보안 취약점 점검 도구 연구 동향

김 윤 정*

◈ 목 차 ◈

1. 서 론

급격한 인터넷 사용인구의 증가와 아울러, 해킹 및 침해 사고에 대한 보고가 빈번히 일어나고 있다. 표 1은 우리나라 연도별 사이버 범죄의 발생 건수로, 그 수가 대단히 빠른 속도로 증가함을 보여준다. 이 중 해킹, 바이러스 관련 분야로 검거가 이루어진 건수만도 2002년 8,099건, 2003년 10,762 건이나 된다[1].

(표 1) 우리나라 사이버 범죄 발생 현황

연도	1997	1998	1999	2000	2001	2002
사이버 테러	5	18	23	452	10,638	14,159
일반사이버범죄	116	376	1,686	1,992	22,651	45,909
계	121	394	1.709	2,444	33,289	60.068

안전한 컴퓨팅 환경을 마련해주는 보안 시스템 중 대표적인 두 가지는, 침입탐지 시스템과 침입차단 시스템이다. 침입 차단 시스템은 침입을 미리 차단해주는 것으로 방화벽(firewall) 등의 제품을 말하고, 침입 탐지 시스템은 침입 발생시 이를 탐지하는 IDS (intrusion detection system) 등을 말한다. 국내에서도 이 2 가지 시스템의 중요성을 인지하여, 정보보호 진흥원에서 이들에 대한 평가인증 작업을 진행하고 있다[2,3,4,5].

이들 두 시스템 외에, 안전한 시스템 구성에 효율적으로 사용될 수 있는 한 가지는, 보안 취약점 점검 도구이다. 유닉스 계열의 서버에 대하여, 보안설정 사항을 안전하게 유지하는 것은 안전한 시스템을 만드는 최선의 방법인데, 보안 취약점 점검 도구란 바로, 이러한 기능을 수행해 주는 프로그램을 말한다[6].

본 고에서는 보안 취약점 점검 도구의 연구 동향에 대하여 기술하고자 한다. 이를 위하여, 먼저 2장에서는 시스템의 잘못된 설정에 기인하여 발생했던 인터넷 보안 침해 사례를 살펴보고, 이들 보안 사고를 막기 위해 사용될 수 있는 취약점 점검 기능을 살펴본다. 3장에서, 보안 취약점 점검 도구의 정의 및 일반적인 분류에 대하여 기술한다. 그리고, 다음으로 4장에서 일반적인 취약점 점검 도구의 구성 및 전반적 기능에 대하여 살펴보고, 5 장에서 국내외 취약점 점검 도구의 현황에 대하여 기술하며, 끝으로 결론을 맺는다.

2. 보안 위협 사고 사례 및 이의 방지 예

2.1 보안 위협 사고 사례 - 인터넷 웜 사건

1988년 발생한 "인터넷 웜" 사건은 짧은 시간 안에 인터넷을 마비시켜, 보안의 중요성을 인식시키는 계기가 된 사건이다 [7]. 이 사건에서, Robert T.

* 서울여자대학교 정보통신공학부 조교수

Morris는 3200 줄의 C 프로그램을 이용하여, BSD와 Sun OS가 동작하는 VAX 기계에 대하여 다음과 같은 침입을 수행하였다. 웜에 감염된 기계는 임의로 선정한 희생자 기계에 대하여 네트워크를 통한 연결을 수행하고, 희생자의 기계에서 본 쉘 (Bourne Shell)을 수행시키고 부트스트랩 프로그램 (99 줄의 C 프로그램)을 희생자 기계에 복사하고 컴파일 하여 실행시킨다. 부트스트랩 프로그램은 자신을 적재한 원래의 기계에 연결을 요청하여 실제 웜 기능을 하는 코드를 자신의 프로세스 이미지로 실행하도록 한다. 즉, 희생자의 기계도 감염이 된 것이다. 이제 희생자 기계는 또 다른 희생자를 찾아 작업을 계속해 나간다. 또한, 희생자 기계에서 패스워드를 유추하여 성공하는 경우 이를 침입에 이용하기도 한다.

