi de rendre ces données accessibles, et donc pérennes, et de pouvoir totalement émuler/virtualiser d'anciennes générations de machines.

Dans le cadre de la virtualisation, fabriquer une image disque du système d'exploitation et des disques d'installation des principaux logiciels dont on souhaite équiper la machine virtuelle permet de centraliser toutes les ressources nécessaires à la virtualisation sur un seul et unique disque dur physique contenant l'intégralité des éléments nécessaires au système virtuel.

https://www.commentcamarche.net/informatique/windows/757-creer-ou-ouvrir-un-**fichier-iso**-sur-pc/

https://fr.wikipedia.org/wiki/Virtualisation
=> disposer de disques différents pour chaque système

mainframe : https://fr.wikipedia.org/wiki/Ordinateur_central

https://fr.wizcase.com/blog/meilleurs-**serveurs-dns**-gratuits/ : Domain Server Name (Cf Arnaud)

Installation pour faire le Bonus WordPress :
https://reposhub.com/python/deep-learning/ZakariaMahmoud-Born2beRoot_101.html

Project overview

- How a virtual machine works.
- Their choice of operating system.
- The basic differences between CentOS and Debian.

CentOS vs Debian are two flavors of Linux operating systems. CentOS, as said above, is a Linux distribution. It is free and open-source. It is enterprise-class – industries can use meaning for server building; it is supported by a large community and is functionally supported by its upstream source, Red Hat Enterprise Linux. Debian is a Unix like computer operating system that is made up of open-source components. It is built and supported by a group of individuals who are under the Debian project. Debian uses Linux as its Kernel. Fedora, CentOS, Oracle Linux are all different distribution from Red Hat Linux and are variant of RedHat Linux. Ubuntu, Kali, etc., are variant of Debian. CentOS vs Debian both are used as internet servers or web servers like web, email, FTP, etc.

- The purpose of virtual machines.
- If the evaluated student chose Debian: the difference between
aptitude and apt,

apt (Advanced Package Tool), is a collection of tools used to install, update, remove, and otherwise manage software packages on Debian. and its derivative operating systems, including Ubuntu and Linux Mint. APT works through the use of repositories, or special directories that hold collections of software packages. You can check this file: # cat /etc/apt/sources.list

and what APPArmor (vs SELinux) is.

“These security systems provide tools to isolate applications from each other and in turn isolate an attacker from the rest of the system when an application is compromised.

AppArmor is a Mandatory Access Control framework. When enabled, AppArmor confines programs according to a set of rules that specify what files a given program can access. This proactive approach helps protect the system against both known and unknown vulnerabilities

During the defense, a script must display information all every 10 minutes. Its operation will be checked in detail later.

Simple SETUP

- Ensure that the machine does not have a graphical environment at launch.

A password will be requested before attempting to connect to this machine.
Finally, connect with a user with the help of the student being evaluated.
This user must not be root.
Pay attention to the password chosen, it must follow the rules imposed in the subject.

- Check that the UFW service is started with the help of the evaluator.

> sudo ufw status

- Check that the SSH service is started with the help of the evaluator.

> sudo service ssh status

- Check that the chosen operating system is Debian

> cat /etc/debian_version

USER

> cat /etc/login.defs => password Age (3 durees)
> cat /pam.d/common-password => password strengh (7 a 8 param dans ligne pam-pmquality)

```
pam_pwquality.so retry=3 minlen=10 ucredit=-1 dcredit=-1 maxrepeat=3
reject_username difok=7 enforce_for_root
```

The subject requests that a user vbauer is present on the virtual machine. Check that it has been added and that it belongs to the "sudo" and "user42" groups.

> getent group user42

> cat /etc/passwd ?

Make sure the rules imposed in the subject concerning the password policy have been put in place by following the following steps.

1. create a new user. Assign it a password of your choice, respecting the subject rules. Normally there should be 1 or 2 modified files.

> sudo adduser toto

> cat /etc/pam.d/common-password

2. Now that you have a new user, ask the student to create a group named "evaluating" in front of you and assign it to this user. Finally, check that this user belongs to the "evaluating" group.

> sudo addgroup evaluating

> sudo adduser toto evaluating

3. ask the student to explain the advantages of this password policy, as well as the advantages and disadvantages of its implementation.

HOSTNAME AND PARTITIONS

- Check that the hostname of the machine is correctly formatted as follows: login42

> hostnamectl avec autres infos comme version Debian ..

> cat /etc/hostname pour recup le hostname seulement

- Modify this hostname by replacing the login with yours, then restart the machine.

