리눅스 환경에서의 침입방지시스템(IPS) 설계

이상훈* · 김우년* · 이도훈* · 박응기*

요 약

정보통신망의 빠른 발달과 이로 인한 인터넷 사용의 급증으로 인하여 해킹, 바이러스 등의 정보통신 역기능 또한 빠르게 발전하고 있다. 이를 방지하기 위해 F/W, IDS, VPN 등의 보안 제품이 많이 사용되고 있다. 그러나, 1.25 인터넷 대란에서 알 수 있듯이 현 상황은 관리자가 보안 제품들에서 발생하는 경고 메시지를 확인하고 해당 내용을 대응할 수 없을 정도로 빠른 시간에 확산된다. 따라서, IDS와 더불어 자동 대응 기능을 갖추고 있는 침입방지시스템(IPS)이 절실히 요구되어지고 있고, 널리 사용되어지고 있다. 본 논문에서는 linux 운영 체제 환경에서의 공개된 도구인 snort와 iptables를 이용하여 시스템 구축 비용이 최소화될 수 있는 방향으로 설계되었다. 또한, snort에서 발생시킨 경보 메시지를 iptables와 연계하여 자동 대응을 수행하도록 구성되었으며, 이를 통하여 관리자 개입을 최소화하고 해킹사고에 대한 피해를 최소화 할 수 있도록 제안되었다.

Design of Intrusion Prevention System(IPS) in Linux Environment

Sang Hun Lee* · Woo Nyon Kim* · Do Hoon Lee* · Eung Ki Park*

ABSTRACT

The growth of incidents on the Internet has reflected growth of the internet itself and growth of the computing power. while in previous years, external attacks tended to originate from those interested trend in exploring the Internet for its own sake and testing their skills, there is an increasing trend towards intrusions motivated by financial, political, and military objectives. so, attacks on the nation's computer infrastructures are becoming an increasingly serious problem. Even though the problem is ubiquitious, government agencies are particularly appealing targets and they tend to be more willing to reveal such events than commercial organizations. The threat of damage made necessity of security's recognition, as a result, many researches have been carried out into security of system actively. Intrusion Detection technology is detection of intrusion using audit data differently from using traditional simple filtering and informs manager of it. It has security manager of system deal with the intrusion more quickly. but, cause current environment of Internet manager can't doing response Intrusion alert immediately. That's why IPS needed. IPS can response automatically the intrusion alert. so, manager is more comfortable and can response quickly.

Key words : Intrusion Prevention System, Intrusion Detection, Attack

* 국가보안기술연구소

1. 서 론

컴퓨터의 급속한 발전과 인터넷의 보급 확산은 정보의 공유, 전송의 고속화, 대용량 데이터의 효율적인 전송 등의 긍정적인 효과와 더불어 정보의 유출 및 변경, 훼손, 불법적 사용 등의 부정적인 효과를 야기시키고 있다. 특히, 초고속 인터넷의 보급 확산은 이러한 네트워크의 부정적 기능을 더욱 배가시키고 있다. 네트워크를 통한 침입 시도는 해가 갈수록 증가되고 다변화되고 있으며, 악의적인 사용자에 의한 독창적이고 새로운 침입 방식은 침입 발견을 어렵게 하여 해당 침입에 대한 대응 수행을 어렵게 하고 있다[1]. 그리고, 초고속 통신 보급의 확산으로 인하여 각 기관이나 업체뿐만 아니라 각 가정의 컴퓨터도 바이러스나 인터넷 웜, 해킹의 위험에 노출되어 있다. 이러한 여러 가지 위험들로부터 네트워크와 컴퓨터를 보호하기 위하여 많은 정보보호 기술 및 제품들이 각광을 받고 있다. 이러한 정보보호 기술 및 제품 중에서 방화벽, 공개키 기반 구조(PKI), 바이러스 백신 등과 함께 최근 각광을 받고 있는 기술이 바로 침입탐지 기술이다[1]. 침입 탐지 기술은 해커의 공격 형태가 점점 다양화되고 대규모화됨에 따라 기존의 정보보호 기술만으로는 정보 시스템 또는 네트워크를 안전하게 보호할 수 없다는 인식과 함께 더욱 주목을 받고 있다.

