UDP Flooding

서비스 거부 공격(Dos)의 한 방식으로 UDP 패킷을 다량으로 전송하여 정상적인 서비스를 이용하지 못하도록 대역폭을 소모시키는 공격

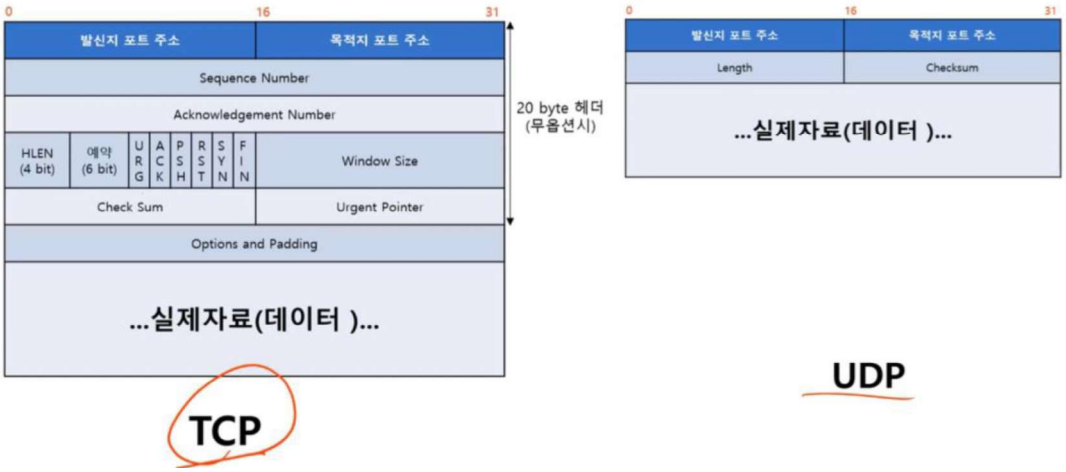
UDP Flooding 공격 방법

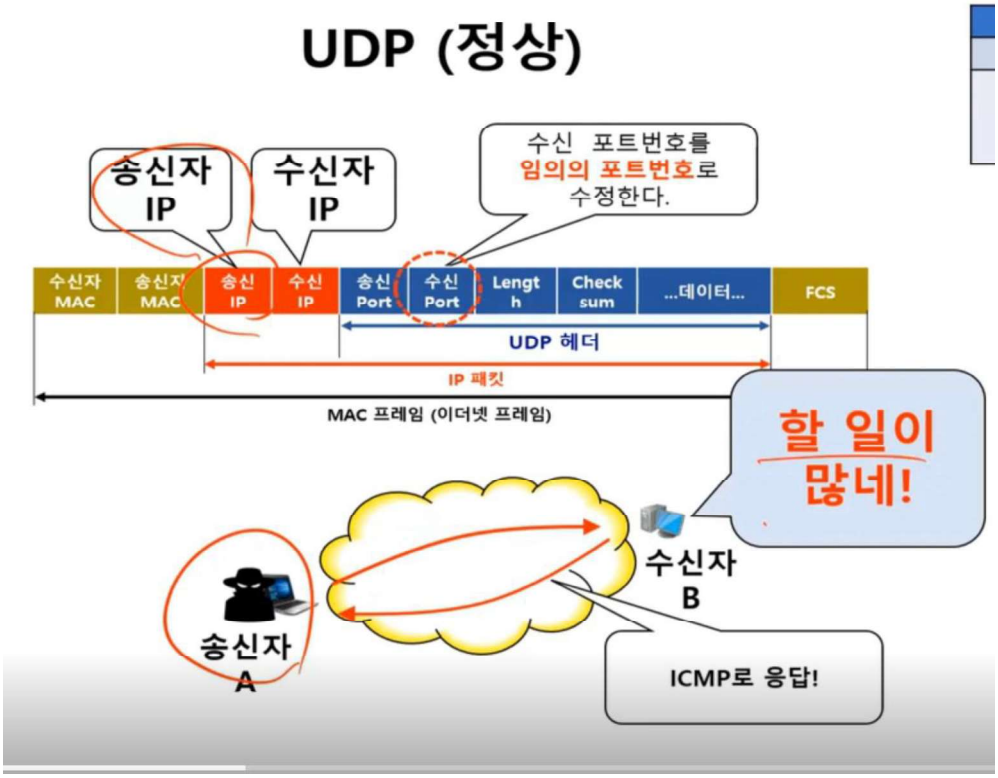
1) UDP/ICMP 패킷 이용

ICMP(Internert Control Message Protocol)는 인터넷 환경에서 오류에 관한 처리를 지원하는 용도로 사용되며, ICMP 패킷을 받으면 수신자는 송신자에게 자기 상태를 보고하도록 약속한 프로토콜

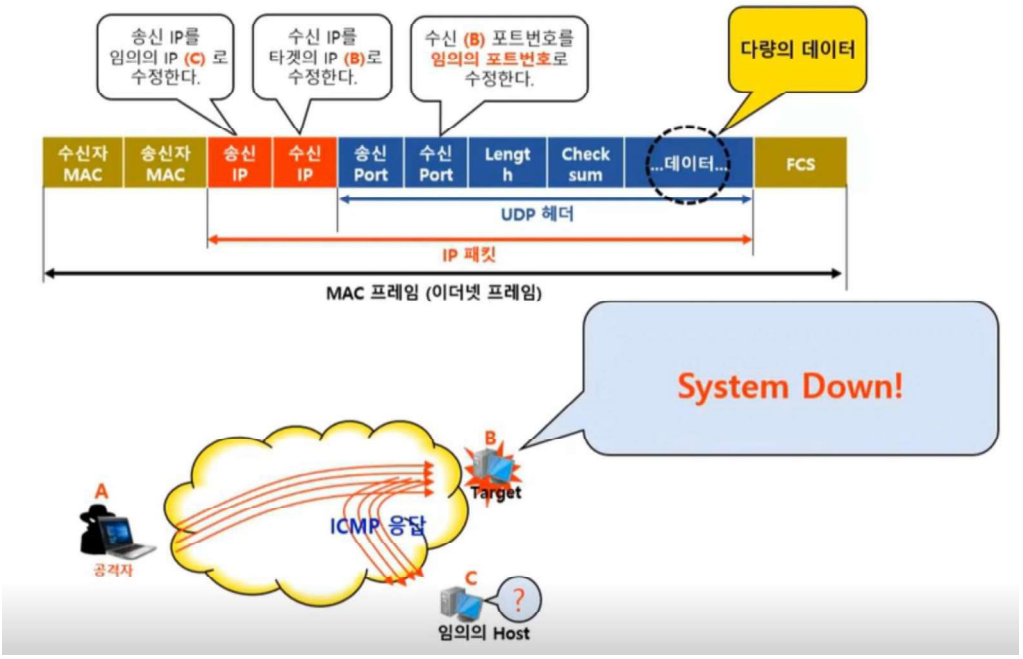
2) 공격자는 대량의 UDP 패킷을 A의 임의의 포트번호로 보내면 패킷을 받은 A는 포트를 사용하는 애플리케이션을 조사하여 포트를 사용하는 애플리케이션이 없다는 것을 확인한다.

3) 포트를 사용하는 애플리케이션이 없다는것을 확인하면 ICMP 패킷 중 Destination Unreachable 패킷을 공격자가 보낸 패킷의 송신자 주소를 보내게 되는데 대부분의 경우 공격자 UDP 패킷의 송신자 주소를 희생자 주소로 스푸핑하여 보내기 때문에 ICMP 패킷을 공격자에게 전달되지 않는다.





UDP Flooding 공격



다량의 데이터 패킷을 보낼 시 쪼개서 보내야 하므로 System의 리소스를 소모함.

