# 웹 기반의 자동화된 네트워크 서비스 보안 취약성 분석 및 관리 시스템

임문희, 양진석, 김현구, 장범환, 정태명
성균관대학교 전기전자 및 컴퓨터 공학과
e-mail:{mhlim, jsyang, hkkim, bhchang}@rtlab.skku.ac.kr
tmchung@ece.skku.ac.kr

# Web-based Automated Network Service Security Vulnerability Analysis & Management System

Mun-Hee Lim, Jin-Suck Yang, Hyun-Ku Kim,
Beom-Hwan Chang, Tai Myung Chung
Dept. of Electrical & Computer Engineering Science,
SungKyunKwan University

요 약

인터넷이라는 거대한 네트워크에 연결되어 있는 시스템의 보안 상태를 주기적으로 점검하여 외부로부터의 공격에 취약한 부분을 보완하여 주는 일은 공격에 대한 방어를 위하여 가장 기본적인 일이다. 그러나 수많은 호스트가 상호 연결된 네트워크 관리 시스템에서 관리자가 각 시스템의 보안상 취약점을 전부 인지하고 이에 대한 보완을 수행하는 것은 상당히 어려운 일이다. 따라서 관리자의 수작업에 의한 취약점 분석 작업보다는 자동화된 관리 도구에 의한 취약점 분석이 효율적이다. 이에 본 논문에서는 네트워크 서비스인 HTTP, SMTP의 취약점을 원격에서 분석하는 시스템을 설계 및 구현하였다. WAVAMS는 에이전트와 독립된 mobile 코드의 이동에 의한 동적 분석 모듈의 추가로 가장 최근의 취약점을 신속하게 분석 할 수 있으며 확장성이 높다. 또한 웹 기반으로 설계되어 관리자가 용이하게 관리할 수 있다.

## 1. 서 론

정보 통신 시스템의 발달과 인터넷의 급속한 확산으로 인해 컴퓨터 시스템은 해킹이나 인터넷 웜 등의 많은 위험에 노출되어 있다. 또한 개별적으로 존재하던 호스트들을 상호 연결한 네트워크의 발달은 이러한 위험들이 개별 호스트에 머무는 것이 아니라, 네트워크로 연결된 각 시스템에 유해를 입힌다는 점에서 그 피해가 심각할 수 있다. 때문에 네트워크 관리자들은 네트워크에 연결된 각 시스템들의 보안 상태를 주기적으로 점검하여 인터넷이나 외부 네트워크로부터의 공격에 취약한 부분을 세심히 파악하고 사전에 방어하고 대처할 만반의 준비를 해야 한다. 그러나 정보시스템과 네트워크의 규모가 커질수록 관리자가 네트워크에 연결된 호스트들의 취약성을 수작업으로 관리하기는 어려운 일이다.

본 논문에서는 네트워크 관리 시스템에서 외부의 인터넷과 밀접하게 연관된 HTTP 프로토콜, SMTP 프로토콜에 대한 취약성을 자동으로 분석하는 서비스 관리 시스템(WAVAMS)을 설계 및 구현하였다.

WAVAMS은 웹 기반으로 구현되어 원격에 있는 관리자가 네트워크에 연결된 많은 호스트들의 관리를 용이하게 할 수 있다. 또한, 현재 시스템에 존재하는 HTTP, SMTP 취약점 분석 기능 뿐 아니라 분석 모듈의 동적 추가로 새롭게 발견된 취약점들에 대해 정확하고, 신속하게 대처할 수 있는 기능을 가지고 있다.

본 논문은 총 5장으로 구성되어 있다. 2장에서는 망 관리 시스템에서의 HTTP, SMTP 취약점 분석에 관련 연구들을 기술하고 3장에서 WAVAMS의 시스템 구성 요소들을 살펴보고 4장에서는 WAVAMS의 웹 기반의 관리자 인터페이스에 대해 살펴본 후 마지막 5장에서 결론을 내린다.

## 2. 관련 연구

앞서 언급했듯이 정보 시스템 내의 보안을 손상시키는 취약성이 존재하는지의 여부를 분석하는 것 은 시스템 보안의 가장 기본이 된다. 유닉스 시스템 은 환경설정 잘못으로 인한 보안 취약성과 이미 알려진 버그로 인해 많은 취약성을 내재하고 있으며 이러한 취약성을 이용한 시스템 침해가 증가하고 있다. 현재 이러한 시스템 내의 보안과 관계된 상태를 스캐닝 하여 보여주는 많은 도구들이 개발되어 있다.

### 2.1 기존의 취약성 분석 도구들

[표1]은 네트워크나 시스템에 존재한 취약성을 분석 및 진단하는 도구들 중 가장 많이 사용되고 있는 은 SATAN과 공개용 ISS에 대한 설명이다.

