

# HW1\_과제설명

2019.09.30

조재희

jehee1204@gmail.com

# 요약

## ❖ 환경설정

- VirtualBox 설치
- 가상머신 환경 다운로드 및 설치
  - SEED\_LAB\_CSOS.ova

## ❖ HW\_1 개요

- Race condition Attack

## ❖ HW\_1 실습

- Race condition vulnerability 설명
- Race condition Attack 실습

## ❖ HW\_1 제출

- 평가기준
- 제출/문의

# 환경설정

2019.09.30

조재희

jehee1204@gmail.com

# 환경설정

## ❖ VirtualBox 다운로드

- (<https://www.virtualbox.org/wiki/Downloads>)

### Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

#### VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 5.2 packages, see [VirtualBox 5.2 builds](#). Please discontinued in 6.0. Version 5.2 will remain supported until July 2020.

#### VirtualBox 6.0.12 platform packages

- [Windows hosts](#)
- [OS X hosts](#)
- [Linux distributions](#)
- [Solaris hosts](#)

The binaries are released under the terms of the GPL version 2.

See the [changelog](#) for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages *treated as insecure!*

# 환경설정

## ❖ 가상머신 환경 다운로드

- SEED\_LAB\_CSOS.ova
  - <http://securesw.dankook.ac.kr>

### ○ 학부 강의자료 (Lecture Notes)

#### ▷ Operating System Security (운영체제보안 / 2019-2학기)

- HW\_00: 개인과제 가상머신 - 다운로드
- HW\_01: 개인과제 - Race condition(09/28)

