4주차 3차시 서비스거부공격

【학습목표】

1. 서비스거부공격의 개념을 설명할 수 있다.
2. 취약점 공격형, 자원 고갈 공격형, DDoS 공격을 구분할 수 있다.

학습내용1 : 서비스거부공격의 개념 및 취약점 공격형

1. 서비스거부공격의 개념

- 서비스거부공격 → 일종의 훼방

2. 취약점 공격형

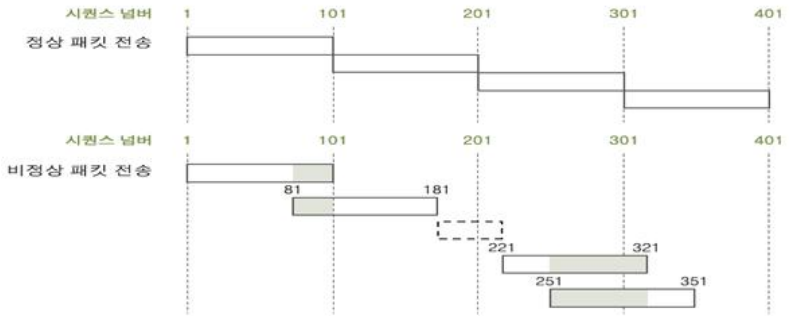
1) Boink, Bonk, TearDrop 공격
* TCP의 신뢰성 있는 연결을 위한 기능 패킷의 순서가올바른지확인
- 중간에 손실된 패킷은 없는지확인
- 손실된 패킷의 재전송요구
- 프로토콜은 이러한 사항이 확인되지 않는 데이터 전송에 대해 신뢰도를 확보하기 위해 반복적인 재요청과 수정을 함

* Boink, Bonk, TearDrop란 : 모두 이러한 반복적인 재요청과 수정을 공격 대상이 계속하게 함으로써 시스템의 자원을 고갈시키는 공격

- TCP 패킷 안에는 각 패킷이 데이터의 어느 부분을 포함하고 있는지를 표시하기 위하여 시퀀스 넘버가 기록되어 있는데, 이러한 공격들은 시스템의 패킷 재전송과 재조합(Reassembling)에 과부하가 걸리도록 이 시퀀스 넘버를 속임
- 시퀀스 넘버가 조작된 패킷의 흐름은 공격 대상에게 절대로 풀 수 없는 퍼즐을 던져주는 것과 같음
- 이러한 취약점은 패치를 통해서 제거되어 옴
- 과부하가 걸리거나 계속 반복되는 패킷은 무시하고 버리도록 처리함

[그림 3-16] Bonk 공격

[그림 3-17] TearDrop 공격 시 패킷의 배치



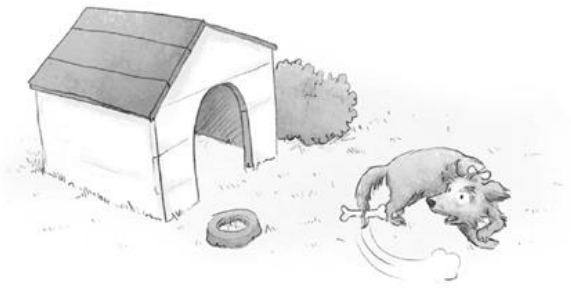
[표 3-6] TearDrop 공격 시 패킷의 시퀀스 넘버

패킷 번호	정상 패킷의 시퀀스 넘버	공격을 위한 패킷의 시퀀스 넘버
1	1~101	1~101
2	101~201	81~181
3	201~301	221~321
4	301~401	251~351

2) Land 공격
* Land 공격이란 : 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소값을 똑같이 만들어서 공격 대상에게 보내는 공격

- 이 때 조작된 IP 주소값은 공격 대상의 IP 주소여야 함
- Land 공격에 대한 보안 대책은 주로 운영체제의 패치 관리를 통해 마련하거나, 방화벽과 같은 보안 솔루션을 이용

