# 정보보안론 3주차 강의

Kali 리눅스는 한글폰트가 안 깔려 있다.

sudo apt install fcitx-hangul : 한글 입력기 다운

! 시험 !

스푸핑이 무엇인지

스푸핑 : 사기치는 것의 일종

칼리리눅스 한영전환 : ctrl + space

! 시험 !

3-웨이 핸드셰이킹

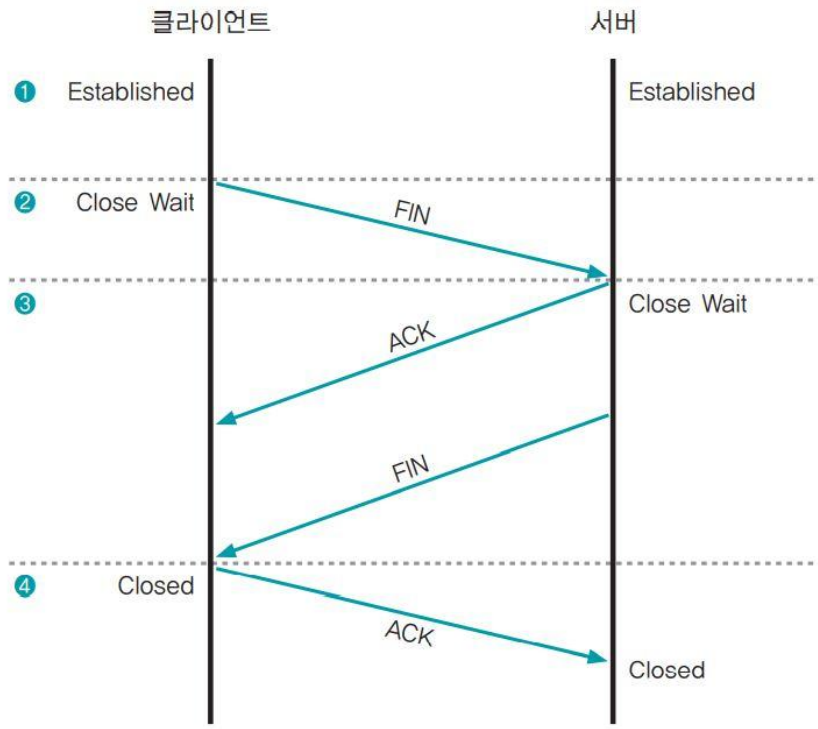



그림 3-14 TCP의 연결 해제 과정

❶ 통신 중에는 클라이언트와 서버 모두 Established 상태

❷ 통신을 끊으려는 클라이언트가 서버에 FIN 패킷을 보내고 클라이언트는 Close Wait 상태가 됨

❸ 서버는 클라이언트의 연결 종료 요청을 확인하고 응답으로 클라이언트에 ACK 패킷을 보내면 서버도 클라이언트의 연결을
종료하겠다는 의미로 FIN 패킷을 보내고 Close Wait 상태가 됨

❹ 클라이언트는 연결 종료를 요청한 것에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버에 보냄

! 시험 !

**서비스 거부 공격(DoS)**

취약점 공격형

- 특정 형태의 오류가 있는 네트워크 패킷의 처리 로직에 문제가 있을 때 공격 대상이 그 문제점을 이용하여 오작동을 유발하는 형태
- 보잉크/봉크/티어드롭 공격, 랜드 공격

자원 고갈 공격형

- 네트워크 대역폭이나 시스템의 CPU, 세션 등의 자원을 소모시키는 형태
- 랜드 공격, 죽음의 핑 공격, SYN 플러딩 공격, HTTP GET 플러딩 공격, HTTP CC 공격, 동적 HTTP 리퀘스트 플러딩 공격, 슬로 HTTP 헤더 DoS(슬로로리스) 공 격, 슬로 HTTP POST 공격, 스머프 공격, 메일 폭탄 공격

! 시험 !

