대규모 네트워크 환경하에서의 해킹 분석 및 대책

김상춘*
*삼척대학교 정보통신공학과 교수

요 약

인터넷이 발전해감에 따라 사이버 세계라고 하는 대규모 네트워크 환경이라는 또 다른 세상이 창출되었다. 그러나 대규모 네트워크 환경하에서는 정보보호의 취약성 때문에 인터넷 서비스를 이용하는 네티즌들의 안전성이 보장되지 않는다. 이처럼 불법 침입자들로부터 선의의 이용자를 보호하기 위해서는 그들이 해킹 기법과 그 대응책을 숙지해야 할 것이다.
이 논문에서는 대규모 네트워크 환경하에서 발생되고 있는 해킹에 대하여 분석하고 그에 대한 대책을 제시하는데 그 목적이 있다.

A Hacking Analysis and Counterplan under large-scale network environment

Kim Sang Choon*

1. 서 론

대규모 네트워크 환경하에서는 전산망 해커 등 침입자에게 매우 취약한 면을 보여주고 있다. 청소년들이 미국 국방성의 시스템을 침입하거나 정부기관 등 주요기관의 시스템에 공격하여 서비스를 마비시키는 등 세계의 이목을 집중시킬만한 중요한 사건들은 대규모 네트워크 환경하에서는 자주 일어나는 일이다. 이처럼 대규모 네트워크 환경인 인터넷이 해커들의 공격대상이 되는 이유를 들어보면 다음과 같다.

첫째, 인터넷의 개방성이다. 인터넷은 상호 정보교환을 대화형으로 빠르게, 원활하게 제공하여 전세계 어디서나 연구개발 정보 등을 자유롭게 전달하도록 하므로 침입자들에게는 시스템에 침입할 수 있는 기회가 많이 주어지는 것이다. 가령 예전에는 각 기관에서는 guest, sonnim 등의 계정을 만들어 자신의 시스템을 누구나 사용할 수 있도록 하였는데 침입자가 이를 이용하기도 한 것이다. 더구나 국경 없는 전세계의 전산망으로서 여러 국가들 사이에 문제가 발생할 수 있다.

둘째, UNIX, TCP/IP 등의 소스가 개방되어 있는 것이 문제이다. IBM/SNA 등과 같은 업체 제품에서는 개발업체만이 소스를 독점하고 있으므로 해당 전산망의 정보보호에는 큰 문제가 없었지만, TCP/IP 프로토콜이나 유닉스 시스템은 수많은 학교나 연구소 등에서 소스를 소유하고 있을 뿐 아니라 연구나 실습용으로 자주 공개되어 성능이 개선되기를 바라고 있어 이를 악용하고 있다. 그리고 소스뿐만 아니라 서점에서 많은 교재들이 제공되고 인터넷에서는 여러 가지 문서들도 무료로 배포되므로 선의의 연구대상이 아닌 악의적 공격대상으로 인터넷에 심취할 수 있는 것이다.

셋째, 침입자들의 상호정보교환이 손쉽다는 것이다. 인터넷에서는 검열이라는 것이 불가능할 정도로 너무나 많은 전자게시판(BBS)과 온라인 정보교환을 위한 방법들이 제공되므로 어떤 침입자의 새로운 침입방법 등이 손쉽게, 은밀하게 서로 교환되어 침입자들이 양산되는 것이다. BBS의 여러 게시판과 IRC(Internet Relay Chatting), 전자우편, 네트워크뉴스그룹을 통한 정보의 전달은 순식간에 방송되듯이 모든 이들에게 알려지곤 한다. 또한 어떤 곳에서는 정상적인 관리자들을 위해 어떻게 해킹을 당할 수 있다는 경고의 문서를 개방하는데 도리어 이것이 침입자들에게 도움이 되는 자료가 될 수 있다.

인터넷의 이러한 취약점은 대부분 인터넷에서 활동하는 불법 침입자에 대한 취약요소로서 침입자들이 일으킬 수 있는 위협요소들은 악의적 목적에 의한 불법 접근과 비인가 된 시스템의 사용, 정보의 열람, 파괴 및 변조, 정상적인 시스템 서비스 방해 등을 생각해 볼 수 있다.

정보시스템들이 인터넷을 통해 연결되면서 지역적인 거리와는 무관하게 전세계가 하나의 네트워크 화되어 가고 있다. 이러한 추세에 따라 국내에서 발생되고 있는 해킹기법도 외국의 최신 해킹기법과 크게 차이가 없으며, 외국에서 발표된 최신 해킹 기법을 이용한 공격이 국내의 정보시스템을 공격하는 데에도 동일하게 적용되고 있다.[1]

2. 대규모 네트워크 환경인 인터넷에서 발생되는 해킹 수법

2.1 해킹 수법의 개요

지금까지 90년대 초반에 많이 이용되던 해킹 수법들은 이제 업체들의 수정판 배포 및 버전업과 시스템 관리 실무자들의 관심으로 취약점들이 많이 해소되기는 하였으나 여전히 해커지망생들에 의해 이용되고 있으며, 관심을 가지고 대처방법을 구현해야 한다.[2] 정보보호사고의 수가 늘어감에 따라 유형 또한 변화하는데, 1988년도에 단순한 계정 및 패스워드에 대한 공격 형태를 보였으나 1990년대를 접어들면서 파일 시스템과 네트워크의 취약점을 이용한 형태로 바뀌었다. 우선 인터넷에서 해킹에 이용되는

취약점들을 알아보고, 그중 대표적인 수법으로 IP Spoofing, Packet Sniffing, NFS Attacks, Sendmail Attacks, Network Scanning 등에 대하여 분석한다.

2.2 대규모 네트워크 환경인 인터넷에서의 해킹 취약점

해킹을 방지하기 위해서는 해킹에 이용되는 취약점을 알아야 할 것이다. 유닉스는 국내 인터넷에서 쓰이는 주된 서버로 미국의 CERT에서 발행하는 CERT-Advisory 문서들을 참고할 때 거의 유닉스 기종별로 다양한 문제점들을 가지고 있는데, 이러한 문제점들의 많은 부분이 유닉스 시스템이 가진 버그에 의한 문제점들과 시스템을 잘못 관리하면서 생긴 문제점들이다. 여기에는 유닉스 상에 존재하는 세 가지 정보보호 분야에 대하여 이야기 해보겠다.

2.2.1 패스워드 및 계정 정보보호

패스워드 및 계정 관련 정보보호 취약성은 패스워드의 유추, 불필요한 계정, 그리고 패스워드가 없는 계정 등이다. 침입자들이 시스템에 침입할 수 있는 가장 쉬운 방법이 시스템 상의 특정 사용자 계정을 훔치는 것이다. 이러한 정보보호 취약성은 많은 시스템들이 그 기관에 속해있지 않은 사용자의 계정과 추측하기 쉬운 패스워드를 가진 계정을 허용한다는 점에서 출발한다. 또한, 오랫동안 사용하지 않거나 불필요한 계정을 그대로 두는 것은 매우 위험하기 때문에 오랫동안 사용치 않는 계정은 패스워드에 에이징 기능을 부여하여 일정 기간 사용치 않는 경우 계정을 막아버리는 방법이 좋다.

외부의 사용자들을 위하여 guest', 'sonnim' 등과 같은 계정을 만들어 둔다면 누구라도 시스템에 대한 접근 권한을 얻게 된다. 마지막으로 가장 주의해야 하는 정보보호 취약성은 패스워드를 가지고 있지 않은 계정이다. 몇몇 유닉스에서는 who', 'date', 'lp' 등과 같은 패스워드를 가지고 있지 않은 계정을 기본으로 제공하고 있다. 이러한 계정들은 시스템을 설치할 당시 awk -F: '$2 == "" {print}' /etc/passwd"를 실행하여 패스워드 없는 계정에 대한 대비를 하여야 한다.

