# 해킹 사례를 통한 네트워크 시스템의 보안 위험성 분석

김봉한*, 이봉근**, 길민욱***

요약

본 논문은 침입차단 기술과 침입탐지 기술의 발전을 위한 이전 단계의 연구로서, 실제 발생한 해킹사례를 중심으로 네트워크 시스템의 보안 위험성을 분석하였다. 세부 연구내용은 손상된 파일의 문제점을 파악하고 관련된 로그파일과 프로세스들을 분석하는 기법, 해킹도구에 대한 분석과 보안 도구를 적용하는 방법, 그리고 네트워크 프로토콜에서 발생할 수 있는 보안 위험성을 분석하였다. 질의와 응답 형식으로 위험성 분석하여 향후 비슷한 형태의 침입이 발견되었을 경우, 직접 적용할 수 있도록 연구하였다.

# Security vulnerabilities analysis in Network Systems based on the Hacking Incidents

Bong-han Kim*, Bong-gun Lee**, Min-uk Kil***

ABSTRACT

In this paper, possible security vulnerabilities analysis in network system environments are studied by analyzing previous hacking incidents. The paper suggests a method to identify problems with the files tampered by security attacks as well as to analyze the related log files and processes. In addition, tools used in attacks are analyzed to find efficient ways to apply security enhancement tools, and security vulnerabilities in network protocols and their countermeasures are also examined. Possible security vulnerabilities is analyzed following a "query-and-response" approach, so that they can be easily applicable to similar attacks detected in the future.

Key Words : Hacking, Countermeasure, TCP/IP, Security vulnerabilities, Log analysis

* 청주대학교 컴퓨터정보공학과
** (주)에이티엔 기술연구소
*** 문경대학교 복지정보과
· 제1저자(First Author) : 김봉한 · 교신저자(Correspondent Author) : 길민욱
· 접수일(2010년 3월 16일), 수정일(1차 : 2010년 4월 19일), 게재확정일(2010년 4월 23일)

## Ⅰ. 서 론

정보화 사회의 활성화와 각종 통신장비의 고속화, 지능화로 인해 정보통신의 인프라로서 인터넷의 중요성이 급속히 부가되어 인터넷이 생활 또는 비즈니스에서 큰 비중을 차지하게 되었다. 그러나 해킹 및 바이러스 등 각종 정보 침해 범죄의 증가로 인해 여러 가지 정보보호의 문제점들 또한 심각하게 대두되고 있다. 따라서 이러한 침해 사고를 예방하고 효과적인 대응방법을 마련하기 위하여 침입차단 기술, 침입탐지기술 등의 다양한 정보보호 기술들이 개발되고 있다.

이러한 정보보호 기술들은 다양한 해킹 기술과 대응 기술에 대한 중점적인 연구와 경험을 통해 발전할 수 있다. 현재 국내에서는 한국인터넷진흥원(KISA)과 민간기관에서 해킹기술과 대응 기술을 습득하고 경험할 수 있는 훈련환경을 제공하고 있다. 그중에서도 한국인터넷진흥원에서는 정보보호기술 온라인 학습장을 운영하여 다양한 해킹사례와 기법을 제시하고 이러한 해킹기법을 해결할 수 있는 대응방안에 대하여 많은 토론과 연구를 진행하고 있다[1].

본 논문에서는 침입차단 기술과 침입탐지 기술의 발전을 위한 이전 단계로서, 실제 발생한 해킹사례를 중심으로 연구하였다. 손상된 파일의 문제점을 파악하고 관련된 로그파일과 프로세스들을 분석하는 기법, 해킹도구에 대한 분석과 보안 도구를 적용할 수 있는 기술, 그리고 네트워크 프로토콜의 보안 문제점과 대응방안을 연구하였다. 그리고 논문의 서술 방법으로 질의와 응답 방식을 사용하였다.

## Ⅱ. 시스템 로그 및 프로세스 분석

본 장에서는 침입이 발생하였을 때, 손상된 파일을 검색하는 방법과 수행해야할 시스템 로그 작업 그리고 분석해야 할 프로세스에 대하여 연구하였다[2].