이 때, 웜이 이용한 시스템의 취약점은 rsh, SMTP (Simple Mail Transfer Protocol), fingerd, 패스워드의 유추가능성 등이다. Rsh은 권한이 있는 사용자로 하여금 원격의 기계에서 임의의 명령어를 실행할 수 있도록 해 준다. 이 때, 권한은 /etc/hosts.equiv 파일이나, .rhost 파일의 설정에 의해 결정된다. 즉, 침입자가 이 두 가지 파일을 수정할 수 있다면, 임의의 기계로부터 오는 명령 수행 요구를 수행하게 된다. 다음으로, SMTP는 debug나 wizard 명령어가 지원되는 경우, 부트스트랩 파일을 다운로드 하여, 컴파일하고 실행할 수 있는 방안이 제공된다. 그리고 웜이 이용한 또 다른 프로그램인 fingerd 프로그램은 내부에서 gets() 시스템 콜을 사용하는데, gets()는 512 byte의 버퍼를 사용하면서, 버퍼크기 제한을 검사하지 않는다. 웜은 536 바이트가 gets()의 인자로 주어지도록 하면서, 버퍼를 오버플로우시켜, gets()를 호출한 함수로 복귀하지 않고 본 쉘을 실행하도록 한다. 마지막으로, 짧은 단어로 구성된 패스워드 또는 로그인 ID와 동일한 패스워드 등 유추 가능한 패스워드를 이용하는 사용자가 존재하는 경우 이를 찾아내어 침입에 이용하였다.

즉, 인터넷 웜 프로그램이 동작 가능했던 이유들은, rsh의 사용이 허가되어 있거나, SMTP가 debug나 wizard 명령어 모드를 갖고 있거나, gets() 시스템 콜을 이용하는 fingerd 프로그램이 사용 가능하거나, 유추 가능한 패스워드의 사용이 있었기 때문이었다. 따라서, rsh을 사용하지 않도록 하고, debug나 wizard 명령이 없는 SMTP를 사용하고, finger daemon이 수행되지 않도록 하고, 또 유추가능한 패스워드를 사용하지 않도록 했다면, 인터넷 마비라는 극단적 상황은 발생하지 않았을 것이다.

2.2. 보안 위협 사고 방지 예

버그가 있다고 발표된 경우에는 빨리 해당 명령어나 프로그램을 공격 위험성이 없는 것으로 대체해 주어야 한다. 보통 위험 요소가 내포된 프로그램이나 명령어가 발견되면, 미국 CERT (Computer Emergency Response Team: www.cert.org)나 국내 Concert (www.certcc.or.kr)에 통보되고, 위험 사실을 안 시스템 판매자들은 위험요소를 제거한 패치를 내어놓는다. 따라서, 패치가 내어 놓여질 때마다 이것으로 기존의 버그 있는 프로그램을 대체한다면 보안 상 위협은 그만큼 줄어들게 된다.

3. 보안취약점 점검도구의 정의 및 분류

유닉스 시스템은 현재 전 세계의 서버 시장을 장악하고 있는 막강한 운영체제이다. SUN 사의 SunOS와 Solaris, HP의 HP-UX, IBM의 AIX, NCR의 MP-RAS, 국산주전산기의 운영체제인 Unixware, 그리고 프리웨어로서 많은 인터넷 열광자들이 애용하고 있는 Linux 및 최근에 서버 시장에서 시장 점유율을 넓히고 있는 Microsoft의 NT 등이 모두 유닉스 계열의 운영체제이다.

이러한 유닉스 계열의 시스템들은, TCSEC (trusted computer system evaluation criteria) C 등급의 시스템들로[8], 이들을 사용하는 사용자 및 관리자들이 어떻게 시스템을 설정하느냐에 따라 시스템의 안전도가 달라지게 된다. 관리자가 일일이 보안 설정을 검사해야 하는 과정을 자동으로 수행함으로써, 서버나 네트워크 상의 잠재적 보안 위험요소를 자동으로 진단해 주어, 현재의 보안 상태에서 발생 가능한 문제점을 해결할 수 있도록 하는 것이 보안 취약점 점검 기능의 정의이자 목적이다.

보안 취약점 점검 도구는 크게 호스트 기반의 점검 도구와 네트워크 기반의 점검 도구로 나눌 수 있다. 호스트 기반의 취약점 점검 도구는 한 호스트 내에서 시스템 설정 정보 (네트워크 관련 사항 포함) 등을 검사해 보는 것으로, 시스템 관리자가 자신이 관리하는 서버들을 진단할 때, 수퍼 사용자 권한으로 강력한 점검을 행할 수 있다는 장점이 있다. 네트워크 기반의 취약점 점검 도구는 보안 점검 도구가 설치된 시스템 상에서 네트워크 접속을 통하여 네트워크에 연결된 여러 호스트들의 보안 상태를 점검해 준다. 이 경우, 보안 점검 도구가 설치되지 않은 호스트의 보안 사항도 점검할 수 있다는 장점은 있으나, 해당 호스트의 외부에서 보안 사항을 점검함으로써 내부 시스템 환경 설정 등의 관리 환경 오류로부터 발생 가능한 취약점은 발견하지 못한다는 단점을 갖는다.

