웹 환경을 이용한 보안 취약점 점검 도구 개발에 관한 연구

장승주, 최은석
동의대학교 컴퓨터공학과
sjjang@deu.ac.kr

A Study on Implementation of Vulnerability Assessment Tool on the Web

Seung-Ju Jang, Eun-Seok Choi
Dept. of Computer Engineering, Dong-Eui University

요 약

본 논문은 웹을 이용한 보안 취약점 점검 도구를 개발한다. 본 논문은 보안 취약점 점검 도구들을 이용하여 웹상에서 사용자의 컴퓨터 시스템에 대한 점검을 통해서 결과를 보여주는 환경을 개발한다. 개발된 웹 보안 취약점 점검 도구는 쉽게 자신의 서버 컴퓨터의 취약점을 점검할 수 있다. 본 논문에서 구현된 보안 취약점 점검 도구의 기능은 포트 스캔, SQL injection 취약점 점검 기능으로 구성되어 있다. 포트 스캔 취약점 점검 도구의 기능은 열려져 있는 컴퓨터 시스템의 포트 점검을 통하여 불필요하게 열려져 있는 포트를 점검한다. 이런 점검을 통해서 보안 취약점을 사전에 차단한다. SQL injection 기능은 DB에서 SQL 구문의 취약점을 점검한다. 본 논문에서 제안하는 보안 취약점 점검 기능에 대해서 실험을 수행하였다.

1. 서 론

우리나라가 IT 강국으로 성장할 수 있었던 배경은 여러 이유가 있지만, 그 이유들 중에서 "Web"의 탄생을 생각하지 않을 수가 없다. "Web"이라는 매개체는 서비스를 제공자들 사이에서 상호연결을 쉽게 해주고, 새로운 직업과 기회를 주었다. 또한 업무의 효율성을 거의 무한대로 제공한다. 하지만 접근하기 쉬운 Application과 Application들 간의 통합이 됨에 따라 보안에 대한 문제가 발생한다. 보안에 문제가 생김에 때라 일반적으로 해킹(hacking)으로 알려진 크래킹(cracking)이 빈번하게 일어난다. 이러한 보안의 문제는 보안상의 취약점(Vulnerability)을 크래커(cracker)들이 사용하기 때문이다. 보안 취약점(Vulnerability)은 시스템 및 네트워크의 보안정책을 위반하여 공격되어지는 시스템 및 네트워크 설계, 구현, 운영, 관리상의 약점이라고 할 수 있다. 이러한 보안상의 취약점을 점검하는 도구들은 공개되어 있는 프로그램들도 있지만 상용화된 프로그램들도 있다. 이러한 프로그램들은 보안상의 취약점을 검사하고 그 결과를 사용자에게 보여 준다. 이는 보안상의 취약점을 예방하는 차원에서 개발되어 졌지만, 악의적인 용도로 사용되어 질 수도 있다.

본 논문은 웹 환경을 이용하여 보안 취약점을 점검해 줄 수 있는 점검 도구의 개발을 연구 하고자 한다. 사용자는 웹에 접속하여 자신의 서버 컴퓨터에 대한 보안 취약점을 점검할 수 있다. 개발된 웹 보안 취약점 점검 도구는 쉽게 자신의 서버 컴퓨터의 취약점을 점검할 수 있다. 본 논문에서 구현된 보안 취약점 점검 도구의 기능은 포트 스캔, SQL injection 취약점 점검 기능으로 구성되어 있다.

본 논문의 구성은 다음과 같다. 2장에서 본 연구와 관련 있는 연구를 설명하였고, 3장에서는 보안 취약점 점검 도구의 설계에 대해 기술하였다. 4장에서는 웹 관련 보안 취약점 점검 도구에 대하여 웹상에 직접 구현하였다. 5장에서는 구현된 보안 취약점 기능에 대해서 실험을 수행한다. 6장에서는 본 논문의 결론으로 구성한다.

2. 관련연구

보안에 대한 중요성을 지속적으로 알리고 정보를 제공하고 있는 국내 Web site중 안철수 연구소는 보안 취약점을 파고드는 신종 악성코드와 스파이웨어들에 대해 지난해인 2006년 1월부터 11월까지의 동향을 분석하였다. 악성코드는 바이러스, 웜, 트로이목마처럼 PC 정보를 손상하거나 유출하려는 악의적 목적으로 만들어진 프로그램을 통칭한다. 스파이웨어는 사용자의 인터넷 사용 습관, 즉 즐겨 검색하는 단어, 자주 클릭하는 배너 광고 등을 수집해 마케팅에 활용하기 위한 만든 프로그램이다. 최근에는 애초의 목적과 달리 악성 코드와 결합돼 부정한 방법으로 금전적 이익을 취하는 업자들에 의해 이용되고 있다. 표 1은 신종 악성 코드 발견 통계이다.

