

네트워크 고전 해킹 기법의 이해

by DongKi, Yeo (superdk@hanmail.net)

2008. 06.

이 글의 목표는 네트워크 고전 해킹 기법의 원리를 정확하게 이해하여, 네트워크 프로토콜을 이용한 공격이 무엇인지를 이해하고, '전문가'라 불리는 사람들까지도 최근 중국에서 빈번하게 시도하고 있는 DDoS 공격을 손쉽게 방어하지 못하고, 결국에는 공격에 노출될 수 밖에 없는지에 대해 보안에 관심이 있는 사람들에게까지 알려져 이 문제의 심각성을 인식할 수 있는 계기를 마련하고자 한다.

더불어, 더 많은 사람들이 DDoS 공격의 심각성을 인식하여 자신의 PC가 botnet의 숙주 PC가 되지 않도록 하기를 바라는 마음이다.

목차

1. Prologue
2. (TCP) SYN Flooding
3. Land Attack
4. Smurf Attack
5. Ping of Death
6. Tear Drop
7. DoS (Denial of Service) & DDoS (Distributed Denial of Service)
8. DRDoS (Distributed Reflection DoS)
9. Epilogue

1. Prologue

먼저, 본문에서 구현된 모든 공격실습은 실제 네트워크에 피해를 발생시키지 않도록 저자가 공격자와 대상자만이 존재하는 실습용 네트워크를 만들어서 테스트 한 것이므로, 이 글을 읽은 독자는 일반 네트워크에서 동일한 테스트를 하면 안된다는 것을 분명히 기억해야 한다.

그리고, 이 글을 읽은 호기심이 많은 독자가 직접 실습을 해봤을 때, 여기에서 설명된 고전 기법인 (TCP) SYN Flooding, Tear Drop 등의 네트워크 공격기법으로 인한 대상 서버의 Crash를 유발시키지 못할 수 있다. 왜냐하면 이러한 공격기법이 사용되었던 때와 비교해서, 독자의 컴퓨터 사양이 너무 우수하기 때문이다.

이러한 현실 때문에 공격자 입장에서는 "1-tier -> 2-tier(DoS) -> 3-tier(DDoS)"와 같이 보다 많은 트래픽을 발생시킬 수 있는 구조로 공격 기법이 진화될 수 밖에 없었던 과정을 자연스럽게 이해할 수 있을 것이다.

다음으로, 본문에서 사용된 용어와 프로그램에 대해서 아래의 의미를 두고 사용하였으니, 이를 기억하고 본문을 읽는다면 필자의 의도를 보다 정확하게 파악할 수 있을 것이다.

가) 용어

1. Client: 접속을 요청하는 Sender로 공격자(Attacker)를 의미한다.
2. Server / 대상 서버(PC): 접속을 받아들이는 Receiver로 희생자(Victim)를 의미한다.
3. Botnet: 관리 프로그램의 제어를 받아 DDoS 공격에 사용되는 Worm.
4. Src IP / Dst IP: Source IP / Destination IP의 약어

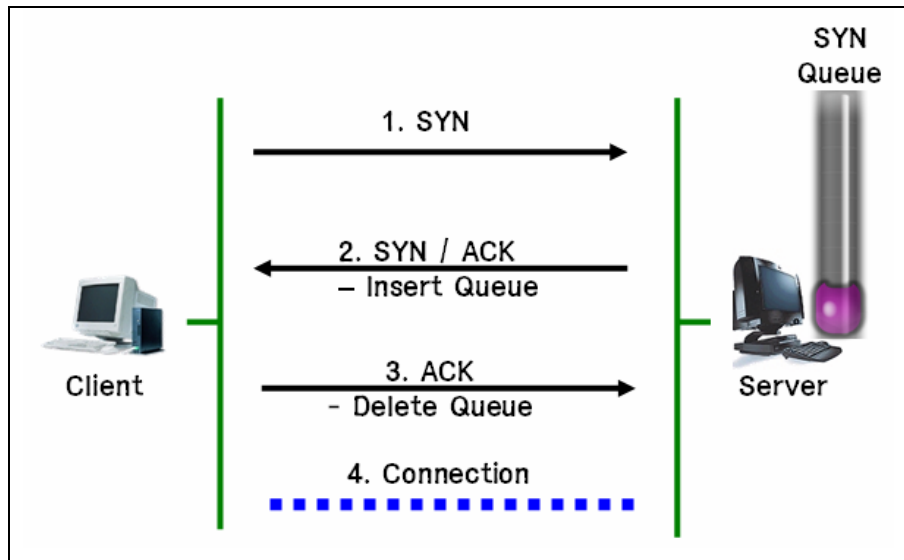
나) 프로그램

1. Wireshark: Windows OS 용 패킷 캡처 프로그램 (Freeware)
2. hping: 패킷 생성 프로그램 (Freeware)
3. 보안장비: Watch Mode 방어의 예에서는 Juniper Netscreen Firewall을 사용함.
4. smurf: smurf 공격이 구현된 Open Source
5. teardrop: teardrop 공격이 구현된 Open Source

2. (TCP) SYN Flooding

2-1.TCP 3-Way handshaking

TCP Connection은 반드시 3-Way handshaking 과정을 거친 후 Session을 형성하고, 통신이 시작된다. 그러므로, 이 과정을 이용한 공격을 이해하기 위해서는 먼저, 이 과정을 이해하여야 하므로, TCP 3-Way handshaking 이 무엇인지를 먼저 살펴보자.



(그림 2-1-1)

위의 (그림 2-1-1)을 순서대로 설명하면 아래와 같다.

1. 접속을 원하는 Client에서 접속을 허용할 Server로 SYN Packet을 보낸다.
2. Server에서는 이 SYN Packet에 대해서 접속할 준비가 되었다는 의미로 SYN/ACK Packet을 Client로 보낸다.(이 때, Server의 SYN Queue에 해당 정보가 Insert 된다.)
3. Client는 지금 접속을 하겠다는 의미로 Server에게 ACK Packet을 보내게 되고,
(이 ACK Packet을 받게 되면, Server의 SYN Queue에서 해당 정보가 Delete 된다.)
4. Client와 Server 사이에는 Session이 형성되며, 통신이 시작된다.

패킷 캡처 프로그램인 Wireshark를 이용하여 대표적인 TCP 통신인 HTTP 접속시의 패킷을 캡처하여 위의 과정이 이루어지는지를 확인해 보자.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.20	211.115.77.212	TCP	1915 > http [SYN] Seq=0 Len=0 M...
2	0.018901	211.115.77.212	192.168.0.20	TCP	http > 1915 [SYN, ACK] Seq=0 Ack...
3	0.018949	192.168.0.20	211.115.77.212	TCP	1915 > http [ACK] Seq=1 Ack=1 W...
4	0.019074	192.168.0.20	211.115.77.212	HTTP	GET / HTTP/1.1

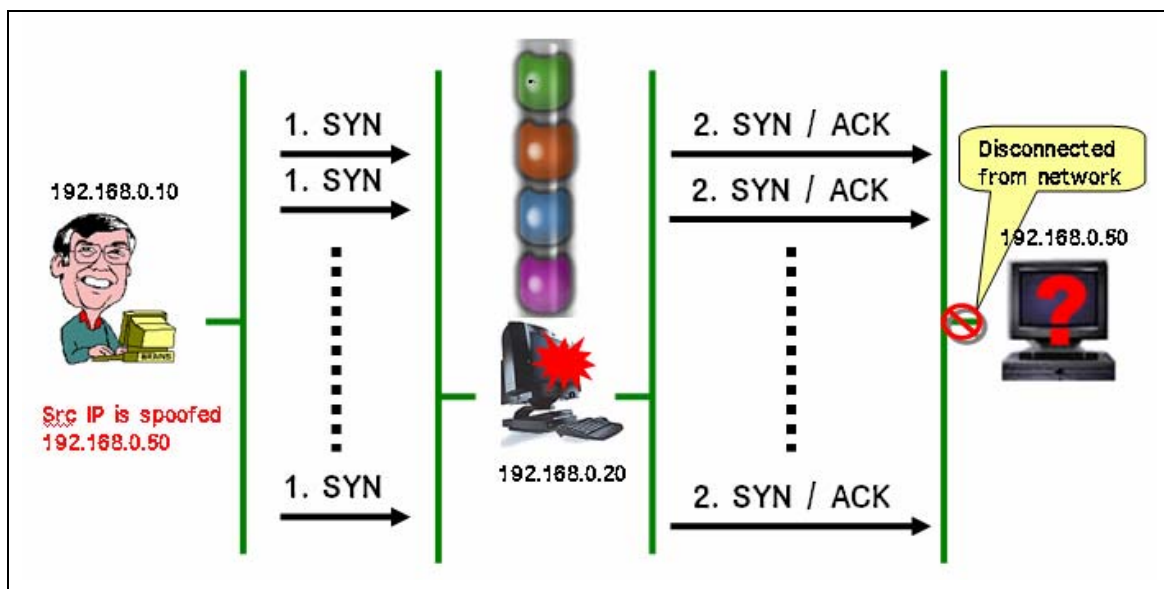
(그림 2-1-2)

실제 패킷을 캡처한 (그림 2-1-2)에서 보는 바와 같이 위와 순식간에 일어나는 일이라서 사용자들이 의식하지 못할 뿐, 모든 TCP Connection에서는 이와 같은 선행 과정이 실제로 일어난다.

(그림 2-1-2)을 자세히 보면, “SYN -> SYN, ACK -> ACK -> Get / HTTP/1.1”의 순서로 (그림 2-1-1)에서 설명한 3-Way handshaking 과정을 정확하게 거치고 홈페이지의 내용을 읽어오는 것을 볼 수 있다.

2-2. SYN Flooding

“SYN Flooding”이란 SYN을 넘치게 한다는 말이다. 즉, Client가 서버의 SYN Queue를 Overflow시켜서 서버를 오동작시키거나 Crash시키는 기법이다. 이 때 정상적인 IP로 대상 서버에 SYN 패킷을 보내면 위의 3-Way handshaking 개념에서 본 것과 같이 서버의 SYN Queue는 정상적으로 비워진다. 그러므로, 반드시 비정상적인 IP로 SYN Packet을 보내서 Client로부터 ACK Packet을 받지 못하도록 하여야 한다. 여기에서 말하는 “비정상적인 IP”는 반드시 네트워크에 존재하지 않는 IP여야만 한다.



(그림 2-2)

위의 (그림 2-2)를 순서대로 설명하면 아래와 같다.

1. 공격자는 존재하지 않는 IP로 Spoofing하여 대상 서버에 SYN Packet을 보낸다.
2. 서버는 Source IP인 “192.168.0.50”으로 SYN/ACK Packet을 보내지만,
“192.168.0.50”컴퓨터는 네트워크에 존재하지 않으므로, 서버에 “ACK” 신호를 보낼 수 없다. 그러므로, 서버에서는 SYN Queue의 내용이 지워지지 않는다.
3. 공격자는 대상 서버에 이러한 SYN Packet을 무한히 많이 보낸다.
4. 결국 대상 서버의 Queue에는 Insert만 되고, Delete가 되지 않기 때문에 서버의 SYN Queue가 Overflow 된다.
5. 서버가 오동작하거나 Crash 된다.

