SYN-flooding attack

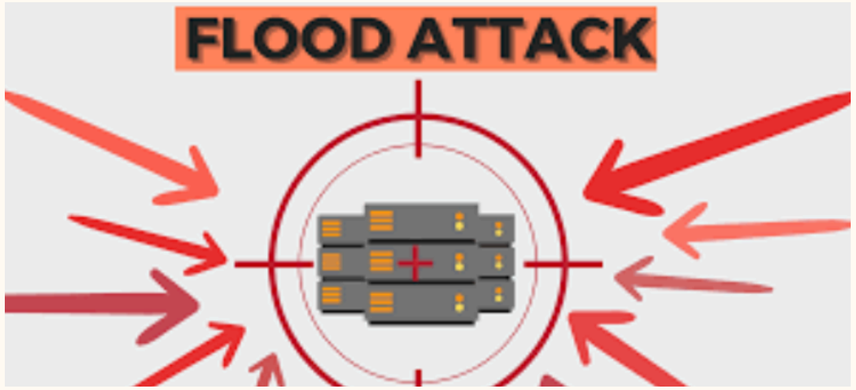
설 현 원

flooding?(홍수)

플러딩 은 단기간에 목표 시스템(서버, 네트워크, 서비스)으로

대량의 트래픽이나 요청을 **쏟아부어**(resource exhaustion)
정상 동작을 방해하는 행위 또는 현상이다.

- 의도적(공격)일 수도 있고, 설정 오류나 버그로 인한 우발적 과부하일 수도 있다.



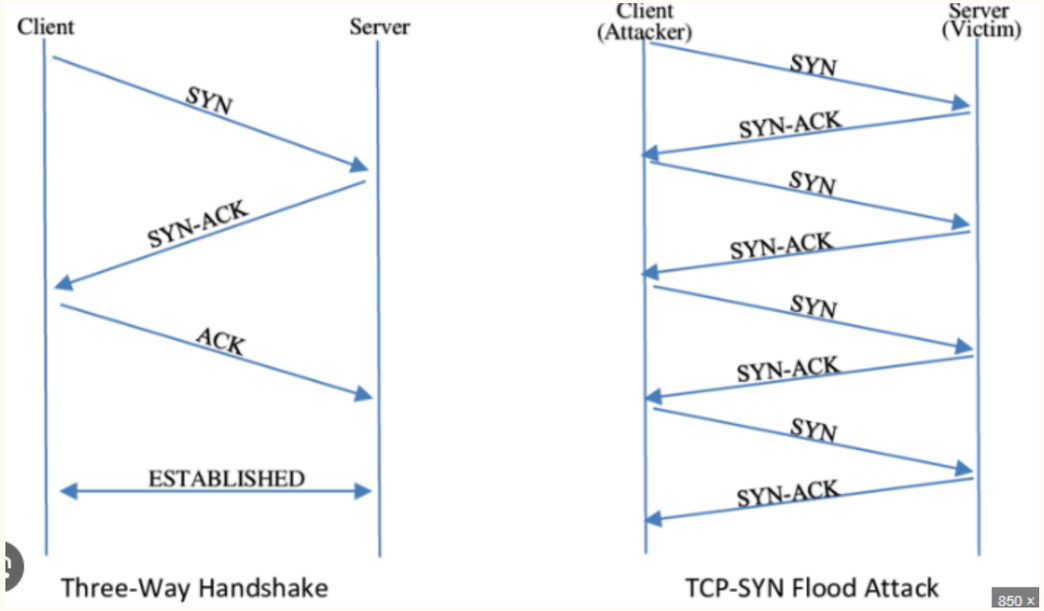
**플러딩은 DoS의 한 종류

(TCP)
SYN-flooding

3-Way Handshake(TCP 연결 설정 과정)의 취약점을 이용한 공격

적은 노력(비용)으로 서버 쪽 상태(state)와 소켓 자원을 빨리 소모시킬 수 있기 때문에
대표적·효율적인 공격 방식으로 꼽힌다.

HOW?



