

**Born2beroot**

**sungjuki**

## 1. preliminaries

# 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.

## Preliminary tests

- Defense can only happen if the evaluated student or group is present.  
This way everybody learns by sharing knowledge with each other.
- If no work has been submitted (or wrong files, wrong directory, or wrong filenames), the grade is 0, and the evaluation process ends.
- For this project, you have to clone their Git repository on their station.

Yes

No

별 다른 사항 없음.

## 2. general instructions

### General instructions

#### General instructions

- During the defense, as soon as you need help to verify a point, the student evaluated must help you.
- Ensure that the "signature.txt" file is present at the root of the cloned repository.
- 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 two signatures. If necessary, ask the student being evaluated where their ".vdi" file is located.
- As a precaution, you can duplicate the initial virtual machine in order to keep a copy.
- Start the virtual machine to be evaluated.
- If something doesn't work as expected or the two signatures differ, the evaluation stops here.

Yes

No

#### 참고

shasum은 SHA(secure hash algorithms) 형식으로 된 데이터를 연산하고 그 결과를 표준 출력으로 출력하는데 쓰이는 명령어.

리눅스에선 sha1sum, 맥, 유닉스에서는 shasum이다.

소프트웨어 패키지 혹은 cd/dvd 파일을 공유할 때, shasum 파일이 함께 배포되는 경우가 많음. shasum 파일은 원본 파일과 정확히 동일한 파일인지 확인할 때 체크하는 파일이다. 체크섬 정보가 포함되어 있음.

\*체크섬 : 중복 검사의 한 형태로, 송신된 자료의 무결성을 보호하는 단순한 방법.

\*b2r 프로젝트를 제출할 시점의 가상머신과 동료평가를 받을 때의 가상머신이 정확히 동일한지 확인하는 방법으로 shashum이 사용되는 것이며, 이를 signature.txt에 담아 제출한 것.

#### 확인할 것

- signature.txt 파일이 깃 레포에 있는지 확인
- signature.txt 파일이 평가 받을 vm의 ~.vdi와 같은지 확인
- 이후 vm 작동시켜서 평가 진행

```
$shashum "sungjuki.vdi" > eval.txt  
$diff signature.txt eval.txt
```

#### ref

<https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=wideeyed&logNo=221300065871>

<https://ciksite.com/ko/chapters/10470-shasum-command-on-linux>

### 3. mandatory part / project overview

#### Mandatory part

The project consists of creating and configuring a virtual machine following strict rules. The student evaluated will have to help you during the defense. Make sure that all of the following points are observed.

##### Project overview

- The student evaluated should simply explain to you:
  - The basic functioning of its virtual machine.
  - His choice of operating system.
  - The basic differences between Centos and Debian.
  - The interest of virtual machines.
  - If the evaluated student chose CentOS, he should explain to you what SELinux and DNF are.
  - If the evaluated student has chosen Debian he will need to explain the difference between aptitude and apt and what APPArmor is.
- During the defense, a script must display information all every 5 minutes. Its operation will be checked in detail later. If the explanations are not clear, the evaluation stops here.

✓ Yes

✗ No

5분마다 스크립트 띄우기

\$chmod +x monitoring.sh

\$crontab -e

\$\*/5 \* \* \* \*/root/monitoring.sh | wall

참고

\$crontab -e

-e 옵션은 새로 예약된 작업을 등록하거나 수정할 때 사용하는 옵션.

#### 확인할 것

- vm의 기본적인 작동 방식, vm의 이점
- 어떤 운영 체제를 선택했는지 (centos 와 debian 중)
- centos 와 debian의 기본적인 차이점
- 만약 debian을 선택했다면, aptitude와 apt가 무엇이고 둘의 차이가 무엇인지
- apparmor가 무엇인지
- 평가 중 5분마다 script 띄우기

### 3. mandatory part / project overview

-vm의 기본적인 작동 방식, vm의 이점

vm(virtual machine, 가상 머신)은 컴퓨팅 환경을 소프트웨어로 구현한 것. 하드웨어 컴퓨터와 마찬가지로 운영체제, 응용프로그램 등을 설치 및 실행할 수 있음.

