



Born2beRoot

Summary: This document is a System Administration related exercise.

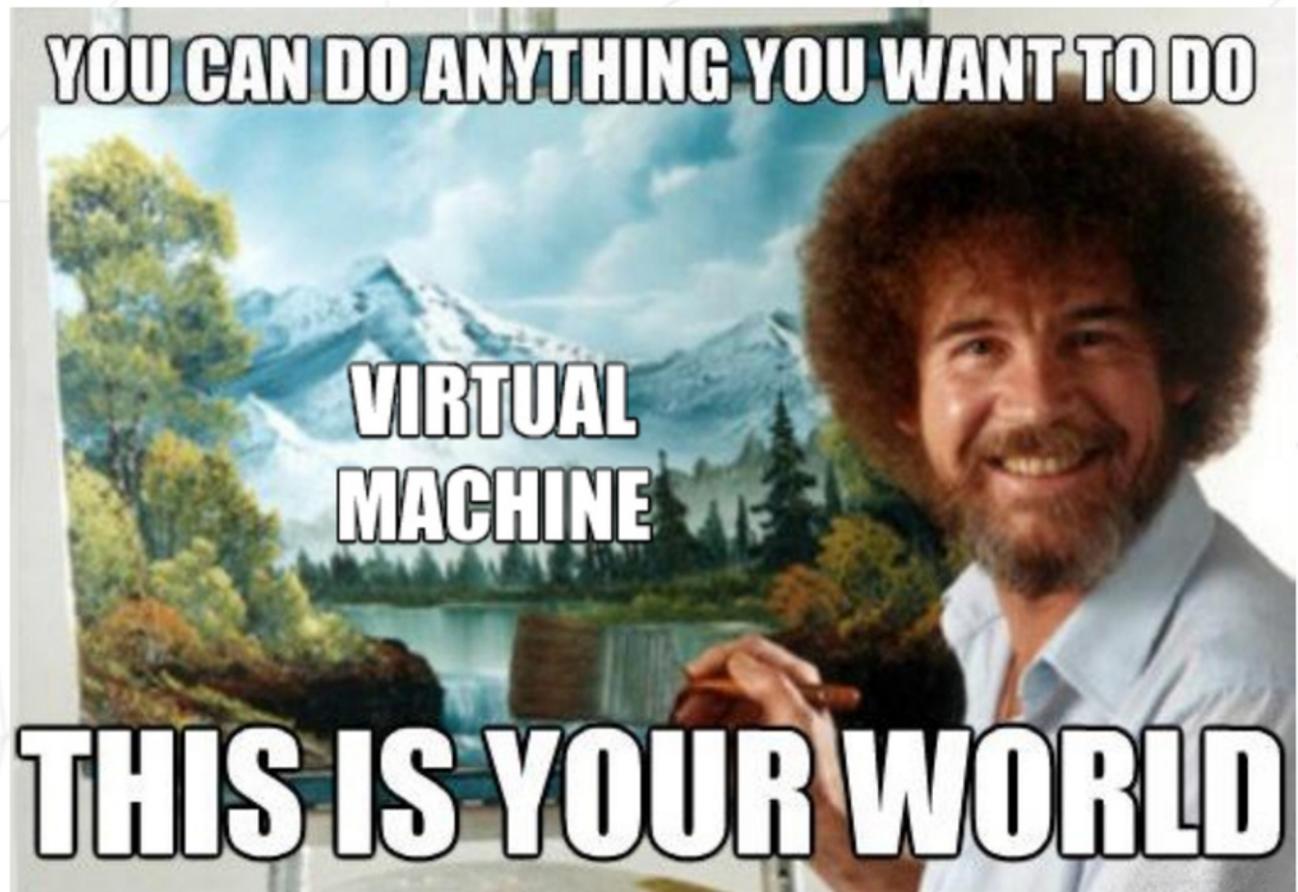
Version: 3.2

Contents

I	Preamble	2
II	Introduction	3
III	General guidelines	4
IV	Mandatory part	5
V	Bonus part	10
VI	Submission and peer-evaluation	12

Chapter I

Preamble



Chapter II

Introduction

This project aims to introduce you to the wonderful world of virtualization.

