네트워크를 통한 시스템 침입에 대한 고찰

신원[†], 윤희영[‡],이경현[‡]
† 부경대학교 전자계산학과
‡ 부경대학교 전산정보학과
‡ 부경대학교 컴퓨터멀티미디어공학전공

A Study on Computer System Intrusion through Network

Weon Shin[†], Hee-Young Yoon[‡], Kyung-Hyune Rhee[‡]
† Department of Computer Science, PKNU
‡ Department of Computer and Information Science, PKNU
‡ Department of Computer and Multimedia Engineering, PKNU

요약

본 논문에서는 최근 인터넷을 통한 시스템 침입 시나리오를 살펴보고 그에 따른 침입 탐지 및 대처 방안을 분석한다. 이러한 대처방안은 최근 빈번한 해킹사고에 대한 효과적인 대책 수립에 사용될 수 있을 뿐만 아니라 추후 개발될 침입차단시스템 및 침입탐지시스템에 본 분석결과를 반영한다면 네트워크를 통한 시스템 침입 방어 및 보안에도 사용될 수 있을 것으로 판단된다.

1. 서론

컴퓨터 보급의 확대와 정보 통신 기술의 급격한 발달로 인하여 수많은 네트워크가 구성되고 있으며, 새로운 기술을 도입한 각종 서비스들이 등장하고 있다. 특히, 인터넷 기술을 기반으로 하는 Mail, FTP, Telnet, News Group, WWW(World Wide Web) 서비스를 위한 상용 및 공개 서버가 구축되고 있으며 이를 이용하기 위한 많은 클라이언트 시스템이 구성되고 있다. 최근 전자상거래 확산에 힘입어 상용 네트워크가 구성되고 있으며 정부·연구기관, 대학 등을 중심으로 인터넷 기술을 활용하여 업무, 교육, 연구에 적용하고 있다. 따라서 엄청난 양의 정보와 재화들이 인터넷을 통하여 교환되고 있는 실정이다.

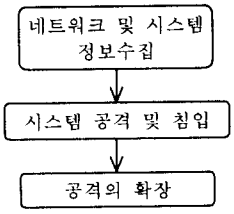
최근 이러한 인터넷을 통한 많은 위협 및 범죄가 등장하고 있으며 이를 통한 막대한 시간 및 경제적인 피해가 보고되고 있다. 얼마전 미국의 Yahoo나 CNN 등 유명한 전자상거래의 대표적인 사이트가 서비스 거부 공격(Denial of Service)을 당한 것은 네트워크를 통한 공격이 얼마나 심각한 정도에 다다랐는지 보여주는 단적인 예이다. 이제 많은 가상기업 및 인터넷관련 기관들이 자신의 정보와 시스템을 보호하기 위한 노력을 기울이고 있으며 네트워크 및 시스템 보안 문제에 많은 관심을 가지고 주목하고 있다. 그러나 이러한 노력에도 불구하고 현재 시스템의 취약점을 이용하는 공격용 프로그램들은 날로 복잡하고 정교해지고 있으며 새로운 공격 기법들이 속속 등장하고 있다. 따라서 이러한 공격에 대처하기 위한 새로운 방어 방법들이 개발되고 그 방법을 파훼하기 위한 발전된 공격방법이 역시 개발되고 있는 실정이다.

본 논문에서는 날로 정교해지는 네트워크를 통한 시스템 침입 시나리오를 설정하고 모든 시스템 공격 기법의 시작이 되는 정보수집단계에서의 여러 방법을 살펴본 후 이를 이용하여 시스템 공격을 방어할 수 있는 메커니즘을 살펴본다. 2장에서는 네트워크

를 통한 시스템 침입 단계에 대해서 논하고, 3장에서는 네트워크 및 시스템 정보수집 과정을 중심으로 시스템 침입 및 방어 방법을 살펴본다. 마지막으로 4장에서는 결론을 유도하고 향후 연구과제에 대하여 기술한다.