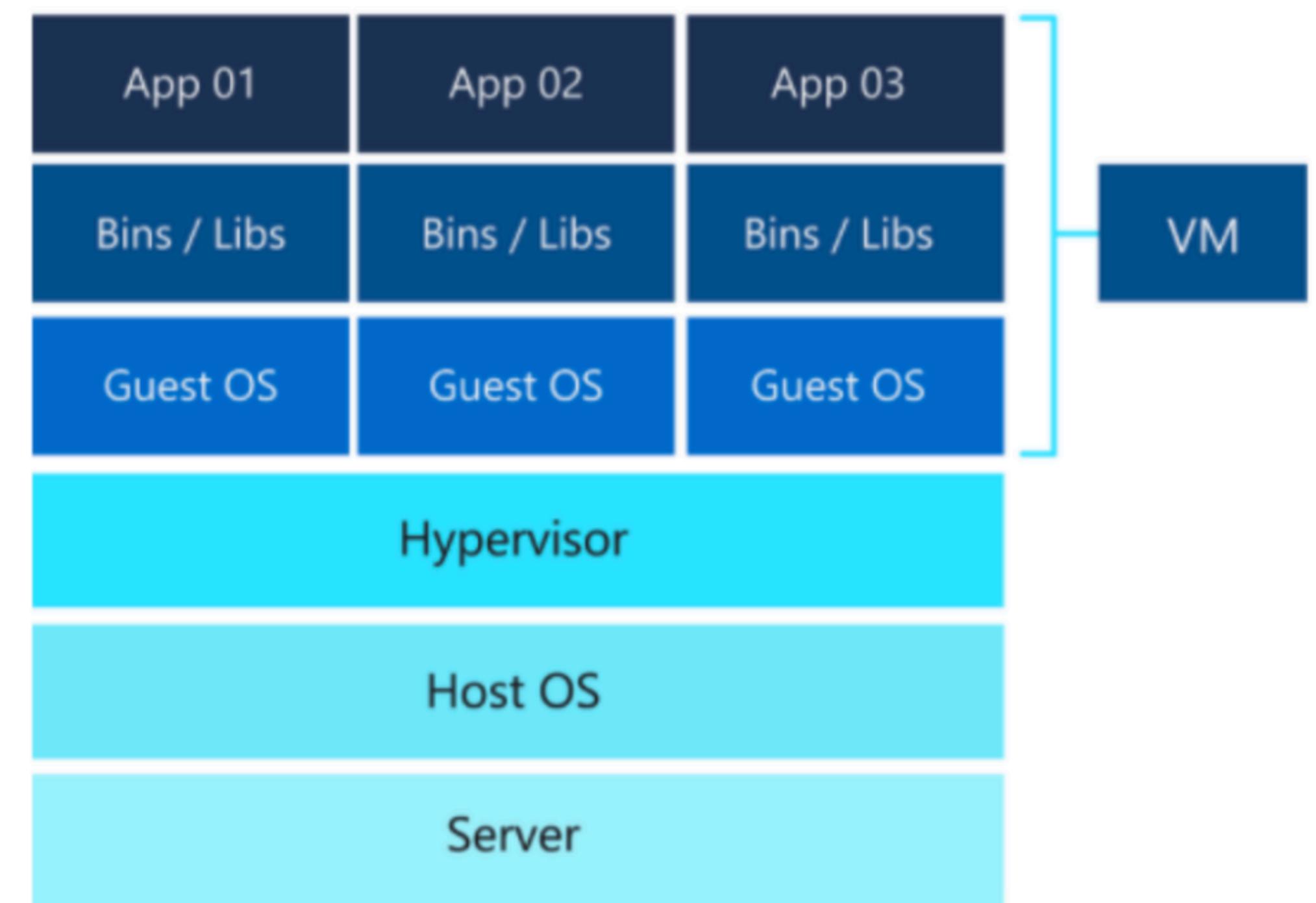
vm은 하이퍼바이저에 의해 구현됨. 하이퍼바이저가 호스트의 cpu, 메모리 등의 리소스를 처리하여 가상 머신(guest)에 할당하여 리소스를 관리해주는 방식으로 vm이 구현됨.

\*하이퍼바이저

vm을 생성하고 구동하는 소프트웨어임. b2r을 하기 위해 사용하는 virtual box도 하나의 하이퍼바이저.

vm을 사용하면, 물리적 리소스 추가 구매 비용, 전력, 공간 등등의 비용을 감소시킬 수 있음.

또한 분리된 환경으로 상호 방해 없이 테스트 환경 등을 쉽게 추가 가능.

