論文
2-11-3

인터넷 쇼핑몰의 보안 시스템에 관한 연구
(A Study of Security System for Internet Shopping Mall)

이 내 준*
(Nae-Joon Lee)

요 약

최근의 폭증하는 해킹사고와 컴퓨터 바이러스의 피해 증가로 보안관리의 중요성이 강조되고는 있지만 뛰어난 해커의 역량을 저지하기에는 역부족인 것이 사실이다 그러나 기본적인 서버시스템의 보안설정만으로도 해킹의 대부분을 차지하고 있는 초보나 중급수준의 피해로부터 더욱 안전해 질 수 있지만 많은 부분의 중형시스템과 개인의 보안상태는 아직도 무방비 상태로 놓여 있음을 알 수 있었다.

소프웨어적으로 혹은 하드웨어적으로 완벽한 정보시스템은 없다. 언제든지 생각지 못한 방법으로 자신의 시스템들은 해커와 바이러스로부터 피해를 볼 수 있다는 사실을 인식할 필요가 있다. 모든 컴퓨터 사용자는 이에 대비하여 끊임없는 대처 방안 연구가 필요하다.

본 논문에서는 배스천호스트의 구성을 제안한다. 배스천호스트의 구성을 통해서 현재까지 알려진 해당 호스트에 대한 내/외부에서의 침입위험으로부터 안전할 수 있도록 하는 것이다.

ABSTRACT

Through the extension of damages caused by hacking and computer virus, although security control has been emphasized, hackers' capability exceeded the security controllability. The basic security setup of server system will be free from the damages by primary and intermediate level which are the major group. It should be noted that security condition of most middle-sized and personal systems is widely open for hacker's intrusion.

There is no perfect information system either software-wise or hardware-wise. It has to be recognized that our systems will be attacked easily by the hackers and computer virus. Computer users are demanded to be prepared for these types of surprise attacks. In this paper, I will propose a formation of Bastion server. This will protect risks from inside & outside intrusion which have been known till today.

1. 서론

현재 우리나라의 인터넷 사용은 적어도 양적인 면에서는 세계최고의 수준에 있다. 정보화의 혜택을 받은 사람들은 인터넷을 통해 극장의 표를 예매하고 외국행 비행기의 표를 산다.

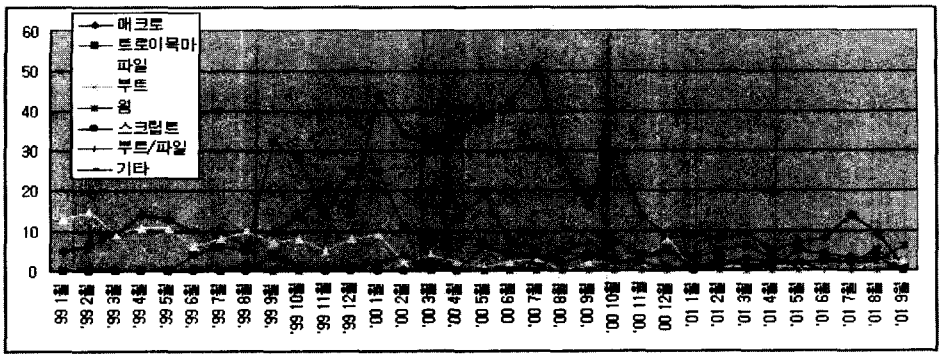
그리고 우리정부는 정보화 정책에 많은 관심을 갖고 초고속 통신망 구축과 정부기관의 정보화에 힘을 아끼지 않아 인터넷 인프라도 세계의 부러움을 사는 실정이다.

* 정회원 : 충북과학대학 부설 국제IT전문교육원

논문접수 : 2001. 10. 26.
심사완료 : 2001. 11. 7.

<표 1> 바이러스 종류별 발생상황

<Table 1> Occurrence Status of Computer Virus



자료 : http://www.certcc.or.kr

이러한 분위기에 걸맞게 많은 인터넷상의 쇼핑몰이 등장하여 온라인 쇼핑이라는 새로운 형태의 전자상거래를 선보이게 되었다. 이런 정보화의 편리함에 많은 사람들의 더욱 쉬운 구매를 가능하게 하였고 또 중간 유통단계를 통하지 않아 더욱 싼 상품의 구매 가능성을 높여 주었다.

그러나 정보화의 역기능 또한 심각한 수준으로 사회 문제가 되고 있다. 해킹과 사용자 부주의에 의한 노출된 정보는 인터넷의 엄청난 확산력에 의해 순식간에 유포되기도 하여 노출된 정보나 불순한 의도로 왜곡되어진 정보는 소유자들에게 엄청난 손실을 끼치게 된다. 정부, 기업, 개인 모두가 이러한 인터넷의 역기능으로부터 자유롭지 못하다. 특히 해킹과 컴퓨터바이러스라는 정보화시대의 역기능이 급속도로 증가하고 있는데, 그 피해도 날로 다양하고 심각한 문제로 인식되고 있다.

본 연구는 정보화시대의 역기능의 가장 큰 요소인 해킹과 컴퓨터 바이러스의 피해를 알아보고 대안방법을 제시 하고자 한다. 또 다양해지는 해킹방법과 컴퓨터바이러스의 실태를 파악하고 그 대책에 대해 알아보고 특히 현재 운영중인 한 웹 쇼핑몰의 보안 사례를 통해 대처방안을 모색해 보고자 한다.

2. 컴퓨터바이러스와 해킹의 피해

2.1. 컴퓨터 바이러스의 피해

국내 인터넷 산업이 급속히 발전하고 있는 가운데, 컴퓨터 바이러스 피해를 경험해 본 일반 네티즌들은 전체의 과반수가 넘는 52.6%를 차지해, 바이러스 피해 경험이 없는 47.4%보다 훨씬 많았다. 한편 미국 인터넷 사용가구의 90%가 주요 웹사이트들에 대한 해커들의 최근 공격에 대하여 우려하고 있으나, 인터넷 공간에서의 치안관리를 누가 담당하여야 하는지에 관해서는 의견이 분분한 것으로 조사됐다[1].