표 1. 악성코드발견 통계

월	악성코드	스파이웨어
1 월	258	426
2 월	132	202
3 월	241	250
4 월	240	1,079
5 월	413	661
6 월	233	542
7 월	247	516
8 월	306	476
9 월	703	506
10 월	565	652
11 월	693	857
합 계	4,031	6,167

표 1의 조사에서 시간이 지날수록 신종 악성코드와 스파이웨어가 증가함을 보여 주고 있다. 안철수 연구소는 악성코드의 경우 전년도 동기 대비 50.9%, 스파이웨어의 경우 9.7%정도 증가했다고 밝혔다. 특히 허위 안티스파이웨어, MS 보안 취약점을 이용한 제로 데이 공격(Zero Day Attack) 등은 보안상의 취약한 부분을 공격하여 주요정보가 노출될 수 있는 위험을 갖고 있다. 제로 데이 공격(Zero Day Attack)은 취약점이 발견된 후 개발사의 공식적인 취약점 패치 발표 이전에 해당 취약점을 공격하는 악성코드나 스파이웨어가 제작되는 것을 말한다. 허위 안티 스파이웨어는 사용이 무료라고 광고해서 사용자를 현혹시킨 후에 사용자 컴퓨터에 프로그램을 설치하게 된다. '악성코드'를 잡는다는 명분으로 주로 스파이웨어를 진단하며 정상적인 파일까지 진단하거나 사용자 PC의 파일을 암호화해 불안감을 자극한다.

전 세계 운영체제의 대부분이 MicroSoft 사(이하 MS)의 Windows 운영체제 계열이다. MS의 Windows 와 Windows 용 응용프로그램도 보안 취약점이 발견되고 있다. 최근에 와서는 이러한 보안 취약점이 개발사에서 발견되어 패치 버전을 배포하기 전에 시스템을 공격당하는 일이 빈번하게 발생하고 있다. 이에 따라 MS는 보안관련 Web site를 운영하고 있다. 이 site는 보안관련 동향, 뉴스, 자체 개발 기술 등을 개시하여 이용에게 보안의 중요성을 알림과 동시에 컴퓨터 시스템의 보안 취약점을 매우는 역할을 하고 있다. MS는 STPP(전략적 보안지원 프로그램; Strategic Technology Protection Program)의 일환으로 일반적으로 틀리기 쉬운 보안 관련 설정을 간단히 확인하는 방법에 대한 고객의 요구에 따라 MBSA(Microsoft Baseline Security Analyzer)를 개발하여 제공하고 있다.

보안 취약점을 이용하는 공격자의 입장에서 시스템에 침입하기 위해 제일 먼저 하는 행위는 바로 해당 네트워크 및 시스템에 대한 보안 취약점 점검이다. 광범위한 보안 취약점 점검을 통해서 현재 어떠한 서버가 네트워크에 연결되어 있는지 또한 각각의 서버에서는 어떠한 서비스가 제공 중이며 이러한 서비스를 통해서 해당 시스템이 웹 서버인지, DB서버인지 혹은 메일 서버인지 등 어떠한 목적으로 운영되는지도 추측할 수 있게 된다. 반대로 서버 관리자의 입장에서는 자가 보안 취약점 점검을 통하여 자신이 운영하는 서버가 자신이 알지 못하는 사이 다른 포트가 열려 있는지 등을 확인할 수 있다.

초기의 보안 취약점 점검 툴을 들은 자가 보안 취약점 점검을 목적으로 개발되었다. 이러한 보안 취약점 점검 툴을 들이 해킹에 사용하고 있다.

보안 취약점 점검 관련 연구는 운영체제 개발 회사나 관련 업체를 중심으로 활발히 연구되고 있다. 또한 보안 취약점에 대해서 일부 단체를 중심으로 새롭게 발견된 시스템 보안 취약점에 대해서 사용자들에게 보고를 하고 있다.

3. 보안 취약점 점검 도구 설계

본 논문은 웹 환경에서 보안 취약점 점검 도구들을 이용하여 사용자 컴퓨터 시스템에 대한 보안 취약점을 점검하는 도구를 제안한다. 본 논문에서 제안하는 보안 취약점 점검 도구는 사용자 컴퓨터 시스템의 보안 취약점 점검 결과를 사용자에게 알려준다. 본 논문에서 설계한 보안 취약점 점검 도구는 다음 그림 1과 동작한다.