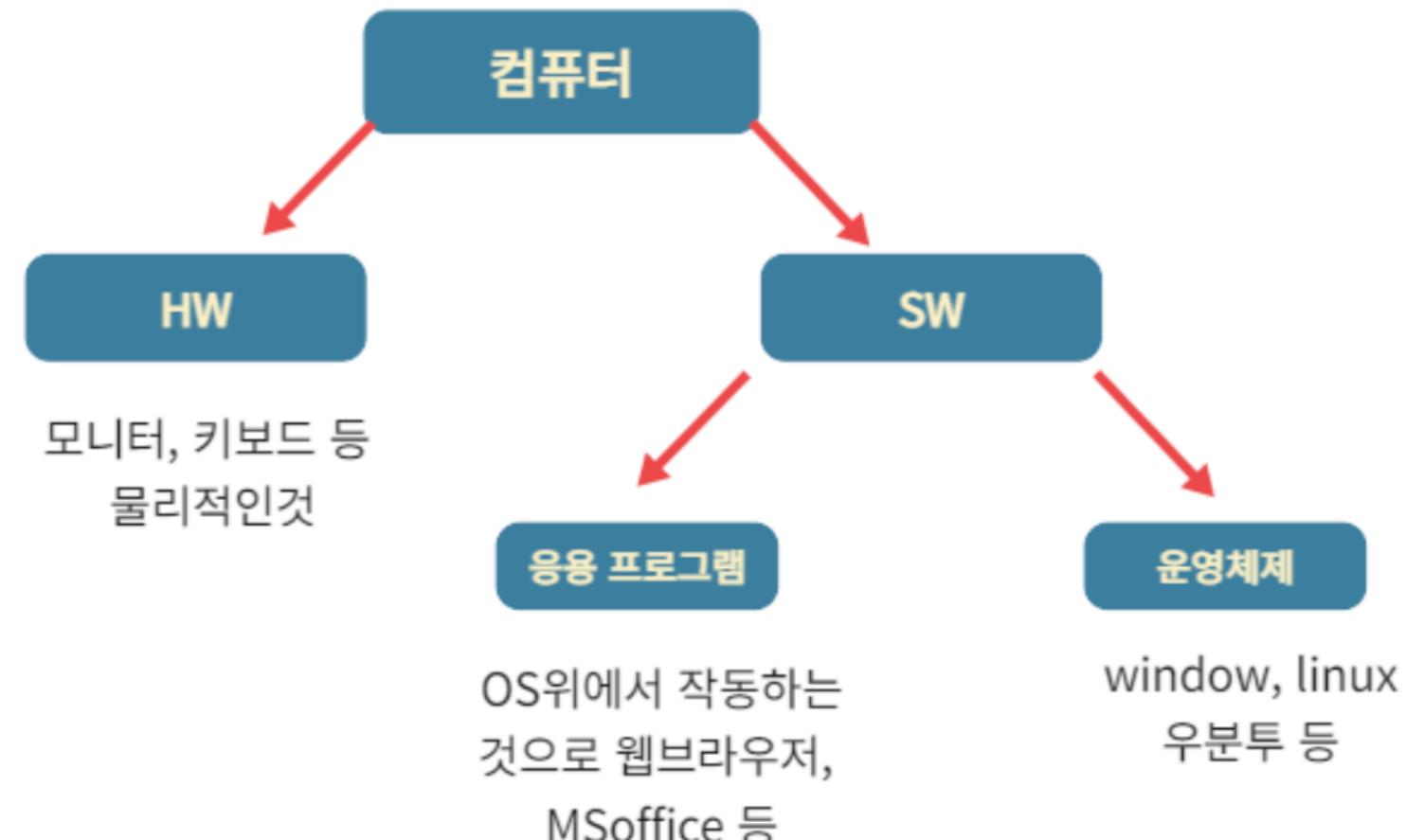


### 3. mandatory part / project overview

- 어떤 운영 체제를 선택했는지, centos 와 debian의 기본적인 차이점

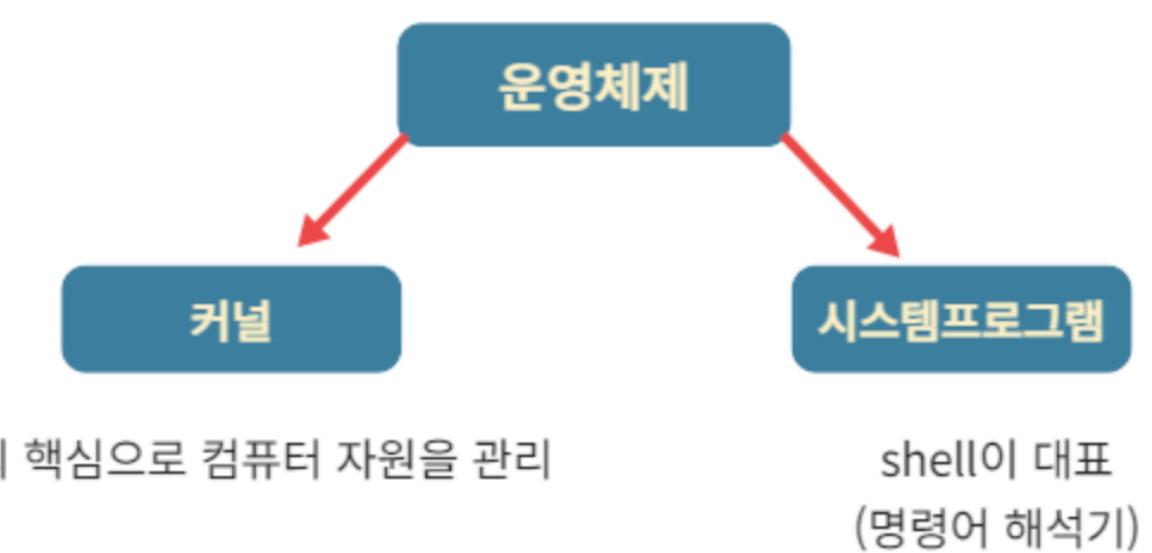
debian 선택.

debian과 centos는 모두 리눅스 배포판임. 리눅스 배포판은 리눅스 커널 + 자유소프트웨어(시스템 프로그램 shell 같은)로 구성된 유닉스 계열의 운영체제를 뜻한다. 즉, debian과 centos는 리눅스 커널이라는 공통점을 갖고 있으며, 자유소프트웨어(시스템 프로그램)에서 차이가 발생한다. 즉, 패키지 포맷, 패키지 관리 툴 등에서 차이가 발생함.



debian은 완전 자유 운영체제이며, 커뮤니티에 의해서 개발되고 디버깅된다. 개인용으로 만들어졌으며 다른 리눅스 배포판(ubuntu)의 기반이다.  
패키지 관리 툴로 apt, aptitude 등을 사용한다.

centos는 기업용(데스크탑/서버)이며, rhell(red hat enterprise linux)를 카피하여 배포된다.  
패키지 관리 툴로 yum, dnf 등을 사용한다.  
주로 서버에 사용된다.



참고

리눅스 커널이란 os의 중추 역할을 하는 것으로 메모리 관리, 프로세스 관리, 장치 드라이버 관리, 시스템 호출 및 보안 관리를 한다.

### 3. mandatory part / project overview

- 만약 debian을 선택했다면 aptitude와 apt가 무엇이고 둘의 차이가 무엇인지

앞서 말했듯, aptitude와 apt는 패키지 관리 툴이다. 둘 다 소프트웨어의 설치, 제거, 검색 등등의 기능을 제공한다.  
가령

```
$sudo aptitude install <package name>
$sudo apt-get install <package name>
```

식으로 사용.