You will create your first machine in **VirtualBox** (or UTM if you can't use **VirtualBox**) under specific instructions. Then, at the end of this project, you will be able to set up your own operating system while implementing strict rules.

Chapter III

General guidelines

- The use of VirtualBox (or UTM if you can't use VirtualBox) is mandatory.
- You only have to turn in a `signature.txt` file at the root of your repository. You must paste in it the signature of your machine's virtual disk. Go to Submission and peer-evaluation for more information.

リポジトリに`signature.txt`ファイルを置くだけ。
そこに自身のマシンの仮想ディスクの署名を貼り付ける必要がある。
詳細については、Submission and peer-evaluationを確認。

サーバーをセットアップするだけなので、必要最小限のサービスをインストールする。
このため、グラフィカル・インターフェースは役に立たない。
したがって、X.orgやその他の同等のグラフィック・サーバーをインストールすることは禁じられている。さもなければ、あなたの成績は0点となります。



Chapter IV

Mandatory part

このプロジェクトでは、特定のルールに従って最初のサーバーをセットアップする。

This project consists of having you set up your first server by following specific rules.



Since it is a matter of setting up a server, you will install the minimum of services. For this reason, a graphical interface is of no use here. It is therefore forbidden to install X.org or any other equivalent graphics server. Otherwise, your grade will be 0.

You must choose as an operating system either the latest stable version of Debian (no testing/unstable), or the latest stable version of Rocky. Debian is highly recommended if you are new to system administration.

オペレーティングシステムとして、Debianの最新安定版(テスト版/不安定版なし)か、Rockyの最新安定版を選択する必要がある。Debianを強くお勧めする。



Setting up Rocky is quite complex. Therefore, you don't have to set up KDump. However, SELinux must be running at startup and its configuration has to be adapted for the project's needs. AppArmor for Debian must be running at startup too.

Debian用のAppArmorをスタートアップで起動しておく必要がある。

You must create at least 2 encrypted partitions using LVM. Below is an example of the expected partitioning:

```
wil@wil:~$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda        8:0    0   8G  0 disk 
└─sda1     8:1    0 487M 0 part /boot
└─sda2     8:2    0   1K  0 part 
└─sda5     8:5    0 7.5G 0 part 
  └─sda5_crypt 254:0  0 7.5G 0 crypt
    ├─wil--vg-root 254:1  0 2.8G 0 lvm  /
    ├─wil--vg-swap_1 254:2  0 976M 0 lvm [SWAP]
    └─wil--vg-home 254:3  0 3.8G 0 lvm /home
sr0       11:0   1 1024M 0 rom
wil@wil:~$ _
```

LVMを使用して少なくとも2つの暗号化パーティションを作成する必要がある。
上記は予想されるパーティション分割の例です：



During the defense, you will be asked a few questions about the operating system you chose. For instance, you should know the differences between aptitude and apt, or what SELinux or AppArmor is. In short, understand what you use!

A SSH service will be running on the mandatory port 4242 in your virtual machine. For security reasons, it must not be possible to connect using SSH as root.

SSHサービスは、仮想マシンの必須ポート4242で実行されます。



セキュリティ上の理由から、rootとしてSSHを使用して接続することはできません。

The use of SSH will be tested during the defense by setting up a new account. You must therefore understand how it works.

SSHの使用は、新しいアカウントを設定することで防衛中にテストされる。

そのため、どのように機能するかを理解しておく必要がある。

You have to configure your operating system with the UFW (or firewalld for Rocky) firewall and thus leave only port 4242 open in your virtual machine.

オペレーティング・システムにUFW (Rockyではfirewalld) ファイアウォールを設定し、仮想マシンのポート4242だけを開放しておく必要がある。



Your firewall must be active when you launch your virtual machine.

For Rocky, you have to use firewalld instead of UFW.