침입 탐지 시스템은 정보 시스템 또는 네트워크로부터 보안 관련 정보들을 수집, 분석해 침입 또는 오용을 탐지할 뿐 아니라 침입에 대한 적절한 대응 행동을 수행하는 기능을 포함하는 시스템으로 정의된다[2]. 침입 탐지에 관한 연구는 80년에 앤더슨이 '시스템의 보안 위협에 대한 분류'를 미 공군 연구보고서에 발표한 것을 기점으로 현재까지 매우 빠르게 진행되어왔다. 그러나, 침입 탐지 기술이 발전하고 있음에도 불구하고 1.25 인터넷 대란에서 볼 수 있듯이, 빠르게 확산되는 웜 공격 및 대규모의 서비스 거부/분산 서비스 거부 공격 등 확산 속도가 빠르고 대규모로 발생되는 공격에 대해서는 관리자가 침입탐지시스템을 통하여 이를 인지하고 적절한 대응을 수행하기에 적합하지 못하다. 이러한 침입탐지 시스템의 단점을 보안하고 관리자의 관리 편의성 및 신속하고 빠른 조치를 수행하고자 대두되는 기술이 침입방지(Intrusion Prevention) 기술이며, 이를 시스템화 한 것이 IPS(Intrusion Prevention System)이다. IPS는 침입탐지 시스템에서 확인된 공격 경보를 방화벽 등의 보안 장비와 연계하여 자동 대응을 수행하기 위한 시스템이다. 이러한 IPS 는 관리의 편의성과 신속한 대응 능력 등 기존 침입탐지시스템에서 가지지 못한 능력인 대응 능력을 탑재하여 현재 빠르게 발전하고 있는 추세이다. 본 논문에서는 공개용 침입탐지시스템인 snort와 linux에서 패킷 필터링을 수행할 수 있는 공개용 도구인 iptables를 이용하여 IPS를 구성할 수 있는 방안을 제시하였다. 이러한 방법은 상용 IPS에 비하여 공개용 도구를 사용하기 때문에 비용 소요가 적고 iptables와 snort를 연계하여 사용함으로써, 관리자의 개입 없이 공격 발생시 자동 대응을 수행할 수 있도록 설계되었다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문을 작성하기 위하여 사전에 연구된 관련 연구에 대하여 기술하고 3장에서는 실제의 시스템 설계 및 동작 원리에 대하여 기술하였다. 4장에서는 결론 및 향후 연구 수행 방향에 대해 이야기하였으며, 마지막으로 이 논문을 작성하기 위해 참고한 참고문헌을 기술하였다.

2. 관련 연구

2.1 침입 탐지 시스템의 역사

침입 탐지에 관한 연구는 1980년에 앤더슨이 '시

스템의 보안 위협에 대한 분류'를 미 공군 연구보고서에 발표한 것을 기점으로 현재까지 매우 빠르게 진행되어왔다. 특히 미국의 도로시 데닝이 1987년에 발표한 실시간 침입탐지모델인 침입탐지 전문가시스템(IDES : Intrusion Detection Expert System)은 지금까지도 다른 침입탐지 시스템의 기반 모델로 사용되고 있다[2]. 1980년대에는 호스트기반 침입탐지시스템이 주류를 이루고 있었으며 미국 데이비스대학에서 개발한 NSM(Network Security Monitor)부터 네트워크 환경에서의 침입탐지시스템이 뿌리 내리기 시작했다[3]. 그 이후 데이비스 대학, 미 공군 암호지원센터, 로렌스, 리버모어 국립연구소, 헤이스택 연구소와의 공동 연구를 통한 DIDS(Distributed Intrusion Detection System), 스탠퍼드 대학의 NIDES(Next generation IDES), EMERALD(Event Monitoring Enabling Response to Anomalous Live Distribution), 퍼듀 대학의 IDIOT(Intrusion Detection In Out Time), 캘리포니아 대학의 STAT(State Transition Analysis Tool) 등의 기초 침입탐지 시스템과 Axent사의 Intruder Alert, ISS사의 Real Secure, TIS의 Stalker 등의 상용 시스템이 출시되어 있는 상태이다[4, 5]. 국내에서도 여러 대학들의 대학 연구소를 중심으로 침입탐지모델을 개발해왔고, 현재는 여러 보안업체들의 참여로 이러한 연구들이 크게 활성화되고 있는 상태이다.

2.2 침입탐지 시스템의 분류

침입탐지시스템은 탐지방법을 중심으로 이루어지는 침입탐지 모델 기반의 분류방법과 탐지 영역을 중심으로 분류하는 데이터 소스 기반의 분류 기법으로 크게 나눌 수 있다[6].

2.2.1 침입탐지 모델 기반의 분류

침입탐지 모델 기반의 분류는 침입탐지방법에 따라 비정상적인 탐지모델 기반의 침입탐지시스템과 오용 탐지 모델 기반의 침입탐지시스템으로 나뉠 수 있다. 이러한 침입탐지 모델은 침입탐지시스템 개발에 있어 요구되는 침입패턴 분석 과 유형별 분류 및 탐지 방법 등을 연구함에 있어 많은 기초 정보들을 제공한다.

