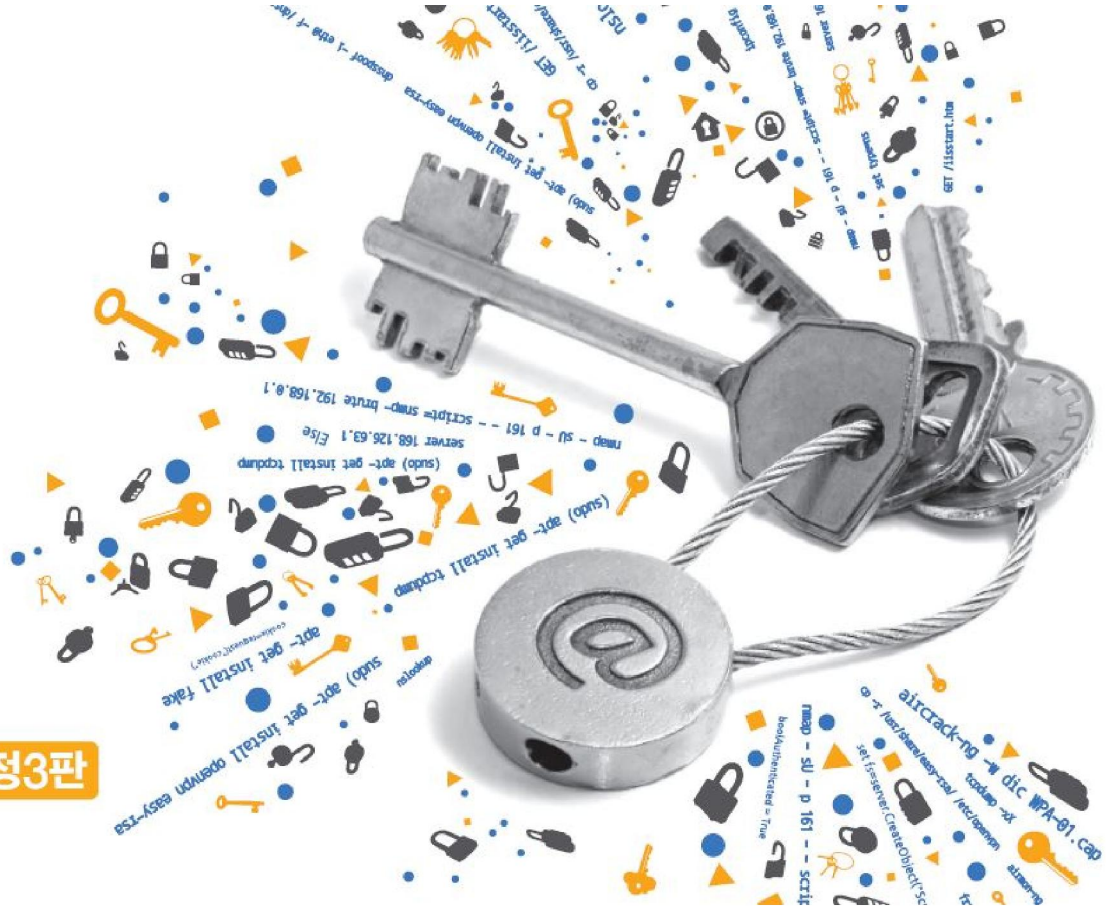
원리를 IT 가르쳐 맛보다

네트워크 해킹과 보안

개정3판

정보 보안 개론과 실습



Chapter 11 DoS와 DDoS 공격

IT COOKBOOK

목차

학습목표

- DoS와 DDoS 공격의 패턴을 이해한다.
- DoS와 DDoS 공격을 실행할 수 있다.
- DoS와 DDoS 공격을 탐지할 수 있다.
- DoS와 DDoS 공격에 적절히 대처할 수 있다

1. DoS 공격

1.1 DoS 공격에 대한 이해

■ DoS(Denial of Service(서비스 거부))

- 공격 대상이 수용할 수 있는 능력 이상의 정보를 제공하거나 사용자 또는 네트워크 용량을 초과시켜 정상적으로 작동하지 못하게 하는 공격

■ DoS 공격의 특징

- 파괴 공격 : 디스크, 데이터, 시스템 파괴
- 시스템 자원 고갈 공격 : CPU, 메모리, 디스크의 과다한 사용으로 인한 부하 가중
- 네트워크 자원 고갈 공격 : 쓰레기 데이터로 네트워크 대역폭의 고갈

■ Ping of Death 공격

① ping을 이용하여 ICMP 패킷의 크기를 정상보다 아주 크게 만듦.

② 크게 만들어진 패킷은 네트워크를 통해 라우팅되어 공격 네트워크에 도달하는 동안 아주 작은 조각으로 쪼개짐.

③ 공격 대상은 조각화된 패킷을 모두 처리해야 하므로 정상적인 ping보다 부하가 훨씬 많이 걸림.

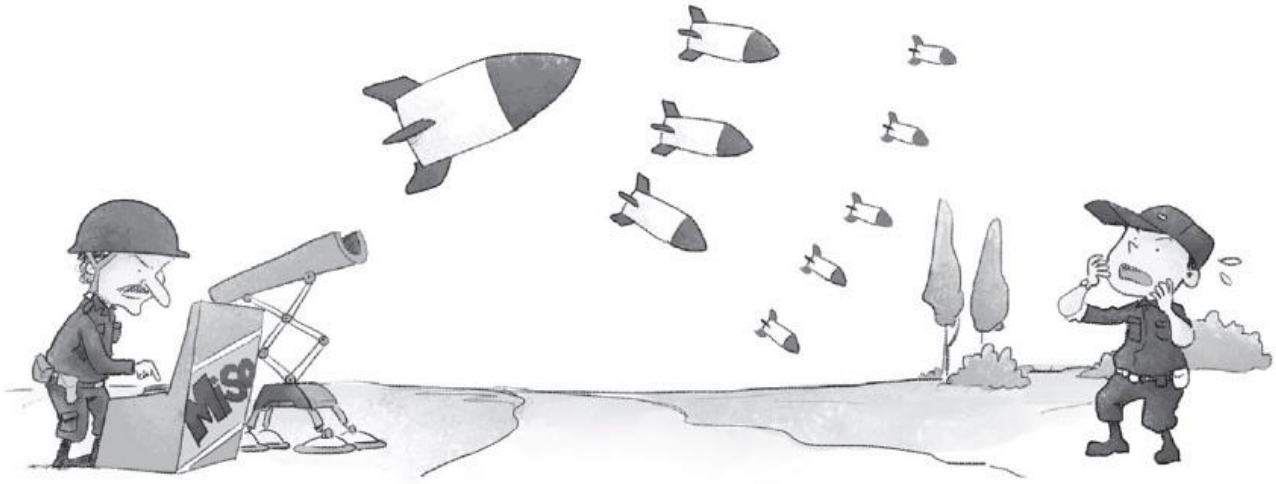


그림 11-2 Ping of Death 공격의 개념

■ 패킷을 왜 작게 분할하여 전달하나?

- 라우팅은 패킷을 전달할 때 특성이 똑같은 네트워크를 지나지 않음.
- 네트워크마다 최대로 전송이 가능한 패킷의 길이가 달라 최대 전송 가능한 패킷의 길이가 작은 네트워크를 지나면 데이터는 더 작게 분할됨.
- 한번 분할된 패킷은 다시 커지지 않음.
- 패킷을 늘리려면 패킷을 저장한 후 다음에 들어온 패킷 데이터를 재조합해야 하는데 라우터 성능에 치명적일 정도로 높은 부하를 야기함.

■ 패킷 분할

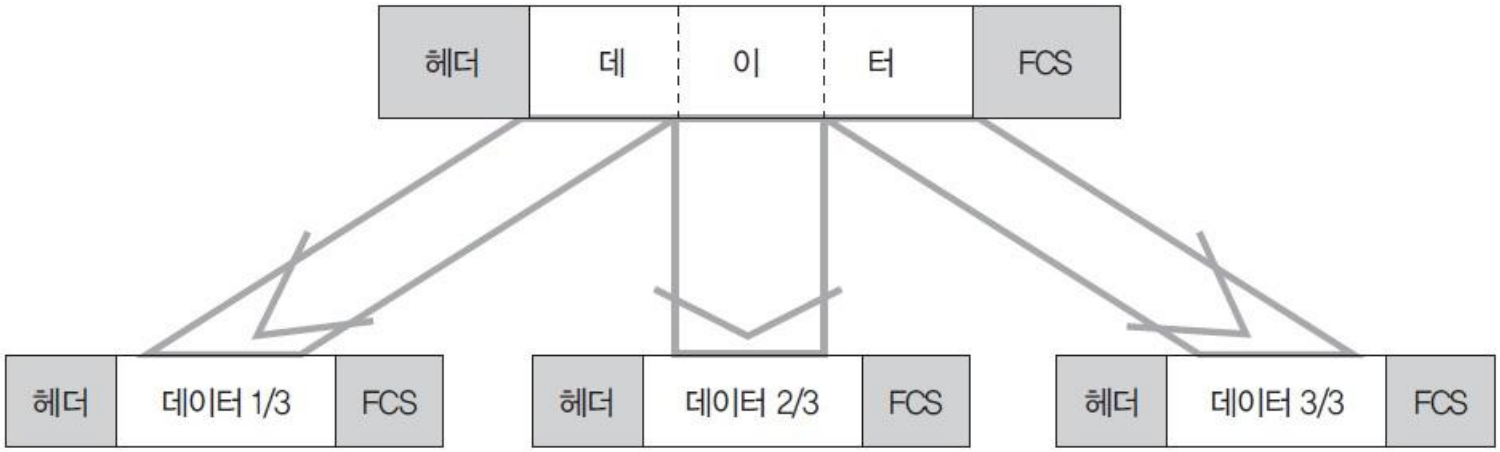


그림 11-3 패킷 분할도

- ICMP 패킷의 최대 길이를 65,500바이트로 임의로 설정
- 최대 크기인 65,500바이트로 네트워크에 ping을 보내면 패킷은 전송에 적절한 크기로 분할
- 패킷이 지나는 네트워크의 최대 전송 가능 길이가 100바이트라면 패킷 하나가 655개로 분할

1. DoS 공격

실습 11-1 Ping of Death 공격하기

실습환경
- 클라이언트 시스템 : 우분투 데스크탑 14
- 공격 대상 시스템 : 윈도우 서버 2012
- 필요 프로그램 : hping3, Wireshark