컴퓨터 바이러스의 수는 1995년 100종을 넘은 이래 해마다 꾸준한 증가세를 보이고 있다. 특히, 1999년에서 2000년까지 1년 동안에는 전년 대비 무려 150% 이상(379종 → 572종)에 달하는 신종 바이러스가 출현하였다. 또한 컴퓨터 이용이 일상생활 깊숙이 침투함에 따라 앞으로도 컴퓨터 바이러스의 피해는 급증할 것으로 예상된다.

이렇게 컴퓨터 바이러스의 수가 해마다 급증하고 있는 현상과 달리 그 피해 경험 비율은 지난해 72.6%에서 올해 오히려 감소하는 의외의 결과가 나타났다. 이는 최근 컴퓨터 바이러스에 대한 연구가 본격화되면서 국내 바이러스대응 전문회사 및 그 제품인 백신 프로그램의 활동이 커졌기 때문인 것으로 해석된다. 특히, 한국정보보호센터에서의 주기적인 예보와 긴급상황에 대처하는 경보체제 기능이 피해

<표 2> 2001년 9월 바이러스 발생상황
<Table 2> Occurrence Status of Computer Virus, Sep. 2001

순위	바이러스이름	바이러스 유형	피해건수	선종여부	국/외산	진료대비
1	W32.Nimda.A	I-Worm	9705	O	외산	-
2	Win32/FunLove.4099	Win32	785	X	외산	63%
3	Win32/Sircam.worm	I-Worm	588	X	외산	11%
4	Win32/Magistr.39921	I-Worm	224	O	외산	-
5	I-Worm/Wininit	Trojan	181	X	외산	90%
6	Win32/Hai.worm	Win32	178	O	외산	-
7	Win32/Weird	Win32	80	X	외산	53%
8	I-Worm/Hybris	I-Worm	74	X	외산	48%
9	Win95/Love	Win95	44	X	국산	58%
10	Win95/CIH	Win95	43	X	외산	50%
기타	-	-	152	-	-	19%
합계	-	-	12,054	-	-	142%

자료: http://www.certcc.or.kr

를 대폭 감소시키는데 커다란 역할을 한 것으로 파악된다. 그러나 지난 2001년 8월에 있었던 코드레드(Code Red)바이러스의 피해는 다시 한번 컴퓨터시스템 보안의 불감증을 나타낸 것이었다. 코드레드 바이러스는 전국 1만3000여개 공공기관 및 기업 등의 4만여 대 서버에 급속히 침투하면서 전산망 가동이 잇따라 중단되는 등의 엄청난 피해를 일으켰는데 이처럼 컴퓨터바이러스에 대한 경계를 늦춰서는 안된다.

컴퓨터 바이러스 감염 빈도의 경우는 인터넷 이용자들의 대부분인 75.9%가 '한두 번' 경험한 것으로 조사되었으며, '가끔' 이상 바이러스에 감염되는 경우도 각각 21.5%(가끔), 2.6%(자주)의 비율을 보이고 있어 앞으로 주의가 요망된다.

이는 올해 유행했던 몇몇 바이러스가 전자우편을 매개로 불특정 다수에게 전달되었고, 그로 인해 지난 한 해 많은 사람들이 피해를 보았던 경험과 맞물리는 사실이다. 또한 '저장매체' 대신 '내부 네트워크'를 통해 바이러스 감염이 올해 많았던 것 역시 이들 바이러스의 특징 때문이다.

2.2 해킹(Hacking)의 현황

허가받지 않은 상태에서 타인의 컴퓨터시스템에 침입하는 행위를 일컫는 해킹은 그 수법이 날로 지능화 되어가고 또한 그 발생수도 폭발적으로 증가하고 있다. 그 수법이 치밀하고 고도의 컴퓨팅 지식을 수반하는 해킹수법으로 얻을 수 있는 정보는 비례적으로 중요한 정보이다. 이렇듯 해킹에 의한 정보의 유출은 민감하다.

해킹사고 중 피해 현황을 보면 기업과 대학이 가장 많은 피해를 입고 있다. 해킹사고가 많은 대학의 경우 네트워크 규모가 방대하고 사용자 또한 교수, 교직원, 학생 등 대단히 다양하여 보안정책을 수립하기가 쉽지 않다. 또 대부분의 대학 해킹사고는 대학의 주요서버이기보다는 각 연구실에서 운영하고 있는 리눅스 서버의 해킹피해가 심각한 것으로 나타났다. 일반 기업의 경우도 대부분의 해킹사고는 보안에 대한 대책을 세울만한 여력이 없는 중소업체 또는 웹호스팅 업체에서 발생하였다. 반면에 대기업의 경우는 침입차단 시스템을 등 보안도구를 활용하여 보안을 강화하고 있어 해킹사고 피해가 비교적 적다[2].

<표 3> 2001년 9월 해킹피해 접수상황

<Table 3> Receipt Status of Damages by Hackers

□월별 국내 해킹피해 접수현황

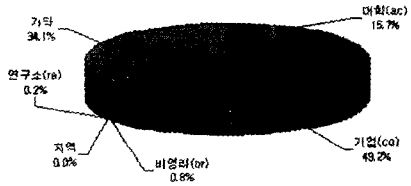
월	'00. 1	'00. 2	'00. 3	'00. 4	'00. 5	'00. 6	'00. 7	'00. 8	'00. 9	'00. 10	'00. 11	'00. 12	계
발생 건수	108	113	129	117	137	117	278	239	237	156	227	85	1943

월	'01. 1	'01. 2	'01. 3	'01. 4	'01. 5	'01. 6	'01. 7	'01. 8	'01. 9	'01. 10	'01. 11	'01. 12	계
발생 건수	261	438	384	537	658	432	364	705	522	-	-	-	4,301

자료: http://www.certcc.or.kr

2001년 9월의 국내 해킹피해접수 건수는 총522건으로 8월의 709건에 비해 크게 증가하였다. 이와 같은 사고증가의 주된 원인은 windows95/98을 사용하는 개인사용자의 사고접수 신고와 지역 도메인과 관련된 침해사고가 급격히 증가하였기 때문이다. 개인사용자와 관련된 침해사고의 대부분은 아이디 도용이나 백오리피스 스캔과 같은 널리 알려진 공격툴과 관련된 사고가 그 주류를 이루고 있다.

