5 일차 3/4 교시

DOS (Denial Of Service)

이 장에서는 최근에 흔히 발생하는 크래킹 사고의 대표적인 크래킹 기술인 DoS(Denial of Service)에 대하여 살펴보고, 또한 DDoS를 비롯한 새로운 형태의 DoS 공격에 대하여 알아본다. 특히, Dos, DDoS 공격의 원리 및 공격 도구에 대하여 자세히 소개하고 있다.

목 차

목 차

1.1 DOS 공격의 개요

- DoS(Denial of Service) 공격
  - 공격자가 호스트의 H/W나 S/W 등을 무력하게 만들어 호스트에서 적법한 사용자의 서비스 요구를 거부하도록 만드는 일련의 행위
  - 보안관리자가 호스트를 테스트 할 목적으로 DOS공격을 시도 하는 것, 이외에 모든 DOS공격은 악의적인 의도를 가지고 있으며 그 행위는 불법
- DDoS(Distributed Denial of Service) 공격
  - 네트워크로 연결된 분산환경에서 여러대의 컴퓨터를 이용하여 한대의 공격대상 시스템에 대한 DoS 공격

1.2 DoS 공격의 특징

- 루트 권한을 획득하는 공격이 아니다.
- 데이터를 파괴 혹은 변조 혹은 훔쳐가는 것을 목적으로 하는 공격이 아니다.
- 공격의 원인이나 공격자를 추적하기 힘들다.
- 공격시 해결하기 힘들다.
- 매우 다양한 공격 방법들이 가능하다.
- 같은 공격에 대해서 각 시스템마다 결과가 다르게 나타날 수 있다.
- 다른 공격을 위한 사전 공격으로 이용될 수 있다.
- 사용자의 실수로 발생할 수 있다.

1.3 DoS 공격의 유형 (1)

- 내부 공격
  - 공격의 형태
    - 시스템이 보유하고 있는 리소스를 점유하거나 모두 고갈시킴으로써 시스템 마비
    - 계정을 가진 내부 사용자에 의해 발생
    - 고의보다는 실수로 인해 발생
  - 공격의 종류
    - 디스크 채우기
    - 메모리 고갈
    - 프로세스 만들기

1.3 DoS 공격의 유형 (2)

- 외부 공격
  - 공격의 형태
    - 거의 대부분이 실제 목표로 하는 시스템을 공격할 목적으로 행해진다.
    - 특정 포트를 관할하고 있는 프로세스를 마비시킨다.
    - 네트워크 기능 자체를 오동작하게 만든다.
  - 공격의 종류
    - 응용 프로그램 수준
      - mail bombing
      - Buffer Overflow
      - Java Applet Attack
    - Protocol 수준
      - SYN Flooding
      - Ping Flooding
    - 네트워크 수준
      - UDP Storming

2. DoS 공격 기법

2.1 로컬 공격

- 디스크 자원 고갈
- 메모리 자원 고갈
- 프로세스 자원 고갈

2.2 리모트 공격

- Mail bombing
- Buffer Overflow
- Java Applet Attack
- 패킷 수준의 공격
- SYN Flooding
- Ping Flooding
- Smurfing Attack
- 네트워크 Bandwidth 공격
- UDP Storming

2.1.1 디스크 자원 고갈

- 공격 원리
  - 임의의 파일을 생성한 후 계속해서 파일의 크기를 증가시켜 디스크를 쓸모없는 데이타로 채우는 공격기법

```
#include <stdio.h>
#include <sys/file.h>
void main()
{
    int fd;
    char buf[10000];
    fd = open("./hiddenfile", O_WRONLY | O_CREAT, 0777);
    ulink("./hiddenfile");
    while(1)
        write(fd, buf, sizeof(buf));
}
```

- 대비책
  - 문제의 프로세스를 찾아 제거
  - 각 사용자에 대한 quota 제한 실시 -> disk quota 설정법(http://www.koreaonline.net/lecture)
  - 공용 디렉토리(/tmp, /var/tmp)에 대하여 독립적인 파티션을 구성

2.1.2 메모리 고갈

- 공격 원리
  - 하나의 프로세스가 시스템에서 사용 가능한 모든 메모리 리소스를 고갈시킴으로써 시스템을 마비시키는 공격기법

```
#include <stdio.h>
void main()
{
    char *c;
    while(1)
        c = malloc(1000);
}
```

- 대비책
  - 각 사용자에 대한 최대 메모리 사용량을 제한한다.
- 사용자 Memory Quota 설정법
  - 내용이 길기 때문에 kldp.org로 가셔서 보시기 바란다.

2.1.3 프로세스 만들기

- 공격 원리
  - 프로세스를 계속 만들어서 시스템 리소스를 고갈시킴으로써 시스템을 마비시키는 공격기법

```
#include <stdio.h>
#include <unistd.h>
void main()
{
    pid_t pid;
        while(1) pid = fork();
}
```

- 대비책
  - 사용자마다 생성 가능한 최대 프로세스의 수를 제한한다.
- 프로세스의 수의 제한 설정법
  - 내용이 길기 때문에 kldp.org로 가셔서 보시기 바란다.

2.2.1 Mail Bombing

- 공격 원리
  - 한 호스트에 계속적으로 메일을 보냄으로써 그 호스트의 메일 시스템을 마비시키는 공격 기법
  - 공격 유형
    - 공격 호스트에 직접 메일을 전송한다.
    - 메일을 메일 익스체인저에게 보내어서 메일을 익스체인저가 메일의 전송을 처리하게 한다.

2.2.2 Java Applet Attack

- 공격 원리
  - 자원을 고갈시키는 애플릿을 이용하여 클라이언트를 순식간에 마비시키는 공격기법

2.2.3 프로토콜 수준 공격

- 공격 원리
  - 임의적인 조작에 의해서 만들어진 패킷들에 의해 이루어지는 공격 기법
- 특징
  - 시스템의 네트워크 기능을 마비 시킨다.
  - 패킷들이 조작되기 때문에 추적이 매우 곤란하다.
  - TCP/IP 모듈을 거치기 않기 때문에 비정상적인 패킷들을 전송한다.