① hping3 설치하기

(sudo) apt- get install hping3

② Ping of Death 공격 수행하기

hping3 --icmp --rand-source 192.168.0.1 -d 65000

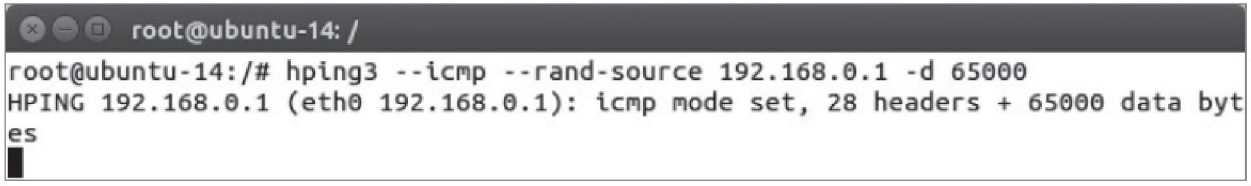


그림 11-4 hping3를 이용한 Ping of Death 공격 수행

③ Ping of Death 공격의 패킷 분석하기

- hping3로 앞에서 보낸 패킷을 윈도우 서버 2012에서 Wireshark로 캡처

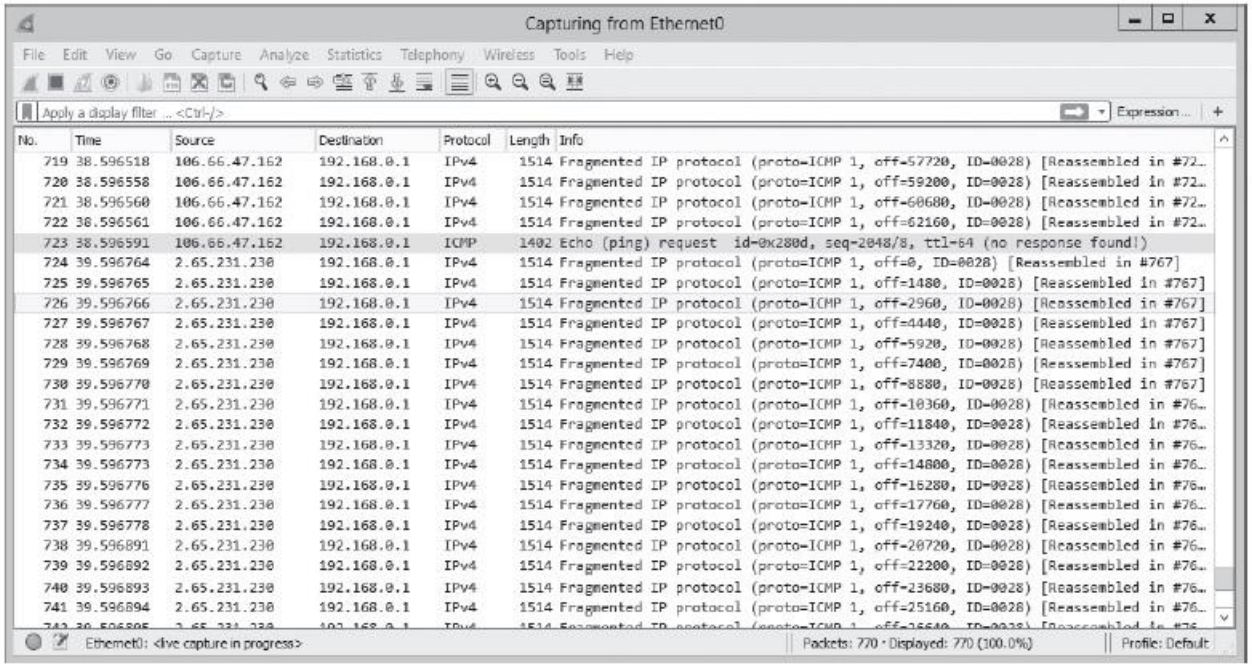


그림 11-5 Ping of Death 공격에서 공격 대상 시스템의 패킷 캡처 결과

③ Ping of Death 공격의 패킷 분석하기

- 724번 패킷 상세 확인

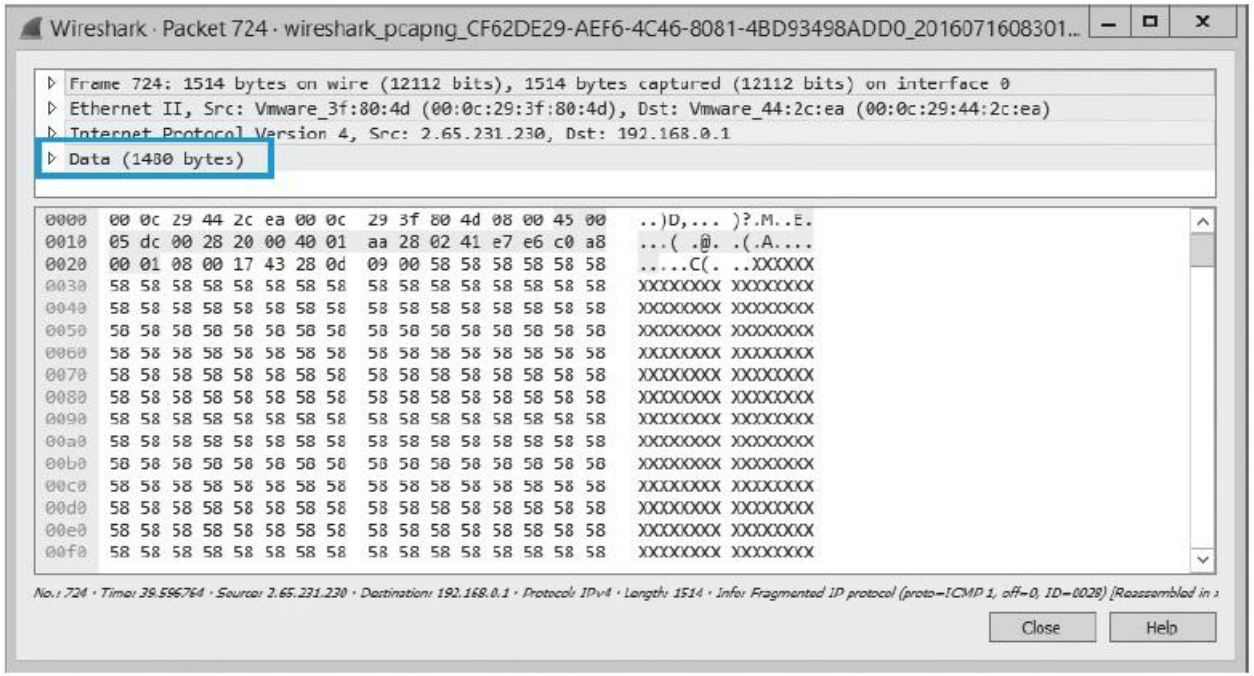


그림 11-6 Ping of Death 공격에서 공격 대상 시스템의 패킷 캡처 결과의 상세 확인

■ 보안 대책

- 반복적으로 들어오는 일정 수 이상의 ICMP 패킷을 무시하도록 설정
- 가장 일반적으로 할 수 있는 대책은 패치

■ SYN Flooding(플러딩)

- 서버별로 한정되어 있는 접속 가능 공간에 존재하지 않는 클라이언트가 접속한 것처럼 속여 다른 사용자가 서비스를 제공받지 못하게 하는 것

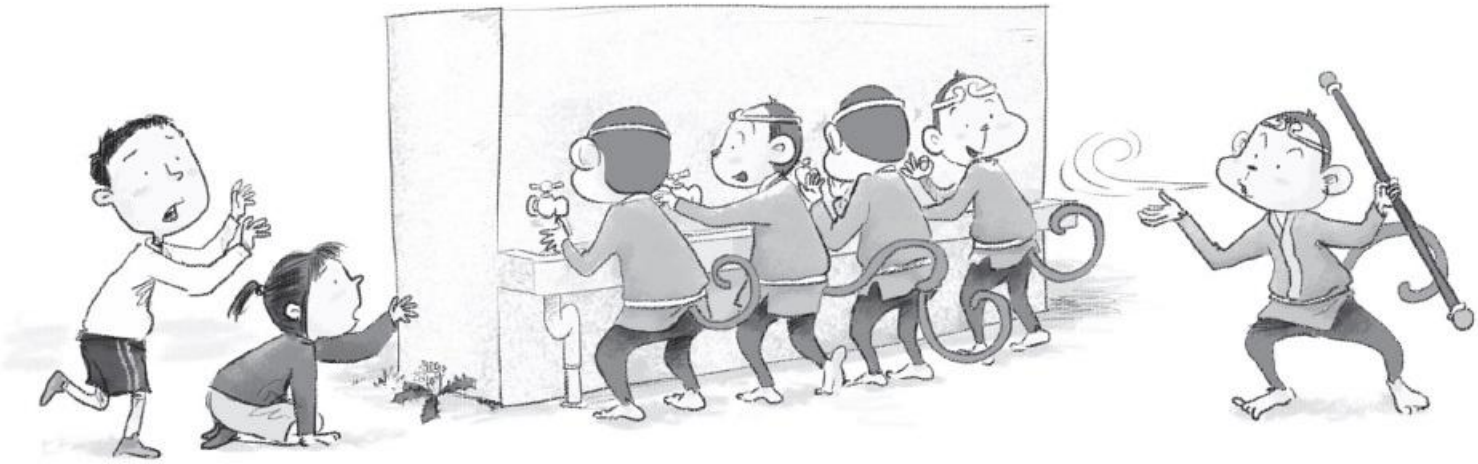


그림 11-7 SYN Flooding 공격의 개념

■ SYN Flooding 공격 이해하기

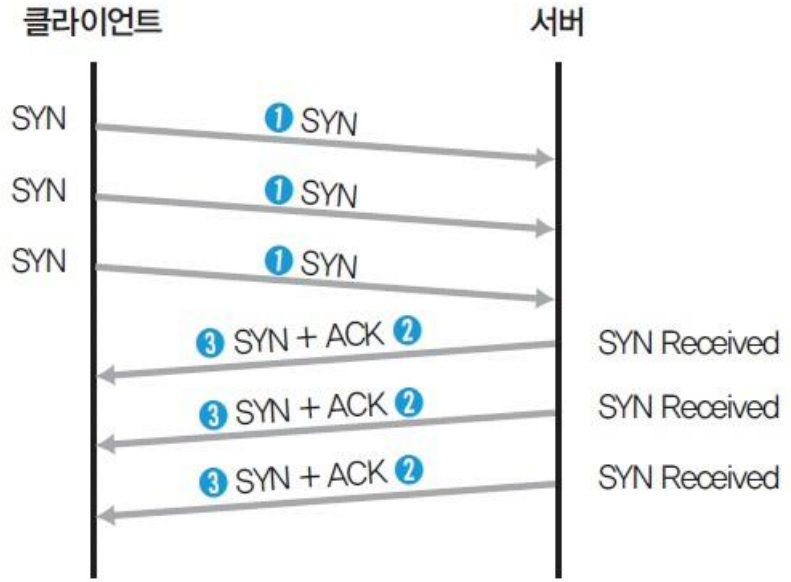


그림 11-8 SYN Flooding 공격 시 쓰리웨이 핸드셰이킹

① 공격자는 많은 숫자의 SYN 패킷을 서버에 보냄

② 서버는 받은 SYN 패킷에 대한

③ SYN/ACK 패킷을 각 클라이언트로 보냄.

④ 서버는 자신이 보낸 SYN/ACK 패킷에 대한 ACK 패킷을 받지 못함.

⑤ 서버는 세션의 연결을 기다리게 되고 공격은 성공함.

■ SYN Flooding 공격 이해하기

- 'SYN Received' 상태로 ACK 패킷을 기다리는 것을 '백로그Backlog에 빠졌다'고 표현

표 11-1 서버별 최대 클라이언트 수(기본값)

