

리눅스 기반 침입방지 시스템 설계 및 구현

장희진, 박민호, 소우영
한남대학교 컴퓨터 공학과

Design and Implementation of a Linux-based Intrusion Prevention System

Hui-Jin Jang, Min-Ho Park, Woo-Young Soh
Dept. of Computer Science, Hannam University

요약

최근 국내외적으로 침해 공격 사고율이 증가에 대한 방안으로 여러 보안 기술이 개발되어 왔다. 그 중 방화벽은 내부의 중요한 자원과 외부 네트워크와의 경계를 생성하고, 정책기반의 접근제어를 효과적으로 제공하고 있지만 DoS공격, 변형 프로토콜을 통한 공격에는 효과적으로 막지 못한다. 또한 침입탐지 시스템은 공격, 침입, 원하지 않는 트래픽을 구별할 수 있다는 점에서 가치가 있지만 정확한 시점에 공격을 차단하지 못하며 침입탐지 이후에 생기는 불법행동에 대한 커다란 위협이 따르며, 실질적인 방어는 관리자의 수동적인 개입을 필요로 하게 된다. 본 논문에서는 이에 대한 해결 방안으로 방화벽의 침입차단 기능과 침입탐지 시스템의 실시간 침입탐지 기능을 갖춘 리눅스 기반의 공개 보안 툴을 결합한 침입방지 시스템을 설계 및 구현한다.

1. 서론1)

네트워크와 컴퓨터의 발달로 많은 컴퓨터 사용자들이 인터넷을 통해서 쉽고 편리하게 원하는 정보를 얻을 수 있게 됨으로써 현대인의 일상생활 속에서 인터넷은 뗄 수 없는 관계가 되었다. 그만큼 쉽게 주변의 곳곳에서 인터넷을 통해서 세계의 어느 곳에 있는 컴퓨터에도 쉽게 접속할 수 있는 시대가 된 것이다. 게다가 한국의 인터넷 망 서비스 및 인트라 구축은 세계의 그 어느 나라에도 뒤지지 않고 그 규모면에서 전 세계적인 면모를 보이고 있다.

그러나 이와 같은 네트워크와 컴퓨터의 발달이 우리의 생활에 이점만을 주는 것은 아니고 그에 따른 부작용도 만만치 않은 실정이다. 최근의 몇 년간 컴퓨터 관련 범죄는 빠르게 증가하고 있다. CERTCC-KR의 통계 자료에 의하면 최근 5년간의 침해 공격 사고 증가율은 평균 200%에 달한다[1]. 따라서 산업체에서는 보안에 대한 관심이 커지게 되었고, 이에 따라서 여러 가지 보안 기술이 나오고 있다.

현재 인터넷의 주요 보안 기술로는 가상사설망(VPN) : 인터넷과 인트라넷간 안전한 통신망 제공, 방화벽

본 연구는 한국과학재단 지역협력연구사업(R12-2003-004-01002-0) 지원으로 수행되었음.

(FireWall : 인트라넷 보호의 일차적인 방어벽), 침입탐지 시스템(Intrusion Detection System : 이차적인 보안 대책), 침입방지 시스템(Intrusion Prevention System 이하 IPS로 대체함)으로 이루어진다. 주요 보안 기술중 방화벽은 패킷의 내용을 검사하여 접근통제를 수행하기보다는 주로 패킷의 헤더부분을 필터링하여 얻어진 정보를 이용하여 접근통제를 수행하는 즉 문제의 가능성이 있는 네트워크를 차단하는 방식이라서 유연성이 떨어진다[4]. 또한 기존 IDS는 이미 알려져 있는 공격 시도를 감시하면서 탐지했을 경우 해당 관리자에게 경고 메시지를 보내고 침입의 진행 상황을 기록하고 보고하는 것으로 끝나 문제를 즉각적으로 처리하지 못한다[6]. 이에 반해 IPS는 방화벽의 침입차단 능력과 IDS의 침입탐지 능력을 결합하여 침입경고 이전에 공격을 중단시키는 것이 목적이다.

