침입정보 통합관리시스템을 위한 테스트베드 구축

이성호*, 박용철**, 이형효***, 노봉남*
*전남대학교 전산학과
**전남대학교 정보보호협동과정
***원광대학교 정보·전자상거래학부
e-mail:shlee2@athena.jnu.ac.kr

The Construction of the Testbed for the Integrated Intrusion Detection Management System

Seong-Ho Lee*, Yong-Cheol Park**, Hyung-Hyo Lee***, Bong-Nam Noh*
*Dept. of Computer Science, Chonnam National Univ.
**Interdisciplinary Program of Information Security, Chonnam National Univ.
***Division of Information and Electronic Commerce, Wonkwang Univ.

요 약

전통적인 IDS는 단일 시스템, 단일 환경하의 침입 탐지만을 제공하므로, 보안대상 제한, 유연성 한계, 다양한 형태의 침입탐지 불가 등의 문제점이 대두되고 있다. 최근 이러한 문제점을 해결하기 위하여 여러 IDS의 침입정보를 통합, 분석하는 연구가 활발히 진행되고 있다. IDWG는 IDS간 상호운용을 지원하고자 침입정보 전송 프로토콜과 메시지 교환 형태를 표준화하는 작업을 진행하고 있다. 본 논문은 이기종 IDS 관리 및 침입정보 통합을 위한 테스트베드 구축 과정을 제시한다. 단위 IDS는 Snort와 Snare를 사용였으며, 국제표준을 준수하는 RoadRunner 라이브러리를 이용하였다.

1. 서론

1980년경부터 지금까지 국내·외 침입 탐지 연구는 시스템의 비정상적인 사용, 오용, 남용 등을 탐지하여 침입 잠재 가능성을 정의하고 시스템 또는 전산망에 대한 침입탐지 연구를 수행하는 방향으로 진행되어 왔다. 하지만, 전통적인 IDS는 단일 시스템 혹은 단일 환경하의 침입 탐지만을 제공하고 있어 보안대상 제한, 유연성 한계, 다양한 형태의 침입탐지 불가 등의 문제점이 대두되고 있다. 최근 IDS의 동향은 호스트 기반과 네트워크 기반의 IDS를 연동하여 침입여부를 판정하고, 각 시스템의 침입탐지 정보를 모아 분석하는 계층적 구조의 침입 탐지 통합이 연구되고 있다.

그러나, 이러한 IDS 프로토타입은 개개의 환경에 적합하게 설계되어 적용됨에 따라 확장의 어려움이 있으며, 이는 각각의 시스템들이 지닌 독자적인 메시지 형태에 기인한다. 이러한 문제를 극복하기 위해 IDS의 상호 연동을 위한 표준이 정의되고 있다. 이는 크게 IDS가 생성하는 로그 형식을 정의한 표준과 IDS간의 통신 규약을 정의한 표준으로 나눈다.

국내 표준에선 로그의 형식에 대한 표준으로 2001년 5월 민간성격의 ISTF-0005 IDS 로그형식 표준이 있다. 국외에선 IETF(Internet Engineering Task Force)내의 IDWG(Intrusion Detection Working Group)에서 IDS 상호연동을 위한 요구사항 명세, 공통 언어 정의, 통신 프로토콜과 데이터 포맷 등의 표준화 동향이 있다. 아직 RFC로 발표되지는 않고, 아래 세 Internet-Draft가 검토 중이다[1,2,3].

- Intrusion Detection Message Exchange Format Extensible Markup Language (XML) Document Type Definition
- The TUNNEL
- The Intrusion Detection Exchange Protocol (IDXP)

본 연구에서는 IDWG의 IDMEF를 이용하여 단위 IDS의 침입정보를 통합하는 테스트베드 구축 과정을 제시한다. 단위 IDS는 Snort와 Snare를 사용하였으며, 국제표준을 준수하는 RoadRunner 라이브러리를 이용하였다.