서버	최대 클라이언트 수
IIS 서버 5.0	100,000
아파치(Apache) 서버	150
FTP, 텔넷(Telnet) 서버	100

1. DoS 공격

실습 11-2 SYN Flooding 공격하기

실습환경
- 공격자 시스템 : 우분투 데스크탑 14
- 공격 대상 시스템 : 윈도우 서버 2012
- 필요 프로그램 : hping3

① 웹 서비스 시작하기

- 공격 대상 시스템에 IIS 설치

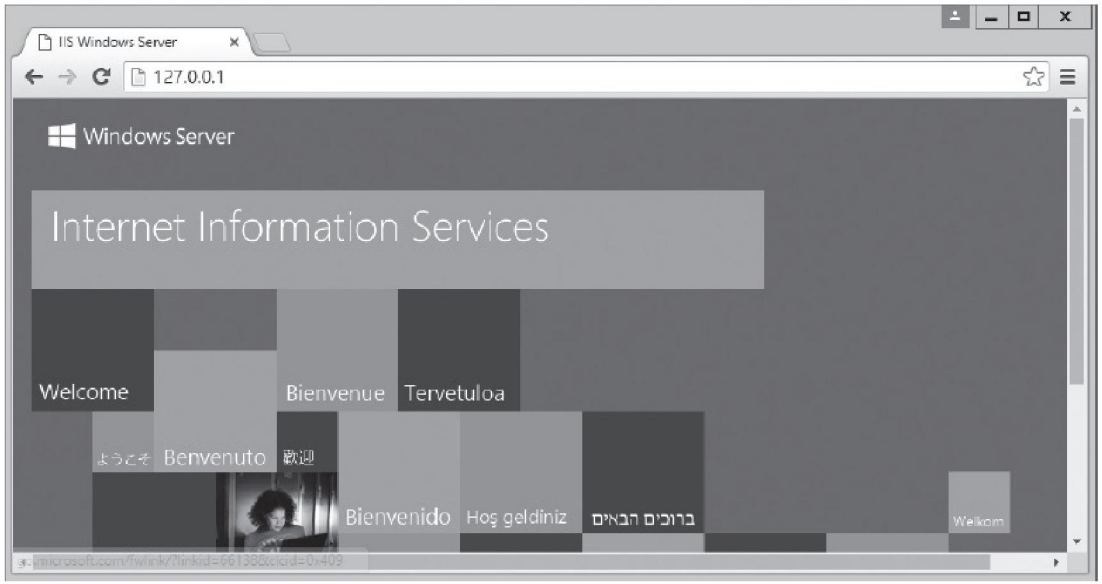


그림 11-9 IIS 웹 서버 설치 후 확인하기

② SYN Flooding 공격 수행하기

- hping3을 이용하면 아주 짧은 시간에 많은 패킷을 보내 SYN Flooding 공격을 간단히 수행할 수 있음

  hping3 --rand-source 192.168.0.100 -p 80 -S

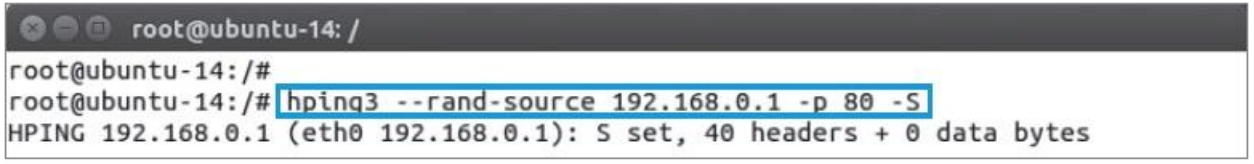


그림 11-10 SYN Flooding 공격 수행하기

- -p 80 : 80번 포트에 대해 패킷 전송
- -S : TCP 패킷 중 SYN만 전송

③ SYN Flooding 공격의 패킷 확인하기

- hping3로 보낸 패킷을 공격 대상 시스템에서 Wireshark로 캡처

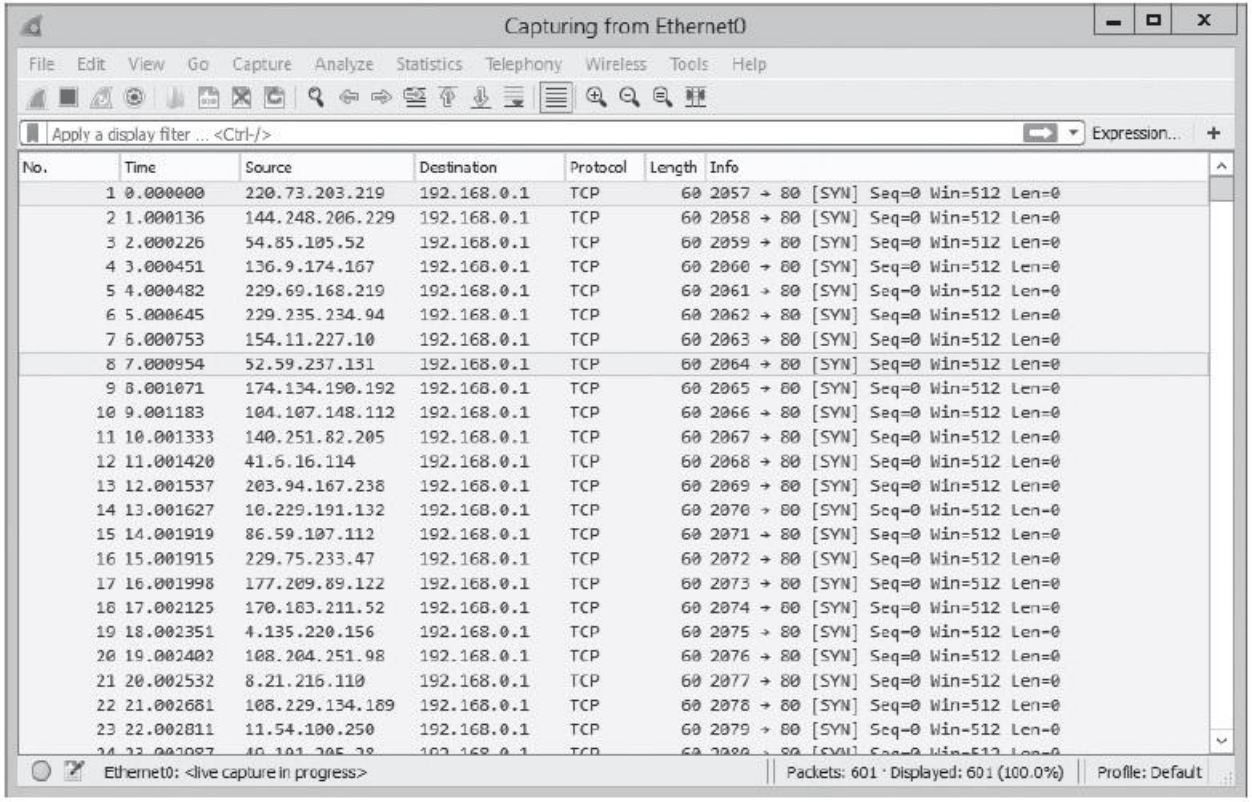


그림 11-11 패킷 확인하기

④ 공격 확인하기

- 현재 연결된 세션에 관한 정보를 볼 수 있는 netstat로 공격 받고 있는지 확인

```
netstat -an
```

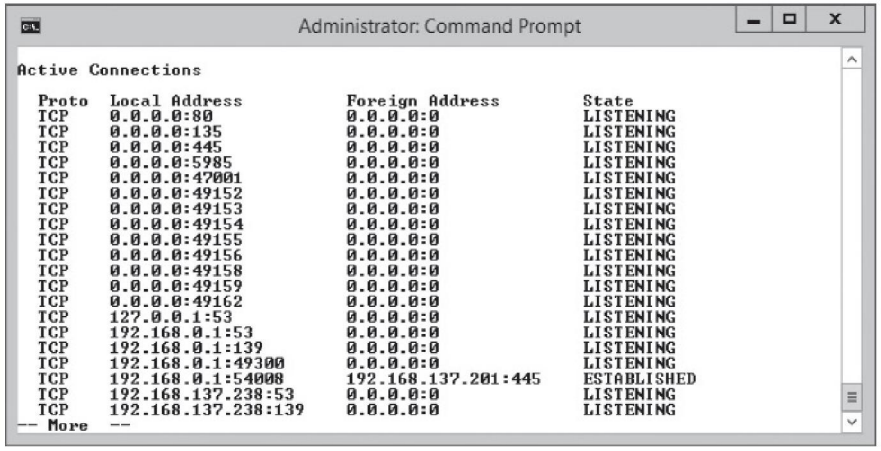


그림 11-12 SYN Flooding 공격 전의 netstat 상태

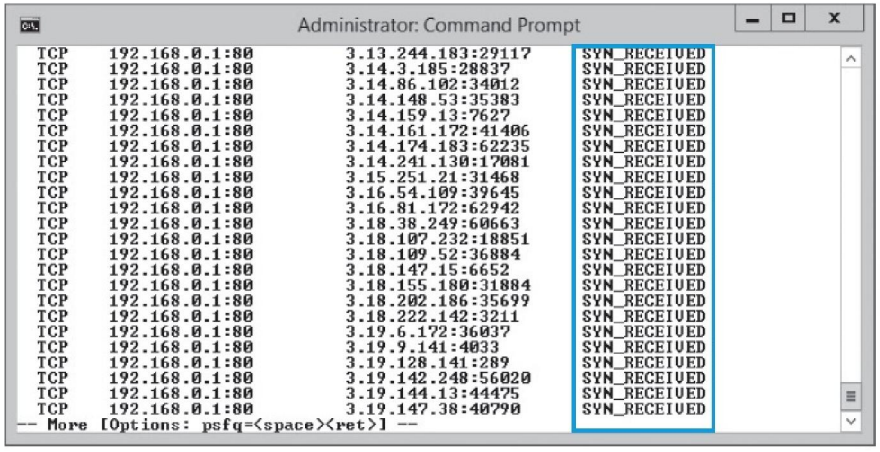


그림 11-13 SYN Flooding 공격 후의 netstat 상태

④ 공격 확인하기

- 다수의 IP에 대해 SYN_RECV 상태가 되어 있으면 웹 서버로 정상 접속이 불가

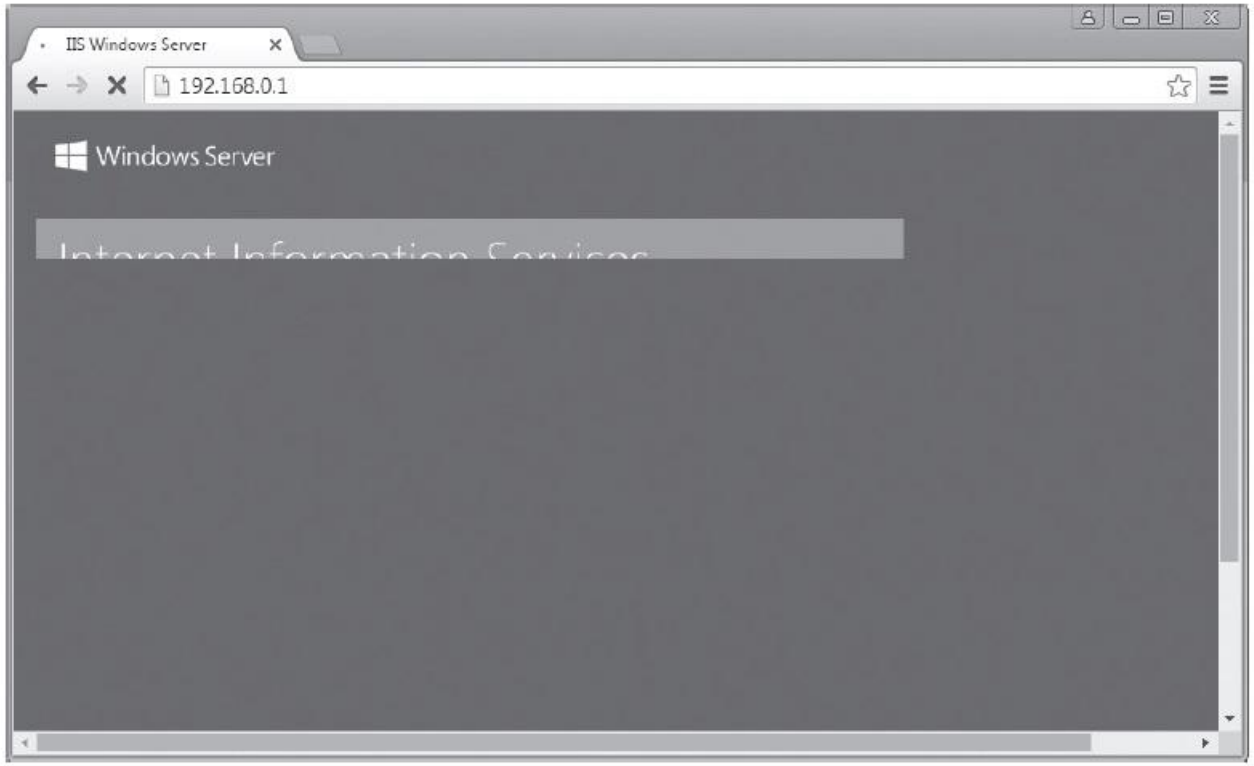


그림 11-14 SYN Flooding 공격 후 접속이 원활하지 않은 경우

■ SYN Flooding 보안 대책

- 시스템 패치 설치
- 침입 탐지 시스템(IDS)이나 침입 차단 시스템(IPS)을 설치
- 짧은 시간 안에 똑같은 형태의 패킷을 보내는 형태의 공격을 인지했을 경우, 그에 해당하는 IP 주소 대역의 접속을 금지하거나 방화벽 또는 라우터에서 해당 접속을 금지시킴.
- 서버에서 클라이언트로 보내는 SYN+ACK 패킷에 암호화 기술을 이용해서 인증 정보가 담긴 시퀀스 넘버를 생성하여 클라이언트에 보내는 Syn_Cookie 이용

■ SYN Flooding 보안 대책

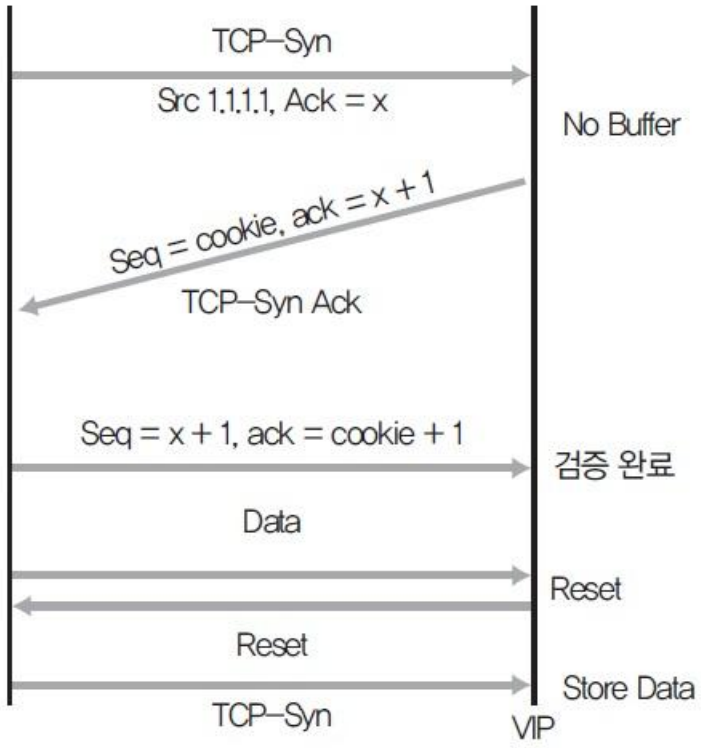


그림 11-15 Syn_Cookie의 동작

① 클라이언트로부터 SYN 패킷을 받으면, 간단한 인증 정보가 담긴 Syn_Cookie를 시퀀스 값에 넣고 세션을 닫음.

② 클라이언트가 Syn_Cookie가 포함된 값으로 ACK를 보내면 서버는 세션을 다시 열고 통신을 시작

표 11-2 SYN 시의 서버별 대기 시간

서버	대기 시간
윈도우 NT/2K	255초
유닉스/리눅스	60초
아파치	300초(/etc/httpd.conf에서 설정 가능)
보안 패치	15초

■ Boink, Bonk, Teardrop

- Boink(보잉크), Bonk(봉크), Teardrop(티어드랍)은 시스템의 패킷 재전송과 재조합에 과부하가 걸리도록 시퀀스 넘버를 속임.

그림 11-17 Bonk, Boink, Teardrop의 개념도

■ Boink, Bonk, Teardrop 이해하기

- Bonk : 처음 패킷을 1번으로 보낸 후 두 번째와 세 번째 패킷의 시퀀스 넘버를 모두 1번으로 조작해서 보냄.
- Boink : 처음 패킷을 1번으로 보낸 후 두 번째 패킷은 101번, 세 번째 패킷은 201번 등으로 정상적으로 보내다가 중간에서 일정한 시퀀스 넘버를 보냄.
- Teardrop : 시퀀스 넘버를 일정하게 바꾸는 것을 넘어 중첩과 빈 공간을 만들어 시퀀스 넘버가 좀더 복잡해지도록 섞음.

→ 전혀 맞지 않는 시퀀스 넘버 때문에 공격 대상이 패킷화된 데이터를 제조합하는 데 혼란이 생겨 CPU에 과부하가 걸리게 됨.

