

Cuckoo Sandbox Settings Manual

20153240

한채연

1. 기본 패키지 / C 라이브러리 설치

- **sudo apt-get install -y python-pip python-dev libssl-dev libjpeg-dev zlib1g-dev tcpdump apparmor-utils libffi-dev swig python-setuptools**
- **sudo pip install pyopenssl**

1. 기본 패키지 / C 라이브러리 설치

python-pip	파이썬 라이브러리를 쉽게 설치하도록 도와주는 도구
python-dev	파이썬 헤더(python.h)를 제공하여 고성능을 위한 파이썬 확장을 위해 설치, 다양한 파이썬 라이브러리들이 퍼포먼스적인 측면을 위해 처리 기능을 C 언어로 구성된다.
libssl-dev	cryptography 파이썬 라이브러리를 설치하기 위해 설치하는 패키지로, 다양한 암호 기능을 제공
libjpeg-dev	pillow 파이썬 라이브러리를 설치하기 위해 설치하는 패키지로, jpeg 이미지 파일을 위해 사용되는 C 라이브러리
zlib1g-dev	pillow파이썬 라이브러리를 설치하기 위해 설치하는 패키지로, gzip과 PKZIP를 지원하기 위해 제작되었지만, PNG 이미지 파일을 위해 사용되는 C 라이브러리
tcpdump	패킷을 캡처를 위한 프로그램
apparmor-utils	Application Armor의 약자로 프로그램의 네트워크 접근, 파일 읽기, 쓰기 그리고 실행 같은 능력을 제어하여 접근 통제할 수 있는 리눅스 커널 보안 모듈로 이를 제어하기 위한 유틸리티

1. 기본 패키지 / C 라이브러리 설치

- **sudo aa-disable /usr/sbin/tcpdump**
- **sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump**
 - 쿠쿠 코어가 네트워크 패킷을 수집할 수 있게끔 하는 과정.
 - Tcpdump를 보호하는 apparmor(aa)를 disable하고,
 - Setcap 명령어로 일반 사용자가 루트 권한 없이 tcpdump를 사용할 수 있게끔 함.
 - Setcap 명령어를 사용할 수 없으면 아래와 같이 libcap2-bin 패키지 설치하기
- **sudo apt-get install libcap2-bin**

1. 기본 패키지 / C 라이브러리 설치

- 샌드박스로 사용될 virtualbox 설치

- echo deb <http://download.virtualbox.org/virtualbox/debian>
xenial contrib | sudo tee -a
/etc/apt/sources.list.d/virtualbox.list
- "deb <http://download.virtualbox.org/virtualbox/debian> xenial
contrib"라는 명령어를 터미널에 출력함과 동시에
"/etc/apt/sources.list.d/virtualbox.list" 경로의 파일에 write
- Tee : 리눅스 화면과 파일에 동시에 출력하는 명령어

1. 기본 패키지 / C 라이브러리 설치

- 샌드박스로 사용될 virtualbox 설치

- `wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc`
`-O- | sudo apt-key add -`
- "https://www.virtualbox.org/download/oracle_vbox_2016.asc" 경로의 파일을 다운로드 후 이 파일 안의 키값을 apt의 키 리스트에 추가
- `sudo apt-get update`
- `/etc/apt/sources.list` 를 읽어 apt를 업데이트 해줌
- `sudo apt-get install -y virtualbox-5.1`

2. 쿠쿠 코어 설치하기

- **sudo pip install cuckoo**

- pip가 python3과 연동될 경우 pip2 명령어를 이용하여 설치하기

```
VersionConflict: (setuptools 20.7.0 (/usr/lib/python2.7/dist-packages), Requirement.parse('setuptools>=27.3'))
```

- 위와 같은 에러가 날 경우

- <https://cuckoo.sh/docs/installation/host/requirements.html> 에서
setuptools 최신 버전 설치

3. 샌드박스 구성

- 가상머신 다운로드 및 가져오기

Download virtual machines

Test Microsoft Edge and versions of IE8 through IE11 using free virtual machines you download and manage locally.

Select a download

Virtual machine

IE8 on Win7 (x86)

Select platform

VirtualBox

DOWNLOAD .ZIP >

➤ <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

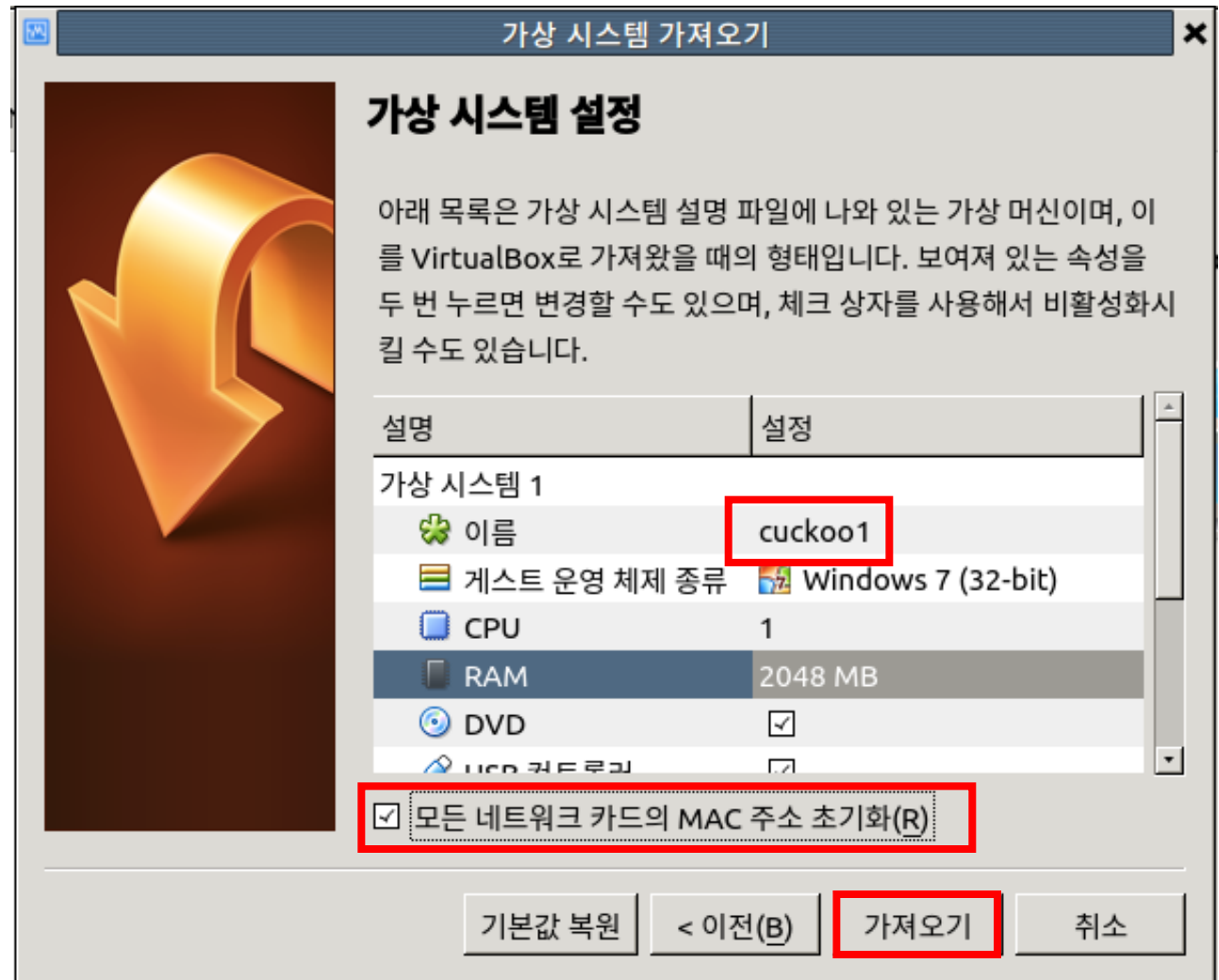
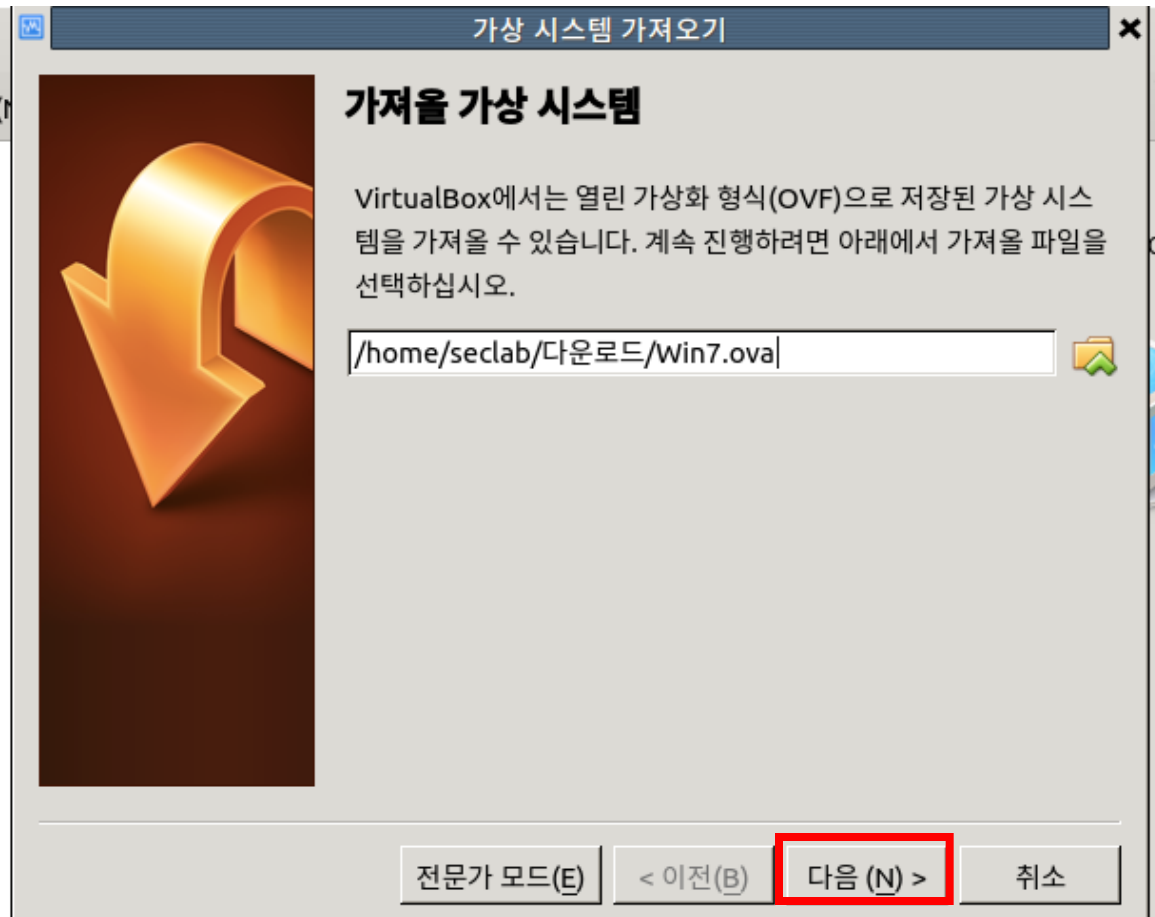
➤ 윈도우 7 32비트 운영체제 선택