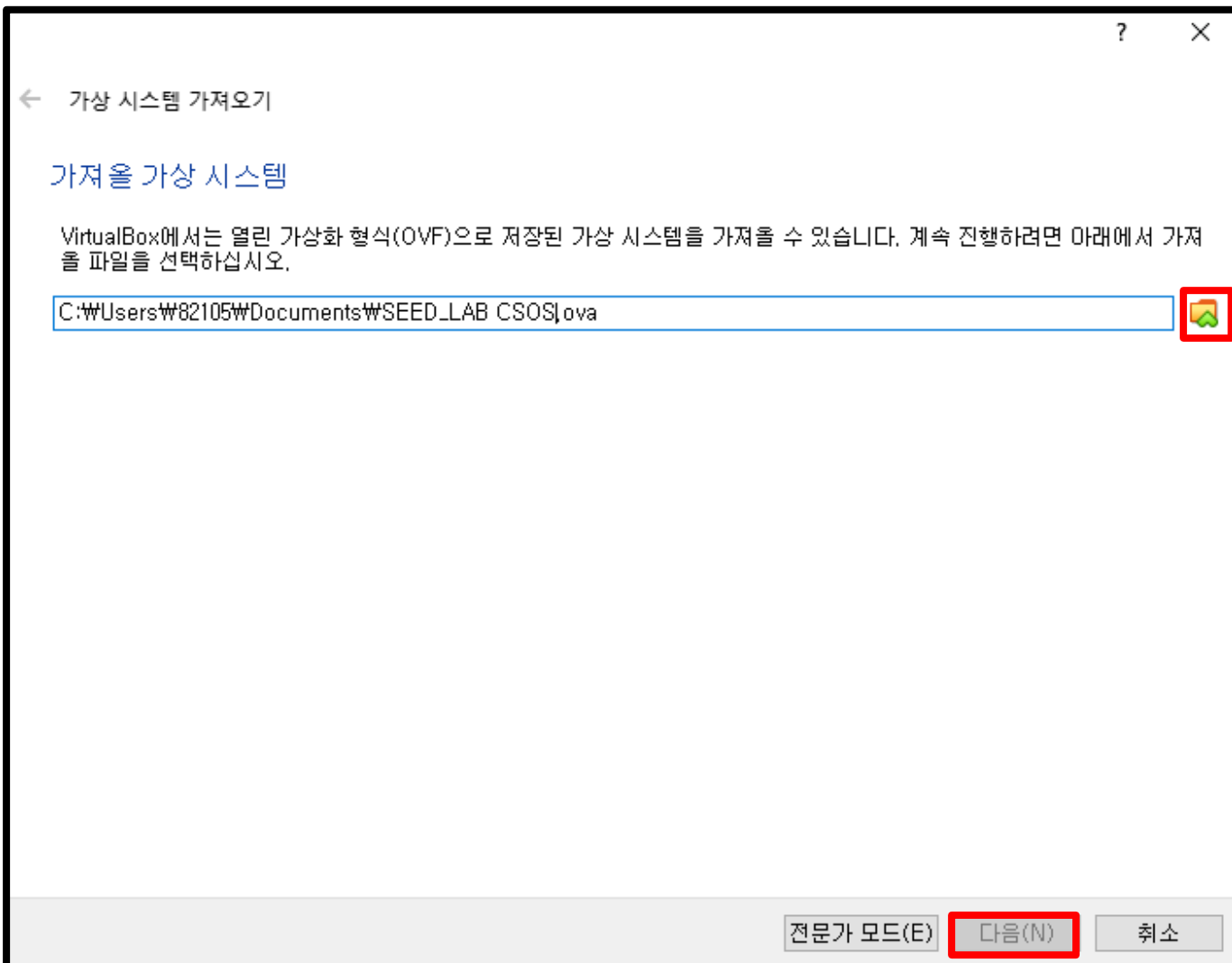
# 환경설정

## ❖ SEED\_LAB\_CSOS.ova 설치(1/6)



# 환경설정

## ❖ SEED\_LAB\_CSOS.ova 설치(2/6)



# 환경설정

## ❖ SEED\_LAB\_CSOS.ova 설치(3/6)

가상 시스템 가져오기

가상 시스템 설정

아래 목록은 가상 시스템 설명 파일에 나와 있는 가상 머신이며, 이를 VirtualBox로 가져왔을 때의 형태입니다. 보여져 있는 속성을 두 번 누르면 변경할 수도 있으며, 체크 상자를 사용해서 비활성화시킬 수도 있습니다.

가상 시스템 1	
이름	SEED_LAB_CSOS
게스트 운영 체제 종류	Ubuntu (32-bit)
CPU	1
RAM	1024 MB
DVD	<input checked="" type="checkbox"/>
USB 컨트롤러	<input checked="" type="checkbox"/>
사운드 카드	<input checked="" type="checkbox"/> ICH AC97

You can modify the base folder which will host all the virtual machines, Home folders can also be individually (per virtual machine) modified.

C:\Users\W82105\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☒ Import hard drives as VDI

