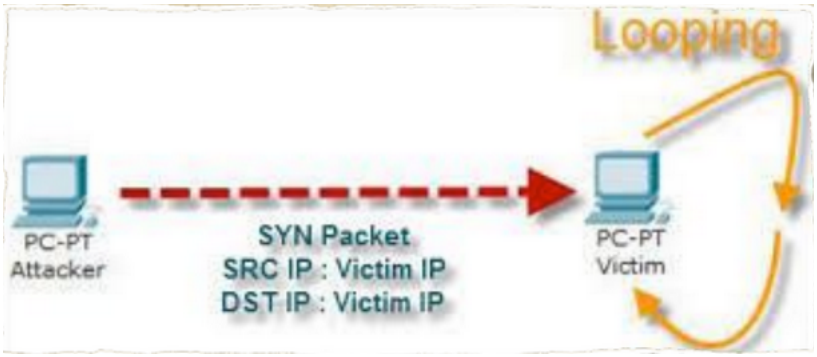
Denial of Service

Denial of Service 란?
-> 서비스 거부 공격
-> 즉 서비스를 막기만 하면 그게 Dos 공격이라는 뜻이다. 주로 논리 공격을 한다.
1990년대에 서버에서 많은 사람들이 접속시 접속을 서비스를 중단하던 것에서 착안해,
90년대 말 Dos 공격으로 응용하게 되었다.

Dos 공격 방식
1. Tear Drop
이거는 ip 패킷 전송이 잘게 나누었다가 다시 재조합 되는 과정을 이용한 공격이다.
보통 ip 패킷은 하나의 큰 자료를 보낼때 잘게 나누어서 보내는다. 이때 offset이라는 걸 이용해서 나누었다가 도착지에서 offset을 이용해 다시 재조합한다.

근데 이때 내가 보내는 패킷 중에 offset을 겹치는게 있게 만들면, 시스템에서 교착 상태가 일어나거나 충돌을 일으킨다.
offset
- 단편화 되어 분할된 패킷을 재구성할 때 사용하는 원본 패킷의 위치 정보를 나타냄.
- TCP 헤더 부분에 있음

2. Land Attack



한 마디로 loop를 만드는 거다. 내가 서버에 그 서버의 ip를 source ip로 하고, dst도 서버의 ip로 설정한다면, 응답을 자기 자신에게 계속 준다. 그러면 결국 네트워크 밖으로 나가지 못해 자기 서버 안에서만 돌게 되어 자원을 고갈시켜 시스템이 다운 된다.

3. Ping of Death
ping은 우리가 ip network를 통해 내가 원하는 호스트에 도달할 수 있는지 테스트 해보는 도구이다.

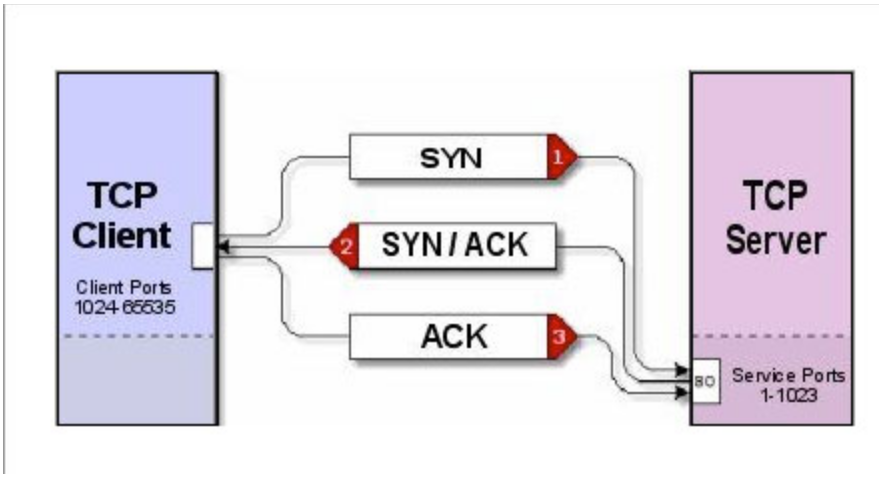
이러한 ping을 이용해서 ICMP 패킷을 정상적인 크기보다 훨씬 크게 만든 다음 네트워크를 통해 라우팅 하면 공격 네트워크에 도달하는 동안 이 패킷은 쪼개져서 Fragment(조각)이 된다.