둘 다 거의 비슷한 기능을 제공하고, 비슷한 방식으로 사용되나  
aptitude는 apt보다 high-level 툴이라는 차이가 있음. 패키지 과정이 apt보다 더 자동화되어 있음. 대화형 인터페이스, 비대화형 인터페이스(cui)를 모두 제공함.  
apt의 프론트엔드 프로그램이라 보면 됨.

- aptitude
  - 1. gui, cli 둘 다 지원
  - 2. apt 보다 high-level 툴. apt를 완전히 대체 할 수 있으며, apt 보다 더 자동화 되어 있음.
- apt
  - 1. cli 만 지원
  - 2. 여러가지 apt(cache, mark, get)에서 자주 사용하는 옵션만 추출하여, 사용자들이 편하게 사용하도록 만든 것.

### 3. mandatory part / project overview

- apparmor가 무엇인지

apparmor는 리눅스 커널의 보안 모듈임.  
debian에 기본적으로 설치되어있음.  
만약 설치되어있지 않다면

\$apt install apparmor apparmor-utils

로 설치 가능.

시스템 관리자가 프로그램 프로필 별로 권한을 제어. (네트워크 엑세스 권한, raw 소켓 액세스 권한, 파일의 읽기 쓰기 실행 권한 등등)  
또한 apparmor는 정책 파일을 통해 어떤 어플리케이션이 어떤 파일/경로에 접근 가능한지를 제어.

enforce 모드와 complain 모드 두 가지가 존재.

enforce mode : 허용되지 않은 파일에 접근 거부

complain mode : 어플리케이션이 허용되지 않은 행동을 하면 로그를 남김

참고

\$aa-enabled  
\$sudo aa-status  
\$pa auxZ | grep -v '^unconfined'

현재 활성화 여부 —> 이것만 체크하면 됨  
모드 확인  
접근 제한된 실행파일 확인

### 3. mandatory part / simple setup

#### Simple setup

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

- 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 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.
- Check that the SSH service is started with the help of the evaluator.
- Check that the chosen operating system is Debian or Centos with the help of the reviewer.

If something does not work as expected or is not clearly explained,

the evaluation stops here.



#### 확인할 것

- gui가 아닌 cli 환경인가?
- 머신에 접속할 때 패스워드를 물어보는가?
- 일반 유저로 접속 후 확인하기 -> sungjuki
  - 패스워드가 규칙에 맞는가(길이 10글자 이상, 대문자 포함, 숫자 포함, 연속된 글자 최대 2 글자)
  - ufw 서비스가 실행되었는지
  - ssh 서비스가 실행되었는지

#### 참고

\$sudo ufw status  
\$systemctl status ssh  
\$cat /etc/os-release(참고)

\$dpkg -l | grep xorg

#패키지 목록 확인

#### 참고

#### systemctl이란?

- RHEL 7에 도입된 systemd를 관리하는 명령어이다.
- /usr/lib/systemd/system 디렉토리의 .service파일을 systemctl 명령어로 서비스를 제어할 수 있다.

### 3. mandatory part / user

#### 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 evaluated student is present on the virtual machine. Check that it has been added and that it belongs to the "sudo" and "user42" groups.

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

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

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.

- Finally, ask the student 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.

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

Yes

No

#### 확인할 것

- 일반 유저(sungjuki)가 'sudo' 'user42' 그룹에 속해있는가?
- 다음에 따라 패스워드 정책 확인하기
  1. 유저 생성
  2. 그룹 'evaluating' 생성 후, 1에서 생성한 유저를 추가하고 확인하기.
- 패스워드 정책의 장단점 설명하기

#### 참고

```
$id sungjuki  
$adduser <NEW_USER>  
$groupadd evaluating  
$usermod -aG evaluating <NEW_USER>
```

유저의 그룹 정보 확인  
유저 생성하기  
그룹 생성하기  
유저를 그룹에 추가

```
$sudo deluser <NEW_USER> <GROUP_NAME>  
그룹에서 사용자 제거
```

```
$sudo userdel -r <NEW_USER>  
사용자 제거
```

### 3. mandatory part / user

#### 패스워드 정책 확인

```
/etc/login.defs
PASS_MAX_DAYS 30      # 패스워드 최대 사용 기간
PASS_MIN_DAYS 2       # 패스워드 최소 사용 기간
PASS_WARN_AGE 7        # 만료 알림 날짜
PASS_MIN_LEN 10       # 패스워드 최소 글자수

/etc/pam.d/common-password      libpam-cracklib

password requisite pam_cracklib.so \
    retry=3                  \
    \# 패스워드 최대 재시도
    minlen=10                \
    \# 패스워드 최소 글자수
    maxrepeat=3              \
    \# 반복 가능한 글자수
    ucredit=-1 lcredit=-1 dccredit=-1 \
    \# 최소 소문자, 대문자, 숫자 글자수
    difok=7                  \
    \# 기존 패스워드와 겹치지 말아야하는 글자수
    reject_username enforce_for_root \
    \# username과 패스워드 일치할 수 없음, root에도 적용
```

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

- Your password has to expire every 30 days.
- The minimum number of days allowed before the modification of a password will be set to 2.
- The user has to receive a warning message 7 days before their password expires.
- Your password must be at least 10 characters long. It must contain an uppercase letter and a number. Also, it must not contain more than 3 consecutive identical characters.
- The password must not include the name of the user.
- 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.
- Of course, your root password has to comply with this policy.

ref

<https://docsplayer.org/224524361-Born2beroot-sarchoi.html>

### 3. mandatory part / hostname and partitions

#### Hostname and partitions

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

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

login42 (login of the student evaluated).