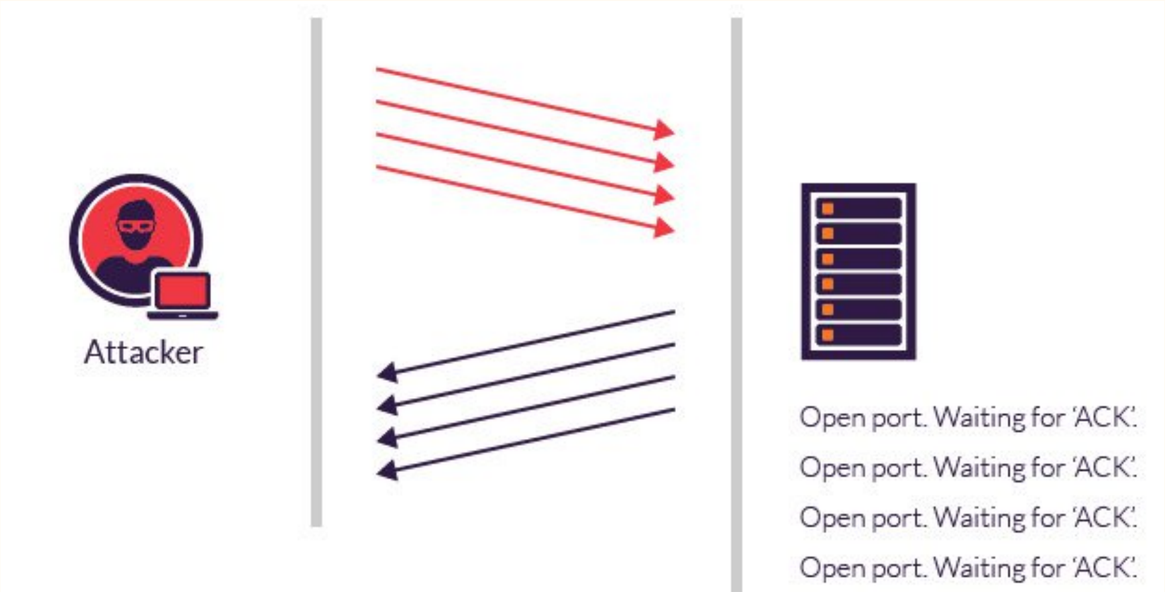
SYN? SYN? SYN?

syn? syn?syn? syn?syn? syn?

H O W ?

공격자(또는 봇)가 대상 서버로 SYN 패킷을 **대량**으로 보냄.

- 단일 클라이언트(단일 IP)에서 반복 전송
- 여러 클라이언트(여러 IP)에서 분산 전송 — DDoS
- 출발지 IP 위조(spoofing)

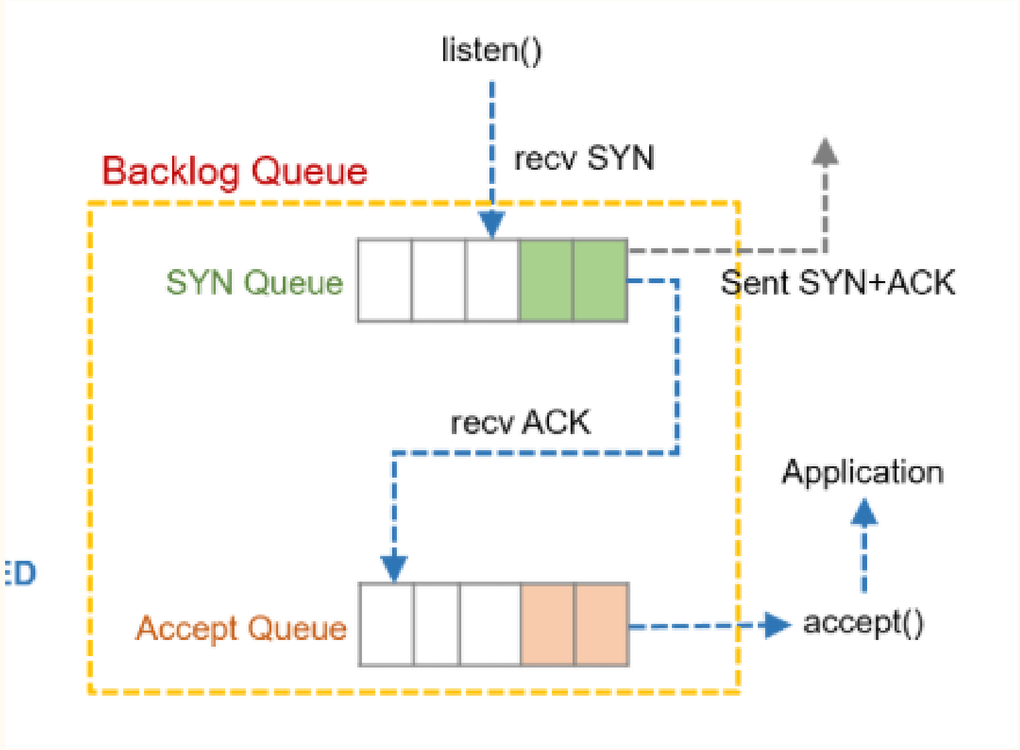


H O W ?

