웹 기반에서 시스템의 취약점 보완

김원진[U] 강태호 이재영
한림대학교 컴퓨터공학부
{wjkim, thkang, jylee}@center.cie.hallym.ac.kr

A Complement of System Vulnerability on the Web-Based

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

요 약

최근에 일어나는 해킹의 대부분은 스캐닝 도구를 이용하여 공격하고자 하는 시스템의 취약점을 수집한 후, 이를 바탕으로 인터넷에서 배포되고 있는 취약점에 대한 공격도구를 이용하여 시스템에 침투하고 있다. 반면 시스템 취약점 보완에 대한 시스템 관리자의 관리 소홀로 인하여 무분별한 해킹의 대상이 되어 다른 시스템을 공격할 수 있는 새로운 시스템으로 이용된다. 따라서 본 논문에서는 웹 기반에서 시스템의 취약점을 보완하기 위한 연구의 일환으로, 리눅스 기반의 시스템을 원격에서 진단하고, 이를 바탕으로 시스템의 취약점이 되는 데몬 서비스 프로그램에 대한 업데이트를 웹에 접속하여 자신의 시스템 진단내용을 확인하고, 업데이트 하고자 하는 서비스 프로그램을 선택하여 생성된 스크립트를 실행함으로써 자동적으로 설치되기 위한 스크립트를 생성해주는 시스템을 개발하였다.

1. 서론

최근 몇 년간 전자 상거래와 맞물려 인터넷 서비스 업체가 호황을 누리고 있고, 그런 업체는 소규모로써 새로운 서비스에 대한 아이템을 가지고 생겨나고 있다.

인터넷을 통한 서비스를 제공하기 위해 사용되는 시스템의 운영체제 중 하나인 리눅스는 무료로 배포되어 사용되어 진다는 장점이 있는 반면에 개방 지향적인 운영체제의 특징으로 인하여 리눅스에 대한 해킹 기술 또한 확산되고 있다.

해킹 기술의 확산과 동시에 해커에 대한 잘못된 인식을 가진 많은 크래커들의 확산 또한 시스템에 대한 공격피해를 증가시키고, 대학이나 소규모의 기업의 시스템 관리자들은 전문적인 교육을 받지 않았거나, 업무의 과중으로 인하여 자신의 시스템이 해킹 당했는지 조차 모르고 있는 경우가 많다.

현재 침해사고 접수 및 처리현황에서 절반 가량의 피해기관은 기업과 대학이고, 접수된 해킹의 처리내용에서 보여진 내용은 각 서비스 데몬의 취약점을 이용한 방법이 가장 많았다. 이 방법은 시스템 스캐닝 도구를 이용하여 시스템에 정보를 찾아 아직 패치가 되지 않은 취약점을 가지고 있는 서비스 프로그램의 데몬에 대한 공격기법을 인터넷 상에서 수집하여 시스템에 공격을 시도한다[1, 2].

본 논문에서는 웹을 통하여 원격의 시스템을 관리하는 방법의 일환으로 네트워크 스캐너를 통하여 자신의 시스템에 대한 취약점을 분석하여 그에 해당하는 보완작업에 대한 스크립트를 생성함으로써 클라이언트 시스템의 취약점 보완을 해결하는데 그 목적이 있다.

2. 취약점 진단 시스템

현재 사용되고 있는 시스템의 취약점 진단 도구는 시스템 스캐너가 있는데 이는 시스템 설정상의 문제에서 발생할 수 있는 잘못된 퍼미션과 계정등의 보안상의 결점을 찾기 위해 로컬 호스트에 대한 분석을 하는 도구로 COPS와 Tiger, Trip-wire등이 있고, 네트워크 스캐너는 네크워크 연결에 대한 문제점을 테스트하기 위해서 이용 가능한 서비스와 포트를 조사함으로써 원격지에서 해커들이 이용할 수 있는 잘 알려진 취약점을 찾아낸다. 네트워크 스캐너로써는 ISS와 SAINT, nmap, sscan등이 있다[3].

3. 취약점 보완 시스템의 구성

본 논문에서는 웹을 통하여 원격의 시스템을 관리하는 방법을 사용하였다.

그림 1은 웹 기반의 취약점 보완 시스템의 구성도로 크게 호스트 시스템과 클라이언트 시스템 두 부분으로 분류 될 수 있다.