- 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.

- You can now restore the machine to the original hostname.

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

- 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.

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.

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:~$ _
```

✓ Yes

✗ No

확인할 것

- hostname이 'login42' 형식인가

- hostname 변경해보기(평가자 id로)

  -> 평가자 아이디로 로그인 해서 호스트명이 변경되었는지 확인

  -> 확인이 되었다면 원래의 호스트명으로 변경 후 다시 평가 진행

- 파티션 확인하기

- LVM이 무엇이고 어떻게 작동하는지

참고

\$hostnamectl

\$sudo hostnamectl set-hostname <NEW\_NAME>

\$sudo reboot

\$lsblk

호스트명 체크

호스트명 변경

블록디스크 구성 확인

\$sudo deluser <NEW\_USER> <GROUP\_NAME>

그룹에서 사용자 제거

\$sudo userdel -r <NEW\_USER>

사용자 제거

### 3. mandatory part / hostname and partitions

- LVM이 무엇이고 어떻게 작동하는가

LVM : logical volume manager

LVM이란 물리적인 디스크를 논리적인 디스크로 할당하여, logical volume을 효율적이고 유연하게 관리하기 위한 커널의 한 부분이자 프로그램.

기존에는 파일 시스템을 블록 장치에 직접 접근해서 쓰는 방식이라면

LVM은 파일시스템을 LVM이 만들어 놓은 가상의 블록 장치에서 읽고 쓰는 방식.

예를 들어,

어떤 윈도우에서 c 드라이브의 용량이 부족할 때 우리는 파일을 지워서 공간을 확보하거나 백업 후, 더 큰 디스크로 교체하고 그 디스크에 다시 백업한 정보를 옮겨야 함.

이는 리눅스도 마찬가지. 개인적으로 컴퓨터를 사용할 경우에는 이런 방식이 큰 문제가 되지 않지만 기업에서 서버를 운영한다고 생각하면, 매번 이렇게 디스크를 교체할 수 없음.

그래서 LVM을 사용하는 것.

“LVM”으로 “LV(logical volume)”을 만들어서 사용하면 기존에 사용중이던 디스크 공간에 추가해 바로 사용할 수 있음. 물리적인 디스크를 사용할 경우에는 이게 불가능함.

ref

<https://mamu2830.blogspot.com/search?q=LVM>

<https://docsplayer.org/224524361-Born2beroot-sarchoi.html>

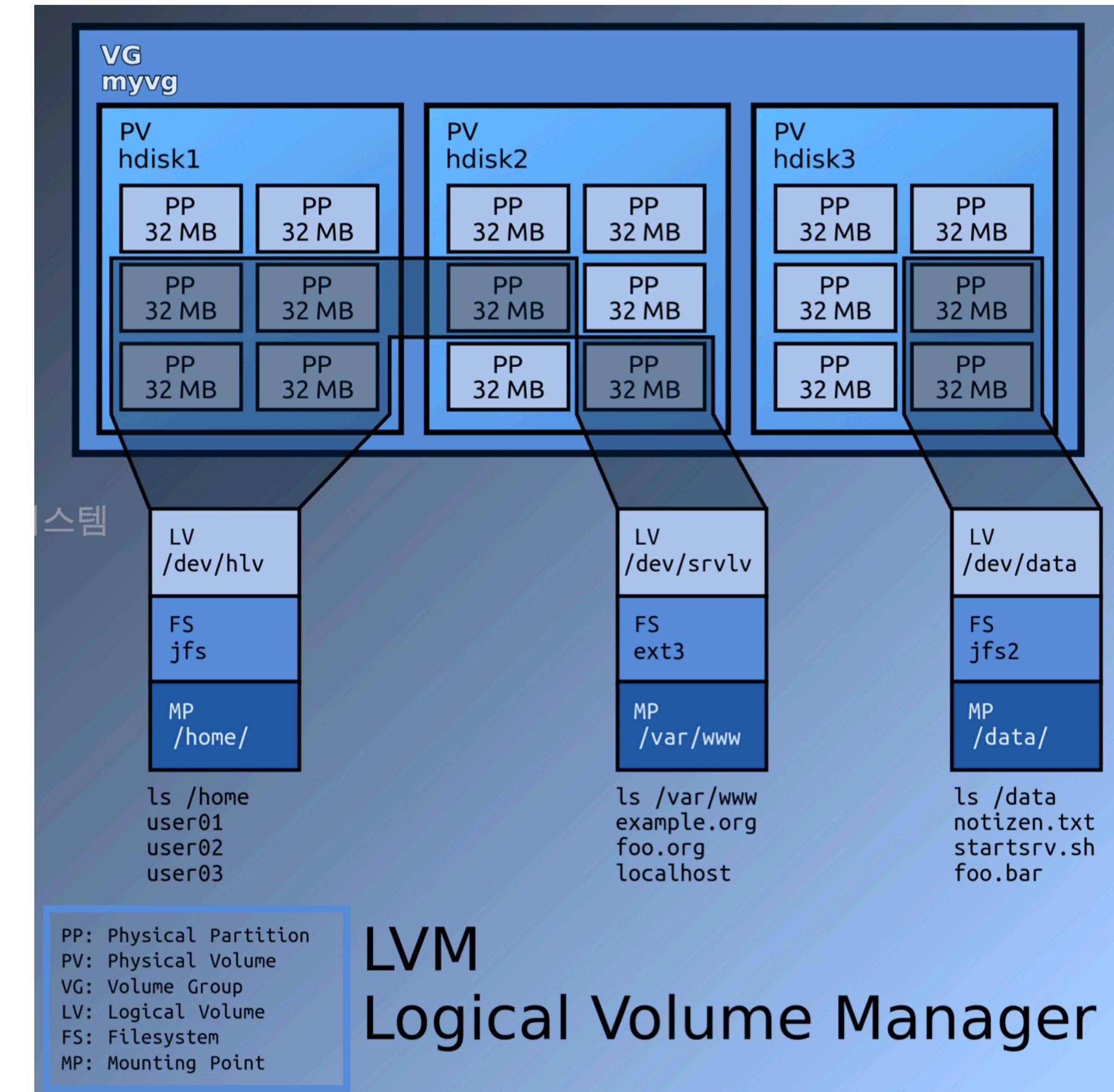
### 3. mandatory part / hostname and partitions



pv는 physical volume이며 pe(physical extent)라는 단위로 구성되어 있음.  
(pv는 기존의 디스크 공간과 별 차이가 없는 물리적 공간이지만 기존의 디스크와 다르다. lvm에서 사용하는 개념이며, pe를 최소 단위로 사용한다는 것.)

이런 pv들을 합쳐서 vg(volume group)로 만듬. 이후에 이런 vg들을 lv(logical volume)로 만들어서 사용함. 그림에서 보면 연속적으로 되어있으나, 불연속적인 것들도 묶어서 사용할 수 있음.

간단하게 작동 방식을 보면  
디스크, 파티션 -> 볼륨 그룹(VG) -> 논리 볼륨(LV) -> 파일 시스템



### 3. mandatory part / sudo

#### SUDO

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

- Check that the "sudo" program is properly installed on the virtual machine.
- The evaluated student should now show assigning your new user to the "sudo" group.
- The subject imposes strict rules for sudo. The evaluated student must first explain the value and operation of sudo using examples of their choice.

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

- 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.

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.

 Yes

 No

#### 확인할 것

- sudo 프로그램이 제대로 설치되어 있는가
- 새 유저를 sudo 그룹에 할당하기
- visudo를 통해 subject 룰들이 제대로 적용되어 있는지 확인
- /var/log/sudo 디렉토리가 존재하는지, 그 디렉토리 밑에 파일이 생성되어 있는가
- 'sudo' 커맨드 실행 후 히스토리 갱신 확인

