제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

OVAL 기반의 리눅스 시스템 취약점 진단 도구 설계

이 희 재* 길민욱** 이 극*
*한남대학교 컴퓨터공학과 **문경대학 인터넷정보계열

요 약

OVAL은 시스템의 특성 및 설정 정보를 대상으로 하여 로컬 시스템상의 취약점을 탐지 할 수 있는 표준 언어로서 MITRE에서 제안하였다. OVAL은 취약점을 정의하는 익스플로잇 스크립트를 사용하지 않고 취약점을 탐지하는 XML 스키마와 SQL 질의문으로 구성되어있다. 본 논문에서는 OVAL을 사용하여 리눅스 시스템의 취약점을 탐지 할 수 있는 진단 도구를 설계한다.

A Design of Linux System Vulnerability Assessment Tool based on OVAL

Lee-Hui Jae*, Min Wook Kill**, Geuk Lee*

1. 서 론

취약점 진단 도구는 컴퓨터 시스템 상에 존재하는 취약점을 미리 진단하고 발견하여 적절한 해결방안 및 패치 정보를 제공함으로서 시스템을 더욱 안전한 상태로 유지할 수 있도록 해주는 보안 도구이다. 취약점 진단 도구의 종류로는 크게 호스트기반 진단 도구, 네트워크기반 진단 도구 그리고 특정 응용프로그램을 대상으로 취약점을 진단하는 어플리케이션 진단 도구 등이 있다. 이러한 취약성 진단 도구들은 주로 익스플로잇(exploit) 스크립트와 같은 공격 코드를 실행하여 시스템상의 취약점을 탐지한다. 그러나 각각의 취약성 진단 도구들은 취약점 탐지에 있어 공통된 기준을 적용하지 않으며 취약점 진단스크립트 또한 다양한 언어를 사용하여 구현하기 때문에 어떤 도구가 정확한 진단 결과를 제공하는지 판단하기가 힘들며 진단스크립트의 개발 및 지에 있어 많은 비용이 든다는 문제가 있다. 이러한 문제들을 해결하기 위해 MITRE는 OVAL을 제안하였다. OVAL(open vulnerability assessment language)은 시스템의 특성 및 설정 정보를 대상으로 하여 로컬 시스템상의 취약점을 탐지 할 수 있는 표준 언어이다. OVAL은 기본적으로 CVE의 취약점을 XML로 정의하며 이를 바탕으로 질의 문을 구성하고 실행함으로서 취약점을 찾아내는 방식을 취한다.

본 논문에서는 MITRE에서 제시한 OVAL을 사용하여 레드햇 리눅스 시스템의 호스트기반 취약성 진단 도구를 설계한다. 2장 관련 연구에서는 기존의 취약성 진단 도구와 OVAL을 분석하였고 3장에서는 OVAL의 리눅스 스키마를 바탕으로 한 데이터베이스와 시스템 정보 수집모듈을 설계하였으며, 4장에서는 결론을 내린다.

본 연구는 과학기술부 지역협력연구사업 (R12-2003-004-02003-0) 지원으로 수행되었음

2. 관련연구

2.1 취약점 진단 도구

취약점 진단 도구(vulnerability assessment tool)는 보통 취약점스캐너(vulnerability scanner) 또는 보안스캐너(security scanner)로 불리며 컴퓨터 시스템 상에 존재하는 취약점을 미리 진단하고 발견하여 해결방안 및 적절한 패치 정보를 제공함으로서 시스템을 더욱 안전한 상태로 유지할 수 있도록 해주는 보안 도구의 일종이다. 이러한 스캐너로는 점검 내용에 따라 호스트스캐너와 네트워크스캐너로 분류한다. 호스트스캐너는 각 운영 플랫폼에 설치되어 관리자의 부주의나 실수 또는 설정 등에서 발생할 수 있는 보안상의 문제점을 찾아내는데 이는 부적절한 파일 시스템의 권한, 불필요한 계정, 샌드메일과 같은 버그가 많은 프로그램 등 해커들이 이용할 수 있는 모든 취약점 및 위험 요소들을 진단하며, 네트워크스캐너는 외부의 해커가 공격 가능한 모든 취약점을 진단한다.