서버는 각 SYN에 대해 SYN+ACK 를 보내고, 연결을 완성하기 위해 ACK 를 기다리며 일부 상태(state)를 예약(half-open).

SYN 큐(또는 incomplete queue):
서버가 SYN을 받고 서버 쪽에서 SYN+ACK를 보낸 뒤 **ACK를 기다리며** 임시로 보관하는 항목들이 들어가는 큐 (half-open 상태).

완성 큐(accept 큐 / completed queue):
클라이언트의 ACK를 받아 핸드쉐이크가 **완료된(ESTABLISHED)** 연결이 들어가서 애플리케이션의 accept()를 기다리는 큐.



HOW?

큐가 꽉 찼다면

새로 들어오는 SYN을 더 이상 위해 할당할 수 없으므로 해당 SYN을 무시(drop)

무시하지 않더라도 많은 지연이 생김

정상적인 클라이언트는 서버랑 통신장애
→ 공격 성공!

대 응 법

이상징후

- SYN 트래픽 급증
- SYN : SYN-ACK 비율이 비정상적으로 높음
  (서버는 응답하지만 연결 완성이 적음).
- SYN_RECV(half-open) 수 증가
-
- 사용자 불만/타임아웃 증가

flooding attack 의심

방화벽이나 DDos 장비에서 같은 IP 주소의 SYN 요청에 대한 임계치를 초과한 경우 해당 연결 요청을 차단

Backlog Queue 크기를 늘려주어 Queue가 full 라는 것을 방지

SYN cookies

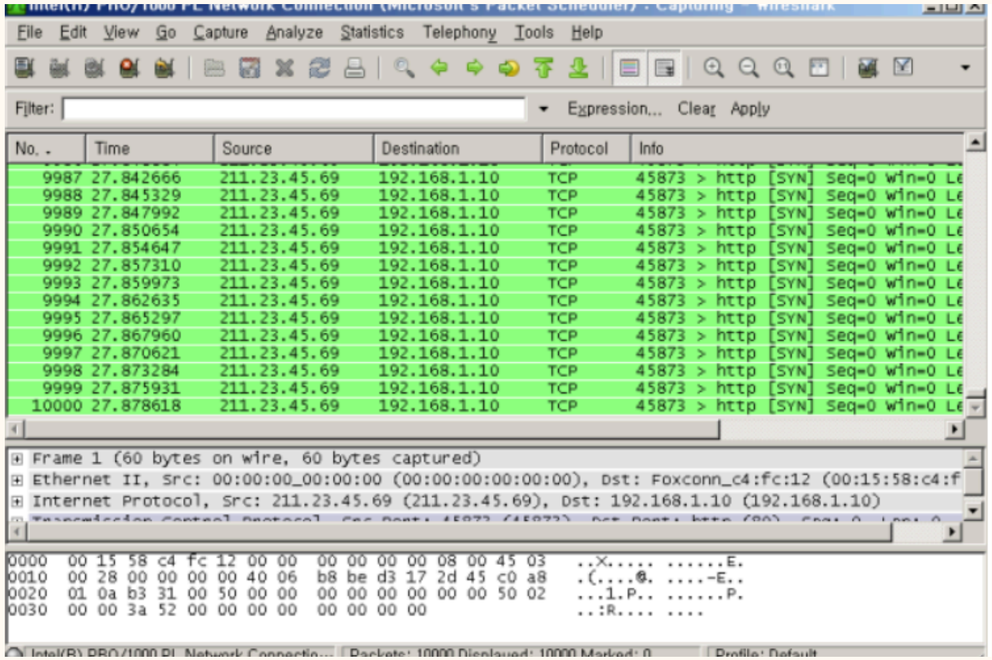
클라이언트가 실제로 ACK로 응답해 올 때만 그 정보를 바탕으로 연결 상태를 재구성하여 자원 소모를 피하는 기법

대 응 법

7	Application Layer
6	Presentation Layer
5	Session Layer
4	Transport Layer

CDN/Anycast, 클라우드 DDoS 서비스(AWS Shield, Cloudflare 등)

rate-limiting, ACL, conntrack 튜닝, ISP 협력



네트워크 공격

설현원

Scanning

네트워크 상의 호스트·포트·서비스·OS 정보를 수집해
'무엇이 열려 있는지' **파악**하는 활동.

