네트워크 보안시스템 보안성 평가 연구*

김 점 구**

요 약

네트워크 보안시스템을 단일 요소로 구분하여 점검하고 있는 현실의 문제점을 개선하기 위해 본 논문은 네트워크 보안시스템 점검은 취약성을 찾는 것이 아니라, 네트워크 보안시스템을 이루는 각 보안장비가 유기적으로 잘 작동하는지 종합적으로 점검하는 것임에 착안 네트워크 보안시스템을 점검하는 자동화 방법을 제안하고 이를 구현하였다.

A Study on Evaluation Technique of Network Security System

Jeom Goo Kim**

ABSTRACT

The problems of current network security system, separated by a single element is checked. To improve this, this thesis is to find vulnerabilities in the network security systems, and network security systems, security equipment, organic to make sure each works is a comprehensive review. Automation also offers a way to check it, it was implemented.

Key words : Network Security System, Evaluation Technique

접수일 : 2009년 6월 3일; 채택일 : 2009년 6월 12일

* 본 연구는 지식경제부 지역혁신센터사업인 산업기술보호특화센터 지원으로 수행되었음.

** 남서울대학교 컴퓨터학과

1. 서 론

정보화 시대로 가면서 인터넷과 네트워크가 차지하는 비중은 매우 크다. 비중이 큰 만큼 위협 또한 갈수록 증가하게 되는데, 한 기관의 네트워크 망의 마비는 금액으로 표현할 수 없을 만큼 피해가 크며, 네트워크로 구성된 인터넷의 마비는 상상할 수 없을 만큼 피해가 크다. 우리는 1.25대란으로 그 피해의 심각성을 경험한바 있다. 따라서 현재 이렇게 다양한 위협을 탐지하고 대응하기 위해서 네트워크 망에 여러 가지 보안장비를 추가로 구성하여 운영하고 있으며, 이런 시스템을 네트워크 보안시스템이라 한다.

하지만, 이렇게 보안시스템을 구축하여 운영해도 위협은 항상 존재하며, 항상 침해를 당한다. 대부분의 침해는 잘못된 보안 정책과 시스템 구성 및 운영에 있으며, 이를 사전에 점검하고 조치를 취한다면 많은 위협을 예방할 수 있다. 따라서 현재 대부분의 기관이나 업체는 주기적으로 네트워크 보안시스템을 점검하고 조치를 취하고 있다. 사전에 보안시스템을 점검하는 것은 매우 올바른 방법이지만 대부분 취약성 점검도구나 단일 보안시스템 점검도구로 네트워크 보안시스템을 점검하는 잘못된 방법으로 점검을 하고 있으며, 이러한 점검 방법은 유기적으로 작동하는 네트워크 보안시스템을 종합적으로 점검할 수 없을 뿐만 아니라, 이를 점검하기 위해서 보안전문가의 필요 이상의 노동력과 시간, 비용이 들어간다.

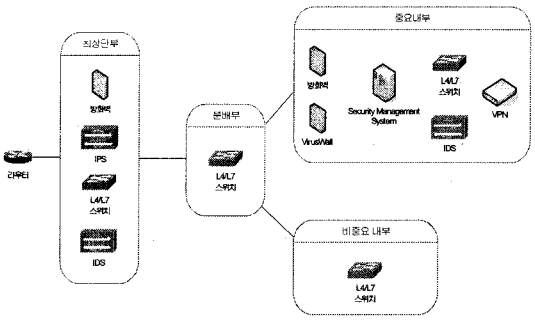
따라서 본 논문은 보다 정확하고 효율적인 네트워크 점검 방법을 제안하고 이를 구현 시험하였다.