보잉크/봉크/티어드롭 공격

프로토콜의 오류 제어 로직을 악용하여 시스템 자원을 고갈시키는 방식

TCP 프로토콜이 제공하는 오류 제거 기능

- 패킷의 순서가 올바른지 확인, 중간에 손실된 패킷이 없는지 확인
- 손실된 패킷의 재전송을 요구

Ping of Death 공격

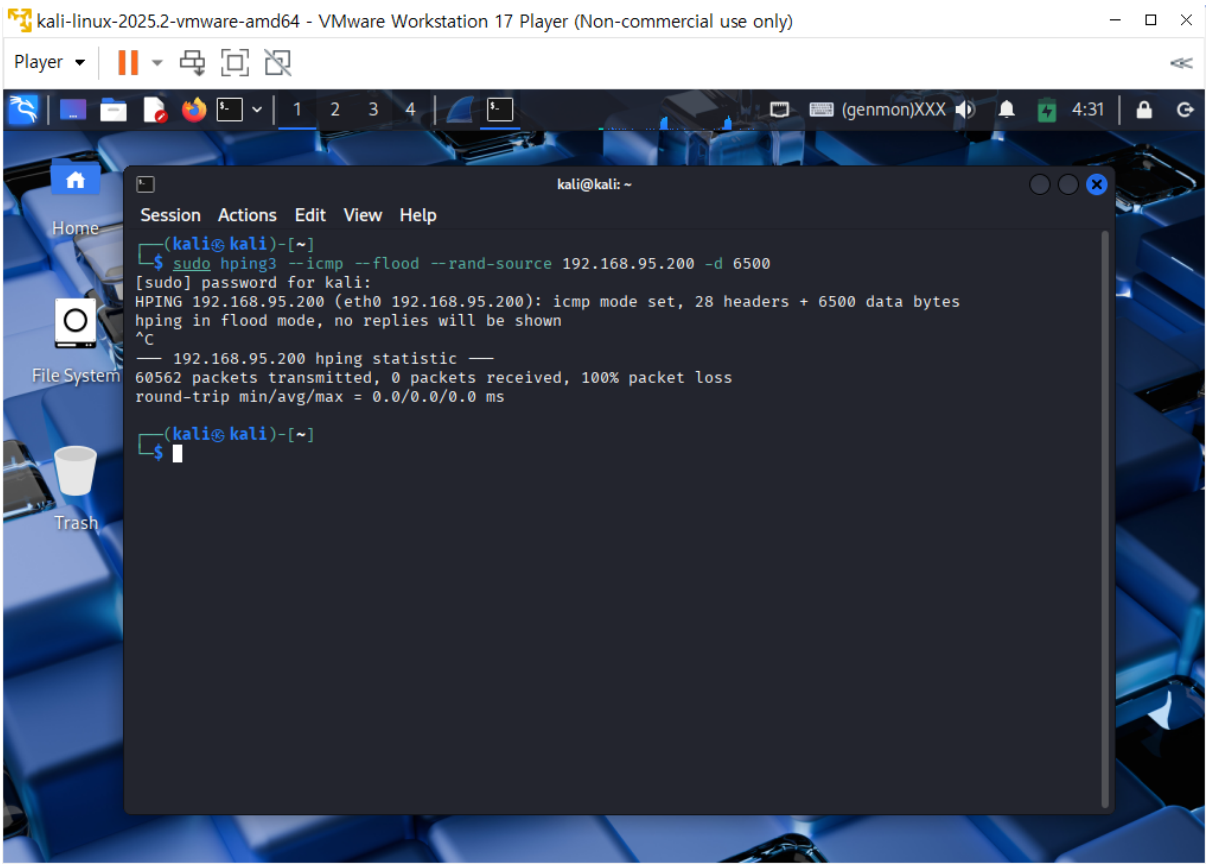
Ping을 이용하여 ICMP 패킷의 크기를 정상보다 아주 크게 만듦.

크게 만들어진 패킷은 네트워크를 통해 라우팅되어 공격 네트워크에 도달하는 동안 아주 작은 조각으로 쪼개짐.

