오픈 소스를 이용한 침입자 감시시스템 구축

최병철*, 서동일*
*한국전자통신연구원 사이버테러기술분석팀
e-mail : corea@etri.re.kr, bluesea@etri.re.kr

Construction of Intrusion Inspection System Using the Open Sources

Byeong-Cheol Choi*, Dong-Il Seo*
*Anti-CyberTerror Team, ETRI

요 약

본 논문은 공개 소프트웨어를 이용하여 침입자 감시시스템을 효과적으로 구축하는 방법을 제안한다. 침입자 감시시스템의 구축에는 Linux, Apache, PHP, MySQL, Snort, ACID, Tcpwrapper 그리고 phpMyAdmin 이 사용되었으며, 침입자 감시시스템의 자체 보안을 위해서 httpd.conf 를 사용한 홈 디렉토리 접근제어 및 Tcpwrapper 의 inetd 방식의 데몬 접근제어를 통해서 관리자만이 시스템에 접근할 수 있도록 하였다. 본 논문의 실험 및 결과에서는 실제 테스트베드를 구축하고, 취약성 점검 툴인 Nessus 를 이용하여 침입자 감시시스템을 공격하였다. 실험 결과는 ACID 를 통해서 웹상에서 효과적으로 분석할 수 있었다. 본 논문은 효율적인 네트워크 보안 관리 및 침입자를 감시 및 역추적하기 위해서 제안된 것이다.

1. 서론

인터넷의 발전과 함께 정보화시대로 접어들면서 정보화 역기능이 심각한 문제점으로 대두되고 있으며, 현 시점에서 침입 차단 시스템과 더불어 침입 탐지 시스템의 중요성이 높아지고 있다. 이러한 침입 탐지 시스템은 상용으로 제공되는 것도 있지만, Snort 와 같이 오픈 소스로 제공되는 것도 있다. Snort 는 네트워크 기반의 침입 탐지 시스템이며, 이러한 공개 소프트웨어도 그 활용을 제대로 하면 해킹 사고 예방에 큰 역할을 할 수 있다고 판단된다. 특히, Snort 는 이것을 효과적으로 활용할 수 있는 많은 가능성을 가지고 있으며, 이와 관련한 공개 소프트웨어도 연구기관 및 학교에서 많이 개발하였다[9,10].

본 논문에서는 이러한 오픈 소스를 어떻게 잘 구성하여 효과적으로 침입자를 감시할 수 있는 시스템을 구축할 수 있는가에 대한 방법을 제안한다. 또한, 구축한 시스템의 자체 보안을 위한 일반적인 방법을 제시한다[1,2,3].

본 논문에서 사용한 오픈 소스는 다음과 같다.

- OS - Linux 7.1
- Web Server – Apache
- CGI Module – PHP 4.0
- Database – MySQL
- NIDS – Snort 1.7
- GUI – ACID
- DB Console – phpMyAdmin
- F/W - Tcpwrapper

본 논문은 오픈 소스를 이용하여 리눅스 시스템에서 침입자 감시시스템을 구축하고, 웹 서버를 통해서 그 결과를 쉽게 감시할 수 있는 시스템을 구축하는 방법을 제안한다. 또한, 침입자 감시시스템의 자체 보안을 위해서 http 데몬 설정을 통한 디렉토리 접근 제어와 Tcpwrapper 를 통한 inetd 방식의 서비스의 접근 제어를 사용한다. 따라서, 본 논문은 오픈 소스를 이용하여 침입자 감시시스템을 구축함과 동시에 관리자만이 시스템에 접근할 수 있도록 시스템 자체의 보안을 위한 방법을 함께 제안하고 있다.

본 논문은 기업, 기관 그리고 학교에서 네트워크 보안을 위해서 공개 소프트웨어를 이용하여 쉽게 해커의 침입을 실시간으로 감시할 수 있는 방법을 제안하고 있으며 그 구축 과정을 상세히 기술하고 있다. 또한, 본 논문에서 제안한 침입자 감시시스템은 침입자 역추적의 기반이 되는 기술인 침입 탐지 시스템

구축을 효과적으로 하는 방법을 기술하고 있다.

