Born2BeRoot – Correction

Pierre Perol-Schneider

février 2022
(rév.6 du 28 fév.)

Abstract

This document the Born2beRoot project correction at 42 school.

1 General instructions

1.1 Preliminaries

If cheating is suspected, the evaluation stops here. Use the "Cheat" flag to report it. Take this decision calmly, wisely, and please, use this button with caution.

1.2 Preliminary tests

1.2.1 Defense can only happen if the student being evaluated or group is present. This way everybody learns by sharing knowledge with each other.

1.2.2 If no work has been submitted (or wrong files, wrong directory, or wrong filenames), the grade is 0, and the evaluation process ends.

1.2.3 For this project, you have to clone their Git repository on their situation.

1.3 General instructions

1.3.1 During the defense, as soon as you need help to verify a point, the student evaluated must help you.

1.3.2 Ensure that the `signature.txt` file is present at the root of the cloned repository.

Vous devez rendre uniquement un fichier `signature.txt` à la racine de votre dépôt `git`.

1.3.3 Check that the signature contained in `signature.txt` is identical to that of the `.vdi` file of the virtual machine to be evaluated. A simple `diff` should allow you to compare the 2 signatures. If necessary, ask the student being evaluated where their `.vdi` file is located.

```
$ cd /sgoinfre/goinfre/Perso/pperol/Born2BeRootMac
$ shasum Born2BeRootMac.vdi
8f390c7f738de5cf16cac82fb5af6790a60bc889 Born2BeRootMac.vdi
$ echo 8f390c7f738de5cf16cac82fb5af6790a60bc889 > correction.txt
$ diff correction.txt signature.txt
```

Remarque : SHA (*Secure Hash Algorithm*) est une famille de fonctions de hachage qui ont été conçues par la NSA. `shasum` signifie *SHA checksum*, soit la somme des SHA. `shasum` est un programme qui calcule et vérifie les hachages. Il est utilisé ici pour vérifier l'intégrité des fichiers de `Born2BeRoot`. Il est installé par défaut dans Debian.

1.3.4 As a precaution, you can duplicate the initial virtual machine in order to keep a copy.

Faire un *snapshot* du serveur à l'aide de VirtualBox (*a priori*, ceci doit être fait avant la correction).

1.3.5 Start the virtual machine to be evaluated.
If something doesn't work as expected or the 2 signatures differ, the evaluation stops here.

2 Mandatory part

The project consists of creating and configuring a virtual machine following strict rules. The student being evaluated will have to help you during the defense. Make sure that that all of the following points are observed. During the defense, a script must display information all every 10 minutes. Its operation will be checked in detail later. If the explanations are not clear, the evaluation stops here.

2.1 Project overview

The student being evaluated should explain to you simply:

2.1.1 How a virtual machine works.

Une machine virtuelle est un environnement virtuel qui fonctionne comme une machine physique, avec son propre processeur, sa mémoire, son interface réseau et son espace de stockage, mais qui est créé sur un système matériel physique (situé sur site ou hors site).
Elle est une illusion d'un appareil informatique créée par un logiciel d'émulation.
L'émulation consiste à substituer un élément de matériel informatique (ici un PC) par un logiciel.
Le logiciel d'émulation simule la présence de ressources matérielles et logicielles telles que la mémoire, le processeur, le disque dur, le système d'exploitation et les pilotes, permettant d'exécuter des programmes dans les mêmes conditions que celles de la machine simulée.

2.1.2 Their choice of operating system.

Debian est libre et est plus facile à installer. CentOS est propriétaire et n'est plus supporté.

2.1.3 The basic differences between CentOS and Debian.

Debian est un OS développé par le projet Debian et composé principalement de logiciels libres et open source portant la licence GNU General Public License. Il inclut également des logiciels non-GPL situés en dehors de ses référentiels officiels afin de se conformer à ses directives concernant la fourniture de logiciels libres.
CentOS a été conçu pour fonctionner correctement avec les distributions de Red Hat Linux (RHL)
CentOS a été conçu pour compléter les versions de Red Hat Enterprise Linux (RHEL) tout en restant libre pour les utilisateurs non professionnels.
Les versions étaient gardées pendant dix ans, ce qui signifiait une longue durée d'assistance et qui rendait ce système d'exploitation idéal pour une utilisation en ligne avec des applications Web.
Red Hat a mis fin au suivi de CentOS depuis le 31 dec. 2021.