[그림 3-18] Land 공격

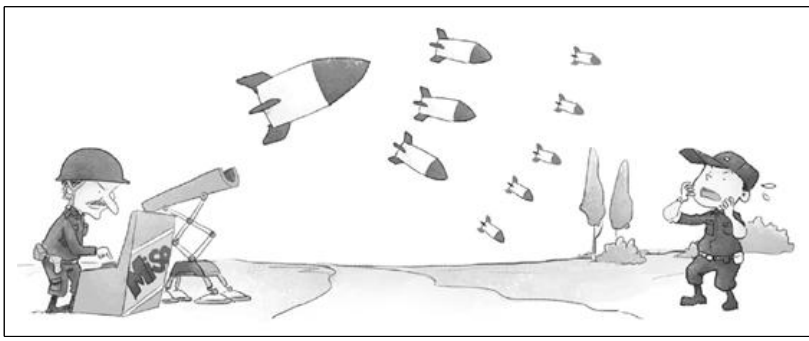


학습내용2 : 자원 고갈 공격형

1. Ping of Death 공격

* Ping of Death 공격이란 : 네트워크에서는 패킷을 전송하기 적당한 크기로 잘라서 보내는데, Ping of Death는 네트워크의 이런 특성을 이용한 것
- 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게 하여(최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게 쪼개져 보내짐

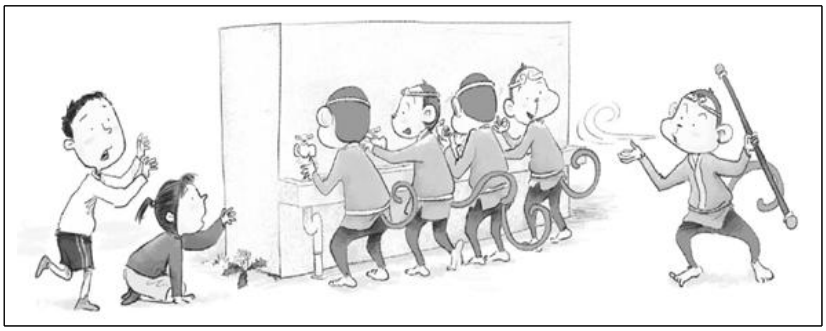
1) [그림 3-19] Ping of Death 공격



2. SYN Flooding 공격

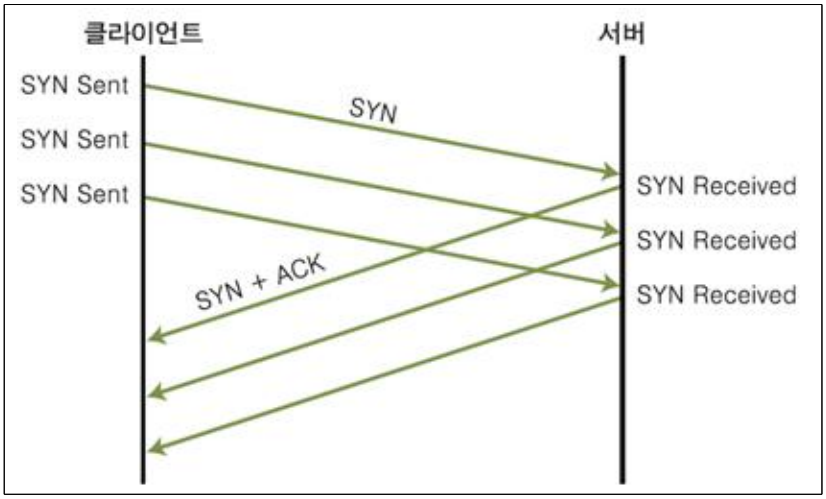
<네트워크에서 서비스를 제공하는 시스템에는 동시 사용자 수에 대한 제한이 있음>
* SYN Flooding 공격이란 : 존재하지 않는 클라이언트가 서버별로 한정되어 있는 접속 가능한 공간에 접속한 것처럼 속여 다른 사용자가 서버의 서비스를 제공받지 못하게 하는 공격

1) [그림 3-20] SYN Flooding 공격



- 서버는 클라이언트가 ACK패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고, 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있음

2) [그림 3-17] SYN Flooding 공격 시 3-웨이 핸드셰이킹



* 공격 차단 방법 : SYN Received의 대기 시간을 줄이는 방법으로 쉽게 해결할 수 있음
- 침입 방지 시스템(IPS)과 같은 보안 시스템을 통해서도 이러한 공격을 쉽게 차단할 수 있음