취약점스캐너는 보통 익스플로잇(exploit)과 같은 탐지스크립트를 사용하여 해당 취약점을 찾아낸다. 그러나 현재 사용되는 상용 및 공개 도구들은 취약점 탐지에 있어 각각의 기준을 적용하며 스크립트 또한 다양한 언어를 사용하여 작성되기 때문에 탐지 결과에 대한 신뢰도가 떨어진다는 문제점이 있다. [표 2-1]은 공개용 취약점 진단 도구와 탐지 스크립트에 사용된 언어를 보여준다.

[표 2-1]

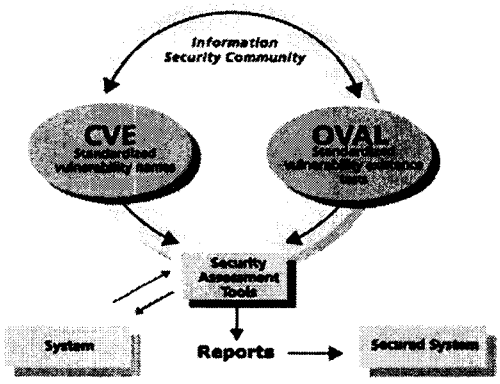
도구명	분류	사용된 언어
Tiger	호스트스캐너	C, 쉘 스크립트
COPS	호스트스캐너	C, 쉘 스크립트
Nessus	네트워크스캐너	NASL
SARA	네트워크스캐너	C, Perl
SAINT	네트워크스캐너	C, Perl
sscan	네트워크스캐너	C
vlad	네트워크스캐너	Perl

취약성 탐지는 보통 탐지 모에서 수행되는데 각각의 취약성을 탐지하는데 있어 익스플로잇 코드와 같은 탐지스크립트를 사용한다.

2.2 OVAL

OVAL(open vulnerability assessment language)은 로컬시스템 상에서 시스템이 가지고 있는 특성 및 설정정보들을 기반으로 취약점을 찾아내기 위한 표준 언어로서 미국의 비영리 단체인 MITRE에서 제안하였으며, 현재 학계, 정부기관 그리고 IBM, 마이크로소프트, CISCO 등 관련 업계의 보안전문가들로 구성되어 표준화작업을 진행 중이다. OVAL은 XML과 SQL을 사용하여 취약점을 정의하고 취약점을 찾아내기 위한 질의 문을 작성한다.

OVAL은 취약점 탐지에 있어 익스플로잇 스크립트 등을 전혀 사용하지 않는데 이는 XML 및 SQL과 같은 가독성 있는 언어를 사용함으로서 보안전문가들이 취약점 탐지에 대한 토론을 쉽고 원활히 할 수 있고 관리자 및 일반 사용자들도 쉽게 이해할 수 있기 때문이다. (그림 2-1)은 OVAL을 적용한 진단 도구의 동작과정을 보여준다.



(그림 2-1) OVAL의 동작과정

기존의 도구들은 익스플로잇 스크립트와 같은

코드를 사용하지만 OVAL은 이와 같은 기능을 하는 OVAL 질의 문을 사용하며, 이는 CVE를 기반으로 작성된다. OVAL을 사용하는 진단 도구는 먼저 시스템의 관련 정보를 수집하여 이를 데이터베이스화한 후 OVAL 질의 문을 실행하여 취약점을 찾아내고 보안관리자는 발견된 취약점에 대하여 적절한 패치를 적용함으로서 시스템을 안전한 상태로 유지할 수 있게 된다.

2.2.1 OVAL 스키마

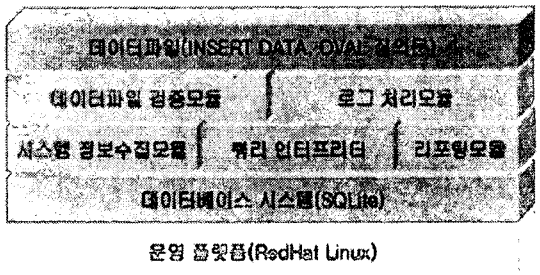
OVAL은 취약점을 정의하고 탐지하기 위한 프레임워크로서 XML 스키마와 SQL 스키마로 구성되어있다. XML과 SQL 언어는 컴퓨터 시스템이 해석할 수 있을 뿐만 아니라 시스템관리자와 보안 분석가 등과 같은 보안전문가들이 쉽게 읽을 수 있어 취약점을 가장 논리적이며 명확하게 정의할 수 있다는 장점이 있다. XML 스키마는 취약점을 정의하기 위한 것으로서 공통 스키마와 각 운영 플랫폼을 위한 스키마로 구성된다. 공통 스키마는 취약점을 기술하기 위한 기본 정보를 표현하며, 운영 플랫폼에 대한 스키마는 각 운영 플랫폼마다 점검해야 하는 요소들을 표현하는 스키마로서 현재 OVAL은 윈도우계열 및 솔라리스, 리눅스 등의 유닉스 계열 운영체제에 대한 스키마를 공개하였다.

