

칼리리눅스

양유진
2018. 12. 21

CONTENTS

I 칼리리눅스란?

II 실습 개요

III 실습

IV 방어대책

I

칼리리눅스란?

- 1 칼리리눅스란?
- 2 환경

칼리리눅스란?

- Offensive Security에서 만든 모의 침투 테스트용 운영체제
- 데비안 기반 기본 프로그램
- 오픈 소스 툴을 깔아 제공하는 OS

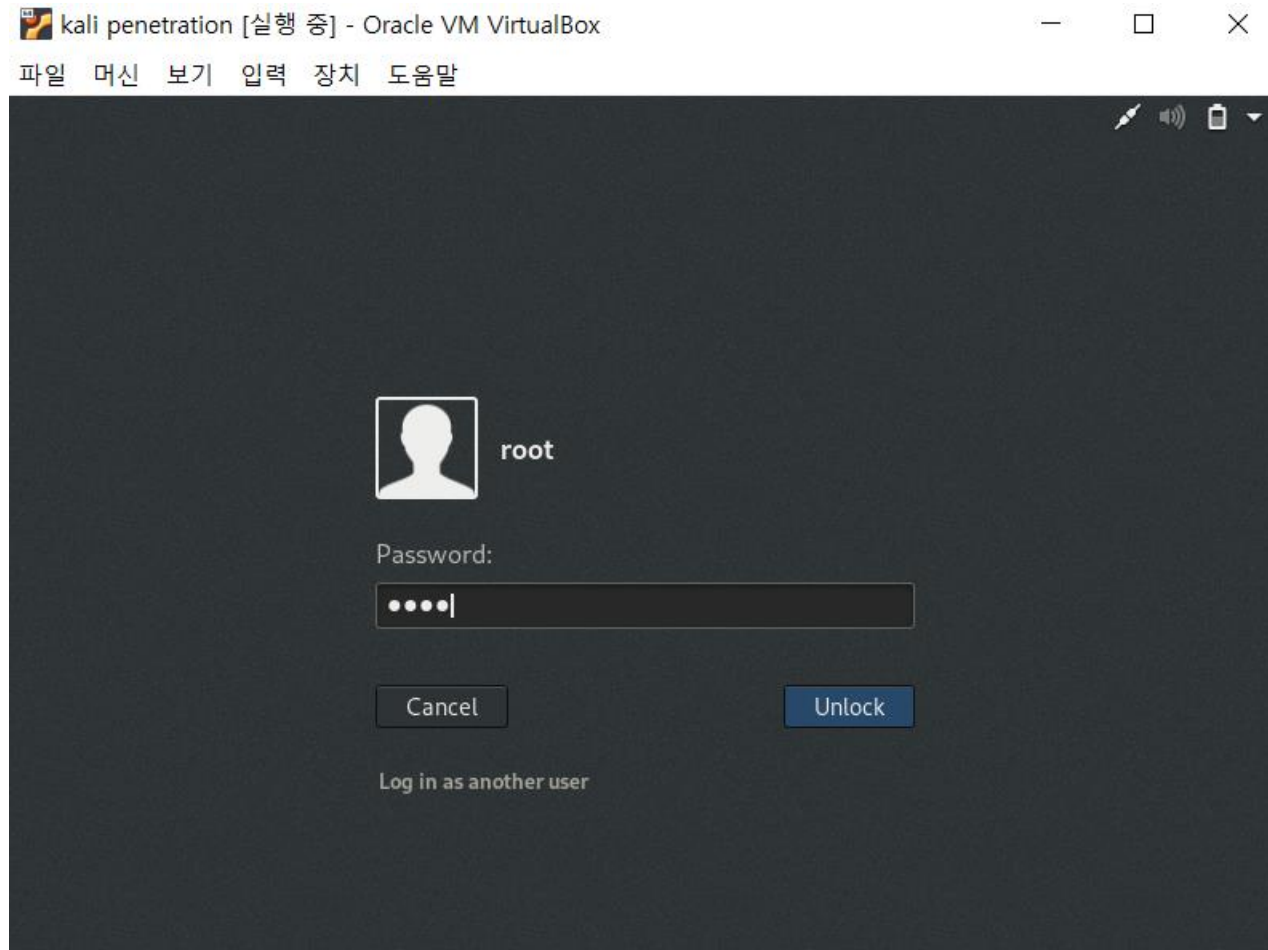
Oracle VM VirtualBox

- 오라클에서 제공하는 가상화 소프트웨어