3. HTTP GET Flooding 공격

* HTTP GET Flooding 공격이란 : 피공격 시스템에 TCP 3-웨이 핸드셰이킹 과정을 통해 정상적인 접속을 한 뒤, 특정한 페이지를 HTTP의 GET Method를 통해 무한대로 실행하는 것

```
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
.....
```

- 공격 패킷을 수신하는 웹 서버는 정상적인 TCP 세션과 함께 정상적으로 보이는 HTTP Get 요청을 지속적으로 요청하게 되므로, 시스템에 과부하가 걸림

4. HTTP CC 공격

- HTTP 1.1 버전의 CC(Cache-Control) 헤더 옵션은 자주 변경되는 데이터에 대해 새롭게 HTTP 요청 및 응답을 요구하기 위하여 캐시(Cache) 기능을 사용하지 않게 할 수 있음
- 서비스 거부 공격 기법에 이를 응용하기 위해 'Cache-Control: no-store, mustrevalidate' 옵션을 사용하면 웹 서버는 캐시를 사용하지 않고 응답해야 하므로 웹 서비스의 부하가 증가하게 됨

5. 동적 HTTP Request Flooding 공격

* 동적 HTTP Request Flooding 공격이란 : 웹 방화벽을 통해 특징적인 HTTP 요청 패턴 차단 기법을 우회하기 위해 지속적으로 요청 페이지를 변경하여 웹 페이지를 요청하는 기법

6. Smurf 공격

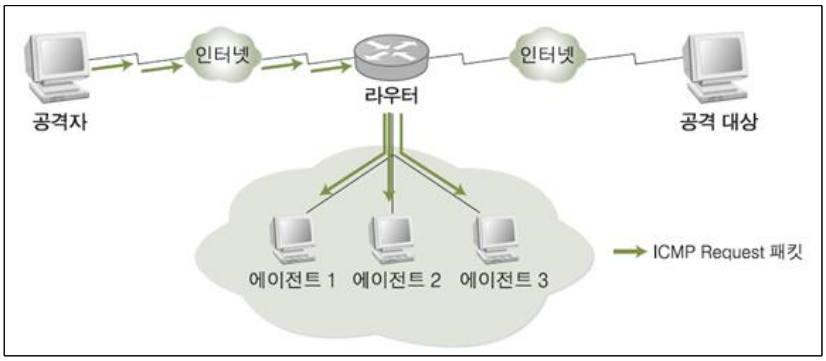
* Smurf 공격이란 : ICMP 패킷과 네트워크에 존재하는 임의의 시스템들을 이용하여 패킷을 확장시켜서 서비스 거부 공격을 수행하는 방법
- 네트워크를 공격할 때 많이 사용

1) [그림 3-22] smurf 공격

* 다이렉트 브로드캐스트(Direct Broadcast)의 이해
: 기본적인 브로드캐스트는 255.255.255.255의 목적지
IP 주소를 가지고 네트워크의 임의의 시스템에 패킷을 보내는 것으로, 3계층 장비(라우터)를 넘어가지 못함

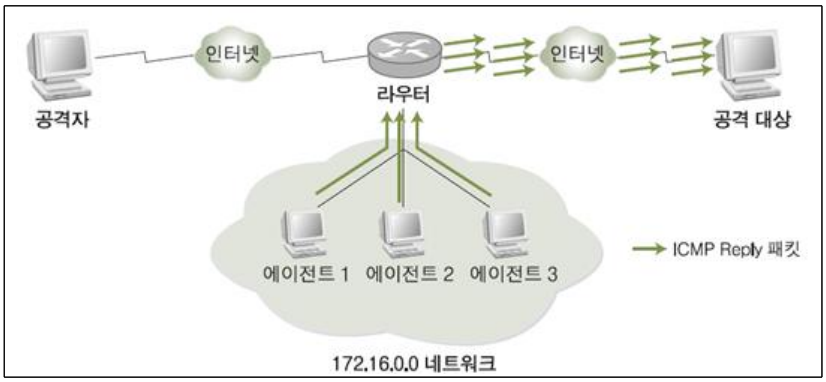
- 172.16.0.255와 같이 네트워크 부분(172.16.0)에 정상적인 IP를 적어주고, 해당 네트워크에 있는 클라이언트의 IP 주소 부분에 255, 즉 브로드캐스트 주소로 채워서 원격지의 네트워크에 브로드캐스트를 할 수 있는데 이를 다이렉트 브로드캐스트라고 함
- 공격자가 172.16.0.255로 다이렉트 브로드캐스트를 하면 패킷이 다음과 같이 전달됨