2-3. SYN Flooding 공격 예

2-3-1. 환경

* **Sender IP: 192.168.0.10** (단, "192.168.0.50" 이 네트워크에 없는 것을 확인)

```
[root@ground root]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:00:E2:59:C7:4B
          inet addr:192.168.0.10 Bcast:192.168.0.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:436 errors:0 dropped:0 overruns:0 frame:0
          TX packets:154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:48301 (47.1 Kb)  TX bytes:19216 (18.7 Kb)
          Interrupt:11 Base address:0x9000 Memory:81a00000-81a00038

[root@ground root]# ping 192.168.0.50
PING 192.168.0.50 (192.168.0.50) 56(84) bytes of data.
From 192.168.0.10 icmp_seq=1 Destination Host Unreachable
From 192.168.0.10 icmp_seq=2 Destination Host Unreachable
From 192.168.0.10 icmp_seq=3 Destination Host Unreachable
From 192.168.0.10 icmp_seq=4 Destination Host Unreachable
```

* **Receiver IP: 192.168.0.20** (단, "192.168.0.50" 이 네트워크에 없는 것을 확인)

```
C:\Documents and Settings\superdk>ipconfig
```

Windows IP Configuration

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix  . :
IP Address. . . . . : 192.168.0.20
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.254
```

```
C:\Documents and Settings\superdk>ping 192.168.0.50
```

Pinging 192.168.0.50 with 32 bytes of data:

Request timed out.

2-3-2. 공격의 예

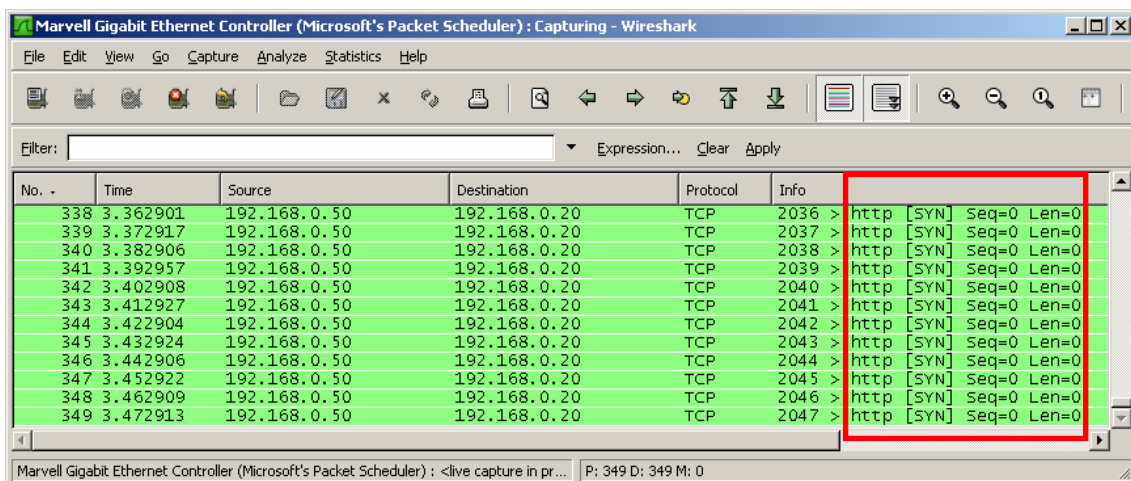
```
[root@ground root]# hping 192.168.0.20 -a 192.168.0.50 -p 80 -S -i u10000
HPING 192.168.0.20 (eth0 192.168.0.20): S set, 40 headers + 0 data bytes

--- 192.168.0.20 hping statistic ---
349 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@ground root]#
```

위 공격의 예를 설명하면 다음과 같다.

Src IP를 "192.168.0.50"으로 Spoofing하여, Dst IP "192.168.0.20"와 Dst Port 80으로 SYN Packet을 초당 10개씩 보내라.

2-3-3. Receiver 에서 해당 패킷 캡처 화면

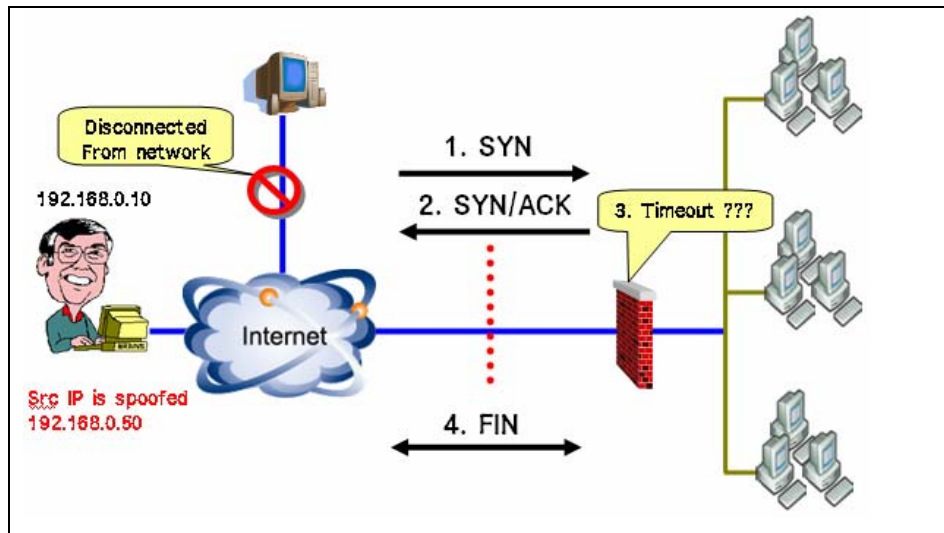


(그림 2-3-3)

위의 (그림 2-3-3)에서 캡처된 것과 같이, 들어오는 SYN 패킷이 존재하지만, Src IP(192.168.0.50)가 존재하지 않으므로 응답을 할 수 없기 때문에, "SYN_ACK" 패킷이나 "ACK" 패킷이 없고, seq 값도 변함이 없는 것을 볼 수 있다.

2-4. SYN Flooding 방어 방법

다양한 방법이 있다. 하지만 개념을 이해한다는 의미에서 대표적인 방법인 Watch Mode를 이해하자.



(그림 2-4)

위의 (그림 2-4)를 순서대로 설명하면 아래와 같다.

1. 대상 서버의 앞에 있는 라우터/방화벽 장비에서 SYN Packet을 감시한다.
2. 내부에서 SYN/ACK Packet을 보낸 후,
3. 외부에서 다시 이에 해당하는 ACK Packet이 오기까지의 시간을 측정한다.
(SYN Flooding 공격이라면 ACK Packet이 정해진 시간 동안 올 리가 없다.)
4. 정해진 시간을 초과하면, 라우터/방화벽 장비에서 FIN Packet을 보내서 연결을 종료시키게 되고, 대상 서버는 SYN Queue에 있는 해당 내용을 지운다.

2-5. SYN Flooding 방어를 Watch Mode로 설정하는 화면

초보 수준의 독자라면 약간 어이가 없을 수도 있겠지만, SYN Flooding과 같이 이미 알려진 기초적인 기법에 대해서는 (그림 2-5)에서 보는 바와 같이 보안장비(방화벽)에서 옵션 체크만 해주면 방어가 된다.

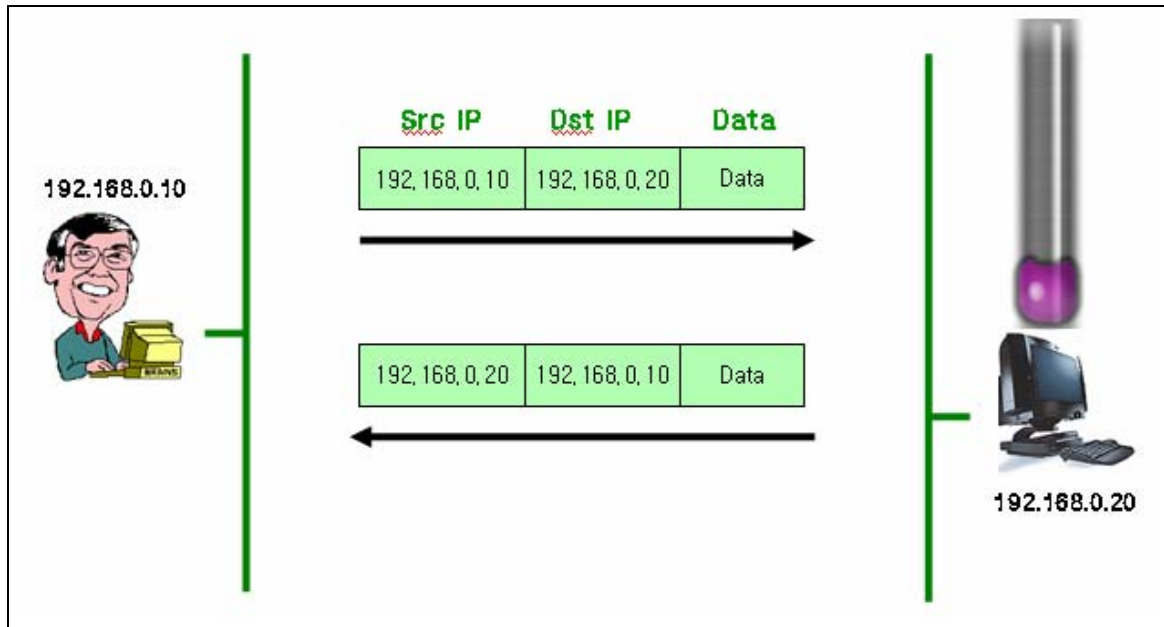
Flood Defense	
<input type="checkbox"/> ICMP Flood Protection	Threshold <input type="text" value="1000"/> pps
<input type="checkbox"/> UDP Flood Protection	Threshold <input type="text" value="1000"/> pps
<input type="text" value="Destination IP"/>	
<input checked="" type="checkbox"/> SYN Flood Protection	Threshold <input type="text" value="200"/> pps
	Alarm Threshold <input type="text" value="1024"/> pps
	Source Threshold <input type="text" value="4000"/> pps
	Destination Threshold <input type="text" value="40000"/> pps
	Timeout Value <input type="text" value="20"/> Seconds
	Queue Size <input type="text" value="10240"/>

(그림 2-5)

3. Land Attack

3-1. 정상적인 패킷의 흐름

(그림 3-1)에서 보는 것과 같이 정상적인 패킷은 자신의 IP를 Source IP로 하고, 대상의 IP를 Destination IP로 해서 Receiver에게 패킷을 보내게 된다.



(그림 3-1)

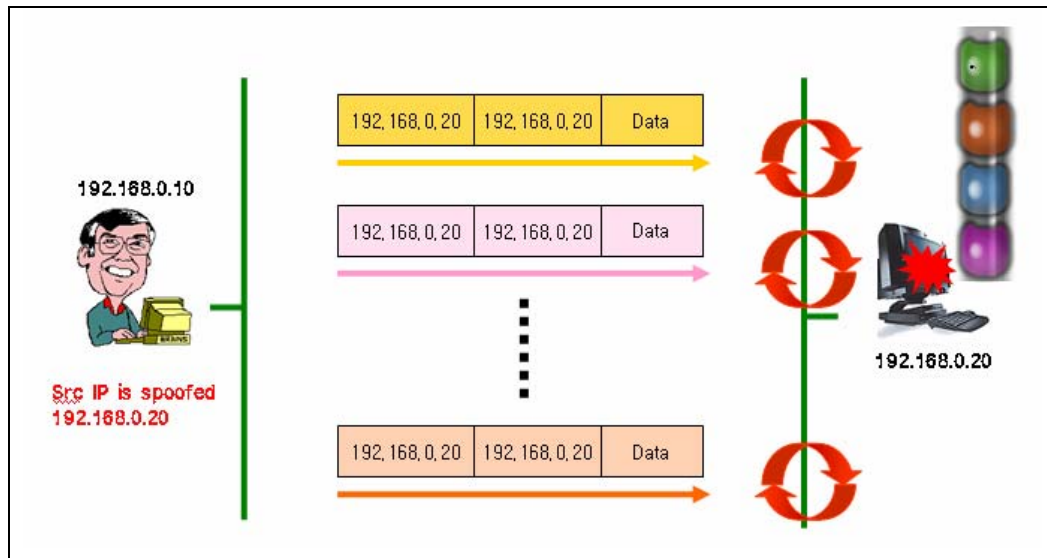
위의 (그림 3-1)을 순서대로 설명하면 아래와 같다.

1. Sender는 Receiver에게 자신의 IP (192.168.0.10)를 Src IP로 하고, Receiver의 IP 192.168.0.20를 Dst IP로 하여 패킷을 보낸다.
2. Receiver는 Sender가 보낸 패킷을 받고, 응답을 한다.
(단, 이때에는 자신(192.168.0.20)이 Sender가 되고, Src IP는 "192.168.0.20"이 되고, Dst IP는 "192.168.0.10"이 된다.)

3-2. Land Attack

"Land Attack"은 전기/전자 이론에 나오는 접지(Ground)를 바닥이 아닌 자기 자신에게 연결한 모양을 연상하면 되는 공격 방법으로 간단한 공격 개념은 아래와 같다.

- Client가 대상 서버로 패킷을 보낼 때, Source IP를 대상 서버의 IP로 Spoofing 하고, Port 정보도 Source / Destination Port 모두를 동일하게 변조한다.
- 대상 서버는 자신이 보낸 적이 없는 Packet을 받게 되고, 이 Packet을 처리하지 못하여 Crash 되거나, 오동작을 한다.



(그림 3-2)

위의 (그림 3-2)를 순서대로 설명하면 아래와 같다.

1. 공격자는 대상자의 IP로 Spoofing하여 대상 서버에 Packet을 지속적으로 보낸다.
2. 서버는 자신이 보낸 적이 없는 이러한 패킷을 처리하지 못하거나, 힘들게 처리하게 된다.
3. 공격자는 지속적으로 대상자에게 이러한 패킷을 보낸다.
4. 결국 서버는 즉시 Crash 되거나, 오동작을 하게 된다.

3-3. Land Attack 예

3-3-1. 공격의 예