2.2.2 데이터 소스 기반의 분류

데이터 소스 기반의 분류는 데이터 소스의 종류에 따라 호스트 기반의 침입탐지시스템과 네트워크 기반의 침입탐지시스템으로 분류될 수 있으며, 각기 다른 종류의 침입유형을 탐지하게 된다. 호스트 기반의 침입탐지시스템은 시스템 로그 정보와 특정 행위에 대한 감사자료 분석 등 시스템 내부에서 생성되는 정보에 대한 분석을 통하여 침입을 탐지하며, 네트워크 기반의 침입탐지 시스템은 네트워크상의 패킷 헤더 및 데이터를 분석하거나 패킷 트래픽량 등을 분석하여 침입 유무를 판단한다.

2.3 침입탐지시스템의 한계점

침입탐지시스템은 탐지 위주의 메커니즘 설계로 인해 몇 가지 한계점을 가지고 있다. 첫째, 오탐지와 미탐지의 문제이다. 침입 행위가 늘어나면서 네트워크 IDS나 호스트 IDS가 제한된 탐지 능력으로 공격 시도들에 대해 적절하게 구분해내기 어려워졌다[7]. 최근 제품들이 세션 기반 탐지 기능을 강화하기는 했지만 아직까지 오탐지율을 줄이기에는 부족한 형편이다. 두 번째로 네트워크 침입탐지시스템은 실시간으로 공격을 막을 수 없다는 것이다. 이는 네트워크상에 있는 패킷들을 감지하지만 차단하지 못하기 때문이며 대부분의 패킷은 네트워크 침입탐지시스템이 판별하기 전에 침입에 성공하게 된다. 현재의 침입탐지시스템은 이 같은 결점들을 보강하기 위해 여러 가지 방법들을 제공하고 있으나, 오탐지 문제, 다량의 로그와 실시간 방어문제는

쉽게 해결할 수 없는 실정이다.

2.4 침입방지시스템

침입방지시스템은 다양하고 지능적인 침입기술에 대해 다양한 방법의 보안기술을 이용해, 침입이 일어나기 전에 실시간으로 침입을 막거나, 알려지지 않은 방식의 침입으로부터 네트워크와 호스트를 보호할 수 있는 시스템을 말한다. 즉, 침입탐지시스템이 더 많은 공격을 정확하게 탐지하는데 목적이 있는 반면에, 침입방지시스템은 공격을 탐지하는 것 뿐만 아니라 공격이 일어나는 것을 근본적으로 방어하는 것을 목적으로 한다[7].

2.5 snort

snort는 1999년 Marty Roesch에 의해 개발되어진 실시간 트래픽 분석과 IP 네트워크상에서 패킷 로깅이 가능한 가벼운 네트워크 침입탐지 시스템이다. snort는 패킷 수집 라이브러리인 libpcap에 기반하여 네트워크 패킷을 감시하며, 침입탐지 규칙들에 일치되는 트래픽을 기록하고 경고할 수 있는 기능을 가진다. snort는 프로토콜 분석, 내용 검색/매칭을 수행할 수 있으며 오버플로우, stealth 포트 스캔, cgi 공격, smb 탐색, os 확인 시도 등의 다양한 공격과 스캔을 탐지할 수 있다. 또한 이러한 탐지 규칙들은 보안 커뮤니티를 통해 지속적으로 업데이트되고 있으며, 네트워크 관리자가 관리하는 네트워크의 특성에 적합하도록 쉽게 규칙을 작성하여 추가할 수 있으므로 최신 공격에 적응이 쉽다는 장점을 가진다[8].

2.6 iptables

iptables는 리눅스 IPv4 방화벽을 설정하는 명령어이다. 1.1 시리즈부터 리눅스 커널은 패킷 필터링을 포함하기 시작하였고, 이를 제어하기 위한 기본 명령어를 제공했다. 리눅스 2.0에서는 커널의 필터링 규칙을 제어하는 사용자 툴로 ipfwadm을 제공하기 시작했으며, 1998년 중반에 리눅스 2.2를 위한 사용자 도구로써 ipchains가 구현되었다. 1999년 중반에 리눅스 2.4에 좀 더 안정적이고 사용을 용이하게 하기 위한 도구인 iptables를 포함하였다[9].

iptables에서 패킷을 검사하는 방법은 다음과 같다.