(표 2) 보안 취약점 점검 도구 특성

	호스트 기반 보안 취약점 점검 도구	네트워크 기반 보안 취약점 점검 도구
기능	한 호스트 내에서 시스템 정보 검사 (네트워크 관련 사항 포함)	점검도구가 설치된 시스템에서 네트워크에 연결된 여러 시스템의 보안 사항 점검
장점	슈퍼 사용자 권한으로 강력한 점검 수행	점검도구가 설치되지 않은 호스트의 보안사항도 점검
단점	점검도구가 설치된 호스트의 보안 사항만 점검	내부시스템 환경 설정 오류로 인한 취약점은 발견 못함

4. 보안취약점 점검 도구의 기능

4.1 호스트 기반 보안 취약점 점검 기능

위에서 기술한, 패스워드 취약성 진단, rsh 관련 설정 파일 진단, 시스템 패치 프로그램 진단 등을 포함하여, 전반적인 보안 관련 취약 사항을 점검하는 것이 호스트 기반 보안 취약점 점검 도구의 주된 기능이다. 보안 취약점 점검 도구의 취약성 진단 영역은 크게, 사용자 패스워드 점검, 사용자 계정 관련 점검, 파일 시스템 구성 사항 점검, 수퍼사용자 관련 사항 점검, 시스템 명령어 변경 여부 점검, 로그인 기록 관련 점검, 예약실행 관련 점검, 시스템 패치 및 메일, 유틸리티 점검, 네트워크 설정 및 접근 가능성 점검, 웹 취약성 점검 등으로 나뉘어 진다. 이들이 표 3에 나타나 있다.

(표 3) 호스트 기반 보안 취약점 점검도구 점검항목

번호	점검항목
1	사용자 패스워드 점검
2	사용자 계정/환경 관련 점검
3	수퍼 사용자 관련 사항 점검
4	로그인 기록 관련 점검
5	예약 실행 관련 점검
6	지정파일/시스템명령어 변경 점검
7	시스템 패치 점검
8	시스템 메일 점검
9	시스템 유틸리티 점검
10	네트워크 설정 점검
11	네트워크 접근가능성 점검
12	웹 취약성 점검

이 중 사용자 패스워드 점검은 각 사용자의 패스워드에 대하여 로그인 ID와 동일한 패스워드, 단어사전의 단어와 동일한 패스워드, 로그인 ID에 특정 접두사가 붙은 패스워드, 로그인 ID에 특정 접미사가 붙은 패스워드, 타 사용자의 로그인 ID와 동일한 패스워드, 단어사전의 역순과 동일한 패스워드를 점검하며, 단어사전의 단어를 대문자로 바꾼 단어를 패스워드로 사용하는지, 단어사전의 단어를 소문자로 바꾼 단어를 패스워드로 사용하는지, 단어사전의 단어 중 이중단어와 같은 패스워드가 있는지 등의 점검을 수행한다. 사용자 계정 관련 점검은 사용자의 계정과 관련하여, 사용하는 사용자 ID 값 (UID)이 제대로 지정되어 있는지 (음수 값이면 안됨), 중복된 사용자 계정이 있는 것은 아닌지, 한 사용자가 여러 개의 그룹에 속한 것은 아닌지 등을 점검한다. 이 점검의 구현은 주로 /etc/passwd 파일 내용과 /etc/group 파일의 구성에 대하여 진행된다. 또한, 사용자마다 가지고 있는 환경 설정이 제대로 되어 있는지도 점검한다. 예를 들