본 논문의 구성은 다음과 같다. 2장은 이기종 IDS관리 및 침입정보 통합을 위한 IDWG의 국제표준 명세 작업에 대해 기술한다. 3장은 NIDS인 Snort와 HIDS인 Snare의 침입정보를 IDMEF 형태로 전송하는 과정 및 침입정보를 수집하는 과정에 대해 기술한다. 마지막으로, 4장은 본문 내용을 요약하고, 향후 방향에 대해 기술한다.

2. 관련연구

2.1 국제 표준 명세

이기종 IDS간 메시지 교환 기술은 IETF내의 IDWG에 의해 표준화가 추진 중이다. IDWG는 IDS에 대해 다음과 같은 구조적인 가정을 바탕으로 표준화를 진행하고 있다. 첫째, IDS를 구성하는 모듈 중, 이벤트 분석기능을 담당한 분석모듈(Analyzer)만이 침입경보(alert)를 생성하고 전달할 수 있다. 둘째, 분석모듈과 관리모듈은 별도의 모듈로서 TCP/IP를 통해 통신한다.

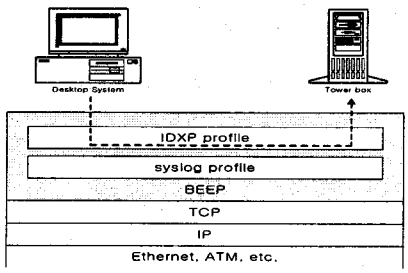
2.1.1 BEEP(Blocks Extensible Exchange Protocol)

BEEP는 응용계층 프로토콜의 개발에 필요한 공통기능들을 제공하기 위해 제안된 프레임워크이다. 프로토콜의 각 메커니즘에 대한 BEEP의 지원 여부는 표-1과 같다[5].

지원 메카니즘	미지원 메카니즘
프레임화(Framing) 코드화(Encoding) 에러보고(Reporting) 비동기교환(Asynchrony) 인증(Authentication) 비밀성(Privacy)	명명화(Naming) 접근통제(Authorization)

[표-1] 프로토콜 메카니즘에 대한 BEEP의 지원 여부

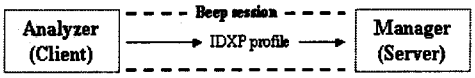
BEEP는 여러 개의 채널을 통해 병렬적인 메시지 전송이 가능하다. BEEP 프레임워크에서 세션이 설정되면 세션 내에 여러 개의 채널이 생성할 수 있고, 병렬적으로 다른 종류의 메시지를 전송할 수 있다. 각 채널은 BEEP 프로파일과 연관된다. 그림-1은 두개의 채널을 갖는 BEEP 세션이다.



[그림-1] 두 개의 채널을 갖는 BEEP 세션

2.1.2 IDXP(Intrusion Detection eXchange Protocol)

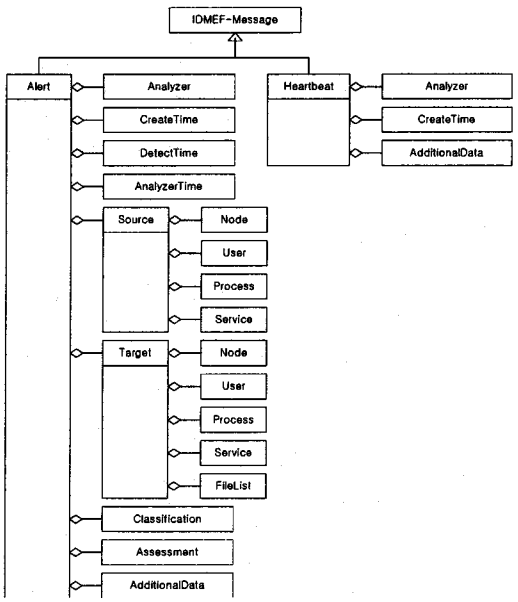
IDXP는 IDS간 침입정보 교환을 위한 표준 프로토콜로, BEEP의 프로파일 형태로 구현된다. 따라서, 전송에 필요한 메커니즘은 BEEP가 제공하며, IDXP는 침입정보 교환에 필요한 채널특성만을 명세한다. 전송 과정에서 보안특성을 지원하지 않으므로, TLS나 SASL 프로파일을 사용하여 인증이나 기밀성을 보장한다[6,7]. 데이터 교환은 연결생성, 보안설정, IDXP 채널생성, 데이터 전송의 네 단계로 진행된다. 그림-2는 IDXP 프로파일을 통한 데이터 전송의 예이다.