- 리눅스, macOS, 윈도우 등의 운영 체제를 가상화하여 제공

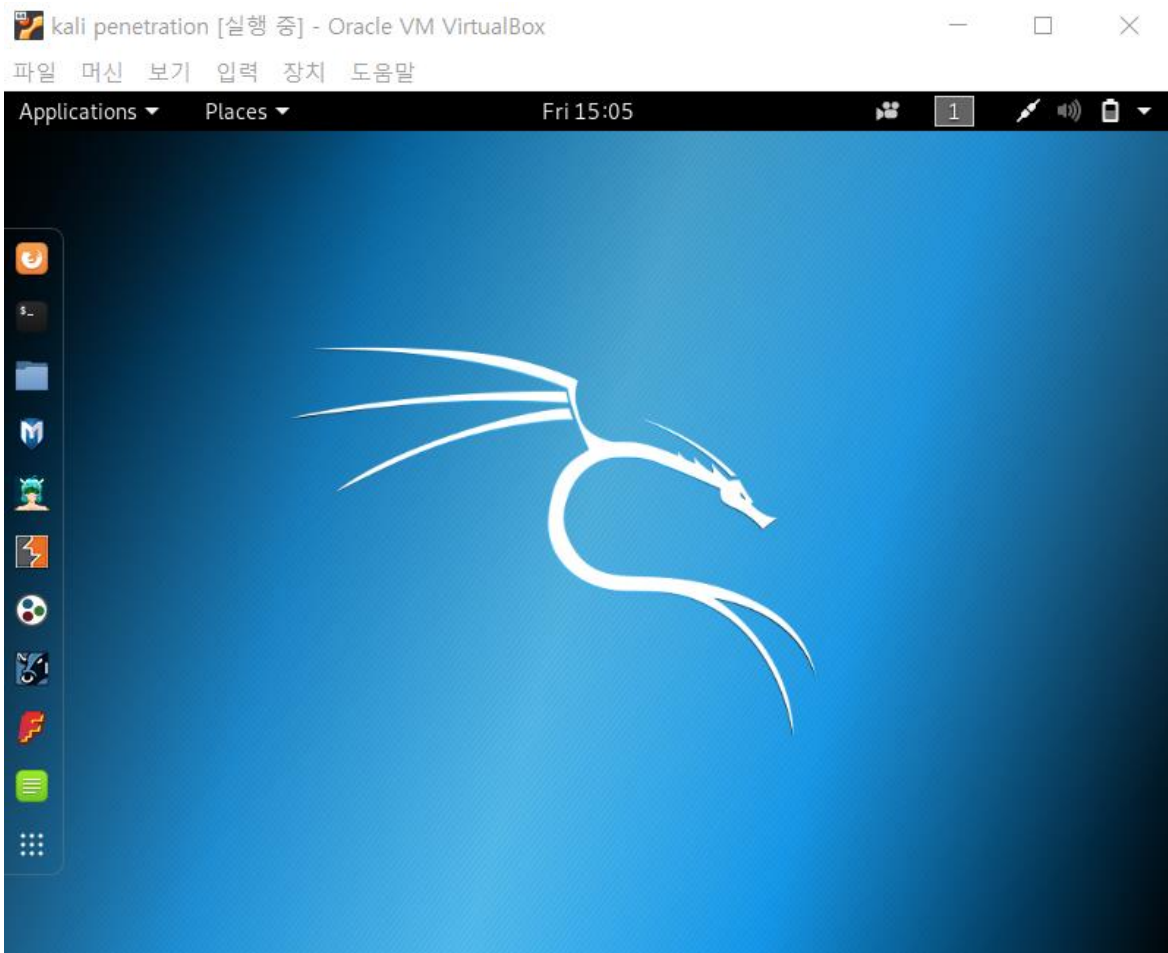
환경



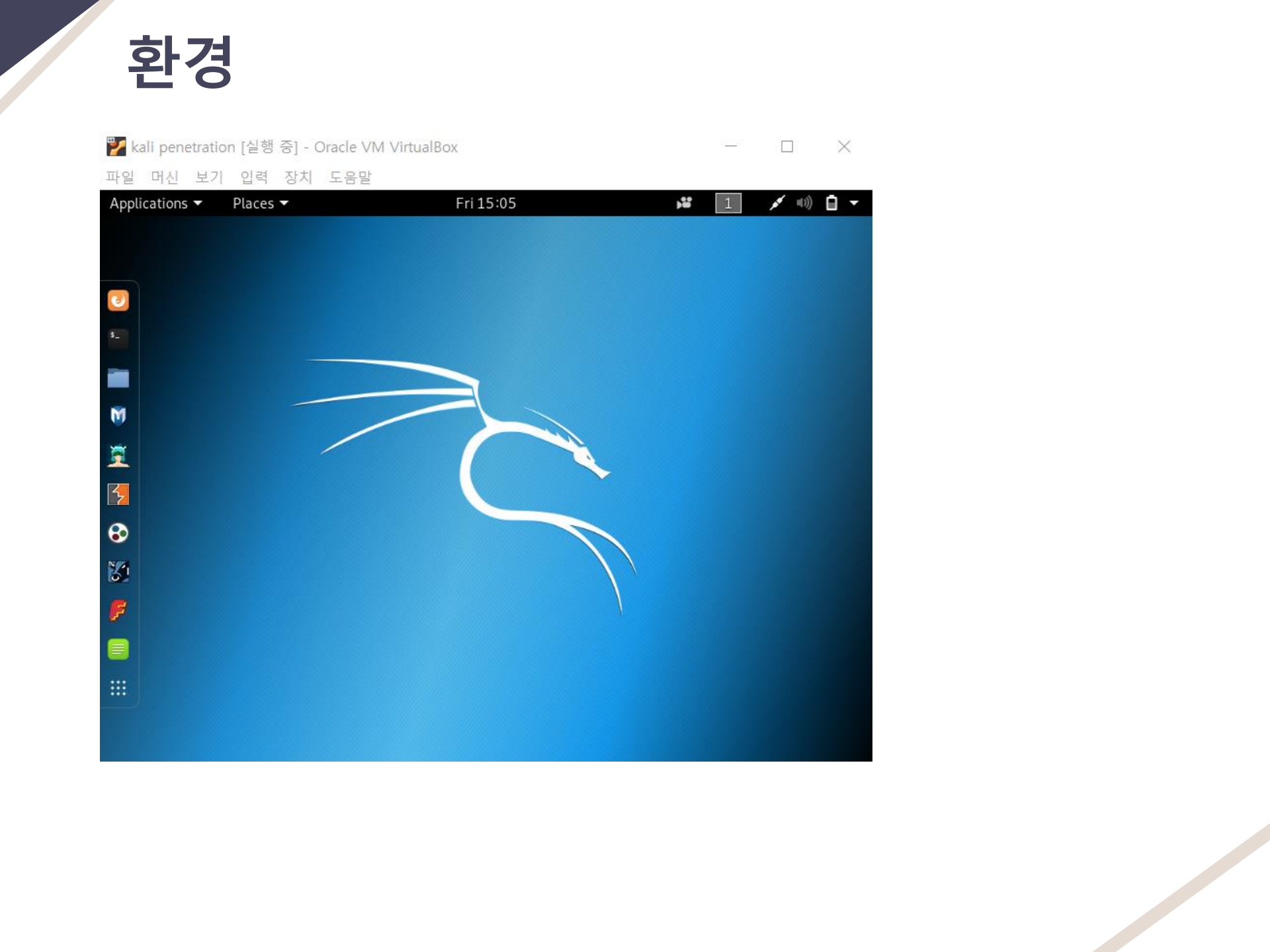
환경



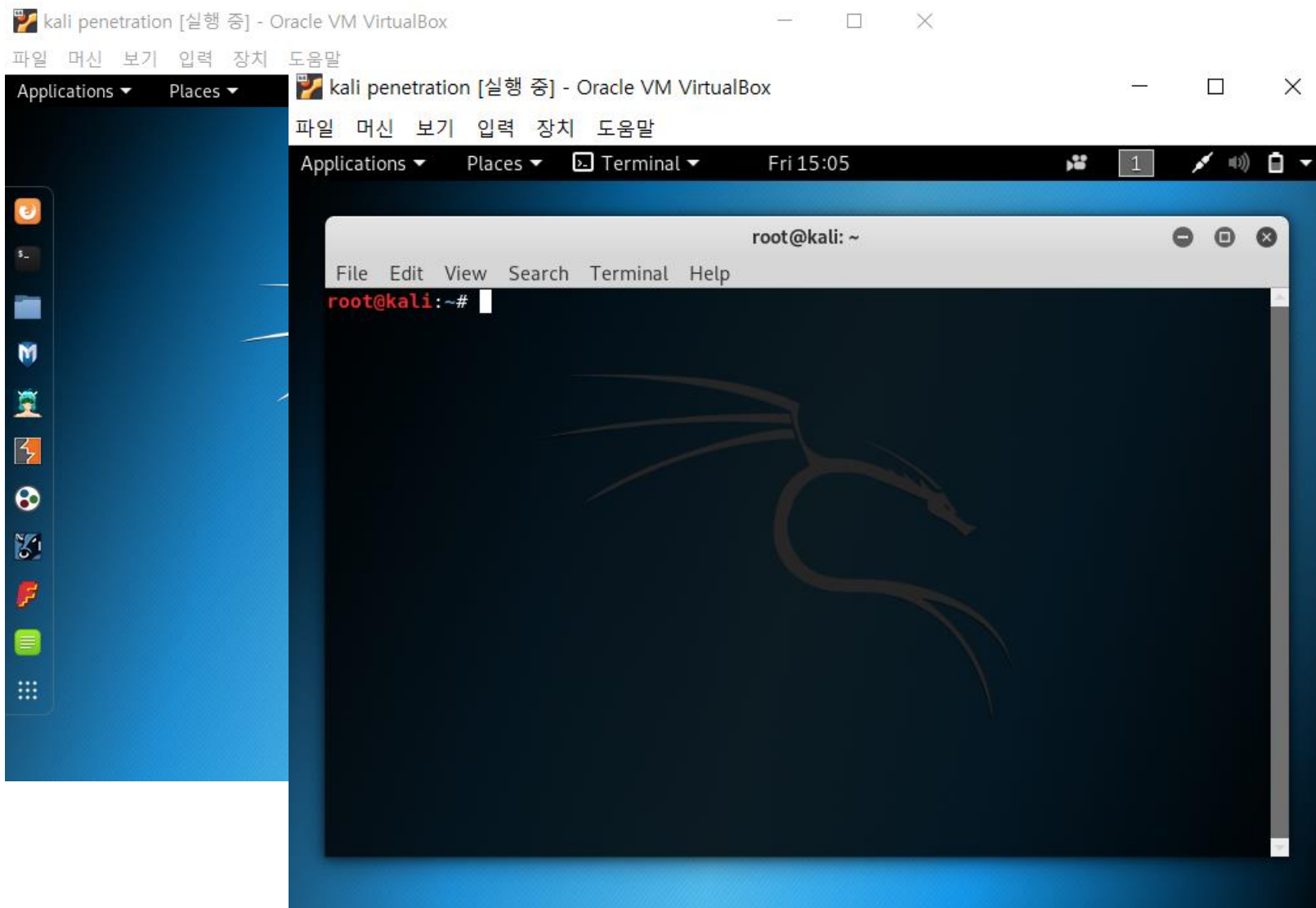
환경



The image shows a screenshot of a Kali Linux virtual machine environment. The window is titled "kali penetration [실행 중] - Oracle VM VirtualBox". The desktop features a blue background with a large white Kali Linux dragon logo. On the left side, there is a vertical dock containing several application icons. The top of the window has a black bar with "Applications" and "Places" menus, a clock displaying "Fri 15:05", and system status icons including a network icon, a volume icon, and a battery icon.



환경



II

실습 개요

- 1 실습 환경
- 2 실습 내용

실습 환경

가상 머신 : VritualBox 6.0.0 (Oracle)

운영체제 : Ubuntu (64-bit)

공격자 : kali penetration IP(192.168.0.120)

희생자 : Windows 10 IP(192.168.0.2)

텔넷 서버 : kali system IP(192.168.100)

