안전한 대학 전산망 운영을 위한 취약점 분석 시스템 설계 및 구현

정성용[0], 이재명, 황윤철, 이상호
충북대학교 전자계산학과
syjeng@trut.chungbuk.ac.kr, {dlwoaud, ychwang, shlee}@cnlab.chungbuk.ac.kr

Design and Implementation of Vulnerability Analysis System for Secure Campus Network Operations

Seong-Yuong Jeong[0], Jae-Myong Lee, Yoon-Cheol Hwang, Sang-Ho Lee
Dept. of computer science, chungbuk national Univ

요 약

오늘날 인터넷 기술의 급격한 성장과, 인터넷을 통한 조직과 개인의 사회적 활동의 증가에 따라 인터넷에 대한 우리들의 생활 의존도가 점차로 커지고 있으며 이에 따른 역작용으로 침해사고 및 정보의 유출, 파괴, 서비스방해, 위조, 변조 등의 컴퓨터범죄가 날로 증가하여 심각한 사회문제로 대두되고 있다. 사이버 공간에서 전산망을 보호하기 위해서 사용자 인증, 무결성 점검, 침입탐지, 파이어월 등 다양한 기술이 사용되고 있다. 하지만 가장 우선시 되어야 하는 것은 공격의 목표가 되는 시스템의 보안 취약점을 찾아내고 이를 제거하는 작업이라고 할 수 있다. 이 논문에서는 대학 전산망의 확대와 해킹기술은 급속히 발달하고 있지만 이에 비해 대학 전산망 보호를 위한 보안장비 및 관리자/사용자들의 보안지식 및 기술은 절대적으로 부족한 실정을 감안해서, 내부 사용자들이 자신의 취약점을 쉽게 점검 및 해결할 수 있고, 관리자들이 전산망의 취약점을 파악하는데 효과적인 시스템을 제안한다.

1. 서 론

오늘날 인터넷 기술의 급격한 성장과, 인터넷을 통한 조직과 개인의 사회적 활동의 증가에 따라 인터넷에 대한 우리들의 생활 의존도가 점차로 커지고 있으며 이에 따른 역작용으로 침해사고 및 정보의 유출, 파괴, 서비스방해, 위조, 변조 등의 컴퓨터범죄가 날로 증가하여 심각한 사회문제로 대두되고 있다.

현재 교육기관의 전산망 구축 사업은 5000여건 이상으로 97년 6월경에 시작해 2000년 12월을 기점으로 완료한 상황이며 신설 학교 등에 대한 사업이 개별적으로 계속되고 있는 실정이다. 또한 현재 서울 1000여 개교, 인천 220개교, 강원 300개교를 비롯해 경북, 대구, 부산, 울산, 경남 1700개교와 충남, 충북, 대전, 전북, 전남 1600여 개교 등이 학내 전산망 구축 대상으로 이들 중 상당수가 전산망구축이 완료되었고[1], 인터넷망에 연동되지 않은 학교도 지방교육청의 관할 하에 계속적으로 전산망 구축 중에 있다.

최근에는 앞에서 언급한 전산망 구축 증가함과 함께 초·중·고교 및 대학교에서 운영하는 인터넷 연동시스템에 대한 해킹사고가 증가하고 있다. 정보보호진흥원의 조사결과를 보면 지난 1999년 11월말부터 교육기관에서의 해킹사고가 증가해 1999년에는 22건, 2000년에는 47건, 2001년 7월까지 379 건으로 이는 지난 7월까지 총 1219건의 전체 해킹사고 중 12%에 해당하는 379건으로 2000년에 비해 6배나 증가한 수치이며 현재 추세대로라면 올해 말에는 600여건 이상에 이를 것으로 예측된다.[2]

교육 전산망의 급격히 해킹사고가 증가한 원인은 교육정보화사업의 일환으로 교육기간의 전산망을 인터넷으로 연동시키는 과정에서 학내 정보시스템의 인터넷 연동에 따른 사용자들의 보안 관리 대책이 허술했고, 학내정보시스템을 위탁·운영하고 있는 업체의 보안관리 소홀을 원인으로 찾을 수 있다. 따라서 학내전산망의 광범위한 구축과 상대적으로 열악한 보안체계로 인해 교육기관과 관련된 해킹사고는 앞으로도 지속될 것으로 예측된다.