3. 설계

3.1 시스템 구성도

본 논문에서는 OVAL에서 제공하는 스키마 중 레드햇(RedHat) 리눅스 계열의 스키마를 기반으로 하는 취약점 진단 도구를 설계하며, 구성도는 (그림 3-1)과 같다.

데이터 파일은 "INSERT DATA"와 "OVAL 질의문"으로 구성되어 있다. INSERT DATA는 시스템 정보수집 모듈이 수집해야 할 데이터들의 목록을 포함하고 있다. OVAL 질의문은 쿼리 인터프리터의 입력 데이터로 수집된 시스템정보에서 취약점을 찾아내기 위한 조건들이 SQL 질의문 형태로 작성되어 있다.



(그림 3-1) 시스템 구성도

데이터파일 검증 모듈은 주어진 데이터 파일이 정확한지 검증하는 역할을 하며, 로그처리 모듈은 시스템에서 발생 할 수 있는 에러 등을 처리한다. 시스템 정보수집 모듈은 INSERT DATA를 기반으로 환경설정 정보, 소프트웨어 설치 정보 그리고 파일 및 프로세스 정보 등 다양한 시스템 정보를 수집하여 데이터베이스를 갱신하는 역할을 한다. OVAL 질의문은 SQL 언어로 작성되기 때문에 OVAL 기반의 도구들은 적절한 데이터베이스시스템(DBMS)을 사용해야 한다. 본 논문에서는 데이터베이스 시스템으로서 파일 기반의 SQLite를 사용하며, [표 3-1]에는 SQLite의 일반적인 특징들을 나타내었다.

[표 3-1] SQLite 특징

항목	내용
SQL 지원	대부분의 SQL92 Syntax 지원
속도	일반적인 명령 수행에 있어 기존의 DBMS들 보다 2배 이상 빠름
규모	25K 라인 정도의 C 코드로 이루어진 매우 경량의 데이터베이스 시스템
데이터베이스	파일 하나로 데이터베이스의 모든 것을 포함
운영환경	다른 라이브러리의 도움 없이 실행가능

3.2 데이터베이스 설계

OVAL 기반의 시스템에서 정보 수집모듈에 의해서 수집된 시스템 데이터들은 데이터베이스에 저장되며, OVAL 질의문은 이 데이터베이스에 질의를 하여 해당되는 취약점을 찾아낸다. 데이터베이스의 테이블은 각 운영 플랫폼에 대한 OVAL 스키마를 통하여 구성되는데 레드햇 계열의 리눅스 운영체제는 다음과 같이 구성된다.

3.2.1 파일 메타데이터

파일의 메타데이터 정보를 저장하기 위한 스키마로서 [표 3-2]와 같은 항목들로 구성된다.

[표 3-2] 파일 메타데이터

항목	내용
FilePath	파일의 절대 경로
FileType	디렉토리, 정규파일, 장치파일 등
UserID	파일의 소유자
GroupID	파일이 속한 그룹
시간	접근시간(Atime), 상태 변경시간(Ctime), 데이터 변경시간(Mtime)
MD5	파일에 대한 MD5 해시
퍼미션 비트	SUID, SGID, STICKY, UREAD, UWRITE, UEXEC, GREAD, GWRITE, GEXEC, OREAD, OWRITE, OEXEC

3.2.2 인터넷 서버데몬

[표 3-3] 인터넷 서버데몬

항목	내용
Protocol	실행중인 데몬의 서비스 프로토콜(TCP 또는 UDP)
IP 주소	로컬 및 리모트 호스트의 IP 주소
포트번호	로컬 및 리모트 호스트의 포트
UserID	서비스 데몬을 실행한 사용자 ID
PID	서비스 데몬의 프로세스 ID
ProgramName	서비스 데몬의 이름

샌드메일, 웹 서버 등의 인터넷 서비스 데몬의 상태를 정보를 저장하기 위한 스키마로서 [표 3-3]과 같은 항목들로 구성되며, 리눅스의 "netstat-tuwlnpe" 시스템 명령어를 통하여 쉽게 얻을 수 있다.