네트워크 환경 : 핫스팟 연결

실습 내용

공격 내용

가상 머신에 설치되어 있는 arpspoof 이용



희생자의 arp cache 변조



희생자의 접속(텔넷으로 칼리리눅스에) 도청



Root 계정 정보 탈취

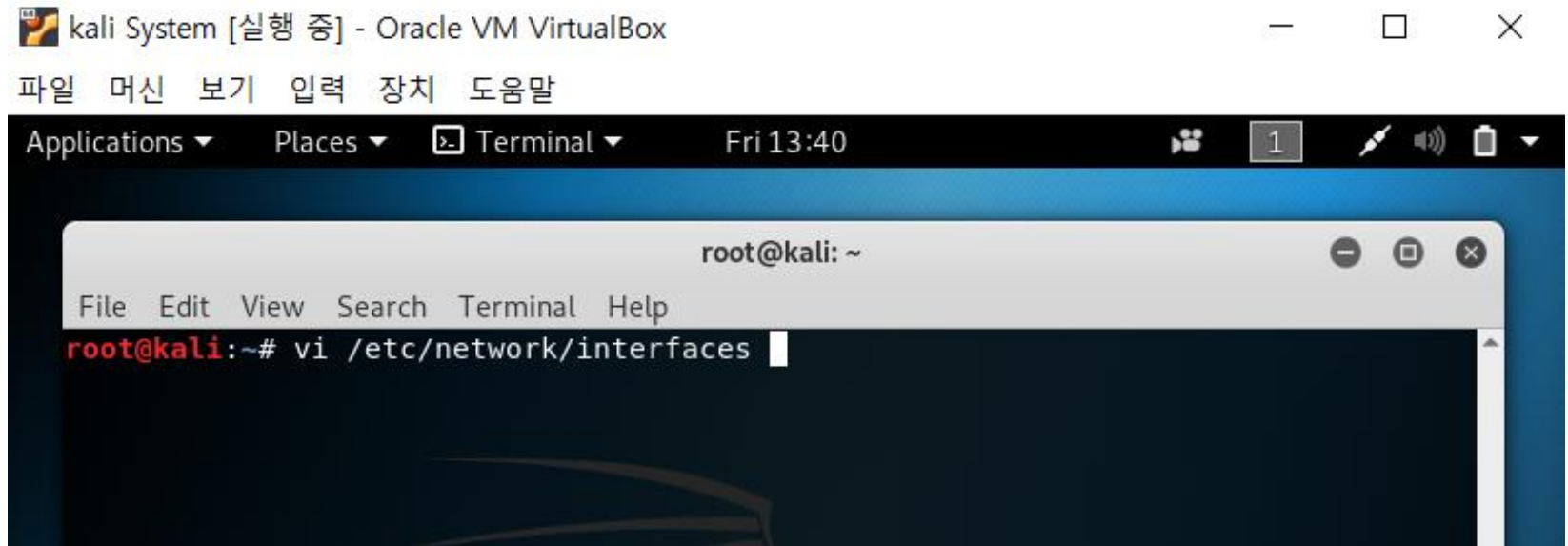
➡ ARP 스푸핑(Spoofing) 방어 대책

III

실습

- 1 실습 전 설정
- 2 텔넷 서버 구축
- 3 ARP 스푸핑(Spoofing)

실습 전 설정 - 네트워크 설정



/etc/network/interfaces를 vi 환경으로 열기

실습 전 설정 - 네트워크 설정

[illegible]