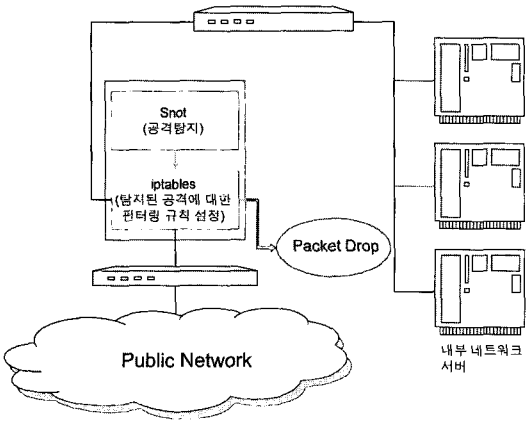
- 패킷이 커널에 도착하면 그 패킷의 목적지를 확인한다.
- 패킷의 목적지가 내부의 호스트인 경우 패킷은 전달돼 입력체인에 도달한다. 패킷이 입력체인을 통과하면 패킷을 기다리고 있던 프로세서가 수신한다.
- 그렇지 않은 경우 커널이 포워딩 불능이나, 패킷을 어떻게 포워딩해야 하는지를 알지 못하는 경우 그 패킷은 'DROP'된다. 포워딩이 가능하게 되어있고 다른곳이 목적지이면 패킷은 포워딩 체인으로 전송된다. 이 체인의 패킷 정책이 'ACCEPT'인 경우 패킷은 포워딩 할 네트워크로 전송된다.
- 마지막으로, 로컬에서 수행하던 프로그램은 네트워크 패킷을 전송할 수 있다. 이 패킷은 즉시 출력 체인에 보내지며 이 체인이 'ACCEPT'되면 이 패킷은 그 목적지가 어디이건 상관없이 전송되어진다.

3. linux_IPS

제안하는 시스템인 linux_IPS의 개념은 (그림 1)과 같다.

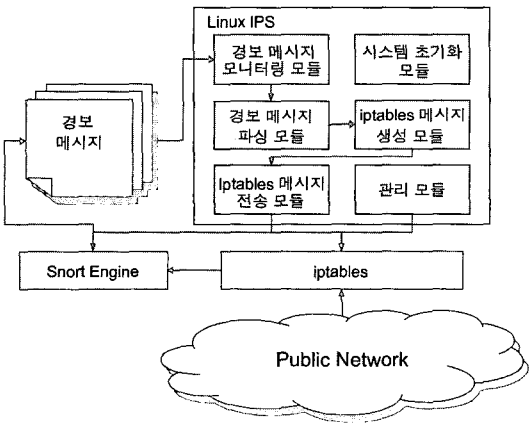
먼저 공개된 네트워크와 내부 네트워크 사이의 접점에 위치하는 시스템에서 snort를 가동시킨다. 이때 iptables를 사용하기 위해 시스템 OS

는 linux로 한정한다. snort에서 탐지된 침입 탐지 내용을 linux 방화벽인 iptables로 전송한다. 탐지내용을 전송받은 iptables는 이에 해당하는 필터링 규칙을 작성하고 이를 적용하여 악성 패킷에 대한 유입을 사전에 방지한다.



(그림 1) linux_IPS 개념도

(그림 2)는 snort와 iptables를 이어주기 위한 linux_IPS의 세부 설계 내용이다.



(그림 2) linux_IPS 세부 구성도

3.1 경보 메시지 모니터링 모듈

경보 메시지 모니터링 모듈은 snort에서 탐지되는 경보 메시지를 모니터링 하기 위한 모듈이다. 이 모듈에서는 snort에서 발생하는 경보 메시지를 실시간 감지하여 이를 경보 메시지 파싱 모듈로 전송하는 역할을 수행한다. 중복 메시지의 방지를 위하여 목적지 IP와 포트, 근원지 IP를 기준으로 Aggregation을 수행한다.

3.2 경보 메시지 파싱 모듈

경보 메시지 파싱 모듈은 snort의 경보 메시지에서 iptables에서 필요한 요소를 추출하기 위한 모듈로써, 이 모듈에서 추출되는 정보는 근원지/목적지 주소, 목적지 포트, 경보 등급 등이며, 경보 등급에 따라 iptables 메시지 생성 모듈로 전송할 것인지 무시할 것인지를 결정한다.

3.3 iptables 메시지 생성 모듈

iptables 메시지 생성 모듈은 경보 메시지 파싱 모듈에서 추출한 여러 가지 요소들을 iptables에 적용할 수 있는 형태로 재구성하기 위한 모듈이다. 이 모듈에서는 근원지/목적지 IP에 따라 FORWARD, INPUT, OUTPUTdmf 결정하기 위해 Inbound/Outbound를 결정하고 결정된 내용을 바탕으로 iptables에 삽입될 수 있는 rule 문자열을 만든다. 만들어진 문자열을 iptables 메시지 전송 모듈로 전송한다.