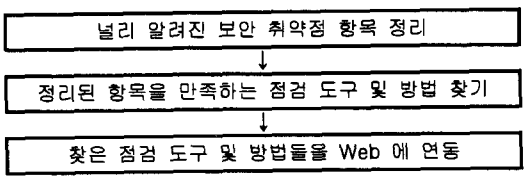

그림 1. 보안 취약점 점검 도구 동작 과정

그림 1은 보안 취약점 점검 도구 동작 과정을 보여준다. 보안 취약점 점검 도구를 설계하기 위하여 우선적으로 널리 알려진 보안상의 취약점에 대한 항목들을 정리한다. 기존의 보안 취약점항목들에 어떤 것이 있는지를 정리하여 이 기능들을 중심으로 보안 취약점 점검 도구의 기능을 설계한다.

표 2. 기존 보안 취약점 항목

점검분야	항 목
네트워크 구조식별	- Ping 스캔 - TCP 포트 스캔 - UDP 포트 스캔
웹	- 웹 서버 취약점
사용자 관련 보안	- 로그인 파라미터 점검 - 패스워드 관련 보안
파일 관련 보안	- 파일시스템 무결성 - Database
시스템 설정 관련 보안	- 네트워킹 서비스 설정사항 - 로그분석 - 레지스트리 설정 점검
OS 관련 보 안	- OS 패치 점검 - 바이러스 감염 점검

표 2는 기존 보안 취약점 항목을 정리한 것이다. 기

존의 보안 취약점을 비슷한 분야별로 나누어 정리하여, 본 논문에서 제안하는 보안 취약점 점검 도구 개발에 중요한 평가 기준으로 사용된다.

그리고 보안 취약점 항목을 만족하는 기존의 점검 도구들을 이용한다. 널리 알려진 보안 취약점에 대해서 정리한 항목에 만족하는 점검 도구를 찾아야 한다. 널리 알려진 보안 취약점에 대한 점검은 기본적으로 만족해야 하는 사항이기 때문에 이 기능을 만족시켜야 한다. 본 논문에서 제안하는 보안 취약점 점검 도구는 이러한 항목들을 만족하도록 한다.

또한 기존의 점검 도구들이 사용자 컴퓨터시스템을 점검할 수 있게 구성한다. 보안 취약점 점검 도구 중에서 공개적으로 사용가능한 도구를 활용하여 웹 환경에서 동작이 가능하게 설계한다. 그리고 이러한 도구들이 기능적으로 미약한 부분을 중심으로 통합 환경을 설계한다. 보안 취약점 점검 툴의 설치, 실행, 제거에 이르기 까지 모든 행위는 웹에서 이루어진다. 웹을 통하여 보안 취약점 점검 도구의 실행 결과를 출력한다.

웹의 구성은 기본이 되는 HTML 언어를 바탕으로 asp, java script, perl등을 사용하여 사용자의 시스템 환경에 영향이 적은 범용 언어들을 사용하여 개발한다.

4. 보안 취약점 점검 도구 구현

본 논문에서 제안한 보안 취약점 점검 도구의 기능을 구현하였다.

4.1. 보안 취약점 점검 도구 구현 환경

본 논문에서 제안하는 보안 취약점 점검 도구 개발에 사용된 컴퓨터 시스템은 다음 표 3과 같다.

표 3. 개발 컴퓨터 시스템 환경

컴퓨터 시스템 I	
CPU	Intel Pentium Zeon 2.8 GHz × 2
RAM	2 GB
하드디스크	SCSI 73 GB × 2
운영체제	Windows 2003 Server
컴퓨터 시스템 II	
CPU	Intel PentiumIV 2.8 GHz
RAM	512 MB
하드디스크	40 GB
운영체제	Windows XP Professional SP2

표 3에서와 같이 본 논문에서 제안하는 보안 취약점 점검 도구의 개발을 위하여 두 대의 시스템을 사용하였다. 컴퓨터 시스템 I 은 웹 서버의 역할을 하기 위한 컴퓨터 시스템이다. 다중 프로세서를 탑재하고 있으며, I/O연산의 속도를 빠르게 하기 위한 SCSI(small computer system interface)방식의 하드 디스크를 사용한다.