2.1.4 The purpose of virtual machines.

Coût, gain de place, sauvegarde (*snapshots*) et sécurité (*honeypots*).

2.1.5 The difference between aptitude and apt, and what is APPArmor

Advanced Packaging Tool (`apt` et `apt-get`) est un système de gestion de paquets permettant :
— une recherche facile et efficace,
— une installation simple et une désinstallation propre de logiciels et utilitaires.
— une mise à jour des distributions et des paquets dès qu'ils sont disponible.

`Aptitude` est un gestionnaire de paquets de haut niveau basé sur l'infrastructure `apt`, c'est-à-dire qu'on peut installer, supprimer et mettre à jour toute les applications. Il présente des fonctionnalités équivalentes à `apt` et `apt-get` mais gère mieux les dépendances. `Aptitude` s'utilise d'une façon semblable à `apt` et `apt-get` ou avec une interface interactive.

`AppArmor` est un système de contrôle d'accès obligatoire (*Mandatory Access Control*) qui s'appuie sur l'interface *Linux Security Modules* fournie par le noyau Linux. Concrètement, le noyau interroge `AppArmor` avant chaque appel système (par ex. le lancement d'un programme) pour savoir si le processus est autorisé à effectuer l'opération concernée. Ce mécanisme permet à `AppArmor` de confiner des programmes à un ensemble restreint de ressources. Par exemple, il permet à l'administrateur système d'associer à chaque programme un profil de sécurité qui restreint ses accès au système d'exploitation.

2.2 Simple setup

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.
If something does not work as expected or is not clearly explained, the evaluation stops here.

2.2.1 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.

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

```
$ sudo service ufw status
```

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

```
$ sudo service ssh status
```

2.2.4 Check that the chosen operating system is Debian or CentOS with the help of the evaluator.

```
$ cat /etc/os-release
```
ou aussi :
```
$ uname -a
```

2.3 User

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.
The subject requests that a user with the login of the student being evaluated is present on the virtual machine. Check that it has been added and that it belongs to the `sudo` and `user42` groups.

```
$ getent group sudo user42
```

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

```
$ chage -l pperol
```

First, create a new user. Assign it a password of your choice, respecting the subject rules. The student being evaluated must now explain to you how they were able to set up the rules requested in the subject on their virtual machine.

> `$ sudo adduser toto (vs. $ sudo deluser --remove-home toto)`
> `$ sudo chage -l toto`
> Contrôle de l'ajout de `toto` : `$ getent group toto` ou `$ getent passwd toto`
> puis les deux fichiers modifiés :
> `$ cat /etc/login.defs | less`
> `$ cat /etc/pam.d/common-password`
> Voir aussi :
> `$ sudo chage -M 30 (-m ou -W)` suivi du `username`