ESC + “:wq” 입력 - 저장 및 vi 환경 나오기

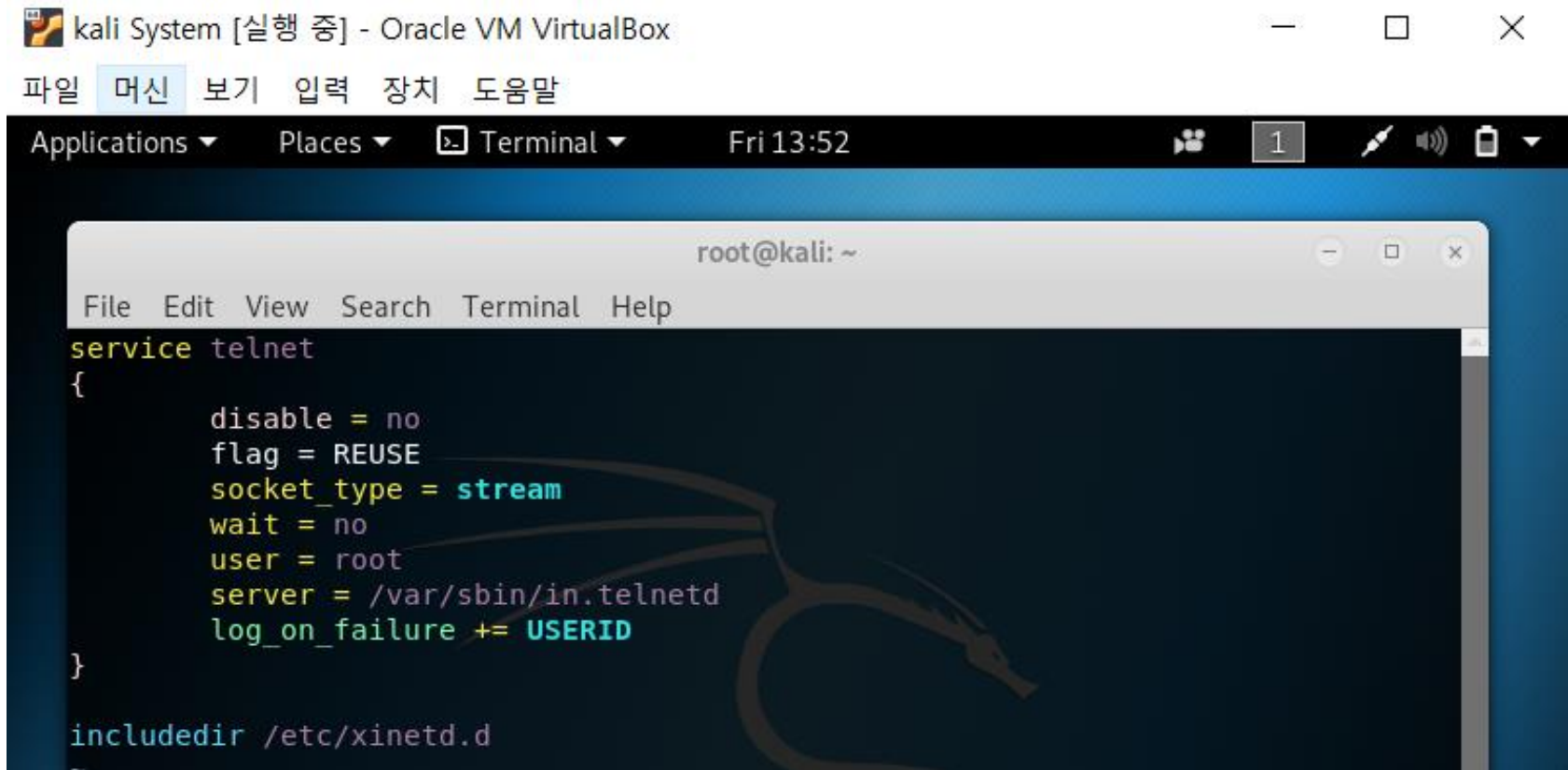
“# service networking restart” – network 데몬 재시작

텔넷 서버 구축 - (1)

apt-get install telnetd - 텔넷 패키지 설치

apt-get install xinetd - 슈퍼 데몬(데몬 관리하는 역할) 설치

vi /etc/xinetd.conf - vi 편집기로 xinetd 설정 파일 열기



The screenshot shows a Kali Linux system running in Oracle VM VirtualBox. The terminal window is titled 'root@kali: ~' and displays the configuration for the telnet service in the xinetd.conf file. The configuration includes settings for disabling the service, reusing flags, using a stream socket, and specifying the server path and log file.

```
root@kali: ~  
File Edit View Search Terminal Help  
service telnet  
{  
    disable = no  
    flag = REUSE  
    socket_type = stream  
    wait = no  
    user = root  
    server = /var/sbin/in.telnetd  
    log_on_failure += USERID  
}  
  
includedir /etc/xinetd.d
```