2.2.2 파일 시스템 정보보호

유닉스 시스템의 정보보호에서 파일 시스템의 정보보호는 가장 필수적이다. 침입자가 어떠한 경로로 시스템에 침입했던 간에 그는 미래의 침입을 위하여 backdoor를 만들거나, 다른 호스트의 침입 혹은 해당 시스템의 루트 권한을 뺏기 위하여 트로이 목마(Trojan Horse) 등의 불법 프로그램을 만들려고 할 것이다. 그밖에도 파일 시스템 내에 논리폭탄(Logic Bomb)등을 이용하여 어떤 사건을 만나면 시스템을 파괴하거나 고장을 일으키는 프로그램을 이용할 수 있으며, 바이러스 프로그램 등을 만들기도 한다. 파일 시스템의 정보보호 취약성을 열거하자면 파일 및 디렉토리 접근 권한 잘못 설정, SUID와 SGID를 가진 실행 파일 및 스크립트 존재 여부, loadmodule 문제, 백도어, 트로이 목마 프로그램 및 주요 파일의 교체 여부, cron, inetd.conf, rc* 파일 내 잘못된 내용 삽입 여부 등이 있다.

2.2.3 네트워크 정보보호

네트워크 정보보호 문제는 인터넷의 발전과 더불어 그 범위가 점점 넓어지고 있는 실정이다.

r' 명령 관련 .rhosts 파일을 이용하면 그 파일에 속해있는 시스템과 사용자들은 사용자 인증 과정을 거치지 않고 시스템에 대한 접근 권한을 얻을 수 있다. /etc/hosts.equiv 파일은 시스템 관리자에 의해 신뢰성 있는 호스트를 지정하여 파일의 내용이 +로만 되어 있다면 /etc/hosts 파일에 속해있는 모든 시스템에서 패스워드 없이 접근할 수 있다.

ftp에 관련된 정보보호 취약성은 크게 구성 파일의 잘못된 설정으로 인한 것이 대부분이다. 구성 파일의 잘못된 구성은 anonymous ftp의 홈 디렉토리, 관련 파일의 접근 권한, ftp 홈 디

렉토리에 여분의 실행파일들을 설치하는 경우이다. 이러한 정보보호 취약성들은 anonymous ftp 서버를 구축할 경우에 조금만 신경 쓰면 미연에 방지할 수 있다.

NFS를 설치한 대부분의 유닉스는 /etc/exports 또는 /etc/dfs/dfstab에서 다른 호스트가 mount 할 수 있는 파일 시스템을 export 할 파일 시스템을 지정할 수 있다. 하지만, 많은 관리자들이 호스트들을 지정하지 않아 그 파일 시스템은 world export된 상태가 되어 인터넷의 어느 호스트에서나 mount 할 수 있게 된다. 이런 경우 외부에서 사용자의 패스워드를 몰라도 일단 export된 디렉토리를 mount한 다음 원하는 사용자의 $HOME/.rhosts를 만들어서 rlogin 또는 rsh을 이용하여 로그인할 수 있다. 또한, nfsbug라는 프로그램을 이용해 시스템 상의 NFS에 대한 취약성을 검색할 수 있다.

sendmail은 초기 설정 상태로 루트 권한을 이용하여 구동되며, 루트 권한을 이용하여 메일을 전달한다. 그 후에 메일을 해당되는 사용자의 ID로 변환해 준다. sendmail은 구성파일 읽을 때 루트 권한을 가지고 모든 일을 처리한다. 이처럼 모든 일을 루트 권한을 이용하여 처리하기 때문에 만일 초기 구성 파일을 잘못 설정한다면 침입자에게 공격당할 가능성이 높아지게 된다. 일반적으로 mailing list는 그 그룹에 속한 일반 사용자에게 쓰기를 허용하는 경우가 많다. 이 경우 그 일반 사용자는 setuid 쉘을 이용하여 비인가 된 권한을 가질 수 있다. 또한 alias 파일의 경우에는 파일내의 메일을 통해 이진 파일을 전송할 수 있는 decode 프로그램들을 실행할 수 있는 entity를 포함할 수 있는 내부 버그에 의한 문제가 존재한다. 이러한 문제점에 대한 해결책은 alias 혹은 관련된 파일은 루트 권한 이외의 사용자에게 쓰기를 허용치 않는 것이다. 운영체제 자체의 문제로는 bin과 같은 시스템 관리에 관련된 권한을 이용하여 프로그램을 실행할 수 있다는 점과 전달된 메일을 다른 지정된 곳으로 전송하는 .forward 파일을 shadow password 파일과 같은 중요한 파일로 링크 해 놓는 경우이다. 이러한 문제들은 현재 배포된 sendmail에서는 교정되어 있어서 sendmail 버전을 업그레이드하는 것으로 문제를 쉽게 해결할 수 있다.

2.3 대규모 네트워크 환경인 인터넷에서의 해킹 수법 및 해결방안

IP Spoofing은 TCP/IP 프로토콜의 구조적 결함, 즉 TCP 시퀀스 번호(sequence number), 소스 라우팅(routing), 소스 주소를 이용한 인증(authentication) 메커니즘 등을 이용한 방법으로서 인증 기능을 가지고 있는 시스템에 침입하기 위해 침입자가 사용하는 시스템을 신뢰성 있는 호스트(trusted host)로 위장하는 방법이다

IP Spoofing을 예방하는 방법으로는 네트워크와 시스템에 대한 대책으로 구별할 수 있다. 먼저 네트워크에 대한 사항으로는 내부 네트워크를 외부의 IP Spoofing으로부터 보호하기 위해서 패킷 필터링 기능과 정보보호 취약성이 보강된 라우팅 프로토콜을 포함하고 있는 라우터를 설치한다. 또한, RIP와 같이 정보보호 취약성이 많은 라우팅 프로토콜을 정보보호 취약성을 보강한 프로토콜로 교체하는 것도 좋은 방법이다. 만일, 라우터가 설치되지 않은 경우 방화벽 시스템을 설치하여 패킷을 필터링 할 수 있는 기능과 함께 소스 IP 주소를 이용하여 인증하는 응용프로그램을 사용하지 않아야 한다. 또한, 외부로 나가는 패킷의 소스 IP 주소를 변경하여 내부 네트워크 정보가 외부에 노출되는 것을 방지하여 침입을 어느 정도 방지할 수 있다. 시스템 내에서는 소스 IP 주소를 이용한 인증에 대한 대책과 시퀀스 번호 조작에 대한 대책을 세워야한다.

Packet Sniffering은 tcpdump, snoop, sniffer 등과 같은 네트워크 모니터링 도구(network monitoring tool)를 이용하여 네트워크에 돌아다니는 패킷의 내용을 분석하여 필요한 정보를 알아내는 것이다. 누구나 쉽게 구할 수 있는 스니퍼는 LAN상의 모든 패킷을 감시하고 유출할 수 있어 이를 이용하여 원격지 접속 시도 시에

전달되는 사용자의 ID와 패스워드를 알아낸다. 보통 이 프로그램은 정상적인 프로그램이름으로 설치되어 알아내기 어려우므로 LAN 인터페이스의 모드를 점검하여 스니퍼 설치 여부를 감지해내는 CPM이라는 도구를 사용하여야 한다. 이 스니퍼의 공격을 차단하기 위해서는 일회용 패스워드(One Time Password)를 사용하거나 통신 중 암호화 전달하는 프로그램인 SSH(Secure Shell)이나 S-Telnet(Secure Telnet)등을 사용하는 것이 좋다.

NFS(Network File System) 공격은 주로 NFS 구성상의 문제로 인해 발생한다. /etc/exports 파일의 구성에서 자리수가 256자를 넘은 경우 누구나 그 시스템의 디스크를 마운트할 수 있으며, 쓰기 권한이 열린 경우라면 불법적으로 .rhosts를 만들거나 계정을 만들어 손쉽게 침입할 수 있게 된다. 정확한 NFS 구성을 하거나 NFS를 사용하지 않는 것이 좋다.

Sendmail은 초기 설정 상태로 루트 권한을 이용하여 구동되며, 루트 권한을 이용하여 메일을 전달한다. 그 후에 메일을 해당되는 사용자의 ID로 변환해준다. 또한, sendmail이 구성 파일을 읽을 경우 루트 권한을 가지고 모든 일을 처리한다. 이와 같은 복잡한 구현과 setuid root 실행모드로 인해 지금까지 수많은 버그들이 발표되었고 해커들이 손쉽게 이용하는 수법 중의 하나이다. 여기에는 패스워드를 크랙할 수 있도록 패스워드 파일을 카피하거나 root 쉘을 뺏는 버그들이 포함되어 있으며 버그가 패치 된 최신 버전을 사용하는 것이 가장 바람직하다. 또한 root 실행이 아닌 일반권한으로 실행할 수 있는 방법들이 제공된다. smap 등과 같은 프락시를 이용하여 사용하는 것이 좋다.

