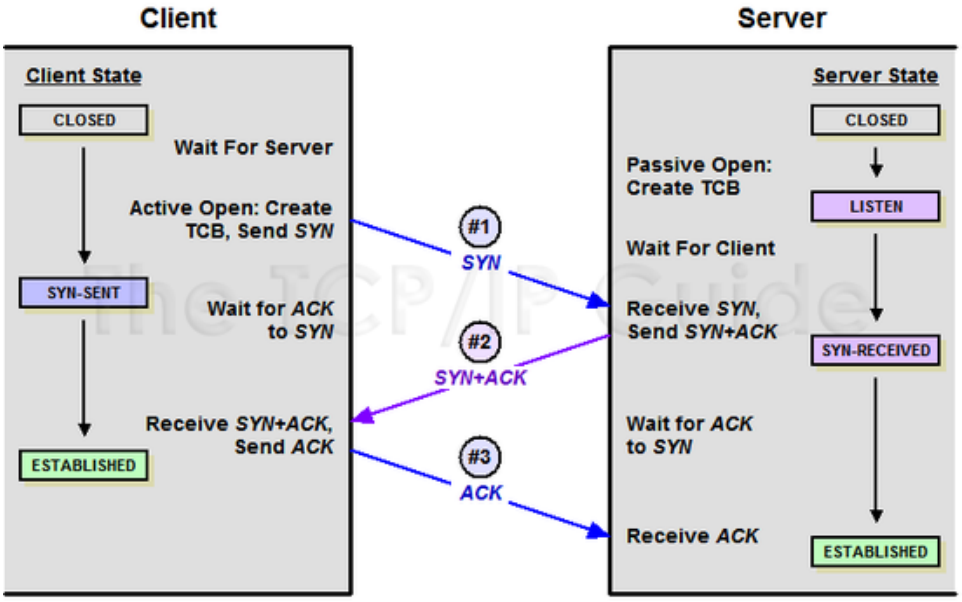
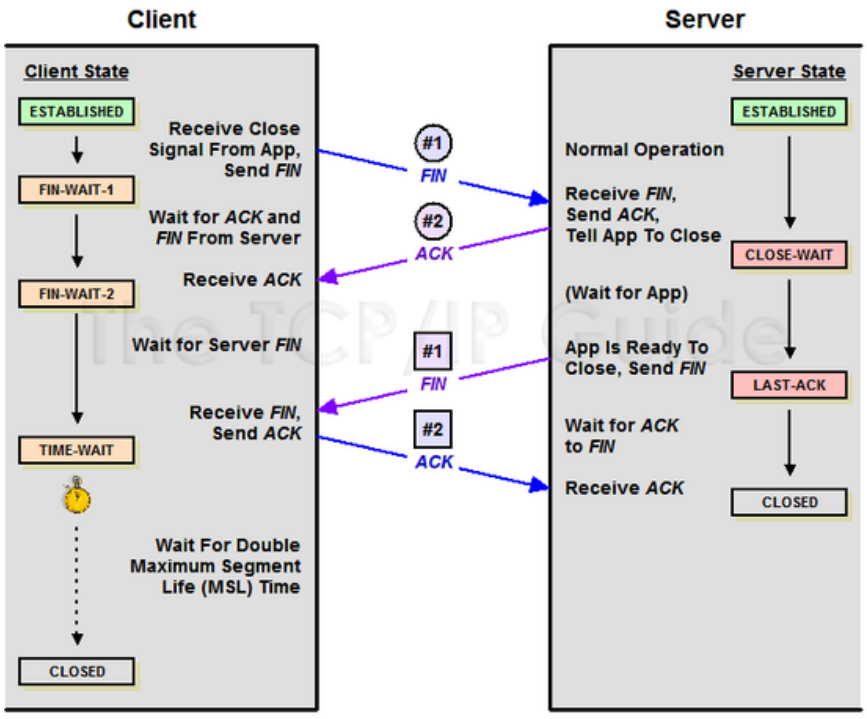
공격들 원리