기관별 해킹신고 사례는 다음 [그림 1]처럼 다양해지고 있다.



○ 피해기관 수

구 분	사고기관	
	기관 수	비율(%)
대학(ac)	82	15.7
기업(co)	257	49.2
비영리(or)	4	0.8
연구소(re)	1	0.2
지역	0	0
기타	178	34.1
합계	522	100

자료: http://www.certcc.or.kr

[그림 1] 2001년 9월 해킹피해기관

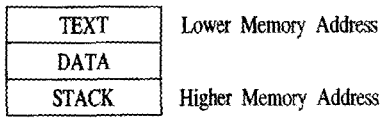
[Fig. 1] Damaged Institutions by Hacking in Sep. 2001

2.3 해킹의 기법

Unix, Windows시스템에서 어떠한 형태의 해킹이 최근 주류를 이루고 있으며 이들은 각각 어떠한 원리에서 동작되는지를 살펴보고 이런 해킹 유형들을 살펴보도록 한다[3].

2.3.1 Buffer Overflow 공격

Unix에서 프로그램이 수행될 때마다 아래와 같은 메모리 구조를 한다.



[그림 2] 메모리 구조[3]

[Fig. 2] Structure of Memory[3]

위에서 Text에 해당하는 부분에 실행되는 프로세스의 프로그램에 저장되며, 이때 다른 프로세스로부터 제약을 받지 않기 위해 대부분 Read-only로 저장이 된다. 또한 Data 영역에서 프로그램이 갖고 있는 변수 값과 같은 데이터와 Static 변수들이 일정한 값을 저장하고 있는 영역이다. 마지막으로 스택부분에는 함수간의 호출관계와 함수에서 사용되는 지역변수 값들이 쌍이며, 이를 이용해 하나의 프로세스가 비로소 완성된다고 할 수 있다. 즉 스택영역을 가리키는 SP포인터에 의해 함수내의 연결관계가 사용되는 변수들이 정의되는 것이다. 결국 Buffer Overflow 버그는 스택영역에 sturcpy()와 같은 함수를 이용해 넘겨받은 인자를 복사함으로써 SP포인터가 가리키는

영역을 변조해 버리는 것이다. 이럴 경우 이 프로세스는 스텍 내의 SP가 가리키는 함수로 실행 권한을 넘기게 되며, 원래 자신이 해야 할 일을 수행하는 것이 아니라 넘겨진 Seed 코드가 가리키는 함수를 수행하게 된다. 물론 대부분의 경우 /bin/ksh등을 실행하게끔 하고, Buffer Overflow의 타켓이 되는 프로그램들은 모두 root 권한의 suid 허락이 설정된 프로그램들이므로, 결국 root 권한을 획득할 수 있게 된다.

Buffer Overflow 공격의 경우 프로그램 개발자의 부주의로 인해 넘겨받은 인자나 쉘 환경변수를 이용함에 있어 넘겨받은 인자에 대해 모두 버퍼의 크기를 넘어서는 내용이 아닌지 확인을 하지 않기에 발생한 해킹 유형이라고 할 수 있다. 또한 디버깅과 운영체제상의 메모리 맵에 대해 어느 정도 지식이 있는 사람들이라면 얼마의 시간을 투자해 얼마든지 새로운 유형의 버그를 발견해 낼 수 있는 유형이다. 때문에 가장 좋은 방법은 새롭게 알려지는 모든 Overflow 관련 해킹 방법들에 대한 공급업체로부터 항상 최신의 패치들을 지원받아 이를 시스템에 적용하여 안전한 시스템을 구축해야 한다.

2.3.2 Spoofing

Spoofing이란, 자신을 타인이나 다른 시스템에서 속이는 행위를 말한다. 예를 들어, 특정 호스트에게만 접근 권한을 준다고 가정했을 경우 해커는 당연히 자신이 특정 호스트로부터 접근하는 것처럼 속이려 할 것이며, 이를 가리켜 Spoofing이라고 할 수 있다.

IP Spoofing 이란 말 그대로 자신의 IP 주소를 속여서 상대방에게 보내는 것을 가리킨다. 케빈 미트닉(Kevin D. Mitnick)이 즐겨 사용하였기에 더욱 큰 파장을 불러일으킨 IP Spoofing은 TCP/IP프로토콜의 취약점 중의 하나를 이용한 것에 불과하다.

일반적으로 두 컴퓨터사이의 인터네트워킹이 이루어질 때에 오고가는 TCP/IP 패킷의 구조는 [그림 3]과 같다.

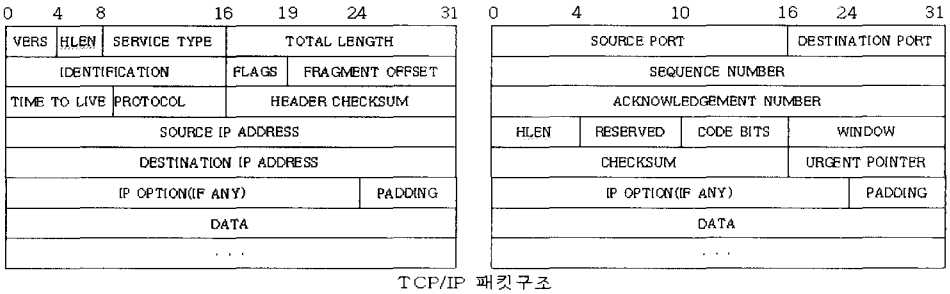
위와 같이 자신의 소스 IP에 32bit 주소와 해당 패킷이 도착해야할 Destination IP(주소)를 담고 있음을 볼 수 있다.