■ Boink, Bonk, Teardrop 이해하기

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

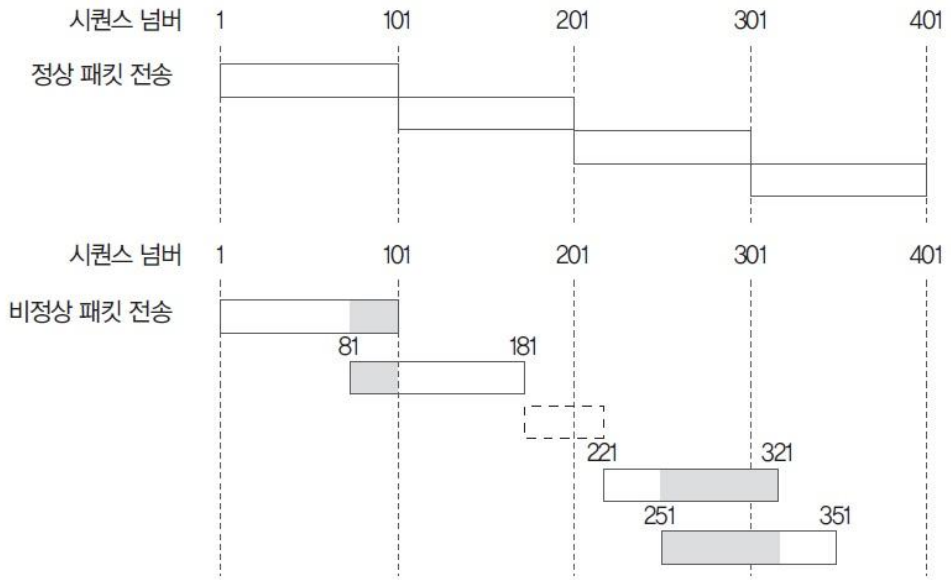


그림 11-18 Teardrop 공격 시 패킷의 배치

1. DoS 공격

실습 11-3 Teardrop 공격하기

실습환경
- 공격자 시스템 : 우분투 데스크탑 14
- 공격 대상 시스템 : 윈도우 서버 2012
- 필요 프로그램 : hping3

① Teardrop 공격 수행하기

hping3 -a 200.200.200.200 192.168.0.1 --id 3200 --seqnum -p 21 -d 320 --flood

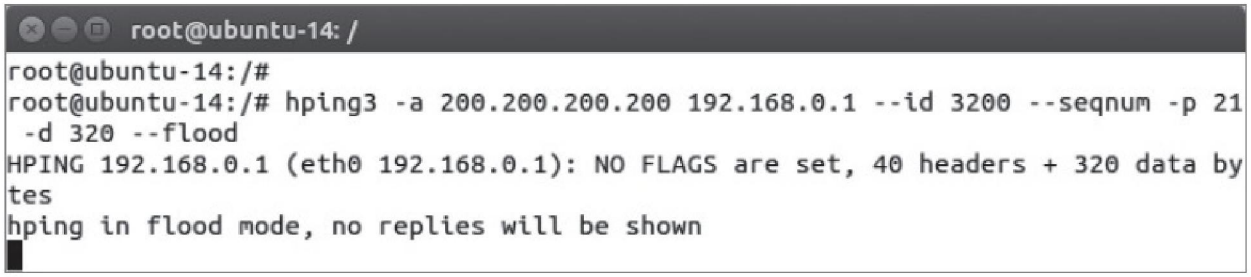


그림 11-19 Teardrop 공격 실행

- --id 3200 : TCP 패킷의 ID 값, 같은 ID 값이면 동일한 세션의 TCP 패킷으로 간주
- --seqnum : TCP 패킷의 시퀀스 넘버를 임의로 설정
- -d 320 : 패킷의 길이를 320 바이트로 설정

② Teardrop 공격의 패킷 분석하기

- TCP 패킷의 시퀀스 넘버가 임의로 생성되어 전달되는 것을 확인할 수 있음.

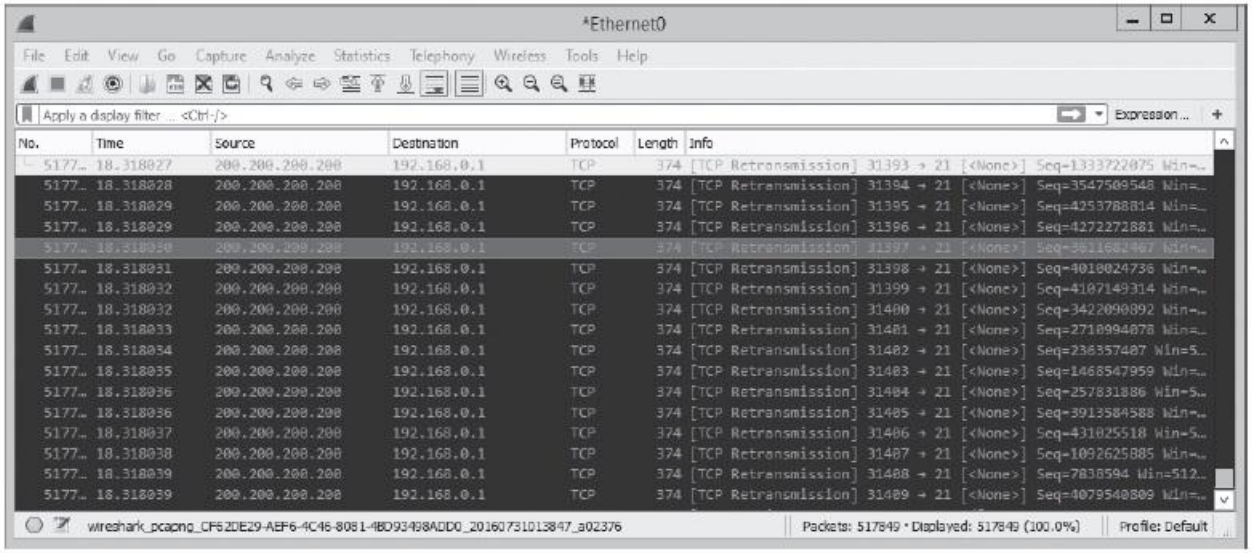


그림 11-20 Teardrop 공격 시 TCP Dump

■ Boink, Bonk, Teardrop 보안 대책

- SYN Flooding이나 Ping of Death 공격의 대응책과 같음.

1.5 Land

■ Land

- 시스템을 나쁜 상태에 빠지게 하는 것
- 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소의 값을 똑같이 만들어서 공
- 격 대상에게 보냄(조작된 IP 주소 값은 공격 대상의 IP 주소여야 함).
- Land 공격법은 동시 사용자 수를 점유하여 CPU 부하까지 올림.

그림 11-21 Land 공격의 개념도

1. DoS 공격

실습 11-4 Land 공격하기

실습환경
- 공격자 시스템 : 우분투 데스크탑 14
- 공격 대상 시스템 : 윈도우 서버 2012
- 필요 프로그램 : hping3

① Land 공격 수행하기

hping3 192.168.0.1 -a 192.168.0.1 --icmp --flood

```
root@ubuntu-14: /
root@ubuntu-14:/# hping3 192.168.0.1 -a 192.168.0.1 --icmp --flood
HPING 192.168.0.1 (eth0 192.168.0.1): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

그림 11-22 Land 공격 실행

② Land 공격의 패킷 분석하기

- hping3로 보낸 패킷을 Wireshark로 캡처

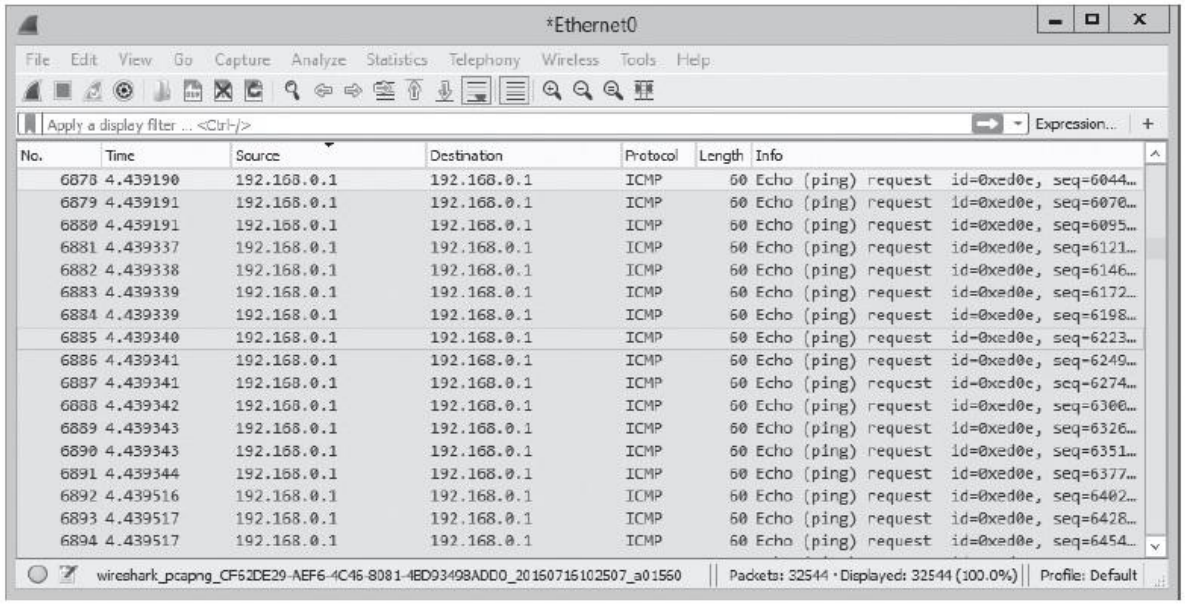


그림 11-23 Land 공격 시 TCP Dump

■ Land 보안 대책

- 라우터나 방화벽에서 출발지 IP 주소가 내부 IP 주소와 동일한 패킷 차단

■ Smurf(스머프) 공격

- 웜이 네트워크를 공격할 때 많이 사용하는 것으로 ICMP 패킷 이용
- 라우터는 기본적으로 브로드캐스트를 지원하지 않아 다른 네트워크에 브로드캐스트를 할 때는 다이렉트 브로드캐스트를 하게 됨.
- 목적지 IP 주소 값을 255.255.255.255로 설정하여 패킷을 보내면 라우터가 외부 네트워크로 나가는 것을 차단하여 내부 네트워크인 랜(LAN) 안에서만 동작

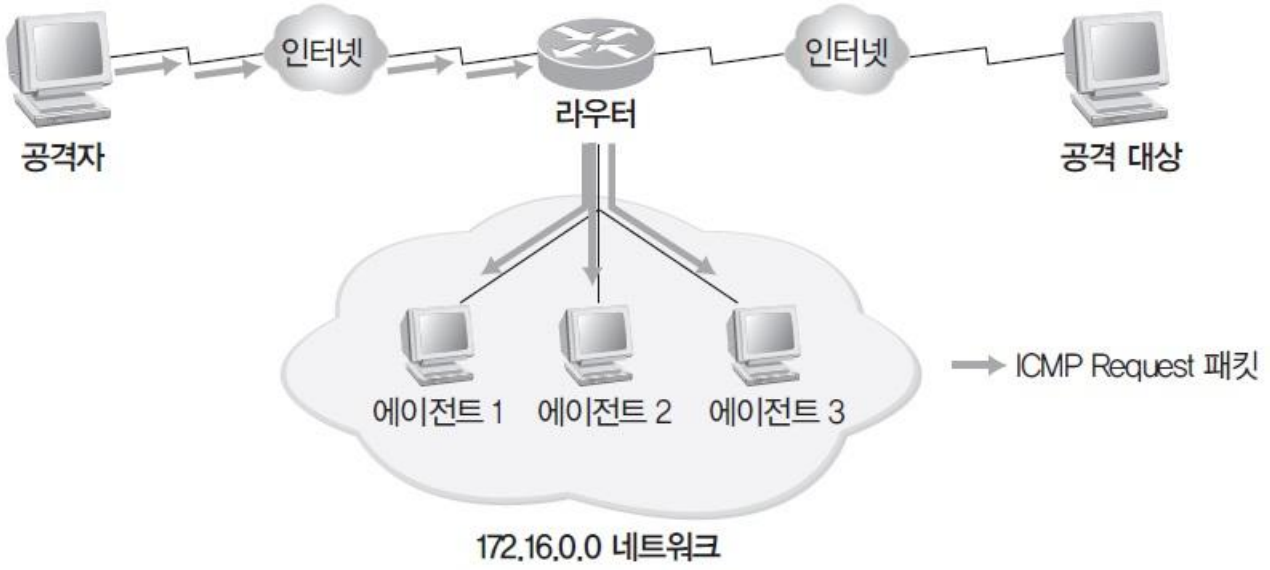


그림 11-25 공격자에 의한 Smurf 공격의 실시

■ Smurf(스머프) 공격

- ICMP Request를 받게 된 네트워크는 ICMP Request 패킷의 위조된 시작 IP 주소로 ICMP Reply를 다시 보냄.
- 공격 대상은 수많은 ICMP Reply를 받게 되고 Ping of Death처럼 수많은 패킷이 시스템을 과부하 상태로 만듦.

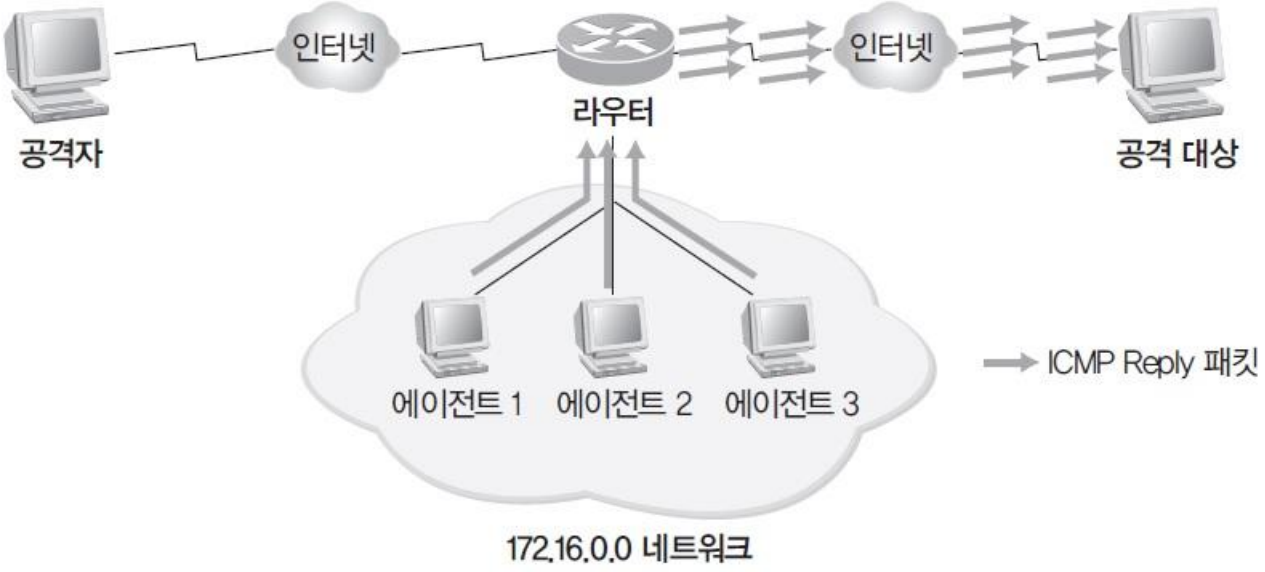


그림 11-26 에이전트에 의한 Smurf 공격의 수행

1. DoS 공격

실습 11-5 Smurf 공격의 원리 이해하기

실습환경
- 공격자 시스템 : 우분투 데스크탑 14
- 에이전트 시스템 : 우분투 서버 16
- 공격 대상 시스템 : 윈도우 서버 2012
- 필요 프로그램 : hping3

① Smurf 공격 수행하기

hping3 192.168.0.2 -a 192.168.0.1 --icmp --flood