```
[root@ground ~]# hping 192.168.0.20 -a 192.168.0.20 -s 100 -p 100 -S -c 100
HPING 192.168.0.20 (eth192.168.0.20): S set, 40 headers + 0 data bytes
```

위 공격의 의미를 설명하면 다음과 같다.

Src IP를 "192.168.0.20"으로 Src Port를 80으로 Spoofing하여, Dst IP "192.168.0.20"과 Dst Port 100에 SYN Packet을 보내라.

3-3-2. Receiver 에서 해당 패킷 캡처 화면

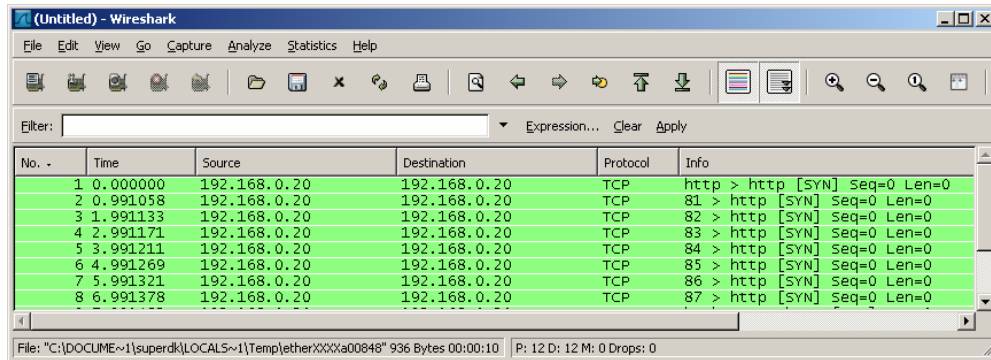
```
[root@test root]# tcpdump -nei eth0 host 192.168.0.20 and port 100
tcpdump: listening on eth0
10:44:11.106556 0:c0:9f:26:6f:a1 78:6:17:38:f:59 ip 60: 192.168.0.20.100 >
192.168.0.20.100: S 965068398:965068398(0) win 512
10:44:12.107852 0:c0:9f:26:6f:a1 78:6:17:38:f:59 ip 60: 192.168.0.20.hostname
> 192.168.0.20.100: S 511956757:511956757(0) win 512
10:44:13.108677 0:c0:9f:26:6f:a1 78:6:17:38:f:59 ip 60: 192.168.0.20.iso-tsap
```

```

> 192.168.0.20.100: S 339688020:339688020(0) win 512
10:44:14.109475 0:c0:9f:26:6f:a1 78:6:17:38:f:59 ip 60: 192.168.0.20.103 >
192.168.0.20.100: S 861288640:861288640(0) win 512
10:44:15.110239 0:c0:9f:26:6f:a1 78:6:17:38:f:59 ip 60: 192.168.0.20.104 >
192.168.0.20.100: S 455383108:455383108(0) win 512

```

(결과 3-3-2)



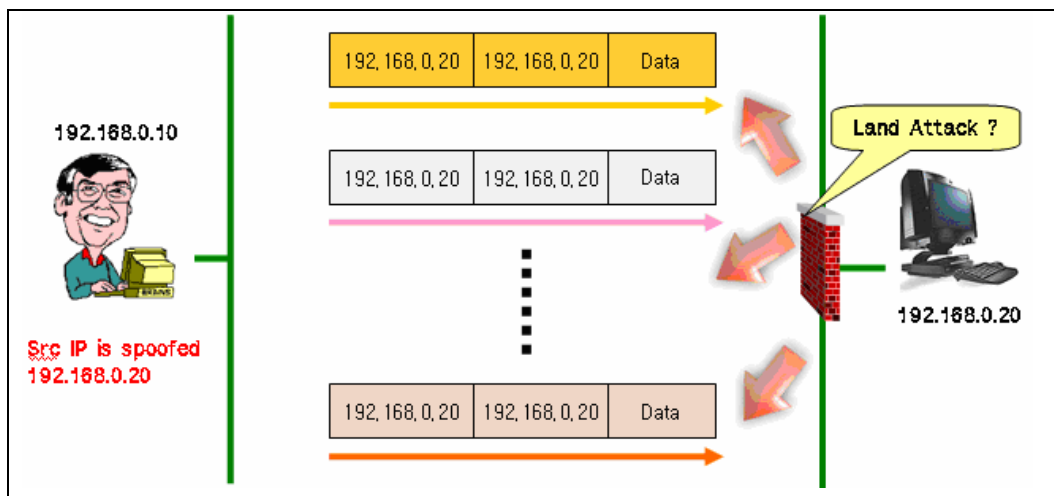
(그림 3-3-2)

위의 (결과 3-3-2)와 (그림 3-3-2)에서 캡처된 것과 같이, 각각의 첫 번째 패킷에서는 "Src IP = Dst IP", "Src Port = Dst Port"인 것을 볼 수 있다. 하지만, Redhat 9와 Windows XP SP2에서는 Land Attack이 패치 되었기 때문에, 이후의 패킷에서는 Src Port가 자동 증가되어 Land Attack에 피해를 입지 않는 것을 확인 할 수 있다.

이 결과를 보면서 독자 여러분은 보안 패치의 중요성과 필요성을 인식해야만 한다. 이 문서는 개념 이해를 위한 문서이므로, 여기까지만 테스트하기로 한다.

3-4. Land Attack 방어 방법

역시 개념을 이해한다는 의미에서 대표적인 방법인 Watch Mode를 이해하자.



(그림 3-4)

위의 (그림 3-4)를 순서대로 설명하면 아래와 같다.

1. 대상 서버의 앞에 있는 라우터/방화벽 장비에서 Packet을 감시한다.
2. Packet 중에서 Source IP와 Destination IP, Source Port와 Destination Port가 동일한 Packet이 있는지 감시한다.
3. Land Attack에 해당하는 Packet인 경우, 라우터/방화벽 장비에서 차단한다.

3-5. Land Attack 방어를 Watch Mode로 설정하는 화면

아래와 같이 보안장비에서 옵션 체크만 해주면 방어가 된다.

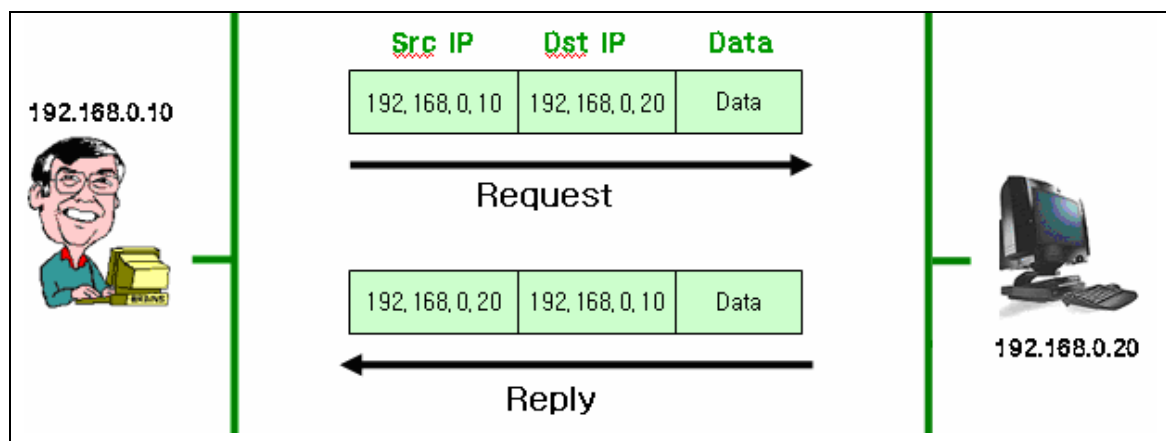
Denial of Service Defense			
<input type="checkbox"/>	Ping of Death Attack Protection		
<input type="checkbox"/>	Teardrop Attack Protection		
<input type="checkbox"/>	ICMP Fragment Protection		
<input type="checkbox"/>	ICMP Ping ID Zero Protection		
<input type="checkbox"/>	Large Size ICMP Packet (Size > 1024) Protection		
<input type="checkbox"/>	Block Fragment Traffic		
<input checked="" type="checkbox"/>	Land Attack Protection		
<input type="checkbox"/>	SYN-ACK-ACK Proxy Protection	Threshold	512 Connections
<input type="checkbox"/>	Source IP Based Session Limit	Threshold	128 Sessions
<input type="checkbox"/>	Destination IP Based Session Limit	Threshold	128 Sessions

(그림 3-5)

4. Smurf Attack

4-1. 정상적인 Ping의 흐름

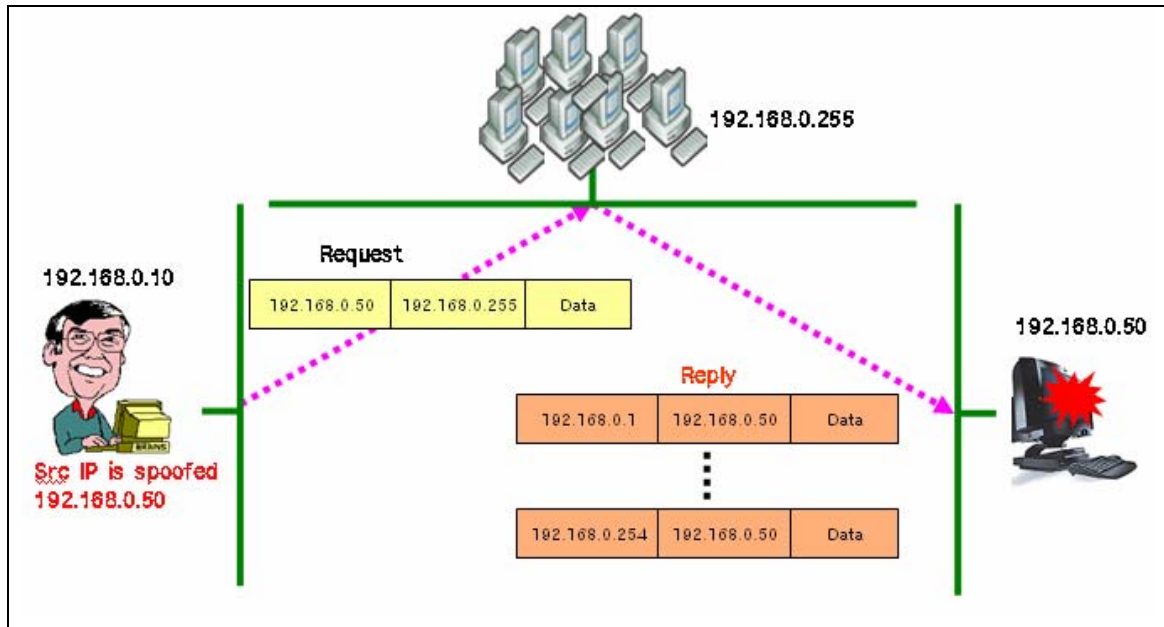
Client가 Server에게 네트워크에 연결되었는지 확인하기 위해서 Request를 보내고, 네트워크에 존재하는 Server가 이 응답요청에 대해서 Reply로 응답한다.



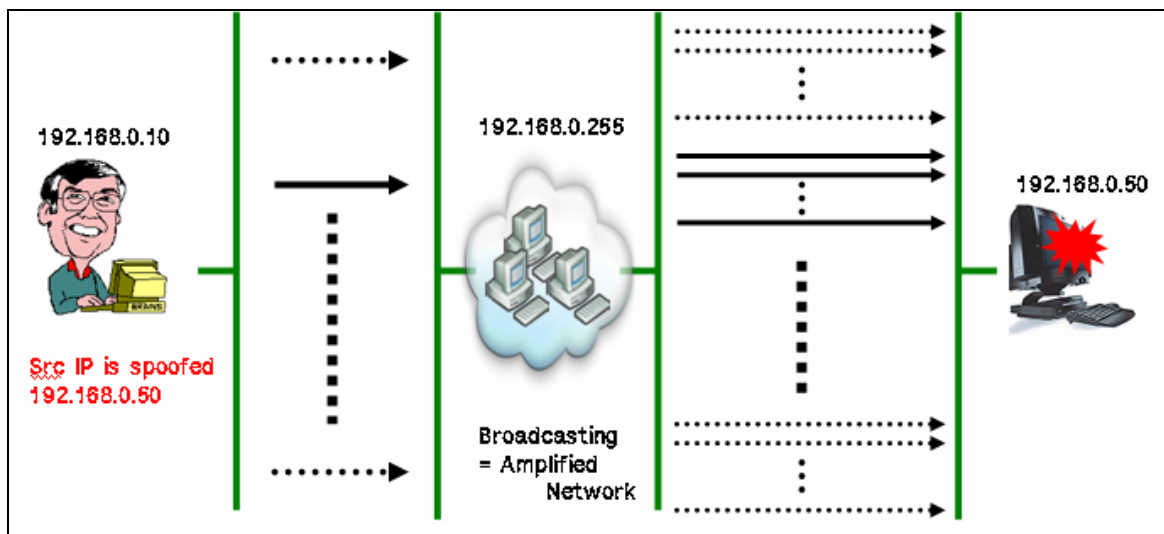
(그림 4-1)

4-2. Smurf Attack

(그림 4-2)와 (그림 4-3)에서 보는 것과 같이 Broadcast Network를 이용하여 대상 서버에게 DoS 공격을 하는 기법이다.



(그림 4-2)



(그림 4-3)

정확한 이해를 돕기 위하여 두 가지의 형태로 표현하였는데, 위의 (그림 4-2)와 (그림 4-3)을 순서대로 설명하면 아래와 같다.

1. 공격자는 대상자의 IP로 Spoofing한 후, 대상자가 속해 있는 Broadcast Network로 Broadcast 요청(Request)을 보낸다.
2. Broadcast Network는 대상 서버에게 응답(Reply) 한다.

3. (네트워크의 규모에 따라서) 대상 서버는 응답(Reply)을 받다가 느려지거나 Crash 된다.

4-3.Smurf Attack 예

4-3-1. 공격화면 예