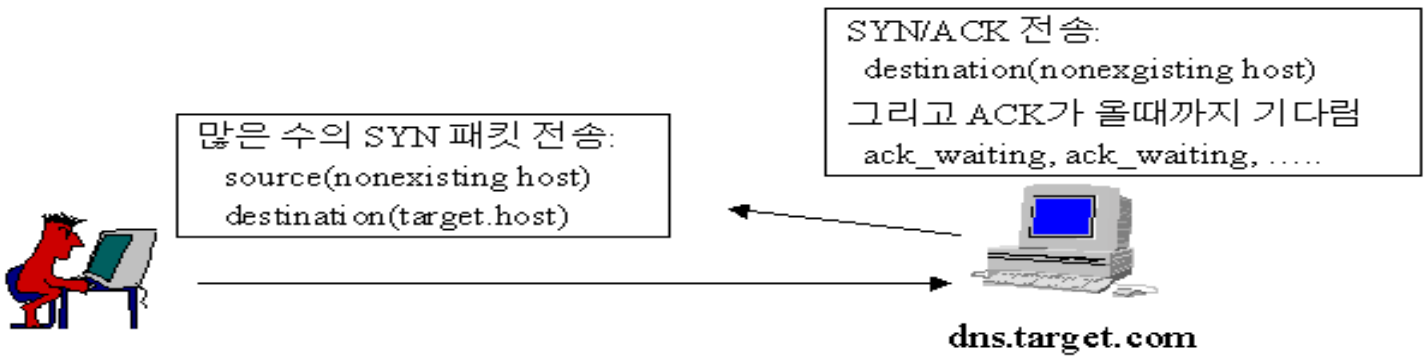
2.2.4 SYN Flooding 공격

●공격 원리

임의적인 조작에 의해서 만들어진 패킷들에 의해 이루어지는 공격 기법

서비스 거부 공격

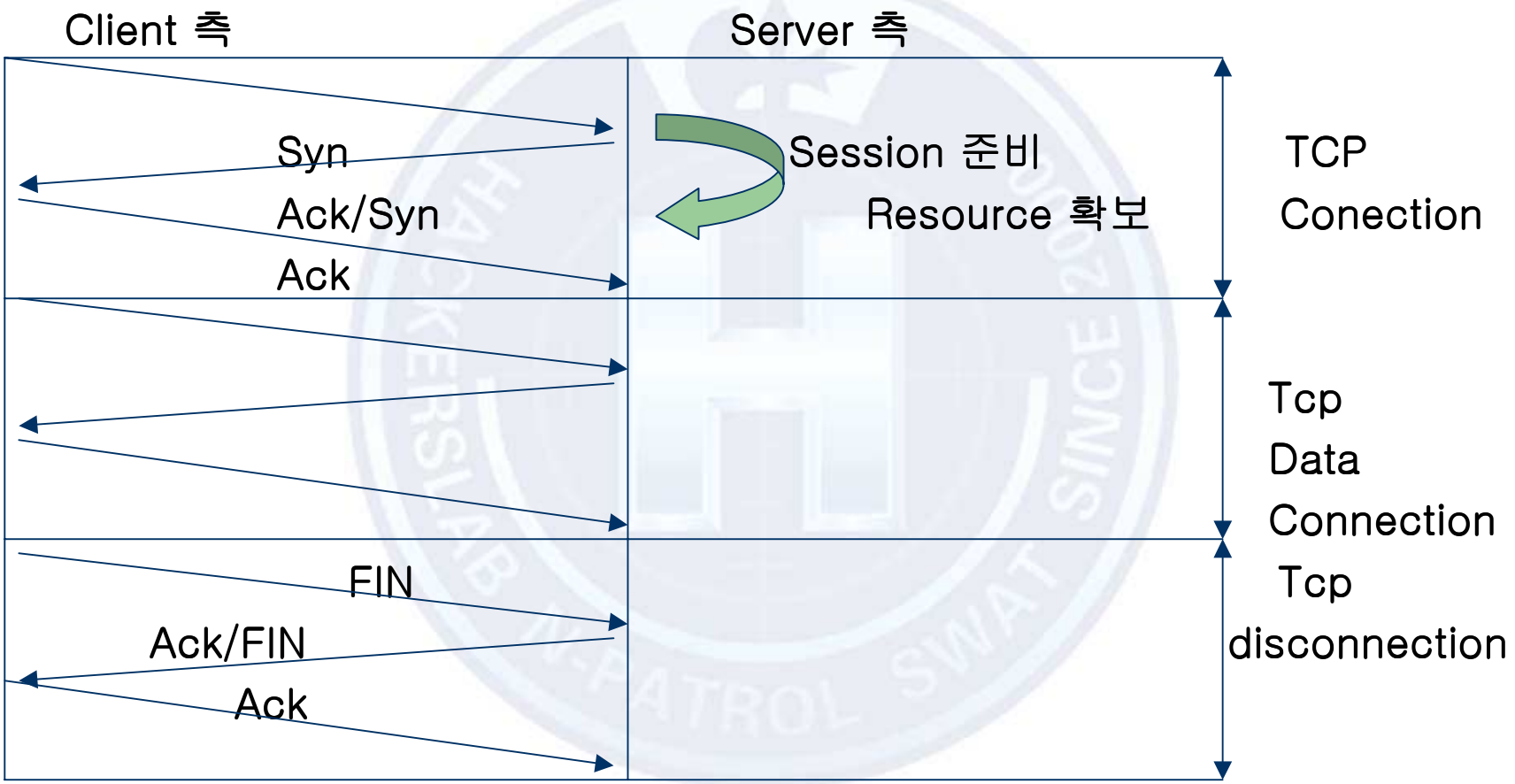
- SYN Flooding
  - 많은 수의 **half-open** TCP 연결을 시도하여 상대 호스트의 **listen queue**를 가득 채움
  - TCP 서비스 연결 거부



2.2.4 SYN Flooding 공격(1)

- 대비책
  - 백 로그 큐의 크기를 증가, Half-Open Time을 적게 한다.
- 공격프로그램 및 구할수 있는곳
  - http://www.koreaonline.net/lecture

2.2.4 SYN Flooding 공격(2)



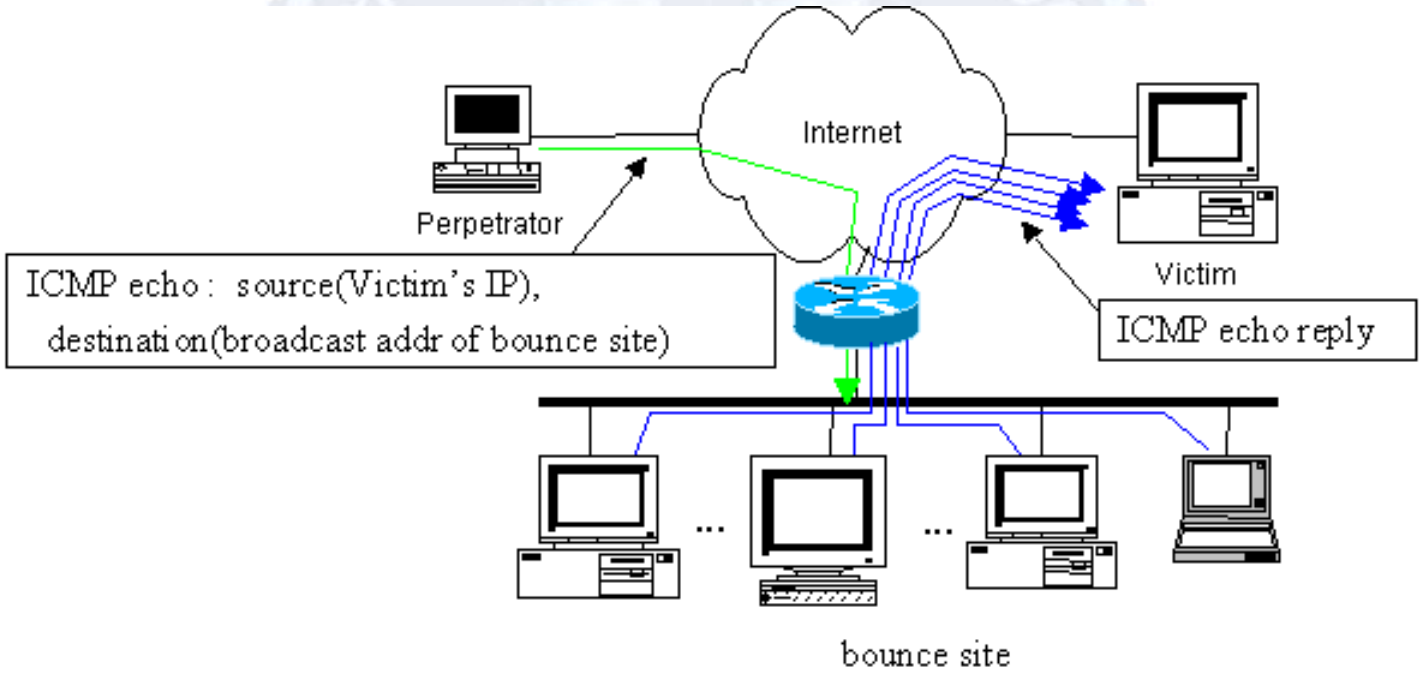
2.2.5 Ping Flooding 공격

- 공격 원리 – ping의 윈도우 버젼이라 생각하시면 됨
  - ICMP 프로토콜을 이용하여 용량초과의 데이터(65535 – 20(header) – 8(ICMP Message))를 전송함으로써 수신측의 버퍼 오버플로우를 발생시키는 공격 기법

- 공격 도구
  - ping : ping 기능으로 대량의 패킷을 보낸다.
  - 프로그램을 구할수 있는곳 http://www.koreaonline.net/lecture

2.2.6 Smurfing Attack(1)

- 공격 원리
  - ICMP 프로토콜과 IP Broadcast 주소를 이용한 공격 기법
  - Broadcast 로의 Echo request 를 보내 대량의 Echo reply를 임의의 주소로 집중 전송되게하는 원리임



2.2.6 Smurfing Attack(2)

- 해결책
  - Smurfing의 차단 방법 모든 라우터의 내부(LAN쪽) interface 마다 Directed Broadcast기능을 막아준다. 즉 자신의 내부 측으로 ?.?.?.255의 주소로 ICMP echo(ping)의 요청이 들어가지 못하도록 한다..