2.3.3 Denial of Service

해커들이 많이 사용하는 Denial of Service 의 유형을 보면 첫째, Service Overloading이며 둘째, Message Flooding으로 특정 message를 연속적으로 보냄으로써 시스템자원을 고갈시킨 후 원하는 작업을 하는 형태를 가리킨다. 예를 들면 UDP7번 서비스인 ecno 서비스에 연속된 메시지를 보낼 경우 시스템은 이를 큐에 담아두게 되며, 결국에는 네트웍 기능이 마비되어 다운되거나 리부팅되는 상태에 도달하고 만다.

2.3.4 Echo/Chargen

흔히 SDP Storm이라고 불리는 이 공격은 UDP 서비스 중 echo, chargen 서비스의 문제점을 이용해



TCP/IP 패킷구조

[그림 3] TCP/IP의 패킷구조[3]

[Fig. 3] Packet Structure of TCP/IP[3]

시스템을 다운시키는 역할을 한다. 또한 인터넷상에 이미 이 서비스들을 타겟으로 한 UDP Stomer란 툴이 존재하므로 아래와 같이 시스템 내에서 제거하는 것이 바람직하다. 실제로 echo/chargen서비스가 사용되는 경우가 드물기 때문에 큰 문제가 생기지 않는다. inetd 수퍼 서버가 관장하는 인터넷 서비스들은 /etc/service에 해당하는 포트와 서비스 이름이 정의되어 있으며, 이를 기반으로 /etc/service와 /etc/inetd.conf파일에서 echo, chargen 서비스를 코멘트 처리하여 제거한 후 inetd 수퍼 서버를 다시 띄우면 된다.

2.3.5 Flooding/storiming

SYN Flooding은 IP Spoofing과정에서 트러스트된 호스트를 다운시키기 위해 이미 기본적으로 사용된 테크닉이었지만, 96년 하반기 Phrack과 alt2600이란 두 단체에 TCP SYN Flooding 이라는 툴의 소스가 공개된 직후, 인터넷상의 수많은 호스트들이 이 공격에 피해를 입게 되었다.

2.3.6 트로이목마 프로그램

트로이목마 프로그램이란 어떤 불법적인 행위를 시도하기 위하여, 합법적인 프로그램으로 위장하거나 실행코드 형태로 다른 프로그램 내부에 존재하는 프로그램으로 사용자가 부주의하게 트로이목마 프로그램을 설치하게 되면 큰 피해를 입을 수 있게 된다. 이러한 트로이 목마 프로그램은 차후 뒷문 프로그램(Backdoor: 비인가 된 프로그램이나 시스템에 접근할 수 있도록 조치를 취하는 프로그램)을 설치하게 된다. 이렇게 뒷문 프로그램을 설치하게 되면 공격자는 시스템 전체를 제어할 수 있어 개인정보유출 등의 공격을 수행할 수 있다.[9] 최근 이러한 윈도우용 트로이목마 프로그램들이 100여 가지가 넘게 발견되고 있으며, 기능의 확장과 사용의 편리성으로 계속적으로 피해가 증가하고 있는 추세이다. 최근 많이 사용되고 있는 트로이목마 프로그램들로는 BackOrifice, Deep Throat3, Sub7 등이 있으며 이러한 프로그램들은 새로운 버전이 계속 출시되어 피해가 확산될 것으로 보인다.

2.3.7 백오리피스

백오리피스는 cDc(Cult Dead Cow)라는 해킹그룹과 Sir Dystic이 만든 MS WIN 95/98용 프로그램으로 널리 알려지게 되었다. 클라이언트/서버 모델로 설계되었으며 원격공격자는 해당 Back Orifice 백도어 서버를 공격대상 시스템에 설치해야 하고 공격자 호스트에 클라이언트 프로그램을 설치해야 한다.

클라이언트 측에서는 서버의 이러한 기능을 이용하여 파일 시스템의 모든 파일들에 대해 접근이 가능하고, 프로세스의 생성·삭제도 원격으로 조정된다. 그리고 시스템 패스워드의 유출, 키보드 모니터링, 사용자의 현재화면 캡쳐도 가능하고 네트워크 자원의 공유지정, 네트워크 접속 재지정, 파일조작, 레지스트리 조작도 가능하다. 이외에도 여러 가지 기능을 강화하여 원격사용자는 마치 자신의 시스템처럼 사용할 수 있다.

2.3.8 Deep Throat

Deep Throat 3.0은 DarkLIGHT Corp에서 공개한 프로그램으로 빠른 업그레이드와 기능 향상을 위해 피드백을 실시하는 기능이 있다. 또한 Deep Throat는 사용하기 편한 CGI를 취하고 있으며 모든 명령을 버튼 식으로 구성하였고, 각 버튼에 해당하는 설명을 화면에 출력하여 별다른 설명서 없이 누구나 쉽게 사용할 수 있다.

2.3.9 NetBus 1.70

NetBus pro는 원격 관리 스파이 프로그램으로 설치가 매우 용이하고, 사용하기 쉬운 인터페이스를 가지고 있다. File Manager, Registry managerem, Application Redirect등과 같은 원격관리 기능과 더불어 화면 캡쳐, 키보드 캡쳐 등과 같은 스파이 기능을 제공한다. 공격자는 NetBus클라이언트 프로그램을 이용하여 NetBus 서버가 설치된 호스트에 접속한 다음 클라이언트 프로그램의 다양한 명령버튼을 이용하여 여러 가지 작업을 수행할 수 있다.