가상 시스템이 서명되지 않았음

기본값 복원

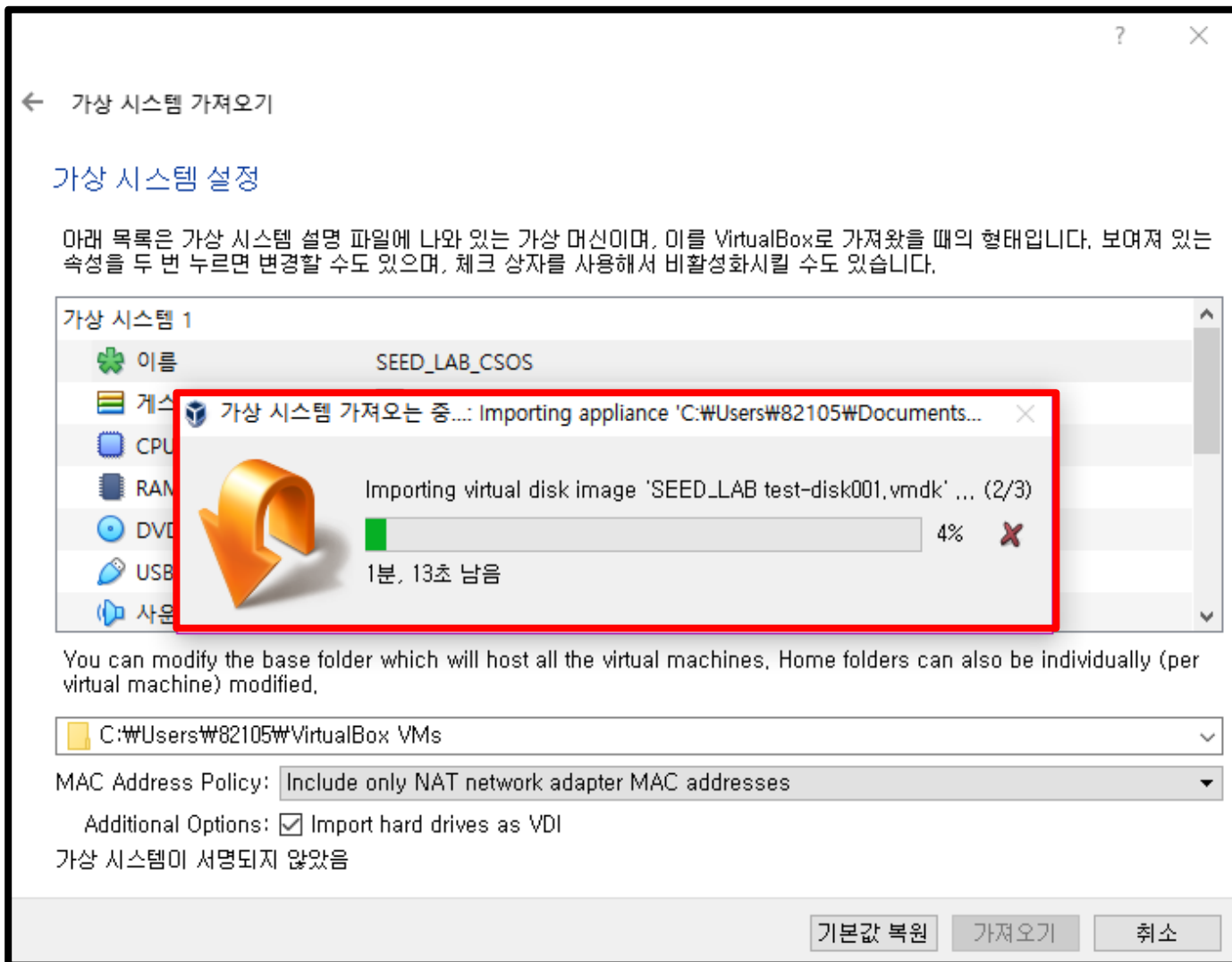
가져오기

취소



# 환경설정

## ❖ SEED\_LAB\_CSOS.ova 설치(4/6)



# 환경설정

## ❖ SEED\_LAB\_CSOS.ova 설치(5/6)



# 환경설정

## ❖ SEED\_LAB\_CSOS.ova 설치(6/6)



# HW1\_Race Condition Attack

공격 실습을 통한 Race Condition 이해

2019.09.30

조재희

jehee1204@gmail.com

# HW1 – Race Condition Attack

## ❖ Race Condition Attack 실습

- CSOS -> HW1 -> RaceCondition

## ❖ HW1

- (1) 수행결과 스크린 샷
  - 1-1) ./resCheck.sh
  - 1-2) ./symp
  - 1-3) /etc/passwd
- (2) 공격프로그램 동작 분석
  - race condition이 발생할 수 있는 원인을 논리적으로 서술
  - 취약점 공격의 동작 과정과 결과를 논리적으로 분석
- (3) 취약점 보완 (보너스)

## ❖ 제출

- 실습 및 과제 내용을 보고서로 제출
- 제출기간 : 9월 30일 (월) ~ 10월 14일 (월)

## ❖ Race Condition (경쟁 조건)

- 여러 프로세스가 동일한 데이터에 동시에 액세스하고 조작할 때 발생
- 조작의 타이밍이나 순서 등이 예상과 다르게 작동하면서 비정상적인 결과가 나올 수 있음

# 실습

## ❖ 목표

- Set-UID프로그램의 Race Condition 취약점을 악용
- 최종적으로 root권한을 얻는 것
  - root권한을 가진 새 사용자 계정을 만드는 것