본 논문의 전체구성은 1 장의 서론, 2 장의 침입 탐지 시스템에 대한 소개, 3 장의 침입자 감시시스템 구축, 4 장의 실험 및 결과 그리고 마지막 5 장의 결론으로 구성되어 있다.

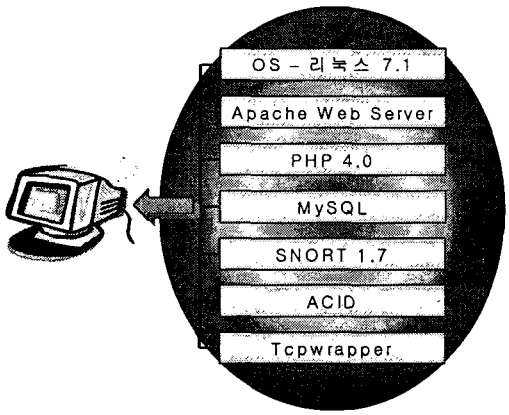

그림 1. 침입자 감시시스템 구조

2. 침입 탐지 시스템 (Intrusion Detection System)

침입 탐지 시스템[4,5,6,7,8]은 크게 호스트기반과 네트워크 기반으로 나눌 수가 있으며, 판단 기준에 따라서 이상탐지와 오용탐지로 나눌 수가 있다. 오용탐지에서는 주로 규칙에 기반한 패턴 매칭 방법을 주로 사용하며, 이상탐지에서는 확률적인 방법을 주로 사용한다. 침입 탐지 시스템은 ISO/IEC 와 IETF IDWG 에서 표준화가 진행 중에 있다. 다음의 그림은 일반적인 침입 탐지 시스템의 분류에 관한 것이다.

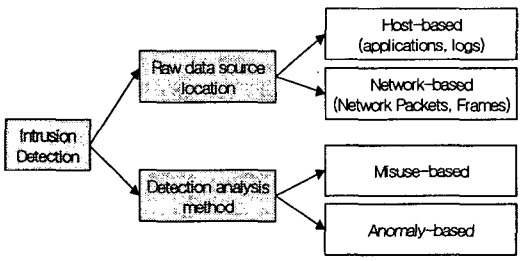

그림 2. 침입탐지시스템 분류

본 논문에서 사용한 Snort 는 네트워크 기반의 패턴 매칭 방법을 사용하는 침입 탐지 시스템이며, 소스를 공개하고 있으며 확장성이 매우 뛰어나다. 또한, 이와 관련하여 ACID, SnortSnarf 와 같은 Snort 를 효과적으로 활용할 수 있도록 공개 소프트웨어들이 많이 제작되고 있다.

3. 제안된 침입자 감시시스템 구축 방법

본 장에서는 제안된 침입자 감시시스템의 구축의 세부 단계를 자세히 기술한다. 침입자 감시 시스템 구축은 다음과 같은 순서로 진행된다.

- 운영체제 설치 – Linux 7.1
  시스템을 설치한 후 불필요한 서비스는 모두 제거하는 것이 바람직하다.

- 웹 서버 설치 – Apache Web Server
  httpd.conf 파일을 수정하여야 한다. 특히, 홈 디렉토리의 접근을 관리자만 허용한다.

- DB 설치 – MySQL
  # tar zxvf mysql-version.tar.gz
  # configure --prefix=/usr --with-charset=euc_kr
  # make; make install
  /usr/local/mysql/bin 디렉토리에서
  # ./mysql_install_db
  # ./safe_mysqld –language=korean &
  # ./mysqladmin –u root password test1234
  (root 의 패스워드는 꼭 변경하여야 한다.)