2.3.10 Sub 7

Sub 7은 일반관리와 스파이 기능과 더불어 IRQ, RC, E_mail 통지 기능이 있어 검색을 하지 않고도 감염상태를 확인 할 수 있다. 또한 클라이언트 프로그램 설정이 가능하여 자신에게 맞게 설정하여 사용할 수 있다는 장점을 가지고 있다.

2.3.11 Keylogger

Keylogger는 사용자의 Keylog를 가로채는 트로이목마 프로그램으로 통합된 토로이목마 프로그램들에서 가장 악의적인 목적으로 많이 사용된다. 이 Acolytes라는 프로그램은 Keylogger 프로그램과 이 프로그램을 시스템에 자동으로 설치해주는 Dropper/Ecokys를 합쳐서 만든 프로그램으로 계속적인 피해가 발생하고 있다.

2.3.12 Window Spawner

Window를 계속적으로 다운시키는 악성 애플릿 공격으로 클라이언트 시스템 자원을 모두 고갈시켜 시스템을 다운시키거나 사용을 방해하는 공격이다.

2.3.13 Java Applet Killer

한계값 이상의 변수를 자바 메소드에 보냄으로써 윈도우 시스템을 다운 시키는 악성 자바 애플릿으로 윈도우 NT 시스템과 윈도우 95/98의 모든 시스템을 공격할 수 있다.

3. 해킹과 바이러스에 대한 방어 대책 연구

3.1 방화벽 시스템

방화벽의 원래의미는 건물에서 발생한 화재가 더 이상 번지는 것을 막는 것이다. 이 의미를 인터넷에 적용한다면, 이는 네트워크의 보안사고나 위협이 더 이상 확대되지 않도록 격리하는 것이라고 할 수 있다. 이는 특히 어떤 기관의 내부 네트워크를 보호하기 위해서는 외부에서의 불법적인 트래픽이 들어오는 것을 막고, 허가하거나 인증된 트래픽만 허용하는 방어대책이라고 할 수 있다[4].

방화벽 시스템의 기본 목표는 네트워크 사용자에게 가능한 투명성을 보장하면서 위험 지대를 줄이고자하는 적극적인 보안 대책을 제공하는 것이다. 방화벽의 구현은 기본적으로 컴퓨터간의 권한이 없는 모든 통신을 막도록 설계되어져야하며 외부에서 내부 망으로 또 내부에서 외부로의 모든 트래픽이 보안 시스템을 반드시 경유할 수 있도록 설계되어야 한다.

실제 방화벽 구현에 있어서는 망기술, 연결의 용량, 트래픽 부하, 조직정책들이 해당 조직에 적합하게 하나의 완결된 구조로 구현되어야 한다. 이를 위해서는 요구되는 처리능력을 파악하는 것이 중요하며 연결의 속도와 같은 속도로 데이터 그램을 처리할 수 있어야 한다. 만약 방화벽이 데이터 그램을 전송할지 여부를 결정하기 위해서 버퍼에 데이터 그램을 지연시키면, 방화벽은 재전송으로 압도될 것이고 결국 버퍼는 넘쳐 방화벽의 오버플로우를 초래하게 될 것이다. 결국 망속도로 동작하기 위해서는 방화벽은 그 작업에 최적인 하드웨어와 소프트웨어를 갖고 있어야 한다.

3.2 방화벽 시스템의 역할

방화벽 시스템은 인터넷과 같은 외부 네트워크와 내부 네트워크 사이에 놓이며, 외부 네트워크로부터 내부 네트워크로의 침입을 감지하여 정보 및 자원들을 보호한다. 즉, 외부 네트워크에서 내부 네트워크로 접근하기 위해서는 방화벽 시스템을 통과하여야만 내부 네트워크로 진입할 수 있도록 하여 내부 네트워크에 존재하는 정보 및 자원들에 대한 트래픽을 사전에 방어하는 것이다[5].

3.3 방화벽 시스템의 한계

방화벽 시스템은 내부 사용자가 내부 네트워크에 존재하는 중요한 정보를 디스크 혹은 테이프와 같은 매체를 통해 가지고 나가는 것은 방어하지 못한다. 또한 외부 네트워크로부터 내부 네트워크로 비인가된 다이얼 모뎀을 통한 접근을 방어하지 못하며, 바이러스 혹은 정보 지향적인 공격에 대해서는 방어하

지 못한다. 따라서 방화벽 시스템은 보호하고자 하는 네트워크에서 내부 네트워크로의 진입을 1차로 방어해주는 기능을 수행한다.

3.4 침입 탐지 시스템 (Intrusion Detection System)

방화벽의 설치이후에도 완벽한 보안을 위한 시스템이 요구된다. 방화벽을 우회한 외부의 각종 위험한 해킹행위가 내부 네트웍에서 발생하고 있다고 판단할 때 방화벽 내부의 불법적인 사용자의 침입이 우려될 때 동시사용자의 폭주로 방화벽의 일시적인 중지가 불가피한 경우가 잦아지는 경우, 무분별한 모뎀접속서버의 사용으로 보안이 걱정될 때 불법적인 침입자의 기록을 남겨 악성IP를 알기 위해서 침입탐지 시스템의 설치가 필요하다.

다음 [그림 4]는 침입 탐지 시스템의 일반적인 구성도이다[6],[7].

침입탐지시스템은 방화벽(FireWall)을 우회하거나 방화벽 내부에서 발생하는 각종 해킹 및 크랙킹 행위를 실시간 패킷분석으로 탐지(Detection)해 접속을 차단하거나 각종 경고, 문자서비스, 전자메일, 호출기, 경고음 등으로 응답하는 시스템이다.