[표 1] 기존 취약성 분석 도구들

| 분석도구 | 기 능 | 단 점 |
|---|---|---|
| SATAN | • 네트워크를 통한 원격 시스템 보안 취약성 조사<br>• 결과 보고서 생성 | • 설치 시 여러 가지 기본 소프트웨어 환경 필요<br>• 설치의 복잡성<br>• 실행속도의 최적화 고려되지 않음<br>• 많은 자원 필요 |
| 공개용 ISS | • 원격 호스트의 포트 스캔<br>• 한번에 많은 호스트들을 한 꺼번에 스캔 | • 일반 사용자도 사용할 수 있으므로 해킹 악용 소지<br>• 취약성 결과에 대한 보완 방법 없음<br>• 불편하고 복잡한 사용자 인터페이스 |

### 2.2 WAVAMS

위에서 설명한 기존의 분석 도구들은 검사 대상 호스트에 설치되어 시스템의 취약성을 검사하는 것 에서는 본 시스템과 동일하지만 설치 방법, 실행속도, 사용자 인터페이스 면에서 단점이 존재한다.
본 논문에서 구현한 WAVAMS는 이러한 단점들을 보완하여 다음과 같은 장점을 가진다.

네트워크 에이전트 설치의 확장성이 높다.
취약성 분석 프로그램의 동적 모듈 추가 기능으로써 업데이트와 실행 속도가 빠르다.
웹 기반의 인터페이스를 제공함으로써 관리자가 위치에 구애받지 않고 관리자의 권한을 가지고 네트워크내의 각 시스템 취약성 검사를 수행 및 보고 받을 수 있다.

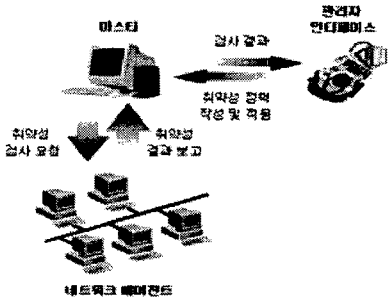
## 3. WAVAMS의 시스템 설계 및 구성

WAVAMS은 네트워크 관리에서 보안에 취약한 시스템의 상태를 검사하여 사전 공격에 대비할 수 있다. 이러한 WAVAMS의 주요 기능은 다음과 같다.

네트워크의 대상 호스트에 에이전트가 설치된다.
HTTP 관련 취약성 검사
SMTP 관련 취약성 검사
취약성 분석 모듈의 동적 추가로 기존 시스템의 수정 없이 취약성 분석 항목 추가
취약성 분석 항목의 선택을 위한 정책 설정 기능
지능형 마스터의 정책 관리기능을 사용한 자동화된 항목 설정
편리한 웹 기반의 관리자 인터페이스 제공

### 3.1 WAVAMS의 개요

본 논문에서 설계 및 구현한 WAVAMS는 관리자 인터페이스, 관리 서버인 마스터, 네트워크 에이전트로 구성된다. [그림 1]은 WAVAMS의 개요이다.

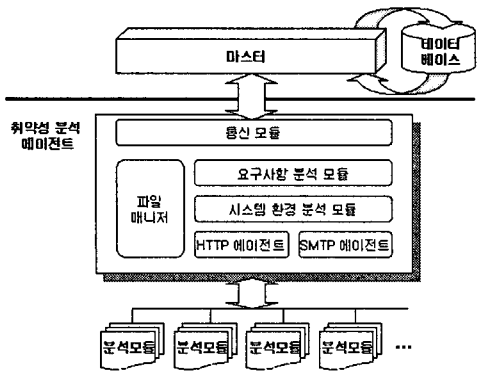



[그림 1] WAVAMS 개요

관리자는 네트워크에 연결된 시스템의 취약성을 검사하기 위해 마스터에 취약성 정책을 작성하고 적용시킨다. 취약성 정책은 어떤 서비스를 검사할 것인지, 또 어떤 항목들을 검사할 것인지에 대한 요구사항을 포함한다. 마스터는 관리자의 정책에 따라 에이전트에 취약성 검사 요청을 하면 각 에이전트는 검사 결과는 마스터에 전달한다.

### 3.2 시스템 설계

위의 개요에서 마스터는 입력된 호스트 시스템 과 에이전트 정보 등을 이용하여 검사 대상 호스트의 상태를 미리 점검한다. 이러한 정보들은 데이터베이스에 저장되어 있다. 점검 상태가 정상적이면 네트워크의 대상 호스트에 설치된 에이전트로부터 분석 모듈을 호출하여 취약성 분석 결과를 받아 원격에 위치한 관리자에게 보여준다. WAVAMS의 모듈 구조는 [그림 2]와 같이 설계되었다.




[그림 2] WAVAMS 모듈 구조

마스터는 원격 에이전트 시스템을 관리하고 에이전트의 보고 사항을 분석하여 관리자 인터페이스에 나타내며 다음과 같은 기능을 가진다.

