서비스 거부 공격의 유형과 특징

서비스 거부 공격(Dos)이란 정당한 사용자가 정보 시스템의 데이터나 자원을 적절한 대기 시간 내에 사용하는 것을 방해하는 행위로 시스템에 과부하를 일으켜 정보 시스템의 사용을 방해하는 공격방식이다. 즉 시스템을 악의적으로 공격하여 해당 시스템의 자원을 부족하게 해 원래 시스템의 의도된 용도대로 사용하지 못하게 하는 공격을 말한다. 특정 서버에 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격을 예시로 들 수 있다. 이 공격의 수단이나 동기, 표적 등은 다양하지만, 보통의 경우에는 인터넷 사이트나 서비스의 기능을 방해 또는 중단한다. 주로 유명 사이트, 은행, 공공기관이나 카드회사의 서버를 상대로 이루어진다. 서비스 거부 공격의 특징은 특정 서버에 많은 접속시도를 만들어서 서버의 TCP연결을 바닥나게 하는 공격이나 서버가 감당할 수 없는 많은 트래픽을 만들어 서버를 마비시키거나, 시스템을 공격하여 자원을 부족하게 해 사용하지 못하게 하는 공격으로 나눌 수 있다.

서비스 거부 공격의 유형은 곡격자의 위치에 따라서 내부공격과 외부공격으로 나눌 수 있고, 공격대상에 따라, 특정 네트워크에서 허용하는 대역폭이 모두 소모되게 방법, 대상 시스템의 자원을 고갈시키는 방법, 프로그래밍 오류에 대한 공격으로 서비스를 거부하게 하는 방법들이 있다. 현재 Dos 공격에 이용되고 있는 몇 가지 공격유형은 다음과 같다.

1. SYN Flooding

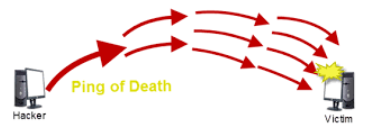
SYN Flooding 공격은 네트워크와 시스템 자원을 대상으로 하는 공격 방법이다. 이 공격 방식은 TCP 연결 과정을 이용하여 공격자가 대상 시스템에 IP address를 Spoofing하여 SYN 패킷을 특정 포트로 전송하면, 이 포트의 대기 큐가 가득 차게 된다. 그러면 포트로 들어오는 연결 요청을 다 무시하게 된다. 이런 방법으로 큐에 들어오는 연결 요청을 다 거부하게 만드는 것이 이 공격의 원리이다.

1. UDP Flooding

UDP(User Datagram Protocol)의 특징은 비연결성과 비신뢰성이다. 이러한 특징들 때문에 UDP는 source address와 port를 Spoofing하기 쉽다. 이런 UDP의 약점을 이용하여 과다한 트래픽을 대상시스템에 전송함으로써 대상 시스템을 마비시키는 원리로 공격이 이루어진다.

1. Ping of Death

대량의 에코 요청(echo request) 패킷을 발생시켜서 서버에 부하를 준다. 시스템을 파괴하는데 가장 많이 사용되었던 초기의 Dos 공격 방법이다. Ping을 이용하여 ICMP(Internet Control Message Protocol) [그림 1]과 같이 패킷을 정상크기보다 훨씬 더 크게 만들면 공격 대상 네트워크에 도달하는 동안 아주 잘게 쪼개져 작은 조각이 된다. 대상 시스템은 이런 식으로 작게 조각난 패킷을 모두 처리해야 하기 때문에 정상적인 Ping보다 훨씬 더 많은 부하가 걸리게 된다. 이러한 원리로 시스템을 과부하 시키는 방법이다.



[그림 1. Ping of Death]

1. Tear Drop

Fragmentation의 취약점을 이용한 공격방법이다. 정상적으로 패킷을 전송할 때 IP Fragmentation이 발생하면 패킷을 재구성할 때 오프셋(offset)이라는 값을 더하게 된다. 하지만 공격자가 오프셋 값을 변형시켜 보내면 패킷을 재구성할 때 시스템이 오류를 일으켜 파괴된다. 따라서 데이터 손실이 발생하게 된다. 즉 이 공격은 시스템에 치명적인 손상을 주기 보다는 대상 시스템의 데이터를 파괴하기 위한 공격이다.

1. LAND attack

Land Attack(**L**ocal **A**rea **N**etwork **D**enial Attack)은 IP spoofing을 이용한 SYN 공격이다. 공격자는 대상 시스템의 IP주소로 출발지 주소를 변경한 TCP SYN 패킷을 보낸다. 패킷을 받은 시스템은 TCP SYN-ACK를 자신에게 보내고, Idle timeout까지 빈 연결(empty connection)을 만들게 된다. 이런 과정을 반복하게 된다면 시스템에는 계속 empty connection이 쌓이게 될 것이고 결국 System Buffer Overflow가 발생하기 된다. 이러한 방식으로 시스템 거부 상태를 만드는 공격이다.

1. Smurf Attack

Smurf Attack 이란, 매우 넓은 범위의 효과로 인해 가장 무서운 DoS 방법 중 하나이다. 이 공격은 IP와 ICMP의 특징을 이용한다. 이 공격은 직접적인 Broadcast와 세 가지 구성요소인 공격자, 증폭 네트워크, 표적을 이용한다. 공격자는 증폭 네트워크의 Broadcast 주소로 공격 서버가 요구하는 것처럼 패킷의 원본 주소를 바꿔 ICMP echo 패킷을 전송한다. 그러면 ICMP echo 패킷을 수신한 증폭 네트워크안의 모든 시스템은 공격 서버에 응답을 하게 된다. 이런 방식으로 광범위하게 공격이 진행된다.