1) 공격자는 수신 IP가 타겟의 IP(B)로 수정되고, 송신IP가 임의의 IP©로 수정되고, 수신포트가 임의의 포트번호로 수정된 UDP 패킷을 전송함

2) 패킷을 받은 Host(타겟) 는 포트를 사용하는 App를 조사하여 포트를 사용하는 App가 없다는것을 확인한 후 ICMP Destination Unreachable패킷을 공격자가 보낸 송신 IP로 보낸다. 이때 시스템 자원을 소비

3) 임의의 HOST는 ICMP Destination Unreachable 수신. 역시 시스템자원을 소비하는 피해를 입는다.

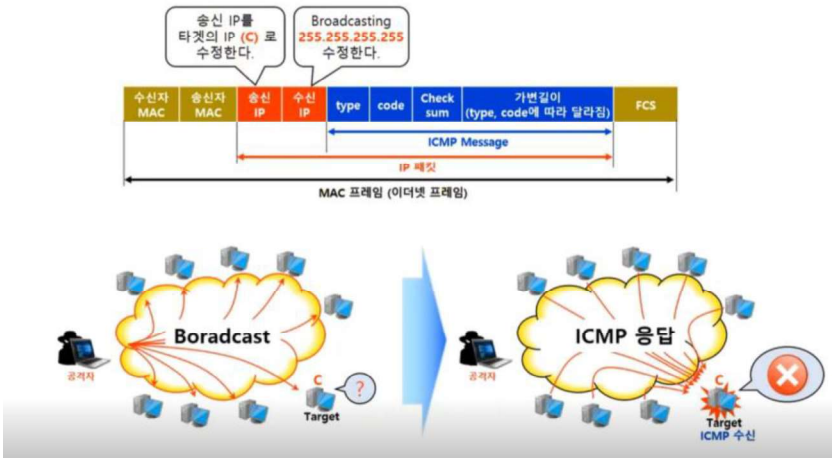
ICMP Flooding (Smurf Attack: 스머프 어택)

1) 목표 사이트에 응답 패킷의 트래픽이 넘쳐서 다른 사용자로부터 접속을 받아들일 수 없게 만드는 것

2) IP 주소에는 한번에 여러 주소를 모아 문의할 수 있게 하는 브로드 캐스트 주소(Broadcast address) 라는 것이 준비되어 있다. 이 주소에 목표 사이트에서 발신된것 처럼 IP 주소를 위조하여 핑(Ping) 패킷을 발신하면 여러 서버에

3) 목표 사이트는 이 응답 패킷의 트래픽이 넘쳐서 다른 사용자로부터 접속을 받아 들일 수 없게 된다.

ICMP Flooding 공격 (Smurf Attack: 스머프 어택)