- Snort DB 를 사용할 수 있는 사용자 추가한다. 본 연구에서는 snort 라는 사용자를 추가한다.

- CGI 모듈 설치 – PHP 4.0
  # tar zxvf php-version.tar.gz
  # configure --with-mysql=/usr --enable-bcmath --enable-sockets
  # make; make install

- NIDS 설치 – Snort 1.7 (Snort 1.8 은 DB 내용의 차이로 ACID 를 아직 사용할 수 없다.)
  # tar zxvf snort-1.7.tar.gz
  # configure --prefix= /etc/snort --with-mysql
  # make; make install
  # mkdir /var/log/snort
  # mv *lib /etc/snort; mv snort.conf /etc/snort
  # vi /etc/snort/snort.conf
  (네트워크 설정 및 DB 설정을 한다.)

- Snort DB 생성 및 Snort DB 의 테이블 생성
  mysql> create database snort; (snort DB 생성)
  /temp/snort-1.7/contrib. 디렉토리에서
  # mysql –u snort –p < create_mysql (테이블생성)

- ACID 설치
  # tar zxvf acid-version.tar.gz
  # mv acid /var/www/html
  # cd /var/www/html/acid
  # vi acid_conf.php (Snort DB 접근 설정)

- PhpMyAdmin 설치
  # tar zxvf phpMyAdmin-version.tar.gz
  # mv phpMyAdmin /var/www/html

- Tcpwrapper 설치
  inetd.conf, host.allow, host.deny 파일을 수정하

여 inetd 방식의 서비스의 접근을 관리자만 할 수 있도록 설정한다.

- 기타
  - ADODB (database abstraction library)
  - GD (graphing functionality for phplot)
  - PHPlot (graphing library)

본 논문에서 제안된 방법은 공개 소프트웨어를 이용하여 효과적인 침입자 감시 시스템을 구축하고, 구축한 시스템의 자체 보안까지도 고려한 방법이다.

다음의 환경설정 파일의 주요 세부 설정이다.

- httpd.conf 설정
- inetd.conf, host.deny, host.allow 설정
- snort.conf 설정
- acid_conf.php 설정

1. httpd.conf 설정

```
<Directory "/var/www/html">
    Order deny,allow
    Deny from all
    Allow from 129.254.xxx.xxx
</Directory>
```

2. inetd.conf 설정

```
ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin
/in.ftpd
telnet stream tcp nowait root /usr/sbin/tcpd /usr/sbin
/in.telnetd
```

host.allow 및 host.deny 설정

```
host.allow => ALL : 129.254.xxx.xxx
host.deny => ALL : ALL
```

3. snort.conf 설정

```
# database: log to a variety of databases
  output database: log, mysql, user=snort password
  =xxxx1234 dbname=snort host=localhost
```

4. acid_conf.php 설정

```
$alert_dbname     = "snort";
$alert_host       = "localhost";
$alert_port       = "3306";
$alert_user       = "snort";
$alert_password = "xxxx1234";
```

위의 환경설정 파일을 정확하게 설정하여야 효과적인 침입자 감시시스템을 활용할 수 있다. 물론, 이러한 환경설정이 제대로 되지 않으면 전체적인 시스템의 운용 및 동작에 문제가 발생할 것이다.

본 논문에서는 httpd.conf 의 웹 홈 디렉토리 접근을 관리자의 IP 로 설정하였고, telnet 과 ftp 등과 같은 inetd 방식으로 동작하는 데몬들은 Tcpwrapper 로 접근 제어를 하였다. 이것은 침입자 감시시스템 자체의 보안을 위한 것이다. 또한, snort.conf 와 acid_conf.php 는 데이터베이스를 사용하기 위한 설정을 추가하는 부분이다. 본 연구에서는 MySQL 데이터베이스를 사용하여 Snort 의 경보 로그를 저장하도록 하였다. 만약, 파일 형태로 저장된 경보를 사용하려면 SnortSnarf 를 사용하여야 한다.