➤ 가상머신은 virtualbox로

- unzip
IE8.Win7.For.Windows.VirtualBox.zip

3. 샌드박스 구성

- 가상머신 다운로드 및 가져오기



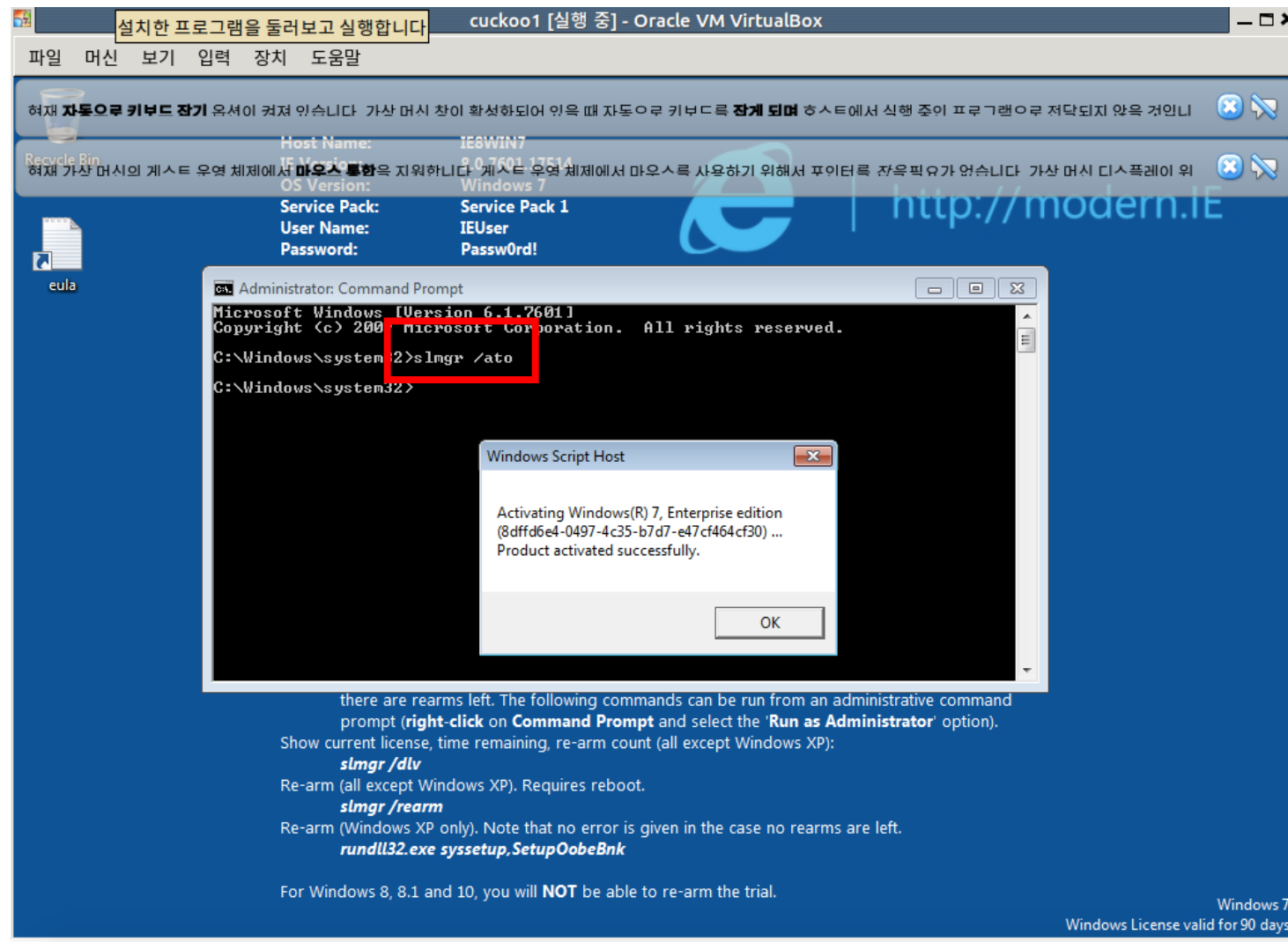
- 필자는 RAM 2GB 할당
- 가상 시스템 이름 기억하고 있어야함. -> 추후에 쿠쿠 설정에 필요