본 논문은 다음과 같이 구성된다. 기존 보안 기술의 취약성과 침입방지 시스템의 필요성을 제시한 서론에 이어 2장에서는 IPS의 장점과 요구사항을 알아보고 리눅스 기반의 공개 보안 툴중 방화벽인 netfilter의 IPTables와 네트워크 침입탐지 시스템(NIDS)인 Marty Roesch의 Snort의 특징을 알아본다. 3장에서는 IPTables의 기본 필터링기능과 Snort의 침입탐지 기

능을 결합한 침입방지 시스템의 설계 및 구현 방법과 실험결과를 살펴보고 4장에서는 결론 및 향후 연구방향에 대하여 기술한다.

2. 관련연구

1. Intrusion Prevention System

가. Intrusion Prevention System 이란?

IPS는 바이러스 웜이나 불법침입/분산서비스 거부공격(DDOS: Distributed Denial of Service) 및 공격 시도를 찾아내 네트워크에 연결된 기기에서 수상한 활동이 이루어지는지를 감시하며, 자동으로 해결 조치를 취한다는 점에서 방화벽이나 IDS와 차별성을 갖는다. 즉 기존 IDS는 이미 알려져 있는 공격 시도를 감시하면서 수상한 네트워크 활동을 찾아내는 것이 목적이며, 이상 네트워크 활동을 찾아냈을 경우 해당 운영직원에게 경고 메시지를 보내고 침입의 진행상황을 기록하고 보고하는 것으로 끝나 문제를 즉각적으로 처리하지 못한다. 즉 IPS는 접근 권한에 의해 허가된 트래픽이라고 해도 공격 의도를 가진 패킷이라면 폐기하게 됨으로써 시스템을 보호할 수 있다.

나. IPS의 장점 및 요구사항

1) IPS의 장점

현 정보보안 시스템에 반해 IPS는 탐지 능력과 차단 능력을 결합한 것으로 명백한 공격에 대해서는 사전 방어 조치를 취함으로써 다음과 같은 장점을 가진다.

- 가) 방화벽에서 취약한 요소를 보완할 수 있는 2단계의 방어(방화벽, IDS)를 제공한다.
 - 나) DoS/DDoS 등과 같은 공격을 차단시킴으로써 네트워크의 악영향을 제거한다.
 - 다) 공격에 대한 조사로 인해 소요되는 관리자 운영 부담을 줄인다.
 - 라) 차단은 모든 트래픽(IP, TCP, UDP 등)을 대상으로 한다.
- 2) IPS 요구사항
- 가) 정확하게 탐지하고 공격을 정밀하게 차단하는 인_라인 장치여야 한다.
 - 나) 라인 속도로 동작하여 네트워크 성능 또는 가용성에 악영향을 주지 않아야 한다.
 - 다) 보안관리 환경 안에 통합되어야 한다.

2. Linux Firewall

가. 리눅스와 방화벽

리눅스는 오픈 소스(Open Source)에 기반을 두고 있기 때문에 운영체제로서의 역할뿐만 아니라 여러 가

지 유용한 도구들을 포함하고 있어 서버 이외의 강력한 기능을 할 수 있는데, 이 중 대표적인 기능이 방화벽이다. 리눅스에서 방화벽 기능을 수행할 수 있는 프로그램은 리눅스의 커널(Kernel) 2.4버전에서는 IPTables가 사용되고 있다.

나. IPTables의 개요

IPTables는 대상 보안 영역으로 설정된 서브넷(Subnet)상의 패킷을 헤더(Header)내용에 따라 필터링 하는 기능을 포함하고 있으며, IPTables의 이와 같은 패킷필터링 기능은 방화벽 구현에 사용될 수 있고 부하분산 등에 필요한 서버에서도 사용될 수 있다.

다. 리눅스 방화벽의 장단점

리눅스 방화벽인 IPTables는 오픈소스에 기반을 두고 있기 때문에 무료로 사용할 수 있고 구현이 매우 쉬우며 유지 및 보수가 간편하다. 또한 Kernel 기반이라 매우 빠르며 소스도 공개되어 있다. 하지만 소스의 공개에 따른 방화벽 우회 공격 등을 비롯 여러 공격 유형에 대처할 수 있는 유연성이 적으며 방화벽 안쪽(Safe Zone)에서의 공격은 막을 수 없다.