Normally there should be one or two modified files. If there is any problem, the evaluation stops here.
Now that you have a new user, ask the student being evaluated 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
$ getent group evaluating
$ su
$# passwd toto
```

Finally, ask the student being evaluated to explain the advantages of this password policy, as well as the advantages and disadvantages of its implementation. Of course, answering that it is because the subject asks for it does not count.

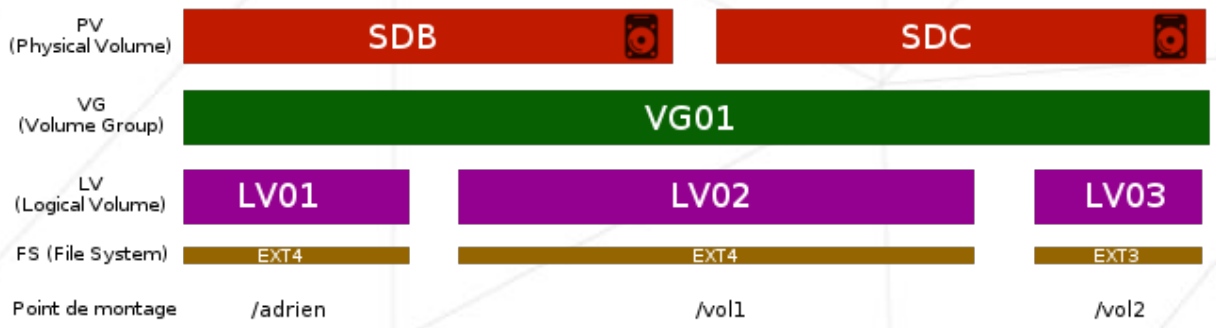
> Avantages : permet de proteger et d'attribuer des droits et de sécuriser l'accès
> Inconvénients : Post-it, contraignant, plus d'accès en cas de perte

If something does not work as expected or is not clearly explained, the evaluation stops here.

2.4 Hostname and partitions

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.
This part is an opportunity to discuss the scores! The student being evaluated should give you a brief explanation of how LVM works and what it is all about.
If something does not work as expected or is not clearly explained, the evaluation stops here.

> LVM est un Gestionnaire de volumes logiques (*Logical Volume Manager*) pour les systèmes d'exploitation Linux. Il fournit une vision de plus haut-niveau de l'espace disque sur un ordinateur que les partitions. Cela offre à l'administrateur plus de souplesse pour allouer du stockage aux applications ou aux utilisateurs. Les volumes de stockage créés sous LVM peuvent être redimensionnés et déplacés presque à volonté.



2.4.1 Check that the hostname of the machine is correctly formatted as follows: `login42` (login of the student being evaluated).

> Éventuellement :
> `$ hostnamectl`

2.4.2 Modify this hostname by replacing the login with yours, then restart the machine. If on restart, the hostname has not been updated, the evaluation stops here.

`$ sudo hostnamectl set-hostname toto42`
(ou `$ sudo vi /etc/hostname`)
`$ sudo vi /etc/hosts`
`$ sudo reboot`

You can now restore the machine to the original hostname.

2.4.3 Ask the student being evaluated how to view the partitions for this virtual machine.

`$ lsblk` (*list blocks*)

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.

2.5 Sudo

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.

2.5.1 Check that the `sudo` program is properly installed on the virtual machine.

`$ dpkg -l | grep sudo` (on liste les paquets Debian puis on trie sur le mot *sudo*)

2.5.2 The student being evaluated should now show assigning your new user to the `sudo` group.

`$ su`
`$# adduser toto sudo` (et éventuellement `usermod -aG sudo toto` pour lui donner aussi les privilèges.)
`$# reboot`

2.5.3 The subject imposes strict rules for `sudo`. The student being evaluated must first explain the value and operation of `sudo` using examples of his choice.

`$ sudo cat /etc/sudoers`

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

Defaults env_reset : réinitialise l'environnement du terminal pour supprimer toutes les variables utilisateur. Il s'agit d'une mesure de sécurité utilisée pour supprimer les variables environnementales potentiellement dangereuses de la session sudo.
Defaults secure_path : spécifie les emplacements du système de fichiers que le système d'exploitation recherchera pour les applications) qui seront utilisés pour les opérations `sudo`. Cela évite d'utiliser des chemins utilisateur qui peuvent être dangereux.
Defaults log_input,log_output,iolog_dir="/var/log/sudo" : archive toutes les commandes sudo vers `/var/log/sudo`
Defaults requiretty : limite l'utilisation de `sudo` au terminal ou à la console (interdit donc l'utilisation de `sudo` dans les scripts `cron` ou `cgi-bin`).

pperol42 ALL=(ALL:ALL) ALL
soit, sur le hostname pperol42 all sudo_users=(all usrers:all groups) all commands
Plus d'info sur la commande `sudo` : https://nos-oignons.net/wiki-admin/Services/Debian/sudo/

2.5.5 Verify that the `/var/log/sudo/` folder 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`.

2.5.6 Finally, try to run a command via `sudo`. See if the file (s) in the `/var/log/sudo/` folder have been updated.

If something does not work as expected or is not clearly explained, the evaluation stops here.

2.6 UFW

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.
If something does not work as expected or is not clearly explained, the evaluation stops here.

2.6.1 Check that the `ufw` program is properly installed on the virtual machine.

```
$ sudo ufw status
```

2.6.2 Check that it is working properly.

```
$ sudo ufw status verbose
```

2.6.3 The student being evaluated should explain to you basically what `ufw` is and the value of using it.

Uncomplicated Firewall : il surveille le trafic réseau entrant et sortant et autorise ou bloque les paquets de donnés en se basant sur un ensemble de règles de sécurité.

2.6.4 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 add by listing the active rules.