### 2.1 키워드 분석

DoS 방어의 피해시스템 이미지를 분석해서, 공격에 사용된 방법을 찾아본다. 공격 시간대를 중심으로 로그 파일을 살펴보면 되는데, 로그 파일에서 공격 흔적은 이미 삭제된 상태이다. 디스크 디바이스를 검색해서 찾아보도록 한다. 공격의 대상이 된 서비스 데몬 이름은 무엇인지 알아본다.

• 분석

strings와 grep의 키워드 검색을 이용하여 로그가 삭제된 시스템에서 공격 흔적을 찾을 수 있다.

```
#cat /etc/vfstab
/dev/dsk/c1t0d0s1       -       -       swap    -       no      -
/dev/dsk/c1t0d0s5  /dev/rdsk/c1t0d0s5  /var  ufs  1  no  -
/dev/dsk/c1t2d0s7 /dev/rdsk/c1t2d0s7  /home1  ufs  2  yes  -
/dev/dsk/c1t0d0s0     4133838  241845 3850655     6%    /
/dev/dsk/c1t0d0s4     8263373 6360669 1820071     78%    /usr
                    <생략>
/dev/dsk/c1t5d0s0      291215       1  262093     1%    /home4
/dev/dsk/c1t5d0s3     1322527    1689 1267937     1%    /home
/dev/dsk/c1t5d0s0    67264763  385964 66206152     1%    /mnt
#strings /dev/dsk/c1t5d0s0 > img
#grep rpc.statd ./img
```

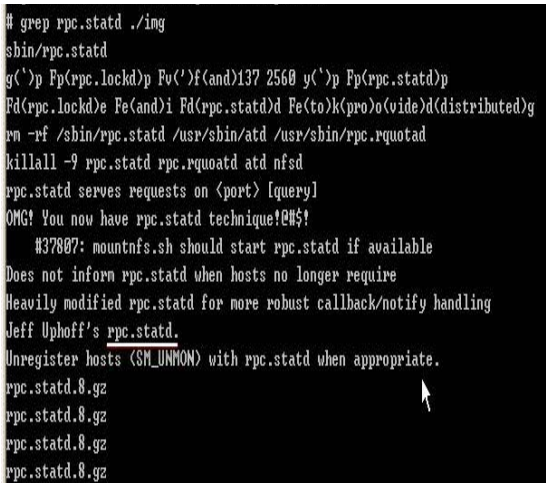


그림 1. rpc.statd 서비스 데몬
Fig. 1. rpc.statd service demon

## 2.2 물리적인 보안영역

관리중인 리눅스 서버로부터 이상한 패킷이 전송되고 있는 것을공격 대상이 된 서비스 데몬 이름은 rpc.statd이다.

여러 방법으로 조사했지만 별다른 이상을 발견할 수 없었다. 마지막으로 LKM 루트킷을 검사할 수 있는 kstat을 이용하여 시스템을 분석한다.

• 분석

kstat를 이용하여 LKM 루트킷을 탐지할 수 있다.

```
#/usr/bin/kstat -P
PID  PPID  UID   GID    COMMAND
 1     0     0    0       init
 2     1     0    0       keventd
128    1     0    0       kjournald
          <중략>
649   551    0    0       in.telnetd
650   649    0    0       login
#ps -ef | grep portmap
#/usr/bin/kstat -M
Module                  Address
knull                  0xc283a000
          <중략>
cdrom                   0xc27a1000
jbd                     0xc2774000
#/usr/bin/kstat -s
SysCall                          Address
sys_exit                         0xc011608c
              <중략>
sys_syslog                0xc011269c
sys_vm86                  0xc0109e70
#cat /etc/rc.d/rc.sysinit
```