마지막으로 Network Scanning 공격 형태는 원격 시스템의 정보보호 취약성을 검색해 주는 프로그램을 이용하여 정보를 수집한 후, 이 정보에 제시된 취약점을 공격하여 비인가 된 접근권한을 얻는 것이다. 대표적으로 ISS와 SATAN 등이 있다.

3. 대규모 네트워크 환경인 인터넷 해킹 대책

3.1 최근 해킹 수법 동향

최근 미국의 CERT/CC에서 발표된 정보보호 권고문과 사고들을 참조하여 분석된 최근 해킹 기법은 다음 (표 1)과 같이 요약할 수 있다.[3]

<표 1> 최근 해킹 기법

해킹명	취약점 및 해킹 기법 요약
rpc.statd 공격	버퍼 오버플로우 취약점 존재 내/외부의 사용자 임의의 명령어를 수행 가능
윈도우즈 시스템 서비스 거부 공격	SYN Flooding, Teardrop, Bonk/Boink, Land, Jolt/Sping, WinNuke 등
대규모 스캔 공격	imap, rpc.statd 등 알려진 취약점에 대한 스캐닝 공격
named/Bind 공격	버퍼오버플로우 취약점 존재 관리자 권한 획득 가능 서비스 거부 공격 가능
Post q/tcpmux	디폴트 계정 존재 패스워드가 없는 계정에 로그인 가능
mscan 공격	phf, test-cgi, handler, imap, statd, named 등의 취약점 스캔
POP/IMAP서버 버퍼오버플로우	버퍼오버플로우 취약점 존재 원격에서 관리자 접근 권한을 획득 가능
mound 공격	TCP 포트번호 12345를 사용하는 NetBus
윈도우 기반 트로이목마 공격	스캔 공격 사실을 숨기기 위한 공격 기술 내트워크 구조 스캔

해킹명	취약점 및 해킹 기법 요약
스텔스스캐닝 공격	mscan에 비해 최신 정보보호 취약점 점검 항목 추가 공격 스크립트를 수행가능
sscan공격	mscan에 비해 최신 정보보호 취약점 점검 항목 추가 공격 스크립트를 수행 가능
트로이목마 공격	ie0119.exe, tcp wrapper, utkl-linux 등
FTP 버퍼오버플로우	wu-ftpd 포함 FTP 서버에 버퍼오버플로우 취약점 원격지에서 관리자 권한 획득 가능
멜리사 매크로 바이러스 공격	마이크로소프트 워드 프로그램에 감염 전자메일을 이용하여 전파 문서 유출 및 네트워크 트래픽 폭주 가능

3.2 인터넷 해킹과 대책

3.2.1 RPC 관련 정보보호 취약점에 대한 대책

최근 들어 국내뿐만 아니라 국외에서도 RPC 서비스의 취약점을 이용한 공격 빈도가 급격히 증가하고 있으며, 대부분의 경우 관리자의 권한을 획득하게 된다. rpc취약점 관련 공격은. 이 프로그램은 원격 클라이언트의 매개변수 크기를 체크하지 않아 버퍼오버플로우(Buffer Overflow)를 통해 루트 권한에서만 수행 가능한 임의의 명령어를 수행시킬 수 있다. 방지 대책으로는 패치를 설치하거나 statd프로그램이 동작하지 않게 한다. statd 프로그램을 정지하려면 lockd 프로그램을 off하고 재부팅 하면 된다.

○ SUN automountd

SUN 솔라리스 시스템의 automountd는 일반적으로 UDP나 TCP프로토콜을 통해서 패킷을 받아들일 수 없지만 rpc.statd가 포워딩 해주는 TLI프로토콜을 통해서는 패킷을 받아들일 수 있다. 공격자는 이를 이용해 자신이 실행시키고자 하는 명령어를 rpc.statd에 패킷형태로 보내 실행시킬 수 있으며, 간단한 명령으로 공격 대상 원격 시스템의 rpc서비스 정보를 얻을 수 있고, rstatd 데몬의 실행 여부를 확인할 수 있다. rpc.statd과 automountd를 OS별로 각각 패치를 하여 막도록 한다..

○ rpc.ttdbserver

ttdbserver는 RPC기반의 ToolTalk 데이터베이스 서버 프로그램인데, 이 프로그램 구현상의 오류로 인해 원격의 침입자가 루트 권한으로 특정 명령어를 실행시킬 수 있다. 이 취약점은 SUN 솔라리스뿐만 아니라 HP, IRIX, AIX등 대부분의 시스템에서도 나타난다. /etc/inetd.conf 파일에서 해당 서비스를 코멘트 처리하여 서버를 실행시키지 않도록 하고 OS별로 패치를 설치한다.

○ SUN rpc.cmsd

rpc.cmsd프로그램은 데이터베이스 관리 프로그램으로 Open Windows의 Calendar Manager와 CDE의 Calendar 프로그램에서 사용한다. 침입자는 이 프로그램의 취약점을 이용 원격에서 임의의 파일을 쓰거나 루트 권한을 얻을 수 있다. OpenWindows와 CDE 패치를 설치하도록 한다.

○ AIX automountd

IBM AIX의 automountd 프로그램은 로컬 AutoFS 파일 시스템 커널의 요청을 처리하는데 수신된 요청이 실제 커널로부터 온 것인지를 검증하지 않아 로컬시스템의 일반 사용자 혹은 원격시스템의 사용자가 automountd 서비스를 요청할 수 있다. 이를 통해 침입자는 원격에서 루트권한으로 임의의 명령어를 실행시킬 수 있다.

○ IRIX autofsd

IRIX의 autofsd 프로그램은 RPC서버로 autofs파일 시스템의 mount, unmount요청을 처

사용하지 않는 서비스를 중지하고 알려진 버그를 패치 해 줌으로써 막을 수 있다.

○ rpc.statd

statd는 시스템 장애 시 NFS에서 파일 복구를 위해 제공하는 lockd 프로그램을 지원하는 도구로 클라이언트와 서버의 상태를 모니터링 하는 rpc프로그램이다 리하며, 지역 파일 또는 네임 서비스 맵을 이용하여 마운트 할 파일 시스템의 위치를 찾아낸다. 하지만 로컬의 일반 사용자가 autofsd에 조작된 요청을 보내어 루트 권한으로 임의의 명령을 실행시킬 수 있다.[4]

3.2.2 서비스 거부공격에 대한 대책

해커들이 즐겨 사용하는 Denial of Service의 유형을 종류별로 분류해보면 서비스 과부하 공격인 Service Overloading, 특정 message를 연속적으로 보냄으로써 시스템 자원을 고갈시키는 Message Flooding, 그리고 물리적으로 네트워크 선을 끊거나 전원을 뽑는 행위로 Signal Grounding이 있다.

전통적으로 위와 같은 형태의 Denial Of Service 가 즐겨 사용되었으나, 아래와 같이 최근 대두되고있는 Denial Of Service 형태의 공격 법들이 존재하니 서둘러 패치 하도록 해야 한다.

○ echo/chargen

흔히 UDP Storm 이라고 불리는 이 공격은 UDP 서비스 중 echo, chargen 서비스의 문제점을 이용해 시스템을 다운시키는 역할을 한다. 또한, 인터넷상에 이미 이 서비스들을 타겟으로 한 UDP Stormer 란 툴이 존재하므로, 시스템 내에서 제거하는 것이 바람직하다. 실제로 echo/chargen 서비스가 사용되는 경우가 거의 드물기 때문에 제거하더라도 큰 문제가 생기지는 않는다.

○ flooding/storming

어떤 시스템(클라이언트)이 서비스를 제공하는 시스템(서버)에 TCP 연결을 시도할 때, 클라이언트와 서버는 다음과 같이 일련의 메시지들을 교환한다. 먼저 클라이언트 시스템은 서버에 SYN 메시지를 보내며, 서버는 SYN-ACK 메시지를 클라이언트에 전송함으로써 접수된 SYN 메시지에 대해 확인한다. 클라이언트는 다시 ACK 메시지를 전송함으로써 접속 설정을 완료한다. 이렇게 함으로써 클라이언트와 서버 사이의 접속이 열리게 되고, 클라이언트와 서버 사이에 서비스에 고유한 자료들을 교환할 수 있게된다. 이러한 접속방법은 모든 TCP 연결(텔넷, 전자우편, 웹 등) 에 대해 적용된다.