```
[root@ground root]# ./smurf 192.168.0.50 bcast 0 10 1000

smurf.c v4.0 by TFreak

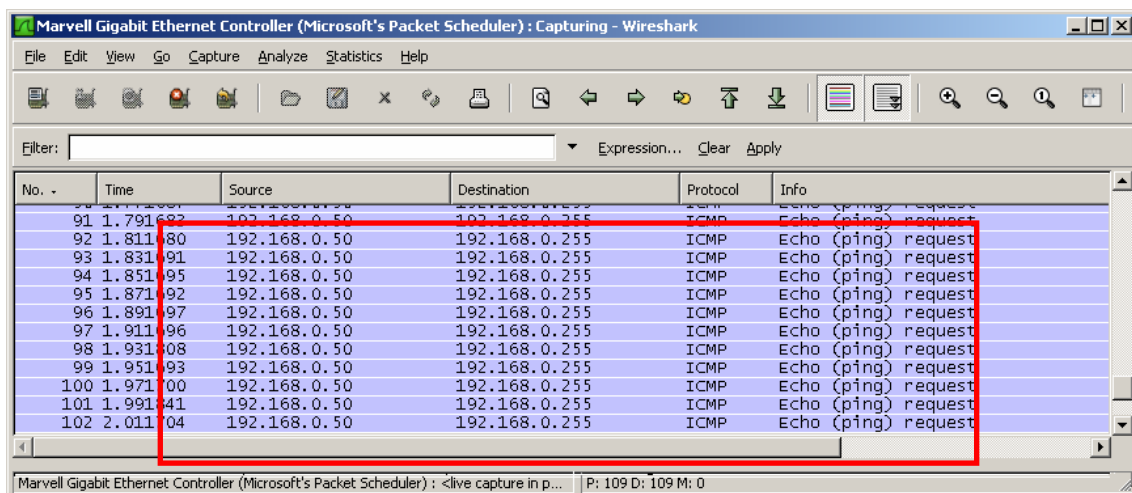
Flooding 192.168.0.50 (. = 25 outgoing packets)

.....
```

위의 공격화면의 의미를 설명하면 다음과 같다.

Dst IP인 bcast (192.168.0.255)로 "192.168.0.50"에서 ICMP Request를 보낸 것으로 위장된 1000 size의 패킷을 10ms 간격으로 보내라.

4-3-2. Receiver 에서 해당 패킷 캡처 화면



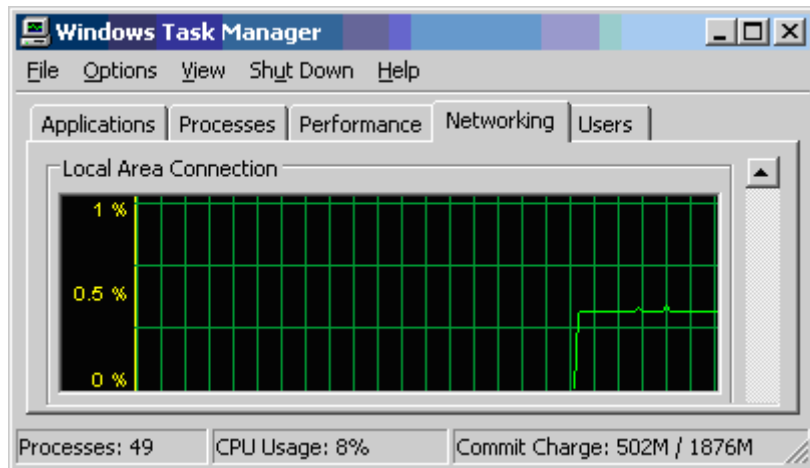
The screenshot shows a Wireshark capture window titled "Marvell Gigabit Ethernet Controller (Microsoft's Packet Scheduler) : Capturing - Wireshark". The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Info
91	1.791682	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request
92	1.811680	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request
93	1.831691	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request
94	1.851695	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request
95	1.871692	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request
96	1.891697	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request
97	1.911696	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request
98	1.931698	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request
99	1.951693	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request
100	1.971690	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request
101	1.991641	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request
102	2.011604	192.168.0.50	192.168.0.255	ICMP	Echo (ping) request

(그림 4-3-2-1)

위의 (그림 4-3-2-1)에서 캡처된 것과 같이, 대상 PC는 Broadcast Network Address로 패킷을 보낸 적이 없지만, 그러한 패킷이 보낸 것과 동일한 트래픽이 발생하고 있다.

여러분의 이해를 돕기 위하여, 필자가 발생시킨 가상의 Smurf Attack이 대상 서버의 Lan Card (NIC)에서 발생시키고 있는 트래픽을 (그림 4-3-2-2)와 같이 시각적으로 볼 수 있다.

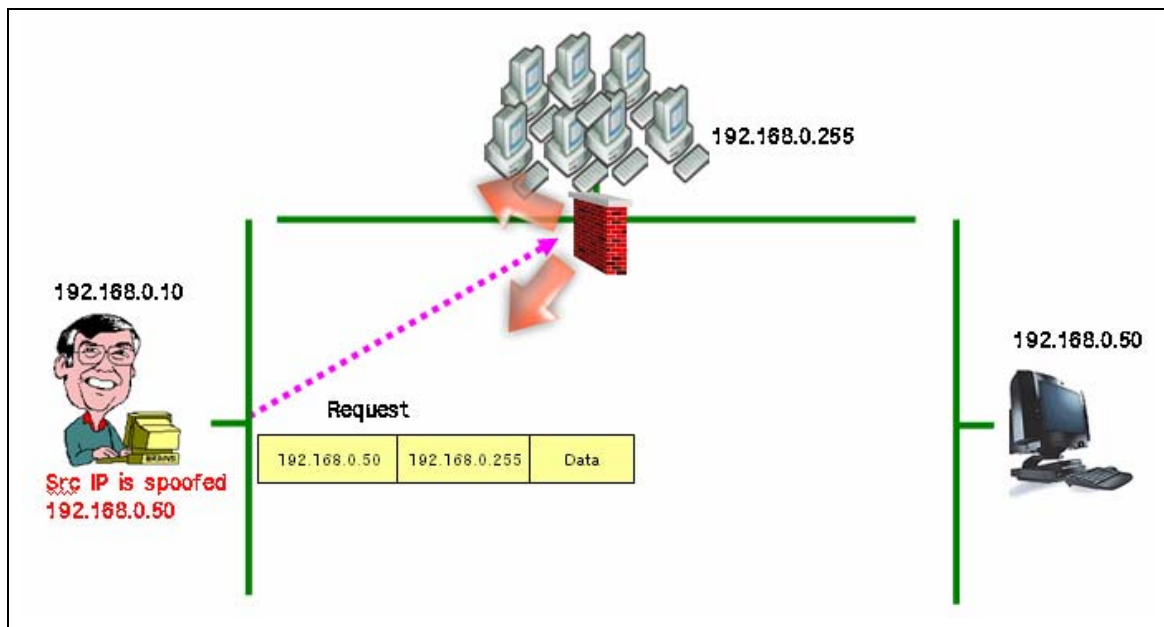


(그림 4-3-2-2)

만일 이 네트워크가 가상으로 만들어진 네트워크가 아니라, 수백 대의 컴퓨터가 존재하는 실제 네트워크였다 가정하면, 위의 그래프는 훨씬 높은 수치를 보였을 것이고, 대상 서버는 큰 영향을 받았을 것이다.

4-4.Smurf Attack 방어 방법

역시 개념을 이해한다는 의미에서 대표적인 방법인 Watch Mode를 이해하자.



(그림 4-4)

위의 (그림 4-4)를 순서대로 설명하면 아래와 같다.

1. 대상 서버의 앞에 있는 라우터/방화벽 장비에서 packet을 감시한다.

2. Destination IP가 Broadcast Address인 Packet을 차단한다.

5. Ping of Death

5-1. 정상적인 Ping 패킷의 구조 (RFC791 참고)

이해를 돕기 위해, 실제 ICMP 패킷을 Capture해서 아래에 표시하였다.

Internet Control Message Protocol																	
Type: 8 (Echo (ping) request)																	
Code: 0																	
Checksum: 0x475c [correct]																	
Identifier: 0x0500																	
Sequence number: 256 (0x0100)																	
Data (32 bytes)																	
0000	00	e0	18	be	90	67	00	13	77	66	e7	d0	08	00	45	00g.. wf....E.
0010	00	3c	7a	ec	00	00	80	01	3e	43	c0	a8	00	0a	c0	a8	.<Z.....>C.....
0020	00	37	08	00	47	5c	05	00	01	00	61	62	63	64	65	66	.7..G\.. ..abcdef
0030	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	ghijklmn opqrstuv
0040	77	61	62	63	64	65	66	67	68	69							wabcdefg hi

(그림 5-1-1) 정상적인 ICMP Request Structure

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x4f5c [correct]

Identifier: 0x0500

Sequence number: 256 (0x0100)

Data (32 bytes)

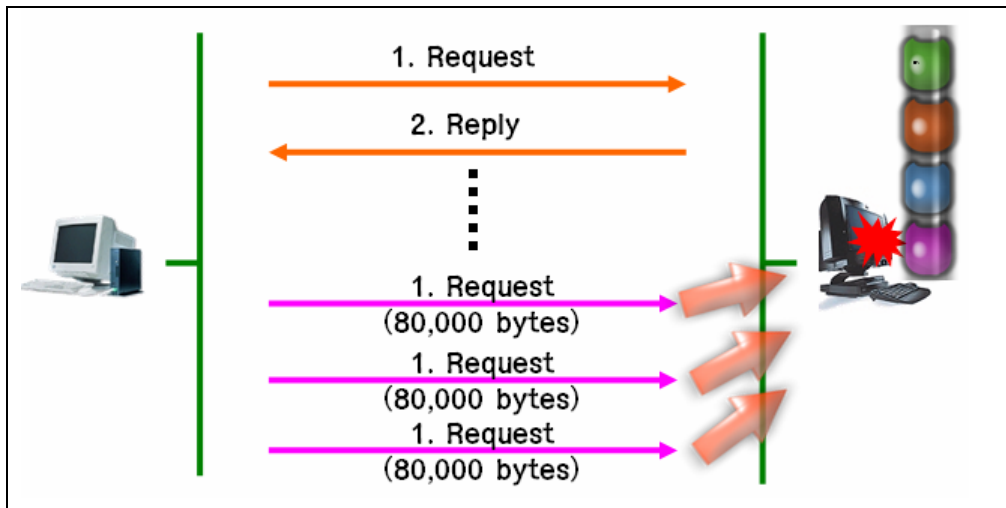
0000	00	13	77	66	e7	00	00	e0	18	be	90	67	08	00	45	00	..wI.... ..g...E.
0010	00	3c	0c	c7	00	00	80	01	ac	68	c0	a8	00	37	c0	a8	.<..... .h...7..
0020	00	0a	00	00	4f	5c	05	00	01	00	61	62	63	64	65	66	...O\.. ..abcdef
0030	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	ghijklmn opqrstuv
0040	77	61	62	63	64	65	66	67	68	69							wabcdefg hi

(그림 5-1-2) ICMP Reply Structure

위와 같이 Type, Code, Checksum, Identifier, Sequence number, Data에 적절한 값이 채워져서 ICMP의 역할을 수행한다.

5-2. Ping of Death

(그림 5-1-1)과 (그림 5-1-2)에서 보는 것과 같이 정상적인 Ping(ICMP) 패킷은 단순한 Control 정보만을 담고 있기 때문에, IP Header를 포함한 최대 크기가 65,535 bytes(=16 bits)까지로 정의되어 있다. 하지만, 공격자가 65,536 bytes 이상의 패킷을 대상 서버에게 보내게 되면, 대상 서버에서 ICMP를 위해 할당된 Buffer가 Overflow 되어, 결국 Crash 되거나 오동작하게 된다.



(그림 5-2)

위의 (그림 5-2)를 순서대로 설명하면 아래와 같다.

1. Client는 대상 서버에 ICMP Protocol 에 정의된 최대 크기보다 큰 80,000 bytes 크기의 ICMP Packet을 보낸다.
2. Fragmentation 되어서 대상 서버로 들어온 패킷은 정해진 Protocol에 맞지 않기 때문에 재조합(Re-assembly)에 실패한다.
3. 해당 Buffer 가 Overflow 되어, 대상 서버는 Crash 되거나 오동작을 일으킨다.

5-3. Ping of Death 예

5-3-1. 공격의 예