2. 네트워크를 통한 시스템 침입 시나리오

<그림 1>은 일반적인 시스템 공격 단계를 보여주는데 대부분의 시스템 공격 절차는 이와 같이 이루어진다. 일반적인 네트워크를 통한 시스템 공격은 그 방법 및 절차가 잘 알려져 있으므로 취약점을 보완하고 시스템을 보호하기 위한 많은 방법과 메커니즘이 나와 있는 상태이다. 먼저 "정보수집" 단계에서 공격 목표로 설정한 시스템에 대한 정보를 수집하고 이를 이용하여 "시스템 공격 및 침입" 단계에서 공격 및 침입을 감행한다. 성공하면 "공격의 확장" 단계에서 백도어(Backdoor)를 심어두어 다시 침투가 용이하도록 하고 또 다른 시스템을 공격하기 위한 교두보를 확보한다. 각 단계를 세부적으로 살펴보면 다음과 같다.



<그림 1> 시스템 공격단계

(1) 네트워크 및 시스템 정보수집

가장 먼저 수행하는 작업으로 공격 및 침입을 위한 네트워크와 시스템을 파악하기 위한 정보 수집을 하는 단계이다. 주로 네트워크 구성, 운영체제, 사용 포트 정보, 관리자 및 사용자 정보, 공유자원 정보 등을 수집하고 취약점을 분석한다.

(2) 시스템 공격 및 침입

앞 단계에서 수집한 정보를 기반으로 시스템의 침입을 감행하는데 시스템의 가장 취약한 단계를 중심으로 수행되며 이를 위한 수많은 방법들이 동원된다. 시스템 및 네트워크 서비스 상의 버그, 네트워크 도청, 시스템 환경 구성상의 오류 등을 이용하여 침입한다.

(3) 공격의 확장

시스템 공격 및 침입 이후 일어나는 공격을 말하는데 이미 공격이후 필요한 정보를 얻은 후 추가적인 정보를 얻기 위해 침입의 흔적을 지우거나 백도어를 숨겨두어 다음의 침입을 용이하게 하고, 다른 시스템을 공격하기 위해 준비하는 단계이다. 이미 확보한 시스템을 기반으로 신뢰관계를 이용한 다른 시스템 공격, 각종 네트워크 트래픽의 감시 및 도청 등을 통하여 다른 시스템을 공격한다.

일반적인 시스템 공격 단계는 대부분 앞의 3 단계로 이루어지나 외부 네트워크를 통하지 않은 내부 공격자인 경우나 트로이 목마(Trojan Horse)를 이용하여 공격하는 경우는 하위 2단계만으로 이루어질 수도 있다. 또한 공격 기술의 발달로 인하여 앞의 3 단계로 설명할 수 없는 공격도 등장하고 있으며 날로 지능화되고 다양화되는 여러 공격 기술들에 방어하기 위한 구체적이고 체계적인 연구가 필수적이다.

오늘날 네트워크 기술의 발전과 정보보호 개념의 정립으로 인하여 침입차단시스템(Firewall) 및 침입탐지시스템(Intrusion Detection System)이 보급되어 다양한 공격에 대응하는 기술이 보편화되고 있다. 그러나 이에 대응하여 공격 방법도 일반적인 단계를 벗어나는 경우도 많으며 특정 대상뿐만 아니라 불특정 다수를 공격 목표로 하는 새로운 방식도 등장하고 있다. 얼마전 소개되었던 "Cult of the Dead Cow"의 Back Orifice[10]는 트로이 목마의 한 형태로 단순한 파일 다운로드, 인터넷 메일 등을 통하여 불특정 다수에게 배포 후 시스템 권한을 획득하는, 보안 개념이 희박한 일반인을 이용한 기존 관념의 틀을 깨는 새로운 방식이다. 현재는 서버에 많이 사용하는 UNIX 시스템 기반의 공격 방법들이 일반인이 많이 사용하는 Windows 계열의 클라이언트로 확산되었으며, 이를 기반으로 하여 서버로 우회 침투하는 방법이 도입되고 있다. 또한 특정 목표 시스템을 공격하여 정보를 빼내는 고전적인 방법에서 정상적인 서비스를 못하도록 인터넷 사이트를 목표로 하는 "서비스 거부 공격"도 우려의 대상이 되고 있다. 그러나 현실적으로 이러한 공격을 완전히 막는 것은 불가능하며 앞으로도 이를 응용한 고도의 공격 방법들이 등장할 것으로 예상된다.