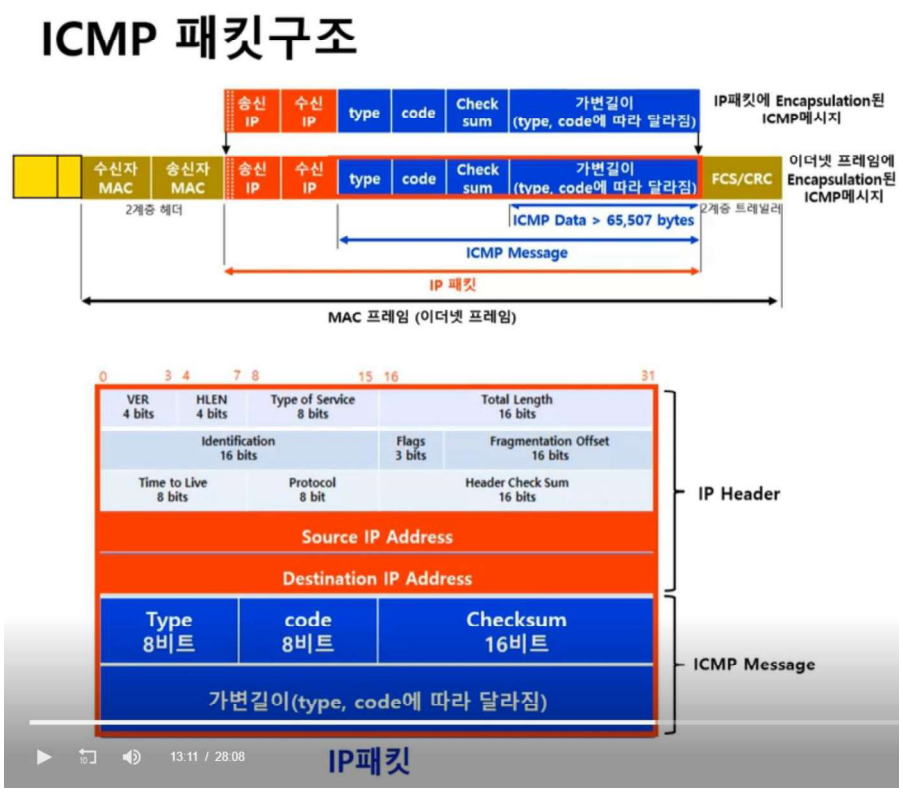


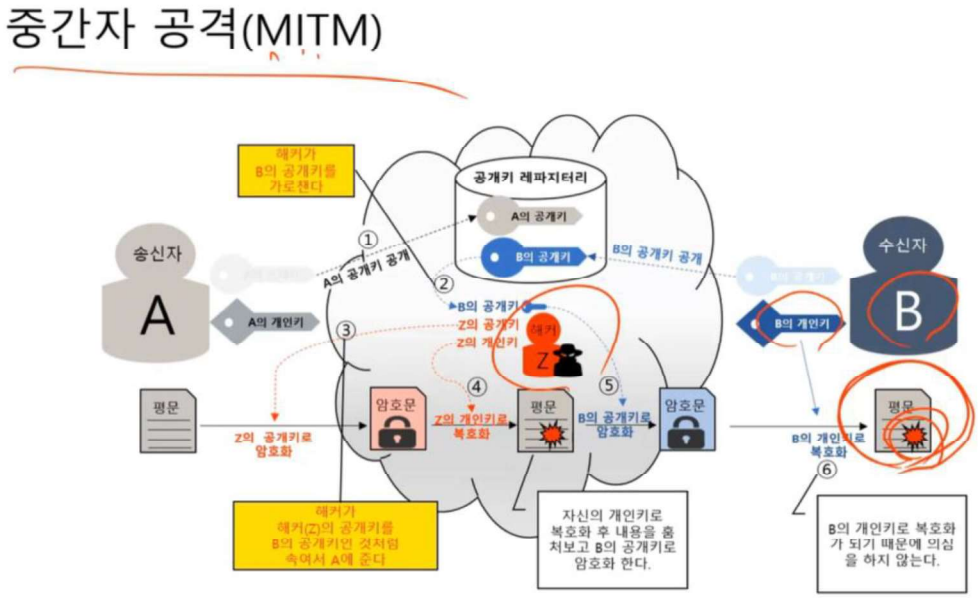
1)ICMP와 BroadCasting(브로드 캐스트는 위험성으로 인해 IPv6에서는 삭제) 을 이용한 공격으로 ICMP 패킷을 특정 브로드 캐스트 주소로 보내어 공격대상이 다량의 ICMP Reply 패킷을 받도록 하는 공격 기법이다.

2) 발신지 IP 주소가 공격대상의 IP 주소로 위조된 ICMP 패킷을 특정 브로드캐스트 주소로 보내어 공격대상이 다량의 ICMP reply 패킷을 받도록 하는 공격기법이다.

3) 공격자가 다량의 ICMP Echo Request의 출발지 IP 주소를 피해 시스템의 IP 주소로, 목적지 IP 주소를 Direct Broadcast IP 주소로 spoofing하는 공격이다.