仮想マシンを起動する際には、ファイアウォールがアクティブになっている必要がある。

- The hostname of your virtual machine must be your login ending with 42 (e.g., wil42). You will have to modify this hostname during your evaluation.
仮想マシンのホスト名は、42で終わるログイン名（例：wil42）。評価中にこのホスト名を変更。
- You have to implement a strong password policy. **強力なパスワード・ポリシーを導入する。**
- You have to install and configure sudo following strict rules.
厳密なルールに従ってsudoをインストール・設定。
- In addition to the root user, a user with your login as username has to be present.
- This user has to belong to the user42 and sudo groups.
**rootユーザーに加えて、あなたのログイン名をユーザー名とするユーザーが存在しなければならない
このユーザーはuser42とsudoグループに属していなければならない。**



During the defense, you will have to create a new user and assign it to a group. **防衛戦では、新しいユーザーを作成し、グループに割り当てる必要がある。**

強力なパスワード・ポリシーを設定するには、以下の要件を満たす必要がある：

To set up a strong password policy, you have to comply with the following requirements:

- Your password has to expire every 30 days. **パスワードの有効期限は30日です。**
- The minimum number of days allowed before the modification of a password will be set to 2. **パスワードが変更されるまでの最短日数は2日に設定される。**
- The user has to receive a warning message 7 days before their password expires. **ユーザーは、パスワードの有効期限が切れる7日前に警告メッセージを受け取らなければならない。**
- Your password must be at least 10 characters long. It must contain an uppercase letter, a lowercase letter, and a number. Also, it must not contain more than 3 consecutive identical characters.
**パスワードは10文字以上でなければなりません。大文字、小文字、数字を含む必要があります。
また連続した同じ文字が含まれてはなりません。**

- The password must not include the name of the user. **パスワードにユーザー名を含んではならない。**
- **root/パスワードには適用されないルール：パスワードは、以前のパスワードの一部ではない、最低7文字。**
- The following rule does not apply to the root password: The password must have at least 7 characters that are not part of the former password.
一個上のルール以外はルート・パスワードはこのポリシーに従わなければならない。
- Of course, your root password has to comply with this policy.

設定ファイルをセットアップした後、rootアカウントを含め、仮想マシンに存在するすべてのアカウントのパスワードを変更する必要がある。



After setting up your configuration files, you will have to change all the passwords of the accounts present on the virtual machine, including the root account.

sudoグループに強力なコンフィギュレーションを設定するには、以下の要件に従わなければならない：

To set up a strong configuration for your sudo group, you have to comply with the following requirements:

sudoを使った認証は、パスワードが間違っていた場合、3回の試行に制限しなければならない。

- Authentication using sudo has to be limited to 3 attempts in the event of an incorrect password.

sudo使用時にパスワード間違いによるエラーが発生した場合、任意のカスタムメッセージを表示しなければならない。

- A custom message of your choice has to be displayed if an error due to a wrong password occurs when using sudo.

sudoを使った各アクションは、入力と出力の両方をアーカイブする。ログファイルは/var/log/sudo/folderに保存。

- Each action using sudo has to be archived, both inputs and outputs. The log file has to be saved in the /var/log/sudo/ folder.

セキュリティ上の理由から、TTYモードを有効にする必要があります。

- The TTY mode has to be enabled for security reasons.

セキュリティ上の理由からも、sudoが使用できるパスを制限する必要がある。例：

- For security reasons too, the paths that can be used by sudo must be restricted. Example:

/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

最後に、monitoring.shというシンプルなスクリプトを作成する必要がある。これはbash開発しなければならない。

Finally, you have to create a simple script called monitoring.sh. It must be developed in bash.

サーバー起動時に、スクリプトは10分ごとにいくつかの情報(以下のリスト)を全端末に表示する(wallを見て)。

バナーは任意。エラーは表示しない。

At server startup, the script will display some information (listed below) on all terminals every 10 minutes (take a look at wall). The banner is optional. No error must be visible.