> sudo hostnamectl set-hostname toto42

> sudo vim /etc/hosts pour modifier le hostname + donne l IP (localhost) 127.0.0.1

> sudo reboot

If on restart, the hostname has not been updated, the evaluation stops here.

- You can now restore the machine to the original hostname

- Ask the student how to view the partitions for this virtual machine.

> lsblk

- Compare the output with the example given in the subject. Please note: if the student evaluated makes the bonuses, it will be necessary to refer to the bonus example. The student being evaluated should give you a brief explanation of how LVM works and what it is all about.

SUDO

- Check that the "sudo" program is properly installed on the virtual machine.

> dpkg -l | grep sudo

- The student should now show assigning your new user to the "sudo" group.

> sudo addgroup sudo

- The subject imposes strict rules for sudo. The student must first explain the value and operation of sudo using examples of their choice.

> cat /etc/sudoers => tries=3 + vbauer ALL=(ALL:ALL) ALL + chemins autorisés

In a second step, it must show you the implementation of the rules imposed by the subject.

- Verify that exists and has at least one file. Check the contents of the files in this folder, You should see a history of the commands used with sudo. Finally, try to run a command via sudo. See if the file (s) in the "/var/log/sudo/" folder have been updated. **> sudo cat /var/log/sudo/sudo.log**

UFW

- Check that the "UFW" program is properly installed on the virtual machine.

> dpkg -l | grep ufw

- Check that it is working properly.
- The student being evaluated should explain to you basically what UFW is and the value of using it.
- List the active rules in UFW. A rule must exist for port 4242.
- Add a new rule to open port 8080. Check that this one has been added by listing the active rules. > **sudo ufw allow 8080**
- Finally, delete this new rule with the help of the student being evaluated.

> sudo ufw status numbered **+ > sudo ufw delete *rule num***

SSH Secure SHell

- Check that the SSH service is properly installed on the virtual machine.

> dpkg -l | grep ssh

- Check that it is working properly.
- The student must be able to explain to you basically what SSH is and the value of using it.
- Verify that the SSH service only uses port 4242.

> sudo service ssh status@localhost -p 4243

- The student should help you use SSH in order to log in with the newly created user.

To do this, you can use a key or a simple password. It will depend on the student being evaluated. => fenêtre Terminal : **> ssh toto@127.0.0.1 -p 4243**
Of course, you have to make sure that you cannot use SSH with the "root" user as stated in the subject.

SCRIPT MONITORING

> sudo cat /usr/local/bin/monitoring.sh

The student should explain to you simply:

- How their script works by showing you the code.
- What "cron" is.
- How the student set up their script so that it runs every 10 minutes from when the server starts.

Once the correct functioning of the script has been verified, the student should ensure that this script runs every minute. You can run whatever you want to make sure the script runs with dynamic values correctly. Finally, the student should make the script stop running when the server has started up, but without modifying the script itself. To check this point, you will have to restart the server one last time. At startup, it will be necessary to check that the script still exists in the same place, that its rights have remained unchanged, and that it has not been modified.

> systemctl disable/enable **cron** + Reboot

BONUS

Check, with the help of the subject and the student, the bonus points authorized for this project:

- Setting up partitions is worth 2 points.
- Setting up WordPress, only with the services required by the subject, is worth 2 points.
- The free choice service is worth 1 point.

Verify and test the proper functioning and implementation of each extra service.
For the free choice service, the student being evaluated has to give you a simple explanation about how it works and why they think it is useful.
Please note that NGINX and Apache2 are prohibited.

/sgoinfre/goinfre/Perso/vbauer/Born2BeRoot :

1. **> sha1sum VM.vdi > signature.txt** a pushe sur la vosgphere
   8bd7f7971546688e643730f81d262c9320b40899 Born2BeRoot0.vdi
2. avant chaque correction : cloner sa VM puis travailler sur le clone avec la correcteur

CARACTERISTIQUES VM :

/etc = editing text config (norm FHS)	
/etc/debian_version	version de debian
/proc = info system (norm FHS)	
/proc/cpuinfo	processeurs , **top**
> lsblk	partitions
> cat /etc/fstab	(static file system information) si diff rep dev/mapper/ : **LVM** utilisé pour encrypter les volumes (8GO)

SECURITE 1. = CREATION USERS & GROUPES via SUDO :