3. 샌드박스 구성

- 가상머신 다운로드 및 가져오기

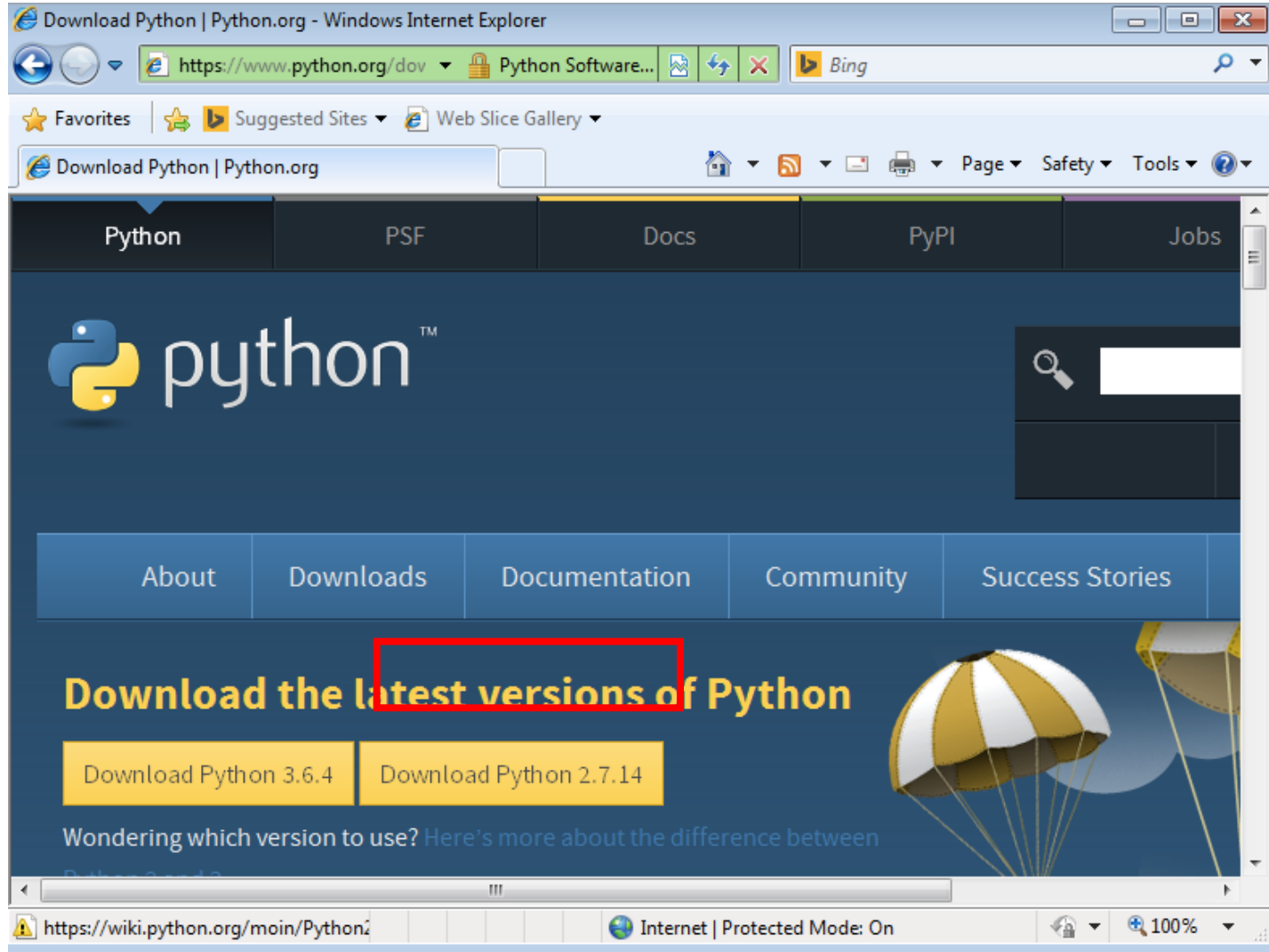
➤ 시작 > Command Prompt 아이콘에서 우클릭한 후 Run as administrator를 선택하여 관리자모드로 윈도우 프롬프트에 접근

• `slmgr /ato`



3. 샌드박스 구성 - 파이썬 다운로드 및 설치

- Python2.7 설치 -> Windows x86 MSI installer 선택
- <https://www.python.org>



3. 샌드박스 구성

- 파이썬 다운로드 및 설치

➤ Pillow 라이브러리 설치

➤ 악성코드 분석을 진행할

때 윈도우 운영체제의 화

면의 스크린샷을 찍어 상

태를 파악하기 위해

- **pip install pillow**

```
C:\Windows\system32>cd c:\Python27\Scripts
```

```
c:\Python27\Scripts>pip install pillow
Collecting pillow
  Downloading Pillow-5.0.0-cp27-cp27m-win32.whl (1.3MB)
    100% |#####| 1.3MB 311kB/s
Installing collected packages: pillow
Successfully installed pillow-5.0.0
```

3. 샌드박스 구성

- 네트워크 구성 및 아이피 고정

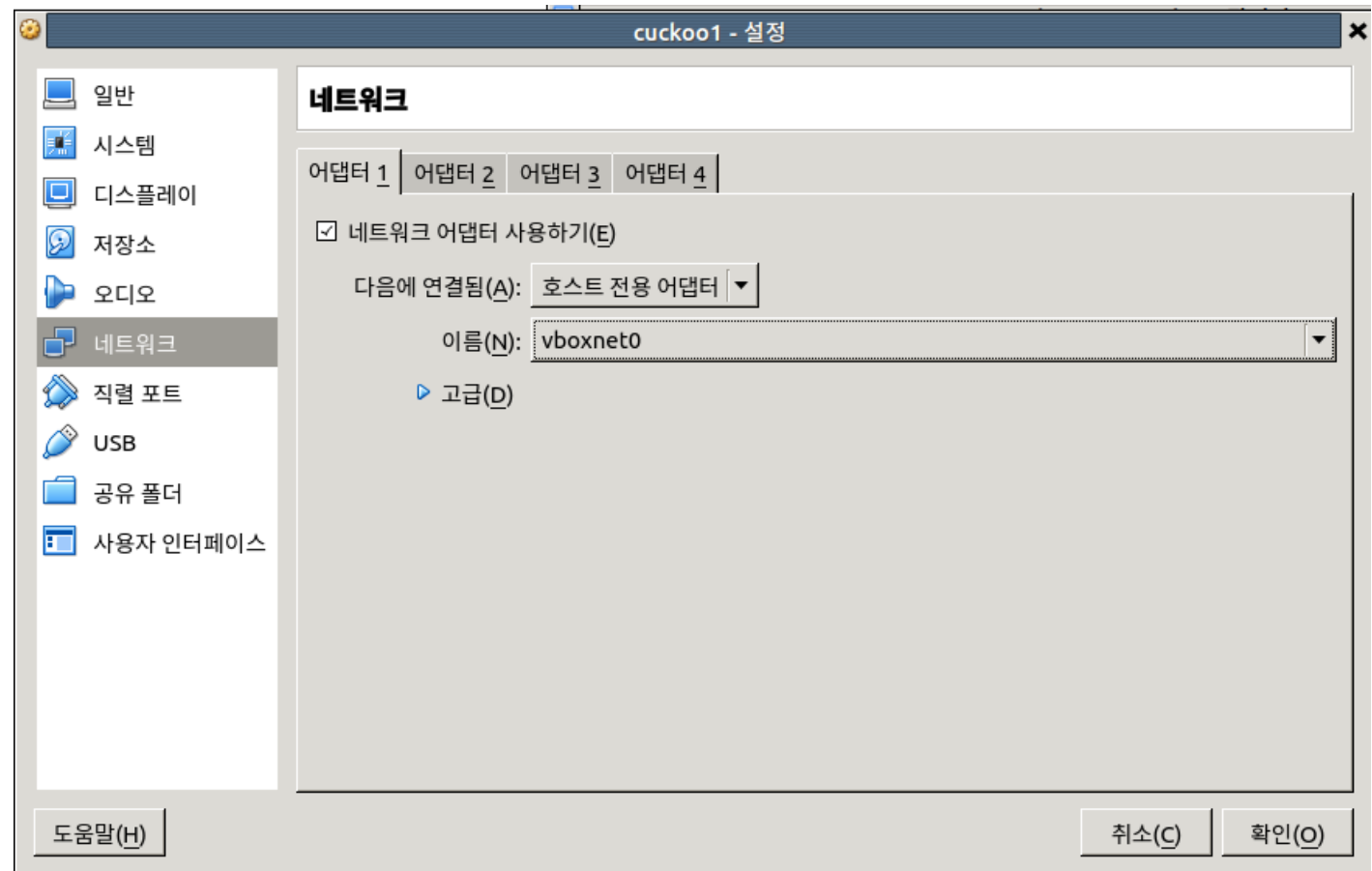
- **vboxmanage hostonlyif create**
- **vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1**

```
seclab@seclab-S2600IP:~$ vboxmanage hostonlyif create
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Interface 'vboxnet0' was successfully created
seclab@seclab-S2600IP:~$ vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1
```