スクリプトは常に以下の情報を表示できなければならない：

Your script must always be able to display the following information:

オペレーティングシステムのアーキテクチャとカーネルバージョン。

- The architecture of your operating system and its kernel version.

物理プロセッサーの数

- The number of physical processors.

仮想プロセッサーの数

- The number of virtual processors.

サーバーで現在使用可能なRAMとその使用率(パーセンテージ)。

- The current available RAM on your server and its utilization rate as a percentage.

サーバーで現在使用可能なストレージとその使用率(パーセンテージ)。

- The current available storage on your server and its utilization rate as a percentage.

プロセッサーの現在の使用率を(パーセント)

- The current utilization rate of your processors as a percentage.

最後に再起動した日時

- The date and time of the last reboot.

LVMがアクティブかどうか

- Whether LVM is active or not.

アクティブな接続数

- The number of active connections.

サーバーを使用しているユーザー数

- The number of users using the server.

サーバーのIPv4アドレスとMAC(Media Access Control)アドレス

- The IPv4 address of your server and its MAC (Media Access Control) address.

sudoプログラムで実行されたコマンドの数

- The number of commands executed with the sudo program.

ディフェンスでは、このスクリプトがどのように機能するかを説明するよう求められる。

また、スクリプトを修正せずに中断させる。cronを見て。



During the defense, you will be asked to explain how this script works. You will also have to interrupt it without modifying it.

Take a look at cron.

以下はスクリプトがどのように動作するかの例：

This is an example of how the script is expected to work:

```
Broadcast message from root@wil (tty1) (Sun Apr 25 15:45:00 2021):  
#Architecture: Linux wil 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux  
#CPU physical : 1  
#vCPU : 1  
#Memory Usage: 74/987MB (7.50%)  
#Disk Usage: 1009/2Gb (49%)  
#CPU load: 6.7%  
#Last boot: 2021-04-25 14:45  
#LVM use: yes  
#Connections TCP : 1 ESTABLISHED  
#User log: 1  
#Network: IP 10.0.2.15 (08:00:27:51:9b:a5)  
#Sudo : 42 cmd
```

以下は、課題の条件のいくつかをチェックするために使用できる2つのコマンドである：

Below are two commands you can use to check some of the subject's requirements:

For Rocky:

```
[root@wil will]# head -n 2 /etc/os-release
NAME="Rocky Linux"
VERSION="8.7 (Green Obsidian)"
[root@wil will]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33
[root@wil will]# ss -tunlp
Netid State  Recv-Q Send-Q Local Address:Port  Peer Address:Port Process
tcp   LISTEN  0      128      0.0.0.0:4242      0.0.0.0:*      users:(("sshd",pid=28429,fd=6))
tcp   LISTEN  0      128      [::]:4242        [::]:*        users:(("sshd",pid=28429,fd=4))
[root@wil will]# firewall-cmd --list-service
ssh
[root@wil will]# firewall-cmd --list-port
4242/tcp
[root@wil will]# firewall-cmd --state
running
[root@wil will]# _
```

For Debian:

```
root@wil:~# head -n 2 /etc/os-release
PRETTY_NAME="Debian GNU/Linux 10 (buster)"
NAME="Debian GNU/Linux"
root@wil:/home/wil# /usr/sbin/aa-status
apparmor module is loaded.
root@wil:/home/wil# ss -tunlp
Netid State  Recv-Q Send-Q Local Address:Port  Peer Address:Port
tcp   LISTEN  0      128      0.0.0.0:4242      0.0.0.0:*      users:(("sshd",pid=523,fd=3))
tcp   LISTEN  0      128      [::]:4242        [::]:*        users:(("sshd",pid=523,fd=4))
root@wil:/home/wil# /usr/sbin/ufw status
Status: active

To                         Action    From
--                         -----   ---
4242                       ALLOW    Anywhere
4242 (v6)                   ALLOW    Anywhere (v6)
```

Chapter V

Bonus part

Bonus list:

- Set up partitions correctly so you get a structure similar to the one below:

```
# lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda                  8:0    0 30.8G  0 disk
|__sda1               8:1    0  500M  0 part  /boot
|__sda2               8:2    0   1K  0 part
|__sda5               8:5    0 30.3G  0 part
|   __sda5_crypt      254:0   0 30.3G  0 crypt
|   |__LVMGroup-root  254:1   0   10G  0 lvm   /
|   |__LVMGroup-swap  254:2   0   2.3G  0 lvm   [SWAP]
|   |__LVMGroup-home  254:3   0     5G  0 lvm   /home
|   |__LVMGroup-var   254:4   0     3G  0 lvm   /var
|   |__LVMGroup-srv   254:5   0     3G  0 lvm   /srv
|   |__LVMGroup-tmp   254:6   0     3G  0 lvm   /tmp
|   |__LVMGroup-var--log 254:7   0     4G  0 lvm   /var/log
sr0                 11:0   1 1024M  0 rom
```

- Set up a functional WordPress website with the following services: lighttpd, MariADB, and PHP.
- Set up a service of your choice that you think is useful (NGINX / Apache2 excluded!). During the defense, you will have to justify your choice.



To complete the bonus part, you have the possibility to set up extra services. In this case, you may open more ports to suit your needs. Of course, the UFW/Firewalld rules has to be adapted accordingly.



The bonus part will only be assessed if the mandatory part is PERFECT. Perfect means the mandatory part has been integrally done and works without malfunctioning. If you have not passed ALL the mandatory requirements, your bonus part will not be evaluated at all.

Chapter VI

Submission and peer-evaluation

Git リポジトリにsignature.txt ファイルを置くだけ。そこに、あなたのマシンの仮想ディスクの署名を貼り付ける。この署名を得るには、まずデフォルトのインストール・フォルダを開く必要がある。(自身のVMが保存されているフォルダ) :

You only have to turn in a `signature.txt` file at the root of your Git repository. You must paste in it the signature of your machine's virtual disk. To get this signature, you first have to open the default installation folder (it is the folder where your VMs are saved):

- Windows: `%HOMEDRIVE%
%HOMEPATH%\VirtualBox VMs\`
- Linux: `~/VirtualBox VMs/`
- MacM1: `~/Library/Containers/com.utmapp.UTM/Data/Documents/`
- MacOS: `~/VirtualBox VMs/`

次に、仮想マシンの「.vdi」ファイル (UTM ユーザーの場合は「.qcow2」) から署名を sha1 形式で取得する。
以下は、`rocky_serv.vdi`ファイルに対する4つのコマンド例である：

Then, retrieve the signature from the ".vdi" file (or ".qcow2 for UTM'users) of your virtual machine in sha1 format. Below are 4 command examples for a `rocky_serv.vdi` file:

- Windows: `certUtil -hashfile rocky_serv.vdi sha1`
- Linux: `sha1sum rocky_serv.vdi`
- For Mac M1: `shasum rocky.utm/Images/disk-0.qcow2`
- MacOS: `shasum rocky_serv.vdi`

This is an example of what kind of output you will get:

- `6e657c4619944be17df3c31faa030c25e43e40af`

仮想マシンの署名は、最初の評価後に変更される可能性があることに注意。

この問題を解決するには仮想マシンを複製するか、状態を保存する。

Please note that your virtual machine's signature may be altered after your first evaluation. To solve this problem, you can duplicate your virtual machine or use save state.



Gitリポジトリに仮想マシンを入れることは禁じられている。防御の間、signature.txtファイルの署名はあなたの仮想マシンのものと比較される。もし両者が同一でなければ、成績は0点となります。



It is of course FORBIDDEN to turn in your virtual machine in your Git repository. During the defense, the signature of the `signature.txt` file will be compared with the one of your virtual machine. If the two of them are not identical, your grade will be 0.



```
0010 01 11 111 001 000 11 01 10 1 0000 01 1 1010 111 11 0 000  
011 00 1 0000 1 0000 0 01 0100 1 0 010 10 01 1 0 0001 0 010 000  
00 111 10 111 0010 001100 001100 001100
```