[그림-2] IDXP 데이터 전송의 예

2.1.3 IDMEF(Intrusion Detection Message Exchange Format)

IDMEF는 침입정보 교환에 사용되는 표준 메시지 형태를 정의하고 있다. IDMEF를 위한 데이터 모델은 UML(Unified Modeling Language)로 명세되었으며, XML로 구현되고 있다. 그림-3은 IDMEF 모델에 정의된 주요 클래스간의 관련성을 보여 준다.



[그림-3] IDMEF 모델의 개요

IDMEF 메시지 타입은 크게 Alert과 Heartbeat의 두 가지 형태로 구성된다. Alert은 침입경보를 생성한 IDS의 이름, 침입경보를 발생시킨 이벤트, 공격의 개시시스템과 목표시스템에 대한 정보 등을 포함한다. Heartbeat는 분석모듈이 관리모듈에게 상태정보를 제공할 때 사용된다.

2.3 국내·외 산업계 동향

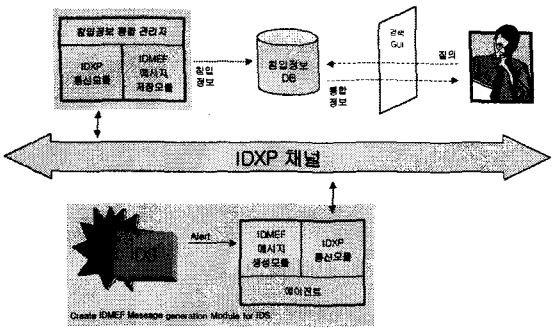
한 가지 솔루션만이 독자적으로 설치되어 운용되는 것이 아니라 각 보안장비들을 통합해서 취약점을 보완한 형태의 통합 솔루션들과 관리 솔루션들이 개발되어 출시되고 있다. 통합보안관리시스템(ESM:Enterprise Security Management)과 인증과 접근제어를 연계한 통합인증 및 권한관리(EAM:Extranet Access Management)를 들 수 있다. 표-2는 현재까지 출시된 주요 국내 제품의 ESM의 종류와 특징을 보여주고 있다.

개발사	제품명	주요특징
디지털이지스	이지스엔터프라이스	자사 침입차단, 침입탐지 등 통합관리, 모니터링
이글루시큐리티	스파이더-1	각종 침입차단, 침입탐지 등 통합관리. 일/디렉토리 관리, 실시간 경보 제공
어울림정보기술	SecureWorks ESM	자사 침입차단, 통합관리, 모니터링, 타사 제품 지원예정
인젠	NeoWatcher ESM	자사 침입차단, 침입탐지 등 통합관리, ESM 컨소시엄 추진
시큐아이닷컴	시큐아이엠에스에스	웹 기반의 보안통합관리 툴 자사의 보안관제서비스에 사용

[표-2] 국내 ESM 제품의 특징

3. 테스트베드 구축

전체 동작과정은 다음과 같다. 먼저, 단위 IDS가 생성한 침입정보를 에이전트는 표준화된 IDMEF 형태로 변환한다. 다음으로, 에이전트는 생성된 IDMEF 메시지를 IDXP 채널을 통하여 안전하게 통합 관리자에게 전달한다. 마지막으로, 통합 관리자는 전송받은 침입정보 메시지를 파싱하여 DB에 저장한다. 전체적인 구성도는 그림-4와 같다.