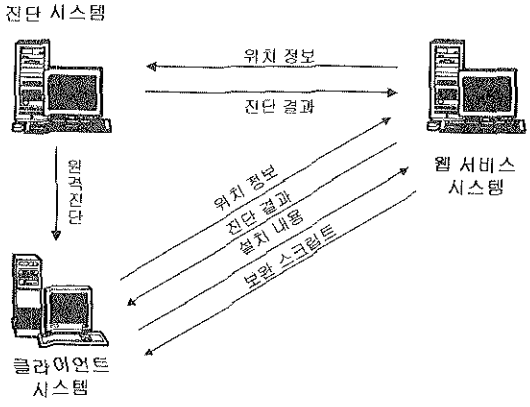

그림 1. 취약점 보완 시스템의 구성도

호스트 시스템은 클라이언트 시스템을 원격으로 진단하기 위한 진단 시스템과 웹 서비스 시스템 그리고 취약점 보완 자료를 저장하기 위한 취약점 보완 DB로 구성된다. 클라이언트의 요청에 대한 호스트 시스템은 그림 2와 같이 몇 단계로 작업을 수행한다.

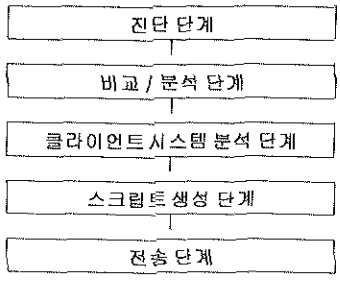

그림 2. 호스트 시스템의 단계별 수행 과정

3.1 취약점 보완 DB

취약점 보완 DB는 웹 서비스 시스템 안에 포함되어 있으며, 국외 리눅스 관련 권고문에서 새롭게 발견된 보안 관련 취약점 자료와 지난 자료가 포함된다.

내용은 국외 리눅스 관련 권고문 자료에서 분류한 취약점이 발견된 데몬, 취약점 내용, 설명, 해결책, 패치 파일, 패치 스크립트 등으로 구성되어 이 정보를 바탕으로 보완 스크립트를 작성한다.

3.2 취약점 보완 시스템의 알고리즘

취약점 보완 시스템은 클라이언트 시스템의 취약점 진단 요청을 받게되면, 클라이언트 시스템에 대한 인증을 거친 후 시스템의 위치 정보를 진단 시스템에게 제공하여 취약점 서비스 데몬에 관한 결과를 웹 서비스 시스템으로 가져와 취약점 보완 DB에 저장된 자료를 바탕으로 결과에 해당하는 보안권고문과 보완해야 할 서비스 프로그램, 공격 가능법을 보여주고, 클라이언트 시스템이 선택한 패치 프로그램의 목록을 스크립트 생성부로 전달하여 취약점 보완 DB를 이용하여 패치 프로그램과 개별적인 설정 파일에 대한 설치 스크립트를 생성하여 클라이언트 시스템에게 제공한다.

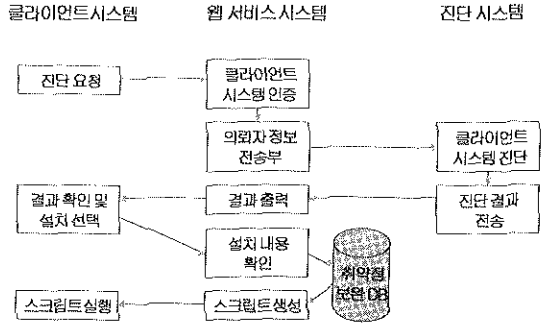

그림 3. 취약점 보완 시스템의 상세도

그림 3에서 취약점 보완 시스템은 취약점 진단 결과와 클라이언트 시스템의 선택적인 프로그램 설치내용을 바탕으로 그에 적용할 내용을 취약점 보완 DB에서 추출, 조합하여 스크립트 생성 알고리즘을 통하여 클라이언트 시스템에게 전달한다. 클라이언트 시스템 정보와 취약점 결과를 가지고 적절한 패치 스크립트를 작성하는 구체적인 방법은 다음과 같다.

(1) 진단 시스템이 보낸 로그내용의 데몬에 따라 취약점 보완 DB에서 취약점 내용과 그에 해당하는 패치 목록, 방법을 클라이언트 시스템에게 보여준다.

(2) 보여진 내용 중 클라이언트 시스템이 패치를 요구한 사항과 설치하기 위한 클라이언트 시스템의 정보를 입력받는다.

(3) 입력받은 선택된 데몬은 취약점 보완 DB에서 데몬에 대한 설치 프로그램과 클라이언트 시스템의 정보에 해당하는 미리 작성된 패치 스크립트를 선택한다.

(4) (3)과 같은 방법으로 다른 선택된 데몬에 대하여도 스크립트를 추가하여 저장한다.

4. 구현 및 검토

4.1 구현 환경

본 취약점 보완 시스템을 구현하는 실험환경으로 클라이언트 시스템과 취약점 진단 시스템은 Redhat Linux 6.2, 웹 서비스 시스템은 IIS4.0의 NT4.0 기반에서 ASP를 이용하여 프로그래밍 하였고, 취약점 보완 DB는 MS-SQL 7.0을 사용하였다.