> apt install sudo	login Root (**> su -**)
> dpkg -l | grep sudo	install sudo ok ?
/etc/sudoers.d/sudoconfig	droits sudo : tries=3 + vbauer ALL=(ALL:ALL) ALL
+chemins autorisés + TTY + log sudo ou **> sudo visudo** pour modif fichier **/etc/sudoers** en sécurité	
> journalctl	system's logging service
> sudo cat /var/log/sudo/sudo.log	liste de toutes les cmdes > sudo …
> sudo adduser toto	
> sudo addgroup user42	
> sudo adduser toto user42	**> getent group user42**
> sudo userdel toto	

SECURITE 2. = PASSWORD POLICY : 2 fichiers

> su username	changer de user
/etc/passwd	users et password
> cat /etc/login.defs	password Age (3 durees : 3/2/7)
> sudo chage *user* **-M 30 -m 2 -W 7**	pour appliquer aux users def avant pswd policy !
verif avec **> sudo chage** *user* **-l**	
> cat /etc/pam.d/common-password	password strengh (with paquet 'pam-pwquality')

SECURITE 3. = SECURE SHELL :

> apt install openssh-server	fin de session : > exit ou > logout
> sudo vim /etc/ssh/sshd_config + reboot	enable port 4242 (22 en std)+ disable Root Login
> sudo /etc/ssh/sshd_config | grep Port	port 4242 activé
> systemctl status ssh	état du service ssh (ou **sudo service ssh status)**
> ssh toto@127.0.0.1(ou localhost) **-p 4243**	connexion à la VM dep une autre machine

SECURITE 4. = FIREWALL :

> sudo ufw status verbose	état du service ufw + ports autorisés
> sudo ufw enable/disable	
> **sudo ufw allow**/deny **4242**	ajout/suppr autorisation port ssh (22)
> sudo ufw status numbered	+ > sudo ufw delete *rule num*

HOSTNAME :

> hostnamectl avec autres infos comme version Debian .. **> cat /etc/hostname** seulement
> sudo hostnamectl set-hostname vbauer43
> sudo vim /etc/hosts pour modifier le hostname apres avoir '> sudo chmod 777 hosts'
> sudo reboot vbauer@vbauer42 => vbauer@vbauer43

ETAT DU RESEAU affiché sur tous les terminaux connectés **:**

> sudo cat /usr/local/bin/monitoring.sh etat du réseau +
/usr = Unix System Ressources (norm FHS), appli. usuelles pour users et leurs fichiers
> sudo crontab -u root -e a job scheduler
avec ajout ligne: */10**** bash /…montoring.sh **| wall** (display sur tous les terminaux du reseau)
> systemctl disable/enable **cron + reboot** ou **> systemctl stop**/start **cron** dans session courante
/etc/init.d/cron stop (ou start)

> ss -tunip connexions UDP TCP (dynamiques)
> sudo /etc/network/interfaces passer d IP dynamiques à statiques pour suppr Port 68

cat /usr/local/bin/monitoring.sh

echo "#Architecture:" `uname -a` : archi d OS + kernel

echo "#CPU physical:" `cat /proc/cpuinfo | grep -c processor`: nb processeur physiques

echo "#vCPU:" `cat /proc/cpuinfo | grep processor | wc -l` : nb processeur virtuels

echo "#Memory Usage:" `free -m | grep Mem: | awk '{printf "%d/%dMB (%.2f%%)",$3,$2,$3*100/$2 }'
: mem. vive dispo en MO

echo "#Disk Usage:" `df -h | grep root | awk '{printf "%d/%dGb (%s)",$3,$2,$5}'`: disk free **h**uman readable

echo "#CPU load:" `top -bn 1 | grep load | awk '{printf "%.2f%%", $(NF-2)}'` : tx util processeur

echo "#Last boot:" `who -b | awk '{print $3 " " $4}'` : who is logged on, **b**oot

echo "#LVM use:" `if cat /etc/fstab | grep -q dev/mapper/; then echo "yes"; else echo "no"; fi`
static file system information

echo "#Consunexions TCP:" `netstat | grep tcp | wc -l` "ESTABLISHED" : connexions actives (tcp = exterieures)

echo "#User log:" `who | cut -d " " -f 1 | sort -u | wc -l`

echo "#Network:IP" `hostname -I` "("`ip a | grep link/ether | awk '{print $2}'`")" : adresses IP + IMAC (Media Access Control = adresse physique, est un identifiant physique stocké dans une carte réseau ou une interface réseau similai

echo "#Sudo:" `journalctl -q | grep sudo | grep TTY | wc -l` "cmd" : TTY = machine host