웹 기반에서 시스템 보안 취약점을 진단하는 시스템

서현진[U] 강태호 이재영
한림대학교 컴퓨터공학과
{cordias, thkang, jylee}@center.cie.hallym.ac.kr

A System to Diagnose Security Vulnerabilityes of Systems on Based Web

Hyun-Jin Seo[U] Tae-Ho Kang Jae-Yung Lee
Dept. of Computer Engineering, Hallym University

요 약

최근에 일어나는 해킹 사고의 대부분은 스캐닝 도구를 사용하여 일차적으로 공격하고자하는 시스템의 취약점 정보를 수집한 다음, 이를 바탕으로 시스템에 대해 공격을 시도하고 있다. 하지만, 대부분의 네트워크 시스템 관리자들은 자신의 시스템의 취약점에 대한 정보 부족과 기술 부족으로 인하여 무방비 상태로 관리하고 있는 실정이다. 그리고, 대부분은 스캐닝 도구들은 처음에는 시스템 보안취약점 진단 목적으로 개발되었으나, 해커들에 의해 악용되고 있다. 따라서, 본 논문에서는 보안에 미숙한 관리자도 시스템의 취약점을 쉽게 발견하고 이를 바탕으로 하여 취약점을 보완할 수 있도록 웹 기반에서 시스템 보안 취약점을 진단하는 시스템을 제안하고자 한다.

1. 서론

최근 들어 전자 상거래, 인트라넷, 클라이언트, 클라이언트/서버 등과 같은 개방된 인터넷을 이용한 각종 수익 사업이 이루어지고 있으며, 인터넷을 통해 중요한 정보의 이동이 급격히 확산되고 있다. 특히 인터넷의 발전과 더불어 개방 지향적인 유닉스 운영체제를 사용하는 컴퓨터의 보급이 확산되고, 정보의 개방을 통한 각종 해킹 기술의 접근이 쉬워지면서 인터넷에서의 불법적인 시스템 크래킹이나. 해킹을 통한 정보 유출 및 불법적인 사용 등이 증가하고 있다[1, 2].

그리고, 최근 등장하고 있는 정보 시스템 기술이나 정보 보호 시스템은 해킹에 대응할 수 있는 각종 방법을 고려해 탄생하고 있지만 뒤질세라 새로운 해킹 기법 또한 우후죽순처럼 생겨나고 있다. 더욱 심각한 것은 국내 시스템 관리자들의 기술력과 인식 부족 탓에 해외 해커의 침입이 전체 해킹 사고의 대부분을 차지하고 있는 실정이다. 다행히 국내 해커들에 의한 범죄는 줄고 있지만 최근 해킹 기법을 정확히 파악해 자신의 학교나 자신이 이용하는 PC, 혹은 현재 관리하고 있는 시스템이 받을 수 있는 피해를 최소화하는 일이 필요하다.

아직 많은 대학의 경우 시스템 관리자를 전문 관리자가 아닌 미숙한 학생들에게 맡기는 경우가 대부분이고, 많은 회사나 기관에도 비슷한 처지이다. 또한, 그들 대부분은 자신의 시스템이 해킹을 당했는지조차 모르는 경우가 많고, 보안에 아예 무관심한 경우도 많이 있어서 문제가 되고 있으며, 대학의 경우 각 연구실이나 실험용 서버의 대부분이 보안에는 취약하다고 알려져 있다.

그리고, 최근 일어나는 해킹사고의 대부분은 스캐닝 도구를 사용하여 일차적으로 공격하고자하는 시스템의 취약점 정보를 수집한 다음, 이를 바탕으로 시스템에 대해 공격을 시도하는 것으로 나타나고 있다. 하지만, 대부분의 네트워크 시스템 관리자들은 자신의 시스템의 취약점에 대한 정보 부족과 기술 부족으로 인하여 무방비 상태로 관리하고 있는 실정이다.

