# 분산 네트워크 환경의 보안취약점 관리 시스템

곽인섭[0], 석원홍[00], 강흥식[000]
인제대학교 정보컴퓨터공학과
{kinsub98}@cs.inje.ac.kr[0] , {babootaeng}@naver.com[00], {hskang}@nice.inje.ac.kr[000]

# Management System of Security Vulnerability on the Distribution Network Environment.

In-Seub Gwag[0], Won-Hong Seok[00], Heung-Seek Kang[000]
Dept. of Information and Computer Engineering, Inje University

**요 약**

인터넷에 정보화가 급속도로 진전되고 정보에 대한 의존도가 확산됨에 따라 정보시설에 대한 침입피해 사례가 급증하고 있다. 일어나는 해킹 사고의 대부분은 취약점 분석 도구를 이용하여 공격하고자하는 시스템의 취약점 정보를 수집한 다음 이를 바탕으로 시스템에 대해 공격을 시도하고 있다. 하지만, 네트워크 시스템 관리자들은 시스템 취약점에 대한 정보 및 기술 부족으로 시스템에 대한 관리가 무방비 상태로 이루어지고 있는 실정이다. 본 논문에서는 보안에 미숙한 관리자도 공격 대상이 되는 시스템의 취약점을 쉽게 발견하고 이를 바탕으로 공격대상이 되는 호스트를 미리 방지할 수 있고 또한 분산 네트워크 환경에서도 관리할 수 있는 취약점 관리 시스템을 설계 및 구현하였다.

## 1. 서 론

인터넷에 정보화가 급속도로 진전되고 정보통신망에 대한 의존도가 확산됨에 따라 정보시설에 대한 침입피해 사례가 급증하고 있다. 이 과정에서 관리자는 시스템을 보완하기 위해서 계속 모니터링하고 로그를 검사해야 한다. 또한 시스템과 네트워크를 안전하게 유지해야 하는데, 소프트웨어의 결함은 하루가 다르게 계속 발견되고 있으며 그 만큼 위험 요소에 노출돼 있다고 볼 수 있다. 이런 문제를 해결하기 위해 침입탐지 및 방화벽 시스템이 현재까지 연구되어 사용되어지고 있고 또, 관리자 측면에서 관리하는 대상 호스트가 가지고 있는 취약성을 미리 파악하여 대상 호스트를 보완할 수 있도록 하는 취약점 분석 도구도 있다. 하지만 이 모든 시스템들이 가지고 있는 특성 상 개별적으로 존재하고 있는 호스트들 간에 상호 연결이 계속 발달하고 있는 현 시점에서 이러한 위협들이 개별 호스트에 머무는 것이 아니라, 네트워크로 연결된 각 시스템에 피해를 줄 수 있다는 점이 그 피해를 더 심각하게 할 수 있다. 피해를 간단히 살펴보면 중요 정보의 유출 및 변경, 컴퓨터 바이러스 및 서비스 거부 공격 등 네트워크 보안 문제점을 계속 발생시키고 있다. 때문에 네트워크 관리자들은 네트워크에 연결된 각 시스템들의 보완 상태를 주기적으로 점검하여 외부 네트워크로부터의 공격에 취약한 부분을 사전에 방어하고 대처할 수 있어야 한다. 그러나 네트워크의 규모가 커질수록 관리자는 연결된 호스트들의 취약점을 주기적으로 관리하기는 어려운 일이다.[1],[2],[3]

본 논문에서는 분산 네트워크 환경에서 발생하는 해킹 사고를 미리 알 수 있도록 취약점 분석 시스템을 설계 및 구현하였다. 또한 시스템 관리자가 한 눈에 알 수 있도록 GTK 환경을 이용하고, 또한 분석 모듈의 동적 추가로 새롭게 발견된 취약점들에 대해 정확하고, 신속하게 대처할 수 있는 기능을 가지고 있다.

본 논문은 총 4장으로 구성되어 있다. 2장에서는 취약점 분석에 관련 연구들을 기술하고 3장에서 취약점 분석 시스템에 대한 구성 요소와 설계 및 구현에 대해서 살펴보고 마지막 5장에서는 결론 및 향후 방향에 대해서 설명하고 있다.