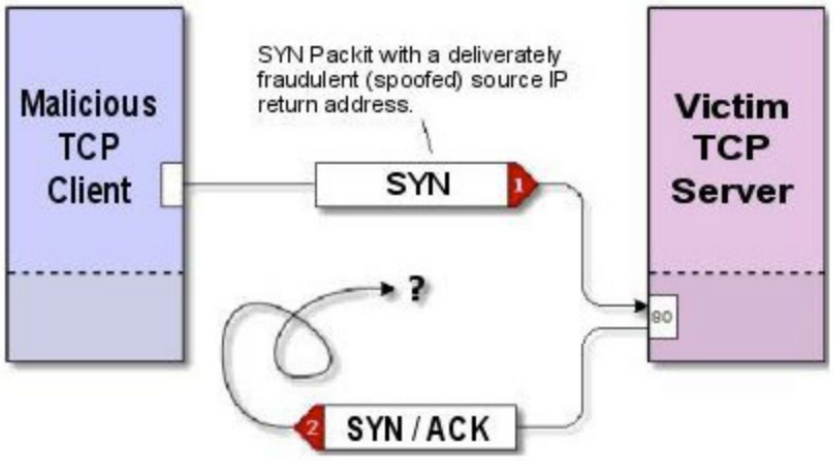
이러면 공격 시스템에서는 작게 쪼개진 아주 많은 Fragment를 처리해야 하므로 정상적인 ping 처리보다 훨씬 많은 부하를 일으킨다.

>ping -n 20000 -l 50000 -a 211.211.211.211
-n : ICMP 패킷을 보내는 횟수
-l : 패킷의 크기
-a : 목표지 주소

4. Syn Flooding

TCP/IP 프로토콜로 통신을 할 때 우리는 Three way hand shake를 하면서 , syn을 주고 받는다. 정상적인 three way hand shake는 다음과 같다.





이번에는 정상적이지 않은 three way hand shake를 보자.

왼쪽 같은 경우는 비정상적인 경우이다.

공격자가 수천, 수만개의 TCP접속 요청 메시지를 서버에게 보낸다고 해보자. 이 때 이 패킷이 내부의 소스 ip 주소를 속이거나, 인터넷 상에서 사용하지 않는 ip값으로 바꾼다면??

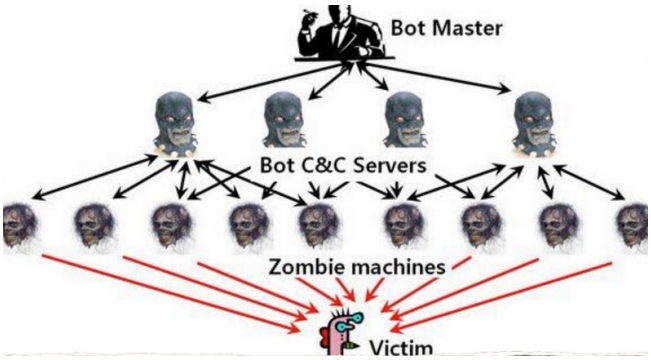
그러면 서버는 실제로 존재하지 않거나 동작하지 않는 ip에게 계속 syn/ack 응답을 하게 되는 것이다.

서버는 클라이언트에게 syn/ack를 보낸 후에 계속 ack를 받기 위해서 기다리게 되는데, 이렇게 되면 서버는 결국 ack 메시지를 받을 때까지 자원을 열어둬서 결국 고갈되어 시스템이 다운되고 만다.

5. HTTP Get Flooding
클라이언트가 get 요청을 다량으로 보내는 것. 서버에 부하 유발.

!!!! 하지만 위의 Dos 공격들은 한계점이 많다.
-> 요즘에는 방화벽이 엄청 잘 막아준다.
-> 패킷 필터링 기능이 서버에 많이 있다.