본 논문에서는 웹을 이용하여 시스템에 대한 정보와 기술이 부족한 미숙한 관리자도 온라인으로 간단하게 자신이 관리하는 시스템의 취약점을 조사, 분석하고 각 취약점에 대해서 바로 보완할 수 있도록 웹 기반에서 시스템 보안 취약점을 진단하는 시스템을 제안하고자 한다.

2. 시스템 취약점 진단 시스템

네트워크 스캐닝이란 특정 호스트에서 사용되고 있는 운영체제, 또는 네트워크 전체 구조에 대한 정보를 수집하기 위한 공격이다. 이들 정보는 시스템 공격을 용이하게 하고, 어떠한 취약점을 공격해야할 지를 알려준다.

일반적인 네트워크 스캔 공격은 ISS와 SATAN이 인터넷을 통해 공개되면서 시작되었다. 이들 네트워크 스캔

도구들은 네트워크의 보안 관리를 목적으로 개발된 공개 소프트웨어이지만 보안 관리를 위해 사용되기보다는 불법적인 시스템 침입을 노리는 악의적인 사용자에 의해 사용될 가능성이 높아 많은 논란을 일으켰다[3].
보안 취약점 점검 도구에 의한 스캐닝 공격에 대한 뚜렷한 대책은 없다. 하지만 보안 취약점 진단은 시스템 공격을 위해 행해지는 최초의 행위이고 여기서 발견된 보안 취약점을 악용하여 실제 시스템에 대한 공격이 이루어지는 경우가 대부분이다. 따라서 시스템 관리자는 공격자가 취약점을 점검하기 이전에 미리 자신의 시스템 및 네트워크의 보안 취약점을 점검하여 발견된 취약점에 대한 조치를 할 필요가 있다[4]. 그러나, 아직도 국내의 경우에 있어서 회사나 기관의 경우 보안의 중요성을 인식하지 못하고 있어 관리의 비중이 적을 뿐 아니라, 학교에 있어서도 몇몇의 중요한 서버를 제외하고 대부분의 실험용 서버들은 시스템의 취약점이 그대로 노출되어 있는 실정이다. 그리고, 대부분의 해커들은 대단위의 네트워크 스캐닝을 통해 취약점을 지닌 시스템을 검색하고, 이를 통해 다음 침입을 이용하기 때문에 피해 규모가 더욱 크게 된다.
시스템의 취약점을 조사하여 분석하는 도구로서 여러 스캐닝 도구들이 배포되었고, 특히 SAINT나 SATAN 등의 도구의 경우에는 웹 기반 취약점 탐지 도구로서 훨씬 쉽게 분석할 수 있지만, 오래되어 효과가 없는 취약점을 점검하기에 때문에 최근의 취약점 진단에는 부족한 점이 있다. 또한, 한국정보보호센터에서도 K-COPS라는 보안 점검 서비스를 제공하고 있다.

3. 웹 기반의 시스템 취약점 진단 시스템

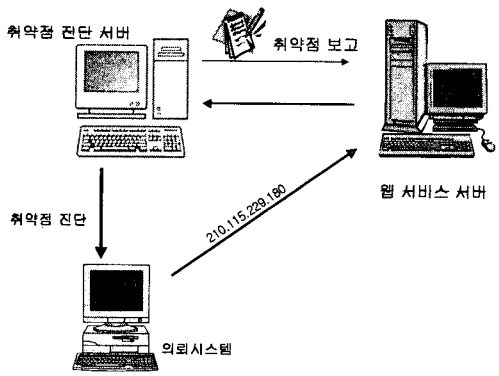

그림 1 웹 기반 시스템 취약점 진단 시스템 구성도

웹을 통한 시스템 관리 기술들은 사용자의 위치에 관계없이 시스템에 대한 접근 권한만 있으면 어느 곳에서라도 서버에 접근하여 시스템 상황을 감시, 관리 할 수 있으며, 웹 기반의 사용자 인터페이스는 웹 브라우저를 사용하여 운용관리 시스템의 기종에 종속됨이 없이 인터넷에 연결할 수 있는 어떠한 시스템을 통해서든 관리가 가능함으로써 관리 시스템의 개발과 운용측면에서 유연성을 극대화 할 수 있는 장점을 가지고 있다[5].
본 시스템에서는 웹을 통하여 특정의 시스템 관리자가 본 시스템에 접속하여 온라인으로 자신의 시스템에 대해 취약점을 조사, 분석하여 그 취약점에 대해 바로 보완하는 서비스를 제공하고 있다. 그리고, 메일링 리스트를 통하여 새로 나타나는 취약점에 대하여 패치 안내를 하게 된다.