3.2.3 패스워드 및 쉐도우 파일 정보

유닉스 계열의 운영체제는 모든 사용자의 패스워드 정보를 passwd 와 shadow 파일에 기록·관리하는데 [표 3-4]와 [표 3-5]는 이를 위한 스키마를 나타낸다.

[표 3-4] passwd 파일정보

항목	내용
Username	사용자의 로그인 ID
Password	암호화된 패스워드
UserID	사용자 식별번호
GroupID	사용자에 대한 그룹 식별번호
GCOS	사용자의 상세 정보
HomeDir	사용자의 홈 디렉토리
LoginShell	사용자의 로그인 쉘

[표 3-5] shadow 파일정보

항목	내용
Username	사용자의 로그인 ID
Password	암호화된 패스워드
ChgLst	마지막 패스워드 변경일
ChgAllow	패스워드 변경 가능일
ChgReq	-
ExpWarn	패스워드 만기 시 경고
ExpInact	사용자의 홈 디렉토리
ExpDate	사용자의 로그인 쉘
PswFlag	사용자의 로그인 쉘

3.2.4 프로세스 정보

시스템 상에서 실행되고 있는 모든 프로세스들의 정보를 저장하기 위한 스키마로서 [표 3-6]과 같다.

[표 3-6] 프로세스 정보

항목	내용
UserID	프로세스를 실행한 사용자의 ID
PID	실행중인 프로세스의 식별번호
PPID	부모 프로세스의 식별번호
Priority	프로세스 우선순위
StartTime	프로세스가 처음 시작된 시간
TTY	터미널
ExecTime	시작된 이후 현재까지의 경과 시간
Command	프로세스 실행 명령어

3.2.5 RPM 설치 및 버전 정보

RPM은 레드햇 계열의 리눅스에서 소프트웨어의 설치와 업그레이드 및 삭제 등을 위한 패키지 관리자이다. [표 3-7]과 [표 3-8]은 설치된 RPM 정보와 관련된 스키마를 나타낸다.

[표 3-7] RPM 정보

항목	내용
RPMName	RPM 패키지의 이름
RPMEpoch	-
RPMVersion	패키지 버전
RPMRelease	패키지의 릴리즈 번호
RPMArch	아키텍처

[표 3-8] RPM 버전 비교

항목	내용
RPMName	RPM 패키지의 이름
RPMTestedEpoch	-
RPMTestedVersion	패키지 버전
RPMTestedRelease	패키지의 릴리즈 번호
RPMInstalledVersion	운영 플랫폼

[표 3-7]은 시스템에 설치되어있는 RPM 패키지에 대한 정보이며, [표 3-8]은 취약한 패키지의 RPM 정보와 현재 설치되어있는 RPM 정보를 비교한 테이블이다. 결국 OVAL 질의문은 이 테이블에서 취약한 패키지를 찾게 된다.

3.2.6 운영 플랫폼 정보

운영 플랫폼에 대한 정보는 "uname -a" 시스템 명령어를 통하여 얻을 수 있으며 이를 위한 스키마는 [표 3-9]와 같다.

[표 3-9] 운영플랫폼 정보

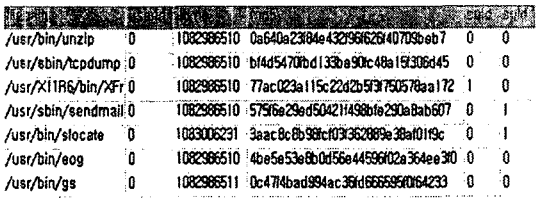
항목	내용
OSName	운영체제 이름
NodeName	노드 명 또는 호스트 명
OSRelease	운영체제의 릴리즈 번호
OSVersion	운영체제의 버전
MachineClass	-
ProcessorType	프로세서 타입

3.2 시스템 정보수집 모듈

시스템 정보수집 모듈은 취약점을 찾아내는데 필요한 시스템 정보를 수집하여 3.2의 데이터베이스에 갱신하는 역할을 한다. 이 모듈이 수집해야할 데이터들은 INSERT 데이터에 명시되어 있다. OVAL은 시스템 정보를 수집하는데 걸리는 시간을 절약하기 위해 INSERT 데이터를 사용한다. 즉, 설치된 모든 패키지 또는 파일 정보를 수집하는 것이 아니라 실제 진단에 필요한 항목들만 INSERT 데이터에 명시한다. 시스템 정보수집 모듈은 다음과 같이 총 8개의 모듈로 구성된다.