3.5 주기적인 바이러스탐지와 시스템점검

정보시스템을 관리하고 있는 사람들은 정기적이고 최신의 컴퓨터 바이러스에 대한 정보를 수집해야 할 의무가 있다. 위에서 살펴보았듯이 신종 컴퓨터 바이러스의 출현은 수시로 이루어지고 있기 때문에 항상 새로운 정보를 파악하고 대처방안을 공고 또는 시행하여 그 피해를 사전에 막아야한다. 특히 정부기관 또는 전문업체들의 정보가 많은 도움을 주고 있어 정보를 충분히 얻을 수 있다.

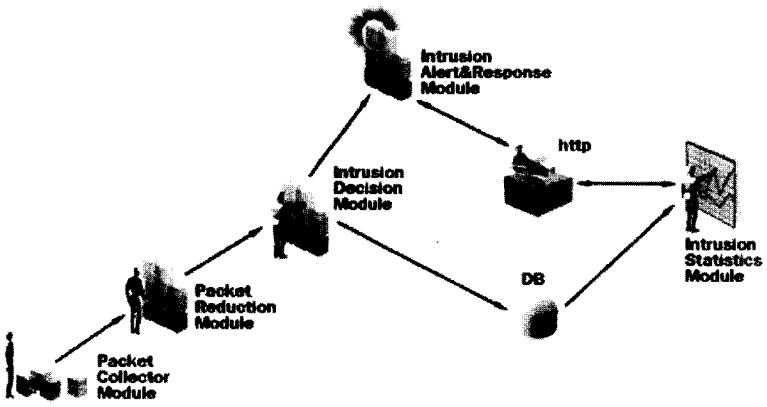
최신 컴퓨터바이러스에 대한 정보는 아래의 주소 등에서 얻을 수 있다[2],[8].

http://www.certcc.or.kr, http://www.cyber118.or.kr, http://www.kisa.or.kr(한국 정보보호 진흥원 산하 조직), http://www.nca.or.kr/(한국전산원), www.ahnlab.com(안철수 바이러스연구소), www.hauri.co.kr((주)하우리)

4. 웹 쇼핑몰 시스템의 점검 사례 연구

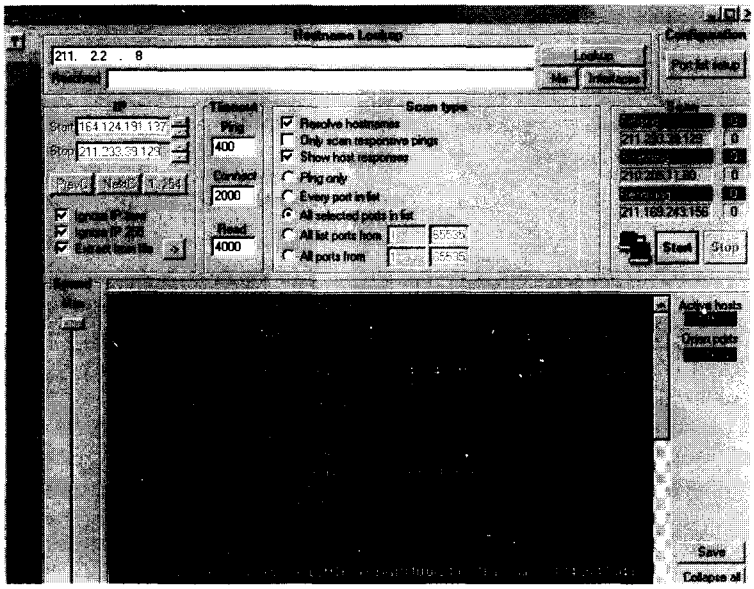
4.1 쇼핑몰 웹서버의 보안상태

2001년 5월 한달 동안 국내의 113개 쇼핑몰 웹서버의 취약점을 포트 스캔을 통해 살펴보았다. 포트 스캔(Port Scan)은 웹서버의 서비스포트 상태를 체크하는 것으로써 서비스되고 있는 포트이외에 열려 있는 서버의 포트를 체크할 수 있다. 대다수의



[그림 4] 침입탐지 시스템 구성도

[Fig. 4] Configuration of Intrusion Detection System



[그림 5] 슈퍼 스캔의 서버 서비스포트 상태 탐색장면

[Fig. 5] A Scene of Investigation by SuperScan for Server Service Port

서버가 많은 포트를 열어 놓은 상태로 서비스를 진행 중이었다. nmap 과 슈퍼 스캔이란 프로그램을 통해서 웹서버의 서비스 포트 상황을 살펴보았다. 다음 [그림 5]는 포트스캔의 동작 모습이다.

탐색 결과, 일반적으로 열어 놓을 수 있는 http, ftp, telnet (혹은 ssh), pop-3 등 이외에도 의미 없이 열려 있는 포트를 쉽게 찾을 수 있었다.

꼭 필요한 서비스 포트만 열어 놓은 이른바 베스천(Bastion) 호스트 상태를 점검해보았다. 다음 <표 4> 113개의 웹서버중 5개미만의 서비스 포트를 갖고있는 베스천 상태의 수를 보여준다.

<표 4> 베스천 호스트의 갯수

<Table 4> No. of Bastion Hosts

포트의 오픈 상태	베스천 호스트	비 베스천호스트	총
서버 수	51	62	113

그리고 어느 특정 포트가 많은 중복이 되어 검색되었지는 않았지만 주로 검색되어진 포트는 다음 <표 5>와 같다.

<표 5> 가장 많이 검색된 취약포트

<Table 5> Delicate Ports of Mostly Searched

서비스	프로토콜	포트넘버
FTP	TCP	21
SMTP	TCP	25
DNS	TCP/UDP	53
NFS	UDP	2049

4.2 보안의 제안과 설정

4.2.1 쇼핑몰의 규모

본 논문에서 살펴 보게될 쇼핑몰은 하루 평균 4만 페이지 뷰와 일일 매출 900만원 규모의 단일 품목 형태의 쇼핑몰이다. 총 16대의 서버가 서비스 중인데, 10대의 웹서버와 4대의 멀티미디어 스트리밍 서비스 서버, 1대의 스토리지 서버, 1대의 데이터 베이스 서버가 운영중이다. 3 여년간의 운영 중 다행히 영업에 지장을 미칠 만큼의 해킹피해는 없었다고 한다.