## 2. 관련 연구

### 2.1 네트워크 취약점 도구

취약점 분석 시스템은 대상 호스트가 가지고 있는 네트워크 보안에 대한 문제점을 발견하고 그것을 관리자에게 보고함으로서 불법적인 침입에 대해서 미리 대응 할 수 있는 시스템이다. 그 종류를 간단히 설명하다.[5]

• SATAN(System Administrator Tool for Analyzing Network)은 리모트 시스템의 보안 취약점을 체크한다. 따라서 이 프로그램을 작동시키는 모든 사용자는 다른 시스템의 보안상 문제점을 발견할 수 있다.

• COPS(Computerrized Oracle and Passward System)는 UNIX system 의 보안점검 프로그램이다. COPS 패키지는 보안을 조사해 주는 실제프로그램들과 설치방법과 작동방법 그리고 결과를 해석하는 도큐먼트들로 구성되어 있다. COPS는 root가 뿐만 아니라 일반 user 도 사용할 수 있다.

• Iss 는 internet security scanner의 약자로서 원격 호스트의 포트 스캔을 기본으로 하는 security checker이다. 주로 public하게 공개되어 있는 호스트 (이를테면 bbs를 돌리는 호스트나 anonymous ftp 서비스를 지원하는 호스트)를 스캔 할 목적으로 제작되었다. 하지만 인터페이스가 상당히 좋지 않기 때문에 그리 좋은 평가는 받지 못했다. 그럼에도 불구하고 한번에 넓은 범위의 호스트들을 한꺼번에 빠른 속도로 스캔 할 수 있다.

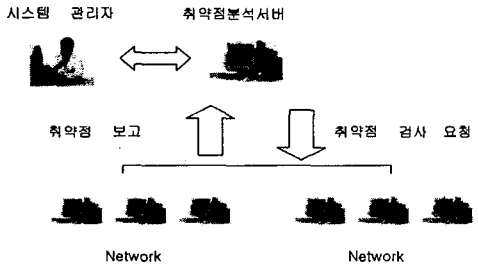
• Crack는 UNIX 시스템의 passwd는 DES(Data Encryption Standard)를 따르므로, 역함수를 구할 수 없다. 하지만, 이 패스워드를 추측하여 사전파일을 만들어 이를 /bin/passwd에 의해 암호화시킨 뒤 이것을 /etc/passwd 파일 내의 암호와 비교하여 암호를 추적하는 것이 Crack이다.

위에서 설명하고 있는 취약점 분석 시스템들이 가지고 있는 문제점들에 대해서 간단히 기술하며, SATAN이 가지고 있는 단점으로는 설치의 복잡성, 실행속도의 최적화 고려되지 않음, 필요한 자원이 많고, 여러 가지 소프트웨어 환경이 필요하다. 또 ISS는 취약점에 대한 보완 방법 없고, OS 차원 버그는 체크를 해주지 못하고, 불편하고 복잡한 사용자 인터페이스를 가지고 있는 것이 단점이다.

## 3. 제안된 취약점 통합 관리 시스템

2장 관련 연구부분에서 설명한 기존의 취약점 분석 시스템들은 검사 대상 호스트에 설치되어 시스템의 취약성을 검사하는 것에서는 본 시스템과 동일하지만 설치 방법과 사용자 인터페이스 면에서 단점을 보완한 시스템 구조로 설계하였다. 본 논문에서 구현한 취약점 분석 시스템은 다음과 같은 장점을 가진다.

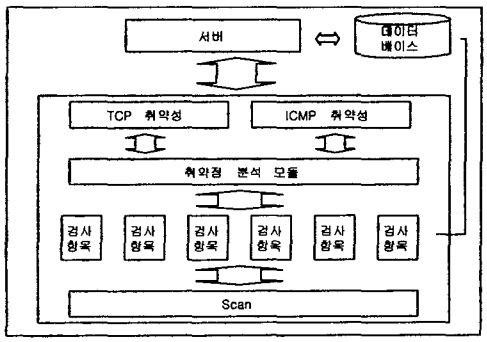
- 분산 네트워크 환경에서 대상 호스트에 대한 취약점 분석이 높다.
- 취약점 분석 프로그램의 동적 모듈 추가 기능으로써 업데이트가 빠르다.
- 관리자 위치에 구애받지 않고 관리자의 권한을 가지고 네트워크내의 각 시스템 취약성 검사를 수행 및 보고 받을 수 있다.