- ☞ 파일 메타데이터 수집 모듈
- ☞ 인터넷 서버데몬 정보 수집 모듈
- ☞ RPM 정보 수집 모듈
- ☞ RPM 버전 비교 모듈
- ☞ 프로세스 정보 수집 모듈
- ☞ 패스워드 파일 정보 수집 모듈
- ☞ 쉐도우(shadow) 파일 정보 수집 모듈
- ☞ 운영플랫폼 정보 수집 모듈

(그림 3-2)는 파일의 메타데이터 정보 수집하는 모듈의 실행 결과로서 파일 정보가 데이터베이스에 갱신된 화면이다.



/usr/bin/unzip	0	1082986510	0a640a23f84e432f96f626f40705beb7	0	0
/usr/sbin/tcpdump	0	1082986510	bf4d5470fbd133ba90c48a15f306d45	0	0
/usr/X11R6/bin/XFr	0	1082986510	77ac023a115c22d2b5f3f750578aa172	1	0
/usr/sbin/sendmail	0	1082986510	575f6e29ed5042f498bfe290a8ab607	0	1
/usr/bin/slocate	0	1083006231	3aac8c8b98fcf0f362089e38af01f9c	0	1
/usr/bin/eog	0	1082986510	4be5e53e8b0d156e44596f02a364ee30	0	0
/usr/bin/gs	0	1082986511	0c47f4bad994ac36fd6665950f64233	0	0

(그림 3-2) 파일에 대한 메타데이터 정보

3.3 쿼리 인터프리터

쿼리 인터프리터는 데이터파일에 저장되어 있는 OVAL 질의문을 정보 수집모듈에 의해 갱신된 데이터베이스에 질의하여 취약점의 존재 유무를 찾아내는 역할을 한다. 이때 질의문이 정상적으로 수행되면 해당 취약점에 대한 CVE ID를 반환하게 되고 리포팅 모듈에 의해서 (그림 3-3)과 같은 결과를 출력하게 된다.

```
[root@redhat9 oval_project]# ant run
java -Djava.library.path=. my.project.oval.Main
WARNING: using non-UTF SQLite engine
Parsing data file
Updating oval schema
Updating insert data
Creating probe vector
Collect ps info.
Collect inet listening servers...
Collect uname info...
Collect passwd info...
Collect shadow info...
Collect RPM info...
Collect RPMVersionCompare info...
Collect file attributes..
    Vulnerability is found : CAN-2003-0686
    Vulnerability is found : CAN-2003-0615
    Vulnerability is found : CAN-2003-0282
    Vulnerability is found : CAN-2004-0083
    Vulnerability is found : CAN-2004-0084
    Vulnerability is found : CAN-2004-0106
    Vulnerability is found : CAN-2003-0989
    Vulnerability is found : CAN-2004-0055
    Vulnerability is found : CAN-2004-0057
Vulnerability is not found : CAN-2003-0140
Vulnerability is not found : CAN-2003-0195
Vulnerability is not found : CAN-2003-0539
Vulnerability is not found : CAN-2003-0081
```

(그림 3-3) 수행결과

3. 결 론

논 논문에서는 OVAL 기반의 리눅스 시스템 취약점 진단 도구를 설계 하였다. OVAL은 MITRE에서 제안한 취약점 탐지를 위한 표준 언어로서 CVE에 이른 두 번째 표준화 진행 절차라는 점에서 큰 의미가 있다. 현재 OVAL은 몇몇 운영 플랫폼만을 위한 스키마를 지원하고 질의문 역시 지속적으로 개발되고 있는 상태 이지만 이러한 것들은 시간이 지나면 해결되는 문제들이다. 따라서 취약점 진단에 표준화된 OVAL을 적용함으로서 많은 비용을 절감 할 수 있을 것이라 예상된다.

참고문헌

[1] 김정희, "컴퓨터시스템 취약성평가 국제표준화 동향", 한국정보보호진흥원 해외정보보호동향 2003년 6월호

[2] "Inttoduction ot OVAL", http://oval.mitre.org/documents/

[3] http://oval.mitre.org