3. 샌드박스 구성

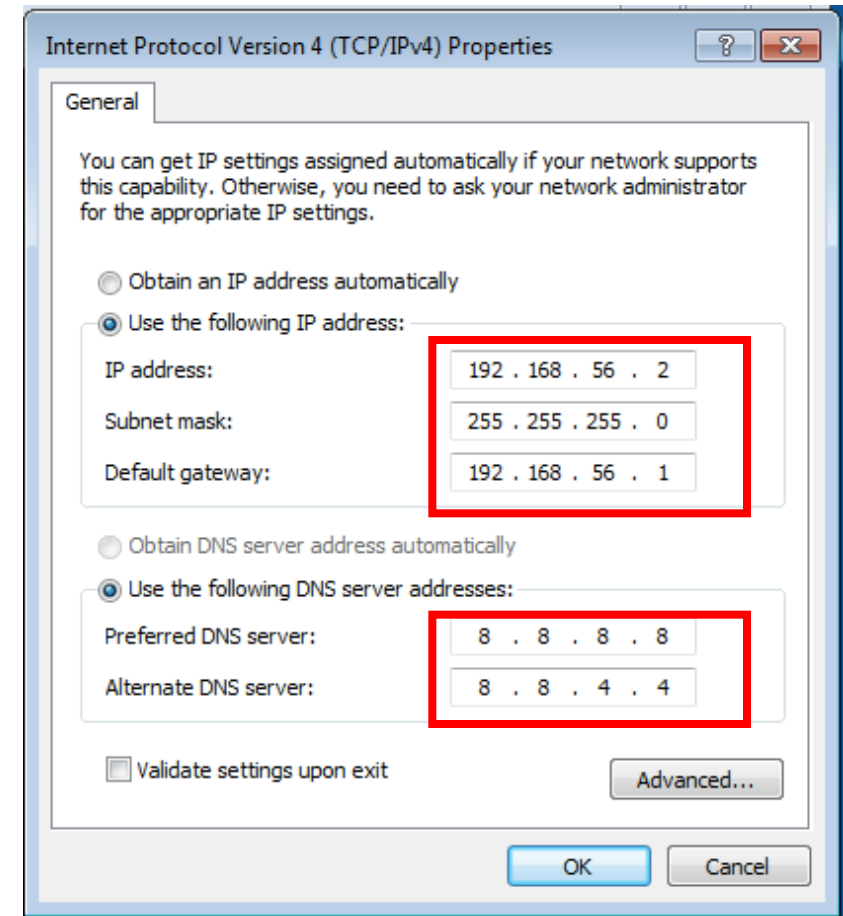
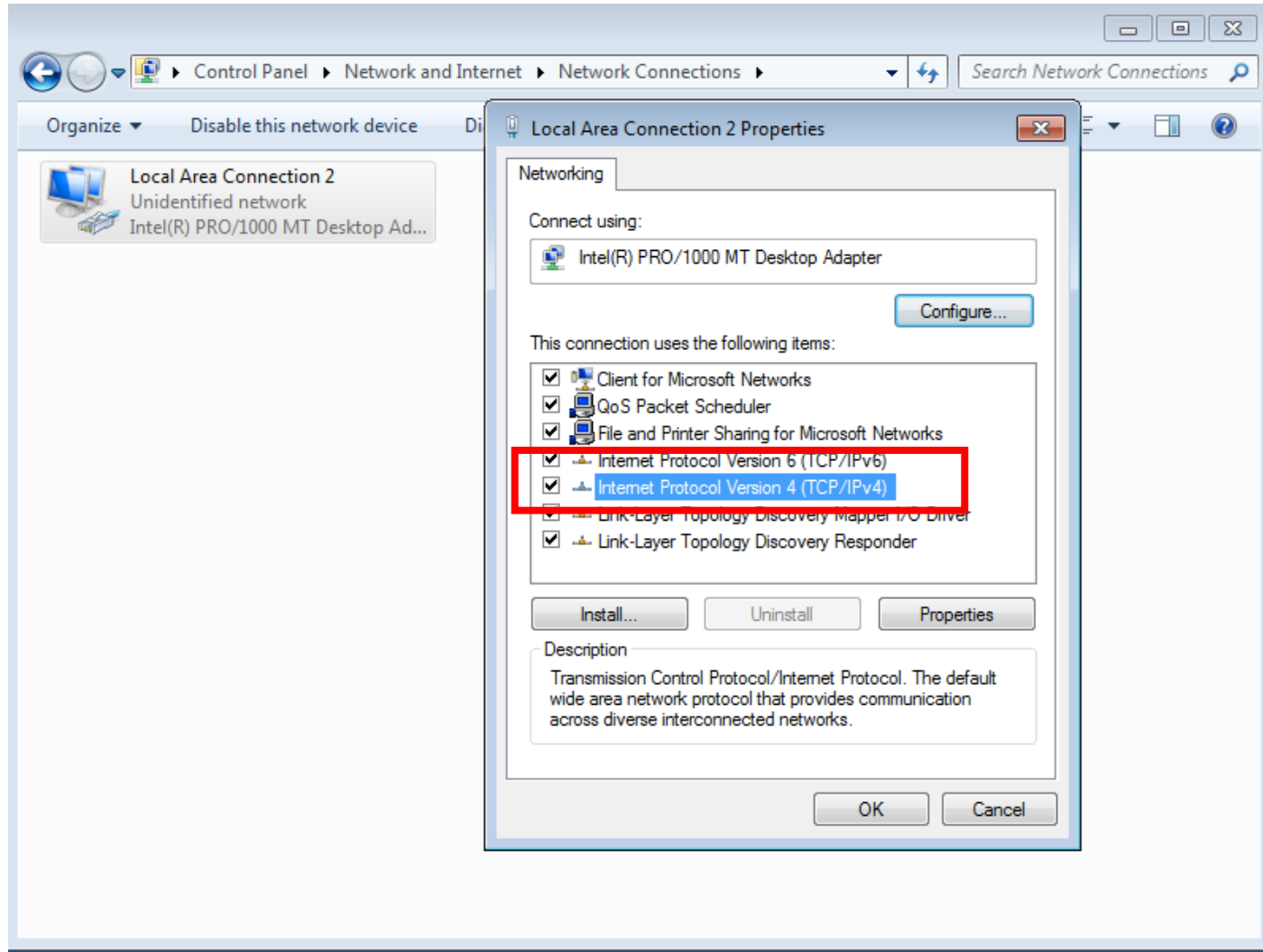
- 네트워크 구성 및 아이피 고정

- 설정 -> 네트워크 -> 호스트 전용 어댑터
vboxnet0 선택



3. 샌드박스 구성

- 네트워크 구성 및 아이피 고정



3. 샌드박스 구성

- 네트워크 구성 및 아이피 고정

```
C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::bdd5:ece4:705f:3fc8%22
    IPv4 Address. . . . . : 10.0.3.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.3.2

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::50e4:18f7:3a7a:fbac%15
    IPv4 Address. . . . . : 192.168.56.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.56.1

Tunnel adapter isatap.{28B6EF9D-D034-4EDE-9FF1-B7816B87F2E0}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

```
C:\Windows\system32>ping www.google.co.kr

Pinging www.google.co.kr [64.233.189.94] with 32 bytes of data:
Reply from 64.233.189.94: bytes=32 time=91ms TTL=127
Reply from 64.233.189.94: bytes=32 time=83ms TTL=127