```
$dpkg -l sudo / sudo --version  
$usermod -aG sudo <NEW_USER>  
$visudo
```

\*sudo를 설치하면, sudoers 파일에 원하는 사용자를 등록 시킬 수 있음. visudo 커맨드를 사용하면, 문법체크 기능이 있어서 실수를 방지할 수 있음.

### 3. mandatory part / sudo

- visudo를 통해 subject 룰들이 제대로 적용되어 있는지 확인할 것

```
visudo

Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:
/bin:/snap/bin"                                # 사용할 수 있는 경로 제한
Defaults    passwd_tries=3                         # 패스워드 3번 틀렸을 경우 제한
Defaults    badpass_message="Password is wrong."   # 잘못된 암호 커스텀 메세지
Defaults    authfail_message="Authentication failed."
Defaults    log_input                               # 입력 로깅
Defaults    log_output                             # 출력 로깅
Defaults    iolog_dir="/var/log/sudo/"             # 로그 디렉토리
Defaults    requiretty                            # 보안 문제 TTY 모드 활성화

root ALL=(ALL:ALL) ALL
<USERNAME> ALL=(ALL:ALL) ALL                      # sudo 사용할 유저 추가
```

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

- Authentication using **sudo** has to be limited to 3 attempts in the event of an incorrect password.
- A custom message of your choice has to be displayed if an error due to a wrong password occurs when using **sudo**.
- 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.
- **The TTY mode has to be enabled for security reasons.**
- 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**

### 참고

#### -secure\_path

sudo 명령 실행 시 현재 계정의 쉘이 아닌 새로운 쉘을 생성하고 그 안에서 명령을 실행하는데, 이때 명령을 찾을 경로를 나열한 환경변수인 PATH값이 바로 **secure\_path**. 트로이목마 해킹 공격에 대한 일차적 방어 기능을 제공.(사용자의 부주의로 현재 계정의 PATH에 악의적인 경로가 포함된 경우, 이를 무시함으로써 sudo를 통해서 전체 시스템이 해킹 되는 것을 방지)

-log\_input #sudo명령어 실행 시 입력된 명령어 log에 저장  
-log\_output #sudo명령어 실행 시 출력 결과를 log에 저장  
-iolog\_dir #sudo log 저장 디렉토리 설정  
-requiretty #sudo가 tty 모두 외부에서 사용되지 않도록 함  
-tty #텍스트모드(콘솔모드) TTY 란 터미널 환경을 뜻한다. iterm과 같은 외부 터미널 환경은 pty라고 하며 이 외에도 여러가지 환경이 있다.

### 참고

<https://nostressdev.tistory.com/m/8>

### 3. mandatory part / sudo

- /var/log/sudo 디렉토리가 존재하는지, 그 디렉토리 밑에 파일이 생성되어 있는지.
- 'sudo' 커맨드 실행 후 히스토리 갱신 확인하기.

sudo는 root가 아닌 사용자가 root에 준하는 능력으로 sudo 다음에 나오는 명령을 실행하게 하는 명령어.

sudo를 사용하면 sudoers에 자신이 노출되기에 침입을 확인할 수 있음. 즉, log가 남아 쉽게 추적 가능(root 계정에서 작업하면 log가 남지 않음)

