# WebServer 구축

192.168.10.30/24
Web Server
(CentOS8)

❶ rpm -qa | grep httpd

❷ dnf install httpd -y

❸ systemctl start httpd

❹ systemctl status httpd

❺ ps -ef | grep httpd

❻ systemctl enable httpd

❼ cd /var/www/html

```
<html>
<head><title>Hello~</title></head>
<body>
  Hello~ SKS^^
</body>
</html>
```

❽ firewall-cmd --add-service=http

# DDoS 공격 패킷분석

- 과도한 트래픽을 공격대상에게 전송하여 서비스를 불가하게 하는 공격 기법
  - 과도한 트래픽 또는 부하를 발생시켜 정상적인 통신이 불가능하게 만드는 통신 유형

# 통신 기본 3요소

**❶ 전송매체(회선)**

- End-to-End 연결통로
- 각 전송 매체 별로 수용 가능한 대역폭을 보유

**❷ 정보원(송수신자)**

- End-to-End
- End-to-End  연결 중계장비
- 각각 처리할 수 있는 최대 선능 존재
- 최대 성능은 CPU/메모리 등 장착되는 부품에 따라 달라짐

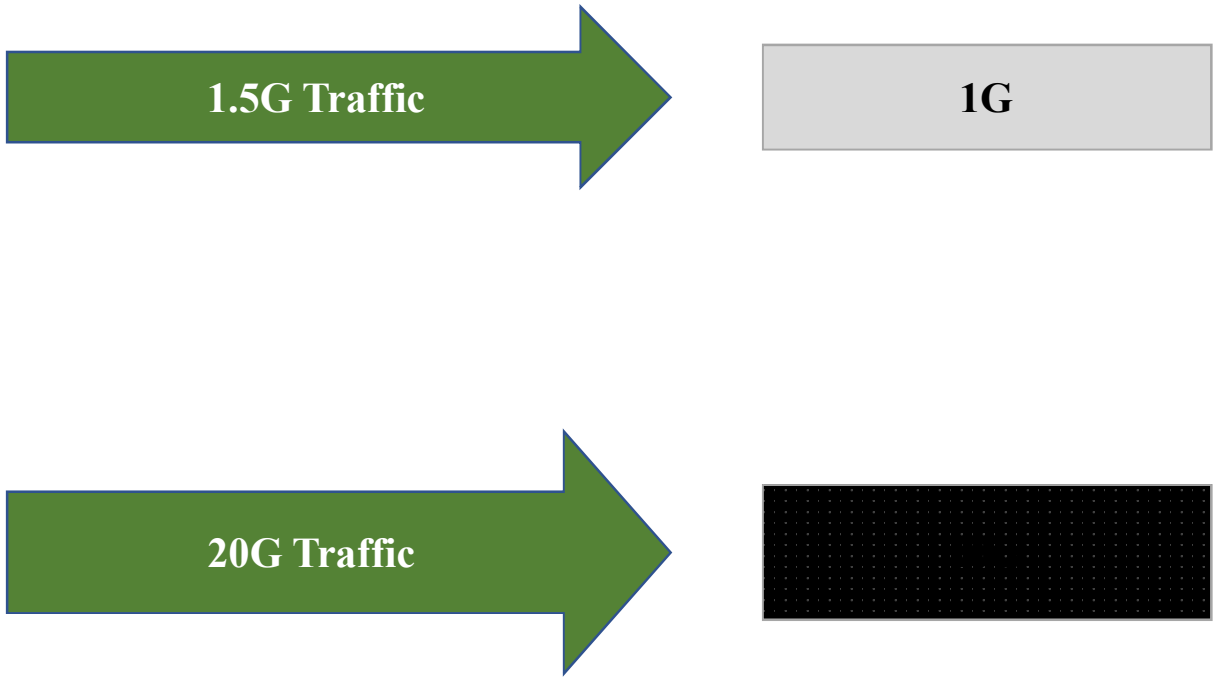
**❸ 프로토콜**

- 통신규약
- 정상적인 통신을 위해 미리 정의된 규약에 맞춰 데이터 송수신



# DDoS 공격 원리

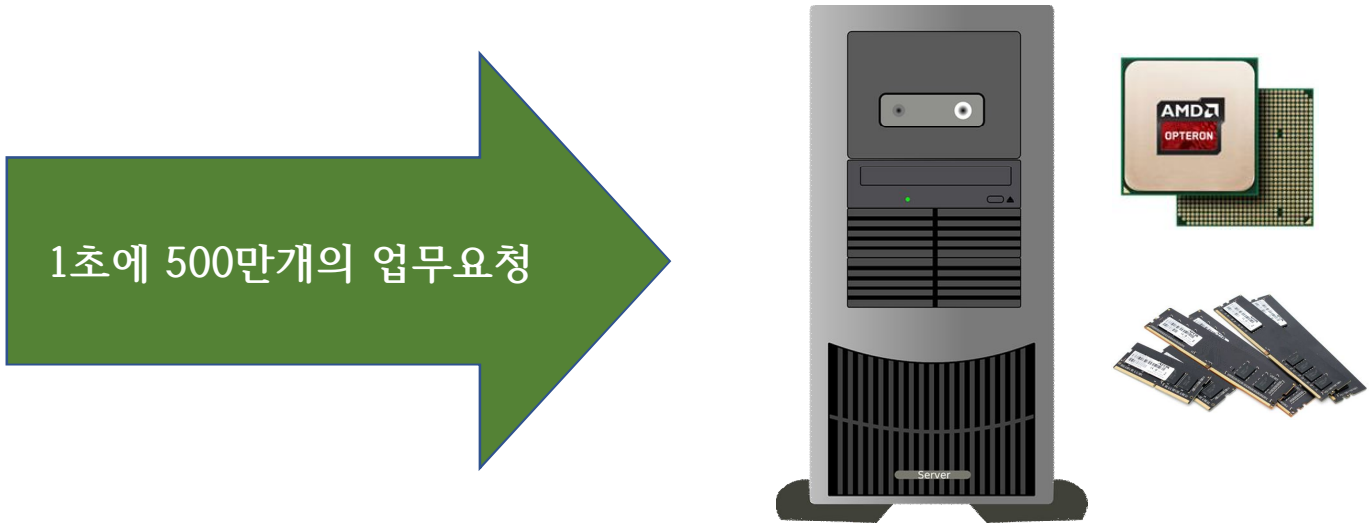
- 전송 매체 별 **자신이 수용 가능한 대역폭 이상의 트래릭이 전송될 경우**, 전송된 트래픽을 수용하지 못하여 정상적인 통신이 불가능해짐




UTP Cable(1G)

Optical Cable(10G)

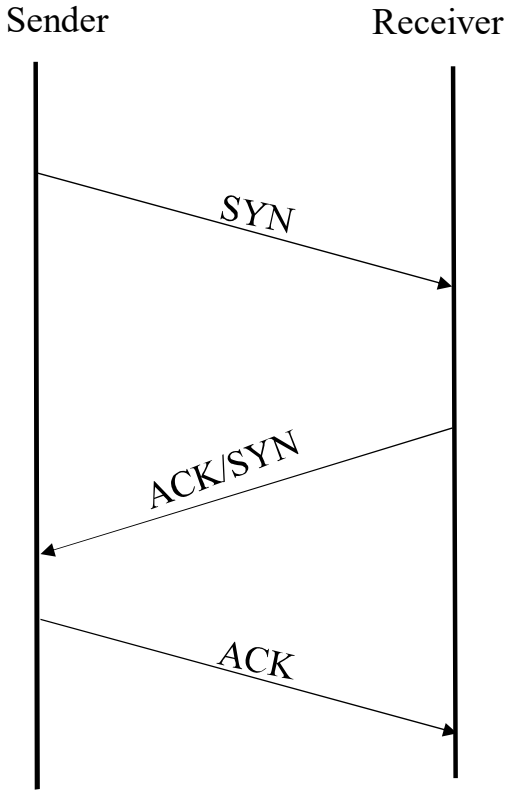
- 각 정보원이 **처리 가능한 성능 이상의 요청이 발생할 경우** 이를 처리하지 못하여 정상적인 통신이 불가능해진다.

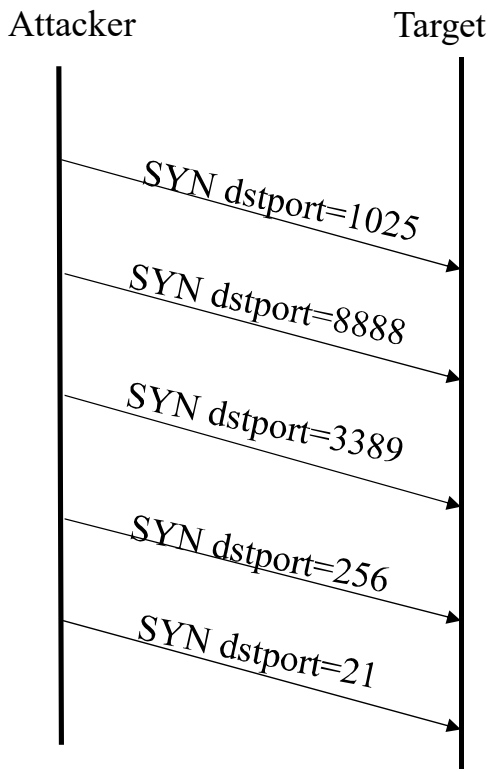



고성능 서버

<<1초에 100만개의 업무처리 >>

- 프로토콜의 허점을 이용하여 운영체제 또는 설치된 애플리케이션이 비정상적 상태에 빠지게 한다.