```
root@ubuntu-14: /
root@ubuntu-14:/# hping3 192.168.0.2 -a 192.168.0.1 --icmp --flood
HPING 192.168.0.2 (eth0 192.168.0.2): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

그림 11-28 Smurf 공격의 실시

② Smurf 공격의 패킷 분석하기

- TCP Dump와 Wireshark로 캡처한 결과 확인

```
root@ubuntu-14: /
22:02:08.463899 IP 192.168.0.1 > 192.168.0.2: ICMP echo request, id 59404, seq 6
4515, length 8
        0x0000:  4500 001c 36b2 0000 4001 c2db c0a8 0001  E...6...@.......
        0x0010:  c0a8 0002 0800 13ef e80c fc03            ............
22:02:08.463903 IP 192.168.0.1 > 192.168.0.2: ICMP echo request, id 59404, seq 6
4771, length 8
        0x0000:  4500 001c 3b6d 0000 4001 be20 c0a8 0001  E...;m..@.......
        0x0010:  c0a8 0002 0800 12ef e80c fd03            ............
```

그림 11-29 공격자 시스템에서 Smurf 공격의 TCP Dump

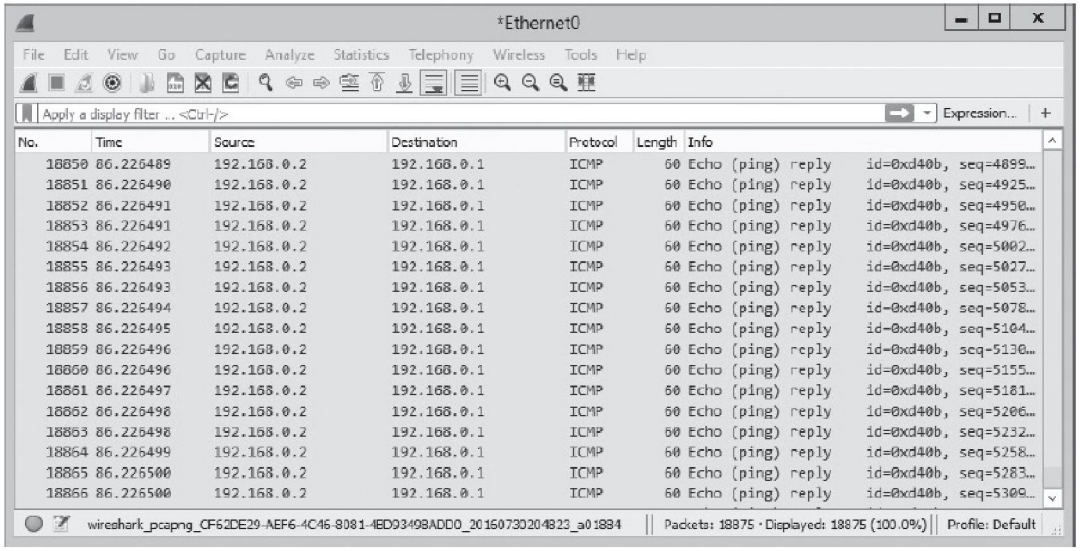


그림 11-30 공격 대상 시스템에서 Smurf 공격의 Wireshark 결과

② Smurf 공격의 패킷 분석하기

- hping3 명령을 조금만 바꾸면, 실제 smurf 공격 수행 가능

  hping3 192.168.0.255 -a [공격 대상 IP] --icmp --flood

■ Smurf 보안 대책

- 다이렉트 브로드캐스트를 막음.

■ 7계층 DoS 공격

- 최근의 DoS 공격은 웹 어플리케이션 등을 대상으로 공격 방향을 전환

표 11-3 3, 4계층 DoS 공격과 7계층 DoS 공격의 차이

	3, 4계층 DoS 공격	7계층 DoS 공격
주요 공격	• 대역폭 고갈 공격 • 세션 고갈 공격	• 서버의 자원 고갈 공격
주요 프로토콜	• TCP, UDP, ICMP	• HTTP, SMTP, FTP, VoIP 등
특징	• 단순한 Flooding 형태의 트래픽을 대량으로 발생시켜 공격 • Spoofed IP로 비정상적인 트래픽을 이용한 공격의 비율이 높음 • 보안 장비를 통해 방어 가능	• 정상 트래픽을 이용한 공격 • 소량의 트래픽을 이용한 공격 • 특정 어플리케이션의 취약점을 이용한 공격

■ 7계층 공격의 주요 특징

- 정상적인 TCP/UDP 연결 기반의 공격으로, 변조된 IP가 아닌 정상 IP를 이용한 접속 요청 후 공격이 진행되어 정상 사용자의 트래픽과 구분하기가 어려워 탐지가 어려움.
- 소량의 트래픽을 이용한 공격으로 오랜 시간에 걸쳐 서서히 공격이 진행되어 탐지가 어려움.
- 특정 서비스의 취약점을 이용하여 공격(현재까지는 웹 서비스의 취약점을 이용한 공격이 주를 이루고 있음)

■ 웹 어플리케이션에 대한 DoS 공격 유형

① HTTP GET Flooding 공격

- 공격 대상 시스템에 TCP 쓰리웨이 핸드셰이킹 과정을 통해 정상적으로 접속한 뒤, HTTP의 GET Method를 통해 특정 페이지를 무한대로 실행하는 방식

② HTTP CC 공격

- DoS 공격 기법에 'Cache-Control: no-store, must-revalidate' 옵션을 사용하면, 웹 서버는 캐시를 사용하지 않고 응답을 해야 하므로 웹 서비스의 부하가 증가

③ 동적 HTTP Request Flooding 공격

- 요청 페이지를 변경하여 웹 페이지를 지속적으로 요청하는 기법

④ Slow HTTP Header DoS(Slowloris) 공격

- 서버로 전달할 HTTP 메시지의 Header 정보를 비정상적으로 조작하여 웹 서버가 헤더 정보를 완전히 수신할 때까지 연결을 유지하도록 하여 시스템 자원을 소비시켜 다른 클라이언트의 정상적인 서비스를 방해하는 공격
- 불안전한 메시지를 수신한 웹 서버는 클라이언트의 요청이 끝나지 않은 것으로 인식하여 웹 로그를 기록하지 않음.

■ 웹 어플리케이션에 대한 DoS 공격 유형

⑥ Slow HTTP POST 공격

- 2010년 11월 미국 워싱턴에서 개최된 2010 OWASP AppSec Conference에서 소개
- 웹 서버와의 커넥션을 최대한 장시간 동안 유지하여 웹 서버가 정상적인 이용자의 접속을 받아들일 수 없게 하는 방식

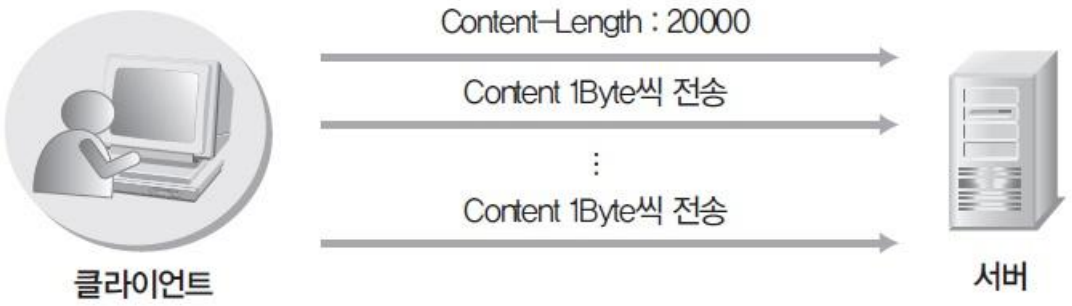


그림 11-31 Slow HTTP POST 공격의 구조

- 필요로 하는 Content-Length를 설정하면 Slow HTTP POST 공격을 어느 정도 대응 가능

■ 웹 어플리케이션에 대한 DoS 공격 유형

⑦ Mail Bomb

- 흔히 폭탄 메일이라고 하며, 스팸 메일도 같은 종류
- 메일 서버는 각 사용자에게 일정한 디스크 공간을 할당하는데, 메일이 폭주하여 디스크 공간을 가득 채우면 정작 받아야 할 메일을 받을 수 없음.

1. DoS 공격

실습 11-6 웹 어플리케이션 DoS 공격

실습환경
- 공격자 시스템 : 윈도우 7
- 공격 대상 시스템 : 윈도우 서버 2012(IIS 웹 서비스)
- 필요 프로그램 : SwitchBlade V4.0, Python 2.7, RUDY

■ Slow HTTP Header DoS(Slowloris) 공격

① 정상적인 웹 접속하기

- 웹 접속 시 생성되는 정상적인 HTTP 패킷 중에서 GET 패킷 확인

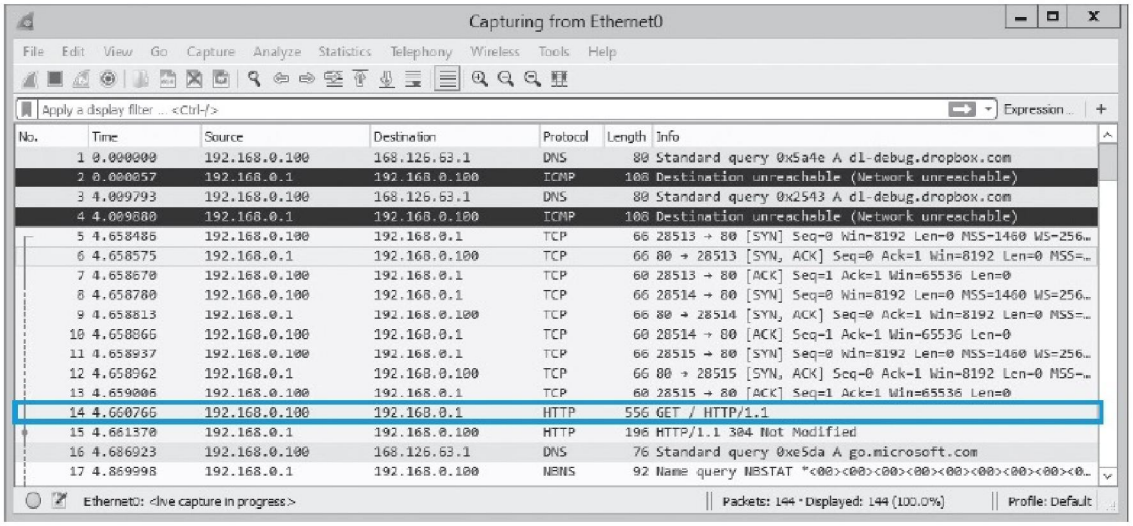


그림 11-32 정상적인 HTTP GET 메서드의 실행 패킷 목록

① 정상적인 웹 접속하기

- GET 패킷의 상세 내용 확인

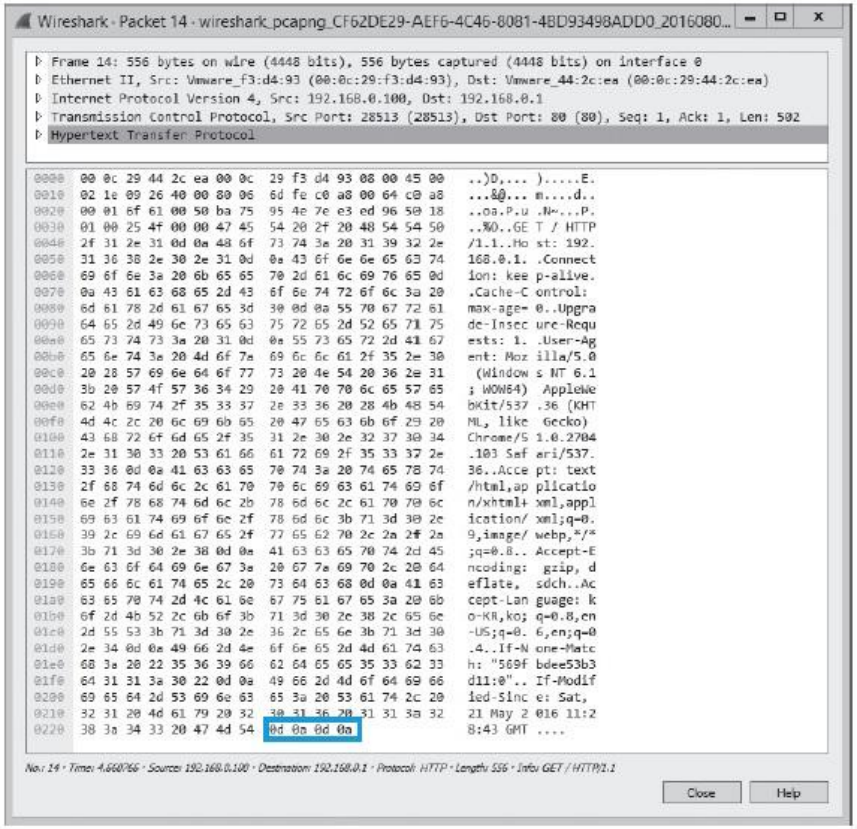


그림 11-33 정상적인 HTTP GET 패킷

② Slow HTTP Header DoS(Slowloris) 공격 수행하기

- SwitchBlade를 다운로드한 파일의 압축을 푼 뒤, 'gui.exe'를 실행
- 패킷 확인을 위해 공격 대상에서 Wireshark를 실행시킨 뒤 <Run attack> 버튼을 눌러 공격을 실행