공격의 가능성은 바로 서버가 클라이언트에 확인 메시지(ACK-SYN)를 보낸 후 클라이언트로부터 다시 확인 메시지(ACK)를 받기 이전의 시점에서 발생한다. 이 상태가 바로 "반만 열린" 연결이라고 불린다. 서버는 모든 진행중인 연결에 대한 정보를 저장하기 위해 시스템 메모리에 자료구조를 구축하며 이 자료구조는 그 크기가 제한되어 있다. 따라서 계속하여 "반 만 열린" 연결을 생성함으로써 이 자료구조를 넘치게 할 수 있다. 반만 열린 연결은 IP 속이기를 이용하면 손쉽게 생성할 수 있다. 공격자 시스템에서 피공격 서버에 적법하게 보이지만 실제로는 ACK-SYN에 대해 응답할 수 없는 클라이언트를 참조하는 SYN 메시지를 발송한다. 따라서 피공격 서버는 최종 SYN 메시지를 받을 수 없게 된다. 마침내 피공격 서버 측의 "반만 열린" 연결을 위한 자료 구조가 가득 차게 되고 이 자료구조가 비워 질 때까지 피공격 서버는 새로운 연결 요구에 대해 응답할 수 없게 된다. 일반적으로 반만 열린 연결에 대해서는 타임아웃 값이 설정되어 있어 일정 시간이 경과하면 자동적으로 취소되게 되므로 새로운 연결에 대해 응답할 수 있게 된다. 그러나 이와 같은 복구에 소요되는 시간보다 빠르게 공격자 시스템이 반복적으로 속임용 IP 패킷을 전송할 수 있다. 대부분의 경우, 이러한 공격의 피해 시스템은 새로운 네트워크 연결 요청을 받아들이는데 곤란을 겪게 되며 서비스제공 능력의 저하를 가져온다. 그러나 기존

의 외부로부터의 연결이나, 외부로의 새로운 접속 요청 전송에는 영향을 받지 않는다. 그러나 특별한 경우, 시스템의 메모리가 고갈되거나, 파괴되거나, 또는 작동 불가능하게 될 수도 있다.

SYN 패킷의 근원지 주소가 가짜이므로 공격의 근원을 알아내는 것은 어려우며 패킷이 피공격 서버에 도착한 뒤에 근원을 알아내는 것은 불가능하다. 네트워크는 패킷을 목적지 주소만을 이용하여 전달하므로 근원을 검증하는 유일한 방법은 입력 소스 필터링을 이용하는 것뿐이다. 현재의 IP 프로토콜 기술로는 IP 속임 패킷을 제거하는 것이 불가능하므로 현재로서는 이 문제에 대한 완전한 해결책이 없는 상태이다. 그러나 관리하고 있는 네트워크로 유입되거나 이로부터 유출되는 IP 속임 패킷을 감소시킬 수 있는 방법이 있다. 즉, 라우터를 적절히 구성함으로써 공격당할 가능성을 줄이거나, 해당 사이트내의 시스템이 공격의 근원이 될 수 있는 가능성을 감소시킬 수는 있다. 현재로서의 최상의 해결책은 외부 접속용 인터페이스로의 유입을 제한하는 필터링 라우터(입력 필터라고 부름)를 설치하여 근원이 내부 네크워크인 모든 패킷의 유입을 금지시키는 것이다. 이에 더하여 근원이 내부 네트워크가 아닌 모든 패킷의 유출을 금지시켜 관리하의 사이트로부터 IP 속임 공격이 발생되는 것을 방지할 수 있다. 그러나 이러한 방법도 외부 공격자가 다른 임의의 외부 주소를 이용하거나, 내부의 공격자가 내부의 주소를 이용하여 공격하는 것에 대해서는 방어하지 못한다.

○ mail bombing/SPAM mail

스팸 메일은 음란물, 피라미드, 무한이용권 등 불법 제품을 광고하는 내용이 대부분이다. 스팸 메일을 보내는 사람은 한 ISP에 개인 가입하여 스패밍한 뒤 해지하거나, 허위 주민등록번호와 허위 전화번호로 가입하여 사용하고, 또 타인의 비밀번호를 알아내어 몰래 이용하는 경우가 많다. 또는 제 2사이트의 인터넷 자원을 도용하여 스팸을 뿌리고, 악성 자동발송 소프트웨어를 이용하기도 한다. 스팸메일은 전자 우편의 편리함을 악용하는 대표적인 해악으로 메일 다운로드 비용이 수신자에게 전가되어 짜증과 항의를 유발하며 메일의 엄청난 폭주로 인하여 ISP의 정상적인 서비스를 방해하기도 하고 대부분 반송되어 뒷청소를 ISP에게 전가하게 된다. 허위 발신자 정보를 가지고 뿌려진 스팸메일은 본문의 신뢰성이 보장되지 않으며 사기 범죄에 이용될 가능성이 크다. 스팸 메일의 유형은 직접적 스팸(Incoming SPAM)과 중계 스팸(Relay SPAM)을 들 수 있다. 먼저 직접적 스팸은 나 또는 내 사이트로 쏟아져 들어오는 스팸으로 불건전 정보로 인한 피해가 상당하며, 원치 않는 트래픽 때문에 회선비용이 증가되고, 폭탄메일화 되면 서버가 다운되는 경우도 있다. 중계 스팸은 스패머가 내 메일 서버를 이용하여 제3자에게 스팸을 보내는 것으로 회선비용이 증가되고, 스팸 사이트라는 불명예를 얻게 되어 타 사이트가 내 사이트의 메일을 수신 거부하게 되는 경우도 있어 직접적 스팸보다 더욱 위험하다.

스팸의 차단을 위해서는 제3자의 중계(relay)를 기본적으로 불허하는 Sendmail 버전 8.9.x를 설치하도록 해야하며, sendmail.cf 파일도 8.9.x용으로 만들어야 한다. access_db는 발신자의 메일 주소 및 IP 주소를 기반으로 수신 또는 중계를 조절할 수 있으며, 기본적으로 제3자 중계는 금지이므로 내부 사이트의 호스트는 relay하도록 설정해야 한다. 또한 내부 불량 사용자에겐 메일을 전달하지 않는 blacklist_recipient 기능과 발신지의 IP 주소를 실시간 DB 조회하여 스팸 사이트이면 메일 수신을 거부하는 RBL(Realtime Blackhole List) 기능을 제공한다. 최근에 발표된 대부분의 메일 프로그램들은 스팸 메일을 필터링 하는 기능들이 추가되었으므로 최신판을 설치하도록 한다. 메일서버가 여러 대인 사이트에서는 메일 게이트웨이 서버를 이용하여 하나의 메일 서버로 메일을 집중한 후 다시 최종 메일 서버로 포워딩 시킬 수 있다. 이처럼 라우터의 Packet Filtering 기능을 이용하면 중앙 집중식 메일 서버 s/w 관리를 할 수 있으며 이메일 정보보호 버그의 구멍을 단일화

하여 효율성이 증대된다.[5]

3.2.3 스캔(Scan) 공격에 대한 대책

최근 정보시스템에 대한 대규모 네트워크 스캔 공격 사례가 늘어가고 있다. 네트워크 스캔 공격은 원격지에서 다수의 시스템에 대해 시스템의 정보보호 취약점을 스캐닝 하는 공격이다. 네트워크 스캔은 시스템으로의 침입을 위해 가장 먼저 수행하는 공격의 하나이며, 공격자는 정보보호 취약점이 발견될 경우 해당 취약점을 공격하여 시스템으로의 침입을 시도하게 된다. 네트워크 스캔 공격은 알려진 여러 개의 정보보호 취약점을 스캔하는 일반적인 네트워크 스캔 공격, 특정한 정보보호 취약점에 대해서만 스캐닝 하는 특정 취약점 스캔 공격, 스캐닝 사실을 숨기기 위한 스텔스(stealth) 스캔 공격, 네트워크 구조 스캔 공격 등이 있으며, 앞으로 하나하나 알아보도록 하겠다.