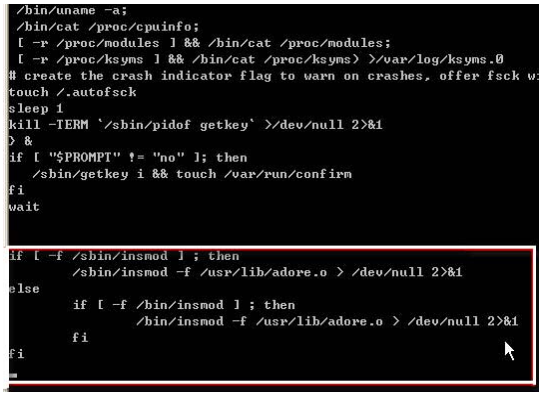


그림 2. 삽입된 LKM 모듈 탐지
Fig. 2. Detect a inserted LKM module

#vi /etc/rc.d/rc.sysinit

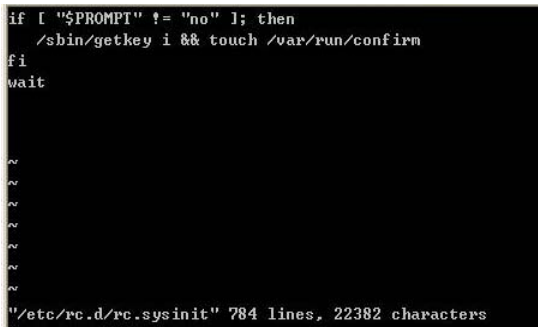


그림 3. 삽입된 LKM 모듈 삭제
Fig. 3. Delete a inserted LKM module

lkm 모듈이 숨기려고 한 프로세스의 이름은 portmap이다.

## 2.3 History 파일 분석

간혹 실수로 또는 관리자에게 탐지되는 것을 대수롭지 않게 여기기 때문에 공격자가 History 파일을 삭제하지 않는 경우를 볼 수 있다. 만약 이러한 history 파일이 남아 있다면 분석자는 이를 해석할 수 있어야 한다. 다음의 피해 시스템에 남겨진 history 파일을 보고, 백도어로 사용되는 포트(여러 개일 경우 ', '로 구분), 공격자가 새로 추가한 계정, 관리자 권한으로 원

격에서 접속하기 위해 수정한 파일 이름, netstat 결과로 백도어 포트가 열려져 있는 것을 보이지 않게 하기 위한 설정 파일 이름 등을 분석한다[3].

• 분석

hacking 등의 사고의 추적을 위해 shell 이 log file을 남기는 경우들이 많다. 이러한 shell이 남긴 로그 파일을 이용하여, 해커의 행동을 추적하도록 한다. hostory 파일은 각 사용자별로 수행한 명령을 기록하는 파일로서, csh, tcsh, ksh, bash 등 사용자들이 사용하는 쉘에 따라.history, bash_history 파일에 기록된다. 해킹 피해시스템을 분석할 때, 불법 사용자 계정이나 root 계정의 history 파일을 분석함으로서, 공격자가 시스템에 접근한 후 수행한 명령어들을 확인할 수 있다.

history 파일은 보통 각 사용자의 홈디렉토리에 생성이 된다. 정상적인 로그인 절차를 거치지 않고 백도어 포트로 접속하여 쉘을 부여받았을 경우는 9704번 포트에 root shell을 바인딩하고 이 포트로 접속을 하게 되면 root의 홈 디렉토리에 .bash_history 파일이 생성되는 것이 아니라, 파일시스템의 최상위 디렉토리에 history 파일이 생성되는 것을 확인할 수 있었다. 즉, /.bash_history 파일에 백도어 포트로 접속하여 사용한 명령어들이 기록된다.