3. Snort

가. Snort의 특징

Snort의 개발자인 Marty Roesch에 의하면 "Snort는 실시간 트래픽 분석과 IP 네트워크 상에서 패킷 로깅이 가능한 가벼운(lightweight) 네트워크 침입탐지 시스템"이라고 한다. Snort는 패킷 수집 라이브러리인 libpcap을 기반으로 한 일종의 네트워크 스니퍼로서 미리 정의된 침입 탐지 rule들을 이용하여 이와 일치되는 패킷들을 감시하고 기록하거나 경고할 수 있도록 한다.

나. Snort의 문제점

- 1) 리눅스 커널 2.4의 기능인 IPTables와 연동이 되지 않는다.
- 2) 해당 호스트로 오는 패킷에 대해서만 탐색이 이루어지지 않는다.
- 3) 공격 패킷에 대한 패킷 drop이 이루어지지 않는다.

3. 침입방지 시스템 설계 및 구현

1. 침입방지 시스템의 구성

본 논문에서는 IPS의 요구사항을 만족시키는 리눅스 기반의 침입방지 시스템을 공개 방화벽인 netfilter의 IPTables와 공개 네트워크 침입탐지 시스템(NIDS)인 Marty Roesch의 Snort를 이용하여 설계 및 구현한다.

IPTables의 패킷 수집은 libipq 라이브러리를 통해서 이루어지고 Snort는 libpcap 라이브러리를 통해서 패킷 수집을 하므로 연동에 있어 문제점이 발생한다. 이 문제점을 해결하기 위해서 Honeynet Project의[9] 일환으로 만들어진 Snort_Inline을[11] 사용해서 IPTables를 통과하는 libipq 패킷을 Snort가 사용할 수 있도록 libpcap 형태로 변화시킨다. 패킷의 흐름을 살펴보면 커널 영역(Kernel Space)에서 netfilter의 IPTables로 하여금 libipq 패킷을 큐잉해서 ip_queue 드라이버가 사용자 영역의(User Space) 프로세스가 사용할 수 있도록 보내주면 사용자 영역에서 Snort_Inline에 의해서 패킷형태를 libpcap형태로 변환시킨 후 Snort의 공격 시그니처 rule과 비교한 후 공격으로 판단이 될 경우에는 IPT_DROP() 함수를 이용하여 drop여부를 수행한다. 예를 들면, IPT_DROP() 함수를 이용하여 portscan plug-in은 port scan 패킷을 탐지했을 경우에 이 패킷이 침입방지 시스템으로 막혀있는 내부 네트워크로 빠져나가기 전에 drop을 시킨다. [그림 1]에 패킷의 이동과정과 공격 패킷의 Snort에 의한 탐지로 drop되는 과정을 보여준다.

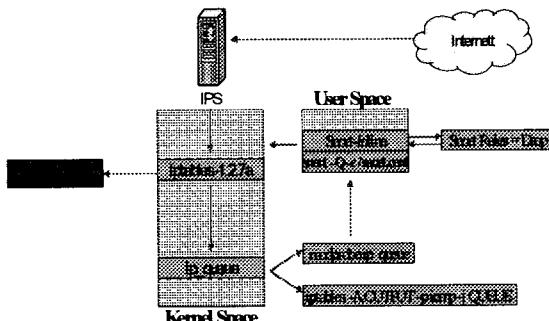


그림2. IPS Packet Drop

2. 침입방지 시스템의 구현

본 논문에서는 리눅스 커널 2.4의 방화벽 도구인 IPTables를 이용하여 NAT환경을 구축하여 외부내트워크와 내부내트워크로 분리시킨 후 Snort Rule의 Alert mode를 Drop mode로 변경시킨 후 Snort_Inline을 IPTables와 결합하여 기존 방화벽의 공격에 대해 능동적으로 대처할 수 있고 침입탐지 시스템의 rule 옵션에 따라 공격 패킷을 DROP 시킬 수 있도록 하였다. [그림 2]에 IPS의 전반적인 구성도를 나타낸다.