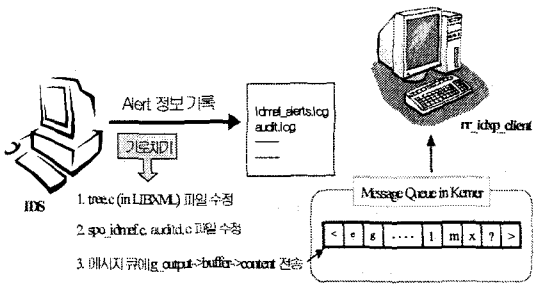
[그림-4] 침입정보 관리 프레임워크

3.1 테스트베드 구축 모듈

테스트 베드 구축에 공개용 NIDS인 Snort와 공개용 HIDS인 Snare에서 발생하는 침입정보를 사용한다. 침입정보를 IDMEF 형태로 변환하며, BEEP기반의 IDXP를 C언어로 구현한 RoadRunner 라이브러리를 활용하여 전송한다. 전송받은 IDMEF 형태의 침입정보 메시지를 파싱하기 위해 SAX 라이브러리를 이용한다.

3.1.1 IDMEF XML 변환 모듈

이기종 IDS에서 발생한 침입정보를 IDMEF 형태로 변환하며, 전송모듈인 rridxp_client를 위해 커널 기반의 메시지 큐에 변환된 메시지를 전달한다. 현재, Snort에 대한 IDMEF XML 변환과정은 이미 Silicon Defense (http://www.silicondefense.com) 에 서 진행되어 플러그인을 제공하고 있다. Snrot의 IDMEF 변환 플러그인은 침입정보를 /var/log/snort/idmefxml_alert.log에 기록하고 있다. Snare는 /var/log/audit/audit.log를 분석하여 IDMEF로 변환하는 플러그인을 개발하고 있다. 그림-5는 변환되는 과정을 보여준다.



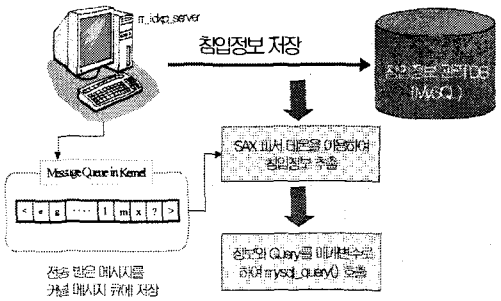
[그림-5] IDMEF 형태의 침입정보 메시지 생성과 rridxp_client로의 전송과정

3.1.2 IDXP 통신 모듈

IDXP 채널을 생성하여 에이전트와 통합 관리자 사이에 침입정보를 전송하는 기능을 담당한다. RoadRunner 라이브러리에서 제공하는 IDXP 프로파일 RRIDXP와 TLS 프로파일 RRTLS를 사용하여 개발하고 있다.

3.1.3 DB저장 모듈

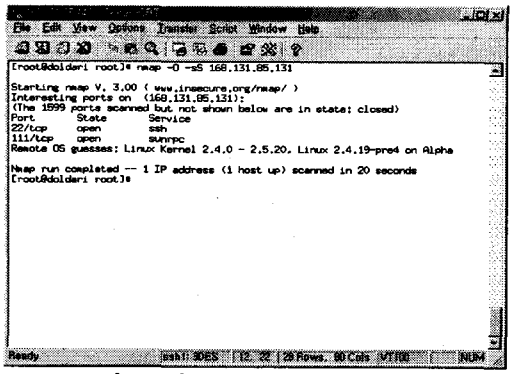
먼저, IDMEF 형태의 침입정보 메시지에서 의미있는 정보단위로 파싱한다. 다음으로, 적절한 질의어와 침입정보를 매개변수로 mysql_query를 호출하여 관계형 DB인 MySQL에 저장한다. 그림-6은 침입정보 통합 관리자내에서 침입정보를 저장하는 과정이다.