4.2.2 서버의 취약점

현재 영업중인 O 웹쇼핑 몰의 10개의 웹서버 중 한 대를 nmap과 nslookup의 명령어를 사용하여 서비스 상태와 해킹의 주경로가 되는 열려있는 포트를 확인해보았다.

Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)
Interesting ports on (211.32.***.***):
(The 1503 ports scanned but not shown below are in state: closed)

Port	State	Service
21/tcp	open	ftp
25/tcp	open	smtp
80/tcp	open	http
135/tcp	open	loc-srv
139/tcp	open	netbios-ssn
199/tcp	open	smux
465/tcp	open	smtps
554/tcp	open	rtsp
1008/tcp	filtered	ufsd
1032/tcp	open	iad3
1433/tcp	open	ms-sql-s
1987/tcp	open	tr-rsrb-p1
2301/tcp	open	compaqdiag
5050/tcp	open	mmcc
5631/tcp	open	pcanywheredata
6666/tcp	open	irc-serv
7007/tcp	open	afs3-bos
8080/tcp	open	http-proxy
9090/tcp	open	zeus-admin
65301/tcp	open	pcanywhere

[그림 6] nmap으로 서버 포트 취약점 탐구

[Fig. 6] Investigation of Delicateness in Server Port by 'nmap'

위의 [그림 6] 에서 보는 것처럼 서버들의 IP주소 노출과 쓸데없는 서비스 포트들을 열어놓은 상태로 서비스 중이란 것을 볼 수 있다. 따라서 우선 배스천호스트 구축으로 웹전용 서버들의 설정을 다시 해 줄 줄 필요가 있다.

4.2.3 네트워 취약점

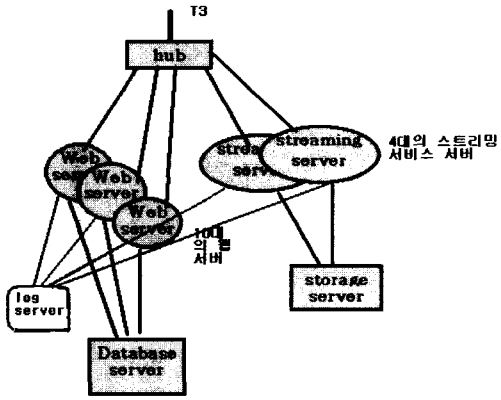
10대의 웹서버들과 4대의 스트리밍 서버는 모두 자체 네트웍 구성없이 IDC 센터 내에 설치되어 바로 백본에 연결되어 있는 상태이다. 모든 웹서버들과 스트리밍 서버들은 데이터베이스 서버에 연결되어 있는 상태인데 취약한 웹서버들 통해 회사의 데이터베이스 서버까지 침입도 가능하다. 라우터를 통한 자체 네트웍 구성이 필요하다.

4.2.4 보안의 제안과 설정

앞서 보았듯이 일단 서버의 자체와 보안 네트웍 구축이 필요하다. 웹서버 10대와 스트리밍 서버 4대를 필요하지 않은 모든 서비스를 제거하여 베스천호스트를 구성한다. 베스천호스트의 구성으로 현재까지 알려진 해당 호스트에 대한 내/외부에서의 침입 위협으로부터 모두 안전할 수 있도록 하는 것이다 [9],[10]. 다음과 같은 방법으로 베스천호스트로 전환을 시킨다.

① 불필요한 계정 및 홈디렉토리 삭제
② 불필요한 서비스 제거
(/etc/services, /etc/inetd 수정)
③ 부트 파일 중 웹서비스시 필요하지 않은 파일 삭제
③ 보안패치(security patch) 수행
④ 보안패치로 해결되지않는 취약점들은 수동으로 보안문제 해결
⑤ 무결성검사 보안도구 설치/운영

다음은 베스천호스트 된 상태의 서버들을 패킷 필터링 기능을 하는 라우터를 중심으로 한 새로운 네트웍을 구축하는 것이다. 기존의 [그림 7] 네트웍을 새로운 네트웍으로 다음 [그림 8]과 같은 제안을 하여 변경하였다.

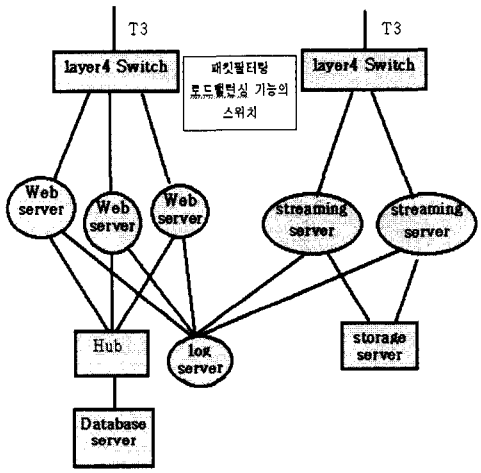


[그림 7] 기존의 O 쇼핑몰의 네트웍

[Fig. 7] A Network of Internet Shopping Mall "O"

제안네트웍 구성도에는 라우터의 ACL(Access List) 필터링 기능과 패킷 필터링의 기능이 해커의 침입 범위와 기회를 그만큼 제어가 가능하다는 것이다. 이렇게 많은 않은 그리고 복잡하지 않은 보안 설정만으로도 많은 부분에 보안기능이 추가되는 것이다. 다음은 개선된 네트웍 환경이다. 이로써 기존의 알려진 해커의 경로가 많은 부분 차단되었다