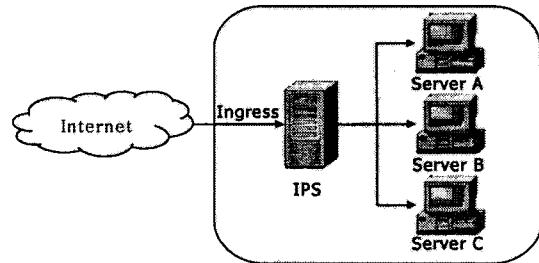


그림2. Intrusion Prevention System

가. 침입방지 시스템을 구현하기 위한 Shell Script

1) Convert-IPS

Snort의 프로토콜 분석, 내용 검색, 매칭을 수행할 수 있으며 오버플로우, Stealth 포트 스캔, CGI 공격, SMB 탐색, OS fingerprint 시도 등의 다양한 공격과 스캔탐지 rule들을 Alert mode에서 Drop mode로 변경해주는 shell script이다.

Snort DOS RULES
<pre>alert ip \$EXTERNAL_NET any -> \$HOME_NET any (msg:"DOS Jolt attack"; ...) drop ip \$EXTERNAL_NET any -> \$INTERNAL_NET any (msg:"DOS Jolt attack"; ...)</pre>

표1. dos.rules에 Conver-IPS.sh를 적용시킨 결과

2) NAT.sh

IPTables를 NAT mode로 설정하고 libipq에 의해 수집된 패킷을 'modprobe ip_queue' 구문을 이용해서 커널 영역에서 사용자 영역으로 보내주고 Snort에 의해 탐지된 Attack Packet을 Drop 시킬 수 있도록 IPTables의 rule을 설정하는 shell script이다. Rob McMillen의 Honeynet Project에[9] 의해 만들어진 rc.firewall.sh script를[10] 수정하였다.

3) startup.sh

현재 실행되고 있는 네트워크 인터페이스를 모두 종료시키고 NAT.sh와 Snort_Inline.sh를 실행한다.

4) snort_inline.sh

Snort_Inline을 데몬 모드로 설정하고 탐지 및 drop 결과를 패킷의 세부내용 까지 로그로 남기도록 실행시킨다[11].

(※ Shell Script 내용은 생략하였음..)

5. 침입방지 시스템 실험 결과 분석

본 논문에서 실험한 환경은 다음과 같다.

- Server

Pentium III 933MHz, 512M RAM, 3c509 10M

Ethernet Lancard, Intel Ether Express 10/100
Managed PCI LAN CARD, Linux Kernel 2.4.18

■ Client

Pentium III 500MHz, 256M RAM, 3c589 10M
Ethernet Lancard, Linux Kernel 2.4.3

먼저 서버에 [표2~6]의 Shell Script를 이용하여 침입방지 시스템을 구축하고 NAT환경을 구축하여 외부네트워크와 내부네트워크로 분리한후 외부네트워크의 클라이언트에서 트래픽 발생기로 MIT's Lincoln Labs에서[12] 제공하는 공격 패킷 데이터를[표 7] 사용하여 내부네트워크로 공격 패킷을 전송시 서버에 구축된 침입방지 시스템의 작동으로 접근 권한에 의해 허가된 트래픽이라고 해도 공격 의도를 가진 패킷을 검출하여 drop시킴으로써 능동적인 방어를 하게되어 관리자의 개입을 더욱 줄일 수 있게 되었다. [그림 6]은 DROP된 패킷에 대한 로그를 보여준다.