- 취약성 분석 정보 저장
- 취약성 수집 정보 저장
- 에이전트 시스템의 등록 및 관리
- 분석된 취약성 정보를 에이전트 시스템들로 전달

데이터베이스는 관리자의 취약성 분석 정책, 취약성 분석 모듈 및 검사 항목, 상세 설명, 분석의 요청, 결과, 결과의 위험도, 해결 방법 등을 저장하여 취약성 검사 작업 수행 시 마스터에 분석 정보 및 이전 검사 결과 정보를 제공한다.

취약성 분석 에이전트는 네트워크에 연결된 호스트 시스템에 설치되는 에이전트 프로그램으로써 취약성 검사 방법, 유형, 해결 방법 등에 대한 검사를 수행한다.

[표 3] 에이전트 주요 클래스

| 클래스 명 | 주요 기능 및 역할 |
|---|---|
| VA_AGENT (취약성분석에이전트) | 취약점 분석 에이전트 프로그램의 메인 클래스 |
| UDP_COMM (통신모듈) | 관리서버(마스터)와 통신을 담당하는 클래스. 소켓을 이용하여 구현 |
| VgentRequestAnalyser (요구사항분석모듈). | 마스터에서 받은 명령을 분석하여 해당 모듈을 호출하는 클래스 |
| RunEnvChecker (시스템환경분석모듈) | 에이전트의 실행 환경을 검사하는 클래스 |
| FileManager (파일매니저) | 에이전트의 실행 환경을 검사하는 클래스, 파일들을 읽어 각 분석 모듈로 전달. |
| VA_HTTP (HTTP에이전트) | HTTP 관련 취약성 검사를 수행하는 클래스. 해당 취약성 검사 모듈을 호출 |
| VA_SMTP (SMTP에이전트) | SMTP 관련 취약성 검사를 수행하는 클래스. 해당 취약성 검사 모듈을 호출 |

[표 3]은 에이전트의 주요 클래스들을 나타내고 있으며 각 모듈은 java 언어로 구현되었다.

### 3.3 취약성 분석 에이전트

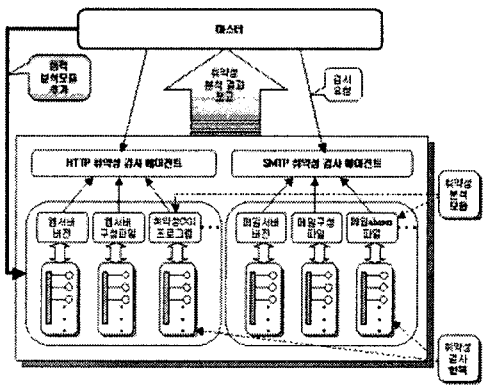
에이전트 시스템은 마스터 시스템이 취약성 정보를 수집, 분석하고자 하는 네트워크내의 호스트 시스템에 설치되어 마스터와 통신하며 취약성을 분석하는 모듈을 의미한다.

마스터에서 설정된 정책과 지시에 따라 해당 시스템의 HTTP, SMTP 취약성 검사 결과를 마스터에게 전송한다. [표 4]는 마스터와 에이전트간에 주고받는 메시지 항목들을 나타낸다.

[표 4] 마스터-에이전트 메시지 항목

| 항 목 | 상 세 설 명 |
|---|---|
| AgentID | 분석 에이전트 ID |
| ModuleID | 실행 모듈 ID |
| VulnerabilityID | 취약성 ID |
| VulnerabilityName | 검사할 취약점 이름 |
| CheckAgentName | 서비스 이름 (예:SMTP/HTTP) |
| ModuleDiscription | 취약성에 대한 상세 설명 |
| Remedy | 발견된 취약성 해결 방법 |
| Risk | 취약성의 위험 정도 |
| AgentIstalledFile | 실행 모듈의 파일 이름 |

WAVAMS의 가장 중요한 기능 중의 하나는 구현자에 의해 작성된 취약성 분석 모듈이 마스터로부터 네트워크이나 호스트에 설친 된 에이전트로 전달된다. 이러한 동적 모듈 추가 기능은 네트워크의 확장에 용이하며 대규모의 네트워크에서의 빠른 실행시간을 가진다. [그림 3]은 에이전트의 세부 구성요소를 나타내며 각 기능 설명을 포함한다.