미존재IP
IP:??????

# DDoS 공격 목적

<< **일반적인 해킹목적** >>

특정 시스템의 취약점을 이용하여 시스템에 침투하거나 파일을 유출 또는 변조하는 행위

**금전요구**

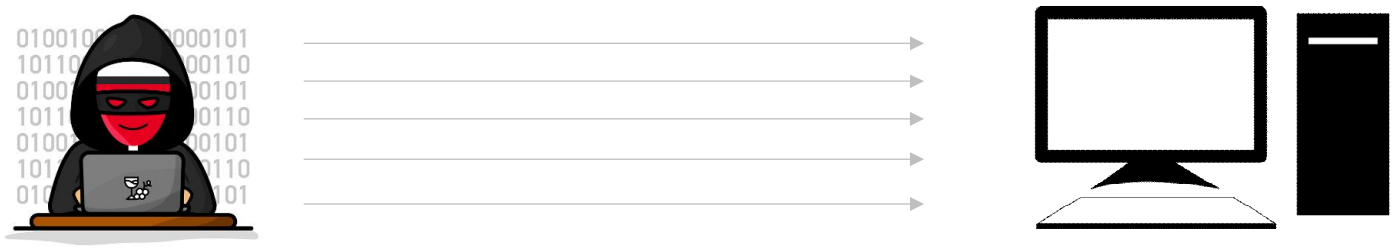
**개인적 원한**

**경쟁상에 의한 공격/청부**

**핵티비즘**

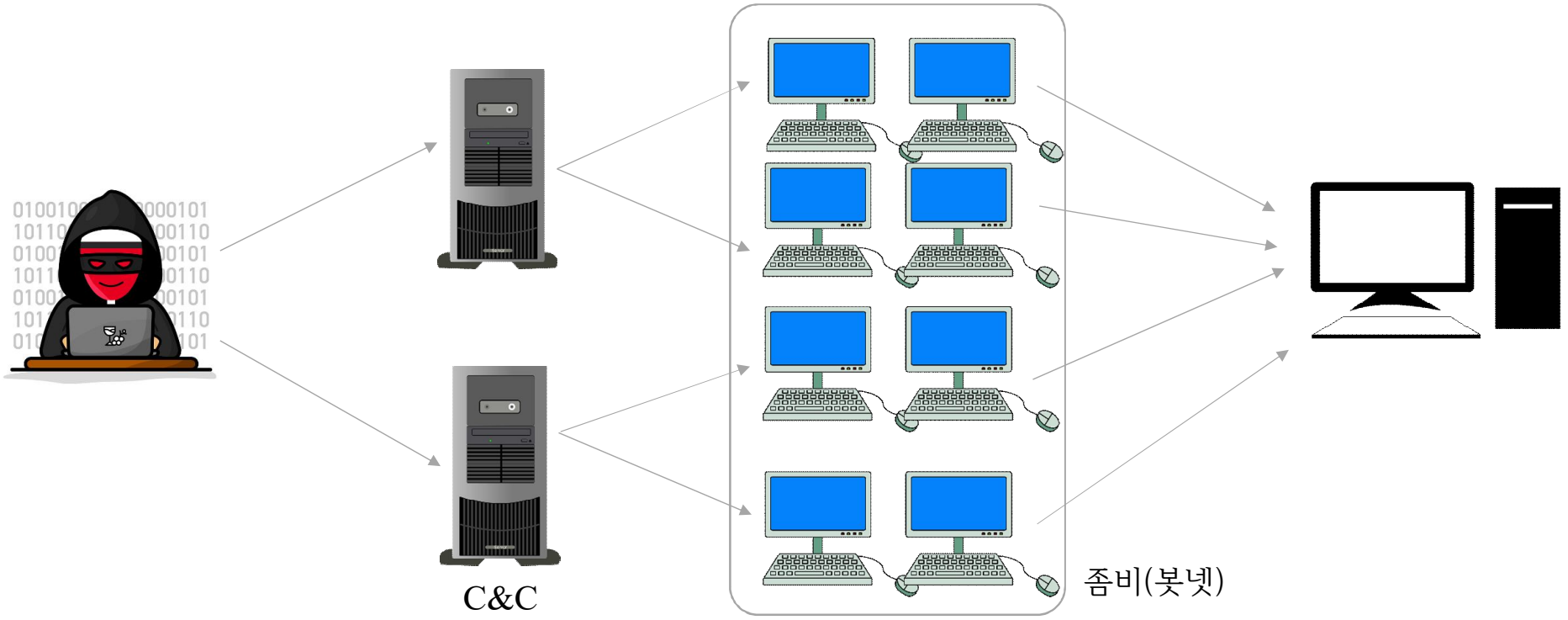
# DoS (Denial of Service, 서비스 거부 공격)