2. 관련연구

2.1 네트워크 보안시스템 구조 분석

우선적으로 네트워크 보안시스템 점검하기 위해서는 네트워크 보안시스템의 구조가 어떻게 이루어지고 있는지 알아야 한며, 네트워크 보안시스템 구조를 분석하기 위해서는 구조를 이루는 요소가 무엇인지 알아야 한다. 모든 네트워크 구조를 분석할 순 없지만, 몇몇의 대표적인 관공서, 금융망, 학교 망을 비교 분석함으로써, 대표적으로 네트워크 보안시스템을 이루는 구성요소가 무엇인지 알 수 있다

네트워크 보안시스템 구축 우수 사례 15개 망을 비교 분석하면서 네트워크 보안시스템 환경에 대한 공통적인 부분과 상이한 부분을 찾을 수 있었다. 공통적인 부분은 네트워크 보안시스템을 이루는 최소한의 보안장비를 갖추고 있었으며, 상이한 부분은 시스템의 자원의 중요도와 효율성에 따라 보안시스템을 이루는 요소의 배치가 다양하게 이루어지고 있다는 것이다. 다음 (그림 1)은 다양한 네트워크 보안시스템 망을 일반화 한 것이다.



(그림 1) 일반화된 네트워크 보안시스템 구성

(그림 1)의 일반화한 네트워크 보안시스템 망을 이용하여 구성요소들을 구분 및 분류하였으며 그 내용은 <표 1>과 같다.

〈표 1〉 네트워크 보안시스템 구성 요소

네트워크 시스템	보안 시스템
라우터, 스위치, 허브, 서비스 서버, PC	방화벽, 침입탐지시스템, VPN, ESM,

<표 1>과 같이 네트워크 보안시스템을 크게 네트워크시스템과 보안시스템으로 구분할 수 있다. 네트워크시스템은 서비스를 제공 및 사용하는 요소들로 이루어져 있으며, 보안 시스템은 네트워크 시스템이 안전하게 작동되고 유지될 수 있도록 도와주는 보안/관리 요소로 이루어져 있다. 본 논문에서는 서비스 제공과 이용에 관련된 네트워크 시스템 요소들을 점검하는 방법은 제외하며, 순수하게 보안시스템을 점검하는 방법에 대해서 언급을 한다. 또한, VPN와 ESM은 네트워크 위협에 대한 탐지와 방어, 대응적 요소가 없기 때문에 점검하는 방법에서 제외한다.

따라서 본 논문에서는 네트워크 보안시스템을 이루는 다양한 구성 요소 중 필수적으로 사용 및 운용되고 있는 방화벽와 침입탐지시스템에 대해서 이 두 시스템들이 유기적으로 올바르게 작동하고 있는지 점검하는 방법에 대해서 언급을 하겠다.

2.2 보안시스템 점검 방법

네트워크 보안시스템을 구성하는 요소들은 네트워크 환경과 규모에 따라 다양하다. 이런 다양한 네트워크 보안 시스템을 점검을 하려면 일관성 있는 점검방법과 시나리오가 필요하게 된다. 기존의 네트워크 보안시스템의 점검 방법을 분석하고 본 논문에서 제안하는 3단계 시나리오 기반 점검 방법에 대해서 알아보겠다.

2.2.1 기존 네트워크 보안시스템 점검 방법

현재 대부분 이루어지고 있는 네트워크 보안시스템 점검 방법은 취약성 점검 도구를 이용하는 방법과 단일 점검 도구를 이용하는 방법이 있다. 대표적인 취약성 점검 도구로는 nessus가 있으며,단일 보안 장비 점검 도구로는 영국 블레이드 소프트웨어사 IDS infemer와 Firewall infemer가 있다.

우선 취약성 점검도구는 시스템 및 운영체제에 대한 취약성은 찾을 수 있지만, 네트워크 보안시스템이 유기적으로 올바르게 작동되는지 점검할 수는 없다. 뿐만 아니라, 침입탐지시스템과 방화벽을 스텔스 방법을 이용하여 구성했다면, 더욱더 점검하기가 까다롭다. 따라서 취약성 점검도구를 이용한 네트워크 보안시스템을 점검하는 것은 매우 부적절한 방법이지만, 아직도 많이 사용되고 있는 실정이다. 두 번째 방법인 단일 보안 장비를 점검하는 방법은 단일 네트워크 보안 장비를 효율적으로 점검할 수 있으며, 독립적으로 폐쇄된 환경에서 점검을 할 수 있다는 장점이 있다. 또한, 점검 방법이 매우 단순하여 쉽게 사용할 수 있다는 장점이 있다. 단일 시스템 점검 작동 방식은 실제 payload가 없는 해킹 공격코드를 만들어 네트워크상에 패킷을 내보내며, 이를 침입탐지시스템이나 방화벽이 올바르게 대처하는지 모니터링 하는 방식이다. 이러한 단일 보안 장비를 점검하는 방법은 아쉽게도 하나의 보안장비만을 점검한다는 단점이 있으며, 네트워크 환경에서 유기적으로 보안시스템이 작동하는지는 점검할 수 있는 방법은 없다.