4.2 시스템 구현 및 결과

그림 4에서는 클라이언트 시스템의 취약점 진단 결과를 웹 서비스 시스템에서 서비스 데몬과 그에 해당하는 취약점을 보여준다.

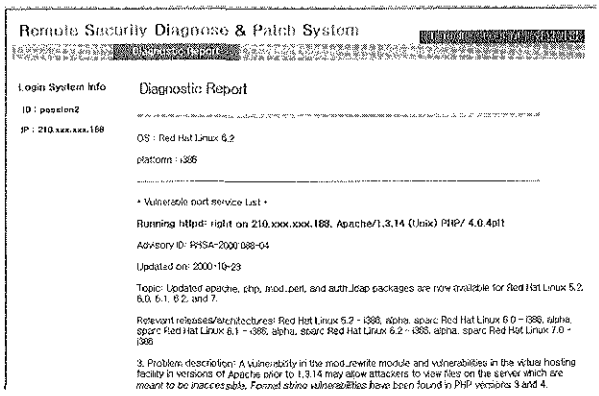

그림 4. 클라이언트 시스템의 취약점 목록

그림 5에서는 취약점이 발견된 각 데몬에 대한 패치 프로그램을 설치할 목록과 함께 설치 사항을 클라이언트 시스템 관리자가 자신의 시스템에 맞게 선택하도록 하여 그 선택 사항에 대하여 보완 스크립트를 작성한다.

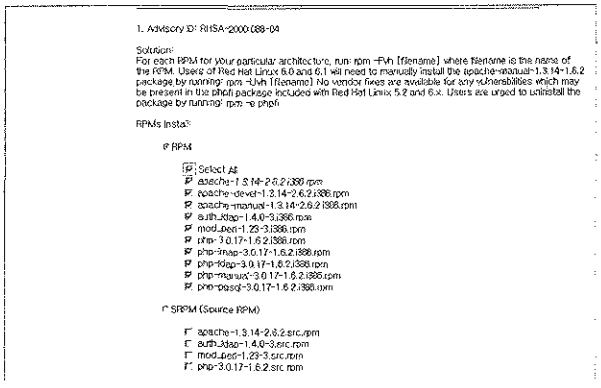

그림 5. 취약점 보완 프로그램 설치 목록

취약점 보완 스크립트는 기본적인 패치 프로그램의 설치 명령어로 구성되고, 패치 프로그램을 다중으로 선택하여 여러 가지 패치 프로그램을 일괄적으로 보완함으로써, 웹의 접속으로 손쉽게 작업을 수행할 수 있도록 제공한다. 하지만, 리눅스 시스템의 권한 상의 이유로 패치 스크립트는 클라이언트 시스템에서 실행하도록 생성된다. 본 시스템에서는 시스템에 관한 전문지식이 없는 시스템 관리자도 취약점 보완 시스템에 접속하여 시스템에 대한 취약점과 그에 해당하는 취약점이 수정된 패치 프로그램을 자동으로 설치 해주는 스크립트를 실행하도록 하여 효율적인 관리를 제공한다.

5. 결론 및 향후 연구과제

본 논문에서는 웹 기반에서 시스템 보안 취약점을 진단하여 그에 해당하는 취약점을 해당 시스템에 적합한 방법으로 손쉽게 보완하는 스크립트를 생성하여 시스템 관리자가 스크립트의 실행만으로 설치 가능하도록 하였다. 리눅스 기반의 클라이언트 시스템에 대한 취약점을 웹을 통하여 확인하고, 확인된 시스템의 취약점을 가진 데몬의 서비스 프로그램 버그를 수정한 패치 프로그램을 설치함으로써 이를 이용한 해커들의 침입을 방지 할 수 있었다. 향후 연구과제로 본 논문에서 구현된 시스템은 클라이언트의 설치항목을 자동으로 판단 할 수 없는 문제점으로 인하여 그림 5와 같이 클라이언트의 선택으로 설치 스크립트를 생성하였는데, 설치 스크립트 생성의 향상과 시스템에 대한 효율적 측면의 평가가 필요하다.

6. 참고문헌

[1] 한국 정보 보호 센터, "2000년 해킹 피해 현황" ,http://www.kisa.or.kr/press/2001/data/20010108.hwp

[2] 한국 정보 보호 센터, "네트워크 스캔공격 탐지 통계 분석", 2000

[3] Anonymous, "MAXIMUM LINUX SECURITY", Sams, 1999

[4] LinuxSecurity Advisories http://www.linuxsecurity.org/advisories/redhat.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, 1999

[6] 서현진, 강태호, 이재영, "웹 기반에서 시스템 보안 취약점을 진단하는 시스템", 한국정보과학회,학술발표논문집, 제27권 2호,2000