[그림 2] 제안된 보안취약점 관리 시스템

### 3.1 시스템 설계

본 논문에서 설계 및 구현한 취약점 분석 시스템은 크게 서버와 관리로 나누어진다. 서버는 분산 네트워크 관리에서 보완에 취약한 시스템의 상태를 검사하여 사전에 공격될 수 있는 호스트를 미리 방어할 수 있고 시스템 관리자는 분산 네트워크에 연결된 시스템의 취약점을 분석하기 위해 취약성에 대한 정책을 작성하여 DB에 저장하고 그 정책을 적용시킨다. 취약성 정책은 대상이 되는 호스트를 검사할 것인지, 또는 어떤 항목들을 검사할 것인지에 대한 요구사항을 포함한다. [그림 3]에서 시스템 세부 구성요소를 나타내며 각 기능 설명을 포함하다.




[그림 3] 시스템 구성요소

다음의 [그림 3] 시스템 구성요소에 대한 기능에 대해서 설명하고 있다.

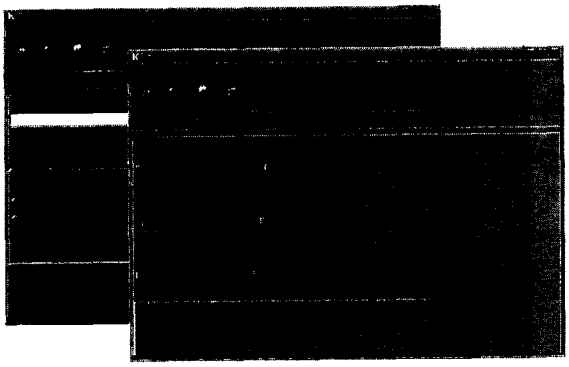
1) 취약성 검사 항목 : 대상 호스트 시스템으로부터 전달 받은 정보를 가지고 검사 항목에서 비교 분석하여 취약점에 대한 보고를 수행하는 부분이다.
2) 취약점 분석 모듈 : 취약점을 분석하고자 하는 호스트 시스템으로부터 받은 OS정보, 사용하고 있는 포트 정보, 그 시스템이 가지고 있는 구성파일 등 실제로 취약점을 검사하는 모듈로서 각 취약점의 특성에 따라 모듈들이 구성되며 새롭게 발견되는 취약점을 쉽게 추가하거나 분석하기 위해서 사용되는 부분이다.
3) 서버 : 취약점 정보를 수집하기 위해서 그 대상이 되는 네트워크 내에 설치되어 관리자가 취약점 분석을 할 수 있도록 하는 부분이면 서버에서 설정된 정책과 지시에 따라 해당 호스트의 취약점을 검사하여 DB로 전달하여 그 결과를 관리자에게 보여주는 기능이다.
4) 데이터 베이스 : 관리자의 취약점 분석 모듈과 취약점 검사 항목, 세부 설명, 분석 요청, 분석 결과, 결과 보고서, 해결 방안 등을 저장하여 관리자가 필요 또는 시스템 취약점 검사 수행 시 이전에 검사와 기존에 검사를 비교하여 그 결과 정보를 보여줄 수 있도록 정보를 제공하는 부분이다.

### 3.2 시스템 구조

취약점 분석 시스템은 분석되어 관리자 인터페이스로 전달된 정보를 관리자가 효율적으로 관찰 및 관리할 수 있게 설계, 구현하였다. 이 시스템이 구현된 환경 정보이다.

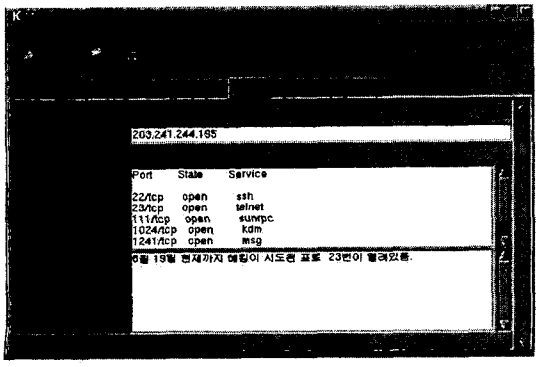
취약점 분석 시스템 : Linux 7.2
관리자 인터페이스 : GTK
취약성 분석 프로그램 : C , C++

취약점 분석 시스템에서 처음으로 관리자에게 보여지는 화면이 [그림 3]이 인터페이스가 초기 화면이다.