- 공격 프로그램 및 구할수 있는곳

  Smurf.c ,winsmurf

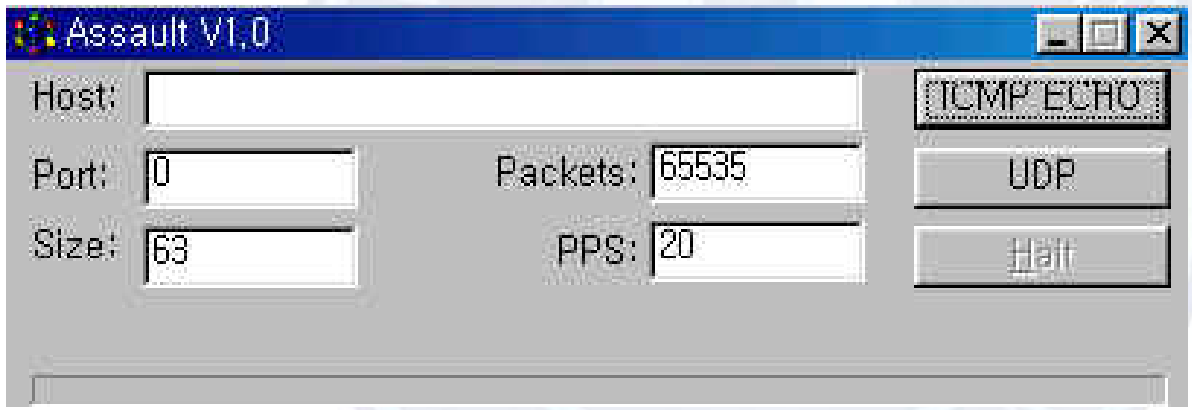
  http://www.koreaonline.net/lecture

2.2.7 Network Bandwidth 공격

- 공격 원리
  - 네트워크 트래픽을 증가시켜 시스템의 사용에는 문제가 없지만 이 시스템이 속한 네트워크를 마비시킴으로써 시스템들이 네트워크 서비스를 올바르게 수행하지 못하도록 하는 공격 기법

2.2.8 UDP Storming

- 공격 원리
  - icmp echo request 와 reply 를 이용한 공격
  - udp를 이용한 공격
  - 포트 번호 7, 9, 13, 19번 포트의 취약성을 이용한 공격 기법
  - 대표적으로 7번 echo 기능을 이용한 공격



- 공격 도구
  - Assault : ICMP, UDP 공격 도구

3. DoS 공격 도구 및 방어 기법

- DoS 공격 도구의 분류
  - ICMP Flooders
  - SYN Flooders
  - UDP Flooders
  - Windows DoS Attack Tools
  - Macintosh DoS Attack Tools
  - Local UNIX DoS Attack Tools
  - Remote Unix DoS Attack Tools
  - 기타

3.1 DoS 공격 도구 (1)

- Blood Lust

- 139번 포트는 NetBIOS Interface를 사용하는 시스템 환경에서 NetBIOS 자원을 식별하는 데 사용된다. NetBIOS 이름을 사용하는 대표적인 예는 Windows NT에서 네트워크상의 개별 서버 이름이다. Windows NT 시스템은 사용자가 지정한 서버 이름에 서버를 의미하는 식별자20(hex)를 붙여서 이를 고유 이름으로 등록한다

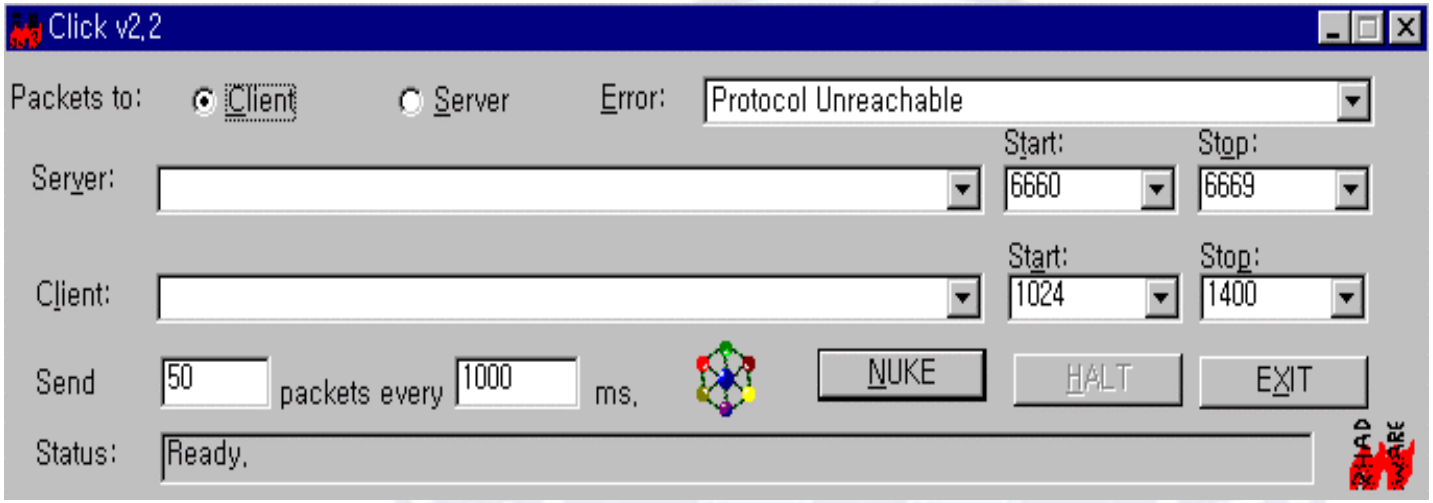
3.1 DoS 공격 도구 (2)

- Bitch Slap

- 특징 및 기능
  - IP주소만 입력하여 주면 되는 간단하면서도 파워 있는 툴
  - 오로지 139 포트로의 OOB 공격을 전문으로하는 툴
  - 프로그램을 어디서 구할수 있는곳
    http://www.koreaonline.net/lecture

3.1 DoS 공격 도구 (3)

- Click



- 특징 및 기능
  - IRC 전문 프러딩 공격 툴이다.
  - IRC 서버가 해당 아이피가 프러딩을 읽으킨다고 혼돈하게 만들어 접속을 끊어 버리는 방법을 사용한다.
  - server irc서버 주소를 입력한다.
  - client 공격 대상의 IP주소를 입력한다.
  - 구할수 있는곳 http://www.koreaonline.net/lecture

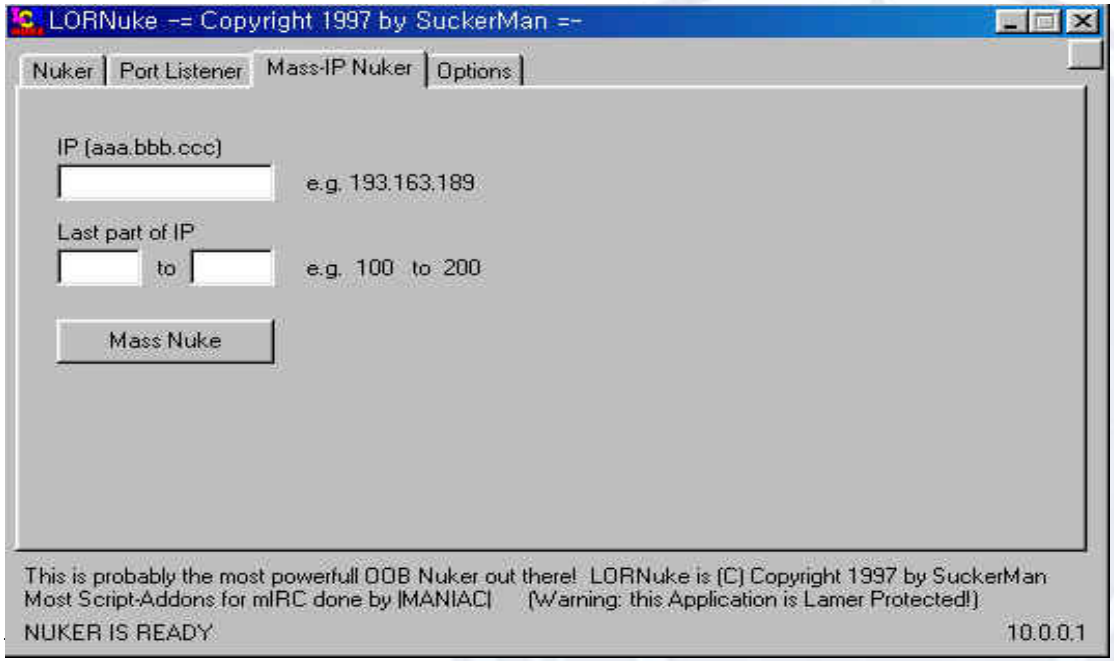
3.1 DoS 공격 도구 (4)