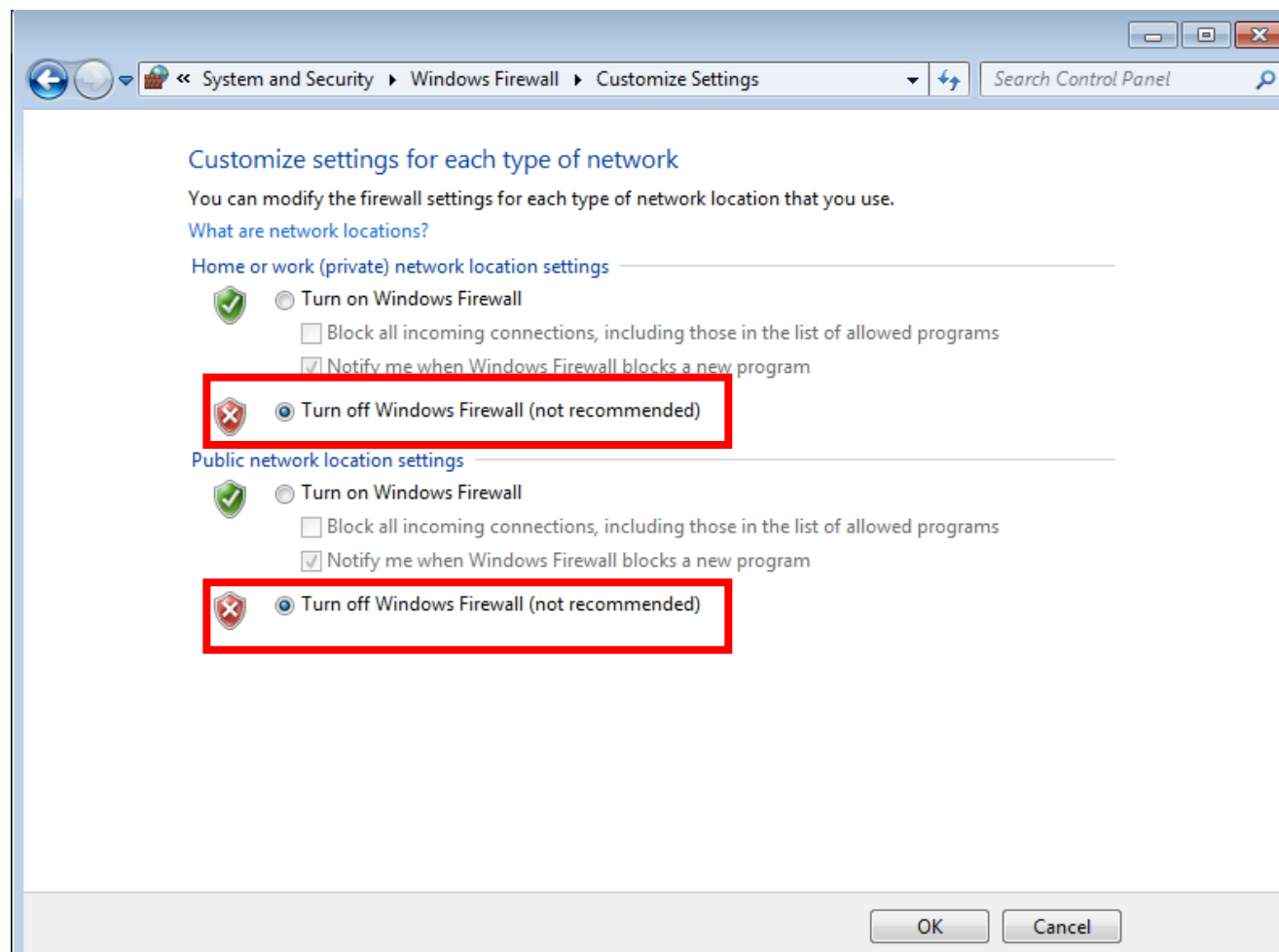
Ping statistics for 64.233.189.94:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 83ms, Maximum = 91ms, Average = 87ms
```

➤ ipconfig, ping으로 네트워크 설정 잘 되었는지 확인

3. 샌드박스 구성

- 방화벽/업데이트 비활성화

- 시작 > Control Panel > System and Security > windows Firewall > Customize settings
- Turn off windows Firewall 선택

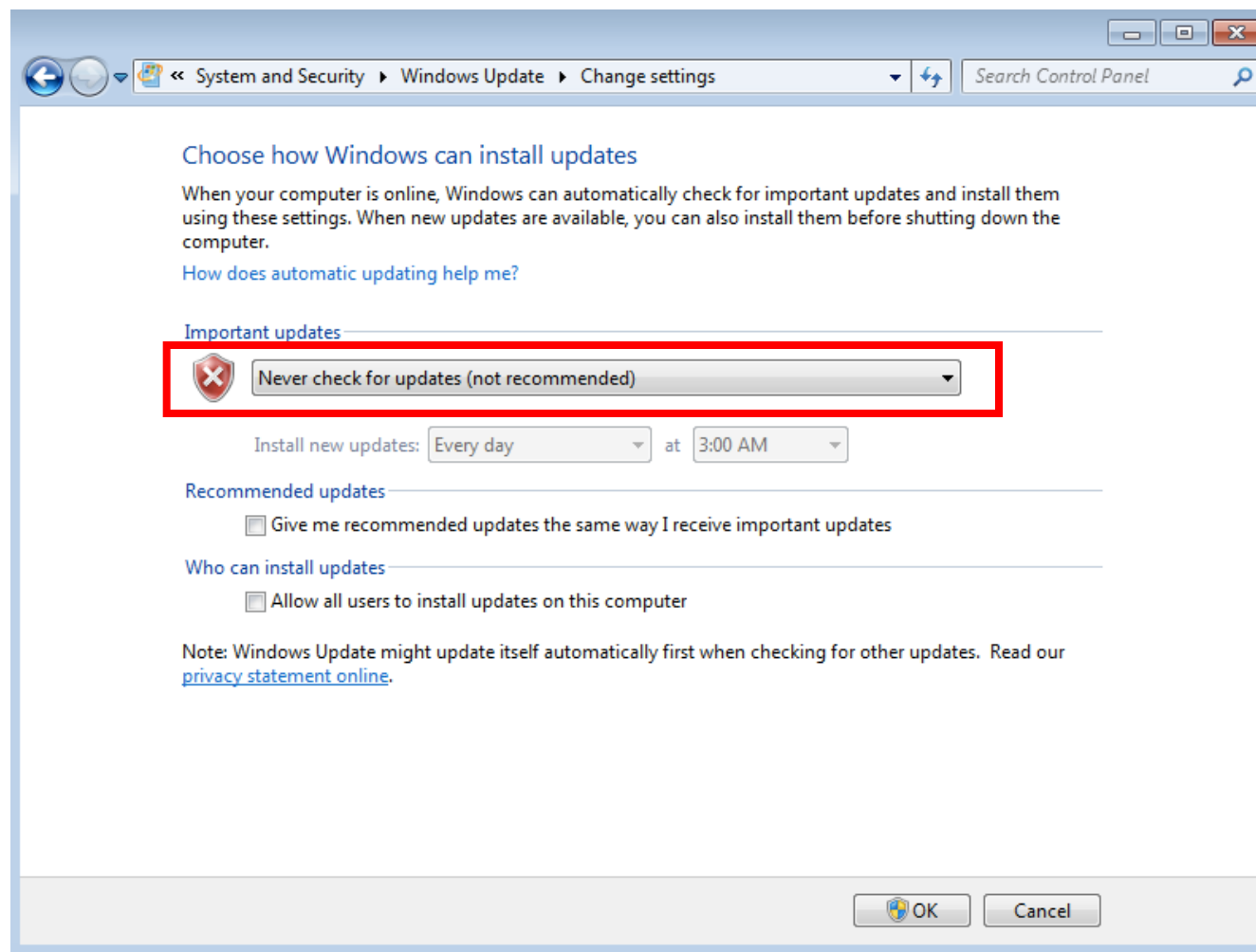


3. 샌드박스 구성

- 방화벽/업데이트 비활성화

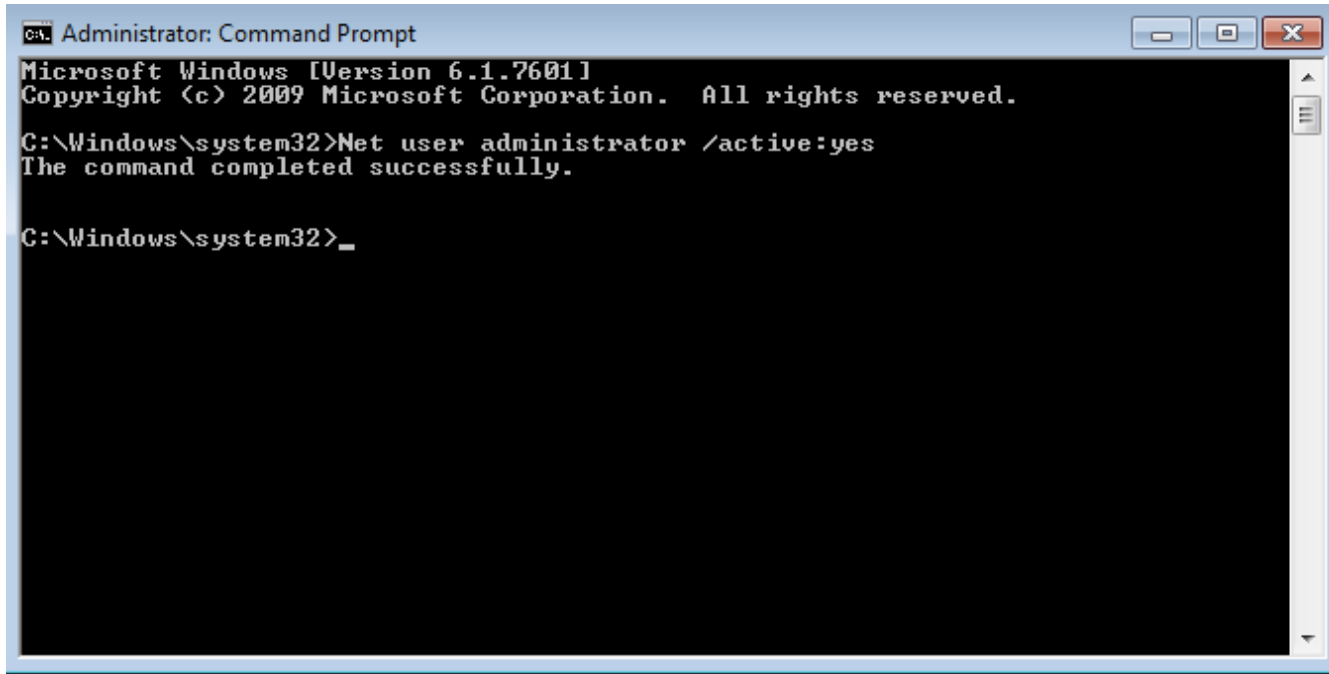
➤ 시작 > Control Panel >
System and Security >
Windows Update > Change
settings

➤ Window update 비활성화



3. 샌드박스 구성

- Administrator 계정 활성화 및 로그인



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>Net user administrator /active:yes
The command completed successfully.

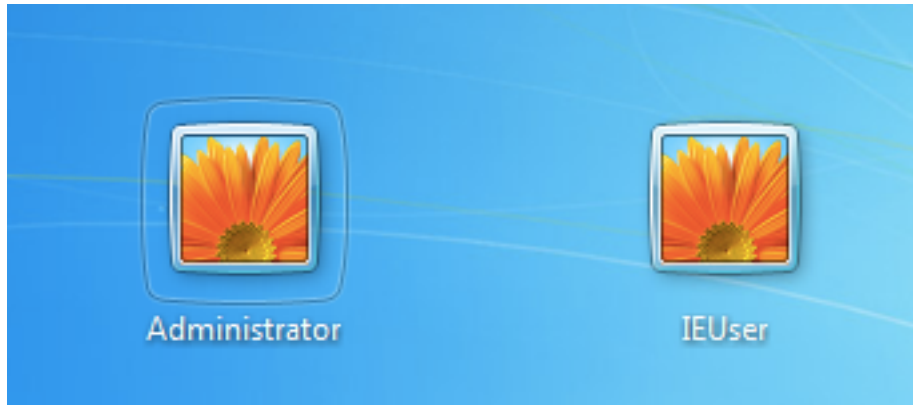
C:\Windows\system32>_
```