네트워크 스캔 공격은 ISS(Internet Security Scanner)와 SATAN(Security Analysis Tools for Audition Networks)이 인터넷을 통해 공개되면서 시작된다. 90년대 초기에 발표된 이들 네트워크 스캔 도구들은 네트워크의 정보보호 관리를 목적으로 개발된 공개 소프트웨어이다. 하지만 정보보호 관리를 위해 사용되기보다는 불법적인 시스템 침입을 노리는 악의적인 사용자에 의해 사용될 가능성이 높아 많은 논란을 일으켰다. 최근 네트워크 스캔 공격이 대단히 활발히 발생하고 있는데 이는 미국의 J. S. Bach라는 사람이 개발한 mscan('98년 6월 발표)과 sscan('99년 1월 발표)이라는 강력한 네트워크 스캔 도구 때문이다.

mscan은 98년 6월에 Jabach에 의해 개발된 네트워크 스캔 도구로 도메인 전체를 스캔하여 도메인 내에 있는 wingate, test-cgi, NFS exports, statd, named, ipopd, imapd 등 최근에 유행하는 주요 취약점을 한번에 스캔할 수 있는 해킹 도구이다.

99년 1월에 발표된 sscan은 지난 98년에 개발된 mscan에 비해 네트워크 정보보호 취약점 점검 기능이 매우 강력해졌으며, 취약점을 공격할 수 있는 해킹 스크립트를 수행하도록 설정할 수도 있다. mscan과 sscan의 점검항목을 비교하면 다음과 같다.

<표 2> mscan과 sscan의 점검항목

점검 항목		mscan	sscan
운영체제 버전 확인		○	○
네트워크 포트 스캐닝		○	○
QPOP root 버퍼 오버플로우		○	○
IMAP root 버퍼 오버플로우		○	○
Sendmail EXPN			○
solaris x86 listen/nlps_serv 원격 root 버퍼 오버플로우			○
리눅스 mSQL 2.0 원격 스택 오버플로우			○
리눅스 bind/iquery 버퍼 오버플로우			○
취약한 CGI 점검	/cgi-bin/phf	○	○
	/cgi-bin/Count.cgi		○
	/cgi-bin/test-cgi	○	○
	/cgi-bin/php.cgi		○
	/cgi-bin/handler	○	○
	/cgi-bin/webgais		○
	/cgi-bin/websendmail		○
	/cgi-bin/webdist.cgi		○
	/cgi-bin/faxsurvery		○
	/cgi-bin/htmlscript		○
	/cgi-bin/pfdisplay.cgi		○
	/cgi-bin/perl.exe		○
	/cgi-bin/wwwboard.pl		○
윈도우즈 시스템의 백오리피스 (31337 포트 점검)			○
NFS 취약점 - export 목록 - 모든 사용자에 읽기/쓰기 가능 여부		○	○

점검 항목	msc an	ssca n
리눅스 mountd 원격 버퍼 오버플로우		○
statd 버퍼 오버플로우	○	○
solaris NIS 서비스 (rpc.nisd) 원격 오버플로우		○
solaris nlockmgr 원격 오버플로우		○
X11 점검 - X 출력 화면 덤프, 스니핑 가능성	○	○
Wingate 동작 유무		○
FINGER 점검 - 사용자 확인(default : root, guest) - 한번도 로그인하지 않은 사용자 확인		○
스크립트 모듈 수행	○	○
named		
IRIX default 계정 유무		

특정 취약점 스캔 공격은 다수의 정보보호 취약점을 스캔하는 것과는 달리 공격하고자 하는 특정 취약점이 있는 시스템을 찾아내기 위하여 대규모 네트워크를 대상으로 스캔하는 공격이다. phf_scan, impd-scan, winscan 등이 있다.

일반적인 스캔 공격은 로그나 패킷 분석 등에 의해서 공격을 추적 당할 수 있지만, 스텔스 스캔 공격은 침입탐지 시스템이나 시스템 관리자에게 발견되지 않고 목표 사이트의 네트워크 구성 상태나 시스템 취약점 정보를 수집하는 기술이다. 이를 위해서 역 매핑(Inverse Mapping)" 과 느린 스캔(Slow Scan)" 기술이 사용된다.

네트워크 구조 스캔 공격은 특정 호스트에서 사용되고 있는 운영체제, 또는 네트워크 전체 구조에 대한 정보를 수집하기 위한 공격이다. 이들 정보는 시스템 공격을 용이하게 하고, 어떠한 취약점을 공격해야 할 지를 알려준다.

네트워크 스캐너들은 일정 시간동안 많은 포트들에 접속하여 서비스를 요구하는 특징이 있다. 스캔 공격을 탐지할 수 있는 방법은 로그 분석과 포트 모니터링이 있다. 첫 번째 방법인 로그분석은 시스템에 존재하는 각종 로그파일을 분석함으로써 해당 시스템에 대한 공격사실을 탐지하는 방법으로 시스템 관리자에 의해 수동으로 행하여지는 경우가 많다. 두 번째 방법인 포트 모니터링은 시스템에서 일정 단위 시간동안 일반적인 서비스 요구를 넘어서는 접속이 이루어지고 있는지를 감시하는 방법으로 침입탐지 시스템 및 기타 자동화된 도구에서 사용하는 기술이다. 이를 구현한 대표적인 스캔 탐지 전용 도구는 다음과 같다.

<표 3> 스캔 탐지 도구

Natas	임의의 5개의 포트를 선택하여 30초 안에 그들 중 2개의 포트가 연결되어지면 불법적 시스템 스캔으로 간주한다.

네트워크 해킹 취약점 스캔 공격에 대한 주기적인 탐지와 함께 라우터나 침입차단시스템에서 허용하고 있는 트래픽 이외에는 모든 트래픽을 차단하고, 정보보호 취약점 점검도구를 사용하여 자신의 네트워크 및 시스템에 대한 정보보호 취약점을 찾아내고 이를 패치 한다. 특히 필요하지 않은 네트워크 서비스는 즉시 중지하도록 한다.[3]

3.2.4 트로이 목마와 백도어에 대한 대책

비인가 된 사용자에 의한 불법 침입이 가능한 트로이 목마 버전의 TCP Wrapper, MS사에서 제공하는 유용한 패치 프로그램을 가장한 IE의 트로이목마 프로그램, 그리고 최신 버전의 루트킷(rootkit) 발표 등 최근 트로이 목마와 백도어 관련 사고가 증가하고 있다.

트로이 목마(trojan horse)는 정상적인 기능을 할 것처럼 보이나 실제로 다른 기능을 하는 프로그램을 말하고 백도어(backdoor)는 시스템에

비인가 된 접근을 가능하게 하는 프로그램을 말하는 것으로써, 트로이 목마가 시스템의 불법적인 침입을 위한 백도어로 사용되기도 한다.

전형적인 트로이 목마는 유용한 것으로 가장하여 사용자가 그 프로그램을 실행하도록 속인다. 사용자가 의심하지 않고 그 프로그램을 실행하게 되면 실제 기대했던 기능이 수행된다. 하지만 실제 목적은 사용자의 합법적인 권한을 사용하여 시스템의 방어 체제를 침해하고 공격자는 접근이 허락되지 않는 정보를 획득하는 것이다. 트로이 목마는 새로운 시스템 기능에 대한 정보를 보여주거나 새로운 게임이라고 하는 프로그램들에 숨어 있는 경우가 많다. 어떤 트로이 목마는 자기 존재의 흔적을 남기지 않아 발견될 염려가 없고, 의심받지 않는 소프트웨어에 숨어 있다. 또 발견되기 전에 스스로를 파괴하도록 프로그래밍 될 수도 있다.

도구명	설 명
Coutney	tcpdump로부터 하나의 시스템으로부터 일정 시간 범위 동안에 발생된 새로운 서비스들의 수를 입력으로 일정 시간동안 비정상적으로 많은 서비스 접속을 요청하면 그 시스템을 스캔 공격 호스트일 것이라고 간주한다.
Gabriel	네트워크 스캔 탐지도구로 고역 시스템을 찾아내어 이 사실을 삐삐, 전화, E-mail 또는 화면에 출력하여 시스템 관리자에게 알린다.

백도어는 시스템 설계자나 관리자에 의해 고의로 남겨진 시스템의 정보보호 허점으로 응용프로그램이나 운영체제에 삽입된 프로그램 코드이다. 즉 백도어는 시스템 접근에 대한 사용자 인증 등 정상적인 절차를 거치지 않고 응용 프로그램 또는 시스템에 접근할 수 있도록 한다. 이러한 정보보호 허점을 남겨두는 이유가 항상 악의적인 것은 아니다. 경우에 따라서는 현장 서비스 기술자나 시스템 공급자의 유지보수 프로그래머가 사용할 목적으로 특수 계정을 허용하는 코드를 운영체제나 응용프로그램에 넣을 수도 있다. 이러한 백도어는 디버깅 시 개발자에게 인증 및 셋업시간 등을 단축하기 위한 뒷문으로 사용된다. 하지만 이러한 백도어가 비양심적인 프로그래머가 비인가 된 접근을 시도하거나 개발이 완료된 후 삭제되지 않은 백도어가 다른 사용자에 의해 발견될 경우 대단히 위험할 수도 있다.