2) [그림 3-23] 공격자에 의한 에이전트로의 브로드캐스트



- ICMP Request를 받은 172.16.0.0 네트워크는 ICMP Request 패킷의 위조된 시작 IP 주소로 ICMP Reply를 다시 보냄
- 결국 공격 대상은 수많은 ICMP Reply 를 받게 되고 Ping of Death처럼 수많은 패킷이 시스템을 과부하 상태로 만듦

3) [그림] 에이전트에 의한 스머프 공격의 실행



7. Mail Bomb 공격

- 흔히 폭탄 메일이라고 함
- 스팸 메일도 여기에 해당
- 메일 서버는 각 사용자에게 일정한 양의 디스크 공간을 할당하는데, 메일이 폭주하여 디스크 공간을 가득 채우면 정작 받아야 하는 메일을 받을 수 없음
- 즉 스팸 메일도 서비스 거부 공격이 될 수 있음

학습내용3 : 분산 서비스 거부(DDoS) 공격

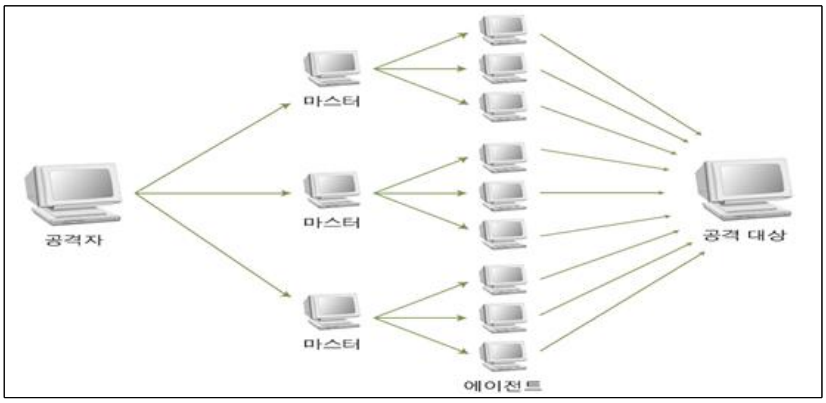
1. 분산 서비스 거부(DDoS) 공격이란?

<1999년 8월 17일 미네소타 대학에서 발생한 것으로 알려져 있음>

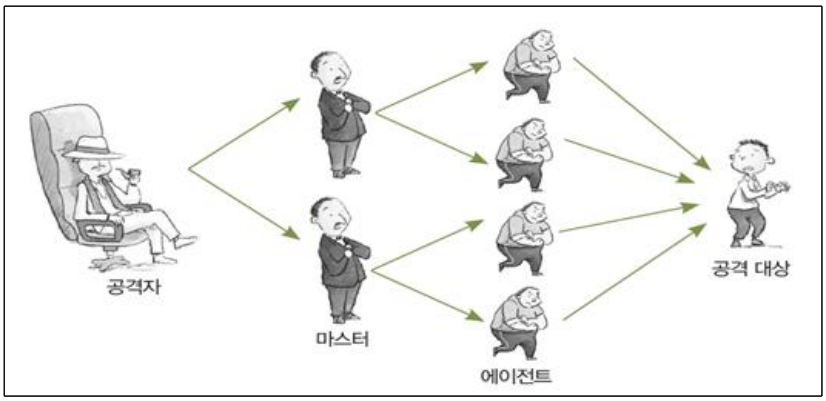
- 야후, NBC, CNN 서버의 서비스를 중지시킴
- 피해가 상당히 심각하며 이에 대한 확실한 대책 역시 없고 공격자의 위치와 구체적인 발원지를 파악하는 것도 거의 불가능에 가까움
- 대부분의 공격 → 특성상 자동화된 툴을 이용
- 공격의 범위가 방대하며 DDoS 공격을 하려면 최종 공격 대상 이외에도 공격을 증폭시켜주는 중간자가 필요함