웹 서버로 IIS(Internet Information Services) 6.0을 사용하였다. 기본적으로 설치가 잠겨 있어 추가 설치를 하여야 사용할 수 있다. IIS 6.0 및 Windows Server 2003은 내결함성, 요청 대기열, 응용 프로그램 상태 모니터링, 자동 응용 프로그램 재활용, 캐싱 등을 통해 가장 신뢰성 있으며, 생산성 높고, 연결성이 뛰어난 통합 웹 서버를 제공한다.

4.2. 보안 취약점 점검 도구 구현

보안 취약점을 점검하는 도구들 중 네트워크 관련 즉, 원격으로 점검하는 점검 도구들의 대부분이 PORT 스캔 기능을 가지고 있다. PORT 스캔이란 것은 네트워크의 모든 IP 주소로 특정 packet을 특정 port에 발송한 후 특정 packet에 대한 응답이 오면 이를 해석하여 해당 네트워크의 특정 port에 연결이 되어 있는지를 판별할 수 있다. 따라서 해당 네트워크에서 어떠한 port가 열려 있는지를 알 수 있다.

본 논문에서 제안하는 보안 취약정 점검 도구 개발에 사용되는 PORT 스캔은 TCP Connect 스캔이다. TCP Connect 스캔은 해당 PORT 가 열려 있으면 열려 있다는 응답을 출력시켜준다. 해당 PORT 가 닫혀 있으면 닫혀 있다는 응답 메시지를 출력해준다.

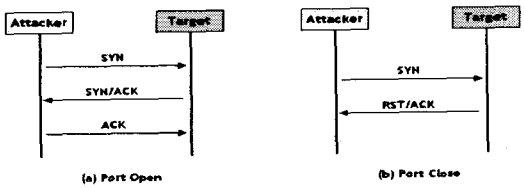

그림 2. TCP Connect 스캔 동작 과정

그림 2는 TCP Connect 스캔의 동작을 보여주는 그림이다. TCP Connect 스캔에서 target 시스템의 해당 PORT 가 열려 있을 경우에 target 시스템은 SYN/ACK packet(동기화 신호)을 전송하며, 포트가 닫혀 있는 경우에는 RST/ACK packet(응답 종료 신호)을 전송하게 된다.

보안 취약점 중에서 중요한 분야가 데이터베이스이다. 일반 사용자들의 경우에는 데이터베이스를 잘 사용하지 않는다. 하지만 기업의 경우에는 아무리 작은 기업이라도 데이터베이스를 사용한다. 이는 자료의 관리나 웹을 사용할 때 계정 관리 및 자료관리가 쉽기 때문이다. 이러한 데이터베이스를 이용 할 때 노출되기 쉬운 보안상의 취약점이 SQL Injection 이다. 이는 악의적인 데이터베이스 명령어 주입 공격으로 SQL Server의 프로그램을 사용할 때 생기는 취약점이다.

CGI 버그, 아파치 HTTP 데몬의 초기 배포판(release)은 phf, finger, test-cgi 같은 불안전한 CGI 프로그램을 포함하고 있다. /cgi-bin/phf 프로그램을 실행하는 것은 원격의 사용자가 'nobody' user로 웹서버상의 파일을 볼 수 있게 한다. /cgi-bin/finger 프로그램은 finger gateway로 동작하고 TCP.port 79에서 실행되는 fingerd service를 악용할 수 있는 것과 같은 방법으로

크래커가 호스트의 사용자를 finger할 수 있도록 한다. /cgi-bin/test-cgi 스크립트는 웹서버상의 파일 리스트를 얻는데 악용될 수 있다. 그러므로 공격자는 취약한 스크립트가 실행되고 있는 웹서버에 어떤 패키지가 설치되어 있는 지를 확인할 수 있다. 이런 웹서버의 취약점을 줄이기 위해서는 불필요한 샘플파일을 제거하거나 항상 최근의 버전의 웹서버를 설치하는 것이 좋다.

5. 보안 취약점 점검 도구 실험

본 논문에서 제안하는 보안 취약점 점검 도구를 실제 구현하여 동작 여부를 실험했다. 실험 방법은 표 2의 컴퓨터 시스템 I 에 웹 환경을 구축하고, 표 2의 컴퓨터 시스템 II에서 접속하여 컴퓨터 시스템 II의 보안 취약점을 점검 받는 형식으로 수행되었다.

다음 그림 3은 포트 스캔을 구현한 내용에 대한 실험 화면이다.