4.3 추가적 보완이 필요한 보안기능[6],[7]



[그림 8] 제안 네트웍

[Fig. 8] A proposed Configuration of Network

1) 접근제어, 패스워드 인증기능 사용
.htaccess, .htpasswd를 사용하여 주요 디렉토리에 사용자인증기능을 추가하여 운영한다. 이 기능만으로 부족할 경우에 보다 강화된 인증기법을 사용할 수도 있다.
2) 로그강화
시스템로그(wtmp, utmp, sulog, pacct등)와 www 로그를 수시로 백업하고 가능하다면 로그 서버를 따로 운영하여 2중 관리하는 것도 바람직하다.
3) 암호화 기능 이용
스니퍼링방지 스니퍼링을 통한 정보유출을 막기 위하여 주요정보 송수신시 SSL, SHTTP등 암호화기능을 사용한다.
4) 철저한 백업
수시로 정기적인 백업을 하여 해킹이나 재난으로 인한 사고에 대비한다.
5) 원격관리
웹서버의 관리는 콘솔에서 하는 것을 원칙으로 하고, 원격 접근 시 해당 로그를 남기도록 한다.
6) 바이러스 또는 침입탐지시 경고기능
임의의 사용자가 주요 관리화일 접근시 관리자에게 알려주거나 네트워크를 통한침입시도 가 있을 경우 경고기능을 추가하고(침입탐지용 상용도구설치/운영) 또 바이러스의 주기적인 체크를 위해 다중의 바이러스체크 시스템을 설치한다. 별도로 시스템 운영자는 바이러스 상황을 공고하여 사내구성원 개개인에게 경각심을 주어 사내의 개인 시스템에서의 시작되는 바이러스 피해를 최소화시킨다.
7) 각종 보안도구의 설치/운영
공개용/상용 보안도구를 서비스의 특성에 맞게 설치, 운영한다. 시스템의 취약점을 점검해주는 도구 및 무결성 점검도구는 반드시 설치한다.

5. 결론

본 논문에서는 최근의 해킹기법과 컴퓨터 바이러스의 피해를 예로 들고 체계적으로 대처하고, 안전한 정보화의 활용을 위한 정보 시스템의 구축 방법에 대하여 기술하였다.

최근의 폭증하는 해킹사고와 컴퓨터 바이러스의 피해 증가로 보안관리의 중요성이 강조되고는 있지만 뛰어난 해커의 역량을 저지하기에는 역부족인 것이 사실이다 그러나 기본적인 서버시스템의 보안설정만으로도 해킹의 대부분을 차지하고 있는 초보나 중급수준의 피해로부터 더욱 안전해 질 수 있지만 많은 부분의 중형시스템과 개인의 보안상태는 아직도 무방비 상태로 놓여 있음을 알 수 있었다.

시스템 관리자들은 특히 보안에 관한 이슈에 대한 연구와 사례분석을 하여 보다 안전한 정보화사회를 위한 노력을 해야 할 것이다. 또한 국가차원에서도 해킹방지를 위한 전문인력 양성과 교육을 위한 지원 프로그램을 통해 적극적으로 노력해야 할 것이다.

소프웨어적으로 하드웨어 적으로 완벽한 정보시스템은 없다. 언제든지 생각지 못한 방법으로 자신의 시스템들은 해커와 바이러스 또는 다른 종류의 정보화 역기능요소로부터 피해를 볼 수 있다. 모든 컴퓨터 사용자는 이에 대비하여 끊임없는 대처 방안 연구가 필요하다.

본 논문에서는 배스천호스트의 구성을 제안한다. 배스천호스트의 구성은 현재까지 알려진 해당 호스트에 대한 내/외부에서의 침입위험으로부터 안전할 수 있도록 하는 것이다.

※ 참고문헌

[1] 양유석, "전자상거래의 비즈니스 모델과 미국의 EC동향", 삼성경제연구소, 2000. 5.

[2] Exploit017, "리얼 해킹", 파워북, 2001.

[3] 진영승, "인터넷에서의 해킹기법과 보안방법에 관한 조사분석", 연세대학교. 1999.

[4] 백의선 외 8인, "정보화 역기능 사례집" 한국정보보호센터, 2000.12.

[5] 성백훈, "해킹과 보안정책에 관한 연구", 성균관대학교 석사학위논문, 1999.

[6] 유영렬, "해킹할 것인가, 당할것인가", 삼각형프레스, 2000.

[7] 최홍석, "인터넷 전자상거래의 보안시스템에 관한 연구", 청주대학교 석사학위논문, 1999.

[8] 장태우, "정보시스템 구축 시 정보보호를 위한 보안체제", 연세대학교 석사학위논문, 1994.

[9] 정상수, "Unix 환경에서의 해킹 방지를 위한 침입탐지 시스템의 설계에 관한 연구", 국방대학원, 1996.

[10] 신재호외 3인, "Network Bible", 영진출판사, 1999.

※ 인터넷 참조사이트

http://www.kisa.or.kr

http://www.certcc.or.kr

http://www2000.ogsm.vanderbilt.edu/papers/1995_Internet_estimates.html

http://shum.huji.ac.il/jcmc/vol1/issue3/hoffman.html

http://haas.berkeley.edu/~citm/wp-1005-summary.html

http://www.cisco.com/warp/public/3/kr/online_seminar

이 내 준

1985 : 부산대학교 기계설계학과 졸업(공학사)

1987 : 미국 앨라배마 주립대 대학원 기계공학과 졸업(공학석사)

1988 : 미국 어번 주립대 대학원 생산 경영학과 수료

2000 : 충북대학교 경영대학원 경영학과 졸업(경영학석사)

2001~현재 : 충북대학교 대학원 국제 경영학과 박사과정

현재 : HMT Korea 대표, 충북과학대학 전자상거래학과 겸임 교수