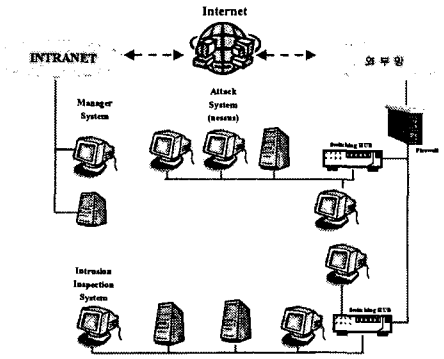

그림 3. 테스트베드 구성

4. 실험 및 결과

본 장에서는 제 3 장에서 구축한 침입자 감시시스템을 실험을 하고 그 결과를 분석한다. 실험에 사용한 공격 툴로는 Nessus 를 사용하였다. Nessus 는 시스템 취약성 분석 툴이며, 여러 가지 공격 테스트를 수행한다. 이 공격 및 감시 실험을 위해서 다음과 같은 테스트베드를 구축하였다.

그림 3 에서는 테스트베드의 구성을 나타내었다. 관리자가 존재하는 네트워크, 공격자가 존재하는 네트워크 그리고 침입자 감시시스템이 존재하는 네트워크의 3 개의 작은 네트워크로 구성되어 있다. 관리자는 윈도우 환경에서 원격으로 모든 서버에 접속 가능하며, 특히 침입자 감시시스템은 오로지 관리자에게만 telnet. http 그리고 ftp 를 허용하게 된다. 이러한 테스트베드의 구성은 일반적인 네트워크 공격형태를 고려하여 구축된 것이며, 테스트베드에서 자체 방화벽이 있기 때문에 이 테스트베드는 외부에서는 공격이 불가능하다. 참고적으로 스위치를 사용하기 때문에 포트 미러링을 하여야 로컬 네트워크 전체의 침입을 감지할 수 있다. Snort 를 여러 네트워크에 설치하여 동시에 ACID 에서 관찰할 수도 있다. ACID 는 여러 개의 센서(IDS)를 동시에 관찰할 수 있도록 설계된 것이다.

실험 순서는 다음과 같다.

- 침입자 감시시스템 구축
- 환경 설정
- 테스트베드구성
- Snort 데몬 구동
- Nessus 공격 실시
- ACID 로 결과 보기
- 결과 분석

/etc/snort 에서 수행
snort –d –h 129.254.125.0/24 –l ./ -c snort.conf 또는
snort –d –D –h 129.254.125.0/24 –l / -c snort.conf

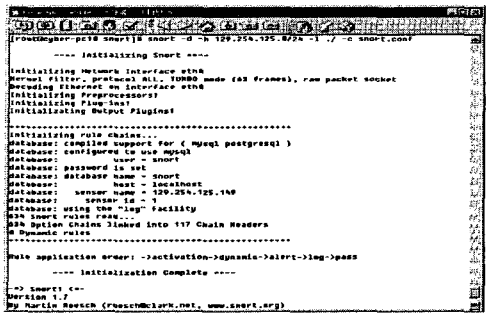

그림 4. Snort 데몬 구동

nessus (Nessus 가 설치된 다른 시스템에서 공격)