#ls
#cat history.bak

```
cp -f ps /bin/ps
cp -f top /usr/bin/top
cp -f linsniffer /bin/crand
cp -f netstat /bin/netstat
echo "3 38117" >> /dev/ptyq
echo "3 38118" >> /dev/ptyq
userdel -r paint ; echo "rm -rf /.bash_history" >> /etc/c
psend
```

그림 4. 백도어 포트번호
Fig. 4. Backdoor port number

```
cd /var/log
cat "" > secure
cat "" > messages
netstat -n
cat /dev/ptyq
w
w
cd /var/named
ls
useradd -p "" paint
```

그림 5. 설정파일 탐지
Fig. 5. Detect a setup file

백도어로 사용되는 포트는(여러 개일 경우 ", "로 구분) 38117, 38118이고 공격자가 새로 추가한 계정은 ishcor이다. 관리자 권한으로 원격에서 접속하기 위해 수정한 파일 이름은(','로 구분) hosts.allow, securetty 이다. 또한 netstat 결과로 백도어 포트가 열려져 있는 것을 보이지 않게 하기 위한 설정 파일 이름은 ptyq이다.

## III. 해킹/보안 도구 분석

본 장에서는 침입에 사용되는 해킹도구를 찾아낼 수 있는 방법과 찾아낸 해킹도구에 대응할 수 있는 보안도구를 실제 사례별로 분석하였다[4].

### 3.1 Investigation

dd를 이용하여 생성한 디스크 이미지를 통해 피해시스템을 분석하려고 한다. 디스크 이미지는 피해를 당한 서버의 / 디렉토리를 백업한 것이고, 현재 시스템의 /data 디렉토리에 마운트 되어 있는 상황이다. 피해시스템에서 침입자가 어떤 공격툴을 설치하였는지 단서를 얻기 위해 삭제된 파일을 찾아 복구하고 이를 통해 침입자가 사용한 것으로 추정되는 공격이 무엇인지 찾아본다.

• 분석

포렌식 도구인 tct를 이용하여 삭제된 파일을 복구

하고 침입자의 행동을 분석한다. unrm을 사용하여 파티션이 할당되지 않은 디스크 공간의 데이터 복구한다. lazarus를 사용하여 unrm으로부터 수집된 law 데이터를 분석하여 데이터 형태와 내용확인을 확인한다.

※ tct파일 압축해제

```
#cd /home1/user016
drwxr-xr-x    2 user016  training       512 Aug  7 14:13 .
drwxr-xr-x  108 root      root          2048 Jan 26  2005 ..
-rw-r--r--   1 user016  training       185 Aug  7 13:40 .profile
-rw-r--r--  1 user016  training       124 Aug  7 13:40 local.cshrc
-rw-r--r--  1 root      root      726658 Aug  7 14:13 tct-1.12.tar.gz
#gunzip tct-1.12.tar.gz
#tar xvf tct-1.12.tar
```

※ 파일 시스템 확인

```
#cat /etc/vfstab
```

※ 삭제된 파일의 이미지를 만들어 준다. vfstab에 기록된 c1t0d0s6으로 이미지를 생성시 정상적인 이미지가 만들어지지 않는다.

```
#cd bin
#./unrm -f ufs .dev/dsk/c1t1d0s6 > img
#ls -al img
#../lazarus/lazarus -h ./img
```

※ tct 환경 설정을 새롭게 구성

```
#cd /home1/user016/tct-1.12
#./reconfig
#../lazarus/lazarus ./img
#cd ..
#cd blocks
#ls -al
#cat 122.c.txt | more
```

※ 복구된 파일 내용에서 adore lkm rootkit을 발견할 수 있다.

```
#include <linux/capability.h>

#include "adore.h"

extern void *sys_call_table[];

int (*o_getdents)(unsigned int, struct dirent *, unsigned int);
```

그림 6. 웜 발견
Fig. 6. Detect a worm

해당 피해시스템에 설치된 것으로 발견된 worm 의 이름은 adore이다.

## 3.2 악성 프로그램 분석

관리중인 웹서버의 게시판에 의심되는 파일이 업로드 된 것을 발견하였다. 업로드 자료의 저장소는 /usr/local/apache/data 이다. 파일을 찾아 내용을 분석한다.