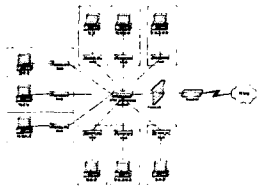
사이버 공간에서 전산망을 보호하기 위해서 사용자 인증, 무결성 점검, 침입탐지, 파이어월 등 다양한 기술이 사용되고 있다 하지만 가장 우선시 되어야 하는 것은 공격의 목표가 되는 시스템의 보안 취약점을 찾아내고 이를 제거하는 작업이라고 할 수 있다.[3][4]

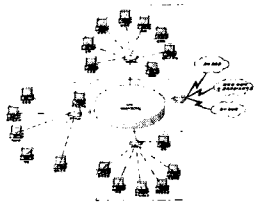
이 논문에서는 대학 전산망의 확대와 해킹기술은 급속히 발달하고 있지만 이에 비해 대학 전산망 보호를 위한 보안장비 및 관리자/사용자들의 보안지식 및 기술은 절대적으로 부족한 실정을 감안해서, 내부 사용자들이 자신의 취약점을 쉽게 점검 및 해결할 수 있고, 관리자들이 전산망의 취약점을 파악하는데 효과적인 시스템을 제안하고자 한다. 논문의 구성을 살펴보면, 2장에서는 대학 전산망의 구조에 대하여 기술하고, 3장에서는 대학 전산망의 취약점을 분석할 수 있는 시스템을 설계하며, 4장에서 안전한 대학 전산망을 운영할 수 있는 취약점 분석 시스템을 구현하고, 5장에서 결론 및 향후 연구과제를 기술한다.

2. 대학 전산망

대학 전산망 구조는 각 대학의 건물 구조나, 기능, 규모, 사용한 네트워크 망의 종류에 따라 다양한 구조로 이루어져 있다. 그러나 각 대학들의 전산망 구조를 살펴보면 하나의 Segment로 이루어진 단순구조와 이 단순구조가 여러 개 모여서 만들어진 복합구조로 구성되어 있음을 알 수 있다. 아래의 [그림 1]은 네트웍의 기본을 이루는 요소들로 구성되어 있기 때문에 단순하다. 이러한 단순구조를 가지는 전산망은

소규모 벤처기업, 2년제 전문 대학이나 소규모 종합대학에서 찾아 볼 수 있다. 복합구조로 이루어진 대학 전산망은 [그림 2]과 같은 네트워크 구조로 이루어져 있으며, 여러 개의 계열사를 거느리고 있는 대기업, 규모가 큰 종합대학 및 중/고교 및 대학을 운영하는 대규모 학원에서 볼 수 있다.

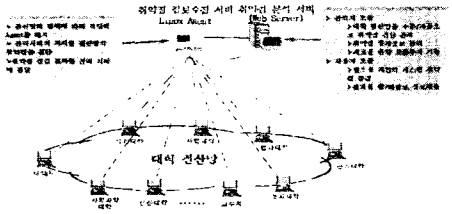




[그림 1] 단순구조 대학전산망 [그림 2] 복합구조 대학전산망 구조

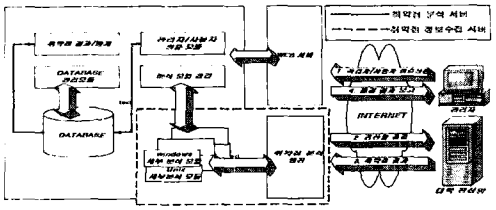
3. 대학 전산망을 위한 취약점 분석 시스템 설계

대학 전산망 관리자가 전산망 내에 존재하는 많은 시스템들의 취약점들을 네트워크를 통해서 자동으로 점검하고 발견된 문제점들에 대한 해결 방법을 보안에 대한 지식이 부족한 개별 시스템 사용자들에게 제공하여 해킹과 범죄들을 미연에 방지할 수 있는 시스템을 설계한다. 즉 취약점 분석시스템은 시스템 내부에 존재하는 것이 아니라 외부에 설치되어 네트워크를 통해서 점검한다. 대학 전산망 취약점 분석 시스템은 단순·복합 구조로 이루어진 대학 전산망을 근간으로 하여 구성하여 보면 아래 [그림 3]과 같고 취약점 분석 서버, 취약점 정보수집 서버, 대학 전산망 세 부분으로 구성된다.