- 특정 공격 PC 또는 서버 1대에서 공격 대상 서버 1대로 과도한 트래픽 또는 패킷은 전송하는 1:1 형태



# DDoS (Distributed Denial of Service, 분산서비스거부공격)

- 서버와 차단 장비의 성능이 높아짐에 따라 DoS와 같은 1:1 공격은 더 큰 효과를 낼 수 없게 되었음
- 공격 성능을 증대 시키기 위해 탄생한 것
- 악성코드에 감염된 여러 대의 좀비들을 이용하여 동시에 공격하므로 N:1 형태를 띔



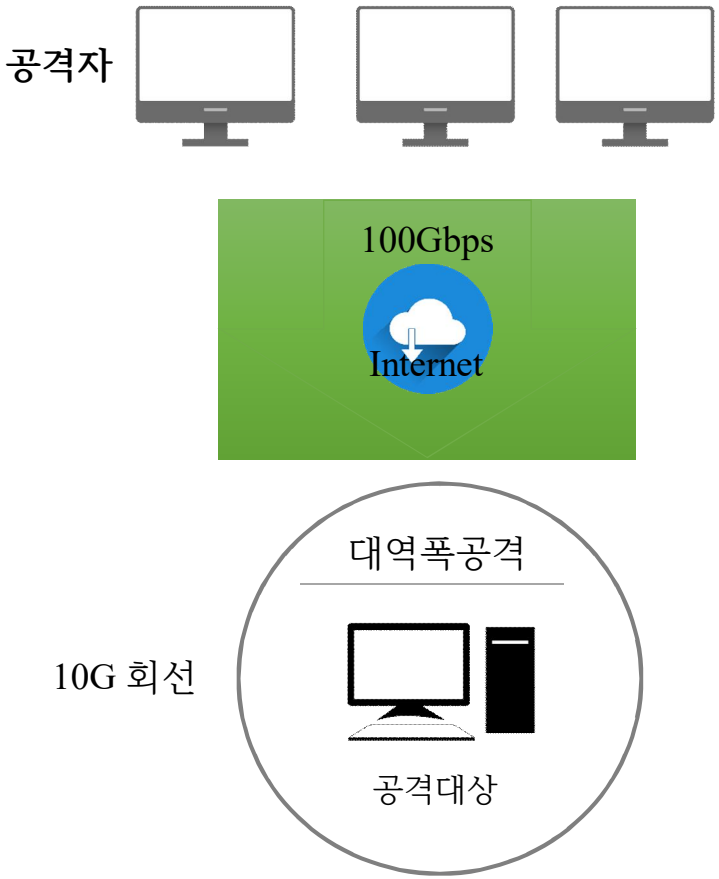
# DDoS 공격 종류

- 7.7 DDoS(2009.0707)
- 3.3 DDoS(2011.03.03)
- 금융권 DDoS(2015.06.26)
- Mirai DDoS(2016.09~10)
- 금융권 DoS(2017.06~07)