3.1. 의뢰 시스템

보통의 유닉스 시스템을 가리키며, 웹 상에서 자신의 시스템의 취약점 점검을 의뢰하고, 나타난 취약점에 대해 각 취약점에 대한 설명과 해결책을 파악하고, OS종류에 따라 패치를 통해 취약점을 보완 할 수 있다.

3.2. 웹 서비스 서버

이 시스템은 주로 사용자에게 시스템 취약점에 대한 정보와 각 취약점에 대한 설명과 해결책을 웹을 통해 디스플레이 하는 기능을 한다. 그리고, 보안취약점 DB와 각 취약점에 대한 패치 파일을 가지고 있다.
대부분의 경우, 전달받은 의뢰시스템에 대한 취약점에 대한 내용은 시스템과 네트워크에 대한 전문적인 지식이 없으면 쉽게 이해하기 어려운 부분들이다. 그리고, 대부분 이해하더라도, 이들 취약점의 내용을 이해하고 해결책에 따라 패치하는 것은 여간 번거러운 일이 아니다. 그래서, 많은 관리자들은 이를 무시하고 시스템을 운영하고 있다. 그리고, 이것이 해커들의 주된 공격대상이 되는 것이다.
따라서, 본 서버는 웹으로 의뢰 시스템에 진단된 취약점 목록을 디스플레이하고, 보안 취약점DB에서 의뢰시스템의 취약점에 해당하는 보안 권고문을 선택하여 각 취약점에 대한 보안 권고문을 디스플레이한다.
그리고, 각 취약점 보완에 대한 패치 파일을 제공하여, 의뢰 시스템 관리자가 나타난 취약점에 대한 보완을 바로 할 수 있도록 하였다. 이렇게함으로써, 취약점 보완에 관한 여러 단계에 일들을 손쉽고 간단하게 할 수 있게 된다.

3.2.1 보안 권고문 DB

보안 권고문은 국외의 IRT(Incident Response Team), 운영체제 개발업체, 보안관련 메일링리스트 등 다양한 출처에서 수집된 보안관련 정보를 신속하게 알리고자 하는 목적으로 작성되었다[6]. 보안 권고문은 취약점목록, 설명, 해결책 등으로 구성되고, 여기에서는 이러한 보안 권고문을 DB에 저장하여, 취약점으로 나타나는 것에 대한 상세 정보를 제공한다.

3.2.2. 취약점 보안 패치 파일

각 취약점에 대해서 각 vendor나 관련 사이트에서는 각 버전별, OS별 패치 파일을 제공하고 있다. 이를 이용해서 취약점이 드러난 시스템의 취약점을 보완할 수 있다.

3.3. 취약점 진단 서버

이 시스템은 실제로 의뢰시스템에 대한 취약점을 점검하는 기능을 하게된다. 그리고, 나타난 네트워크 및 시스템에 대한 취약점에 대한 정보를 웹서비스 서버에 전달한다.

4. 실험 및 검토

4.1 실험 환경

본 진단 시스템에 대한 실험은 의뢰시스템과 취약점 진단 서버는 Solaris 2.6 x86, 웹 서비스는 MS-SQL 7.0, IIS4.0의 NT4.0 기반에서 ASP로 프로그래밍하였다.

4.2 시스템 구현 및 결과

그림2와 같은 초기화면에서 우리는 의뢰하고자하는 시스템의 주소를 입력하고, 취약점을 진단하게 된다. 여기에서는 오로지 자신의 서버에 대해서만 취약점을 파악할 수 있도록 제한을 두었다.