```
$ sudo ufw status
$ sudo ufw allow 8080
```

2.6.5 Finally, delete this new rule with the help of the student being evaluated.

```
$ sudo ufw deny 8080
$ sudo ufw status numbered
$ sudo ufw delete 8
$ sudo ufw delete 4
$ sudo ufw status
```

2.7 SSH

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.

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

```
$ sudo service ssh status
```
ou
```
$ sudo systemctl status ssh
```

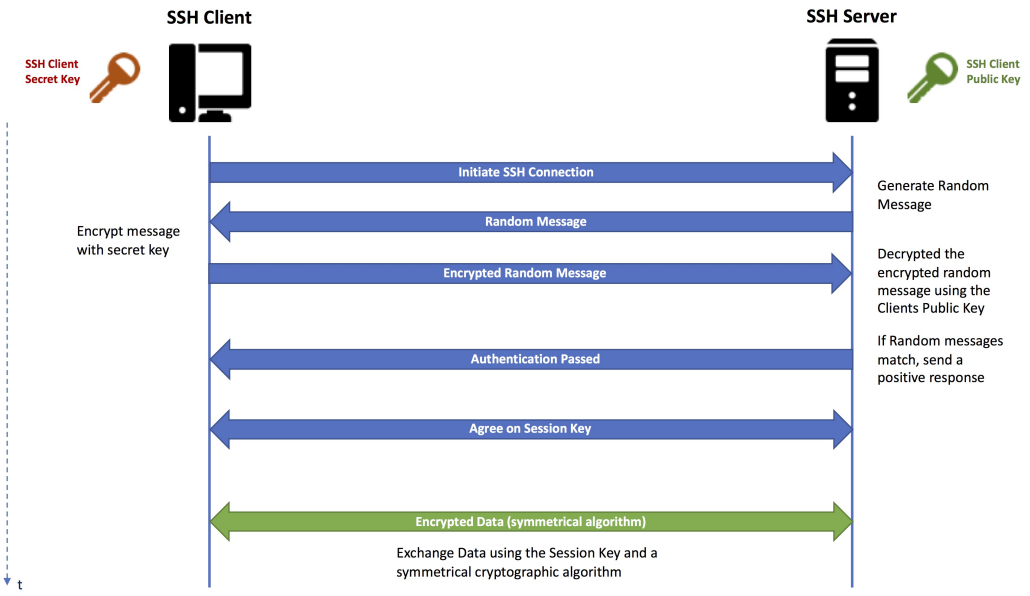
Check that it is working properly.

2.7.2 The student being evaluated must be able to explain to you basically what SSH is and the value of using it.

Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. TCP : *Transmission Control Protocol*

2.7.3 Verify that the SSH service only uses port4242.

`$ sudo systemctl status ssh` (ou `$ sudo systemctl status ssh`)
éventuellement, on peut aussi vérifier :
`$ sudo vi /etc/ssh/sshd_config`



2.7.4 The student being evaluated 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.

```
$ ssh toto@localhost -p 4242
```

Of course, you have to make sure that you cannot use SSH with the "root" user as stated in the subject.
If something does not work as expected or is not clearly explained, the evaluation stops here.

2.8 Script monitoring

Remember: Whenever you need help checking something, the student being evaluated should be able to help you.
The student being evaluated should explain to you simply:

2.8.1 How their script works by showing you the code.

`monitoring.sh` est un script qui s'affiche toutes les 10 minutes.
Il est écrit en bash.
Il ustilise les commandes `free, df, grep, awk, print, printf, sort, uniq, who, netstat` et `journalctl` pour trier et afficher le contenu des fichiers appelés.
`$ cat /sbin/monitoring.sh`

2.8.2 What "cron" is.

Cron est la troncation de `crontab`, lui-même la troncation de *chrono table*.
Il permet d'exécuter automatiquement des scripts, des commandes ou des logiciels à une date et une heure spécifiée à l'avance, ou selon une fréquence définie.
Cron est un `daemon`, il s'exécute donc en arrière-plan
Réglage : mm hh jj MMM JJJ `/path/monitoring.sh` (où le `path` est à préciser)

2.8.3 How the student being evaluated 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 being evaluated should ensure that this script runs every minute.