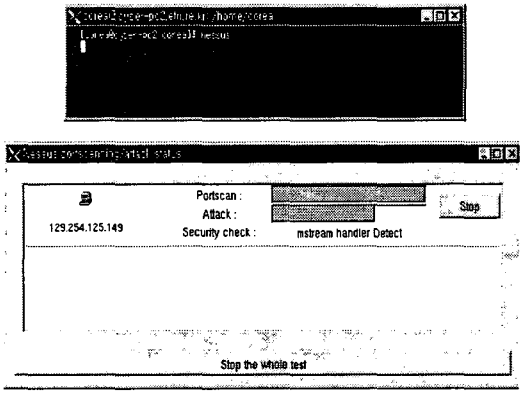

그림 5. Nessus 로 공격 실시

http://localhost/acid

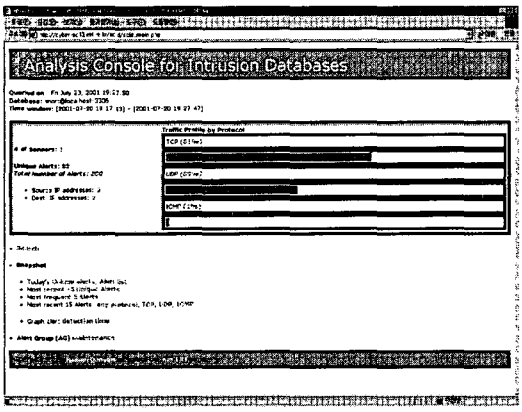

그림 6. ACID 로 결과 보기

그림 4 에서는 Snort 의 데몬을 구동하였다. 여기에서 –d 는 디렉토리, -h 는 호스트, -l 은 로그, -c 는 설정파일을 의미한다. 데몬 모드로 Snort 를 동작하려면 –D 를 추가하여 명령어를 입력하면 된다.

그림 5 는 취약성 점검 툴인 Nessus 를 다른 리눅스 시스템에 설치한 후, 이것을 이용하여 침입자 감시시스템을 공격한 것이다. Nessus 는 TCP, UDP, ICMP 등의 여러가지 프로토콜을 모두 점검할 수 있다.

그림 6 은 침입자 감시시스템의 NIDS 인 Snort 가 탐지해 낸 경고 로그의 결과를 ACID 를 통해서 웹 상에서 살펴본 것이다. 프로토콜별, 공격 IP 별 및 여러가지 형태의 결과를 볼 수 있는 환경을 제공하여, 관리자가 쉽게 공격자를 확인해 볼 수 있다.

본 장에서는 침입자 감시시스템이 어떻게 동작하는가를 실제 공격을 통해서 실험해 본 것이다. 공격은 자동화된 취약성 분석툴인 Nessus 를 사용하였다. 웹 상으로의 로그 정보를 ACID 를 통해서 살펴보았다.

5. 결론

본 논문은 네트워크 보안을 위해서 공개 소프트웨어를 이용하여 효과적인 침입자 감시 시스템을 구축하는 방법을 제안한 것이다. 본 논문에서는 네트워크 기반 침입 탐지 시스템인 Snort 를 사용하였으며, ACID 를 사용하여 그 결과를 웹 상으로 살펴보았다. 특히, httpd.conf 파일의 디렉토리 접근제어 및 Tcpwrapper 의 설치로 inetd 방식의 서비스의 접근제어를 통해서 관리자만이 이 침입자 감시시스템에 접근할 수 있도록 설정하였다. 실제 테스트베드를 구축하고 취약점 분석 툴인 Nessus 를 사용하여 침입 감시시스템의 동작 및 성능을 테스트 하였다.

앞으로의 과제는 이러한 침입자 감시시스템을 이용하여 효과적으로 침입자를 역추적 할 수 있는 방법을 연구하는 것이다.

참고문헌

[1] AEleen Fish, "Essential Sytem Administartion", O'Reilly, 1996
[2] Anonymous, "Linux Security", SAMS, 1999
[3] PLUS, "Security PLUS for UNIX", Youngjin, 2001
[4] Rebecca Gurley Bace, "Intrusion Detection", Macmillan Technical Publishing, 2000
[5] Terry Escamilla, "Intursion Detection – Network Security Beyond the Firewall", Wiley, 1998
[6] Sandeep kumar, "Classification and Detection of Computer Intrusions", Purdue University, 1995
[7] S. J. Hashim, K. Jumari and M. Ismail, "Computer Network Intrusion Detection Software Development", IEEE, 2000
[8] http://www.ietf.org
[9] http://www.snort.org
[10] http://www.andrew.cmu.edu/~rdanyliw/snort