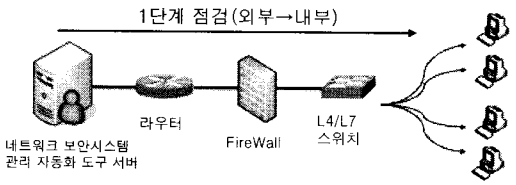
2.2.2 3단계 시나리오 기반 점검방법

이와 같이 현재 이루어지고 있는 점검방법들은 단일 보안장비를 점검하기에는 부족함이 없지만, 종합적으로 네트워크 보안시스템을 점검할 수 있는 방법이 없다. 따라서 본 논문에서는 네트워크 보안시스템이 유기적으로 잘 작동하고 있는지를 종합적으로 점검할 수 있는 3단계 시나리오 기반의 방법을 제안한다.

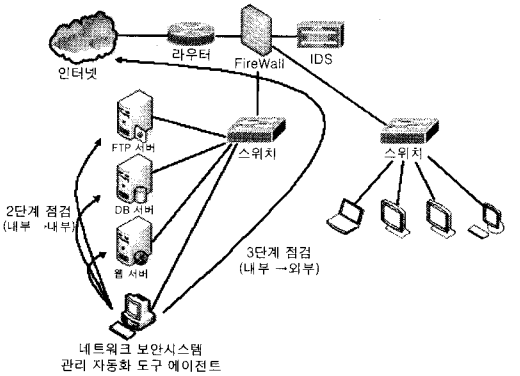
3단계 시나리오 기반 점검방법은 가상의 외부침입자 역할을 하는 서버와 가상의 내부 침입자 역할을 하는 에이전트를 구성하여 점검하는 방법이다. 점검 서버는 (그림 1)과 같이 외부에서 내부 네트워크 망을 점검하며, 내부 침입자 역할을 하는 에이전트는 (그림 2)와 같이 내부 네트워크 망과 내부에서 외부 네트워크 망을 점검한다.

이와 같은 점검방법은 현재 이루어지고 있는 모든 네트워크 위협을 표현하여 점검할 수 있는 장

점이 있으며, 네트워크 보안시스템이 유기적으로 올바르게 작동하는지와 보안시스템 구성에서 취약한 부분을 찾을 수 있는 장점이 있다.



(그림 2) 1단계 점검 시나리오



(그림 3) 2, 3단계 점검 시나리오

2.2.3 No payload를 이용한 점검

네트워크 보안시스템을 점검은 각 보안시스템을 이루고 있는 구성 요소인 장비들이 올바르게 위협을 탐지하고 방어하는지를 점검하는 것이다. 이러한 점검 방법은 점검을 하기 위한 위협 이벤트가 필요하다. 다시 말해, 이는 위협이 있어야 각 보안 장비들이 반응을 보이며, 이 반응에 대한 메시지를 분석함으로서, 적절하게 대응하는지를 알 수 있는 것이다. 이렇게 위협에 대한 보안시스템의 반응과 처리 대응 결과를 보기 위해서 실제 사용되고 있는 해킹 툴이나 위협 도구를 사용해서는 안 된다. 따라서 네트워크 보안시스템에 장애를 주지 않고 점검할 수 있는 점검 방식이 필요하며, 본 논문에서는 실제 해킹 툴이나 공격 도구들을 수집 분석하여 공격 payload 부분을 제거한 점검 방식을 이용하였다. 이는 각각의 해킹 툴이나 위협 도구들을 분석해야 하는 어려움이 있지만, 이 방식은 위협을 매우 유사하게 표현할 수 있으며, 보안장비로부터 확실하게 반응과 대응의 결과를 유도할 수 있는 장점이 있다.