Dos -> DDos!!! 진화!!!!
-> Distributed- Dos



여러 대의 좀비 피씨를 이용해 Dos 공격을 훨씬 더 많이 가하는 것이다.

Dos vs DDos
도스는 한 지점에서 공격하는 것이고, 디도스는 여러 지점에서 동시에 공격하는 것이다.
이 차이점을 물어보는 질문을 가끔 한다고 한다.
예를 들면 HTTP Get flooding 공격은?? 도스인가 디도스인가?? 라고 물어보면??
-> 일단 질문 자체가 좀 이상한거다. 이거에 대해서 도스입니다. 디도스입니다 답하기는 어려운 것이다.
-> 이 HTTP Get flooding 공격을 여러대가 한번에 공격하는 것인지, 한개의 attacker가 하는것이지 물어보고 답을 해야 하는 것이다.

DDos 7.7 대란
2009년 7월 4일 부터 7일 까지 국내, 외 주요 웹 사이트들을 대상으로 동시다발적인 DDOS 공격이 발생했던 사건이다.

웹 하드의 업데이트 파일들을 모두 악성 프로그램으로 교체하고 총 4개의 C&C서버(명령 제어 서버) 를 이용해서 공격했다.
(좀비피씨 관리서버, 파일 정보 및 수집 서버, 악성 코드 공급 서버, 좀비 피씨 파괴 서버)

이렇게 서버를 구성해서 각 좀비 피씨들이 특정 시간에 일정한 주기로 숙주 서버에 접속해 공격 대상과 공격 시간을 스케줄링 받아 체계적으로 공격했던 사건이다.

그 당시 국내 주요 공격 피해 사이트

구분	국가/공공기관 (7)	금융기관 (7)	민간기관(7)		
			언론사	포털/정보매업체	보안업체
사이트	청와대 국회 국방부 외교통상부 한나라당 국가사이버안전센터 전자민원G4C	농협 신한은행 외환은행 기업은행 하나은행 우리은행 국민은행	조선일보	옥션 네이버(메일) 네이버(블로그) 다음(메일) 파란(메일)	알툴즈 안철수연구소

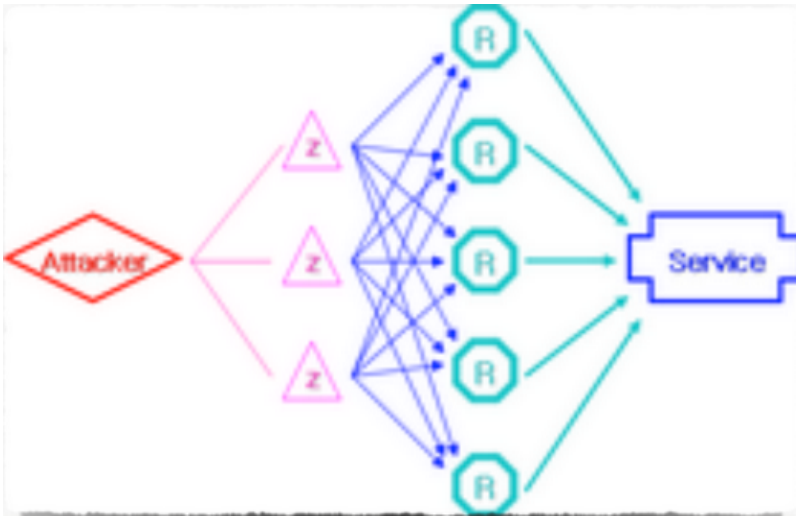
이러한 ddos공격에도 한계는 있다.
-> 다량의 좀비 pc를 확보해야함
-> 이 좀비 pc의 성능도 확보해야 함.

그래서 또 진화된게 DRDos 공격!!!
-> R은 reflection!

반사체라는 개념을 이용한다.
외부 공격자와 타겟과는 아무 상관 없는 서버를 이용하여 공격자는 반사체가 표적을 공격하게끔 유도하는 것이다. ip soopfing이라는 걸 이용한다.