어, 파일 생성시 파일의 읽기-쓰기 허가 모드를 설정하는 umask 값이 자신 이외의 사용자에게 쓰기 권한이 있는지 등을 조사한다. 수퍼사용자 관련 사항 점검은 수퍼 사용자 소유 파일의 설정이 올바른지 점검하고, 수퍼 사용자의 수행 환경이 일반 사용자는 접근할 수 없도록 안전하게 설정되어 있는지 점검한다. 로그인 기록 점검은 시스템에 오랫동안 로그인하지 않은 계정이나 로그인이 여러 번 실패한 계정 정보를 출력하며, 예약 실행 관련 점검은 예약 실행할 명령어가 위험한 것은 아닌지 등 예약실행과 관련한 at/cron 설정이 올바른지를 점검한다. 지정파일/시스템 명령어 변경 점검 기능은 미리 등록된 관리상 중요하다고 지정된 파일이나 시스템 명령어에 대하여, 읽기 쓰기 모드가 변경되었는지, 소유자가 변경되었는지 파일의 내용이 변경되었는지 등을 점검한다. 이것은 이들 파일들에 대한 정보를 미리 기록하였다가 점검 시마다 기록된 값과 현재 시스템에 있는 파일들의 값을 비교함으로써 수행되며, 침입 프로그램에 의하여 해당 파일들이 변경되었는지를 알아낼 수 있는 유용한 기법이다. 시스템 패치 점검은 시스템 판매자가 제공하는, 버그가 수정되었거나 기능 개선된 시스템 명령어들을 최신의 것으로 대체했는지를 조사하는 것으로, 버그가 내재된 명령어로 인한 침입을 막을 수 있는 유용한 것이다. 시스템 패치 점검 중 메일과 관련된 설정 등을 추가로 점검하는 기능이 시스템 메일 점검 기능이며, 시스템 패치 점검 중 특정 유틸리티에 대하여 조사하는 것이 시스템 유틸리티 점검이다. 네트워크 설정 점검은 anonymous ftp, tftp, nfs 등 네트워크 관련 설정이 제대로 되었는지를 점검하며, 네트워크 접근 가능성 점검은 시스템이 제공하는 네트워크 서비를 점검하여 보안상 취약한 네트워크 서비스나 알려지지 않은 네트워크 서비스가 되고 있는지를 점검한다. 웹 취약성 점검은 웹과 관련한 CGI의 설정 및 디렉토리, 프로그램의 안전성을 점검한다.

네트워크 기반의 보안 취약점 점검 도구는 네트워크 접속 상에서 발생하는 취약점을 점검하는데, NFS (network file system), NIS (network information system), sendmail 버전 관련, rexecd 수행 관련, tftp 수행 관련, 쓰기가능한 익명 FTP 홈디렉토리, 원격 쉘 수행, 접근제어 없는 X 서버 등을 점검한다.

4.2 보안취약점 점검 기능의 부가 기능

취약성 진단기능 이외에 보안 취약점 점검도구가 갖는 부가적인 기능으로는, 그래픽 인터페이스를 통한 편리한 사용성, 진단 기능의 예약을 통한 취약점 점검 도구 수행 시각 지정, 사용자가 원하는 형식으로 지원되는 다양한 보고서 기능 등을 들 수 있다.

호스트 기반 취약점 점검 도구는 보통 취약점 분석 모듈을 각각의 서버에 설치하고, 점검 결과를 관리자가 한 곳에서 받아 관리할 수 있도록 구현된다. 이 때 구동방안을, 도구 설치 서버들, 관리자 컴퓨터의 2 단 구조로 하느냐, 아니면 도구 설치 서버들, 점검 결과가 저장되는 중간지, 관리자 컴퓨터의 3 단 구조로 하느냐에 따라 구현 방식이 달라진다. 2 단 구조는 간단하다는 장점이 있고, 3단 구조는 다수의 관리자가 존재하는 경우, 관리자들이 점검 결과가 저장되는 중간지에 중복 접속하여 점검 결과를 공유함으로써 효율적이라는 장점이 있다.

5. 보안 취약점 점검 도구의 국내외 제품 현황

보안 취약점 점검 도구는 역사는 1991년 COPS (Computer Oracle and Password Systems)로 거슬러 올라간다[9]. CMU (Carnegi Mellon University) CERT (Computer Emergency Response Team)의 Dan Parmer와 Purdue 대학의 Eugene H. Spafford는 유닉스의 취약점을 자동으로 점검해 주고자 하는 목적으로 COPS를 개발 공개하였다. COPS는 호스트 기반 취약점 점검도구이다. 네트워크기반 취약점 점검 도구의 효시는, 역시 Dan Farmer와 Wietse Venema가 1995년 작성 공개 한 satan (security administration tool for analyzing networks)이다[10]. 국내에서는 1998년 한국정보보호진흥원에서 호스트기반 보안 취약점 점검 시스템인 SecuDr를 개발한 바 있으며, 이를 민간 업체에 위탁하여 상업용 버전을 출시토록 한 바 있다. 이 때 지정된 민간업체가 나일 소프트와 데이터게이트 인터내셔널로, 나일 소프트의