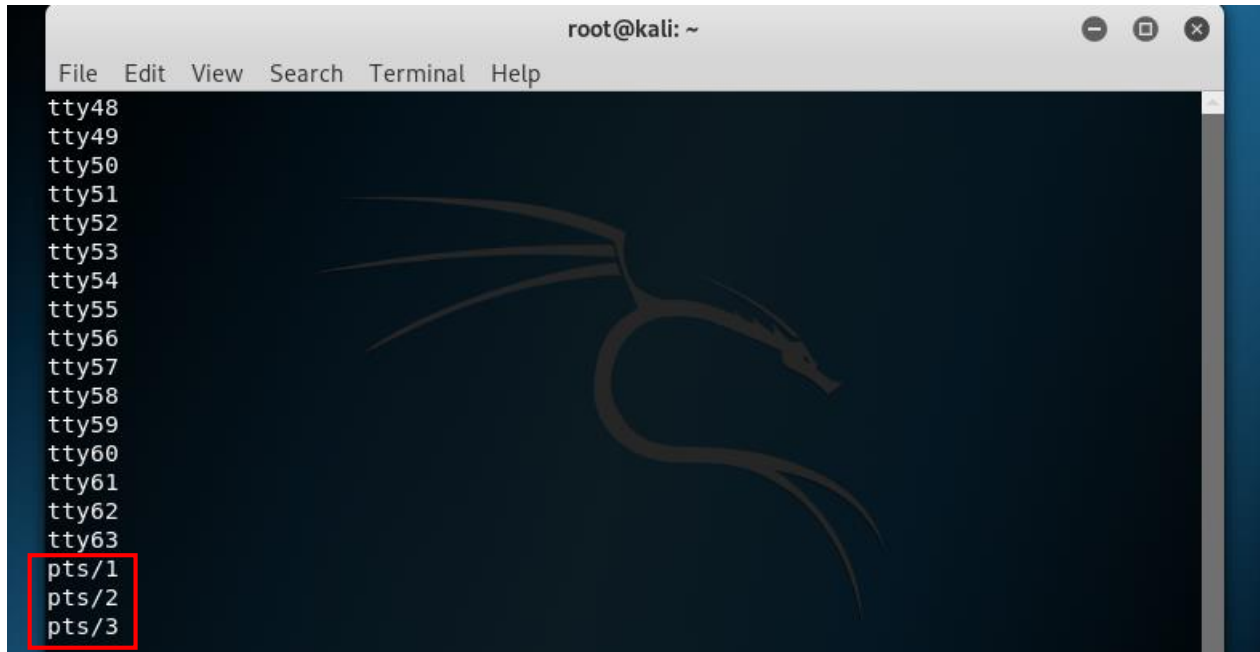
텔넷 서버 구축 - (2)

vi /etc/securetty - **PTS**(Pseudo-Terminal slave) 추가

PTS(원격 접속 가상 터미널)란?

우분투/데비안 계열 리눅스에서는 원격에서 root 접속을 하지 못하게 설정되어 있음

→ **root** 접속을 위해 PTS 추가



service xinetd restart - xinetd 데몬 재시작

ARP Spoofing

ARP란?

- 주소 결정 프로토콜(Address Resolution Protocol)
- 해당 IP에 해당하는 MAC 주소(물리적 주소)를 ARP table에서 찾음
 - IP주소를 MAC주소로 변환
 - 통신 가능하게 함

Spoofing(스푸핑)이란?

- 속이다, 도용하다
- IP에서 MAC 주소로 변환하는 과정을 속이는 해킹 기법
- 사용자의 신분(MAC, IP, 메일 주소 등) 도용하거나,
비정상적인 사용자가 정상적인 사용자인척 속이는 것을 의미

ARP Spoofing이란?

ARP Cache에 등록되는 정보를 속이는 공격 기법

ARP Spoofing - 희생자 PC의 게이트웨이 IP의 MAC 주소 확인

> arp -a : arp cache table 보기

```
C:\Users\did93>arp -a
```

인터페이스: 192.168.43.184 --- 0xa	인터넷 주소	물리적 주소	이동형
192.168.43.1	d0-13-fd-42-12-3e		정적
192.168.43.255	ff-ff-ff-ff-ff-ff		정적
224.0.0.2	01-00-5e-00-00-02		정적
224.0.0.22	01-00-5e-00-00-16		정적
224.0.0.251	01-00-5e-00-00-fb		정적
224.0.0.252	01-00-5e-00-00-fc		정적
239.255.255.250	01-00-5e-7f-ff-fa		정적
255.255.255.255	ff-ff-ff-ff-ff-ff		정적

인터페이스: 192.168.56.1 --- 0x12	인터넷 주소	물리적 주소	이동형
192.168.56.255	ff-ff-ff-ff-ff-ff		정적
224.0.0.22	01-00-5e-00-00-16		정적
224.0.0.251	01-00-5e-00-00-fb		정적
224.0.0.252	01-00-5e-00-00-fc		정적
239.255.255.250	01-00-5e-7f-ff-fa		정적
255.255.255.255	ff-ff-ff-ff-ff-ff		정적

IV

방어대책

1 방어대책

방어 대책

cmd에 ">arp -d" 입력 : 희생자 PC에서 ARP Cache 삭제



">arp -s (gateway ip주소) (gateway mac주소)"

희생자 pc의 cache table에서 gateway mac 주소를 정적으로 바꿔줌

Thank you