```
[root@ground root]# hping -l 192.168.0.50 -d 100000
HPING 192.168.0.50 (eth0 192.168.0.50): icmp mode set, 28 headers + 34464 data
bytes
len=1500 ip=192.168.0.50 ttl=128 DF id=34243 icmp_seq=0 rtt=4.4 ms
len=1500 ip=192.168.0.50 ttl=128 DF id=34247 icmp_seq=1 rtt=4.3 ms

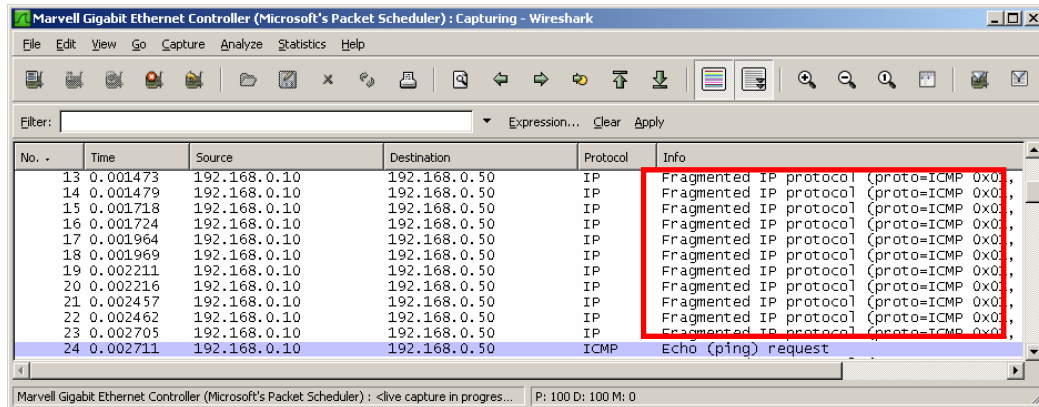
--- 192.168.0.50 hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 4.3/4.4/4.4 ms
```

위 공격의 의미를 설명하면 다음과 같다.

"192.168.0.50"으로 Size가 100000인 ICMP 패킷을 보내라.

* 패킷의 사이즈가 비정상적으로 크기 때문에, RTT(Round Trip Time)도 상당히 긴 시간 값을 가진다.

5-3-2. Receiver 에서 해당 패킷 캡처 화면

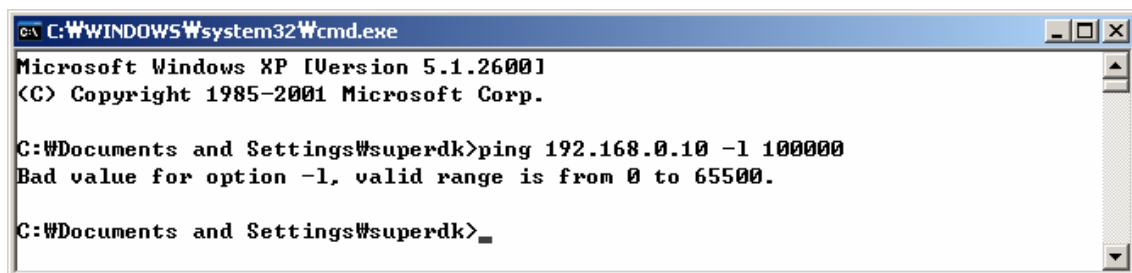


(그림 5-3-2)

위의 (그림 5-3-2) 에서 캡처된 것과 같이, 대상 서버에는 size 100000 인 icmp 패킷이 23개로 Fragmentation 되어서 들어왔다.

5-4. Ping of Death 방어 방법

Windows OS에서는 (그림 5-4-1)과 같이 ICMP Packet의 최대 크기를 지정하고, 사용자가 이를 초과하는 사이즈를 사용한 경우 명령어의 동작을 제한하도록 패치 되었고,



(그림 5-4-1)

Watch Mode의 관점에서는 Packet의 경유경로에서 ICMP 패킷을 열어볼 수 있는 보안 장비에서 (그림 5-4-2)와 같이 차단할 수 있다.

Denial of Service Defense		
<input checked="" type="checkbox"/>	Ping of Death Attack Protection	
<input type="checkbox"/>	Teardrop Attack Protection	
<input type="checkbox"/>	ICMP Fragment Protection	
<input type="checkbox"/>	ICMP Ping ID Zero Protection	
<input type="checkbox"/>	Large Size ICMP Packet (Size > 1024) Protection	
<input type="checkbox"/>	Block Fragment Traffic	
<input type="checkbox"/>	Land Attack Protection	
<input type="checkbox"/>	SYN-ACK-ACK Proxy Protection	Threshold <input type="text" value="512"/> Connections
<input type="checkbox"/>	Source IP Based Session Limit	Threshold <input type="text" value="128"/> Sessions