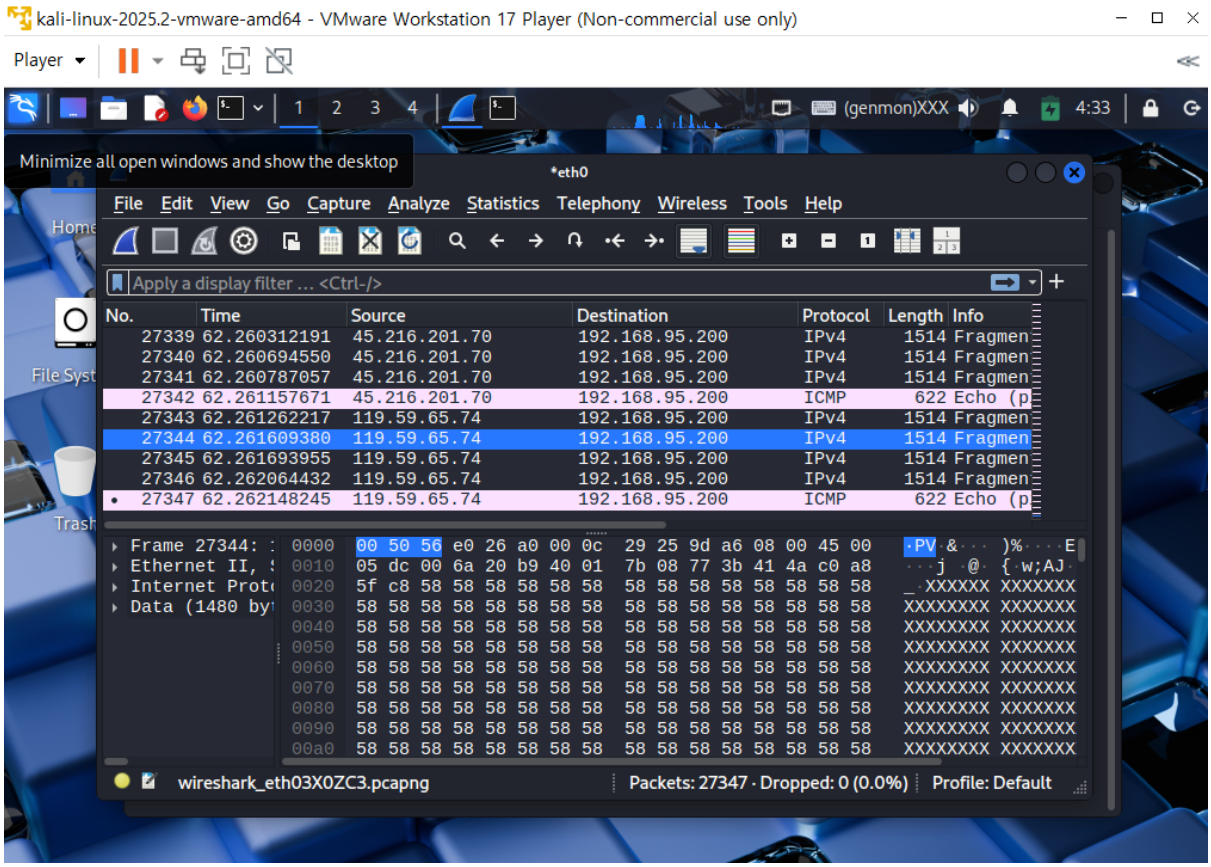
공격 대상은 조각화된 패킷을 모두 처리해야 하므로 정상적인 ping보다 부하가 훨씬 많이 걸림.

Ping of Death 공격 테스트

➔ sudo hping3 –icmp –flood –rand-source 192.168.95.200 -d 6500 명령어를 통해 Ping of Death 공격 실행



Wireshark를 통해 ping3로 보낸 패킷 분석




보안 대책

반복적으로 들어오는 일정 수 이상의 ICMP 패킷을 무시하도록 설정

가장 일반적으로 할 수 있는 대책은 패치

현대 서버 운영체제에서는 반복 ICMP 차단 기능 탑재