공격 전 정찰(공격 표적 선정), 방어 측의 자산 인벤토리 및 취약점 스캔.

- TCP SYN(stealth) 스캔
- TCP Connect 스캔
- UDP 스캔
- ACK/FIN/NULL/XMAS 스캔

Sniffing

네트워크 상을 흐르는 패킷을 캡처·분석해 내용(헤더·페이로드)을 **확인(도청)**하는 행위

평문 HTTP, 쿠키, 세션 토큰, DNS 요청, ARP/LLMNR 트래픽

- 스위치 미러링/SPAN, 네트워크 TAP(수동 복제)
- 호스트의 promiscuous 모드(직접 수신)
- ARP/NDP 스푸핑을 통한 MITM(가로채기)
- 무선 네트워크 모니터링(프레임 캡처)

Spoofing

송신자 정보(IP/ARP/DNS/이메일 등)를 **위조**해 수신자나
중간 장비를 속이는 기법

트래픽 가로채기·중간자 공격, 서비스 장애·정보 탈취,
대규모 반사 DDoS 유발.

- IP 스푸핑: IP 출처 주소를 위조
- ARP/NDP 스푸핑 (LAN)
- DNS 스푸핑 / 캐시 포이즈닝로채기).
- 이메일 스푸핑: 발신자 주소 위조

Hijacking

경로·세션·식별 정보를 조작해 트래픽을 유도하거나 세션을 **탈취**하는 공격의 총칭

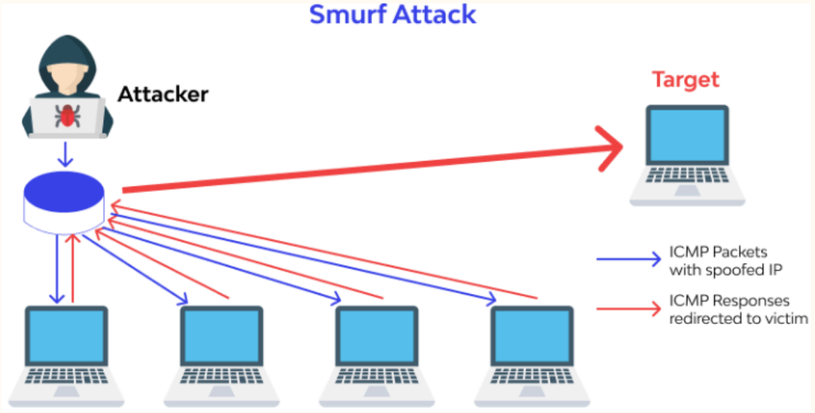
트래픽 , 쿠키, 세션 등 가로채기·감청·우회 또는 서비스 차단 유발.

- BGP 하이재킹
- DNS 하이재킹
- 세션 하이재킹
- BROWSER / OAuth 토큰 하이재킹

Smurfing

네트워크 증폭/반사 공격

공격자가 피해자 IP를 **출발지로 위조**한 ICMP(또는 UDP) 에코 요청을
브로드캐스트 주소로 보내면, 브로드캐스트에 포함된 다수 호스트가 피해자에게 응답해
피해자에게 대량 트래픽이 집중되는 증폭·반사 공격.



- Classic Smurf (ICMP Echo Broadcast)
- Directed-broadcast Smurf
- Distributed Smurf

worm,virus

파일을 손상시키거나 조작하는 **악성** 프로그램

- 웜: 네트워크 기반 자가 전파

자신을 **복제**하여 네트워크 연결을 통해서 다른 컴퓨터로 스스로 전파되고 확산

- 바이러스: 숙주 파일 의존적 전파,

자신 또는 자신의 변형을 복사하는 프로그램으로 가장 큰 특성은
다른 네트워크 컴퓨터로 스스로 전파되지는 않음