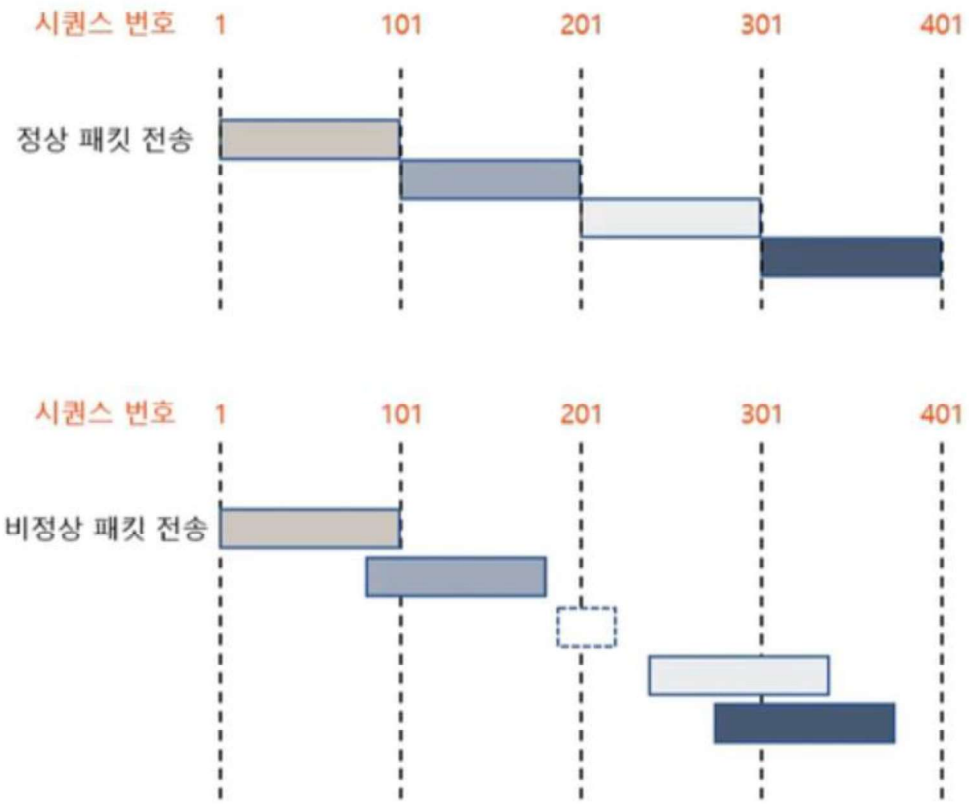
4) ICMP는 TCP/UDP 헤더를 필요치 않으며 IP 헤더와 IP 데이터 부분에 ICMP 메시지를 포함하여 패킷을 전송한다.



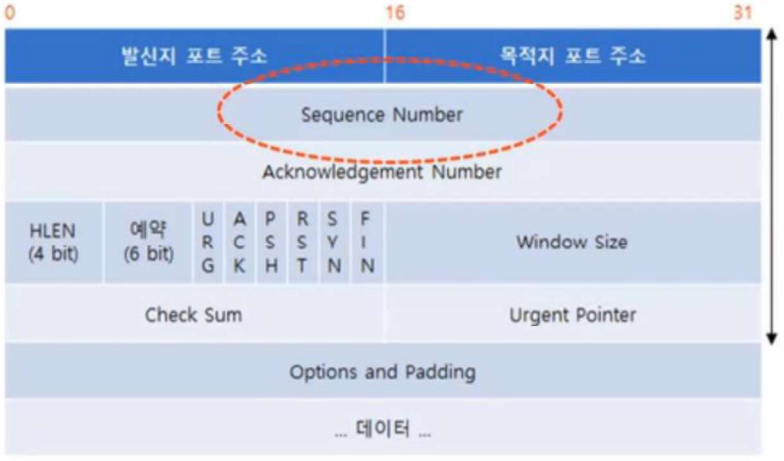


살라미 공격(Salami) : 티끌모아 태산. 많은 사람들로부터 눈치 채지 못할 정도의 적은 금액을 빼내는 컴퓨터 사기수법의 하나이다. 이탈리아 음식 살라미 소시지를 조금씩 얇게 썰어먹는 모습을 연상시킨다고해서 붙은 이름이다.