# DDoS 공격 주요 유형

- 대역폭 공격
- 자원 고갈 공격
- 응용 계층 공격

# ❶ 대역폭 공격




❶ 목적 : 대용량의 트래픽 전송으로 인한 네트워크 회선 대역폭 고갈

❷ 영향 : 회선 대역폭 고갈로 인한 정상 사용자 접속 불가

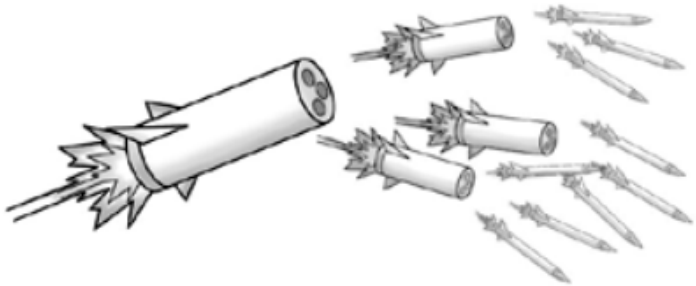
❸ 주요 프로토콜 : UDP, ICMP

❹ 특징 : 주로 위조된 큰 크기의 패킷과 위조된 출발지 IP 사용

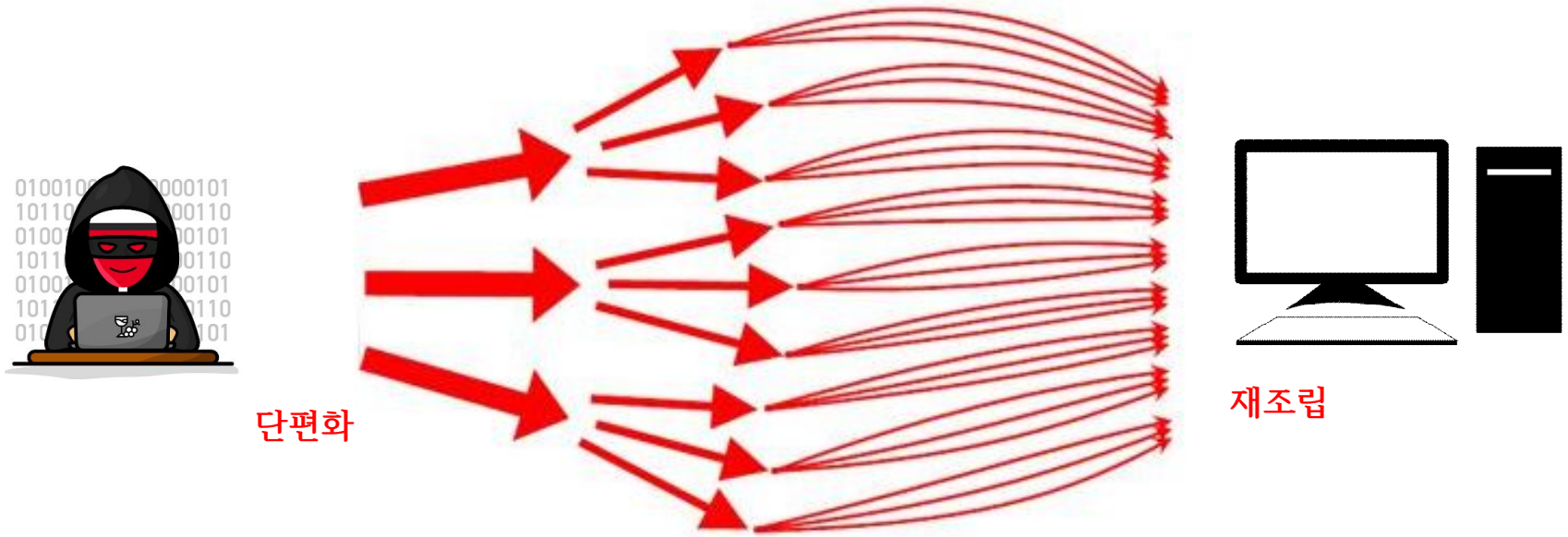
| 구분 | 내용 |
|---|---|
| 대표적인 공격유형 | UDP flooding<br>ICMP flooding<br>Fragment Flooding |
| 공격목적 | 회선 대역폭 잠식 |
| 공격기법 | bps(bit per second) |
| 공격계층 | 네트워크 계층(layer 3/4) |