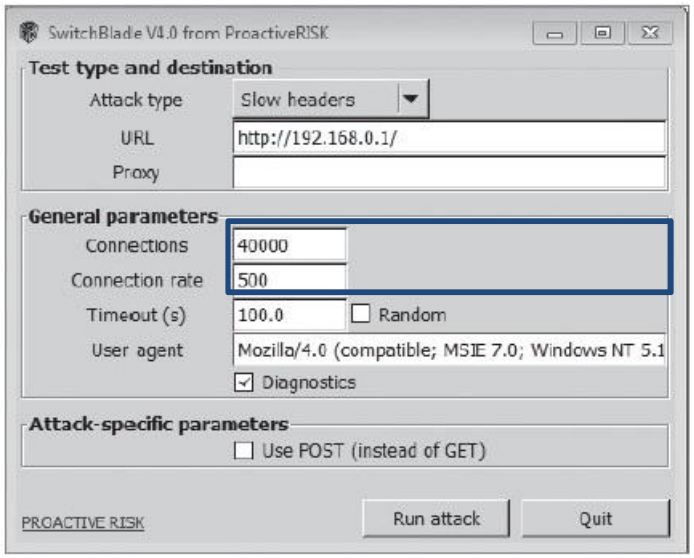


그림 11-34 Slow HTTP Header DoS 공격의 설정 및 실행

② Slow HTTP Header DoS(Slowloris) 공격 수행하기

- 공격이 끝나면 Slow HTTP Header DoS 공격 시에 해당 서버에서 최대로 가능한 연결 수를 확인할 수 있음.

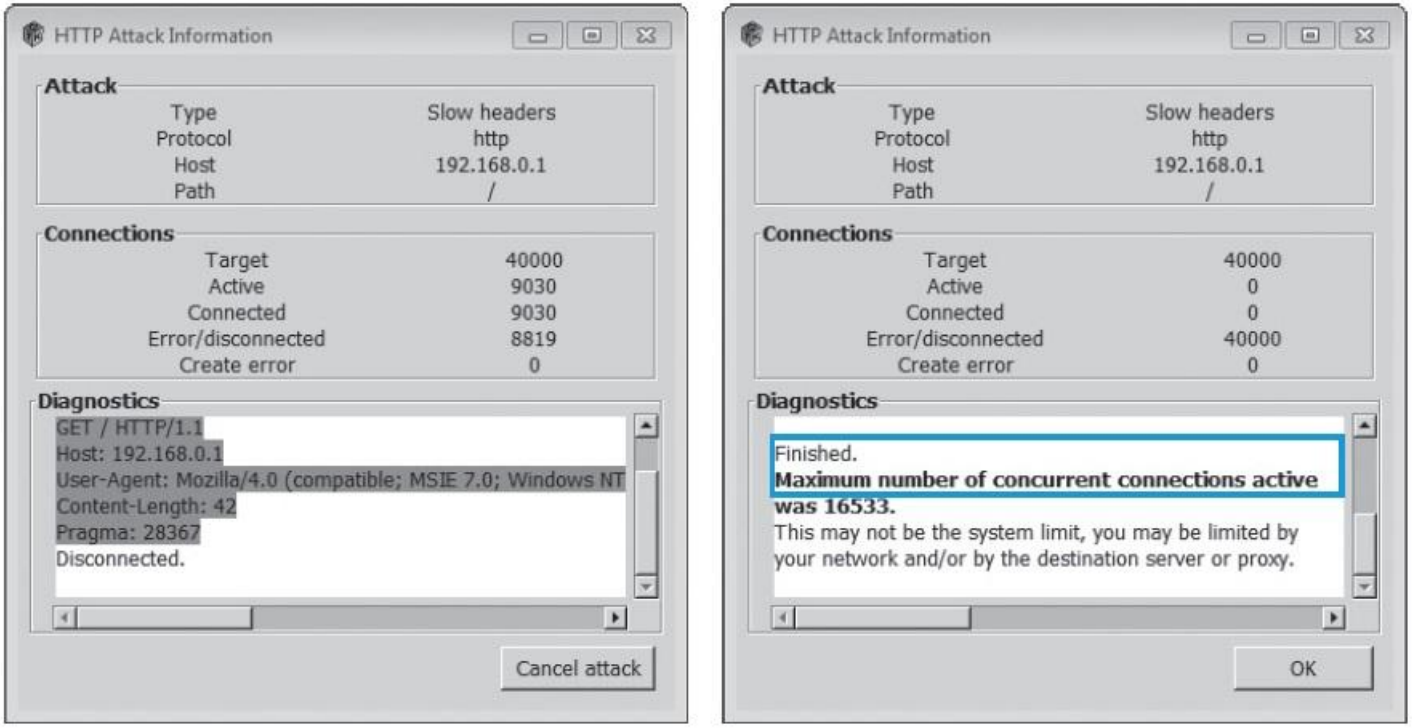


그림 11-35 Slow HTTP Header DoS 공격 중과 후의 결과 화면

③ Slow HTTP Header DoS(Slowloris) 공격 패킷 확인하기

- 공격 대상 서버에서 패킷을 확인

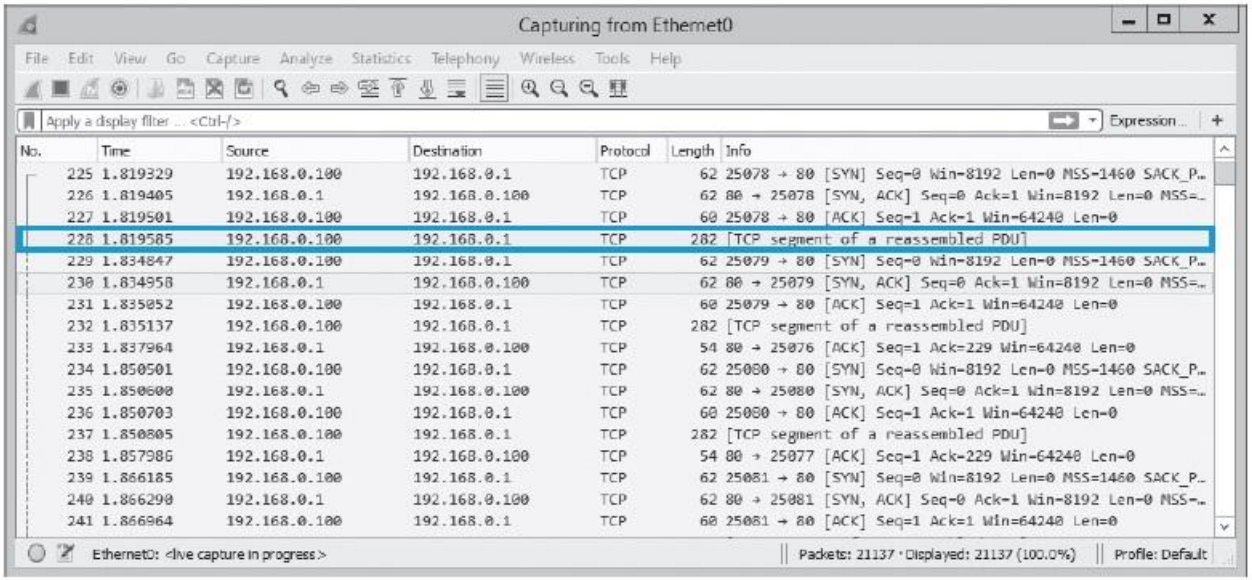


그림 11-36 Slow HTTP Header DoS 공격의 패킷 목록

③ Slow HTTP Header DoS(Slowloris) 공격 패킷 확인하기

- 공격자는 해당 패킷이 완료되지 않은 것처럼 웹 서버를 속이고 해당 연결을 유지시켜 웹 서버의 자원을 고갈시킴.

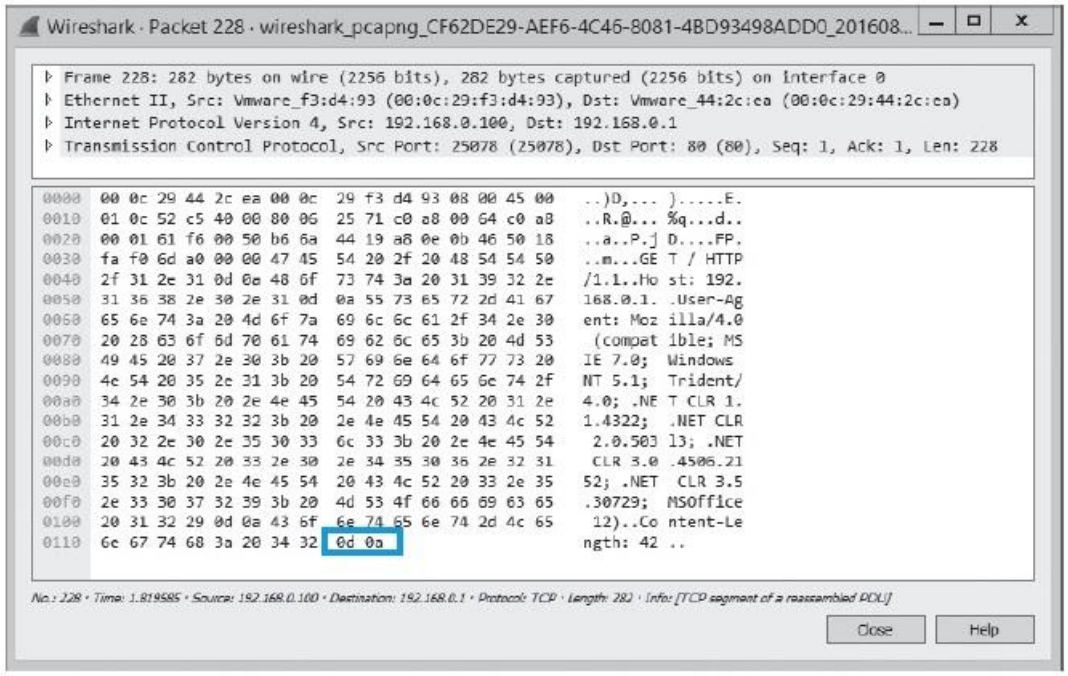
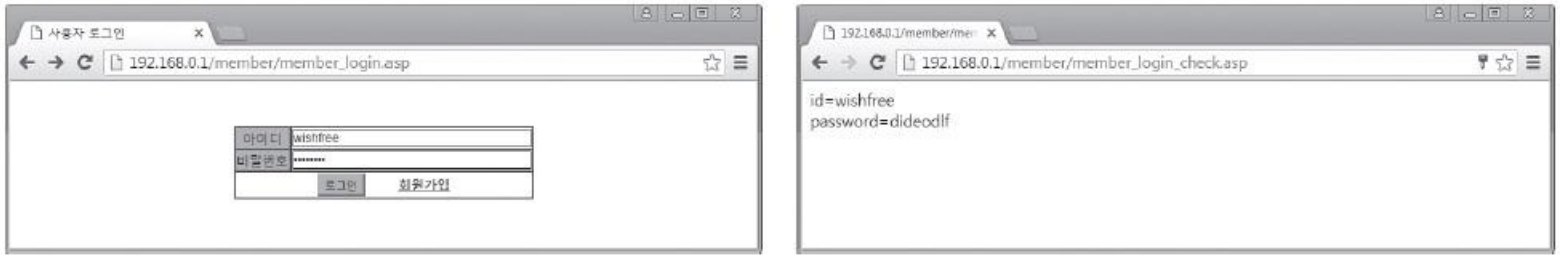