컴퓨터 시스템에 침입하려는 공격자들은 시스템에 비정상적인 방법으로 시스템에 접근하고자 백도어 기술을 개발하였다. 침입을 위한 백도어 프로그램들은 모든 패스워드들을 바꾸는 등 관리자가 안전하게 관리하려고 함에도 불구하고 시스템에 침입할 수 있으며, 발견되지 않고 시스템에 침입할 수 있다. 대부분의 백도어 프로그램은 로그를 남기지 않고, 온라인으로 들어왔음에도 불구하고 이를 발견할 수 없다. 그리고 시스템에 최단 시간에 침입할 수 있는 특징이 있다.

최근 유닉스 시스템뿐만 아니라 윈도우즈 시스템에서도 각종 트로이 목마가 등장하고 있어 주의를 요한다. 다음은 최근에 발견되고 있는 트로이 목마들이다.

○ 인터넷 익스플로러(IE)의 거짓 업그레이드

마이크로소프트사의 IE 웹브라우저를 무료로 업그레이드하라는 내용의 전자 우편이 광범위하게 배포되고 있다. 그러나 마이크로소프트사는 패치나 업그레이드를 전자우편을 통해서 제공하지 않고 전자우편을 통해서는 정보보호 게시(security bulletins)만을 한다고 발표했다. 메일 메시지에는 Ie0199.exe라는 실행 프로그램이 첨부되어 있다. 사용자가 무심코 첨부된 Ie0199.exe 프로그램을 설치하여 실행하게되면 그 프로그램은 몇몇 시스템 파일에 대한 수정과 다른 원격 시스템으로의 접속을 시도하는 행위를 한다.

○ 트로이 목마 버전의 TCP Wrappers

TCP Wrappers는 유닉스 시스템에서 네트워

크 서비스를 필터링하고 모니터링 할 수 있는 유용한 도구로써 시스템 정보보호를 위해서 광범위하게 사용되고 있다. 최근 공격자에 의해 소스가 변경되어 트로이 목마가 숨겨진 tcp-wrappers-7.6.tar.gz이 배포되고 있다. 이 트로이 목마는 1999년 1월 21일 이후, 몇몇 FTP 서버에서 발견되고 있다. 트로이 목마 버전의 TCP Wrapper는 소스 포트가 421번을 가지고 있는 접속이 시도될 경우 root로의 접근을 허락한다. 또한 이 트로이 목마 버전은 컴파일 도중에 사용자 계정과 시스템의 정보를 'whoami'와 'uname -a'를 이용하여 얻은 후 외부에 전자메일을 통해 발송한다. 이 트로이 목마 버전의 TCP Wrapper가 동작 중인 호스트에 공격자는 시스템 관리자 권한으로 불법 침입이 가능해 진다.

○ 트로이 목마 버전의 util-linux

util-linux는 리눅스 시스템을 위한 몇몇 기본적인 유틸리티를 포함하는 배포 판이다. 1999년 1월 22일에서 1월 24일 사이에 최소한 한 ftp 서버의 util-linux-2g.tar.gz 파일에 트로이 목마가 있다. 이 트로이 목마는 미러 FTP 사이트를 통해서도 배포될 수 있었다. 트로이 목마 버전의 util-linux에는 /bin/login이 수정되어 있다. 이 수정된 코드는 호스트 이름과 로그인한 사용자의 uid를 포함하는 내용을 전자우편을 통해 공격자에게 보낸다. 또한 어떤 사용자에게 명령을 실행시킬 수 있는 로그인 프롬프트를 제공해 주도록 수정되었다.

트로이 목마 프로그램은 시스템에 대한 재침입을 위한 백도어로 사용하기 위해 시스템에 설치하는 경우가 많다. 다음은 공격자에 의해 사용될 수 있는 넓은 의미의 백도어들을 소개하기로 한다.

○ 패스워드 크래킹 백도어

유닉스 시스템에 접속하기 위한 최초이며 고전적인 침입 방법으로 백도어들은 패스워드 크래커를 실행하여 취약한 패스워드를 가진 계정을 알아낸다. 이러한 계정들은 시스템에 침입하기 위한 백도어의 가능성을 내재하고 있다. 침입자들은 취약한 패스워드를 가진 사용하지 않는 계정들을 탐색하여 그 패스워드를 어려운 계정으로 바꾸어버린다. 시스템 관리자가 유추 가능한 취약한 패스워드를 찾아 사용을 금지시키려 해도 이미 이러한 계정을 찾을 수 없는 상태가 된다.

○ Rhosts + + 백도어

네트워크에 연결된 유닉스 시스템에서 사용의 편리성을 위해 rsh, rlogin 등의 서비스를 많이 사용하고 있다. 이 명령어들은 호스트 이름에 의해 인증이 이루어지고 추가적인 패스워드를 묻지 않는 정보보호 취약성을 내재하고 있다. 침입자는 어떤 사람의 rhosts 파일에 "+ +"를 넣어 어떤 호스트의 어떤 사용자라도 해당 사용자로 패스워드 없이 들어올 수 있도록 한다. 많은 침입자들은 NFS가 홈 디렉토리를 모든 호스트에 export하고 있을 경우에 이 방법을 많이 사용한다. 이 계정들은 시스템에 침입할 수 있는 백도어가 된다. 시스템 관리자가 rhosts 파일에서 "+ +"를 검사할 수 있으므로, 침입자는 여기에 자신이 해킹한 다른 계정을 등록함으로써 발견 가능성을 줄인다.

○ Checksum과 Timestamp 백도어

침입자들이 실행파일을 자신의 트로이 목마 버전으로 교체시키는 경우가 있다. 많은 시스템 관리자들은 타임 스탬프와 유닉스의 sum 프로그램 등과 같은 체크섬 값에 의해 실행파일의 변경유무를 진단한다. 하지만 침입자들의 기술도 발달되어 트로이 목마 프로그램의 타임 스탬프를 원래 파일의 타임 스탬프 값으로 생성시킬 수 있고, CRC 체크섬 값도 원래의 체크섬 값으로 가장할 수 있다. MD5 체크섬은 이러한 임의적인 가장이 불가능하므로 무결성 보장을 위한 도구로 권고되고 있다.

○ Login 백도어

유닉스 시스템에서 login 프로그램은 사용자가 텔넷을 통해 시스템에 접속할 경우 패스워드

인증을 수행한다. 침입자들은 login.c 프로그램을 수정하여 특정한 백도어 패스워드가 입력될 경우 관리자가 어떤 패스워드를 설정해 놓는지에 상관없이 로그인을 허용하고, utmp나 wtmp와 같은 로그파일에 기록도 하지 않도록 한다. 침입자는 침입한 흔적을 남기지 않고 시스템에 로그인하여 쉘을 획득할 수 있다. 시스템 관리자는 "strings"라는 명령어를 사용하여 login 실행 프로그램에 백도어 패스워드의 유무를 점검하기도 하지만, 침입자들은 백도어 패스워드를 암호화하여 저장함으로써 이러한 명령어에 의한 발견을 피할 수 있다. 가장 좋은 방법은 MD5 체크섬을 이용하여 이러한 백도어들을 탐지해 내는 것이다.

○ Telnetd 백도어

사용자가 시스템에 텔넷 접속을 할 때, inetd 서비스가 그 포트를 주시하고 있다가 in.telnetd에 연결시켜 주고, in.telnetd는 login 프로그램을 구동한다. 어떤 침입자는 시스템 관리자가 login 프로그램을 수시로 점검하기 때문에 아예 in.telnetd를 수정하는 경우도 있다. in.telnetd는 사용자들로부터 터미널 종류 등 몇 가지 사항을 점검한다. 일반적으로 터미널은 Xterm이나 VT100으로 설정되어 있다. 침입자는 터미널 종류가 "letmein" 등 특수하게 설정되어 있을 경우 인증과정 없이 쉘을 부여하도록 in.telnetd를 수정할 수 있다. 침입자는 어떤 서비스에 백도어를 설치하여 특정 소스 포트로부터 오는 연결에 대해서는 쉘을 부여하도록 할 수도 있다.