- Cyber

- 특징 및 기능
  - Cyber kit 의 ping 기능으로 대량의 패킷을 보내는 DoS공격이 가능하다.
  - 구할수 있는곳 http://www.koreaonline.net/lecture

3.1 DoS 공격 도구 (5)

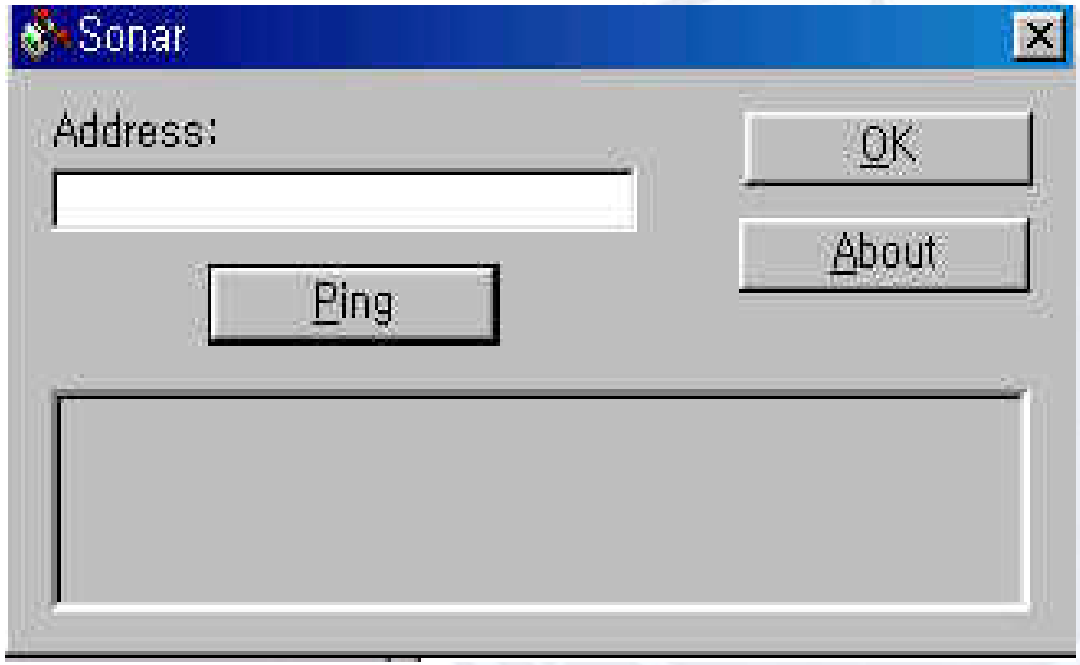
- Lornuke



  - Nuker 누킹 기능
  - Port Listener포트 감지 기능
  - Mass-IP Nuke 다중 IP공격
  - Options IRC공격 기능
  - 구할수 있는곳 http://www.koreaonline.net/lecture

3.1 DoS 공격 도구 (6)

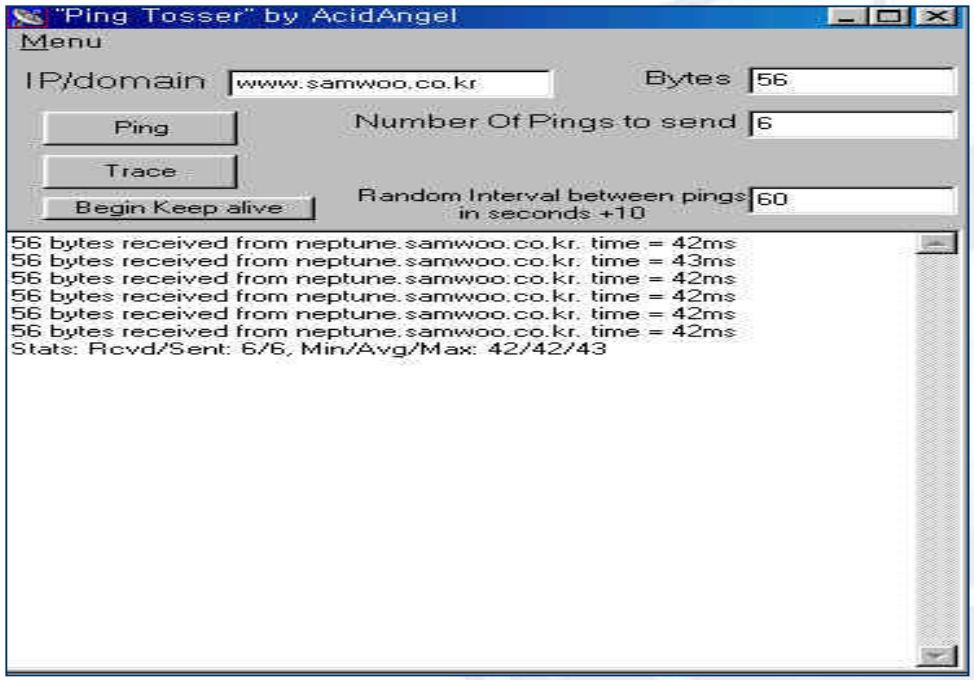
- Sonar



- 특징 및 기능
  - Ping을 이용한 DoS공격용 툴이다.
  - 구할수 있는곳 http://www.koreaonline.net/lecture

3.1 DoS 공격 도구 (7)

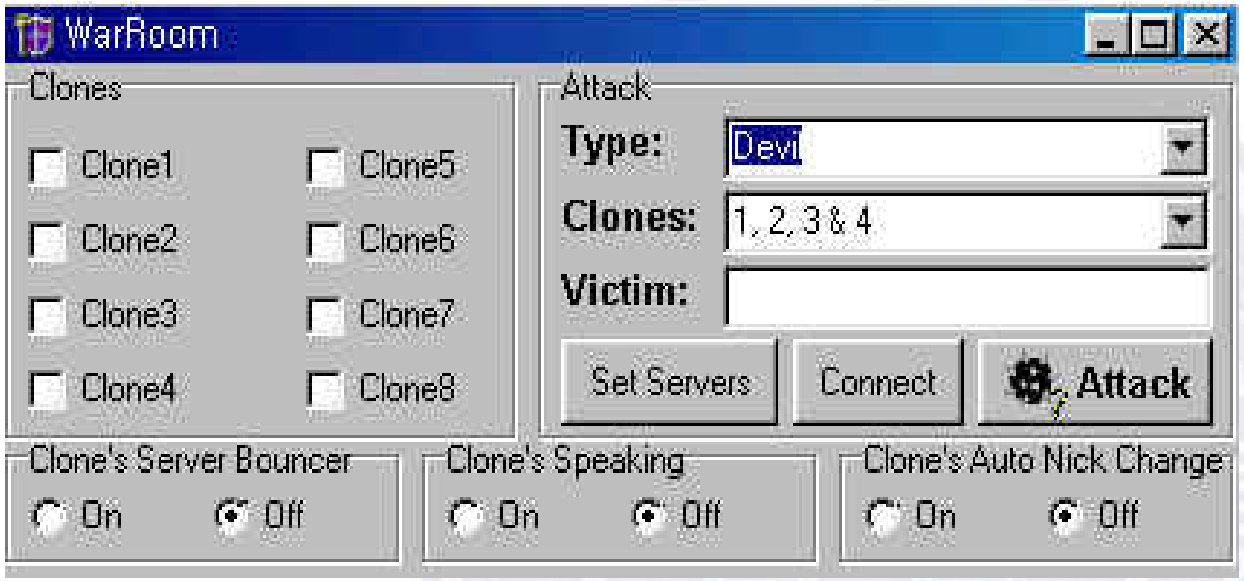
- Tosser



- 특징 및 기능
  - Ping을 이용한 공격 툴로서 옵션이 다양하다.
  - Trace 목표 타겟까지 경유 호스트를 추적하여 준다.
  - 구할수 있는곳 http://www.koreaonline.net/lecture