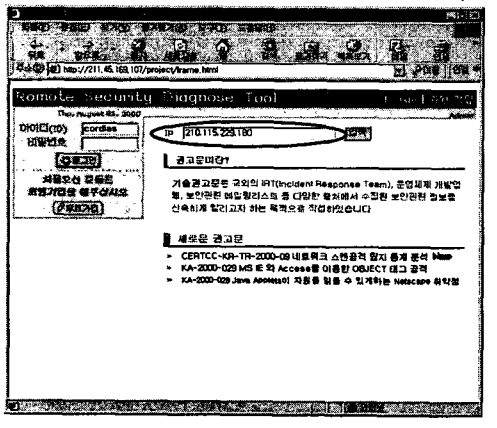

그림 2 취약점 진단 의뢰 화면

보안도구를 이용하여 의뢰시스템의 취약점을 원격지에서 취약한 네트워크 포트 점검, 버퍼 오버플로우 점검, RPC 취약점 점검, BIND, Sadmin 취약점 점검 등을 수행하고 의뢰 시스템의 취약점 진단 결과를 웹 서비스 서버에 통보한다.

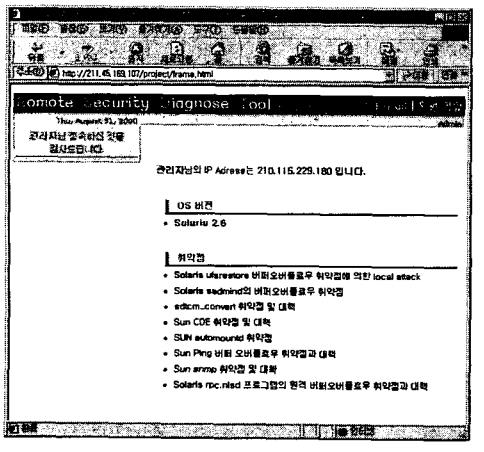

그림 3 의뢰 시스템의 취약점 목록

그리고, 취약점 보고결과를 바탕으로 보안 취약점 DB에 검색하여, 일치되는 취약점의 목록을 접속자 ID와 진단 시스템의 주소와 함께 기록하여, 그림3과 같이 웹을 통해 Html문서로 나타내게 된다. 그래서, 시스템 관리자들은 취약점 진단에 관한 도구를 설치하지 않고도 웹을 통해 쉽게 진단할 수 있게 된다.

그리고, 웹을 통해 나타난 취약점 목록에서 각각의 취약점에 대한 세부 정보를 각 취약점에 대한 세부정보 즉 취약점에 대한 설명, 해결책, OS에 해당되는 패치 파일을 제공한다.

본 시스템에서는 네트워크에 대한 전문적인 지식과 기술이 부족한 관리자들도 자신의 시스템에 취약점의 진단 도구의 설치없이, 웹을 통한 온라인으로 쉽게 각 취약점을 보완할 수 있는 서비스를 제공함을 알 수 있다.

5. 결 론

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 최소화하기 위해 먼저 시스템에 대한 취약점을 보완하는 것이 필요하다.

따라서, 본 논문에서는 보안에 관한 기술 부족과 관리 소홀의 시스템의 취약점을 보완할 수 있도록 웹 기반의 온라인으로 취약점을 진단하고 보완할 수 있도록 하였다.

참고문헌

[1] 한국 정보 보호 센터, 불법 침입자 실시간 역추적 시스템 개발에 관한 연구, 1998

[2] 한국 정보 보호 센터, 실시간 네트워크 침입 탐지 시스템, 1998

[3] Fyodor, "The Art of Port Scanning", Phrack Magazine Volume 7 Issue 51, 1997.

[4] 중요정보통신망 해킹시 침입자 기법 분석과 대응, http://www.certcc.or.kr/paper/tr1999/199901/Docs/tr1999001.html

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

[6] CERTCC-KR 보안 권고문, http://www.certcc.or.kr/advisory/adv_certcckr.html