CERTCC-KR[9]에서 분석한 보고서에 의하면 최근 3년 간 매년 300%의 증가율로 해킹사고가 접수·보고 되고 있으며, 1999년 통계자료에서 사용자 도용(68건), S/W 보안오류 이용(3건), 버퍼오버플로(Buffer Overflow) 취약점(214건), 구성·설정 오류(2건), 악성 프로그램 (58건), 서비스거부공격(16건), E-mai 관련 공격(20건), 취약점 정보수집(272건), 사회공학(4건)이 보고되었다. 1999년이 주로 공격 대상이 대학(ac.kr)이었는데 반해, 2000년 1~3월에는 기업(co.kr)으로 전이되고 있으며 취약점 정보수집이 큰 비율로 증가하여 전체 57.64%(215/373)를 차지하고 있다. <표 1>은 이미 보고된 CERTCC-KR의 통계자료를 보여주고 있다. 그러나 보고되지 않은 피

해까지 생각한다면 그 규모는 훨씬 더 클 것이라 예상된다.

<표 1> CERTCC-KR 2000년 통계자료

공격기법	1월	2월	3월	합계
사용자 도용	4	1	4	9
S/W 보안오류 이용	1	0	0	1
버퍼오버플로 취약점	24	24	17	65
구성·설정 오류	1	0	0	1
악성 프로그램	12	26	26	64
프로토콜 취약점	0	0	0	0
서비스 거부 공격	4	4	2	10
E-mail 관련 공격	2	3	3	8
취약점 정보수집	74	61	80	215
사회 공학	0	0	0	0
합 계	122	119	132	373

3. 시스템 침입과 방어 방법

2장의 <표 1>에서 설명한 바와 같이 최근 국내의 시스템 공격 현황은 취약점 정보 수집이 많은 부분을 차지하고 있으며, 이렇게 정보를 수집한 후 목적 시스템을 결정하고 버퍼오버플로 취약점을 이용한 실제 공격 및 서비스 거부 공격을 하는 경향으로 분석할 수 있다. 그 외의 부분을 차지하는 사용자 도용, 악성 프로그램, E-mail 관련 공격 방식 등은 내부 공격자나 트로이 목마를 이용한 공격에 해당된다 할 수 있다. 따라서, 시스템에 불법적인 침입을 하기 위한 사전 준비단계로써 공격 가능한 보안취약점을 찾기 위한 "네트워크 및 시스템 정보수집" 단계에서 침입을 감지하고 방어할 수 있다면 70~80%에 해당하는 공격을 사전에 차단할 수 있다는 예측이 나온다.

본 논문에서는 "네트워크 및 시스템 정보수집"단계를 중심으로 하여 침입을 탐지할 수 있는 방법을 논의한다. 먼저 공격자 입장에서 수행하는 작업은 다시 3단계로 나눌 수 있는데, "목적지 정보 수집", "네트워크 스캐닝", "공격 목표 검색"이다. 각각을 세부적으로 알아보면 다음과 같다.

3.1 네트워크 및 시스템 정보수집 단계

(1) 목적지 정보 수집

일종의 예비조사 단계로 공격 대상을 찾는 과정이다. 방대한 네트워크 중에서 범위를 좁히기 위해 다양한 도구를 통하여 네트워크 구성, IP 주소 범위, 관리자 정보, DNS 정보 등을 수집하여 공격을 목표로 하는 네트워크를 선정한다. 단순한 whois, traceroute, nslookup, host 등의 명령어가 사용될 수 있고 더 향상된 기법으로 MX(Mail Exchange) Record 처리 장소 검색, Zone transfer를 위한 axfr[5] 도구를 사용할 수 있다.