3.1 DoS 공격 도구 (8)

- WarRoom

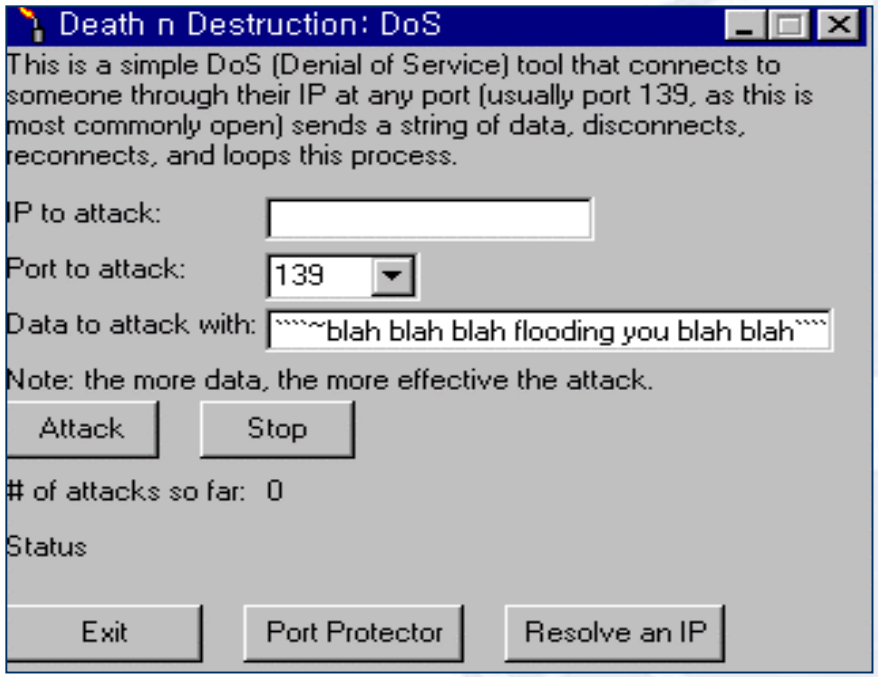


- 특징 및 기능
  - 8개 까지의 클론을 생성하여 공격할 수 있는 툴 이다.

구할수 있는곳 http://www.koreaonline.net/lecture

3.1 DoS 공격 도구 (9)

- Death'n Destruction



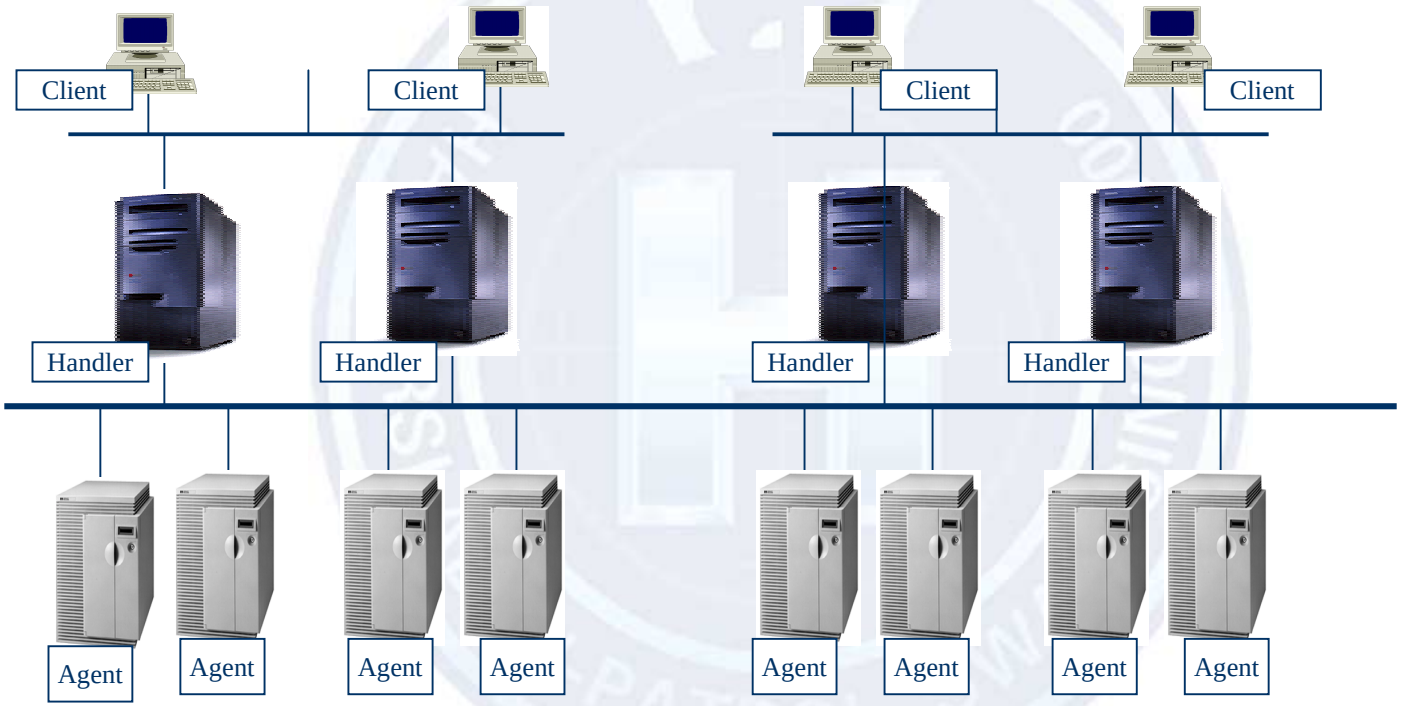
- 특징 및 기능
  - 포트 139 공격용 DoS툴 이다
  - Port Protector 포트 방어 기능
  - Resolve an IP 아이피 resolve기능

3.2 DoS 공격 방어 기법

- VirusScan & Netshield 이란 툴이 최근 아주 널리 쓰인다.
  - EXTRA.DAT 를 해당 디렉토리에 복사해 넣으면 업데이트가 된다.
- DrSolomon 을 사용한다.
  - AVTK를 AVTK 디렉토리에 복사하여 넣는다.
  - AVD를 AVD 디렉토리에 복사하여 넣는다.
- Conceal 방화벽이 테스트 결과 완벽한것으로 증명이 되었다
- Cleaner3.1을 사용하여 제거하면 된다.

4.1 DDoS 공격의 개요 (1)

- DDoS 공격의 개요도



4.1 DDoS 공격의 개요 (2)

- DDoS 공격의 원리
  - 목표를 완벽하게 치명적인 위해를 입히기 위해서 철저하게 타인의 시스템을 사용.

  - 공격방식은 일반적인 공격에 사용될 컴퓨터에 서버나 에이전트를 이식하는 것으로 시작하고 특히 에이전트를 이식하는 것으로 시작
  - 공격유형을 감추기 위하여 지시되는 명령들은 전부 암호화
  - TFN2K나 stacheldraht에 의하여 사용되는 모든패킷을 암호화가 가능하고 스니퍼나 IDS는 이것들을 사고팻킷이 아닌 일반팻킷으로 인식하게 된다.
- 대응방식
  - traffic pattern masking
  - ustream sniffing

4.2 DDoS 공격 도구 및 특징 (1)

- Trin00는 다음의 포트를 사용한다.
  - 1524 tcp, 27665 tcp, 27444 u에, 31335 udp
- TFN
  - ICMP ECHO와 ICMP ECHO REPLY packets.
- Stacheldraht
  - Stacheldraht는 철조망을 뜻하는 독일어 이다.
  - Trin00나 TFN과 유사한 특징을 가진다.
  - 아래의 포트와 패킷들을 사용합니다.
    - 16660 tcp, 65000 tcp
    - ICMP ECHO, ICMP ECHO REPLY
- TFN2K
  - 특정포트를 사용하지 않으며 크래커에 의해 설정될 수 있다.
  - UDP, ICMP와 TCP Packets패킷들을 사용한다.