[그림 3] 취약점 분석 시스템 구성

첫 번째로 데이터베이스는 취약점에 대한 정보 및 관리자/사용자들의 대한 정보를 가지고 있고 시스템 분석 서버 및 정보수집 서버에 의해서 사용된다. 두 번째로 취약점 분석 서버는 관리자가 책임지고 있는 전산망의 취약점을 웹을 통해서 수동/자동으로 취약점 정보수집 서버에 전달하며, 점검 결과를 웹을 통해서 취약점 정보를 제공한다. 세 번째로 취약점 정보수집 서버는 취약점 분석 서버에서 전달받은 명령을 실행하는 역할을 수행하며, 취약점 점검 대상이 되는 대학 전산망을 선택하여 점검을 수행하고, 점검이 완료되면 대학 전산망 보안에 활용될 수 있는 결과를 취약점 분석 서버에 보낸다. 마지막으로 대학전산망은 취약점 점검 대상이 되는 시스템으로 취약점 정보 부족 및 기술부족으로 인하여 무방비로 관리되고 있는 대학전산망에 존재하는 모든 윈도우 및 유닉스 시스템을 말한다.

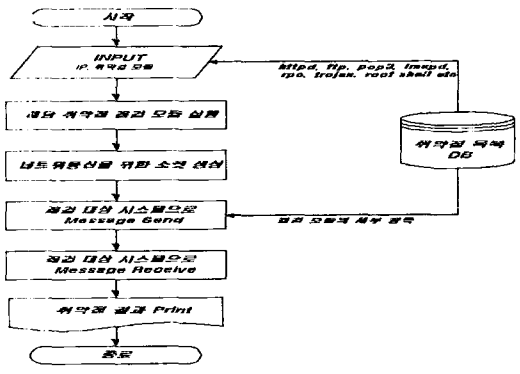


[그림 4] 시스템 구조

취약점 분석 시스템은 위 [그림 4]와 같은 세부구조로 이루어져 있다. 첫 번째 취약점 분석 서버는 시스템을 사용할 권한이 있는지를 점검해 주는 관리자/사용자 인증 모듈, 사용자/관리자들의 정보 및 취약점들에 대한 정보를 가지고 있는 데이터베이스, 관리자가 데이터베이스의 내용들을 생성 및 수정할 수 있는 데이터베이스 관리 모듈, 데이터베이스에 저장된 시스템들의 취약점의 결과를 출력해주는 취약점 결과/통계 모듈, 새로운 취약점 분석 모듈을 추가하거나 삭제할 수 있는 취약점 분석 모듈 관리로 구성되어 있다. 두번째 취약점 정보수집 서버는 점검 대상 시스템들의 취약점을 실제로 점검해주는 세부 분석 모듈과 세부 분석 모듈을 실행시키는 취약점 분석 엔진으로 구성되어 있다.

4. 대학 전산망을 위한 취약점 분석 시스템 구현

취약점 정보수집 서버는 취약점 분석 서버에서 전달받은 ip 목록에 대하여 운영체제에 따라서 취약점을 점검하는 기능을 수행한다. 취약점 점검 모듈을 모두 수행한 후 그 결과를 취약점 분석 서버에게 전송한다. 취약점 정보수집 서버 내부에서 동작되는 개별 취약점 점검 모듈은 아래 [그림 5]와 같다.



[그림 5] 개별 취약점 점검 모듈

4.1 취약점 분석 서버

취약점들의 결과를 분석하는 취약점 분석 서버의 운영체제는 윈도우2000을 사용했으며 데이터베이스는 MS-SQL, 웹서버는 IIS 5.0을 사용하였다.

구분		사양
하드웨어 환경	CPU	Pentium IV1Giga
	Ram	256 MB
	HDD	20 GB
소프트웨어 환경	OS	Windows 2000
	웹서버	IIS 5.0
	데이터베이스	MS-SQL 2000

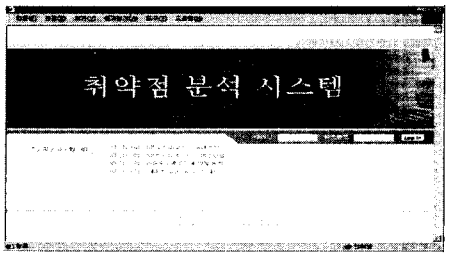
4.2 취약점 정보수집 서버

시스템의 취약점을 분석하는 취약점 정보수집 서버는 리눅스 7.0을 사용했으며, 취약점들을 점검하는 모듈은 Perl을 사용하여 작성하였다.