구 분	내 용
데 이 터 랑	1,538 MB (1999년 3월, 5일간 수집데이터)
공 격 대 상	Solaris, SunOS, Linux, Win-NT
공 격 내 용	18개 공격 유형에 대한 42회 공격 실사

2. DARPA-11 Attack Data

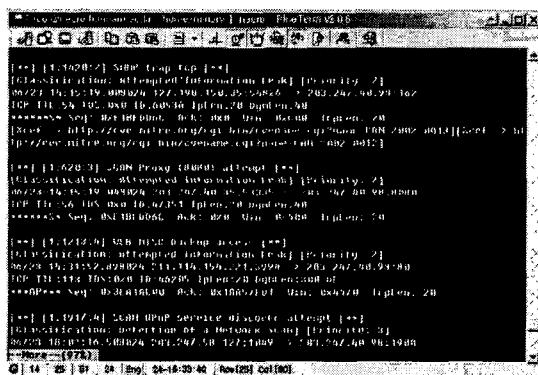


그림4. Attack Packet Drop Log

5. 결론 및 후회 연구방법

최근 국내외적으로 침해 사고율이 증가함에 따라 전 산망에서 주요 정보 유출 및 파괴를 막기 위해 여러 가지 보안 기술이 나오고 있다. 여러 보안 기술 중 방화벽은 내부의 중요한 자원과 외부 네트워크와의 경계를 생성하고, 정책기반의 접근제어를 효과적으로 제공하고 있지만 방화벽은 네트워크 사용 목적상 열린 포트를 가지게 되며, HTTP 웹, DoS공격, 변형 프로토콜을 통한 공격에는 효과적으로 막지 못한다. 또한 침입탐지 시스템은 공격, 침입, 원하지 않는 트래픽을

구별할 수 있다는 점에서 가치가 있다. 하지만 침입탐지 시스템은 정확한 시점에 공격을 차단하지 못하며 실질적인 방어는 관리자의 수동적인 개입을 필요로하게 된다. 따라서 이를 중 정확한 이벤트 정보를 선별하는 것은 관리자에게 과도한 부담을 주며 실제 공격을 놓칠 수도 있다.

본 논문에서는 방화벽의 효과적인 정책기반 접근제어와 침입탐지 시스템의 공격 시그니처 분석에 따른 공격 탐지능력을 결합한 리눅스 기반의 공개 보안 툴인 IPTables와 Snort를 이용하여 침입방지 시스템을 설계 및 구현함으로써 접근 권한에 의해 허가된 트래픽이라고 해도 공격 의도를 가진 패킷을 검출하여 drop시킴으로써 능동적인 방어를 하게되어 관리자의 개입을 더욱 줄일 수 있게 되었다. 향후 연구 과제로는 부정확한 탐지에 의한 정상적인 패킷의 drop을 방지하고 알려지지 않은 공격패턴에 대한 효과적인 대응 방안에 대한 연구가 필요하다.

[참고문헌]

- [1] CERTCC-KR, 통계자료, <http://www.certcc.or.kr/statistics/hack/2002/hack-200206.html>, 2002
 - [2] Martin Roesch, "Snort - Lightweight Intrusion Detection for Networks", USENIX LISA, 1999
 - [3] Paul Rusty Russell, "Netfilter Hacking HOWTO", <http://www.netfilter.org>, 2000
 - [4] Paul Rusty Russell, "Linux 2.4 Packet Filtering HOWTO", <http://www.netfilter.org>, 2000
 - [5] 정성재, "리눅스 iptables를 이용한 다중 서버 통합 보안 시스템 설계 및 구현", 한남대학교 공학논문지, 2003, pp.3-5
 - [6] 고영준, "IDS(침입탐지시스템) 완벽할수만은 없다", <http://www.realattack.com>, 2001
 - [7] 정현철, "Snort 설치 및 운영 가이드", 한국정보보호센터, 2001. pp.5-22
 - [8] 김상정, "Honeypots & Honeynets" KAIST ISC, 2002
 - [9] fyodor, "Know Your Enemy: GenII Honeynets", <http://www.honeynet.org>, 2003
 - [10] Rob McMillen, "rc.firewall.sh", <http://www.honeynet.org>, 2003
 - [11] redmaze, "Snort_Inline Project", <http://sourceforge.net/projects/snort-inline>
 - [12] MIT's Lincoln Labs, "DARPA-LL Attack Data", <http://www.ll.mit.edu>, 1999