제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

네트워크 기반 침입탐지 시스템의 취약성 규칙 DB를 자동적으로 갱신하는 에이전트 설계

양은목*, 이상용**
*공주대학교 컴퓨터공학과
**공주대학교 정보통신공학부 컴퓨터전공
e-mail:{*emyang,**sylee}@kongju.ac.kr

The design of Agents for update automatically vulnerability rule DB in Network based Intrusion Detection Systems

Eun-mok Yang*, Sang-yong Lee**
*Dept of Computer Engineering, Kongju National University,
**Division of Information & Communication, Engineering

요 약

네트워크와 컴퓨터시스템의 보안을 강화하기 위해서는 보안상의 취약성이 발견되는 대로 파악하고 점검해 주어야 한다. 그러나 대부분의 네트워크기반 침입탐지 시스템은 취약성을 파악하기 위해서는 국내외 관련 사이트들을 수동적인 방법으로 검색하기 때문에, 취약성 규칙을 갱신하는 것은 매우 어렵다.

본 논문에서는 에이전트가 스스로 관련 사이트에서 취약성 정보를 검색하여 새로운 취약성 정보를 추출한 후, Snort의 최적 규칙 형태로 변환하고 취약성 규칙을 갱신해주게 된다. 본 에이전트에 의해 갱신된 취약성 규칙 DB는 많은 규칙이 추가될지라도 침입을 탐지하는 속도가 떨어지지 않고, 확장성 및 이식성이 용이하다는 특징을 가진다.

1. 서론

네트워크기반 침입탐지 시스템은 파일에 저장된 침입정보를 이용해 네트워크기반의 침입을 탐지해왔다. 이와 같은 파일을 작성하기 위해서는 관리자가 네트워크의 취약성 관련 정보사이트를 검색/분석하여 이를 규칙화한 후 파일에 저장하여 이용하였다. 하지만, 이러한 작업들은 새로운 취약성이 발표되었을 때, 취약성의 존재를 모르는 경우와 많은 업무 때문에 제대로 적용을 못 하는 경우가 많다.

본 논문에서는 새로운 취약성 정보를 관련 사이트에서 수집하는 에이전트와 이러한 취약성을 분석하고 규칙을 생성하기 위해 정보들을 추출한다. 그리고, 규칙을 생성하여 침입 탐지 시스템에 적용하는 에이전트 시스템을 설계한다. 본 시스템은 실시간으로 취약성을 탐지할 수 있고, 새로운 취약성에 대해 신속하게 대응할 수 있다. 그리고 다중의 Snort 센서로 구성되어지므로 침입 탐지 시스템의 로그분석을 통해 네트워크 고장원인을 파악할 수 있는 관리자 인터페이스를 제공한다. 본 취약성 DB는 많은 규칙이 추가될지라도 침입을 탐지하는 속도가 떨어지지 않고, 확정성 및 이식성이 용이하다

논문의 구성은 2장에서 Snort와 에이전트에 대하여 알아보고, 3장에서 시스템의 구조와 에이전트의 구조, 규칙 DB의 형태를 설명하며, 4장에서는 결론을 기술한다.

2. 관련연구

2.1 Snort

Snort는 실시간 트래픽 분석과 IP 네트워크 상에서 패킷 로깅이 가능한 가벼운(lightweight) 네트워크 침입탐지시스템이다[2]. 또한 패킷 수집 라이브러리인 libpcap에 기반한 네트워크 스니퍼인데, 쉽게 정의할 수 있는 침입탐지 규칙(rule)들과 일치되는 네트워크 트래픽을 감시/기록/경고할 수 있다. 그리고 프로토콜 분석, 내용 검색/매칭을 수행할 수 있으며 오버플러우, Stealth 포트스캔, CGI 공격, SMB 탐색, OS 확인 시도 등의 다양한 공격과 스캔을 탐지할 수 있다[3][5][8].

<표 1>은 현재 존재하는 침입탐지 규칙의 종류이다.

<표 1> 침입 탐지 가능한 규칙의 종류

탐지 가능한 규칙의 종류
attack-responses, backdoor, bad-traffic, ddos, dns, dos, exploit, finger, ftp, icmp, icmp-info, info, local, misc, netbios, policy, porn, rpc, rservices, shellcode, smtp, sql, telnet, tftp, virus, web-attacks, web-cgi, web-coldfusion, web-iis, web-frontpage, web-misc, x11

2.2 취약성 정보 제공 사이트

본 연구에서 취약성 정보를 자동으로 얻기 위하여 아래의 웹 사이트를 사용한다.