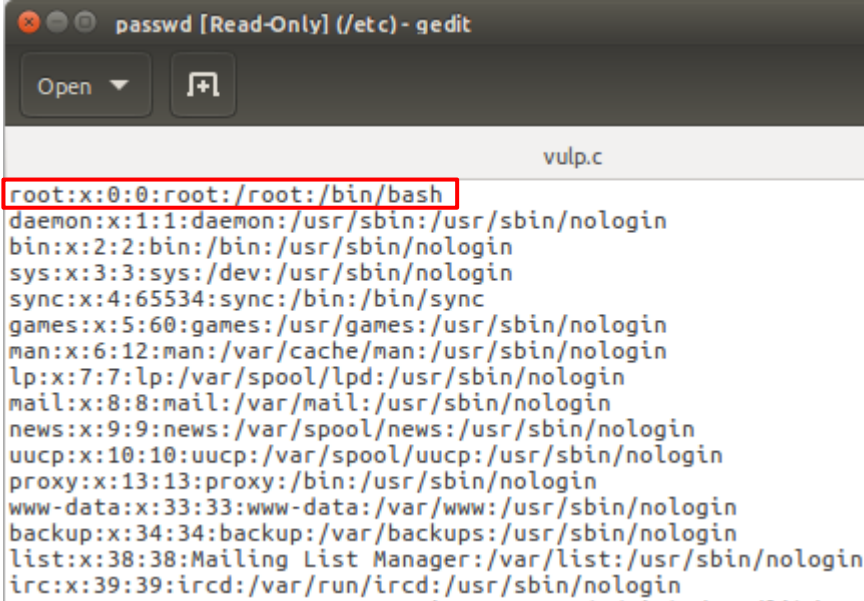
```
STOP... The passwd file has been changed!  
[09/25/19]seed@VM:~/.../RaceCondition$ su test  
Password:  
root@VM:/home/seed/Desktop/CS0S/HW1/RaceCondition# id  
uid=0(root) gid=0(root) groups=0(root)  
root@VM:/home/seed/Desktop/CS0S/HW1/RaceCondition#
```

- 일반 사용자가 쓸 수 없는 암호파일(/etc/passwd)을 대상으로 선택
  - 암호파일에 레코드를 추가하여 root권한을 가진 새 사용자 계정 생성

# 실습

## ❖ 암호파일(패스워드 파일)

- /etc/passwd
- 리눅스 계정 정보를 담은 텍스트 파일
  - 이름과 달리 passwd 정보는 보이지 않음
    - 원래는 passwd 해시값을 보관 했으나
    - 현재는 그 값을 /etc/shadow 파일에 저장하고
    - 그 자리에는 x가 기입되어있음



```
passwd [Read-Only] (/etc) - gedit
vulp.c
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
```



## ❖ 암호파일(패스워드 파일)

- 콜론(:) 으로 구분된 7개의 필드로 구성
  - root : x : 0 : 0 : root : /root : /bin/bash

①   ②   ③   ④   ⑤            ⑥            ⑦

- ① 사용자 이름
- ② 패스워드(or 암호필드) (/etc/shadow 파일에 암호화되어 있음)
- ③ 사용자 계정 uid
  - Root사용자의 경우 uid 필드가 0
  - 즉 root사용자가 로그인 할 경우 프로세스의 uid가 0으로 설정  
-> 프로세스에 root권한 부여
  - Root권한으로 계정을 만들고 싶다면 3번째 필드에 0을 입력
  - 기본적으로 root계정의 권한은 사용자 이름 필드가 아니라 uid 필드에서 오는 이름
- ④ 사용자 계정 gid
- ⑤ 사용자 계정 이름(정보)
- ⑥ 사용자 계정 홈 디렉토리
- ⑦ 사용자 계정 로그인 셸

## ❖ 암호파일(패스워드 파일)

- input.txt
  - test :U6aMy0wojraho:0:0:test:/root:/bin/bash
    - “There is a magicvalue used in Ubuntu live CD for a password-less account, and the magic value is U6aMy0wojraho (the 6th character is zero, not letter O). If we put this value in the password field of a user entry, we only need to hit the return key when prompted for a password.”