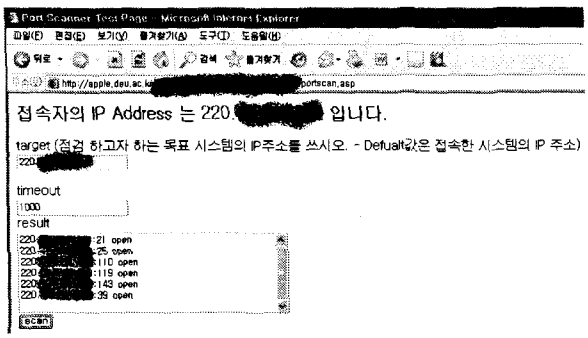

그림 3. 포트 스캔 취약점 점검 과정

그림 3은 컴퓨터 시스템 II의 포트 스캔 취약점을 점검하기 위한 보안 취약점을 점검하기 위한 웹 페이지 접속 화면이다. 보안 취약점 점검 시스템에서 접속자의 IP Address를 스스로 인지하여 그림 4의 아래 부분에 있는 [scan] 버튼을 클릭하면 "result" 부분에 점검 대상 시스템에서 열려진 포트 정보를 출력해준다. 이 정보는 현재 점검 대상 시스템에서 포트 공격의 가능성이 있는 열려진 포트 정보를 보여준다.

본 논문에서 설계한 보안 취약점 점검 도구 기능중 SQL injection 기능에 대한 동작 과정에 대한 실험은 다음과 같다.

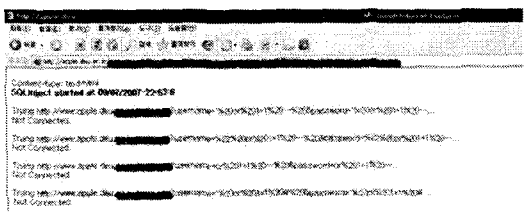

그림 4. SQL Injection 결과

그림 4는 SQL Injection 취약점을 점검한 결과를 보여준다. "Trying http ~~"로 되어 있는 부분은 실제로 해당 Target 시스템에 SQL Query문을 보내어 그 결과를 받아서 취약점 여부를 판단해 준다.

5. 결론

널리 알려진 보안 취약점들은 일반인들도 손쉽게 접할 수 있는 부분이 많은 만큼 서버를 관리하는 입장에서는 위험하다. 보안에 대한 비 전문가도 간단한 프로그램 몇 가지로 중요한 시스템에 접근이 가능하다. 본 논문은 웹을 이용한 보안 취약점 점검 도구를 개발한다. 본 논문은 보안 취약점 점검 도구들을 이용하여 웹상에서 사용자의 컴퓨터 시스템에 대한 점검을 통해서 결과를 보여주는 환경을 개발한다. 개발된 웹 보안 취약점 점검 도구는 쉽게 자신의 서버 컴퓨터의 취약점을 점검할 수 있다. 본 논문에서 구현된 보안 취약점 점검 도구의 기능은 포트 스캔, SQL injection 취약점 점검 기능으로 구성되어 있다. 포트 스캔 취약점 점검 도구의 기능은 열려져 있는 컴퓨터 시스템의 포트 점검을 통하여 불필요하게 열려져 있는 포트를 점검한다. 이런 점검을 통해서 보안 취약점을 사전에 차단한다. SQL injection 기능은 DB에서 SQL 구문의 취약점을 점검한다. 본 논문에서 제안하는 보안 취약점 점검 기능에 대해서 실험을 수행하였다.본 연구를 통하여 국제적인 크래커들의 경유지인 서버들을 보호한다. 본 논문의 연구가 마무리되면 여러 점검도구들이 하나의 점검 도구인 것처럼 서로가 연동이 되어 외부의 크래커들로부터 컴퓨터 시스템을 안전하게 보호할 수 있다.

참고문헌

[1] 기반보호팀, "네트워크 취약점 점검도구 선정 지침", p120-142, 한국정보보호진흥원
[2] 보안관리팀, "공개용 보안프로그램을 활용한 취약성 점검", p14-24, 한국정보보호진흥원
[3] http://microsoft.co.kr/
[4] YTN 김세호, "전문 해커 조직 적발, 국세청도 해킹", 2003.11.19
[5] http://home.ahnlab.com/
[6] http://sourceforge.net/
[7] http://itfind.or.kr/
[8] http://nilesoft.co.kr/
[9] 전계현, "웹 애플리케이션을 위한 보안 감리 점검 항목", 강원대학교 정보과학석사학위논문 2006. 8
[10] Matin Tamizi, "Automated Checking for Windows Host Vulnerabilities", ISSRE'05, 2005
[11] Anil Sharma, Jason R. Martin, "A Host Vulnerability Checking Tool" DARPA