```
$sudo ls /var/log/sudo  
$sudo apt update  
$sudo ls /var/log/sudo/00/00
```

구분	SU	SU -
환경변수	TERM	변경
	HOME	변경
	SHELL	변경
	USER	변경
	LOGNAME	변경
	PATH	유지
	기타	유지
워킹디렉토리	유지	변경

참고

su는 root 패스워드가 필요하지만 sudoer에서 사용을 허락한 사용자는 모두 패스워드와 관계없이 쓸 수 있음.

su <변경하고자 하는 사용자 id>

: 다른 계정으로 전환하는 것. 현 사용자를 로그아웃하지 않고, 다른 사용자의 권한을 획득할 때 사용함.

su 뒤에 변경할 사용자 id를 입력하지 않으면 su root와 동일하게 작동함.

su - : 다른 계정으로 전환 + 그 계정의 환경변수 적용

su - 에서 -l 혹은 --login과 동일한 명령어. 즉 su - 는 su --login root와 동일한 명령어이다.

### 3. mandatory part / ufw

#### UFW

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

- Check that the "UFW" program is properly installed on the virtual machine.
- Check that it is working properly.
- The evaluated 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.
- Finally, delete this new rule with the help of the student evaluated.

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

✓ Yes

✗ No

#### 확인할 것

- ufw가 제대로 설치되어 있고, 제대로 작동하는가
- ufw가 무엇인가
- 활성화 되어있는 ufw의 규칙 리스트 보여주기. 4242포트가 있어야 함.
- 8080 포트 새로 추가하고 리스트 확인하기.
- 새로 추가한 8080 포트 지우기

\$ sudo ufw status (verbose) #작동 상태 확인

### 3. mandatory part / ufw

- ufw가 무엇인가
- 활성화 되어있는 ufw의 규칙 리스트 보여주기. 4242포트가 있어야 함.
- 8080 포트 새로 추가하고 리스트 확인하기.
- 새로 추가한 8080 포트 지우기

ufw란?

uncomplicated firewall

ufw는 데비안 계열 리눅스 환경에서 작동하는, 이름 그대로 ‘복잡하지 않은’ 방화벽 관리 프로그램이다. 서비스명(ex: ssh), ip주소, 포트번호, ping 요청 등을 허용/거부 할 수 있는 기능을 제공한다. 가령, b2r 과제에서 맥 터미널에서 vm 환경으로 접속할 수 있는데, 그 때 22 port 대신 4242 port를 사용하게 제한하는데, 이런 역할을 해주는 것이 ufw.

보안확보를 위해 내부 네트워크와 외부통신을 제어하고, 내부 네트워크의 안전을 유지할 수 있게 하는 기술.  
(데비안 및 리눅스에서 작동되고 파이썬으로 개발되었다고 함)

참고

\$sudo apt install ufw	#ufw 설치
\$sudo ufw enable	#부팅 시 ufw 활성화
\$sudo cat /etc/ufw/user.rules	#rules 조회
\$sudo allow 4242	#4242 port 개방
\$sudo default deny	#기본 정책을 차단
\$sudo ufw status numbered	#정책들에 번호를 붙여 나열하며 확인
\$sudo ufw delete <rule number>	#정책 번호로 삭제

### 3. mandatory part / ssh

#### SSH

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

- Check that the SSH service is properly installed on the virtual machine.
- Check that it is working properly.
- The evaluated 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.
- The student 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.  
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.

Yes

No

#### 확인할 것

- ssh 프로그램 설치 여부 및 작동 확인
- ssh가 4242포트에서만 사용되는지
- 새로 만든 사용자로 ssh 접속 시도해보기. 이 때 key 혹은 패스워드를 사용할 수 있음
- root 유저로 ssh 접속이 되지 않는 것 확인하기
- ssh가 무엇이고 왜 사용하는지

\$ apt search openssh-server #ssh가 설치되어 있는지 검색

\$ sudo ssh -V

\$ systemctl status ssh #ssh 작동 여부 확인

\$ ss -tnulp

mac\$ ipconfig getifaddr en0 #호스트 ip 체크

mac\$ ssh USERNAME@<호스트IP> -p 4242

\$ apt install openssh-server #설치

\$ apt sudo ufw allow 4242 #4242port 개방

### 3. mandatory part / ssh

-ssh가 무엇이고 왜 사용하는지

#### ssh(secure shell)

네트워크로 연결된 두 호스트 간 rsa암호화(공개키 암호화 혹은 비대칭 키 암호화) 기술을 사용하여 통신 중 데이터 노출의 위협이 없도록 하는 보안 프로토콜.  
원격 호스트(shell)에 접속하기 위해 사용됨.

1995년에 나온 프로토콜이며 기본 포트는 22번. 이름대로 shell로 원격 접속을 하는 것이기에 접속 후에도 CLI에서 작업하게 됨.

key를 이용하여 보안을 구성하고, 기본적으로 ssh key는 public key, private key 두 가지로 이루어진다.

비공개 키는 로컬 머신(게스트)에 위치하며, 공개키는 리모트 머신(호스트)에 위치해야 한다. ssh 접속을 시도하면 로컬 머신의 키와 리모트 머신의 키를 비교하여 일치하는지 확인함.

#### 작동 원리

클라이언트와 호스트가 각각 키를 보유하고 있고, 이를 활용하고 주고 받는 데이터를 암호화함.  
키가 없으면 중간에 데이터를 가로채도 무슨 정보인지 알 수 없음.

### 3. mandatory part / script monitoring

#### Script monitoring

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

The student evaluated should explain to you simply :

- The operation of its script by displaying its code.
- What is "cron".
- How the evaluated student set up her script so that it runs every 10 minutes when the server starts up.

Once the correct functioning of the script has been verified, the student evaluated should ensure that this script runs every 30s. You can run whatever you want to make sure the script runs with dynamic values correctly, and the student evaluated should make the script stop running when the server starts up, but without modifying the script. in himself. 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.

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

 Yes

 No

#### 확인할 것

- 매 1분마다 실행되게 변경하기
- 서버 시작 시 뜨지 않게 변경해보기
  - 스크립트 파일 내용 변경 금지, 파일 위치 이동 금지, 파일 권한 변경 금지
- cron 이란

#### 참고

멈추기

\$/etc/init.d/cron stop

시작

\$/etc/init.d/cron start

reboot 후에도 멈추게 하려면 아래의 명령도 추가

\$sudo systemctl disable cron

\$sudo reboot

\$sudo service cron status

\$sudo systemctl enable cron

### 3. mandatory part / script monitoring