구분		사양
하드웨어 환경	CPU	PentiumIII 500(dual)
	Ram	516 MB
	HDD	60 GB
소프트웨어 환경	OS	Linux 7.0
	language	Perl

4.3 대학 전산망

점검대상 시스템이 속해있는 대학 전산망의 전체구조는 복합구조로 이루어져 있다. 실험에서 전산망 전체를 점검은 시스템 설치 및 내부의 어려움으로 인하여 취약점 분석 시스템이 설치되어있는 전체 전산망중 일부인 제1자연대 건물하나를 대상으로 적용을 하였다. 이 건물에는 두 개의 서로 다른 ip class를 사용하고, 사용자들은 학생들이 실습하는 실습실 1개와 교수연구실, 대학원연구실로 구성되어 있다. 네트워크의 구성은 전자계산소에서 연결된 라인이 스위칭허브를 통해서 건물내의 컴퓨터와 연결되어 있다.



[그림 6] 취약점 분석 시스템 메인 화면

5. 결 론

네트워크를 통한 침입자들은 특정 취약점을 찾기 위해 원격에서 스캔하고, 발견한 후에 그것을 공격한다. 그들이 사용하는 대부분의 도구들은 자동화 되어 있고 조작이 거의 필요 없다. 해커들이 손쉽게 침입을 하는 반면에 사용자들은 보안 지식 및 기술 부족으로 인하여 이러한 위협으로부터 시스템을 보호하기에는 어려움을 가지고 있다.[5][6][7] 이 논문에서 설계한 취약점 분석 시스템은 단순·복합 구조로 이루어진 대학 전산망을 근간으로 하여 취약점 분석 서버, 취약점 정보수집 서버, 대학 전산망, 데이터베이스로 구성하였고, 데이터베이스는 취약점에 대한 정보 및 관리자/사용자들의 대한 정보를 가지고 있고 시스템 분석 서버 및 정보수집 서버에 의해서 사용된다. 그리고 취약점 분석 서버는 관리자가 책임지고 있는 전산망의 취약점을 웹을 통해서 수동/자동으로 취약점 정보수집 서버에 전달하고 점검 결과를 웹을 통해서 취약점 정보를 제공한다. 취약점 정보수집 서버는 취약점 분석 서버에서 전달받은 명령을 실행하는 역할을 수행하며, 취약점 점검 대상이 되는 대학 전산망을 선택하여 점검을 수행하고, 점검이 완료되면 대학 전산망 보안에 활용될 수 있는 결과를 취약점 분석 서버에 보낸다. 마지막으로 대학전산망은 취약점 점검 대상이 되는 시스템으로 취약점 정보 부족 및 기술부족으로 인하여 무방비로 관리되고 있는 대학전산망에 존재하는 모든 윈도우 및 유닉스 시스템을 말한다. 이 논문에서 제안한 취약점 분석 시스템은 대학전산망이라는 환경하에서 구동되는 시스템으로 보안의식이 부족한 사용자와 관리자의 입장에서 보안 취약점을 점검 할 수 있도록 하였고, 점검 결과를 웹을 통하여 점검 대상이 된 대학전산망의 취약점분석 서버에 보내 취약점을 복구할 수 있도록 하였다. 그러므로 대학전산망의 취약점을 쉽게 파악하여 대학 전산망에 대한 신뢰성 및 안정성을 보장되도록 하였다. 이 논문에서는 취약점 분석 시스템에 대한 데이터베이스 관리 및 세부 취약점 분석 모듈, 발견된 모든 취약점 점검에 대해서 구현하지 못하였다. 앞으로 이 논문에서 설계한 모듈에 대한 구현과 새로이 발견되는 취약점에 대한 점검모듈의 추가가 필요하며, 발견된 취약점들에 대한 네트워크 및 시스템상의 취약점들에 대하여 자동적인 대응 방안을 연구할 필요가 있다.

[참고문헌]

[1] 교육인적자원부, http://www.moe.go.kr/bbs1/moebbs/47_전산망구학교현황.hwp

[2] 한국정보보호진흥원, http://www.certcc.or.kr/statistics/hack/2001/hack-200108.html

[3] 박정현, 정현철, "보안 취약성 점검을 위한 전산망 안전진단 소프트웨어의 개발", SISC'96, 1996

[4] 이현우, 네트워크 공격기법의 패러다임 변화와 대응방안, CERTCC-KR, 2000. 5

[5] Gafinkel & Spafford, Practial Unix and Internet Security, 1996

[6] Daniel Farmer and Eugene H. Spafford, the Cops Security Checker System", Technial Report CSD-TR-993, Software Engineering

[7] J. P. Martin-Flatin, "Push vs. Pull in Web-Based Network Management", Proceedings of the Sixth IFIP/IEEE Internatonal Symposium on Intergrated Network Management, May, 1999