```
$ sudo crontab -u root -e
```
réglage : * * * * * `/sbin/monitoring.sh`

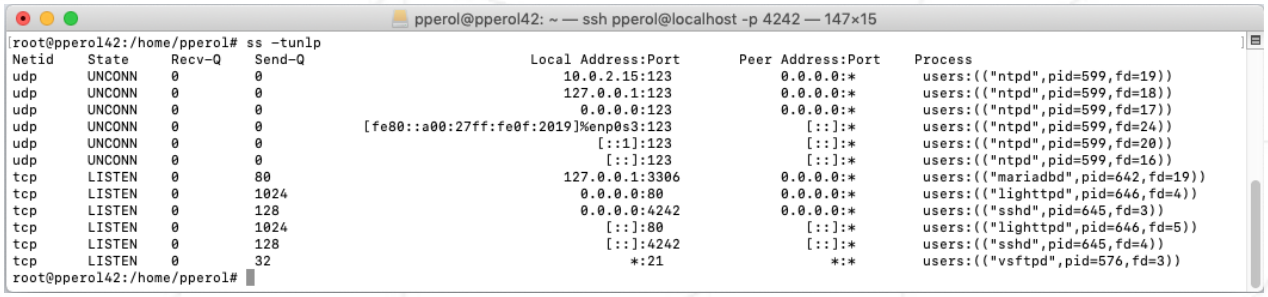
You can run whatever you want to make sure the script runs with dynamic values correctly.
Finally, the student being evaluated should make the script stop running when the server has started up, but without modifying the script itself. To check this point, you will have to restart the server one last 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.

Méthode #1 (à éviter) :
`$ su`
`$# systemctl disable cron`
`($# systemctl enable cron)`
Cette méthode stoppe (ou redémarre) **tous** les scripts.

Méthode #2 (commenter la ligne cron) :
`$ sudo crontab -u root -e`
réglage : `#* * * * * /sbin/monitoring.sh`
Cette méthode est plus sécurisé car elle évite de supprimer le déclenchement d'autres scripts éventuels.

If something does not work as expected or is not clearly explained, the evaluation stops here.

Le correcteur regardera probablement si une addresse IP fixe est bien présente.
Avec les bonus, la commande :
`$ ss -tunlp`
devra afficher :



(Pour une sortie sans bonus, se rapporter à la page 9 du sujet.)
Le port 68 (eg. `0.0.0.0:68`) **ne doit pas apparaître** dans la sortie.

3 Bonus

Evaluate the bonus part if, and only if, the mandatory part has been entirely and perfectly done, and the error management handles unexpected or bad usage. In case all the mandatory points were not passed during the defense, bonus points must be totally ignored.
Check, with the help of the subject and the student being evaluated, the bonus points authorized for this project.
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.

3.0.1 Setting up partitions is worth 2 points.

`$ lsblk`

3.0.2 Setting up Wordpress, only with the services required by the subject, is worth 2 points.

Dans un navigateur, ouvrir : `127.0.0.1` ou `localhost`
puis `$ sudo service --status-all`
puis éventuellement :
`$ mariadb -u pperol -p`
`MariaDB [(none)] SHOW DATABASES;`

```
> ...
> exit
```

MariaDB : base de données.
lighttpd : (ou *lighty*) est un serveur web sécurisé, rapide et flexible (comme Apache).
PHP : langage de programmation libre, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP.

3.0.3 The free choice service is worth 1 point.

Pour la sécurité du serveur :
fail2ban est une application qui analyse les logs de divers services (SSH, Apache, FTP...) en cherchant des correspondances entre des motifs définis dans ses filtres et les entrées des logs. Lorsqu'une correspondance est trouvée une ou plusieurs actions sont exécutées. Typiquement, fail2ban cherche des tentatives répétées de connexions infructueuses dans les fichiers journaux et procède à un bannissement en ajoutant une règle au pare-feu iptables ou nftables pour bannir l'adresse IP de la source.

Pour la sécurité du serveur et la synchronisation des horloges :
ntpdate : Serveur de temps qui lit l'heure réelle à partir d'une horloge de référence et distribue ces informations à ses clients.

Pour le transfert de fichiers sans passer pas SSH :
vsftpd : VsFTPd est un serveur FTP conçu avec la problématique d'une sécurité maximale. Contrairement aux autres serveurs FTP (ProFTPd, PureFTPd, etc.), aucune faille majeure de sécurité n'a jamais été décelée dans VsFTPd.