- Net user administrator /active:yes

➤ 관리자 계정을 활성화하고 로그인하는 이유? -> 악성 코드가 동작하는데 방해가 없어야 하기 때문

3. 샌드박스 구성

- Administrator 계정 활성화 및 로그인



- Log off 후 Administrator 계정으로 다시 로그인
- 만약 비밀번호가 걸려있다면? -> 바탕화면의 비밀번호를 확인하기

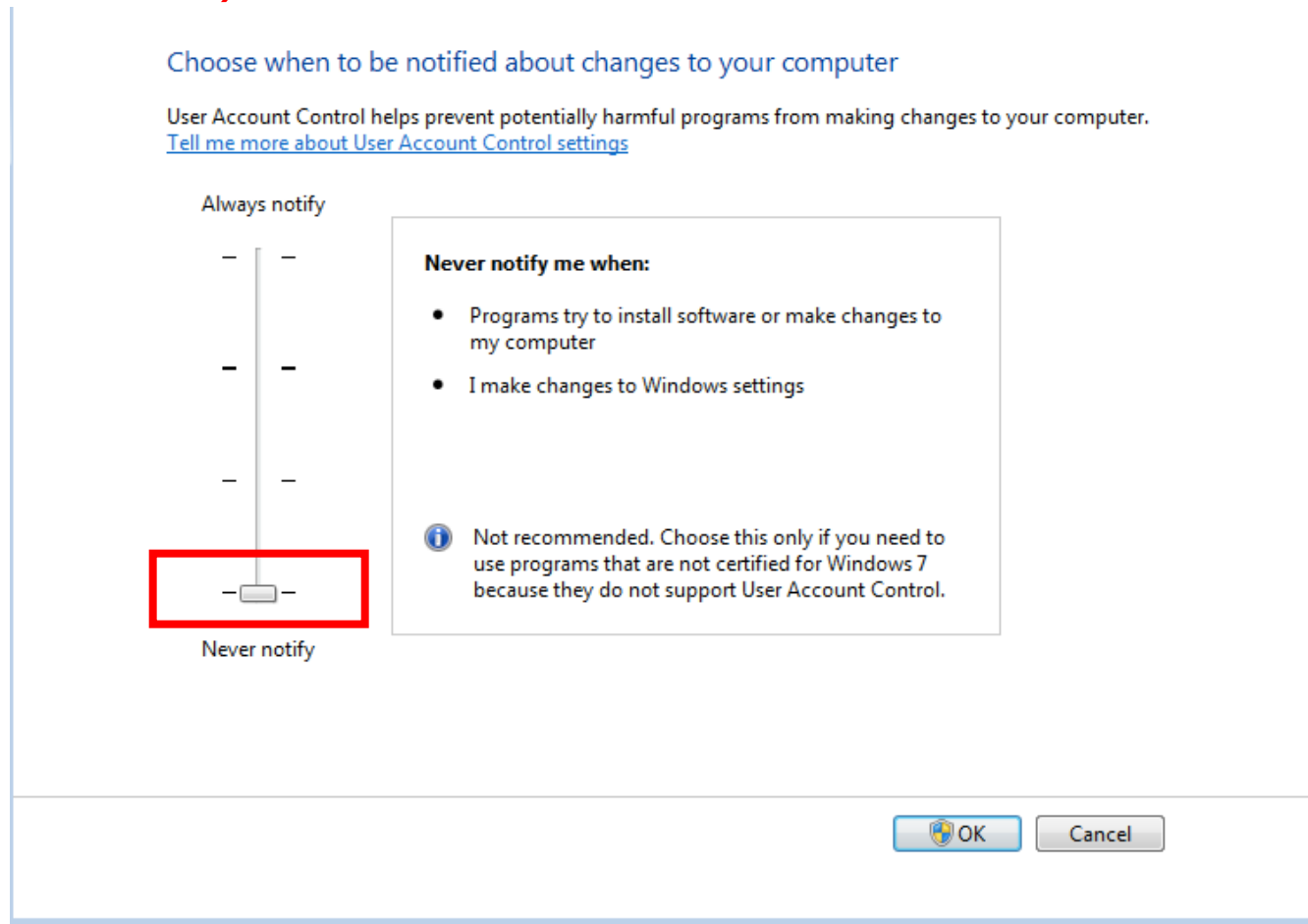
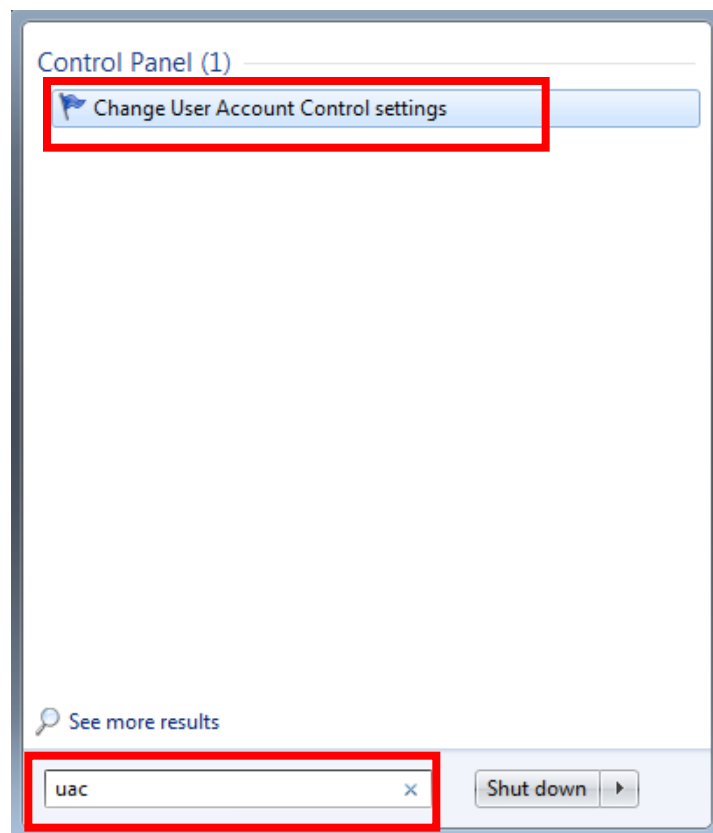
Password:

Passw0rd!

샌드박스 구성

- UAC 비활성화

➤ UAC(User Account Control) : 사용자 계정을 제어하는데 사용



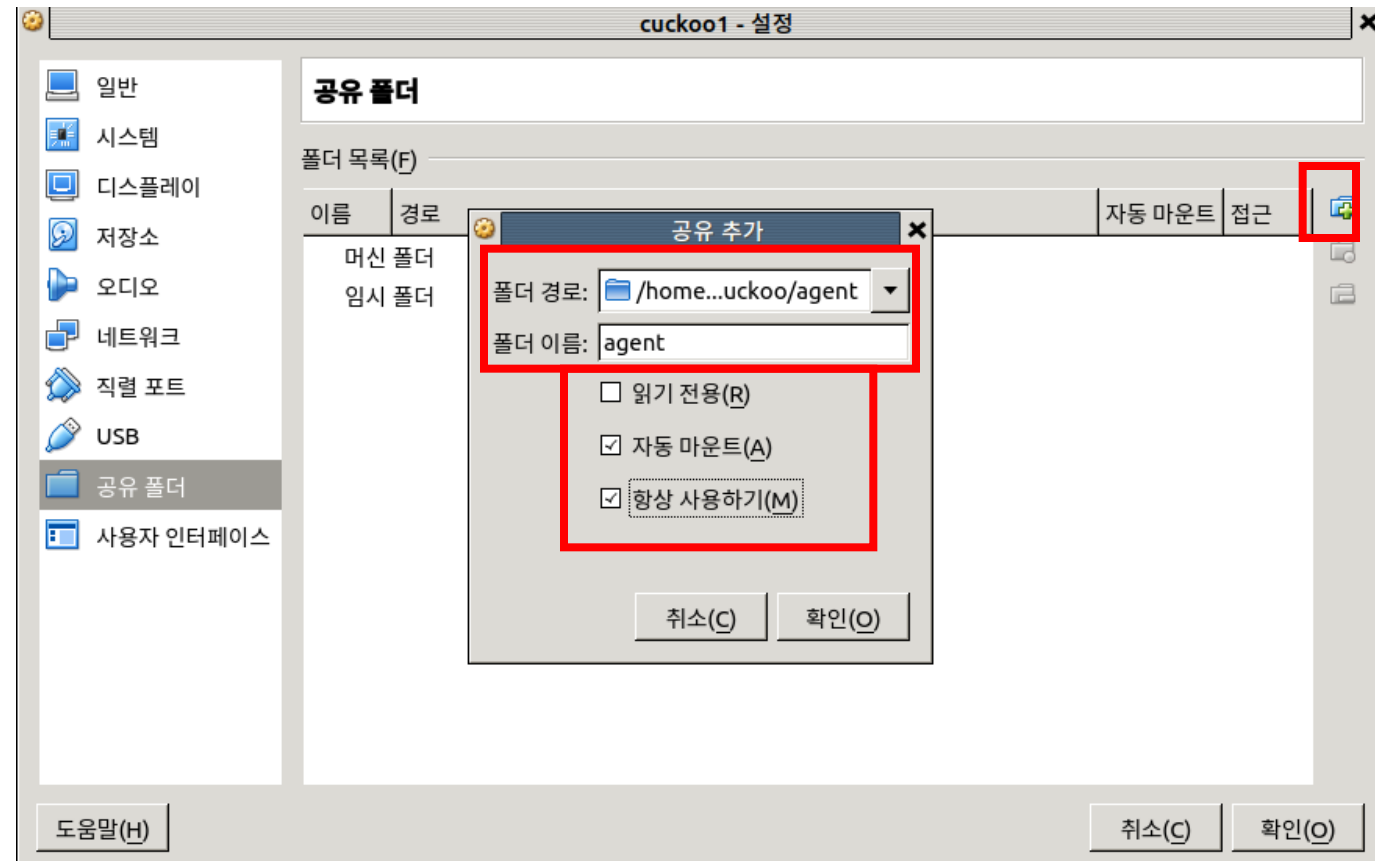
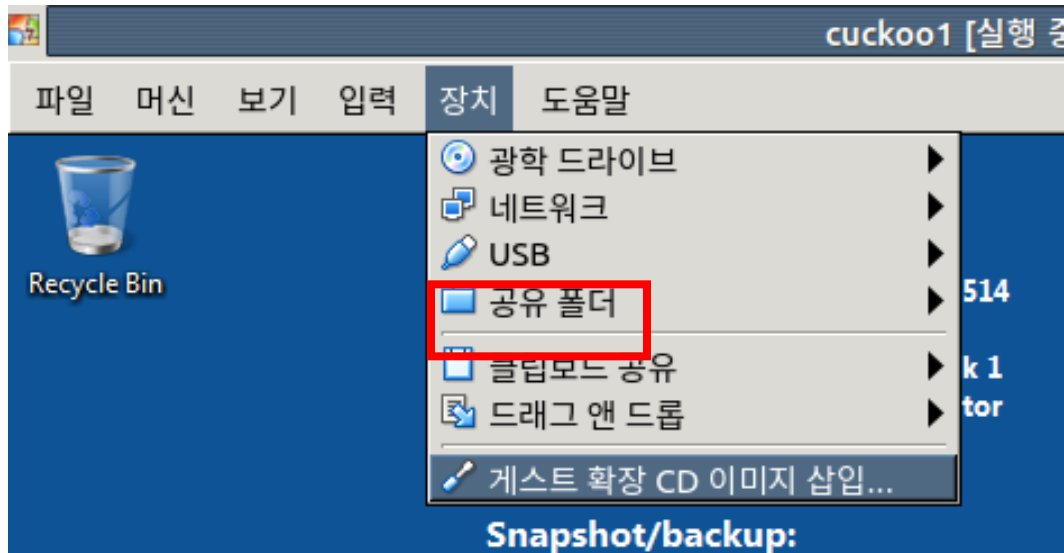
샌드박스 구성

- agent.py 실행과 스냅샷 구성

➤장치 > 공유 폴더

➤폴더 경로 :