<input type="checkbox"/>	Destination IP Based Session Limit	Threshold <input type="text" value="128"/> Sessions

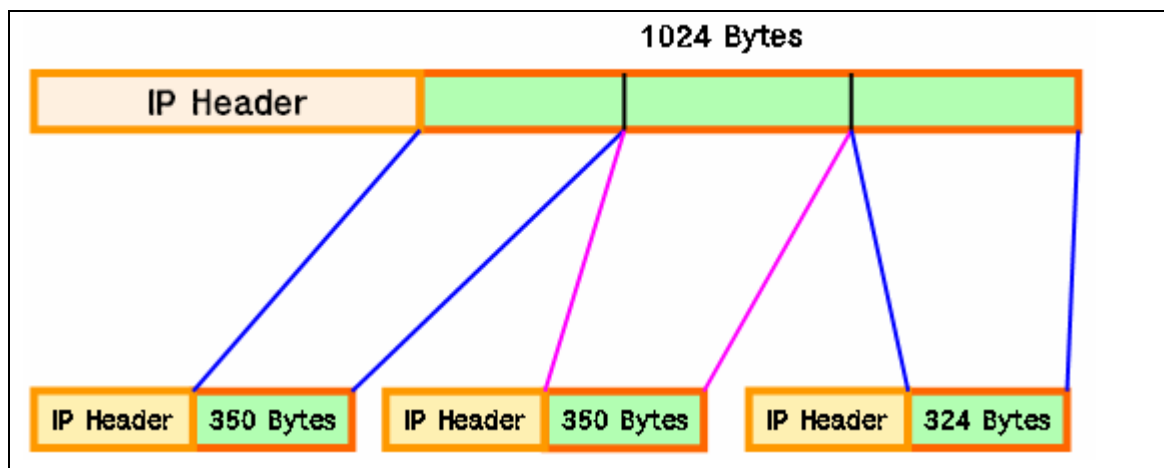
(그림 5-4-2)

6. Tear Drop

6-1. Layer 3에서의 Fragmentation

네트워크를 통해서 패킷이 전달되는 네트워크 통로의 크기를 MTU(Maximum Transmission Unit)라 한다. 즉, 해당 네트워크를 통과할 수 있는 최대 패킷의 크기이다.

만일, 출발지에서 목적지까지의 최소 MTU가 350 bytes라고 한다면 (그림 6-1-1)과 같이 Network Layer(Layer 3)에서 해당 Packet을 Fragmentation 하게 된다.

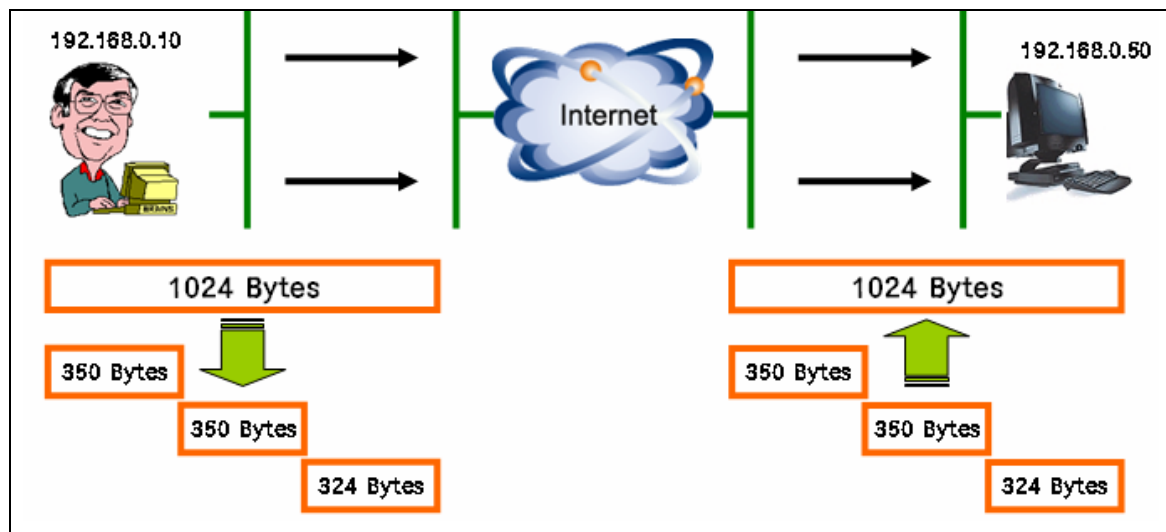


(그림 6-1-1) Fragmentation

단, TCP의 경우 MSS(Maximum Segment Size) 필드를 이용하여, 대상 서버가 처리할 수 없는 큰 크기의 Segment를 Client에서 보낼 수 없도록 할 수 있기 때문에, Tear Drop은 UDP Protocol을 사용한다.

Fragmentation을 이해하였으므로, 정상적인 Fragmentation을 이용하여 패킷이 어떻게

전달되는지를 이해해 보자.



(그림 6-1-2)

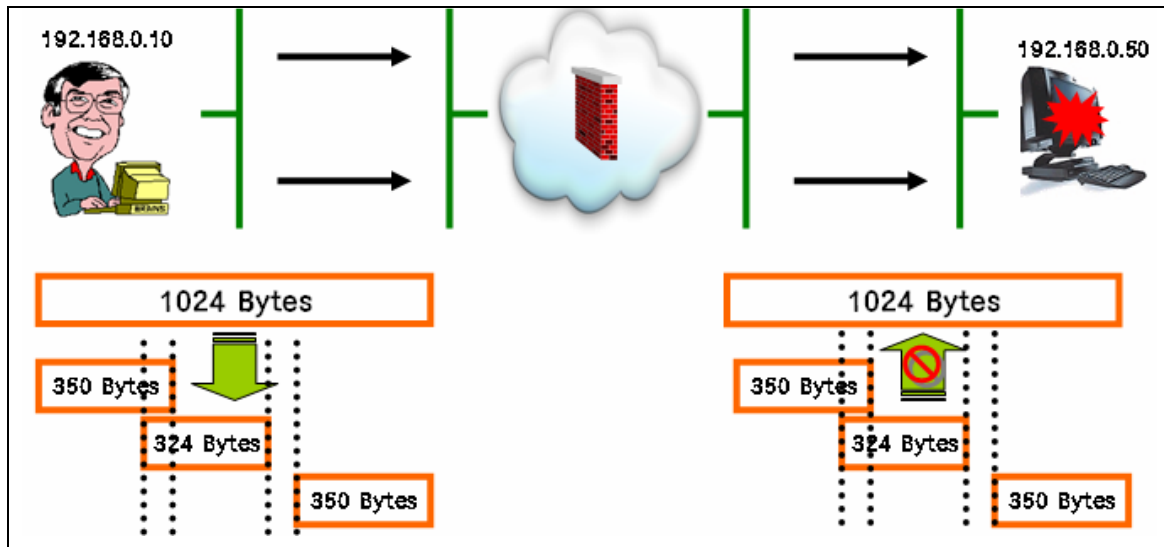
* Offset

Client에서 Packet을 Fragmentation 시킬 때, 대상 서버에서 해당 Packet을 재조합(Re-assembly)을 쉽게 할 수 있도록 순서에 해당하는 Offset으로 사이즈 값을 준다. 예를 들면, 위의 그림에서의 Offset 값은 각각 "0~349", "350~699", "700~1023"과 같이 지정된다. 위의 (그림 6-1-2)를 순서대로 설명하면 아래와 같다.

1. Client에서 서버로 패킷을 보낼 때, MTU 사이즈에 맞도록 Layer 3에서 Fragmentation이 일어난다.
2. Fragmentation된 패킷은 네트워크를 통해서 대상 서버로 전달된다.
3. 대상 서버는 Fragmentation된 패킷을 원래의 패킷으로 재조합(Re-assembly)하여 해석한다.

6-2. Tear Drop

Client가 패킷을 Segmentation 시킬 때, 위에서 설명한 Offset을 어긋나도록 수정하여, 대상 서버가 받은 Segmentation 된 패킷을 재조합하지 못하도록 하여 장애를 발생시키는 공격 기법이다.



위의 (그림 6-2)를 순서대로 설명하면 아래와 같다.

개념에서 설명한 것과 마찬가지로,

1. 공격자는 강제로 Offset이 어긋나도록 패킷을 Fragmentation 시켜서 전송한다.
(마치 딱 맞지 않는 퍼즐 조각을 만드는 것과 같다.)
2. 서버는 받은 Fragmentation 된 패킷을 재조합 하려고 하지만, 맞지 않는 퍼즐 조각으로 재조합에 성공할 수 없다.
3. 공격자는 대상 서버에 지속적으로 문제의 패킷을 보낸다.
4. 이러는 동안 대상 서버는 자원이 고갈된다.
5. 서버가 Crash 되거나, 오동작을 일으킨다.

6-3. Tear Drop 공격 예

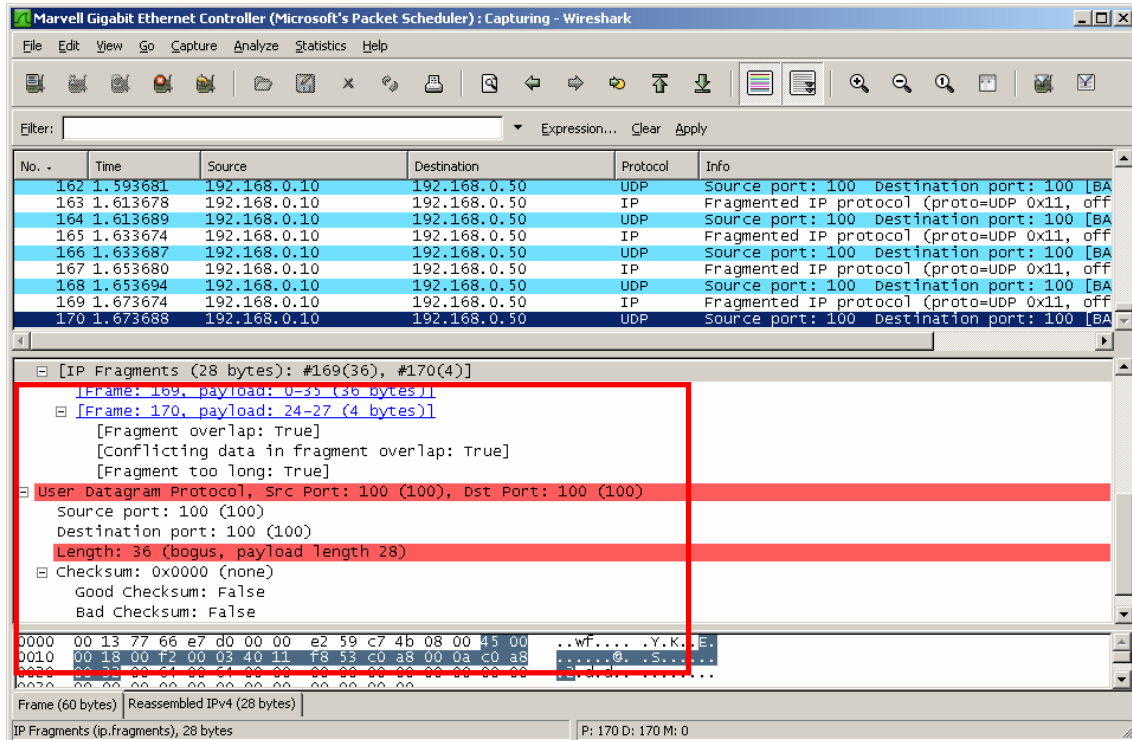
6-3-1. 공격화면 예