○ Services 백도어

대부분의 네트워크 서비스들 즉, finger, rsh, rexec, rlogin, ftp 심지어 inetd 등은 백도어 버전이 존재한다. 이 프로그램들은 uucp와 같이 전혀 사용되지 않는 서비스를 백도어 프로그램으로 교체하여 inetd.conf 파일에 등록하는 경우도 있다. 관리자는 시스템에서 어떤 서비스들이 제공되고 있는지 항상 점검하고, 원래 서비스가 수정되지 않았는지 MD5 체크섬에 의해서 진단해야 한다.

○ Cronjob 백도어

Cronjob은 유닉스 시스템에서 특정 프로그램을 특정 시간에 구동될 수 있도록 한다. 침입자는 백도어 쉘 프로그램을 cronjob에 추가하여 새벽 1시에서 2시 사이에 구동되도록 할 경우 이 시간동안 침입자는 시스템에 접속할 수 있다. 침입자는 cronjob에서 전형적으로 구동되는 합법적인 프로그램인 것처럼 가장한다.

○ Library 백도어

대부분의 유닉스 시스템에서는 공유 라이브러리를 사용한다. 공유 라이브러리는 같은 루틴들을 재 사용하여 프로그램의 크기를 줄이기 위해 사용한다. 어떤 침입자들은 crypt.c나 _crypt.c 프로그램 같은 루틴들에 백도어 프로그램을 넣어 두기도 한다. login.c는 crypt() 루틴을 사용하게 되는데 백도어 패스워드가 사용될 경우 바로 쉘을 부여하게 된다. 관리자가 login 프로그램의 MD5를 점검한다고 하더라도 백도어 코드를 찾을 수 없고 대다수의 관리자들이 백도어의 근원지를 찾아내기가 상당히 힘들다. library 백도어에 대한 대책은 MD5 체크섬 점검기를 정적으로 연결하여 시스템에서 구동하는 것이다. 정적으로 연결된 프로그램은 트로이 목마의 공유 라이브러리를 사용하지 않는다.

○ Kernel 백도어

kernel은 유닉스 시스템이 운용되는 핵심이다. 라이브러리에서 사용되었던 같은 방법으로 MD5 체크섬을 우회할 수 있다. 잘 만들어진 백도어가 설치된 커널은 관리자가 찾기 가장 어려운 백도어일 것이다. 다행히 커널 백도어 스크립트들은 널리 쓰이고 있지는 않지만 아무도 실제 얼마나 배포되어 쓰이고 있는지 모른다.

○ 파일 시스템 백도어

침입자는 서버로부터 획득한 전리품과 데이터들을 관리자에게 발각되지 않고 저장하고자 한

다. 침입자들이 저장하는 파일들은 일반적으로 해킹 스크립트의 도구박스, 백도어들, 스니퍼 로그들, 전자우편 메시지들과 같은 데이터, 소스코드 등이다. 침입자는 특정 디렉토리나 특정 파일을 숨기기 위해 "ls", "du" 그리고 "fsck"과 같은 시스템 명령어들을 수정한다. 그렇지 않으면, 숨기려는 부분을 "bad" 섹터로 보이게 하고, 침입자는 숨겨진 파일을 오직 특수한 도구를 통해서만 보이게 할 수도 있다.

○ Bootblock 백도어

일반 PC에서는 바이러스가 bootblock에 자신을 숨기고 대부분의 바이러스 백신은 bootblock이 바뀌어졌는지를 감시한다. 유닉스 시스템에서는 부트 블럭을 점검할 수 있는 소프트웨어가 거의 없어, 침입자들이 부트 블럭 공간에 백도어를 숨겨두기도 한다.

○ 프로세스 은닉 백도어(Process hiding backdoors)

침입자는 그들이 구동하고 있는 프로그램들을 숨기려고 한다. 그들이 숨기려고 하는 프로그램들은 일반적으로 패스워드 크래커, 스니퍼 프로그램 등이다. 프로세스를 숨기는 방법으로는 숨기려는 프로그램 자신의 argv[]를 수정하여 다른 프로세스 이름으로 보이도록 하거나, 스니퍼 프로그램을 in.syslog와 같은 합법적인 서비스로 이름을 바꿀 수 있다. 관리자가 "ps" 등으로 어떤 프로세스들이 구동되고 있는지 점검하면 정상적인 이름들이 나타나게 된다. 또 침입자는 라이브러리 루틴들을 수정하여 "ps"가 특정 프로세스를 보여주지 못하게 할 수 있다. 백도어 프로그램을 패치 하거나 인터럽트 driven 루틴들을 삽입하여 프로세스 테이블에 나타나지 않도록 할 수 있으며, 커널을 수정하여 특정 프로세스를 숨기도록 할 수도 있다.

○ 루트킷(Rootkit)

백도어를 설치하는 가장 인기 있는 패키지 중의 하나가 루트킷이다. 루트킷에 소개된 전형적인 백도어용 프로그램들은 다음과 같다.

- z2 - utmp, wtmp, lostlog로부터 특정 엔트리를 제거한다.
- Es - sun4 기반 커널들의 이더넷 스니퍼
- Fix - 체크섬 값을 가장하는 도구
- Sl - 매직 패스워드를 통하여 관리자로 로그인하는 도구

○ 네트워크 트래픽 백도어(Network traffic backdoors)

침입자들은 시스템에서 자신들의 흔적을 숨기려고 할 뿐더러 가능하면 자신들의 네트워크 트래픽까지 숨기기를 원한다. 이러한 네트워크 트래픽 백도어들은 간혹 침입차단시스템(firewall)을 거쳐서 침입할 수 있는 것들도 있다. 많은 네트워크 백도어들은 일반적으로 사용하지 않는 네트워크 포트를 사용하여 시스템에 침입하므로 관리자들이 침입자의 트래픽을 간과하기 쉽다.

○ TCP 쉘 백도어

침입자는 침입차단시스템이 막지 않는 높은 TCP 포트에 TCP 쉘 백도어들을 설치할 수 있다. 관리자들은 netstat를 통해서 어느 포트들이 연결을 기다리고 있고, 어느 포트가 연결되어 있는지를 점검할 수 있다. 이러한 백도어들은 SMTP 포트 상에서 구동될 수도 있어, e-mail을 허용하는 침입차단 시스템을 통과할 수 있다.

○ UDP 쉘 백도어

관리자들이 TCP 연결에 대해서는 관리를 잘하고 이상한 행위를 알아차리기가 쉽지만, UDP 쉘 백도어는 유닉스 시스템에 접속한 상태를 netstat 등으로 알기가 쉽지 않다. 많은 침입차단시스템에서 DNS 서비스 등을 위해 UDP 패킷들을 허락하도록 설정되어 있어 침입자는 UDP 백도어를 설치하여 침입차단 시스템을 무사히 통과할 수 있다.

○ ICMP 쉘 백도어

Ping은 ICMP 패킷을 보내고 반음으로써 시

스템이 살아있는지 확인하는 가장 일반적인 방법이다. 많은 침입차단시스템들이 외부로부터 내부 시스템에 대한 ping을 허락한다. 침입자는 ping ICMP 패킷에 데이터를 추가하여 ping을 하고있는 시스템과 쉘을 제공받을 수 있도록 한다. 시스템 관리자는 다량의 ping 패킷들을 발견하겠지만 패킷 속의 데이터를 보지 않는 이상 침입 사실을 알 수 없다.

○ 암호화된 링크

관리자가 스니퍼를 설치하여 쉘에 접근하려는 사람을 찾으려고 할 수 있다. 하지만 침입자는 네트워크 트래픽 백도어를 암호화하여 실제 두 시스템간에 어떤 데이터가 전송되고 있는지를 숨긴다.

○ Windows NT

Windows NT는 유닉스 시스템처럼 단일 시스템에 다수 사용자들을 접속하도록 허락하지 않는다. 이는 침입자가 Windows NT 시스템에 침입하여 백도어를 설치하고 시스템을 공격하는 것을 어렵게 한다. 하지만 Windows NT가 다수 사용자 기술이 발달됨에 따라 Windows NT 시스템에 대한 공격 사례가 늘어나고 있다. 요즘 Windows NT를 위한 telnet 데몬이 이미 나와 있고, 네트워크 트래픽 백도어를 Windows NT 시스템에 설치하는 것이 쉬워졌다.