TearDrop : MTU(Maximun trasmission unit : 최대전송단위) 보다 큰 패킷을 분할하여 전송한 후 패킷의 재조합 과정에 문제점을 이용한 공격방법
서비스 거부 공격(Dos)의 하나로 희생자 컴퓨터에 시퀀스 넘버가 조작된 IP 패킷들을 전송함으로써 컴퓨터의 OS를 다운시키는 공격

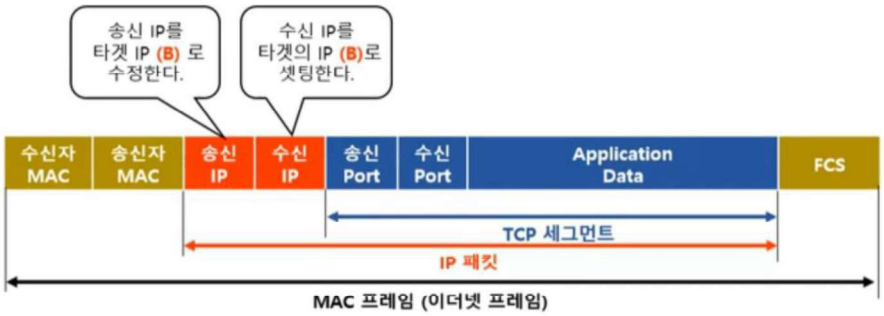


수신측에서 재조합시(Reassembling) 시 시스템의 부하가 증가한다.