```
[root@ground root]# ./teardrop 192.168.0.10 192.168.0.50 -s 100 -t 100 -n
1000
teardrop      route|daemon9nnDeath on flaxen wings:nFrom:      192.168.0.10.
100n  To:      192.168.0.50.  100n  Amt:  1000n[ b00m b00m b00m b00m b00m b00m
b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m
b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m
b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m
b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m
b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m
```

위의 공격화면의 의미를 설명하면 다음과 같다.

Src IP "192.168.0.10"에서 Dst IP "192.168.0.50"으로 Src Port 100과 Dst Port 100으로 지정하여, 1000개의 Teardrop 패킷을 보내라.

6-3-2. Receiver 에서 해당 패킷 캡처 화면

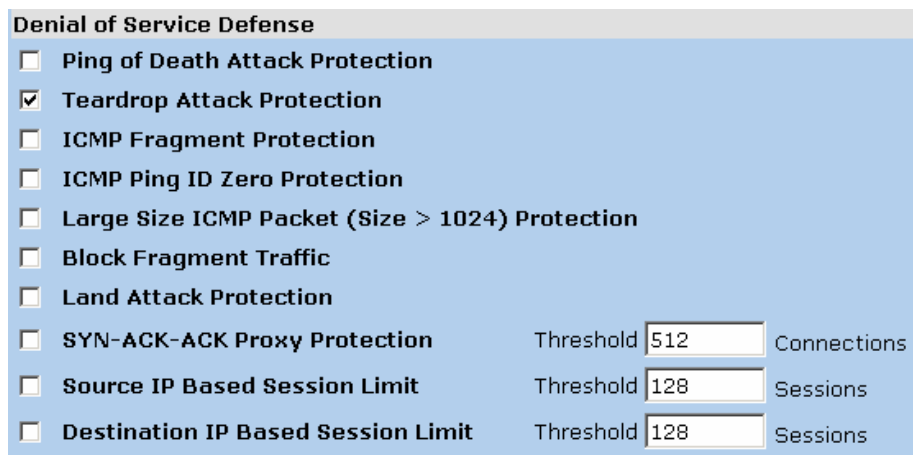


(그림 6-3-2)

위의 (그림 6-3-2)에서와 같이, 대상서버에 문제가 있는 UDP 패킷이 다량 발생한다.

6-4. TearDrop 방어 방법

지나가는 패킷을 분석하여 TearDrop 패킷임이 확인되면 차단한다. 역시 개념을 이해한다는 의미에서 대표적인 방법인 Watch Mode를 이해하자.



(그림 6-4)

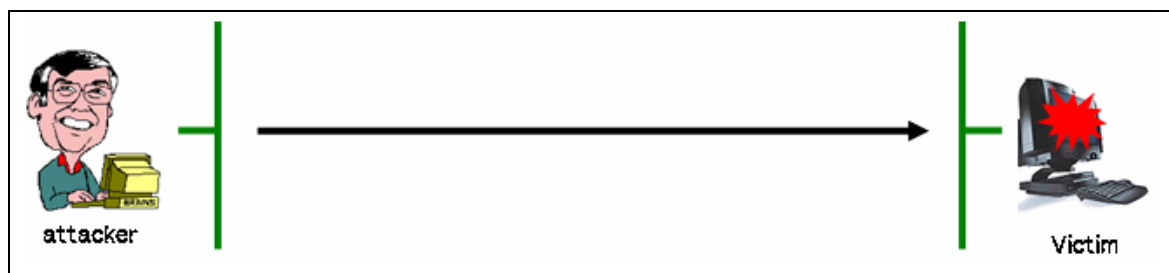
7. DoS(Denial of Service) & DDoS(Distributed Denial of Service)

7-1.DoS 공격의 개념

대상 서버에 부가적인 트래픽을 일으킴으로써, 대상 서버가 그 트래픽을 처리하느라 수행해야 할 기능을 수행하지 못하도록 하는 공격 방법을 말한다.

7-2.DoS 공격의 계층

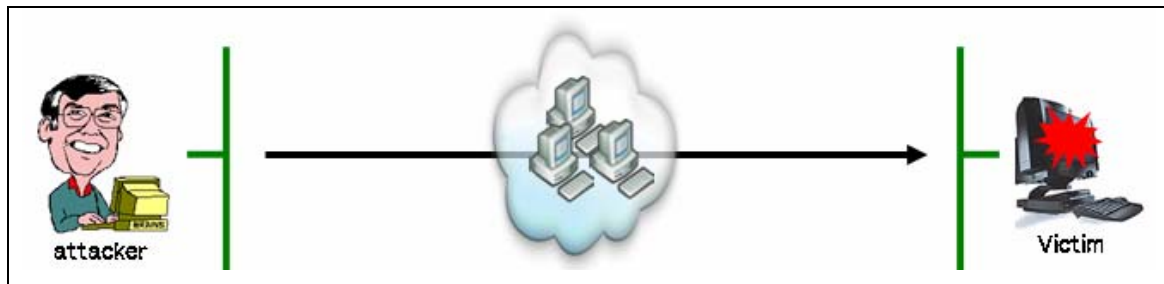
Windows OS와 같은 GUI 개념이 없던 시절에 사용하던 컴퓨터는 공격자가 가진 하나의 컴퓨터에서 발생시키는 적은 양의 트래픽으로도 대상 서버의 서비스에 장애를 일으킬 수 있었지만, 컴퓨터의 성능이 눈부시게 향상되고, 자원이 대용량화 되면서부터는 이러한 초보적인 방법으로 발생시킨 적은 양의 트래픽으로는 대상 서버에 서비스의 장애를 일으킬 수 없게 되었기 때문에, 보다 많은 트래픽을 발생시킬 수 있도록 방법이 지능화 되었다.



(그림 7-2-1) 1-Tier 공격: SYN, Land, Ping of Death, Exhausting disk, Spam mail 등

위의 (그림 7-2-1)을 순서대로 설명하면 아래와 같다.

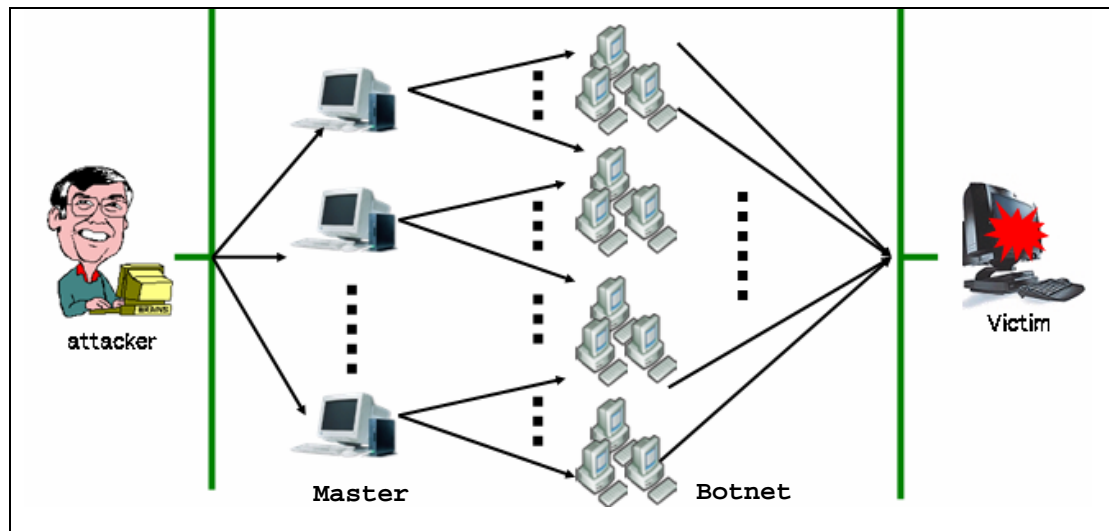
- "1:1" 공격을 의미한다.
- Exhausting disk: 혼자서 대상 서버의 자원(대표적으로 HDD)을 모두 써버릴 경우 다른 사용자는 저장 공간이 부족하여 더 이상 저장을 할 수 없게 된다. 이러한 문제점을 해결하기 위하여, 우리가 제공받는 모든 서비스(대표적인 웹메일)에는 계정당 사용할 수 있는 최대 할당량이 주어져 있다.
- Spam Mail: 스팸 메일을 받아보지 못한 사람은 이해하지 못할 수 있다. 마치 119에 장난 전화가 너무 많이 와서, 실제 위급한 구조요청을 할 수 없는 것과 같다. 내 메일 계정으로 하루에 수십만 통의 불필요한 메일이 온다고 생각해보자. 지우기도 힘들 뿐더러, 반드시 읽어야 하는 메일을 찾는 것도 포기해야 할 것이다.



(그림 7-2-2) 2-Tier 공격: Smurf Attack

위의 (그림 7-2-2)를 순서대로 설명하면 아래와 같다.

- "1 : 다: 1" 의 2계층 구조를 보인다.
- 공격을 발생시키는 attacker와 실제 공격을 수행하는 "다"에 해당하는 네트워크의 2계층을 이룬다.



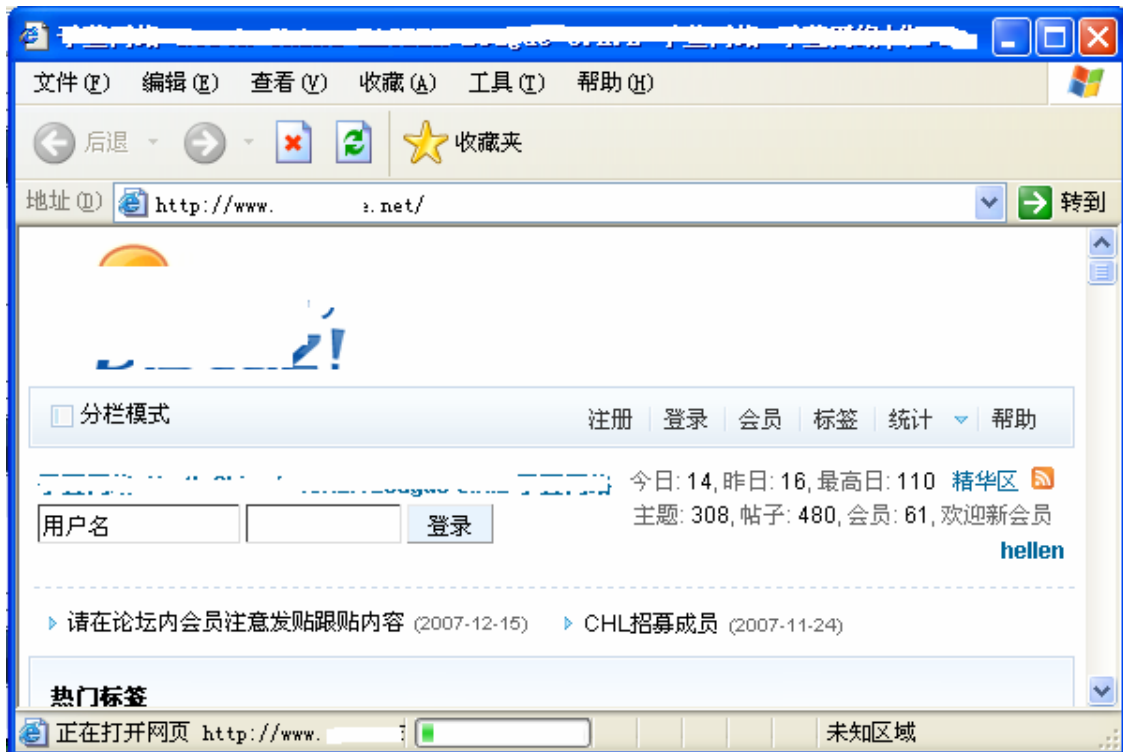
(그림 7-2-3) 3-Tier 공격: Trinoo, TFN(2K), Stacheldraht, botnet

위의 (그림 7-2-3)을 순서대로 설명하면 아래와 같다.

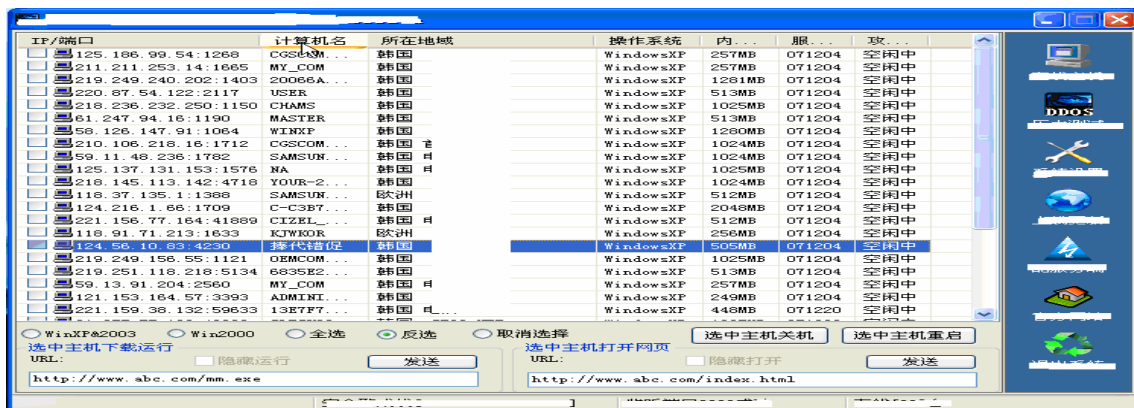
- "1 : 다: 보다 큰 다 : 1" 의 3계층 구조를 보인다.
- 3계층 구조부터 DDoS라고 한다.
- 그림에서 보는 바와 같이 1, 2계층 공격과 비교하더라도 상상을 초월하는 트래픽을 발생시킬 수 있기 때문에 우수한 성능을 지닌 현재의 서버들도 서비스를 수행할 수 없게 된다.

7-3. DDoS 공격 예

독자의 이해를 돕기 위해서 중국에서 테스트한 DDoS 공격 자료 화면을 보자.



(그림 7-3-1) 대상 서버에서 정상적으로 서비스 되는 화면



(그림 7-3-2) Attacker 가 자신의 botnet 을 이용하여 공격을 시작하는 화면



(그림 7-3-3) 공격을 시작한 지, 수초가 지난 후, 대상 서버의 서비스가 거부된 화면

7-4. DDoS 공격에 대한 방어

필자가 보기에 Main Backbone 이나 Main Router 등이 견뎌내지 못할 정도의 트래픽을 유발하는 DDoS 공격이 이미 시작된 상태에서는 공격을 막을 방법이 없다. 왜냐하면 대상 서버로의 트래픽을 이러한 Main 장비에서 차단해 주어야 하는데, 그럴 수 없는 상황이기 때문이다. 마치 쓰나미라 불리는 커다란 해일이 몰려오는 상황에서 속수 무책인 것과 같다.

하지만, (그림 7-2-3)과 (그림 7-3-2)를 보면 attacker가 DDoS 공격을 성공시키기 위해서는 상당히 많은 botnet을 감염시켜야 한다. 그러므로, botnet에 감염되지 않도록 주의하는 것이 최상의 방법이며, 굳이 구체적인 방법을 제시하자면 아래의 내용 정도이다.

개인 사용자의 노력에 대한 의견

- 실시간 OS 패치를 수행하여, OS 취약점을 통한 botnet 감염을 차단한다.
- 실시간 백신 업데이트를 수행하여 알려진 botnet의 감염을 차단한다.
- 검증되지 않은 파일을 다운로드 하지 않는다.