4.2 DDoS 공격 도구 및 특징 (2)

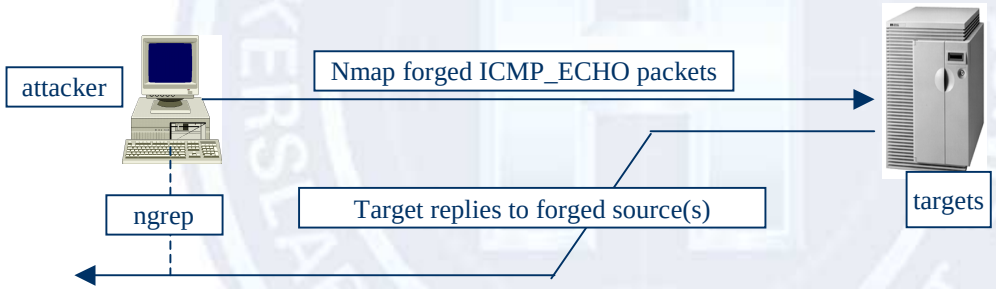
- 트리누(Trinoo), TFN, TFN@K, 스테첼드래트(Stacheldraht)등의 공격 툴은 인터넷 상에서 쉽게 구할수 있다. (아마존,야후,유고 공습때 사용)
  - 크래커는 마스터와 다량의 데몬을 호스트에 심는다.(일반적인 해킹법)
  - 크래커는 마스터에 접속후 데몬을 부른다(자동으로 데몬의 목록이 작성됨)
  - 크래커는 마스터를 통해 데몬에게 목표물을 지정해준 후 공격 지시를 내린다.
  - 지시를 받은 모든 데몬은 목표물을 공격한다.
    - 마스터 27655 포트 사용
    - Drogon이 대용량의 트래픽의 빠른 네트웍 속도로 fragmented packe을 잡아 낼 수 있음.
    - 데몬 27444 포트 사용
    - 마스터용 패스워드는 실행파일에 암호화 되어 저장된다.
    - 데몬용 패스워드는 평문 형태로 저장된다.
    - 데몬들은 “rpc.trinoo,rpc.irix,irix,trinix,ns “와 같이 다양한 Fake 파일명으로 위장된다.
    - crontab에 등록을 시켜 놓아 주기적으로 실행되게 한다.

4.3 DDoS 공격의 유형

- 포트스캔 공격
- 특정포트나 특정트레픽상의 Byte Pattern recognition의 변경 공격
- 크래커 공격시 사용하는 모든 명령어는 암호화 되어 사용
- TCP/IP, ICMP등의 포트를 수시로 변경하며 공격

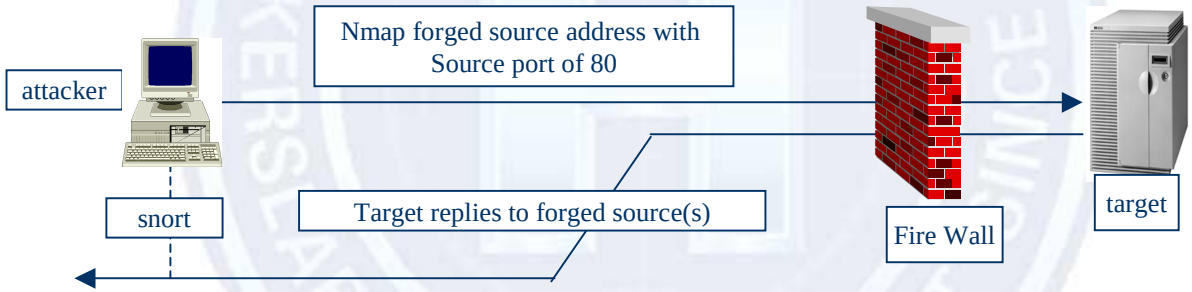
4.3.1 공격결과로 보는 침투유형 (1)

- “공격대상목록”
  - 어느 호스트가 공격과 스캔이 가능한가에 대한 결정을 짓는 행위
    - 아래의 유형은 날조된 ICMP_ECHO패킷을 보내서, 답변도 역시 날조된 주소로 오도록 한 후 sniffer하는 방법
    - 침투자의 호스트가 공격대상의 호스트로 부터 upstream상황이라면 Nmap나 ngrepemd을 사용하면 쉽게 낚아 챌수 있다.



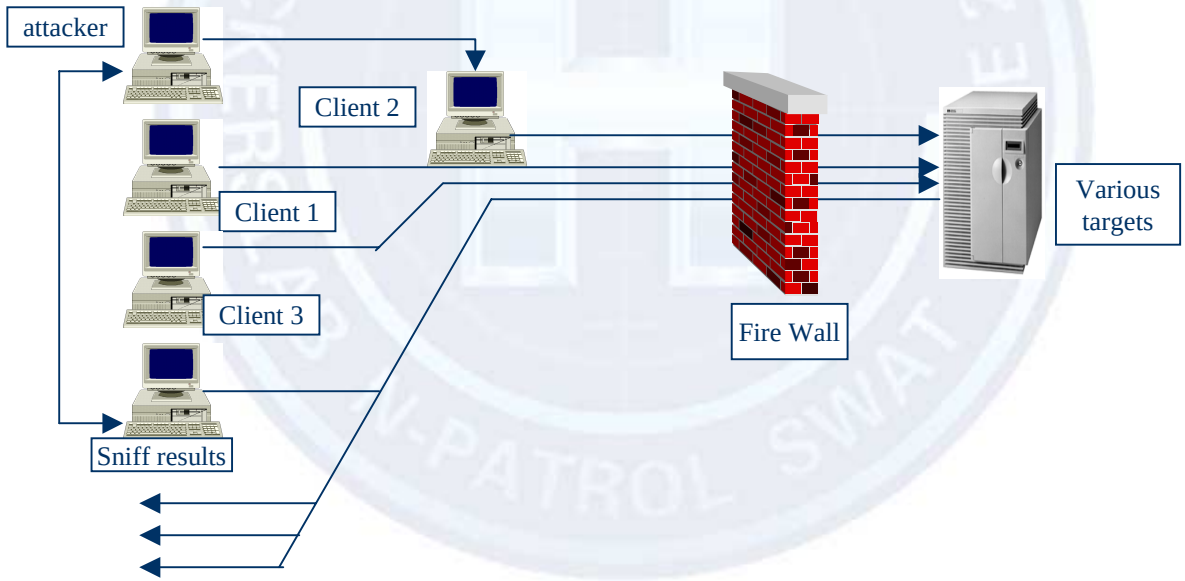
4.3.1 공격결과로 보는 침투유형 (2)

- 일단 source포트 80으로 보내어지는 SYN/ACK는 방화벽을 통과 할 수 있는 허점을 이용하여 방화벽 뒤쪽의 포트와 OS를 스캔 한다.
  - “공격대상목록”에서 얻은 공격가능한 호스트의 리스트를 이용해서 스켄을 시도하는 것
  - 날조된 소스 어드레스가 스캔되는 것을 막는다. ->
  - 돌아오는 패킷은 snort로 잡으면 된다.