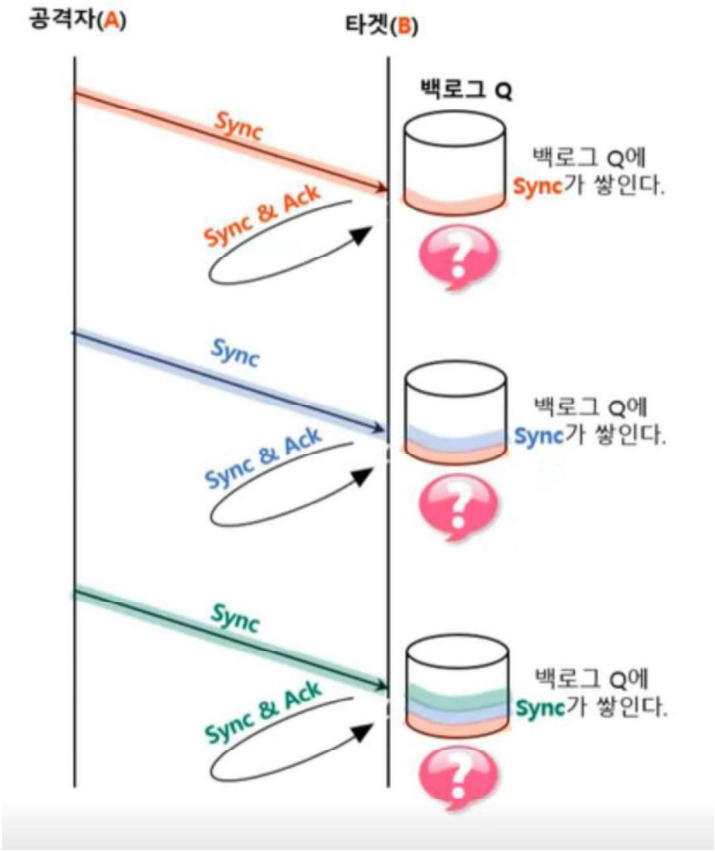


TCP 세그먼트

6) LAND Attack



출발지와 목적지 IP가 동일하게 위조된 SYN 패킷을 전송하는 공격

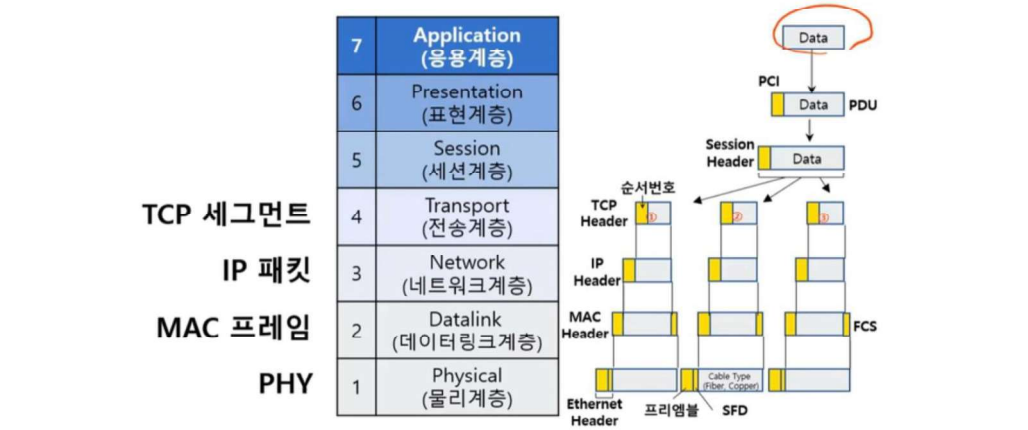


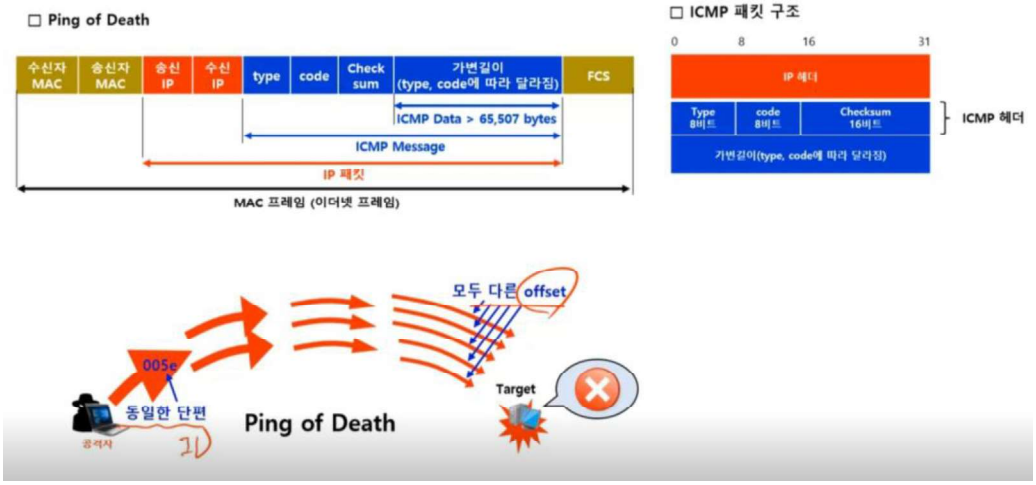
Ping of Death

ICMP 패킷을 통해 전송하면, 라우팅 시 조각화 된 패킷으로 인해, 공격대상 시스템의 성능을 떨어뜨리는 공격이다.

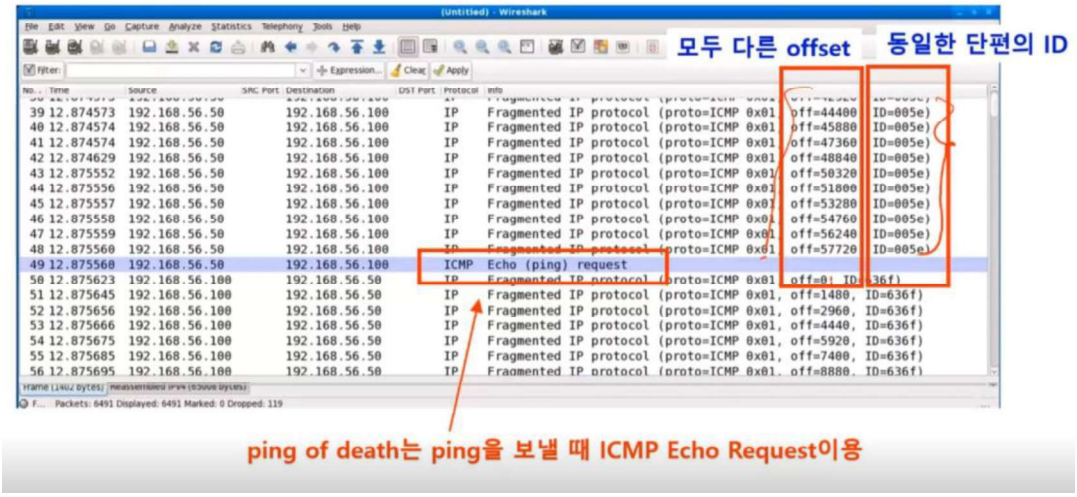
Ethernet의 경우 1,500 Bytes, 즉 IP 패킷의 최대 크기가 1500 Bytes이기 때문에 IP 헤더부(기본 20 Bytes)를 제외하면 ICMP 패킷은 최대 1480 Bytes의 크기로 생성