- 특히, 익명 공유 폴더를 만들지 않는다.
- 흔히 말하는 Default Password를 그대로 사용하지 않는다.

보안 관리자의 노력에 대한 의견

큰 규모의 망을 관리하는 관리자도 "DDoS 공격이 시작되었을 때 이를 어떻게 막을 수 있는가?"라는 질문을 많이 합니다만, (적어도 저자에게는 이런 질문을 한다는 것이 DDoS의 정의를 정확하게 알지 못하는 관리자라고 여겨진다.), 저자가 보기에 이러한 관리자가 말하는 막을 수 있는 DDoS공격이라 함은 "어설폰(?) DDoS"에 해당하는 "과다트래픽 정도"에 불과하다는 주장이다. 즉, 어설폰 DDoS 정도의 트래픽일 것이다. 이 정도의 트래픽이야 장비들을 적절히 제어한다면 서비스가 느려지는 선에서 버틸 수 있기는 하다. 하지만, 제대로 된 공격이 시작되었다면 적어도 저자는 막을 수 없다고 생각한다. 왜냐하면 위의 예에서와 같이 제대로 된 DDoS 공격으로 충분한 트래픽이 발생된다면 원격지에 있는 이러한 과다 트래픽을 쉽게 제어할 수는 없기 때문이다.

그래서, DDoS의 방어는 botnet의 확산 방지가 관건이다.

물론, 상식적인 이야기지만 크게 아래와 같은 세 가지의 방법으로 정리를 해봤다.
요지는 적어도 자신의 네트워크에서 botnet 트래픽이 없도록 노력하자는 것이다.

1. botnet 이 자신의 네트워크에 없도록 하라.

- 지속적으로 네트워크의 트래픽을 모니터링하여 감염된 PC를 실시간 치료한다.

2. Master 로의 통신 트래픽을 이용해서 botnet 과 Master를 제거하라.

- 1번과 반대되는 관점으로 botnet 을 제어하는 Master와의 통신을 막음으로써, botnet 이 동작하지 못하도록 하는 것이며,

구체적인 방법을 예로 들면,

* 최신 botnet 을 무조건 구해서

* 테스트 PC에 설치하여 botnet을 분석한 후 Master PC를 찾고

* Master PC 를 차단하거나 해당 네트워크의 관리자에게 조치를 취하도록 요청한다.

3. 방화벽이나 Router에서 “반드시 허용할 포트” 외에는 모든 패킷을 Deny로 설정한다.

- 이렇게 설정되어 있을 경우 내부에 Botnet 이 감염되었다 하더라도, 내부에서 외부 네트워크로 트래픽이 전달되지 않을 뿐더러, 관제체계 혹은 모니터링 체계가 있다면 Drop 패킷의 모니터링 만으로도 Botnet 의 트래픽을 쉽게 발견할 수 있다.

4. 네트워크 및 주요 시스템을 HA로 구성한다.

자금력이 된다면 삼중, 사중 이상으로 더 강력한 HA를 구성하는 것도 도움이 되겠다. 하지만, 이러한 HA 구성 환경마저도 견디기 힘들 정도의 트래픽(실세계의 쓰나미 정도의 개념)에 대해서는 역시 답이 없다. 단, 과다 트래픽성의 DDoS 라면 개념상 대응 방안이 될 수도 있다.

과다 트래픽성의 DDoS에 대한 의견

과다 트래픽성의 DDoS라 함은 Main Backbone 이나 Main Router 는 견대낼 수 있지만 서버와 같은 시스템은 견디기 어려운 정도까지의 트래픽이라 전제하겠다.

이러한 경우에는 대상 서버로 DDoS 트래픽을 일으키는 botnet IP 들을 찾아서, 이 IP 들의 대역을 Main Backbone, Router, F/W 등에서 차단한다. 이렇게 하면 서버로는 DDoS 성 트래픽이 전달되지 않으므로 서비스에는 문제가 없다. 하지만, 차단된 IP 대역에서의 정상적인 접근까지도 차단되는 문제점이 발생하게 되므로 지역적으로는 여전히 DoS 공격을 당하는 셈이다.

8. DRDoS (Distributed Reflection Denial of Service)

8-1.DRDoS의 개념

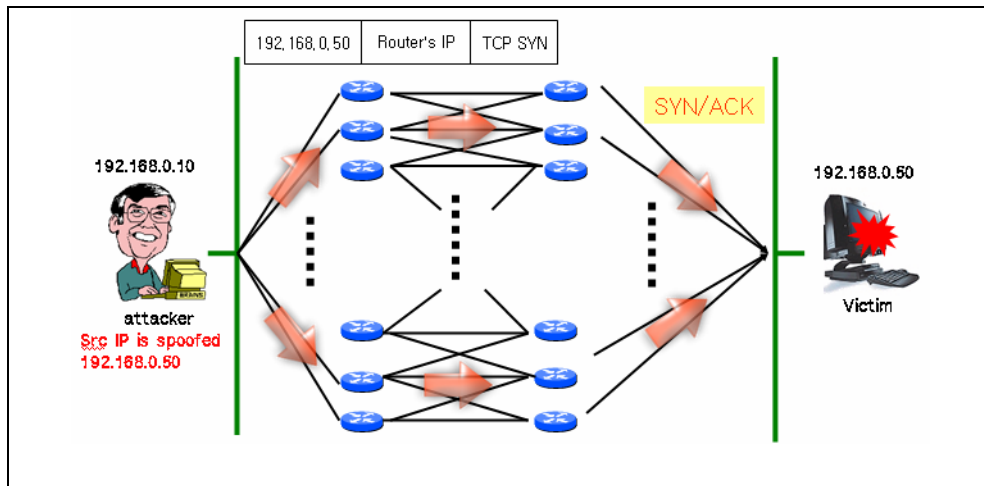
DRDoS를 이해하기 위해서는 반드시 반사(Reflection)라는 용어를 기억해야 한다.

그리고, DRDoS에서는 정상적인 서비스를 이용하기 때문에, 방화벽에서 허용되어 있다는 점이 유사한 공격과 비교했을 때의 특이점이다. 그러므로, DRDoS 에는 BGP와 같은 Routing Protocol 이나 HTTP(80/tcp)와 같은 허용될 수 밖에 없는 서비스들을 이용한다.

햇빛을 거울로 반사시켜 상대방을 교란시키는 상황을 연상해 보자. DRDoS는 Smurf Attack 과 동일한 공격 패턴을 띤다.

즉, DRDoS는 대상서버로 IP를 Spoofing 하여, “공인 IP”를 가진 다수의 서버나 장비에게, 마치 대상서버가 요청한 것처럼 패킷을 보내서, 이 요청에 대한 응답이 동시에 대상서버로 집중되도록 함으로써 대상서버가 서비스를 하지 못하도록 하는 기법이다.

(그림 8-1)에서는 공격자와 대상 서버 사이에 있는 라우터를 이용하여 TCP SYN Attack 을 하는 DRDoS 공격 기법을 표현하였다.

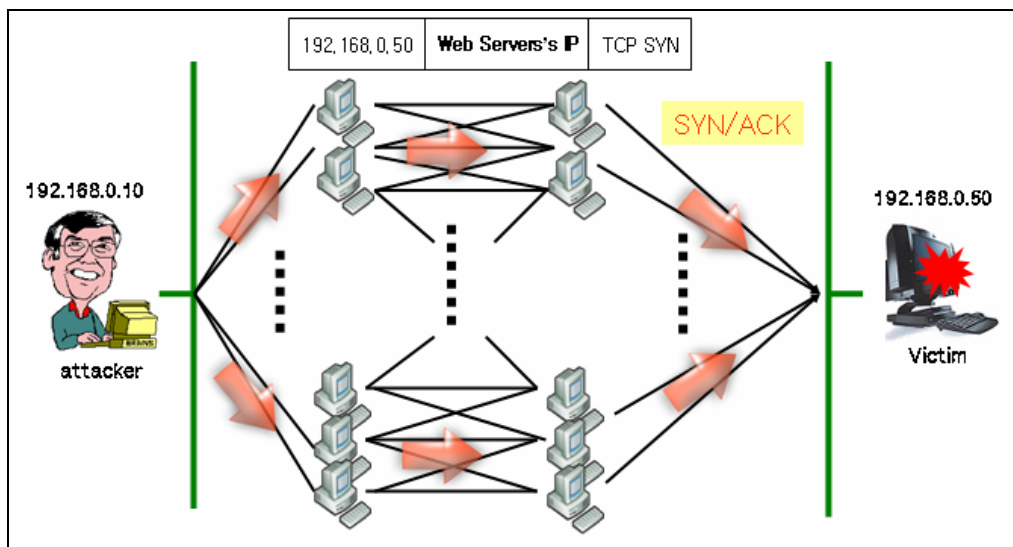


(그림 8-1)

위의 (그림 8-1)을 순서대로 설명하면 아래와 같다.

1. Attacker는 IP와 Port를 Spoofing 해서 수많은 Router들에게 SYN Packet을 보낸다.
2. SYN Packet을 받은 수많은 Router들은 Spoofing 된 Source IP 인 "192.168.0.50"과 해당 포트(예: 80/tcp)로 SYN/ACK Packet을 보내서 응답한다.
3. 대상 서버는 이러한 과부하를 견뎌낼 수 없으므로, 결국 서비스를 제공할 수 없게 된다.

동일한 개념으로 라우터 대신 Google, Yahoo, Naver, Daum 등과 같은 포털 사이트의 웹서버를 이용한 공격도 (그림 8-2)와 같이 가능하다.



(그림 8-2)

8-2.DRDoS 방어 방법

DRDoS 공격 역시 완벽한 방어를 하기는 힘들지만, ISP 업체간 업무를 연계하고, DRDoS 전용 필터를 두어 징후가 나타나면 담당하고 있는 각각의 구간에서 즉시 조치를 취하여 트래픽의 확산을 막는 것이 가장 효과적일 것이라 판단된다.

9. Epilogue

지금까지 Network Attack의 기본적인 개념들을 살펴 보았다. 이 글을 읽은 독자는 각각의 공격에 대한 원리를 정확하게 이해하기를 바라는 마음에서, Network Attack에 대해서 정확하게 설명하려 노력하였다.

어떠한 원리를 정확히 아는 것과 적당히 아는 것에는, 말로 표현할 수 없는 엄청난 차이가 있다. 더 관심이 있는 독자는 원리를 정확하게 이해한 후, 제한된 테스트 환경에서 테스트를 해보고, 소스코드에도 관심을 기울인다면 보다 깊이 있는 정보보호 전문가가 될 수 있으리라 생각한다.