- CVE (http://cve.mitre.org)
- ICAT (http://icat.nist.gov)
- CERT (http://www.cert.org)
- SFCS (http://www.securityfocus.com)
- SF.net (http://www.sourceforge.net)

취약성 정보를 제공하는 사이트들이 독자적인 이름 규칙에 의해 취약성 정보를 제공하면 같은 취약성이라 하더라도 정보의 효율적인 공유가 어렵다. CVE는 이러한 제한점을 극복하기 위해 취약성 정보 제공 사이트들이 취약성 이름에 대하여 표준을 제시한다. 에이전트는 CVE ID를 기준으로 취약성 정보 수집/작성하며 이것은 여러 사이트의 정보를 통합하는데 적절한 기준이 된다[7][9].

2.3 에이전트

정보 수집 에이전트는 원하는 사이트의 원하는 정보에 대한 자동수집 기능으로, 사이트에 접속하지 않더라도 실시간으로 추가 변경정보의 수신이 가능하다.

정보 분석 에이전트는 사용자가 원하는 형태에 맞도록 정보를 가공하고 필터링 해준다. 그리고 끊임없이 유입되는 정보 중에서 필요한 것은 사용하고 필요 없는 것은 무시하며, 정보 분석 에이전트에서는 많은 정보들 중에서 어떠한 것이 실제로 취약성에 관한 정보인지를 판별해 준다.

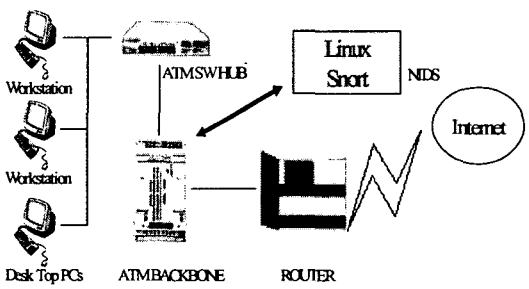
정보 추출 에이전트는 그 문서의 중심적인 의미를 나타내는 특정 구성요소를 인식하여 추출하는 작업을 가리킨다. 정보 추출의 예로는 날씨정보를 제공하는 웹 문서로부터 지역, 날씨, 최고온도, 최저온도, 습도 등의 정보를 뽑아 내거나, 또는 아파트 정보 문서로부터 방의 개수, 매매가, 전세가, 전화번호 등을 추출하는 것들을 들 수 있다.

규칙 생성 에이전트는 원하는 정보를 추출한 다음 DB의 필드에 맞게 변환 후 침입탐지에 사용할 수 있는 형태의 규칙으로 만든다.[2].

3. 시스템 설계

3.1 침입탐지 시스템의 배치

본 논문은 Snort를 기반한 실시간 네트워크 침입탐지 시스템에서 Snort 로그를 DB에 저장하고 탐지하는 규칙도 DB화하여 로그 DB에서는 새로운 침입유형을 추정한다. 그리고 네트워크가 불안정할 경우 네트워크 고장을 예방하거나 고장 원인을 밝혀낼 수 있다. 또한 규칙 DB에서는 새로운 취약성 정보를 스스로 갱신함으로써, 항상 새로운 취약성에 대해서도 탐지할 수 있도록 하였다.

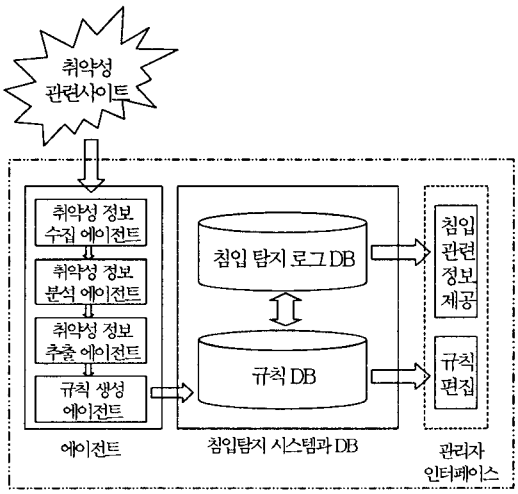


[그림 1] 시스템 배치도

[그림 1]은 네트워크에서의 침입탐지 시스템의 배치도이다. 각각의 PC들과 Workstation은 Switching HUB에 연결되어 있고, 각각의 Switching HUB들은 ATM Backbone에 연결되어 있다. 그리고 라우터를 통해 인터넷에 연결되어진다.

3.2 침입탐지 시스템의 구성

[그림 2]는 취약성 관련 사이트에서 취약성 정보를 수집하고, 취약성 정보를 분석하여 Snort의 규칙 형태로 변환 후 규칙 DB에 저장한다. 그리고, 새로 갱신되어진 정보는 침입탐지 프로세스의 재시작 없이 바로 적용되고 새로운 취약성에 대한 것도 침입탐지 로그 DB에 기록이 된다. 이러한 DB에서 관리자는 침입 정보를 보다 효과적으로 열람할 수 있으며, 네트워크의 불안정 원인을 파악할 수 있다. 침입정보를 열람함으로써 발견되는 규칙정보를 직접 편집하여 새로운 규칙을 유도할 수 있고 유도된 규칙을 적용하여 침입을 탐지한다.