- 분석

정적 분석은 프로그램을 실행시키지 않고 분석하는 방법이다. 피해시스템에서 발견된 프로그램을 사전 분석도 하지 않은 채 실행시켜 보는 것은 매우 위험한 시도이다. 정적 분석은 프로그램을 실행시키지 않기 때문에 운영체제와 상관없이 분석자가 잘 사용할 수 있는 시스템 환경에서 분석할 수 있다. 일차적으로 'file', 'strings', 'nm' 명령들을 이용하여 바이너리 파일을 분석한다.

```
#cd /usr/local/apache/data
#ls -alQ
```

※ non-printable 문자로 이루어진 숨겨진 파일 발견

```
# strings ".. " |more
```

※ Unix 환경에서 실행된다는 문자열과, 제작자의 e-mail 로 추정되는 문자열 발견, 또한 TCP 12345 포트를 사용한다는 것으로 추정할 수 있는 문자열을 발견할 수 있다.


그림 7. 의심되는 서비스와 포트
Fig. 7. Suspected service and port

의심스러운 프로그램의 실행 운영체제 환경은 Unix이고 이 프로그램을 작성한 것으로 간주되는 사람의 메일 주소는 aion@ukr.net이다. 또한 악성 프로그램이 사용할 것으로 의심되는 서비스와 포트는 TCP 12345이다.

### 3.3 Convert-channel 분석

피해 시스템에 백도어가 설치되어 있다. 해당 백도어를 찾아내고 분석해서 공격자 사이트(IP)를 알아보도록 한다. 백도어가 사용하는 어플리케이션 프로토콜, 공격자가 사용하는 시스템의 IP 주소, 공격자의 접속을 TCPDump를 이용하여 모니터링한다.

• 분석

tcpdump를 이용하여, 네트워크상의 공격 정보를 수집하며 분석한다.

```
#cd /var/spool/cron/crontans
#cat root
```

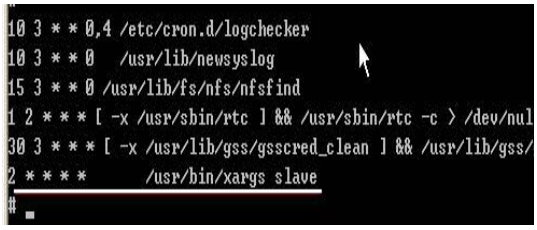


그림 8. 루트 파일 검사
Fig. 8. Check a root file

```
#grep -v "^#" /usr/bin/xargs.19 | head -n15
```

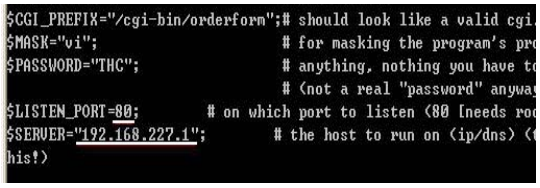


그림 9. IP 주소와 포트번호 탐지
Fig. 9. Detect IP address and port nember

```
# tcpdump -Xn tcp port 80 and host 192.168.227.1
```

백도어가 사용하는 어플리케이션 프로토콜은 http이고 공격자가 사용하는 시스템의 IP 주소는 192.168.227.1이다.

## IV. 네트워크 프로토콜 분석

본 장에서는 침입에 사용되는 TCP 또는 UDP 네트워크 프로토콜의 위험성을 분석하고 그에 대응할 있는 보안 기법을 연구하였다[5, 6].

### 4.1 UDP Flooding

외부 사이트로부터 관리중인 시스템(VSUN)이 특정 시간에 UDP Flooding 서비스 거부 공격을 하고 있다고 한다. 시스템 분석을 통하여 서비스 공격 프로그램을 찾아, 악성 프로세스의 중지 및 보안 조치 수행, 공격 프로그램의 이름, 명령을 하달하는 서버(Master Server)의 주소 등을 분석한다.

• 분석

ps, strings를 이용하여 악성 프로그램을 탐지, 분석하고 cron에 등록되어 있는 악성 프로그램 제거한다. 제거하는 순서는 다음과 같다. 우선 프로세스를 탐지하고 제거한다. strings 이용하여 내용을 확인하고, 악

성 프로그램을 삭제한다. cronttab root 파일을 확인하고 vi 편집기로 내용 수정한다.