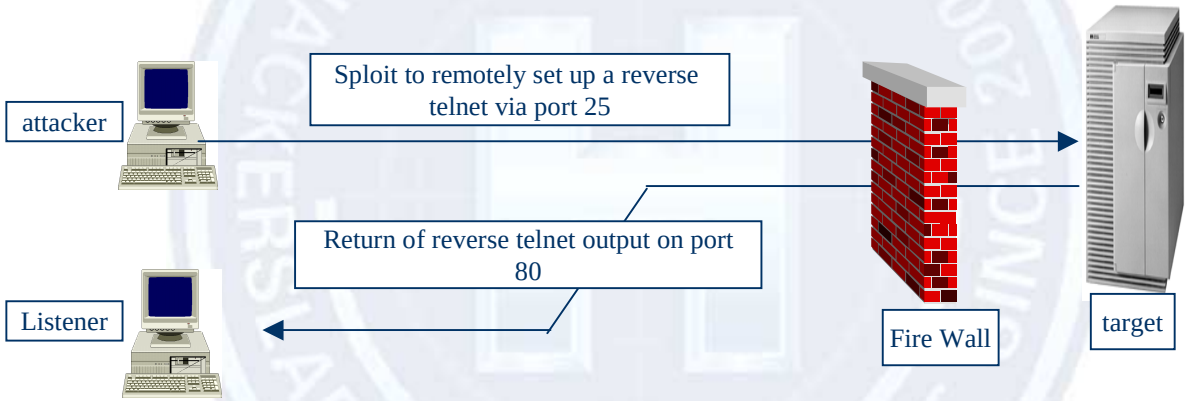
4.3.1 공격결과로 보는 침투유형 (3)

- 이 방법은 소스를 분석해 변형할 수 있고, 프로그램이나 툴 들을 자유자제로 변형, 제작할 수 있는 능력을 가지고 있어야 하기때문에 전문 크래커들에 의해 사용.
  - Client들은 공격대상 호스트와 신뢰관계에 있기 때문에 무사히 방화벽을 출입한다.
  - 포트스캔의 reply는 날조된 주소를 받고, Sniffer는 reply 패킷을 캡쳐한다
  - Sniffer Client는 신뢰된 호스트에 상주하기에 문제가 더 커진다.
  - 심지어는 VPN을 통해서도 침투가 가능해 진다.
  - 공격대상의 호스트를 서서히, 조직적으로, 대규모로 스캔하기 위한 많은 수의 Client를 마스터가 거느리게 된다



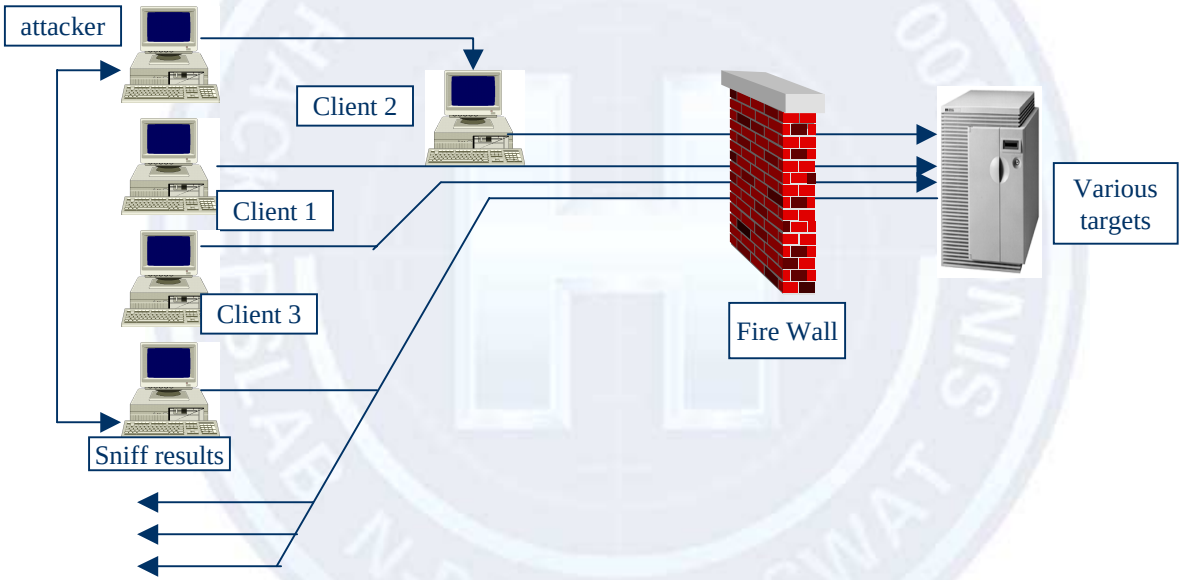
4.3.2 Sendmail 버그 이용 (1)

- 텔넷을 이용한 25번 메일 포트로 접근 sendmail 버그를이용하여 공격한다.



4.3.2 Sendmail 버그 이용 (2)

- 크래커가 그 속에 있는 많은 Client를 조정하면서 타킷을 공격하도록 명령을 내리는 것을 볼 수 있다.



4.3.2 Sendmail 버그 사례(3)

- CERT 보고된 Sendmail 주요 버그들
  - CA-97.05.sendmail – 원격지의 사용자가 루트의 권한을 얻을수 있다.
  - CA-96.25.sendmail_groups – 내부의 공격자가 다른 사용자의 그룹 권한을 얻을 수 있다
  - CA-96.24.sendmail.daemon.mode – 어떤사용자든지 sendmail을 데몬 모드로 실행 실행시킬수 있다.
  - CA-96.20.sendmail_vul – 자원기아문제와 버퍼오버플로우 문제가 발생하였다.

4.4 DDoS 공격 탐지 기법

- 공격 패턴 탐지법
  - 파일, 패킷, 혹은 메모리 등에서 공격의 징후를 찾아 내는 것.
    (기존의 패턴을 변형 시키는 원인을 조사하는 것)
    - 파일사이즈 512Byte의 증가를 조사하는 것.
    - 램의 특정 바이트 sequence를 조사하는 것.
  - IDC(Intrusion Detection System)에 의해서 사용되어 지는 간단한 방법인 phf.cgi 의 스트링을 조사하는 것

- 공격 결과 탐지법
  - 공격의 결과나 그 결과가 미치는 영향으로 감지 하는 것
    (특정 로그 엔트리나 시스템이 예정에 없는 리붓이 되어버린다던가 하는 예)

4.4.1 DDoS 공격 탐지

- tcpdump나 snoop명령으로 탐지
- nmap를 이용하여 탐지
  - # nmap -PI -sT -p 27665 -m 2766.log xxx.xxx.xxx.1-254
  - # nmap -PI -sU -p 31335 -m 31335.log xxx.xxx.xxx.1-254
  - # nmap -PI -sU -p 27444 -m 27444.log xxx.xxx.xxx.1-254 (rpc 공격의 경우)
  - # nmap -PI -sT -p 1524 -m 1524.log xxx.xxx.xxx.1-254
  - # nmap -PI -sT -p 600 -m 600.log xxx.xxx.xxx.1-254
- Nmap프로그램을 다운 받을 수 있는 곳
  - http://www.insecure.org/nmap/

4.5 DDoS 공격 방어 기법

- 가능한 포트 트레픽을 제거
  - 방화벽의 “DNS GUI control을 설정을 하면 53,25번 포트는 Open된다.
    - 항상 설정이전에 침투위험성을 심사숙고 후 결정을 할 것
  - 모든 Public System (Web, FTP, Mail등) 다른 네트워크로 분리 사용
    - 내부 네트워크와의 Network conversations이 허락이 된다면 이러한 서버들은 Open된 포트를 사용하여 내부 네트워크로 침투하는 통로 제공
  - 인터넷에 연결된 모든 서버에서 컴파일러 제거
    - 필요한 최소한의 서비스 가동
  - 관리용 채널이나 포트는 완전히 보안이 유지된 상태이거나 닫아 두어야 함.
    - Check Point 방화벽의 원격관리가 작동될때 256포트가 열리지 않는가?
    - SNMP가 외부와 차단되어 있는가?
    - DMZ으로부터 차단되어 있는가?
- 보안성 향상의 순위
  - 방화벽 설치
  - DMZ구역 설정
  - DMZ구역에 WEB,FTP,Mail서버의 별도 설치

4.5.1 ICMP 방어 기법

- 마스터에서 클라이언트로 노출되지않는 방법으로 명령이 지시되는 일반적인 방법으로 ICMP Echo Replay패킷을 사용하는 것
  - Echo Replay들 스스로는 대답할수 없고 방화벽에도 걸리지 않는다.
  - 안호화된 서버와 클라이언트 사이의 Echo Reply packets이 사용된는 방식으로 TFN을 개발하기 위해서 Loki의 개념을 도입한 것 입니다.
- ICMP트래픽을 제거