그림 11-37 Slow HTTP Header DoS 공격 패킷의 상세 내용

■ Slow HTTP POST 공격

① 정상적인 웹 접속하기

- 아이디와 패스워드를 입력하면 해당 내역을 받아 출력해주는 POST 기능 구현



(a) 아이디와 패스워드 입력 (b) 입력받은 아이디와 패스워드를 POST로 출력

그림 11-38 아이디와 패스워드를 입력하면 POST로 출력하는 기능

① 정상적인 웹 접속하기

- POST로 데이터가 전달되고 Content-Length는 31

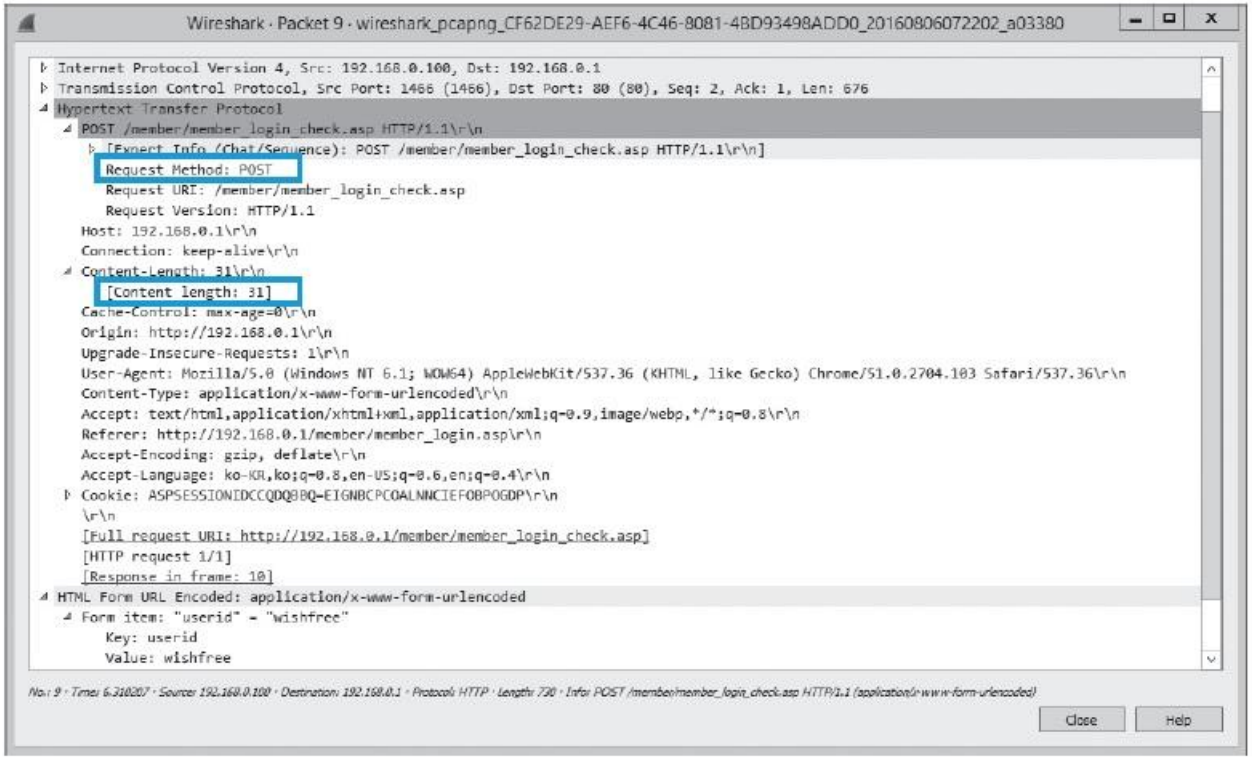


그림 11-39 정상적인 POST 패킷

② Slow HTTP POST 공격 수행하기

- RUDY는 명령을 실행한 뒤 결과 값을 보며 어떤 필드를 이용하여 공격을 할지 선택할 수 있음.

  python r-u-dead-yet.py http://192.168.0.1/member/member_login.asp

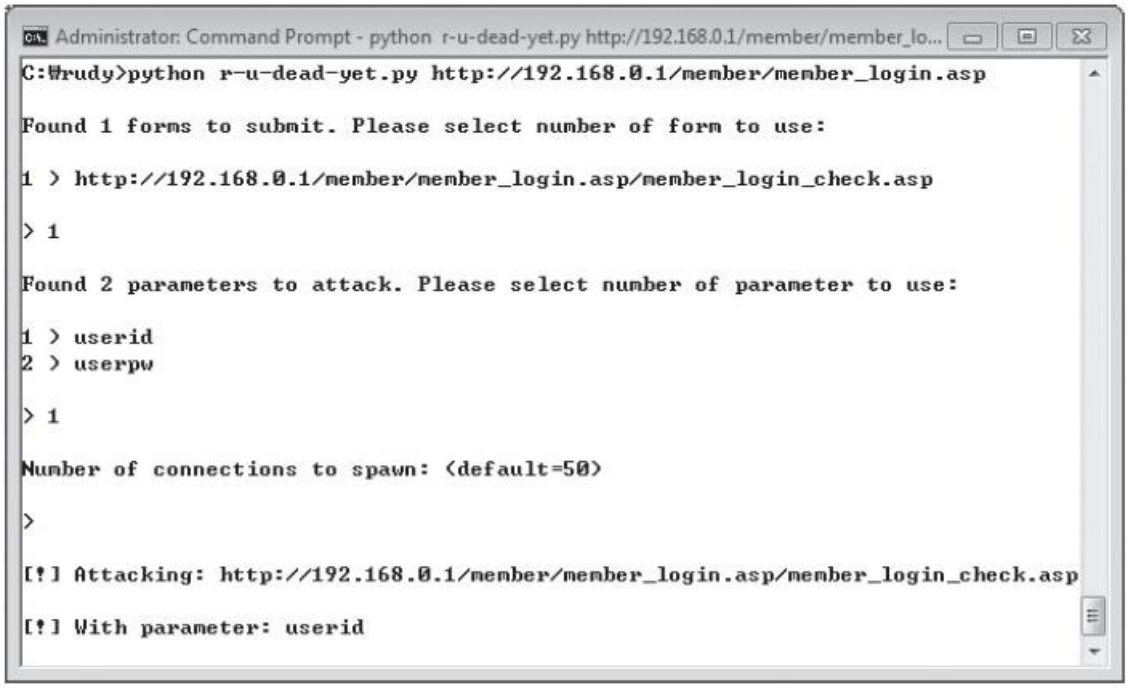


그림 11-40 RUDY로 Slow HTTP POST 공격 수행

② Slow HTTP POST 공격 패킷 확인

- Content-Length 값이 100,000,000으로 설정된 패킷이 전송된 후 길이가 1바이트인 패킷이 전송되는 과정을 확인

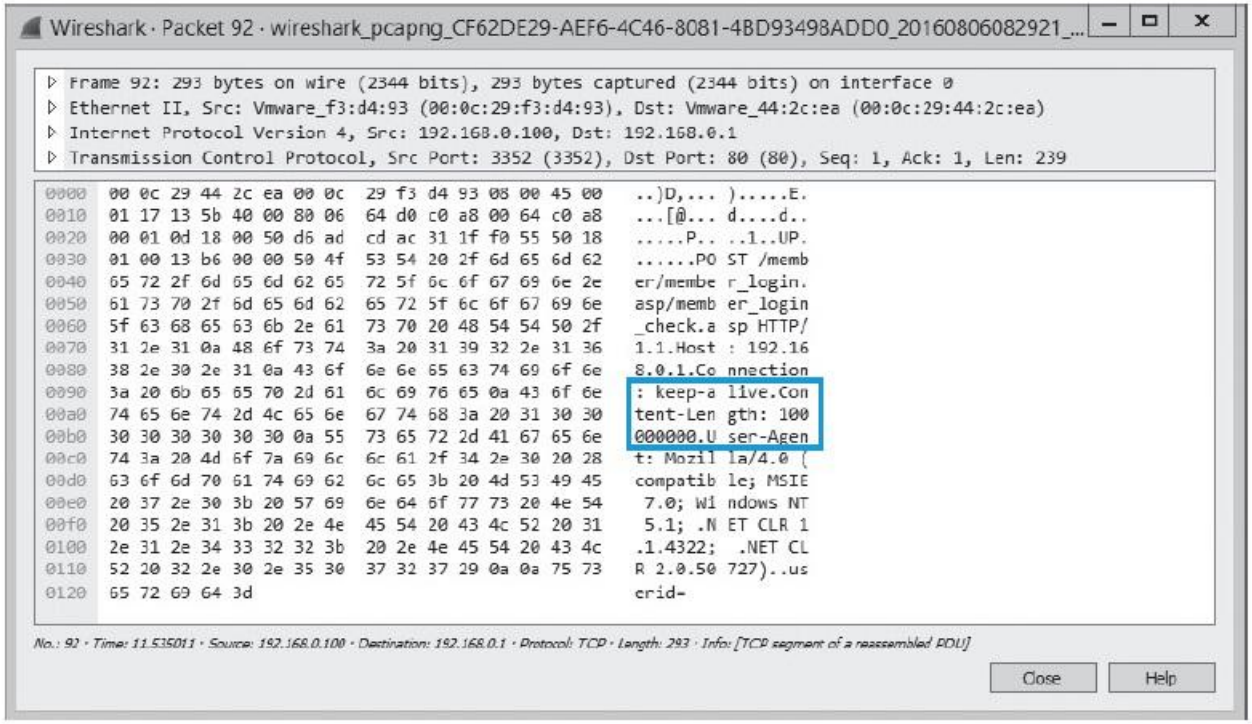


그림 11-41 Content-Length 값을 100,000,000으로 설정한 패킷

② Slow HTTP POST 공격 패킷 확인

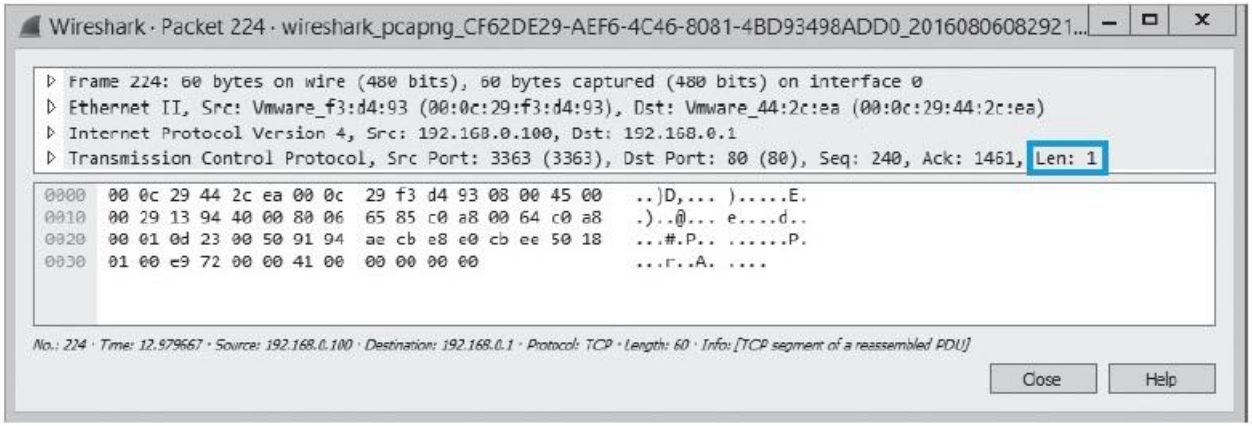


그림 11-42 길이가 1바이트로 설정된 연결 유지 패킷

■ DDoS(Distributed Denial of Service)

- DoS 공격이 발전된 것
- 피해 양상이 상당히 심각하지만 확실한 대책이 없음.
- 공격자의 위치와 구체적인 발원지를 파악하는 일이 무척 어려워 여전히 대응이 어려운 공격 중의 하나
- 특성상 대부분의 DDoS 공격은 자동화된 툴을 이용

■ DDoS 공격이 이루어지기 위한 기본 구성

- 공격자(Attacker) : 공격을 주도하는 해커의 컴퓨터
- 마스터(Master) : 공격자에게 직접 명령을 받는 시스템, 여러 대의 에이전트 관리
- 핸들러(Handler) 프로그램 : 마스터 시스템 역할을 수행하는 프로그램
- 에이전트(Agent) : 공격 대상에 직접 공격을 가하는 시스템
- 데몬(Daemon) 프로그램 : 에이전트 시스템 역할을 수행하는 프로그램

■ DDoS 공격 구성도

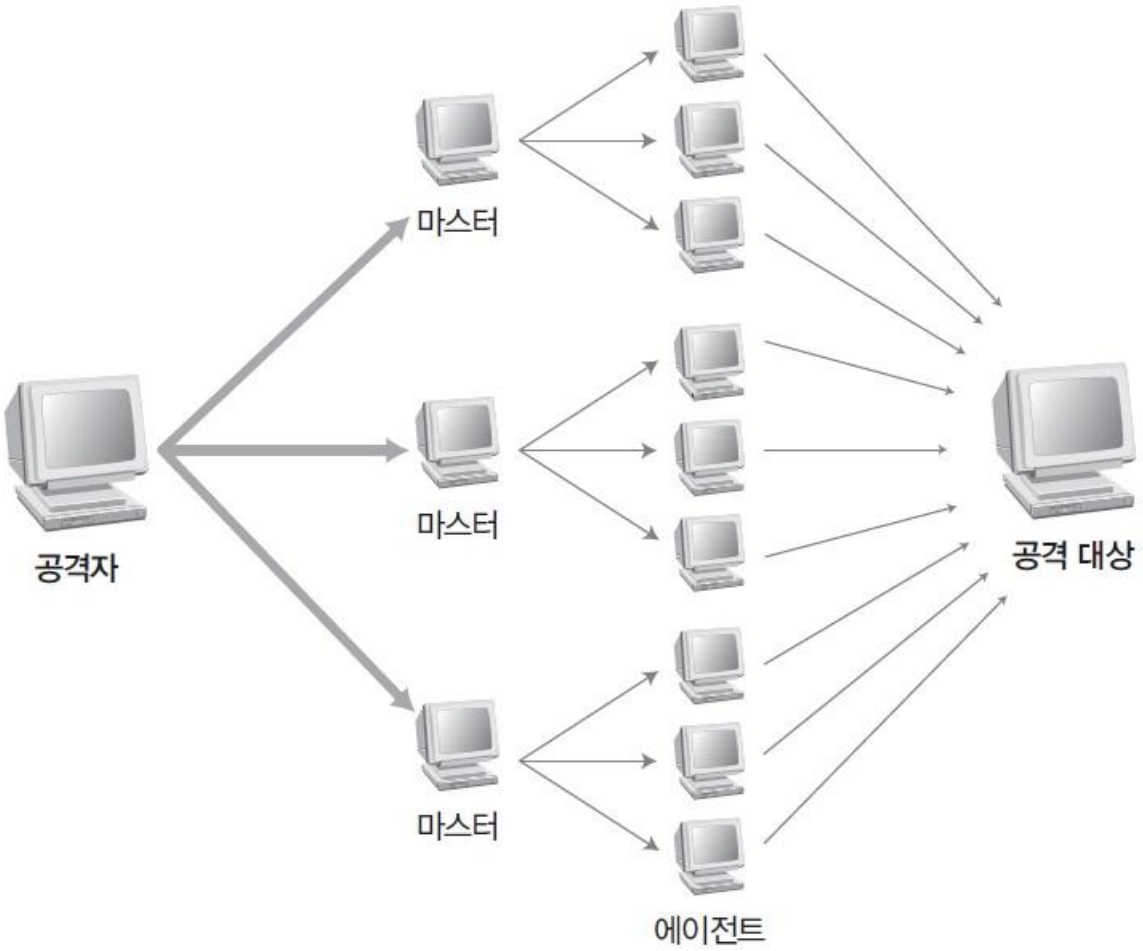


그림 11-43 DDoS 공격 구성도

■ DDoS 공격 개념도

- 공격자는 폭력 조직의 두목, 마스터는 행동대장, 에이전트는 졸개에 비유
- DDoS 공격에서는 중간자 역할을 하는 마스터와 에이전트가 피해자이기도 하다는 것이 폭력 조직과 다름.