#ps -ef

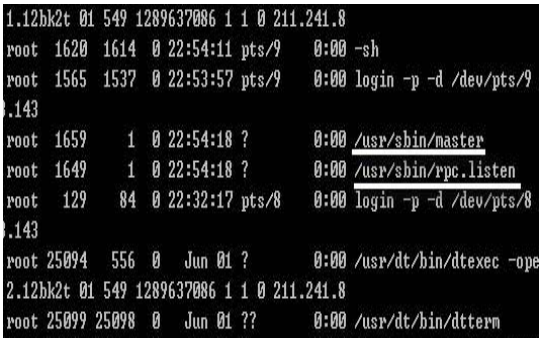


그림 10. 프로세스 검사
Fig. 10. Check a process

#kill -9 1659
#kill -9 1649
#strings /usr/sbin/master
master
/etc/.evrc
RC_ROOT
... 생략 ...
mtimer: usage: mtimer <seconds to DoS>
usebackup: Switching to backup data file, If exist.
help
trinoo>
#strings /usr/sbin/rpc.listen
rpc.listen
127.0.0.1
/etc/.evrc
RC_ROOT
... 생략 ...
udpport
tcpport

#rm /usr/sbin/master
#rm /usr/sbin/rpc.listen
#vi /var/spool/cron/crontabs/root ※ 마지막 부분을 삭제

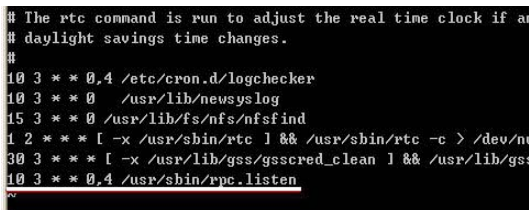


그림 11. 마지막 부분 삭제
Fig. 11. Delete the last part

설치된 DDoS 도구의 이름은 trinoo이고 Master 서버의 IP는 127.0.0.1이다.

## 4.2 네트워크 패킷 분석

네트워크 모니터링을 하던 중, 1524번 포트로 접속하는 공격으로 의심되는 로그를 발견하다. 공격자는 피해 시스템에 접속한 다음 어떤 외부사이트의 ftp에서 특정 프로그램을 다운로드받은 것처럼 보인다. tcpflow 프로그램을 이용하여, 로깅된 트래픽을 분석하고 공격자가 다운로드해서 설치한 프로그램이 무엇인지 알아낸다. ftp로 다운로드한 파일을 네트워크 트래픽에서 추출하여, evidence 이름으로 저장하도록 한다.

• 분석

tcpflow는 TCP 연결에서 송수신되는 데이터를 캡쳐하는 프로그램으로서, 이를 이용하면 네트워크 상의 데이터 분석을 쉽게 할 수 가 있다. tcpflow는 ipA.portA-ipB.portB 같은 포맷의 파일이름으로 수집된 데이터를 저장한다.

#ls
#/usr/local/bin/tcpflow -r 0108@000-snort.log

※ 패킷 로그 데이터에서 각각의 TCP 연결 데이터를 추출한다. 공격자가 접속한 결로, 추측 되는 1524포트에 대한 연결 데이터를 살펴본다.

#cat 208.061.001.06596-172.016.001.102.01524

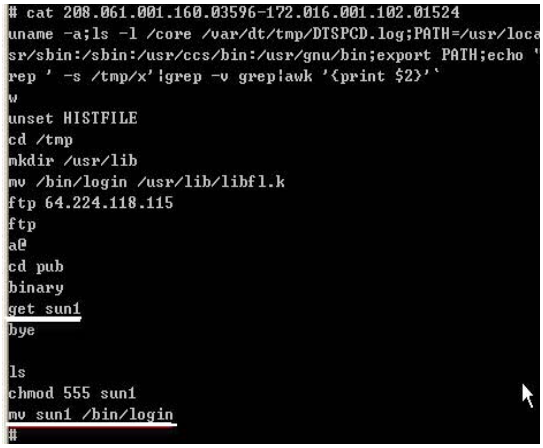


그림 12. 다운로드한 파일과 변조한 파일
Fig. 12. Downloading file and modulated file

※ ftp 연결 데이터를, 증거 파일로 복사한다.
#cp 064.224.118.115.00020-172.016.001.102.33514 evidence

공격자가 다운로드한 파일 이름은 sun1이고 공격자가 변조한 파일 이름은 login이다.