트로이 목마와 백도어에 대한 대책으로 주기적인 무결성 점검이 필수적이다. 무결성 점검과 함께 다음과 같은 대응책을 강구할 수 있다.

첫째, 정보보호 취약점을 점검하여 제거한다. 네트워크가 얼마나 취약한지를 점검하여 정정하여야 하는 정보보호 허점들이 어떤 것들이 있는지 찾아낸다. 네트워크와 시스템의 취약성을 스캐닝 하는 것을 도와주는 많은 상업용 및 공개 도구들이 있다. 시스템 제공업체에서 무료로 보급하고 있는 정보보호 패치를 설치하는 것만으로도 시스템의 정보보호를 상당히 향상시킬 수 있다.

둘째, 침입탐지(Intrusion detection)를 한다. 침입탐지는 시스템에 대한 접속을 통제하는 것과 마찬가지로 중요하다. 예전의 대부분의 침입탐지 기술들은 로그를 기반으로 하였지만 최근의 침입탐지 기술은 실시간 스니핑과 네트워크 트래픽 정보보호 분석에 기반으로 하고 있다. 많은 네트워크 트래픽 백도어들은 이제 쉽게 탐지되어진다. 최근의 침입탐지 시스템 기술은 DNS UDP 패킷을 조사해서 DNS 프로토콜의 요청에 일치하는지를 판별한다. 만약 DNS 포트의 데이터가 DNS 프로토콜과 일치하지 않는다면 주의 경보를 알리고 데이터를 가로채서 좀더 면밀히 분석한다. ICMP 패킷의 데이터도 똑같이 적용되어 실제 정상적인 ping 데이터인지 아니면 암호화된 쉘 세션을 가지고 있는지를 조사하게 된다.

셋째, CD-ROM으로부터의 부팅을 수행한다. 관리자들은 침입자가 설치한 백도어의 가능성을 줄이기 위해 CD-ROM으로부터 부팅하는 것을 고려할 수 있다. 하지만 이 방법은 전체 기업에 대해 적용하기에는 시간과 비용이 많이 든다는 단점이 있다.

마지막으로 새로운 취약성들이 매일 보고되고 있고, 침입자들이 새로운 공격기술과 백도어 기술을 만들어 가고 있기 때문에 어떠한 정보보호 기술도 항상 신경을 쓰지 않고는 효과적이지 못하다는 것을 명심하여야 한다. [6]

3.2.5 버퍼오버플로우 취약점에 대한 대책

popd/imapd, bind, mountd 등 버퍼 오버플로우 취약점을 이용하여 관리자(root) 권한을 빼앗는 경우가 많은데 이들을 살펴보도록 하겠다.

POP서버는 PC 등 클라이언트에서 메일서버에 접속하여 메일을 송·수신하도록 하는 서비스를 제공한다. 사용자가 유닉스 시스템의 POP 서버를 접속할 때 사용자 아이디와 패스워드를 입력하게 되고 이러한 인증절차를 거쳐서 사용자는 유닉스 시스템에 저장된 자신의 메일을 확인할 수 있게 된다. POP 서버가 사용자 확인을 위하여 아이디와 패스워드를 입력받을 때 그 길이에 대한 한계 값에 대한 검사를 충분히 하지

않아 조작된 값을 입력함으로써 원격에서 관리자 권한으로 명령을 수행시킬 수 있다.

현재 많이 사용되고 있는 POP서버 프로그램은 qpopper인데, qpopper 2.5 이전 버전에는 사용자를 인증하는 과정에서 버퍼오버플로우 취약점이 존재하여 최신버전으로의 신속한 업그레이드가 필요하며, 라우터와 시스템 레벨에서 TCPWRAPPER와 같은 프로그램을 사용하여 접근제어를 적용하여 외부 네트워크에서 POP 서버에 접근하는 것을 막아야 한다.[7]

IMAP 서버는 리눅스 운영체제를 설치할 때 기본적으로 설치되는 것으로 사용자의 메일을 서버 쪽에서 관리하도록 해주는 프로그램이다. 보통 일반 사용자들은 POP서버를 사용하며 IMAP 서버는 관리자가 인지하지 못하는 사이에 데몬으로 동작하고 있는 경우가 많다. IMAP 서버의 버퍼오버플로우 취약점을 이용한 해킹프로그램이 인터넷상에 널리 퍼져 있으므로 이 프로그램의 사용에 주의가 필요하다. IMAP 서버도 POP 서버와 마찬가지로 사용자 확인을 위하여 아이디와 패스워드를 입력받을 때 그 길이에 대한 한계 값에 대한 검사를 충분히 하지 않아 조작된 값을 입력함으로써 공격자는 원격에서 관리자 권한으로 명령을 수행시킬 수 있다. IMAP4rev1 v10.234 이전 버전의 IMAP 서버에 버퍼오버플로우 취약점이 존재하며, 신속한 업그레이드가 필요하다. IMAP 서버를 사용하지 않는다면 /etc/inetd.conf 파일에서 imap 부분을 주석 처리하여 데몬의 실행을 막도록 한다.[8]

BIND 4.9.7과 BIND 8.1.2 이전 버전에서 역쿼리(inverse query) 요청에 대한 응답 시 적절한 한계값 검사를 하지 않아 버퍼 오버플로우 취약점이 존재하는 경우가 있다. 이때 공격자는 교묘히 조작한 패킷을 전송해 루트 권한을 임의의 명령으로 실행시킬 수 있는데, 이 공격은 역쿼리 기능을 제거하거나 새로운 버전을 설치해 방지할 수 있다.

NFS는 네트워크를 통해 컴퓨터간에 파일 시스템을 공유하기 위한 C/S 프로그램으로, NFS 클라이언트가 NFS 서버의 파일에 접근하기 위해서는 먼저 파일 시스템을 마운트 한다는 요청을 한다. 이 때 NFS 마운트 요청을 처리하는 소프트웨어(mountd 프로그램)에 버퍼 오버플로우 취약점이 존재한다. 이런 경우 새로운 NFS 서버 패키지를 구해 설치하도록 한다.

4. 결 론

현재 국내외에서 크고 작은 해킹 사건들이 잇따라 보고되고 있다. 패스워드 크랙이나 스니퍼, 루트 권한 뺏기 등의 유닉스 서버에 대한 공격에서 벗어나 네트워크와 윈도우 시스템에 대한 서비스 거부 공격과 바이러스와 웜의 유포 등이 늘어나는 추세이다. 범죄 동기도 단순한 호기심을 넘어선 금전적 이익이나 사회 혼란을 야기할 수 있는 사이버 테러가 나타나고 있다. 특히 전자상거래의 도래로 정보보호 문제가 중요시되어 정보보호에 관한 연구가 활발하게 되었지만, 서비스 거부 공격이나 바이러스 등에 의한 피해는 막기 어려울 것이다.

이 논문은 인터넷상에서 증가하고 있는 해킹을 분석하고 그 대책을 제시하여 앞으로의 연구에 초석이 되고자 하였다. 마지막으로 해킹 수법이 더욱 고도화 될 것이므로 향후 계속적인 연구가 이어져야 할 것이다.

참고문헌

[1] 한국정보보호센터, 정보보호 총서, pp.341-342, 1996. 12

[2] 신훈, 임휘성, 임채호, 인터넷 해킹 수법의 이해 및 대책, 정보과학회지, 제 15권 제 4호, PP.30-31, 1997.

[3] 임채호, 최신 해킹기법 분석과 대응책, KISA, pp. 24-34, 1999.

[4] CERTCC-KR-TR-99-008, "RPC 관련 보안 취약점 및 대책", 1999.8

[5] 이성희, "스팸 메일 대책", '98 한국정보통신 망침해사고대응팀협의회 해킹방지 워크샵 발표자료, 1998
[6] CERTCC-KR-TR-99-006, "트로이 목마와 백도어 분석 보고서", 1999.5
[7] CERTCC-KR-TR-98-009, "IMAP 취약점 분석 보고서", 1998.8
[8] CERTCC-KR-TR-98-008, "POP 서버 취약점 분석 보고서", 1998.8

김 상 춘

1986년 한밭대학교 전자계산학과(공학사)
1989년 청주대학교 전자계산학과(공학석사)
1999년 충북대학교 전자계산학과(이학박사)
1983년 ~ 2001년 한국전자통신연구원 정보보호기술연구본부 선임기술원
2001년4월 ~ 현재 삼척대학교 정보통신공학과 교수