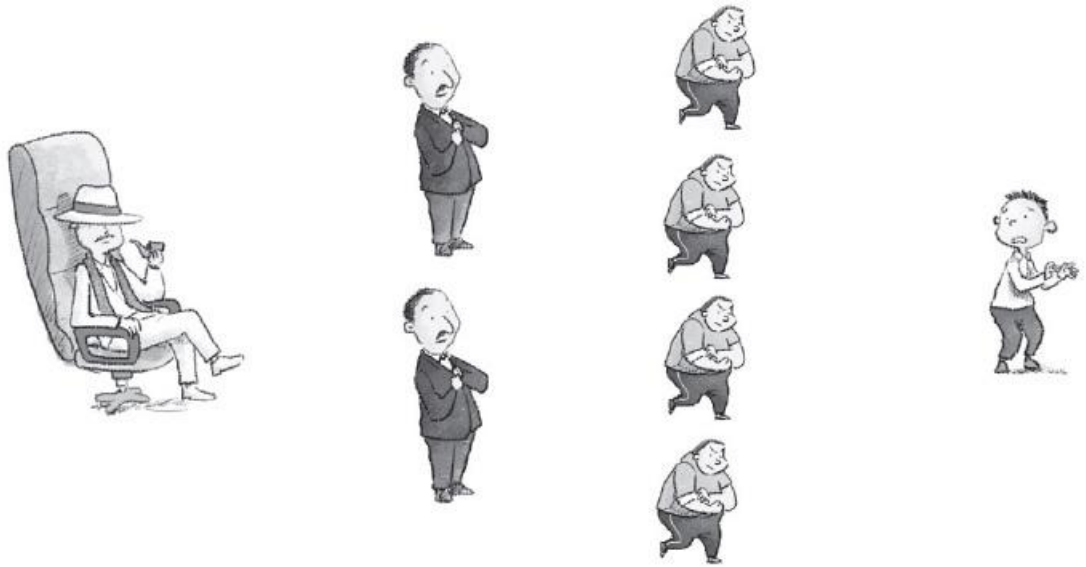


그림 11-44 DDoS 공격 개념도

■ DDoS 공격 순서

① 많은 사람이 사용하며 대역폭이 넓고 관리자가 모든 시스템을 세세하게 관리할 수 없는 곳의 계정을 획득한 후, 스니핑이나 버퍼 오버플로우 등의 공격으로 설치 권한이나 루트 권한을 획득

② 잠재적인 공격 대상을 파악하기 위해 네트워크 블록별로 스캐닝을 실시한 후, 원격지에서 버퍼 오버플로우를 일으킬 수 있는 취약한 서비스를 제공하는 서버를 파악

③ 취약한 시스템 목록을 확인한 후 실제 공격을 위한 Exploit을 작성

④ 권한을 획득한 시스템에 침투하여 Exploit을 컴파일하여 설치

⑤ 설치한 Exploit으로 공격 시작

■ Trinoo(트리누)

- 1999년 6월 말부터 7월 사이에 퍼지기 시작한 것으로, 미네소타 대학 사고의 주범(원래 이름은 Trin00)
- 솔라리스 2.x 시스템에서 처음 발견되었으며, 최소 227개 시스템이 공격에 쓰인 것으로 알려져 있음.
- UDP를 기본으로 공격을 시행하며 'statd, cmsd, ttdbserverd' 데몬이 주된 공격 대상

표 11-4 Trinoo 통신 프로토콜과 포트

접속자	접속 대상	프로토콜	포트
공격자	마스터	TCP	27665
마스터	에이전트	UDP	27444
에이전트	마스터	UDP	31335
에이전트	공격 대상	UDP	

■ Trinoo(트리누)

표 11-5 에이전트와 마스터 패스워드

접속자		패스워드
에이전트		l44adsl
마스터	최초 설치 후 실행	g0rave
	설치 후 원격에서 접속	betaalmostdone
	mdie 명령을 내릴 때	killme

표 11-6 마스터의 주요 명령

명령	기능
die	마스터의 작동을 중지한다.
quit	마스터에서 로그오프(logoff)를 한다.
mtimer N	DoS 공격 시간을 N초로 설정한다. 기본은 300초이며, 1부터 1,999초까지 설정할 수 있다.
dos IP	지정한 IP 주소에 DDoS 공격을 실시한다.

■ Trinoo(트리누)

표 11-7 에이전트의 주요 명령

명령	기능
aaa pass IP_Addr	aaa l44adsl 172.16.0.2와 같이 쓰이며, 공격을 실시한다.
bbb pass N	공격에 대한 시간을 설정한다.
shi pass N	'*HELLO*' 문자열을 마스터의 UDP, 31335번 포트로 보낸다.
png pass	'PONG' 문자열을 마스터의 UDP, 31335번 포트로 보낸다.
d1e pass	Trinoo 데몬을 죽인다.
rsz N	DoS 공격의 버퍼 크기를 N으로 설정한다.
xyz dos IP1:IP2: …	여러 IP 주소에 공격을 실시한다.

■ TFN(Tribed Flood Network)

- 믹스터(Mixter)가 개발한 Trinoo가 약간 발전된 형태
- Teletubby Flood Network라고 부르기도 함.
- Trinoo처럼 statd, cmsd, ttdb 데몬의 취약점을 공격
- 클라이언트(마스터)와 데몬 간에 ICMP Echo Request 패킷을 사용하고, TCP, UDP도 연결도 이루어지지 않아 모니터링이 쉽지 않음.
- 17바이트부터 일정한 형태를 이뤄 구별이 가능해짐.
- 공격자 시스템과 마스터 시스템 간의 연결이 암호문이 아닌 평문으로 전달된다는 약점이 있음.

■ TFN 2K

- 믹스터가 개발한 TFN의 발전된 형태

■ TFN 2K의 특징

- 통신에 특정 포트를 사용하지 않고 암호화되어 있음(프로그램을 통해 UDP, TCP, ICMP를 복합적으로 사용하며 포트도 임의로 결정).
- TCP SYN Flooding, UDP Flooding, ICMP Flooding, Smurf 공격을 씀.
- 모든 명령은 CAST-256 알고리즘으로 암호화됨.
- 지정된 TCP 포트에 백도어를 실행할 수 있음.
- 데몬은 설치할 때 자신의 프로세스 이름을 변경하여 프로세스 모니터링을 회피
- UDP 패킷의 헤더가 실제 UDP 패킷보다 3바이트만큼 더 큼.
- TCP 패킷의 헤더는 길이가 항상 0(정상 패킷이라면 절대로 0일 수 없음)

■ Stacheldraht(슈타첼드라트)

- 독일어로 '철조망'이라는 뜻
- 1999년 10월에 처음 출현한 것으로 알려져 있으며, TFN을 발전시킨 형태
- 공격자와 마스터, 에이전트, 데몬과의 통신에 암호화 기능이 추가됨.
- Stacheldraht의 각 마스터가 제어할 수 있는 데몬의 개수는 기본적으로 1,000개
- 마스터에 에이전트가 자동으로 갱신됨.

■ 악성코드를 이용한 DDoS 공격

- 악성코드에 감염된 좀비 PC는 공격자의 공격 에이전트가 되고, 공격자가 공격 명령을 전달하면 공격 대상에게 DDoS 공격을 수행

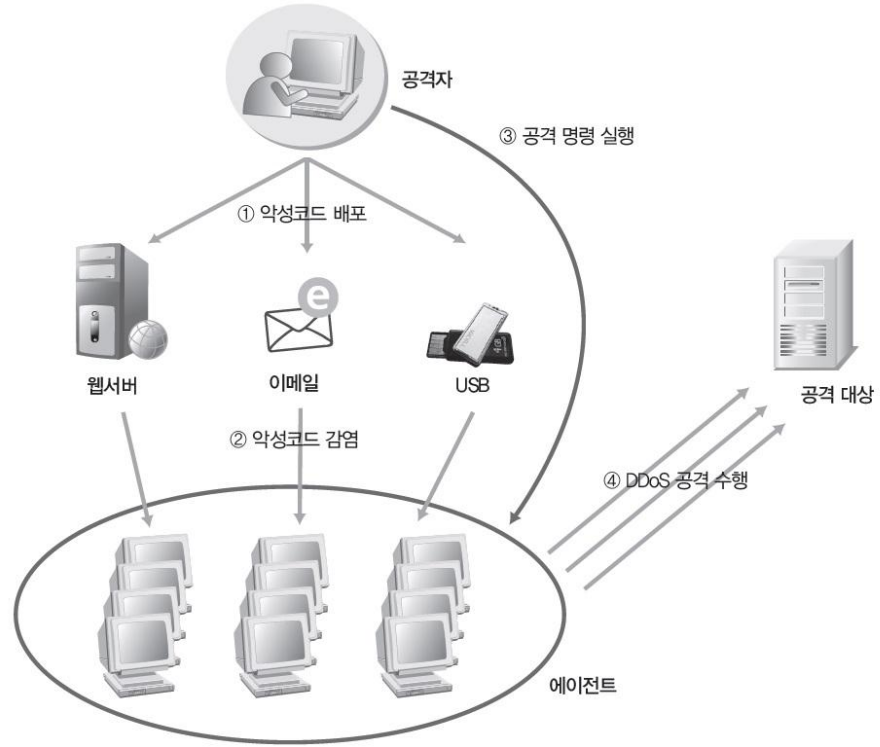


그림 11-45 악성코드를 이용한 DDoS 공격의 개념도

■ 악성코드를 이용한 DDoS 공격

- 대표적인 공격은 2009년 7월 7일에 발생한 ' 7.7 인터넷 대란'
- 총 세 차례(7월 7일 18:00~7월 10일 18:00)에 걸쳐 DDoS 공격이 수행됨.
- 공격에 활용되었던 DDoS 좀비 PC(감염된 PC)는 '소프트웨어적 하드디스크 손상'이라는 자기파괴 증상을 끝으로 생을 마감하게 설계함.

■ 방화벽(Firewall) 설치와 운영

- 보통 내부 네트워크와 외부 네트워크의 경계선에 우선 설치
- 방화벽이 차단할 수 있는 침입은 실제로 30% 정도
- 출발지 주소, 목적지 주소, 침입을 시도하려는 서비스(포트 번호), 프로토콜 침입 차단 가능

■ 방화벽 룰셋(규칙 집합)

- 최소한의 서비스만 제공하고 사용하지 않는 서비스의 포트는 닫음.
- 외부 네트워크에서 들어오는 패킷의 출발지 주소가 내부 네트워크에 존재하는 주소지와 일치할 경우 차단
- 침입 차단 시스템 내부의 구성 요소 간 트러스트Trust(신뢰)를 금지
- 인증 없이 시스템에 접속할 수 있는 내부/외부 사용자를 허용하지 않음.
- 명시적인 서비스 외의 모든 서비스 금지

■ 침입 차단 시스템의 설치와 운영

- 침입 차단 시스템 : 네트워크에 침입해서 들어오는 공격을 탐지하여 능동적으로 대응하기 위한 시스템
- 실제 공격 시 또는 그 전에 공격 양상을 탐지할 수 있으므로 이를 설치하여 새로운 패턴을 인식할 수 있도록 지속적으로 업그레이드하고 관리해야 함.
- 탐지된 공격의 출발지 주소에 대한 방화벽이나 라우터에서의 영구적인 접근 금지도 예방책이 될 수 있음.

■ 시스템 패치

- 시스템에서 바이러스와 해킹 공격에 취약한 점이 발견되면 각 업체에서 패치를 발표하므로, 이를 설치하는 방법
- 해당 패치가 어떤 작용을 하는지 이해한 뒤 설치해야 함(백업 필수).

■ 스캐닝

- 포괄적인 의미의 시스템 분석

■ 서비스별 대역폭 제한

- 각 서비스별로 대역폭을 조절하여 특정 서비스에 대한 공격이 이루어지더라도 나머지 서비스에 대한 영향을 최소화할 수 있음.
- 공격이 이루어지고 있는 서비스도 공격 성공에 필요한 최소 대역폭을 얻을 수 없어 공격에 성공하기 어려움.

감사합니다.

네트워크 해킹과 보안 개정3판

정보 보안 개론과 실습