## V. 결론

본 논문에서 한국인터넷진흥원(KISA)에서 운영하는 SIS에서 선정한 대표적인 해킹사례를 중심으로 네트워크 시스템의 공격방식과 대응방식을 연구하였다. 시스템 로그 및 프로세스 분석에서는 키워드, 물리적인 보안 영역, History 파일을 통해 다양한 시스템 로그 파일의 종류와 내용 분석하고 대응방안을 제시하였다. 해킹/보안 도구 분석에서는 Investigation, 악성 프로그램, Convert-channel을 통해 침입용 도구의 동작행위와 침입이 완료된 후에 동작하는 프로세스 분석하고 그에 대응할 수 있는 기법을 제시하였다. 네트워크 프로토콜 분석에서는 UDP Flooding, 네트워크 패킷, 라우터 설정을 통한 TCP/IP 프로토콜의 문제점과 공격 대응을 분석하고 대응방안을 연구하였다.

그리고 시스템 로그 및 프로세스 분석, 해킹/보안 도구 분석, 네트워크 프로토콜에 대한 분석 및 대응방안을 질의와 응답 형식으로 분석하여 향후 비슷한 형태의 침입이 발견되었을 경우, 직접 적용할 수 있도록 연구하였다.

이러한 다양한 사례를 중심으로 실제적인 대응방법을 연구함으로서 새로운 침입탐지 기술과 대응기술을 개발하여 보다 능동적인 침입탐지 시스템을 개발할 수 있을 것이다.

## 참고문헌

[1] http://www.sis.or.kr/
[2] Nemeth, "*Unix System Administration*", Prentice Hall, 2006.
[3] Chris Pogue, "*Unix ForensicC Analysis DVD Toolkit*", Elsevier Science, 2008.
[4] Carl Endorf, Eugene Schultz, Jim Mellander, "*Intrusion Detection & Prevention*", McGrawHill, 2004.
[5] Michael Rash, Angela Orebaugh, Graham Clark, Becky Pinkard, Jake Babbin, "*Intrusion Prevention and Active Response*", Syngress, 2005.
[6] Bonghan Kim, "*The analysis and problem solving of TCP/IP protocols by network violation instance*", ICCC2009, Vol.7 No.2, pp. 468-471, 2009.
[7] 조상엽, "경제 사회 시스템 보호를 위한 정보보안 정책 및 대응방안 수립", *한국지식정보기술학회 논문지*, 제4권 제1호, pp.11-19, 2009.
[8] 황문영 외, "클라우드 컴퓨팅 환경에 적합한 사용자 중심의 ID 관리기술", *한국지식정보기술학회 논문지*, 제5권 제1호, pp.51-58, 2010.

**김봉한(Bong-Han Kim)**

1994년 청주대학교 전자계산학과
1996년 한남대학교 전자계산공학과
2000년 한남대학교 컴퓨터공학과

2001년~현재 : 청주대학교 컴퓨터정보공학과 교수
※ 관심분야 : 네트워크보안, 가상현실

**이봉근(Bong Keun Lee)**

1997년 한남대학교 컴퓨터공학과
1999년 한남대학교 컴퓨터공학과
2010년 충북대학교 전기전자컴퓨터공학부

2006년~현재: (주)에이티엔 기술연구소 연구개발팀장
※ 관심분야 : 지능형 에이전트, 데이터베이스 보안,

**길민욱(Min-Wook Kil)**

1989년 한남대학교 전자계산학과
1991년 한남대학교 전자계산공학과
2000년 한남대학교 컴퓨터공학과

1997년~현재 : 문경대학 복지정보과 교수
※ 관심분야 : 네트워크보안, 음성인식