그림 처럼 attacker가 자신의 ip를 공격대상 ip로 속여서 반사체 서버에 패킷을 보낸다. 그러면 반사체는 이 요청에 대한 연결을 하기 위해 확인 절차에 들어간다.(three way hand shake) 근데 ip를 속여서 요청을 보냈으니까 엉뚱하게 공격 대상에게 syn/ack를 보내게 되는 거지. 그러면 공격대상은 이걸 받고 띠용?? 이게 뭐지 라는 입장이 되는 거고.

-> 반사체를 통하기 때문에 공격자 은닉



왼쪽 처럼 좀비 피씨로 DRDos를 할 수 있어서, attacker는 최소의 공격력으로 최대의 공격이 가능해 진다.

하지만 이것도 한계가 있기는 하다
-> ip soopfing자체가 굉장히 오래된 수법이다.

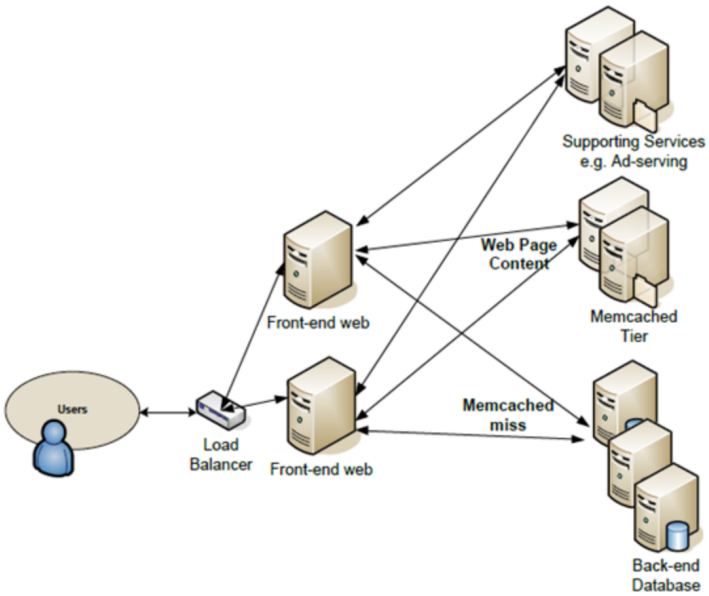
-> 우수한 반사체(버틸 수 있는) 확보가 필요하다.

!! 그래서 요즘 떴던 공격 !!

미라이 봇넷 DDOS(iot기기들 이용)
-> 누군가 미라이라는 이름으로 iot기기들을 숙주로 이용해서 ddos공격을 하는 소스를 공개했고 2016년에 유행한 공격이다. 지금까지도 변형된 공격이 많이 나타난다

-> 대부분의 iot 기기들의 admin id, passwd는 매우 최약하다.
-> 이 iot 기기들을 모두 좀비 피씨로 이용해서 TCP, HTTP, UDP Flooding 기법을 이용해 DDOS 공격을 한다.

맴캐시드 DRDOS공격 (완전 최근 피해도 잇음)
-> '멤캐시드'란 메모리를 사용해 캐시서비스를 제공해 주는 것으로 기업에서 대역폭을 효과적으로 사용하기 위해 구축하게 해준다. 일종의 분산 메모리 캐시시스템이다.



-> 멤캐시드 반사 공격은 공용 네트워크 상에 공개되어 있는 대량의 멤캐시드 서버(분산식 캐시 시스템)에 존재하는 인증과 설계의 취약점을 이용하는 공격이다.

-> 공격자는 멤캐시드 서버 IP주소의 기본 포트인 11211번 포트로 희생자 IP주소로 위장된 특정 명령의 UDP 패킷(stats,set/get 명령 등)을 전송하면 멤캐시드 서버가 희생자 IP로 원래 패킷보다 수배의 패킷(이론상으로는 5만배 까지 가능)을 반사하며 DRDoS 공격을 수행하게 된다.