/home/" <계정> "/.cuckoo/agent

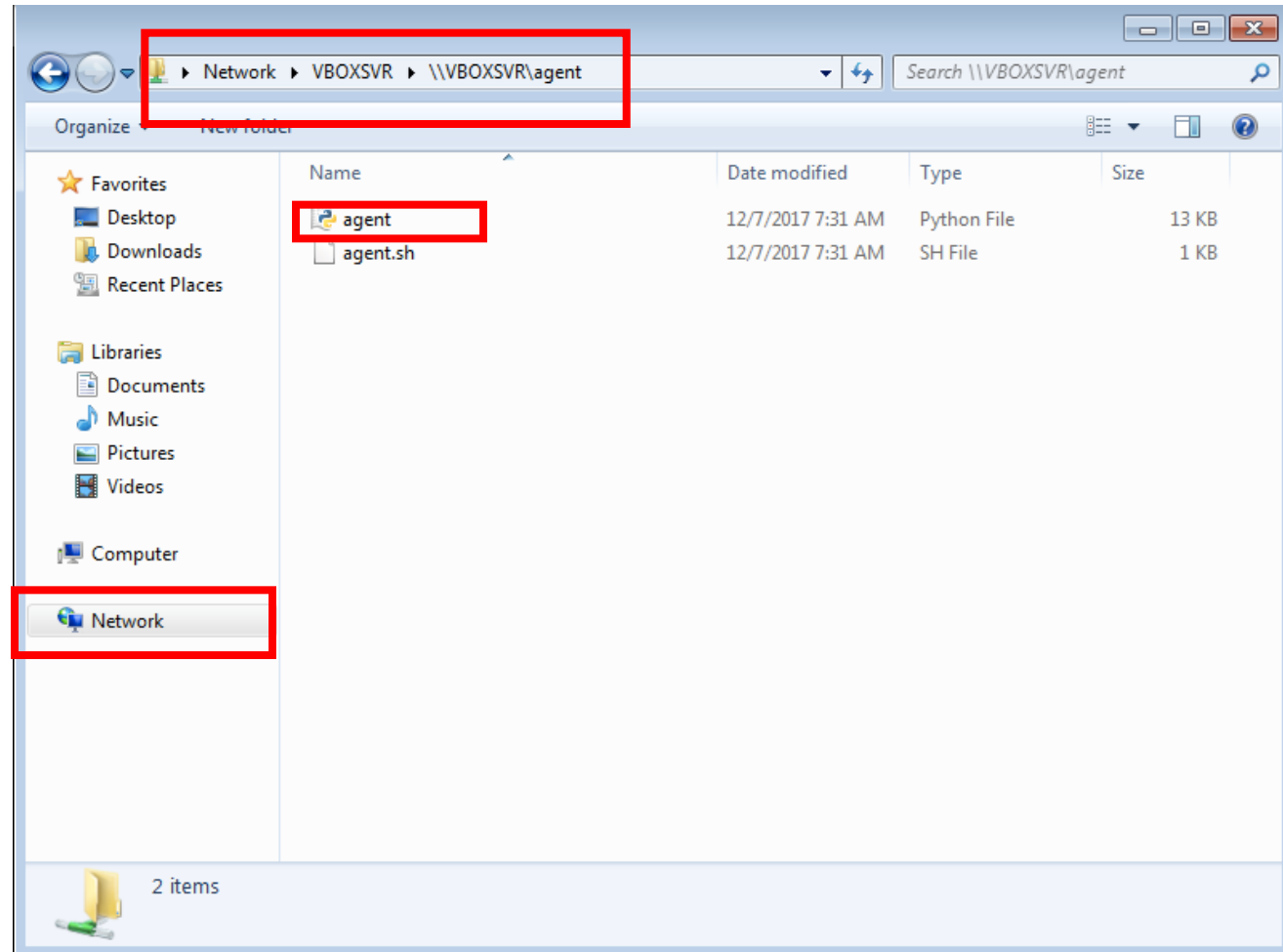


샌드박스 구성

- agent.py 실행과 스냅샷 구성

➤ 시작 > Computer >
Network > 공유 폴더 >
agent.py 파일을 바탕화면
에 복사하기

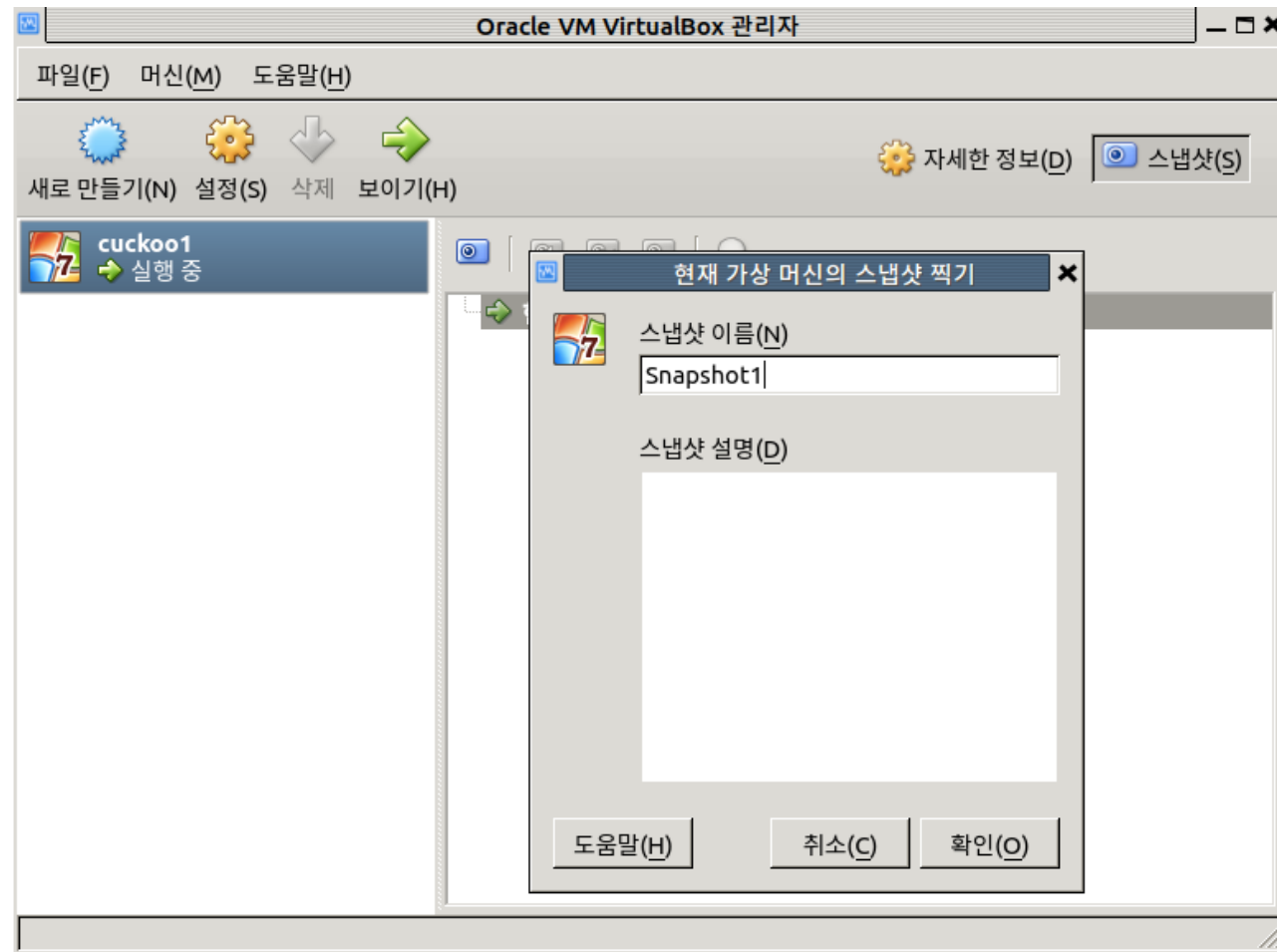
➤ **Agent.py 실행하기!!!!**



샌드박스 구성

- agent.py 실행과 스냅샷 구성

➤ 스냅샷 이름 : Snapshot1(추후 설정에 필요)



참고

- <http://www.hakawati.co.kr/420>
- <http://docs.cuckoosandbox.org/en/latest/>