# ❶ 대역폭 공격

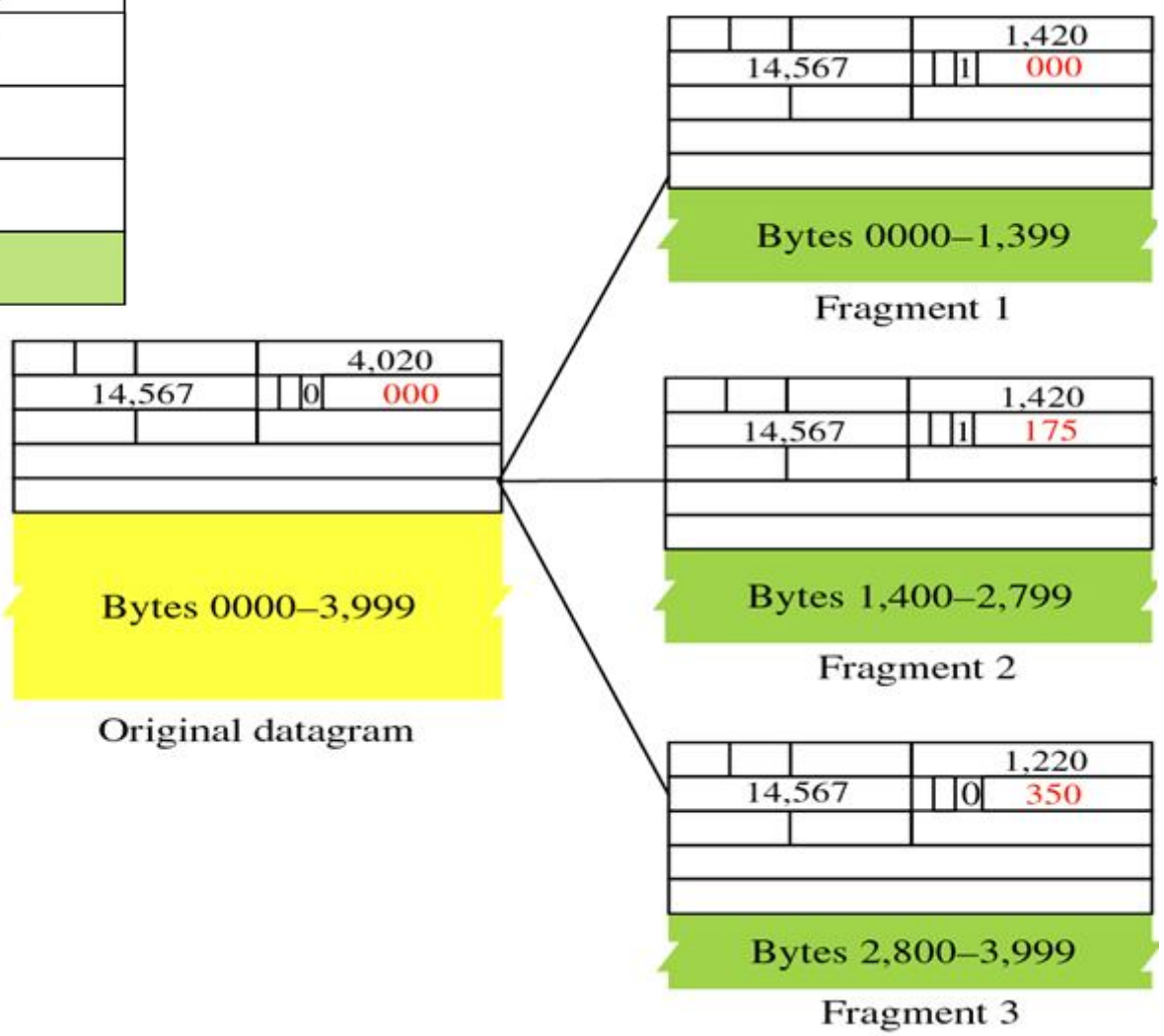
## - Fragmentation Flooding Attack



- 네트워크 기기가 전송할 수 있는 최대전송단위 MTU이상의 크기의 패킷을 전송 시, 패킷이 분할되는 단편화(fragmentation)의 특징을 이용한 공격 유형



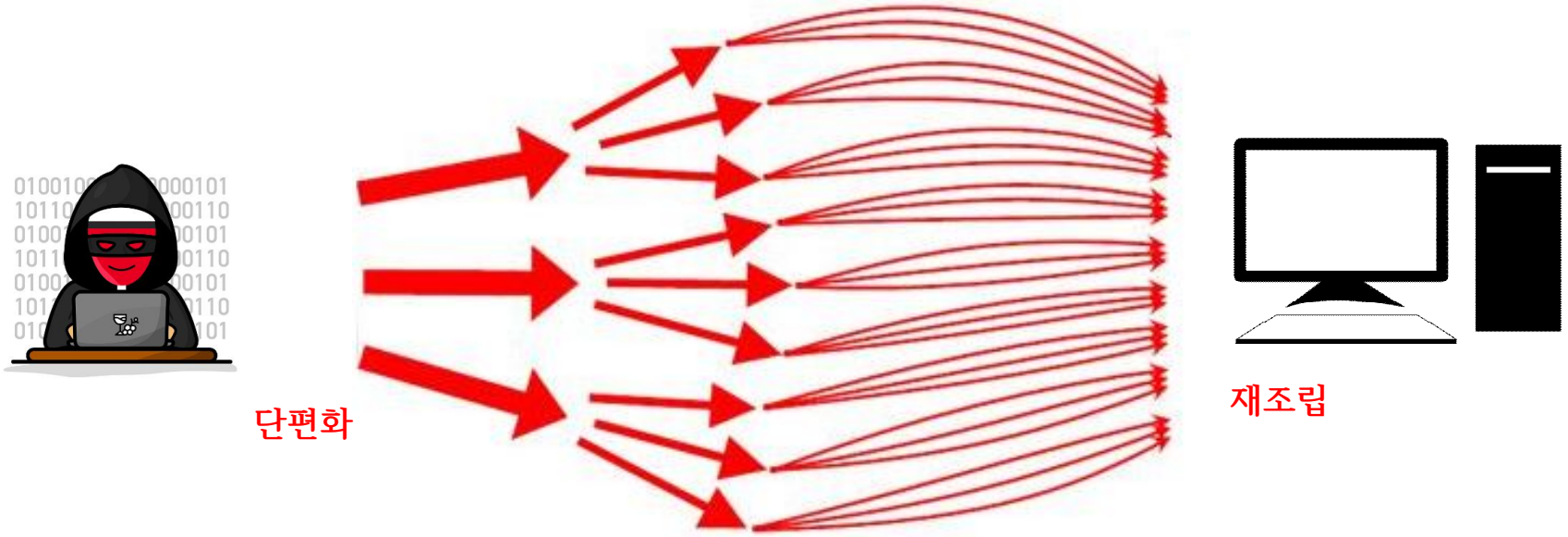
| VER<br>4 bits | HLEN<br>4 bits | Service type<br>8 bits | Total length<br>16 bits | |
|---|---|---|---|---|
| Identification<br>16 bits | | | Flags<br>3 bits | Fragmentation offset<br>13 bits |
| Time to live<br>8 bits | | Protocol<br>8 bits | Header checksum<br>16 bits | |
| Source IP address | | | | |
| Destination IP address | | | | |
| **Option** | | | | |