1) 분산 서비스 거부 공격에 사용되는 구성
① 공격자(Attacker) : 공격을 주도하는 해커의 컴퓨터
② 마스터(Master) : 공격자에게 직접 명령을 받는 시스템으로 여러 대의 에이전트를 관리함
③ 핸들러(Handler) 프로그램 : 마스터 시스템의 역할을 수행하는 프로그램
④ 에이전트(Agent) : 공격 대상에 직접 공격을 가하는 시스템
⑤ 데몬(Daemon) 프로그램 : 에이전트 시스템의 역할을 수행하는 프로그램

2) [그림] 분산 서비스 거부 공격도

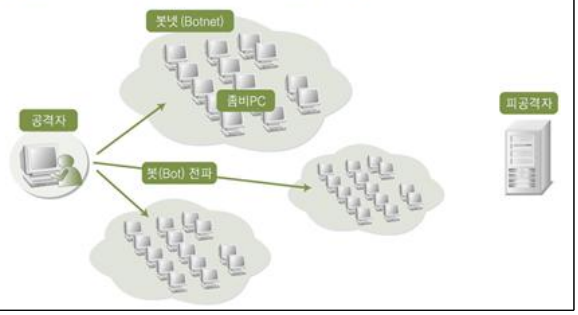


3) [그림] 분산 서비스 거부 공격의 개념도

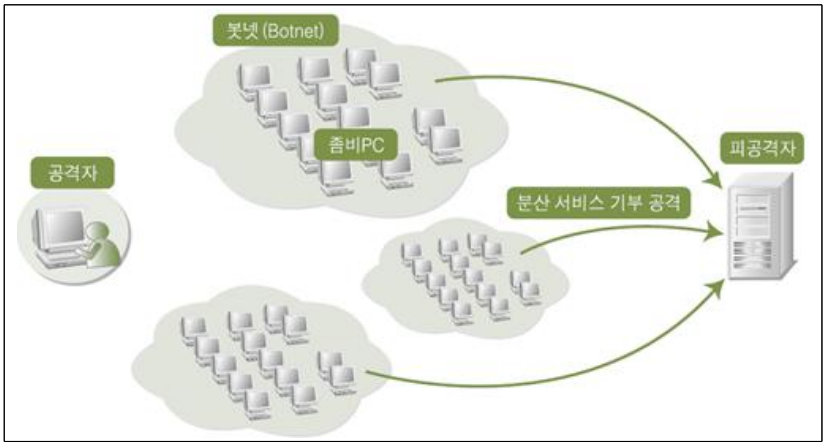


4) 최근의 분산 서비스 거부 공격은 악성코드와 결합하는 형태
- PC에서 전파가 가능한 형태의 악성코드를 작성
- 분산 서비스 거부 공격을 위해 사전에 공격 대상과 스케줄을 정한 뒤 이를 작성한 악성코드에 코딩
- 악성코드(분산 서비스 거부 공격에 사용되는 악성코드를 봇(Bot)이라고 함)가 인터넷을 통해 전파되도록 함
    - 전파 과정에서는 별다른 공격이 이뤄지지 않도록 잠복함
    - 악성코드에 감염된 PC를 좀비 PC라고 부르며, 좀비 PC끼리 형성된 네트워크를 '봇넷(Botnet)'이라고 부름
- 공격자가 명령을 내리거나 정해진 공격 스케줄에 따라 봇넷으로 형성된 좀비 PC들이 일제히 공격 명령을 수행하여 대규모의 분산 서비스 거부 공격이 가능해짐

[그림 3-27]
악성코드(봇)에 의한 분산 서비스 거부 공격 에이전트 전파



5) [그림] 좀비 PC에 의한 분산 서비스 거부 공격 수행



【학습정리】

1. 취약점공격형은 Boink, Bonk, TearDrop이 있으며 반복적인 재요청과 수정을 공격 대상이 계속하게 함으로써 시스템의 자원을 고갈시키는 공격이다.

2. 자원 고갈 공격형은 Ping of Death 공격, SYN Flooding 공격, HTTP GET Flooding 공격, 동적 HTTP Request Flooding 공격, Smurf 공격, Mail Bomb 공격 등이 있다.

3. 분산 서비스 거부(DDoS) 공격은 악성코드와 결합하는 형태로 변하고 있으며 악성코드가 인터넷을 통해 전파되도록 설계되었으며 전파 과정에서는 별다른 공격이 이뤄지지 않도록 잠복한 후 정해진 시점에 일시에 공격을 시도 한다.