Linux 7.1 Release, Snort 1.8.6

[그림 2] 침입탐지 구성도

3.3 침입탐지 시스템의 규칙 DB

일반적인 Snort규칙의 형태는 다음과 같다.

```
alert udp $EXTERNAL_NET any -> $HOME_NET 111 (msg:"RPC portmap request ttdbserv"; content:"|01 86 F3 00 00|"; offset:40;depth:8; reference:cve,CVE 1999-0003; reference:cve,CVE-1999-0687; reference:cve,CAN-1999-1075; reference: cve,CAN-2001-0717; reference:url,www. cert.org/advisories/CA-2001-05.html; reference:bugtraq,122; reference:arachnids,24; classtype:rpc-portmap-decode; sid: 588; rev:5;)
```

[그림 3] Snort의 규칙의 한 형태

[그림 3]과 같은 규칙의 형태의 다음의 취약성 DB구조에 삽입하여 침입을 탐지한다.

```
Create Table Snort_Rule(
        Rule_Actions
        Protocols
        IP_Address
        Port_Number
        The Direction Operator
        Rule Options
        Minfrag
        http Decode
        Portscan Detector
        Portscan Ignorehosts
        Output Modules
        Log_tcpdump
        Advanced Rule Concepts
        Building Good Rules    )
```

[그림 4] 규칙 DB구조

취약성 관련 사이트에서 취약성 정보를 분석하여 [그림 4]에 있는 정보들을 추출한다. 그리고 이것은 각 필드에 맞게 저장을 하고, 새로 추출한 정보를 적용한다.

```
Create Table Snort_Rule_SID(
        SID
        MSG
        Optional References
        Optional References    )
```

[그림 5] Rule Options의 필드에서 MSG ID

[그림 5]는 [그림 3]의 일반적인 규칙에서 볼 수 있듯이 규칙 DB에서 Rule Options중에 MSG부분은 출력할 메시지를 정의한다.

```
Create Table Snort_Rule_ClassType(
        config
        classification
        shortname
        short_description
        priority    )
```

[그림 7] Rule Options의 필드에서 classType

[그림 7]는 [그림 3]의 일반적인 규칙에서 볼 수 있듯이 규칙 DB에서 Rule Options 중에 classtype를 정의한다.

3.4 관리자 인터페이스

관리자 인터페이스는 ACID(Analysis Console for Intrusion Database)로 구성한다. PHP, APACHE와 같은 웹 프로그램으로서 사용자에게 친숙한 관리자 인터페이스를 제공함으로써 많은 자료를 쉽게 보고 규칙 편집과 환경설정 작업을 돕는다. 그리고 침입 탐지 로그를 통해 여러 가지 통계를 제공한다.

4. 결론 및 향후 과제

Snort는 실시간으로 네트워크에서 침입을 탐지하는데 네트워크의 속도를 떨어뜨리지 않으면서 침입을 효과적으로 탐지할 수 있다. 이런 침입 탐지 시스템도 새로운 침입 유형에 신속하게 대응하게 못하면 결국 침입 탐지 시스템으로서의 기능을 잃어버리게 된다. 그러므로 본 논문에서는 보안 정보를 제공해 주는 취약성 정보 사이트에서 보안 정보를 모으고 필터링하여 새로운 보안 정보에 신속하게 대응할 수 있도록 하였다. 또 Snort센서가 다중 시스템에서 설치되어 있으므로 로그 DB를 분석하여 새로운 정보를 찾을 수 있고, 그 정보를 바탕으로 새로운 규칙을 만들어서 적용할 수 있다.

향후 연구 과제로는 네트워크의 침입 탐지뿐만 아니라, 호스트 기반의 감사 자료를 DB화하여 네트워크와 호스트 기반의 하이브리드 침입탐지 시스템에 관한 연구가 필요하다.

참고문헌

[1] Brian Laing Jimmy Alderson "How To Guide-implementing a Network Based Intrusion Detection System" 2000, Internet Security System

[2] Cynthia L. Nelson and Deborah S. Fitzgerald "Sensor Fusion for Intelligent Alarm Snalysis"

[3] Daniel G. Schwartz, Sara Stoecklin, and Erbil Yilmaz "A Case-Based Approach to Network Intrusion Detection" 2002, ISIF

[4] Martin Roesch "Snort Users Manual Snort Release: 1.9.x"

[5] Shin Ishikawa "A Tool for Running Snort in Dynamic IP Address Assignment Environment" http://rr.sans.org

[6] Thomas Goeldenitz "IDS-Today and Tomorrow" http://rr.sans.org

[7] http://www.certcc.or.kr/tool/Snort.html

[8] http://www.sans.org

[9] http://www.snort.org