[그림-6] 침입정보 통합 관리자의 침입정보 저장

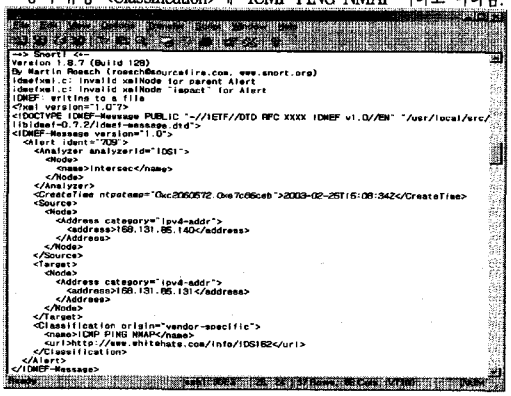
3.2 실험

1) 스캔공격 시도
- 스캔 도구인 nmap을 이용하여 Snort가 설치된 호스트로 공격을 시도함



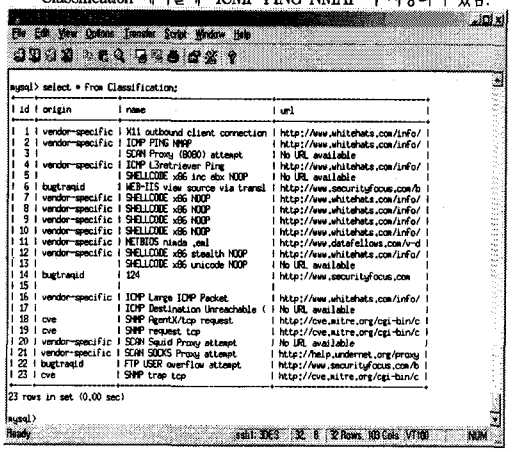
[그림-7] nmap 스캔 공격 시도

2) IDMEF XML 플러그인의 침입정보 메시지 생성
- 공격 유형 <Classification>에 "ICMP PING NMAP"이라고 나타남.



[그림-8] IDMEF XML 플러그인의 침입정보 메시지 생성

3) 침입정보 메시지의 DB 저장
- Classification 테이블에 "ICMP PING NMAP"이 저장되어 있음.



[그림-9] Classification 테이블에 저장된 침입정보

4. 결론 및 향후 연구방향

본 논문에서는 이기종 IDS 관리 및 침입정보 통합을 위한 테스트베드 구축과정을 제시하였다. 테스트 환경에서는 먼저, 공개용 NIDS인 Snort와 HIDS인 Snare의 침입정보를 IDMEF 형태로 변환하고, RoadRunner 라이브러리를 이용하여 침입정보를 에이전트에서 침입정보 통합 관리자로 안전하게 전송한다. 전송된 침입정보는 파싱 과정을 통하여 의미있는 정보단위로 분리된 후에, 관계형 DB인 MySQL에 저장하는 과정을 보여주었다.

향후에는 테스트베드 구축에 나타난 문제점을 보완하고, 수집된 침입정보에 연관성 분석을 수행하여 침입 탐지율을 개선하고자 한다.

참고문헌

[1] T. Buchheim, M. Erlinger, B. Feinstein, G. Matthews, R. Pollock, J. Bester, A. Walther, "Implementing the Intrusion Detection Exchange Protocol," Proceedings of 17th Annual Computer Security Applications Conference(ACSAC '2001), New Orleans, Lousiana, Dec 2001

[2] B. Feinstein, G. Matthews, J. White, "The Intrusion Detectioin Exchange Protocol (IDXP)," draft-ietf-idwg-beep-idxp-04.txt, Jan 2002

[3] D. Curry, H. Debar, "Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language Document Type Definition," draft-ietf-idwg-idmef-xml-06.txt, Dec 2001 Dec 2001

[4] M. Wood, M. Erlinger, "Intrusion Detection Message Exchange Requirements," draft-ietf-idwg-requirements.txt, Feb 2002

[5] M. Rose, "The Blocks Extensible Exchange Protocol Core," RFC 3080, Mar 2001

[6] T. Dierks, C. Allen, "The TLS Protocol Version 1.0," RFC 2246, Jan 1999

[7] J. Myers, "Simple Authentication and Security Layer," RFC 2222, Oct 1997

[8] D. Denning, "An Intrusion-detection Model," IEEE Transactions on Software Engineering, Vol. 13, No. 2, pp. 222-232, 1987