(표 5) 보안취약점 점검도구 국내외 제품 현황

분류	제품명	회사명	비고
호스트기반 취약점 점검도구	COPS	공개 SW	
	SecuGuard SSE	나일소프트	국산
	SecuScope	데이타게이트인터내셔널	국산
	Jindan Dosa	니츠	국산
	ESM	Symmantec	미국
	System Scanner	ISS	미국
네트워크기반 취약점 점검도구	SATAN	공개 SW	
	SecuGuard NSE	나일소프트	국산
	SecuiScan	시큐아이닷컴	국산
	Internet Scanner	ISS	미국
	NetRecon	Symmantec	미국

SecuGuard와 데이터게이트 인터내셔널의 Secuscope는 국내의 대표적 보안 취약점 점검 도구로 볼 수 있다. 이 외의 호스트 기반 보안 취약점 점검도구는 니츠의 Jindan Dosa, 외산제품으로 미국 Symmantec(구 Axent) 사의 ESM (Enterprise Security Management), ISS (Internet Security Systems) 사의 System Scanner 등이 있다. 네트워크 진단 시스템에는 국내 제품으로 NDS 사의 Cyberarmy, 시큐아이닷컴의 SecuiScan, 외산제품으로 Symmantec 사의 NetRecon, ISS 사의 Internet Scanner 등이 있다. 또한 영국 Network Associates 사의 Cybercop 등도 취약점 점검 도구 중 하나이다[11,12,13,14,15].

6. 결 론

이상에서 보안 취약점 점검 도구의 사용 목적 및 국내외 제품 현황에 대하여 살펴보았다. UNIX 및 NT 시스템은 TCSEC C 등급의 시스템으로 시스템을 안전하게 설정해 놓음으로써 보안상의 위협을 급감시킬 수 있다. 보안취약점 점검 도구는 취약점 점검을 자동으로 수행함으로써 관리자가 효율적으로 시스템을 안전한 상태로 유지시키는 데 기여할 수 있다.

참 고 문 헌

[1] 사이버 경찰청, http://www.police.go.kr, 2003.

[2] 한국정보보호진흥원, 정보보호평가 - 침입차단시스템, 침입탐지시스템, http://www.kisa.or.kr, 2002.

[3] 유동영, 침입탐지시스템 제품동향, 한국정보보호진흥원, 2001.

[4] 김명주, Easy Guide Security Expert, 영진닷컴, 2002.

[5] 한국정보보호센터, 정보보호개론, 교우사, 2002.

[6] 보안 취약점 분석 도구, 월간 정보보호21C 정보보호 지침서, 기업정보보호 실천 가이드, 2001.

[7] Donn Seeley, A Tour of the Worm, Department of Computer Science, University of Utah, 1989.

[8] DoD (Department of Defense), Trusted Computer System Evaluation Criteria (Orange Book),, 1985.

[9] Dan Farmer, Eugene Spafford, The cops security checker system, Proceedings of the Summer 1990 USENIX Conference, pp. 165-170, 1990.

[10] Dan Farmer, Wietse Venema, Satan (security administration tool for analyzing networks), satan-1.0.tar.gz 1995.

[11] 나일 소프트, SecuGuard SSE, http://www.nilesoft.co.kr, 2003.

[12] 데이터게이트인터내셔널, SecuScope, http://www.datagate.co.kr, 2003.

[13] 시큐아이다컴, SecuiScan, http://www.secui.com, 2003.

[14] Internet Security Systems, Internet Scanner, System Scanner, http://www.iss.net, 2003.

[15] 시만텍, Netrecon, http://www.symantec,com, 2003.

◐ 저 자 소 개 ◑

김 윤 정

1991년 서울대학교 컴퓨터학과 (공학사)
1993년 서울대학교 컴퓨터학과 (공학석사)
2000년 서울대학교 전기컴퓨터 공학부 (공학 박사)
2000~2001년 (주) 엔씨 커뮤니티 제품개발연구소 차장
2001~2002년 (주) 데이터 게이트인터네셔널 보안기술연구소 차장
2002년~현재 : 서울여자대학교 정보통신공학부 조교수