```
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 (39%)
#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
```

1. 운영 체제 및 해당 커널 버전의 아키텍처
2. 물리적 프로세서의 수
3. 가상 프로세서의 수
4. 서버에서 현재 사용 가능한 RAM 및 사용률(백분율)
5. 서버의 현재 사용 가능한 메모리 및 사용률(백분율)
6. 프로세서의 현재 사용률을 백분율로 표시
7. 마지막 재부팅 날짜 및 시간
8. LVM이 활성 상태인지 여부
9. 활성 연결 수
10. 서버를 사용하는 사용자 수
11. 서버의 IPv4 주소 및 해당 MAC(Media Access Control) 주소
12. sudo 프로그램으로 실행된 명령 수

### 3. mandatory part / script monitoring

-cron 이란

유닉스 계정의 작업예약스케줄러임

특정 작업을 특정 시간에 자동으로 실행시키기 위한 프로세스임.

job scheduler 성격의 데몬 프로세스라고 함.

job : 특정 작업이나 프로세스

scheduler : 특정한 시간마다 혹은 특정한 이벤트 발생시 job을 자동으로 실행시키는 것

데몬 프로세스 : 사용자가 직접 제어하지 않고, 백그라운드에서 돌면서 여러 작업을 하는 프로그램.

백그라운드 프로세스와 다른 점은 사용자와 상호작용하지 않는 독자적인 프로세스라는 것.

반복적인 일들을 자동화해주며 많은 곳에서 두루 활용됨.

특정 시간마다 db를 백업할 수도 있고, 특정시간마다 웹페이지를 스크래핑하는 cron을 만들 수도 있음.

\* \* \* \* command

분, 시간, 날짜(1~31), 월(1~12), 요일(0~6) 순.

그 밖에 옵션들이 있으나, 그때그때 필요한 거 찾아서 적용시키면 됨.

ref

b2r 전반적인 부분

<https://techdebt.tistory.com/18?category=833728>

<https://velog.io/@kurikuri/born2beroot>

<https://infinit.tistory.com/390>

[https://padawanr0k.github.io/posts/ft\\_seoul/born2beroot/01/index/](https://padawanr0k.github.io/posts/ft_seoul/born2beroot/01/index/)

<https://blog.naver.com/PostView.naver?blogId=digitalnomad00&logNo=222414374887&redirect=Dlog&widgetTypeCall=true&directAccess=false>

<https://baigal.medium.com/born2beroot-e6e26dfb50ac>

<https://www.notion.so/born2beroot-2ce1177e08904c329fb437c7fdcd7113#fa7cbae3731748f18dcb49158a854f0b>

<https://sincerity.page/categories/42Seoul/Born2beRoot/>

세부사항

<https://brownbears.tistory.com/227> - sudo, su 차이점

<https://mamu2830.blogspot.com/2019/12/lvmpv-vg-lv-pe-lvm.html> - lvm이란

<https://ciksiti.com/ko/chapters/10470-shasum-command-on-linux> - shsum 명령어

<https://velog.io/@taeskim/cron> - cron 이란

[https://padawanr0k.github.io/posts/ft\\_seoul/born2beroot/01/index/](https://padawanr0k.github.io/posts/ft_seoul/born2beroot/01/index/)

<https://infinit.tistory.com/390>

## 참고

```
uname -a // 시스템의 정보를 출력  
nproc --all // 물리적으로 설치된 프로세스 갯수  
cat /proc/cpuinfo | grep processor | wc -l  
free -m // 메모리 사용량을 mb 단위(-m)로 출력한다  
df -P // 리눅스 내 디스크 메모리 전체 현황을 한줄로(-P) 출력한다  
mpstat // 현재 CPU의 사용량을 출력한다  
who -b // 마지막 리부트 날짜와 시간  
ss -t | grep -i ESTAB // 활성화된 tcp 네트워크 상태를 출력한다 |  
who // 서버를 사용하는 유저들을 출력한다  
hostname -I // IPv4 주소
```