(2) 네트워크 스캐닝

네트워크를 조사하는 단계로 시스템의 취약점을 찾기 위해 가장 빈번하게 이루어지며, <표 1>의 취약점 정보수집 부분이 여기에 해당된다. 단순히 ping 뿌리기, ICMP(Internet Control Message Protocol) 질의만을 이용해도 서비스를 수행하기 위해 Listening 상태에 있는 포트 스캐닝이 가능하며, 나아가 침입차단시스템의 필터링 규칙을 파악하고, IP 스택 구현을 구분하여 사용 서버의 운영체제 구분도 가능하다. 이를 이용하여 침입차단시스템을 우회하고 운영체제의 알려진 취약점을 파악하여 공격할 대상을 구체화한다. 사용되는 도구로는 ping, icmpquery[16], strobe[6], netcat[1], queso[7] 등이 있으며 nmap[12], sscan[8]은 강력한 도구로써 다양한 기능을 이용하여 탐지되지 않고 스캐닝하는 기술을 제공하고 있다.

(3) 공격 목표 검색

스캐닝을 통하여 수집된 정보를 기초로 하여 유효한 사용자 이름, 공유자원에 대한 취약성을 살피는 과정이다. 프로토콜 및 구현상의 취약성을 이용하는데, 단순히 rpcinfo, finger 등의 명령어를 이용하는 것이 가능하고 netcat[1], NetBIOS scanner를 통하여 사용자 그룹, 네트워크 환경 설정, "password" 파일 등을 얻을 수 있다.

3.2 각 과정의 방어 방법

사실상 "목적지 정보 수집" 과정은 인터넷 자체가 개방성을 기반으로 수많은 정보를 공유하는 형태를 취하므로 현실적으로 막을 방법이 존재하지 않는다. 하지만 이러한 행동을 방해하는 패킷 필터 라우터, 부분적으로 탐지하는 tdect[3]가 공개되어 있으며, traceroute에 대한 엉터리 응답을 유도하는 간단한 유틸리티 RotoRouter[2]도 나와있다.

"네트워크 스캐닝" 과정에서는 필수적으로 사용되지 않는 서비스는 사용하지 않도록 설정하고 잘못된 시스템 구성이 없는지를 검사하는 것이 최선의 방법이다. ICMP는 인터넷 표준에 18가지가 정의되어 있지만 실제 사용하는 것은 3가지(ICMP ECHO REPLAY, HOST UNREACHABLE, TIME EXCEED)이므로 최소한의 ICMP 패킷만 네트워크에서 허용하도록 설정한다. ICMP를 이용한 스캐닝은 pingd[11]라는 사용자 데몬을 이용하여 탐지가 가능하다. 또한 각종 TCP나 UDP를 이용하여 포트 스캐닝을 이용하는 경우 이러한 공격에 대한 패턴을 탐지하고 로그를 기록하는 도구로 scanlogd[4], Portsentry[15], BlackICE[14]가 있으며, 이를 막기 위해서는 불필요한 서비스는 사용하지 않도록 UNIX에서는 "/etc/inetd.conf", Windows NT에서는 "Service" 환경을 설정한다. 운영체제를 식별하기 위한 스캐닝은 운영체제의 소스코드로써 IP 구현을 변

경하는 방법이 있으나 현실적으로 불가능하고 견고하고 안전한 프락시(Proxy)나 침입차단시스템을 이용하는 것이 현실적이다. 이를 완전히 차단하는 것은 어렵지만 스캐닝 도구들이 생성하는 패턴을 탐지하여 데이터베이스화하여 로그에 기록하는 방법이 가능하다. 그리고, 최근에는 대부분의 스캐닝 도구가 자동화되는 경향을 띠므로 이를 탐지하는 도구도 역시 자동화되어야만 이에 대응할 수 있다.

"공격 목표 검색"과정에서는 각 사용자 계정과 불필요하게 공유되어 있는 시스템 자원이 공격 대상이 되므로, 관리자는 이를 주의깊게 감시하고 사용자는 충분한 교육을 통하여 남용하는 일이 없도록 해야한다. SNMP(Simple Network Management Protocol), TFTP(Trivial File Transfer Protocol) 서비스는 반드시 필요한 경우가 아니면 설정하지 않도록 하고 finger, rpcbind 명령어는 사용하지 못하도록 하고 sendmail은 항상 최신의 버전을 유지한다. 시스템 자원 공유를 위한 NFS(Network File System), NIS(Network Information System), NetBIOS의 환경설정의 오류는 시스템을 취약하게 하므로 문제를 확인하고, 사용자 및 그룹 관리도 중요하다.