인터넷 프로토콜의 허용 범위 65,356 바이트 이상의 큰 패킷을 고의로 전송하여 발생한 서비스 거부 Dos 공격이다. 공격자의 식별 위장이 용이하고, 인터넷 주소 하나만으로도 공격이 가능하다.

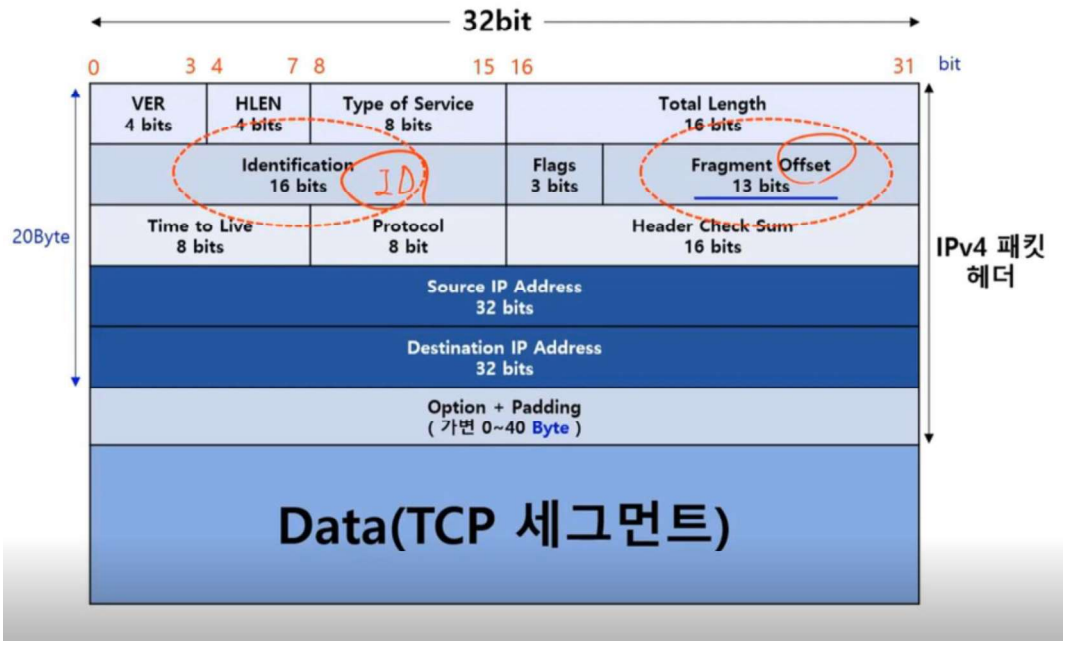




희생자 화면 캡처(wireshark)



IPv4 패킷 구조


32bit
0
3 4
7 8
15 16
31
bit
VER
4 bits
HLEN
4 bits
Type of Service
8 bits
Total Length
16 bits
Identification
16 bits
ID
Flags
3 bits
Fragment Offset
13 bits
Time to Live
8 bits
Protocol
8 bit
Header Check Sum
16 bits
20Byte
Source IP Address
32 bits
Destination IP Address
32 bits
Option + Padding
(가변 0~40 Byte)
Data(TCP 세그먼트)
IPv4 패킷
헤더