4.5.2 DDoS 공격 차단 (1)

- snoop나 tcpdump 명령으로 UDP 패킷,TCP 패킷,ICMP 패킷을 검사
- 포트를 검색하여 라우터에서 해당 포트를 차단
- find_ddos 의 각 os별의 버전을 설치하여 감지 후 지운다.
  - 지원 가능한 os
    - 솔라리스 인텔
    - 솔라리스 스팍
    - 리눅스
- Zombie 유닉스 용을 설치하여 감지 후 제거
- 파일명이 변형 되었을 경우를 대비하여 다음과 같은 파일을 찾아내서 제거
  - master : tserver1900
  - deamon : tsolnmb, ns, httpd, rpc.trinoo, rpc.listen, trinix, rpc.irix, irix
- clontab에 심었을 경우 이를 이용하여 위치를 감지
  - # more /var/spool/cron/crontabs/root
  - * * * * * /dev/isdn/.subsys/tsolnmb > /dev/null 2>&1
- netstat 명령어를 사용
  - # netstat -a

4.5.2 DDoS 공격 차단 (2)

- lsof 프로그램으로 위치를 감지한 후 삭제
  - 마스터의 경우
    - # lsof | egrep ":31335|:27665"
    - master 1292 root 3u inet 2460 UDP *:31335
    - master 1292 root 4u inet 2461 TCP *:27665 (LISTEN) <==PID(1292) 확인
    - # lsof -p 1292
    - COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME
    - master 1292 root cwd DIR 3,1 1024 14356 /tmp/...
    - master 1292 root rtd DIR 3,1 1024 2 /
    - master 1292 root txt REG 3,1 30492 14357 /tmp/.../master <== 마스터파일 위치 확인
    - ...
    - master 1292 root 3u inet 2534 UDP *:31335
    - master 1292 root 4u inet 2535 TCP *:27665 (LISTEN)
  - 데몬의 경우
    - # lsof | egrep ":27444"
    - ns 1316 root 3u inet 2502 UDP *:27444 <==PID(1316) 확인
    - # lsof -p 1316
    - COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME

4.5.2 DDoS 공격 차단 (3)

- ns 1316 root cwd DIR 3,1 1024 153694 /tmp/...
- ns 1316 root rtd DIR 3,1 1024 2 /
- ns 1316 root txt REG 3,1 6156 153711 /tmp/.../ns <==데몬파일 위치확인
- ...
- ns 1316 root 3u inet 2502 UDP *:27444

– lsof 다운로드
  - http://vic.cc.purdue.edu/pub/tools/unix/lsof

4.6 DDoS 공격 차단을 위한 권고 사항 (1)

- 모든 공공 서버를 DMZ로 격리
- 각 서비스마다 별도의 서버를 설치
  - E_Mail서버와 Web서버를 한곳에서 서비스 하지말 것.
- Unix사용 관리자들은 root를 획득 있는 모든 로컬,리모트 BOF공격을 차단하기 위해서 패키와 추가 업데이트를 항상 하기
- SSH(Secure Shell)대신에 PAM(Pluggable Authentication Module)호환을 제공하는 SRP(Secure Remote Password)를 사용 하기
  - SRP는 telnet과 FTP세션의 암호화,zero knowledge공격의 방어 등을 제공
  - 128bit 길이의 패스워드를 사용하여 크랙커가 크랙을 할수 없도록 함.
- SRP가 사용가능한 내부주소 전용의 telnet과 FTP데몬으로 접근을 제한
- 설치된 방화벽 기능 사용하기
- Tripwire를 사용하기

4.6 DDoS 공격 차단을 위한 권고 사항 (2)

- Reassemble된 제품이나 fragmented datagram packets 를 찾아 낼 수 있는 IDS제품을 사용
  - Snort,NFR,Dragon,BlackIce 등
    - Snort의 최신버전은 오로지 아주 작은 패킷 사이즈의 fragmen를 잡아 낼 수 있음
    - Drogon이 대용량의 트래픽의 빠른 네트웍 속도로 fragmented packe을 잡아 낼 수 있음.

- 감시해야 할 대상
  - 현존하는 모든 규칙과 새로운 DDoS새로운 규칙을 적용
  - 이미 차단한 네트워크 트래픽중 일부가 IDS에 치명적일 수 있습니다.
    - 무엇을 왜 Blocking해야 하는지 면밀히 검토하고, 악성 패킷을 찾기위한 IDS규칙을 첨가.
    - 만약 IDS가 포트스캔과 같은 Long periods of time와 같은 공격 감지를 지원한다면, 방화벽을 통해서 허가 받은 신뢰관계에 있는 호스트를 포함.(VPN도 포함)
    - 신뢰관계의 호스트로부터의 날조된 패킷은 정상적인 트래픽으로 보기 때문에 더욱 위험.

4.7 DDoS 공격 사례 (1)

- 국내 B 대학 사례(1999. 9)
  - 영국으로부터 국내 모 대학의 20여개 시스템 해킹사고 통보
  - 솔라리스 rpc 관련 취약점을 이용하여 시스템 침입
  - trinoo가 사용하는 포트와 rpc 공격에 사용되는 포트에 대하여 모 대학 네트워크를 스캔하여 전체 60여 침해 호스트 발견
  - 시스템 침입 후 trinoo master/deamon인 rpc.listen/httpd라는 프로그램 설치 후 실행
  - 해킹당한 호스트를 이용하여 국외 특정 호스트로 UDP flooding 공격
  - 네트워크 과부하 발생
  - 네트워크 과부하 현상 제거 : 라우터에서 UDP 31335, 27444 포트 차단

4.7 DDoS 공격 사례 (2)

- 국내 A 기관 사례(1999. 8)
  - A기관의 시스템 관리자가 비인가된 사이트에서 불법적인 접속을 발견하고 신고
  - 침입자는 솔라리스 rpc 관련 취약점을 이용하여 관리자 권한 획득
  - 시스템 조사결과 cron 테이블을 이용하여 "tsolnmb"라는 trinoo 데몬 실행
    - #strings tsolnmb
    - 161.53.xx.yy
    - Socket
    - Bind
    - Recvfrom
    - %s %s %s
    - alf3YWfOhw.V.
    - PONG
    - *HELLO*
  - 위의 161.53.xx.yy 사이트에 조사요청을 보내 결과를 보고 받은 결과 "tserver1900" 이라는 trinoo 마스터 발견

4.8 관련 뉴스 모음

- 사이버공간의 에이즈 '크래커' "전문해커 10명이면 전세계 마비"
  - (한국일보 2000.02.10)
- 유명 인터넷사이트 해킹피해급증 대책시급 정통부 해킹방지 긴급 대책 마련나서"
  - (전자신문 2000.02.11)
- '유명 웹사이트 해킹' DoS 공격 한달전 예고됐다
  -(중앙일보 2000.02.11)
- 정통부, 해킹방지 긴급 대책마련 나서
  - (전자신문 2000.02.11)
- 독일 해커 stacheldraht 를 만든 '믹스터' 범인색출 도와
  -(한겨레신문 2000.02.15)
- MS·온라인증권사'접속거부'해킹당해
  -(경향신문 2000.02.26)
- 닷컴들은 지난 2월 유명 웹사이트를 강타한 서비스거부공격(DoS) 이후 보험상품 개발을 주문했으며, 업계 에서는 해킹 보험시장이 25억 달러를 넘어설 것으로 보고 있다
  - (머니투데이 2000.07.11)

5. 참고 문헌

- CERT(R) Incident Note IN-2000-01 Windows Based DDOS Agents
- http://www.cert.org/incident_notes/IN-2000-01.html
  - New hacker software could spread by email
- http://news.cnet.com/category/0-1005-200-1555637.html
  - wintrinoo by Gary Flynn
- http://www.jmu.edu/info-security/engineering/issues/wintrino.htm
  - Stacheldraht에 의한 서비스 거부공격 분석 보고서
- http://www.certcc.or.kr/paper/tr2000/2000-03/tr2000-03.html
  - 분산 환경에서의 서비스거부 공격 분석보고서
- http://www.certcc.or.kr/paper/tr1999/1999010/tr1999010.html