3.4 iptables 메시지 전송 모듈

iptables 메시지 전송 모듈은 iptables 메시지 생성 모듈에서 생성된 iptables rule 문자열을 전송 받아 이를 iptables에 적용하는 역할을 수행한다. 먼저 전송받은 문자열에 적용될 규칙이 현재 iptables에 적용되어있는지 확인한 후 만약 적용되지 않았으면 이를 적용하고, 이미 적용되어 있으면 이를 버리는 역할을 수행한다.

3.5 시스템 초기화 모듈

시스템 초기화 모듈은 시스템의 구동시 제일 먼저 구동되는 모듈로써, 시스템에서 사용되는 전역변수 및 구조체, link 등을 초기화하는 모듈이다.

3.6 관리 모듈

관리 모듈은 사용자 인터페이스와 연결되는 모듈로써, 사용자가 iptables의 자동 설정 상황을 감지하고, 이 설정을 변경할 수 있도록 해 주는 모듈이다. 사용자는 이 모듈을 통하여 iptables의 설정, Linux_IPS의 설정, snort의 설정 등 Linux_IPS에 관계되는 모든 프로세스의 설정을 수행할 수 있다.

4. 결론 및 향후 연구 방향

IPS는 현재 침입탐지시스템의 대체 시스템으로 널리 보급되고 있으며, 앞으로도 자동 대응의 필요성 대두에 의하여 점점 더 확산되어갈 것이다. 본 논문에서는 이러한 IPS를 리눅스용 공개 보안도구인 snort와 iptables를 이용하여 구성하였다. 이 구성의 장점은 공개용 도구를 사용하여 비용 소요가 적고, 기존의 상용 IDS보다 rule의 업데이트가 신속하고 용이하며, iptables를 통하여 snort에서 경보 발생 시 신속하게 자동 대응을 수행하는 것에 있다.

향후 연구 방향은 기 설계된 내용을 구현하여 시뮬레이션을 수행함으로써, 기 설계된 내용을 검증할 것이다. 그리고, snort에서 발생하는 false alarm을 최소화하는 연구를 병행하여 침입 판단의 정확성을 높이며, 이를 통하여 Linux_IPS의 향상시킬 것이다.

참 고 문 헌

[1] Bishop, Matt, S. Cheung, C. Wee, "The Threat from the Net", IEEE Spectrum 34, 1997.

[2] D. E. Denning, "An Intrusion-Detection Model", In Processing of the IEEE Symposium on Security and Privacy, 1986.

[3] Heberlin, L. T., "A Network Security Monitor", Proceedings of the 1990 IEEE Symposium, 1990.

[4] Steven R, Snapp, "DIDS - Motivation, Architecture, and An Early Prototype", Proceedings of the Fifteen National Computer Security Conference, 1992.

[5] D. Anderson, T. Frivold and A. Valdes, "Next-generation intrusion detection expert system(NIDES)", Technical Report SRI-CLS-95-07, 1995.

[6] H. Debar, M. Dacier and A. Wespi, "Research Report Towards a Taxonomy of Intrusion Detection Systems", Technical Report RZ 3030, 1998.

[7] web page at url "http://kidbs.itfind.or.kr:8888/cgi-bin/WZIN/WebzineRead.cgi?recno=0901013509&db=t_jugidong&menu=1".

[8] web page at url "http://www.cyber118.or.kr/tools/Snort.html".

[9] web page at url "http://taejuns.com/bbs/view.php?id=system&no=24".

이 상 훈

2000년 성균관대학교 정보공학과(공학사)
2002년 성균관대학교 전기 전자 및 컴퓨터 공학부 (공학석사)
2002년~현재 국가보안기술연구소(연구원)

김 우 년

1996년 안동대학교 컴퓨터공학과(공학사)
1998년 경북대학교 컴퓨터과학과(이학석사)
2000년 경북대학교 컴퓨터과학과(박사수료)
현재 국가보안기술연구소(연구원)

이 도 훈

1989년 한양대학교 전자계산학과(공학사)
1998년 한양대학교 전자계산학과(공학석사)
1991년~2000년 국방과학연구소(선임연구원)
2001년~현재 국가보안기술연구소(선임연구원)

박 응 기

1986년 중앙대학교 전자계산학과(공학사)
1998년 중앙대학교 전자계산학과(공학석사)
1999년 한국전자통신연구원(선임연구원)
현재 국가보안기술연구소(책임연구원)