[그림 3] 취약점 분석 시스템 초기화면

뒤편에 있는 그림이 관리자 초기 화면으로 대상 호스트가 되는 Target의 설정하여 취약점에 대해서 분석하기 위한 처음 단계를 보여주고 있고 앞 그림에서는 Target이 결정되고 대상 호스트에 대한 정보 수집에 필요한 Scan방식을 결정하고 있는 화면이다. [그림 4]에서는 Scan중하나를 선택했을 때 그 취약점에 대한 상세 정보를 보여 주고 있는 결과화면이 Report창으로 나타난다. 또한 본 논문에서 구현한 보안 취약점 시스템은 취약점에 대해서 관리자가 보관하고 추후 관리가 용이하도록 분석 결과를 보고서 형식으로 작성할 수 있는 기능을 가지고 있다.




[그림 4] 취약점 분석 시스템 결과 화면

### 4. 결론 및 향후 연구 방향

시스템을 침입하기 위해 가장 먼저 수행하는 공격의 하나가 네트워크 스캔을 통해 보안 취약점을 파악하고, 보안 취약점이 발견될 경우 해당 취약점을 이용해 시스템으로의 침입을 시도하게 된다. 따라서 이러한 일차 공격으로부터 피해를 최소화기 위해 먼저 시스템에 대한 취약점을 보완하는 것이 필요하다. 따라서 네트워크 시스템 관리자는 시스템이 가지고 있는 보안 취약점에 대해서 미리 파악하여 신속히 대처하여 공격의 대상에서 시스템을 보호해야한다.

본 논문에서는 설계 및 구현한 보안 취약점 분석 시스템은 분산 네트워크 환경에서 취약점 분석을 위해 관리자의 작업을 자동화하고 인터페이스 환경에서 간단히 사용할 수 있도록 시스템을 구성하므로 효율성이 높다. 또한 단일 호스트 기반에 국한되는 것이 아니라 분산 네트워크 망 내의 여러 호스트 시스템에 대한 취약점 분석도 통합적으로 관리할 수 있는 보안 취약점 시스템으로 구현하였다. 그러나 본 시스템은 Scan을 이용한 대상 호스트 포트 정보를 가지고 취약점을 분석, 검사를 수행하므로 향후 많은 취약성 정보를 가지고 좀더 자동화 된 시스템으로 발전할 수 있도록 더욱 확장해 나갈 계획이다.

### 참고문헌

[1] 한국정보보호진흥원, "Hacking 통계자료", http : // www.certcc.or.kr , 2001.
[2] 한국정보보호 센터, 불법 침입자 실시간 역추적 시스템 개발에 관한 연구, 1998
[3] 한국정보보호진흥원, "RTSD 2002년 통계자료", http : //www.certcc.or.kr, 2002.
[4] CERTCC-KR 보안 권고문, http : //www.certcc.or.kr/advisory/adv_certcckr.html
[5] 포항공과대학교 유닉스 보안 연구회, Security PLUS for UNIX, 2000
[6] 서동일, 윤이중, 조현숙, "정보전 대비 실시간 침입자 감지 및 경보 네트워크 구축방안", 정보과학회지, 제18권 제12호,2000년 12월
[7] 이현우, 이상엽, 정현철, 정윤종, 임채호, "대규모 네트워크취약점 검색공격 패턴분석 및 탐지도구 개발", WISC '99, '99.9.
[8] C. Kahn, P.A. Porras, S. Staniford-Chen and B. Tung, "A Common Intrusion Detection Framework-data formats," Internet draft-ietf-cidf-formats-00. txt, Mar, 1998.
[9] H. Debar, M. Dacier and A. Wespi, "Reserch Report Towards a Taxonomy of Intrusin Detection Systems," Technical Report RZ 3030, IBM Research Division, Zurich Research Laboratory, Jun, 1998