[그림 3] 에이전트 구성요소

에이전트 프로그램 : 취약점을 분석하고자 하는 호스트 시스템에 설치되어 마스터와 통신하며 취약성을 분석하는 모듈

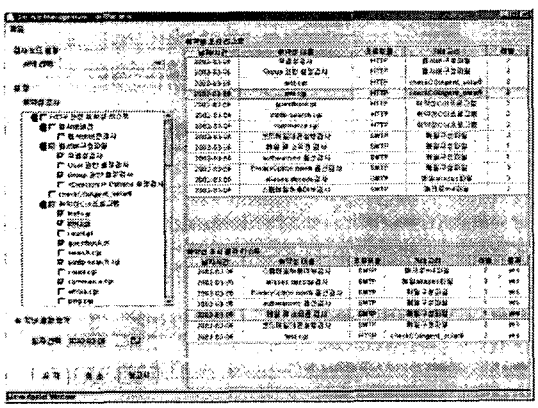
취약성 룰 집합 : 텍스트 파일로 구성되어 있으며 각 취약점의 분류 ID와 실행해야 할 취약점 분석 모듈 정보 등을 가지고 있는 설정 파일
취약성 분석 모듈 : 에이전트 프로그램에 의해 호출되며, 실제 취약성을 검사하는 모듈. 각 취약점의 특성에 따라 모듈들이 구성되며 새롭게 발견되는 취약점을 쉽게 추가하거나 분석을 위한 관리 구조를 용이하게 하기 위해 에이전트 프로그램과 분리하여 독립적인 실행 모듈로 구성되어 있으며 이것은 에이전트 프로그램에서 호출하여 사용

## 4. WAVAMS의 구현

WAVAMS는 분석되어 통신 모듈을 통해 관리자 인터페이스로 전달된 정보를 관리자가 효율적으로 관찰 및 관리할 수 있게 한다. 다음은 이 시스템이 구현된 환경 정보이다.

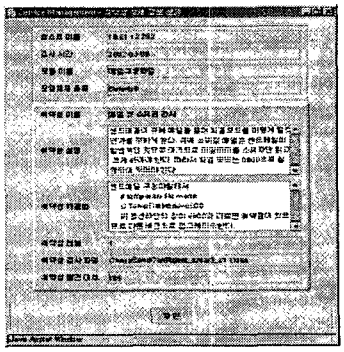
관리자 인터페이스 : Java
마스터, 에이전트 시스템 : Solaris 8
마스터, 에이전트 프로그램 : Java
취약성 분석 모듈 : Java, C, shell-script

관리자는 원격에서 관리자 권한을 가지고 관리 서버인 마스터에 접속한다. [그림 4]는 WAVAMS의 초기 화면이다.



[그림 4] 취약성 분석 초기화면

위 취약성 분석 초기 화면의 왼쪽 트리에 열거된 각 취약성 모듈로부터 대상 호스트 검사 모듈을 선택한다. 분석된 결과는 오른쪽 상단 프레임에 열거되며 이중 취약점이 발견된 모듈은 하단 프레임에 열거된다. 그리고 상단 혹은 하단 프레임에 리스트된 모듈중 하나를 선택했을 때 그 취약성에 대한 상세 정보가 [그림 5]와 같이 취약성 상세 정보 보기 창으로써 나타난다.



[그림 5] 취약성 상세 정보 보기

또한 WAVAMS은 분석된 취약성에 대해 관리자가 문서로 보관하거나 추후 관리가 용이하도록 분석 결과에 대한 보고서 작성 기능을 가지고 있으며 이렇게 작성된 보고서는 웹 브라우저 창으로 나타난다.

## 5. 결 론

내부 혹은 외부의 사용자로부터의 정보 시스템에 대한 침입은 그 시스템이 가지고 있는 보안 취약성을 공격함으로써 이루어진다. 따라서 네트워크 시스템 관리자는 시스템이 가지는 보안 취약성을 신속히 해결하여 공격의 단서를 제거해야 한다.

본 논문에서 구현한 WAVAMS는 네트워크내의 시스템 보안 취약성 검사 및 분석을 위해 관리자의 작업을 자동화하여 시스템의 안정성이 높다. 또한 취약성 분석 모듈의 동적 추가로 네트워크 에이전트의 확장성이 용이하며 모듈 실행 속도가 빠르다.

WAVAMS는 현재 네트워크 내에서 HTTP와 SMTP의 보안관리를 위한 취약성 분석을 수행하고 있지만, 추후 다른 서비스를 제공할 수 있으며, 또한 자동으로 취약성을 보완, 해결하는 모듈에 대한 연구도 진행될 것이다.

## 참고문헌

[1] 한국정보보호센터, "A Study on the Development of Countermeasure Technologies against Hacking and Intrusion on Computer Network System", 1999.

[2] Ivan Krsul, Eugene Spafford, and Mahesh Tripunitara, "Computer Vulnerability Analysis", May 6, 1998.

[3] G. Simson, and S. Gene, Practical Internet and UNIX Security, O'Reilly & Association, 1996.

[4] J. Carroll, Computer Security, 2nd Edition, Butterworth Pub., Stoneham, MA. 1987.

[5] 포항공과대학 전자계산소, Security+ for UNIX3, 1998.