(TCP의 3-way Handshaking 과정)



(TCP의 4-way Handshaking 과정)
3-Way handshake는 TCP의 연결을 초기화 할 때 사용한다면, 4-Way handshake는 세션을 종료하기 위해 수행되는 절차이다.

land Attack

공겨자가 임의로 자신의 IP 주소와 Port를 공격 대상의 IP 주소와 Port로 변조하여 보내는 공격이다.출발지와 목적지가 같은 패킷을 공격대사에 보내면 공격 대상자는 공격자가 처음 보낸 패킷의 출발지 주소 값을 참조하여 응답 패킷의 목적지 주소를 패킷의 출발지 주소로 설정해서 보내게 된다.

이러면 패킷은 네트워크 밖으로 나가지않고 자신에게 다시 되돌아가게 된다. 또한, 돌아온 패킷의 출발지 IP 주소에는 또 다시 자신의 IP주소가 기록되어 있어 무한 반복이 된다.

수신 되는 패킷 중 출발지 주소와 목적지 주소가 동일한 패킷들을 차단함으로써 이 공격을 막을수있다.

---

tcp/udp Flooding Attack

client가 server로 SYN패킷을 보내면 Server는 SYN/ACK를 보내고 해당 connection을 backlog Queue에 넣어준다. 이 Backlog Queue가 더 꽉차서 더 이상 새로운 connection을 형성을 못하는 경우를 SYN Flooding 이라고 하고 이러한 공격을 SYN Flooding Attack 이라고 한다.

UDP Flooding Attack 이란 Dos 공격의 일종으로 대량의 UDP 패킷을 이용하여 대상 호스트의 네트워크 자원을 소모시키는 공격을 말한다.
UDP Flooding 공격의 경우 SYN Flooding 공격과는 달리 네트워크 bandwidth를 소모시키는 것이 목적이다 따라서, 단일 공격 호스트로는 효과를 볼 수 없기 때문에 DDOS로 구성해서 공격이 이루어진다. 보통 , DDOS를 수행하기 위해 최소 수백대 이상의 Zombie 호스트가 필요하다

RUDY 공격

http 헤더의 content-length 를 이용한다.
content-lenght 는 body 길이를 표시한다.
이 값을 본래 body 길이보다 훨씬 큰값을 적용시켜 모든 body 값이 오지않았으니 세션을 유지하도록 하여 Dos 공격을 시행하게 된다.

Slowloris 공격

HTTP Header 정보를 비정상적으로 조작하여 웹서버가 온전한 Header 정보가 올때까지 기다리도록 한다.
서버가 연결 상태를 유지할 수있는 가용자원은 한계가 있으므로 임계치를 넘어가면 다른 정상적인 접근을 거부하게 된다.
HTTP에선 헤더의 끝은 \r\n 이라는 개행문자로 구분한다.
공격자는 이 마지막 개행문자를 보내지 않고 지속적으로 의미없는 변수를 추가한다.
서버는 헤더정보가 아직 전송중이라고 인신하고 연결을 유지한다.

ICMP Flooding 공격

공격자가 다량의 ICMP 패킷을 서버로 전송하여 서버가 보유한 네트워크의 대역폭을 가득 채워 다른 정상적인 클라이언트의 접속을 원할하지 못하도록 유발시키는 공격이다.

Teadrdrop 공격

Teardrop 공격은 IP Fragmentation 조작 공격 이라도 부르며 IP패킷의 재조합 과정에서 잘못된 fragment offset 정보로 인해 수신 시스템이 문제를 발생하도록 만드는 DOS 공격을 말한다.
공격자는 IP fragment offset 값을 서로 중첩되도록하여 전송하고 이를 수신한 시스템이 재조합하는 과정에서 오류가 발생하는것을 유도한뒤 시스템의 기능을 마비시키는 공격입니다.