# ❶ Fragmentation Flooding Attack

문자열 65000 바이트로 네트워크에 ping전송

```
hping3 --icmp --rand-source 192.168.10.20 -d 65000 --flood
```



# ❷ 자원 고갈 공격


❶ 목적 : 정상 혹은 비정상적인 TCP flag 가 설정된 패킷을 서버 또는 네트워크 장비로 전송하여 장비의 자원 고갈

❷ 영향 : 장비의 특정 자원이 고갈되어 정상적인 운영 불가

❸ 주요 프로토콜 : TCP

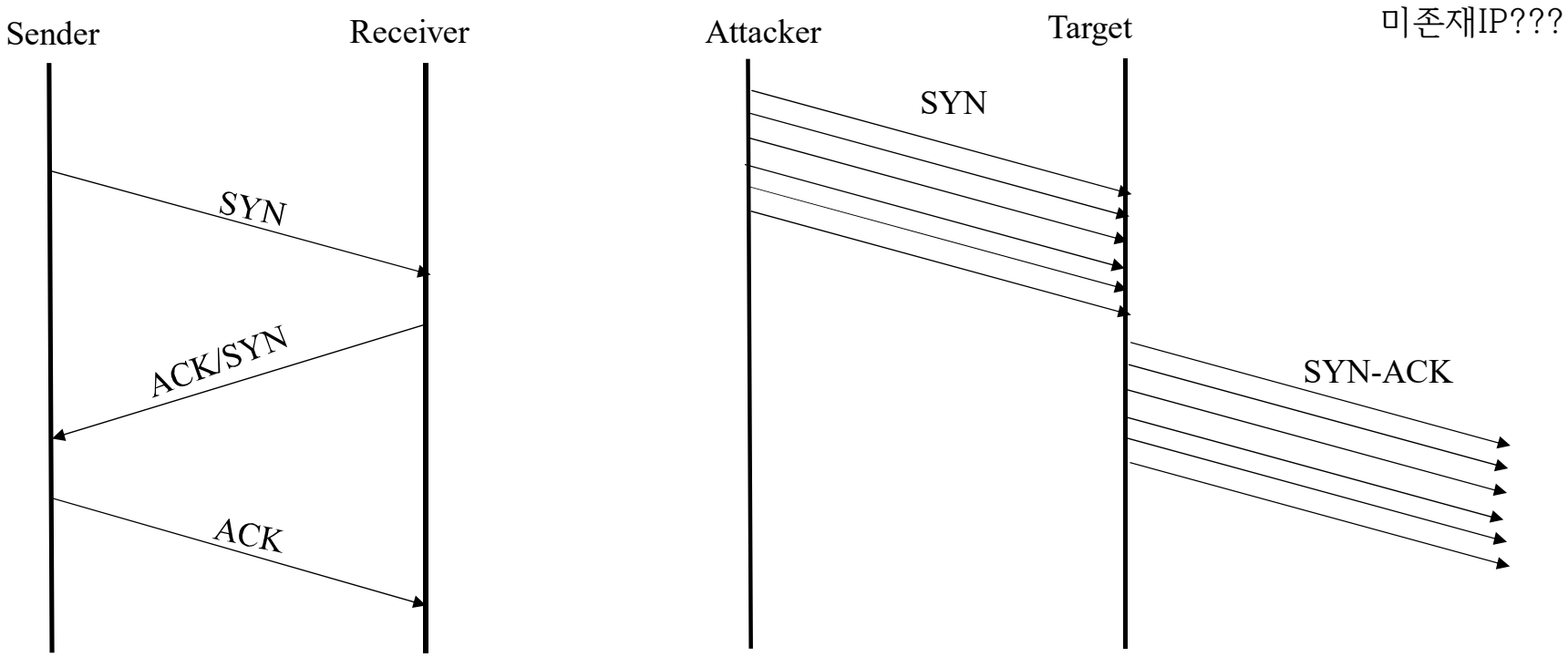
❹ 특징 : TCP flag를 이용하여, 위조된 IP를 사용

| 구분 | 내용 |
|---|---|
| 대표적인 공격유형 | SYN flooding<br>ACK flooding<br>Fragment Flooding |
| 공격목적 | 서버 및 네트워크 장비의 자원 고갈로 인한 장비 운영 불가 |
| 공격기법 | PPS (Packet Per Second) |
| 공격계층 | 네트워크 계층(layer 3/4) |