# 실습

## ❖ vulp 생성 (Set-UID 프로그램 설정)

- gcc vulnerableProgram.c -o vulp
- sudo chown root vulp
  - sudo PW : dees
- sudo chmod 4755 vulp

## ❖ symp 생성 (타겟설정)

- gcc symlinkProgram.c -o symp

## ❖ 파일구성

```
[09/25/19]seed@VM:~/.../RaceCondition$ ls -l
total 588
-rw-rw-r-- 1 seed seed    45 Sep 25 00:26 input.txt
-rwxrwxrwx 1 seed seed   204 Sep 24 22:03 resCheck.sh
-rw-rw-r-- 1 seed seed   371 Sep 24 14:09 symlinkProgram.c
-rwxrwxr-x 1 seed seed  7472 Sep 24 14:09 symp
-rw-rw-r-- 1 seed seed 562022 Sep 25 02:35 textRes.txt
-rw-rw-r-- 1 seed seed   392 Sep 25 01:44 vulnerableProgram.c
-rwsr-xr-x 1 root seed  7640 Sep 25 02:33 vulp
```

## ❖ Symbolic link 제한 (실습 환경에 기본값으로 구성했음)

```
[09/24/19]seed@VM:~/.../RaceCondition$ sudo sysctl -w fs.protected_symlinks=0
[sudo] password for seed:
fs.protected_symlinks = 0
[09/24/19]seed@VM:~/.../RaceCondition$
```

- `sudo sysctl -w fs.protected_symlinks=0`
  - sudo PW : dees
- “symlinks in world-writable sticky directories (e.g./tmp) cannot be followed if the follower and directory owner do not match the symlink owner.”

# 실습

## ❖ ./symp

```
1830 times attempt
1831 times attempt
1832 times attempt
1833 times attempt
1834 times attempt
1835 times attempt
1836 times attempt
^C
[09/24/19]seed@VM:~/.../RaceCondition$
```

## ❖ ./resCheck.sh

```
No permission
No permission
No permission
No permission
STOP... The passwd file has been changed!
[09/24/19]seed@VM:~/.../RaceCondition$
```

# HW1\_평가기준

## ❖ (1) 수행결과 스크린 샷

- Race Condition Attack 실습을 확인하기 위해 아래의 실습 화면을 캡처
  - 1-1) ./resCheck.sh
  - 1-2) ./symp
  - 1-3) /etc/passwd

## ❖ (2) 공격프로그램 동작 분석

- 스크린 샷과 함께 상세한 실습 보고서를 제출
- 수행한 작업과 관찰한 작업을 설명
- 보고서에는 아래의 내용을 포함하여 작성
  - race condition이 발생할 수 있는 원인을 논리적으로 서술
    - race condition이란 무엇이며, vulnerableProgram.c 를 예로들어 서술
  - 제공된 프로그램의 공격 동작 과정과 결과를 논리적으로 분석
- 키워드 : 취약점, Set-UID, Symbolic Link ...

# HW1 - 보너스

## ❖ (3) 취약점 보완

- 아래의 내용을 포함하기를 권장하며, 자세하게 서술 바람
- 제공된 vulnerableProgram.c가 가지는 취약점을 찾아 보완할 수 있는지
  - 프로그램 본래의 기능을 변경해서는 안됨
    - 공격(실습 목표(p.15))을 방어할 수 있는 방법을 서술하고
    - 서술한 방법으로 프로그램을 보완하여 첨부
- 자신의 관심 분야(혹은 언어)에서 Race Condition 에 대한 대책이 있는지

# 제출

## ❖ 9월 30일 (월) ~ 10월 14일 (월)

- 실습 및 과제 내용을 보고서로 제출
- 수업시간에 제출 or 미디어센터 505호로 방문하여 제출
- 부재시 504호 제출
- 표지
  - 과제명, 과목명, 학번/성명, 제출일 반드시 포함

## ❖ 문의

- 이름 : 조재희
- 연락 : [jehee1204@gmail.com](mailto:jehee1204@gmail.com)
  - 메일 제목 앞에 [RaceCondition]이라고 붙여서 보내주시면 감사하겠습니다

- 위치 : 

505호 출입문	
	조재희



# Thank You !