<표 2>는 각 과정에 따른 공격방법과 방어도구를 요약하여 보여준다.

<표 2> 정보수집 단계에서의 공격방법과 방어방법

과정	공격방법	방어방법 및 도구
목적지 정보 수집	네트워크 구성 IP 주소 범위 관리자 정보 DNS 정보	패킷필터라우터 tdect RotoRouter
네트워크 스캐닝	Ping Sweep ICMP Query IP Stack 분석	pingd scanlogd Portsentry
공격목표 검색	유효한 사용자 이름 공유자원에 대한 취약성	올바른 환경설정 사용자 및 그룹 관리

4. 결론 및 연구과제

본 논문에서는 최근 인터넷을 통하여 이루어지는 시스템 공격에 대한 시나리오를 구성하고 근본적으로 이러한 공격을 방지할 수 있는 방법을 논하였다. 수많은 시스템 공격 방법이 등장하고 이를 방어하기 위한 많은 메커니즘이 소개되고 있지만, 항상 새로운 공격 방법이 등장한 후 방어 방법은 과거에 있었던 알려진 공격 방법에 대해서만 대비가 가능하다. 이러한 현실에서 시스템 공격을 방어하기 위해서는 시스템 공격을 위한 정보 수집 단계에서 공격의 시도를 미리 감지하고 대비하여야 한다. 또한 최근의 공격은 서버뿐만 아니라 일반 사용자로 우회하여 공격하는 양상을 띠므로 일반인에 대한 보안 인식을 높이기 위한 교육이 절실하다.

오늘날 많은 국가들이 자국의 정보를 보호하기 위해 국가적 차원에서 해당기관을 구축하고 여러 국가들 사이에 공조체제를 띠는 움직임을 보이고 있다. 국내에서는 정보보호센터[13]가 중심이 되어 침해사고대응팀을 구성하여 시스템 공격 및 침입에 대한 대응과 처리를 전담하고 있으며, 많은 업체들이 정보보호 제품을 설계·제작하여 상품화하고 있다. 그러나 이러한 대응과 제품에 도입되는 각종 메커니즘은 과거의 공격 방식을 데이터베이스화하여 처리하고 있어 새로이 등장하는 수많은 공격법에 대해서는 속수무책이다. 따라서 시스템 침입 및 공격 방식에 대한 포괄적이고 체계적인 연구가 반드시 필요하며, 이것은 기 개발된 네트워크 환경, 운영체제, 서비스 위에서 구체적이고 세부적으로 이루어져야 한다.

본 논문은 시스템 공격을 위한 정보수집 단계에서 예방법에 대하여 논의하였다. 이를 보완한다면 시스템이 공격을 당한 후 탐지 방법, 공격자의 추적, 백도어의 검출 등에 대해서도 심도 깊게 논의되어야 하며 이를 기반으로 현재 시스템의 취약성, 공격 양상을 통하여 미래의 공격 기법을 예측하는 것도 필수적이다. 그리고 많은 보안관련 업체의 침입차단시스템 및 침입탐지시스템은 이러한 메커니즘을 기본으로 갖추어야 경쟁력이 있을 것으로 판단된다.

참 고 문 헌

[1] ftp://coast.cs.purdue.edu/pub/tools/unix/netcat/nc110.tgz
[2] ftp://coast.cs.purdue.edu/pub/tools/unix/trinux/netmon/rr-1.0.tgz
[3] ftp://ftp.deva.net/pub/sources/networking/ids/tdect-0.2.tar.gz
[4] ftp://ftp.technotronic.com/
[5] ftp://ftp.trinux.org/pub/trinux/tools/netmap/axfr-0.5.2.tar.gz
[6] ftp://ftp.win.or.jp/pub/network/misc/strobe-1.05.tar.gz
[7] http://www.apostols.org/projectz/
[8] http://www.cert.org/incident_notes/IN-99-01.html
[9] http://www.certcc.or.kr
[10] http://www.cultdeadcow.com/tools/
[11] http://www.enteract.com/~tqbf/goodies.html
[12] http://www.insecure.org/nmap
[13] http://www.kisa.or.kr
[14] http://www.networkice.com
[15] http://www.psionic.com/abacus/
[16] http://www.securityfocus.com