# ❷ 자원 고갈 공격

## - SYN Flooding 공격(4계층 공격)

- TCP이 3-way-handshake 과정에서 발생 가능한 취약점을 이용한 공격 유형



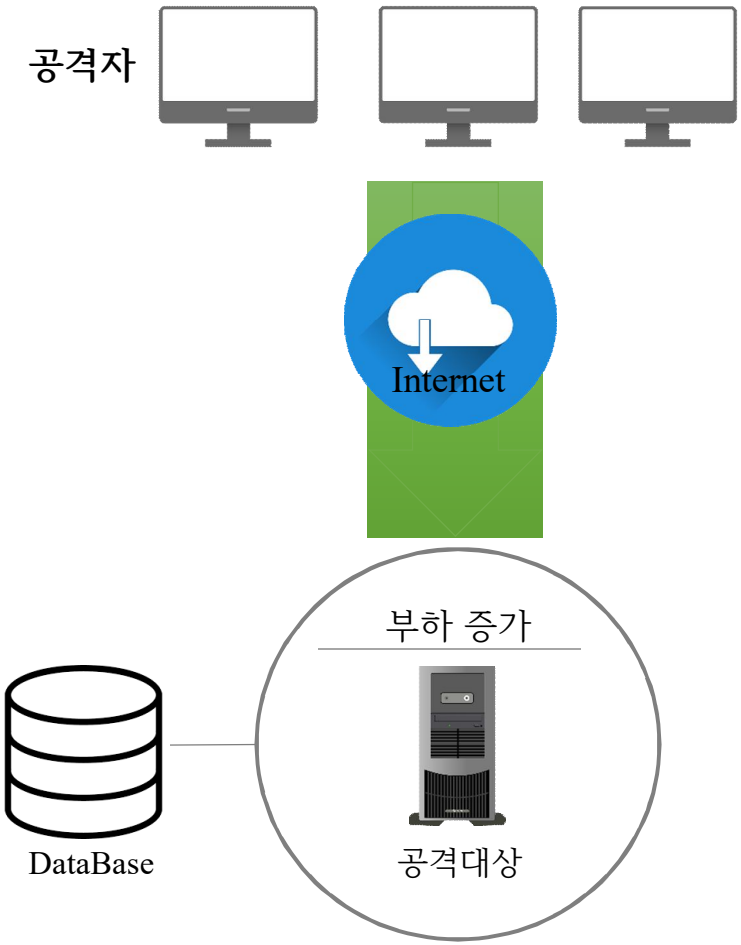
# ❷ 자원 고갈 공격

## - SYN Flooding 공격(4계층 공격)

- SYN Flooding 공격을 이용하여 Web Server의 HTTP 서비스를 지연 또는 정지시킴
- 10초 내에 패킷 50여만개의 SYN 전송

  - hping3 --rand-source 192.168.10.20 –p 80 –S --flood

# ❸ 응용 계층 공격




❶ 목적 : 서버에 설치된 애플리케이션의 부하를 발생시키고, 웹 서버의 경우 연결된 DB에도 부하가 발생

❷ 영향 : 부하 증가로 인한 운영 데몬 다운, 서버자원 부하 발생으로 정상적인 운영 불가

❸ 주요 프로토콜 : HTTP, DNS

❹ 특징 : HTTP 공격은 Real IP를 이용하여 Get 또는 Post를 사용
DNS 공격은 위조된 IP를 이용하여 DNS 질의 요청

| 구분 | 내용 |
|---|---|
| 대표적인 공격유형 | Get flooding<br>Post flooding<br>DNS Query Flooding |
| 공격목적 | 서버의 부하 증가로 인한 운영중인 서비스다운 |
| 공격기법 | RPS (Request Per Second) |
| 공격계층 | 응용 계층(layer 7) |

# ❸ 응용 계층 공격

## HTTP Get Flooding 공격

대량의 HTTP Get 요청을 발생시켜 웹서버의 자원을 소진시키는 공격

* https://github.com/5l1v3r1/TakeitDown 파일 다운로드