3. 시스템 구현 및 실험

3.1 점검항목 데이터베이스 구축

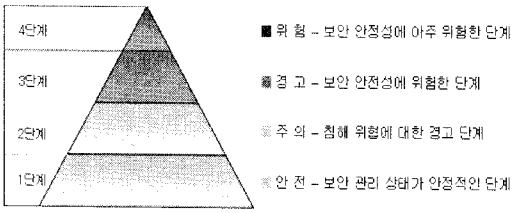
네트워크 보안시스템을 점검하기 위해서는 점검항목들에 대한 자세한 정보와 구분이 필요하다. 이런 자세한 정보는 인터넷이나 기업, 연구기관에서 쉽게 얻을 수는 있지만, 점검 항목에 대한 구분은 각 단체가 기관, 연구소 마다 가지각색으로 구분하여 사용하고 있다.

〈표 2〉 침해 기술 점검항목 구분

구분	침해 기술	설 명	위험등급 (1~4)
네트워크	스캐닝	호스트 및 포트스캔 및 기타	L3~4
	스푸핑	패킷 기반의 스푸핑	L1
	스니핑	패킷 기반의 스니핑	L2~3
	무차별 대입	원격 서비스(ftp, telnet, ssh등)기반의 무차별 대입공격	L2
	서비스 거부	패킷기반의 다양한 서비스 거부 공격	L3
시스템	오버플로우	서비스 기반의 공격	L1~4
	버그	서비스 기반의 공격	L1~4

이는 각각의 장 · 단점이 있기 때문에 쉽게 어느 것이 좋고 나쁘다고 할 수는 없다. 본 논문에서는

<표 2>와 같이 각 점검항목에 대하여 분류하여 데이터베이스화 하였으며, 각각의 위협 항목들을 1~4등급(1. 위험, 2. 경고, 3. 주의, 4. 안전)으로 위험등급을 나누었다.



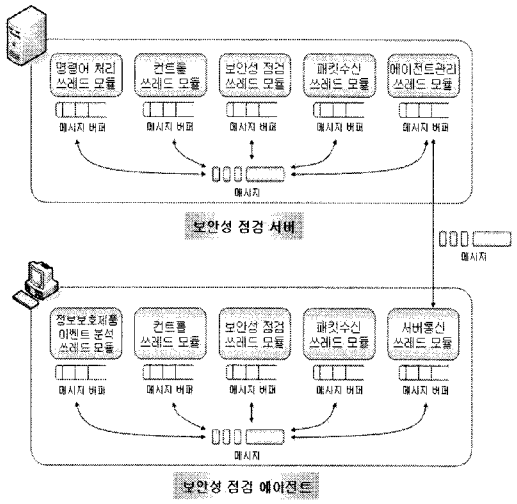
(그림 4) 보안위험등급 표시

3.2 서버/에이전트 기반 점검도구 구현

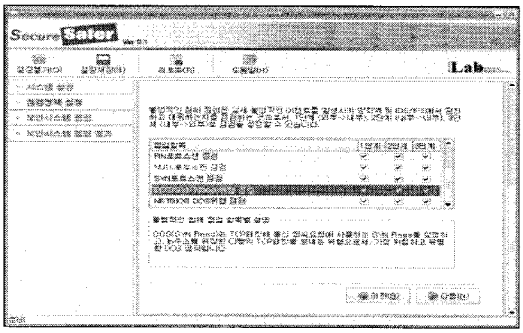
3단계 시나리오 기반으로 네트워크 보안시스템을 점검하기 위해서는 서버와 에이전트 구현이 필수적이다. 또한, 보안장비에 대한 탐지와 대응에 결과 값을 확인하기 위해서는 보안장비로부터 이벤트 값을 받을 수 있어야 한다. 이는 다행스럽게도 현재 모든 보안장비들은 탐지와 대응에 대한 값들을 이기종 시스템에 전송할 수 있는 기능을 포함하고 있다. 대표적으로 사용되는 것이 snmp trap와 syslog가 있으며, 본 논문에서 제안한 점검도구도 snmp trap와 syslog를 이용하여, 보안장비로부터 이벤트 값을 받도록 구현하였다.

(그림 4)와 같이 서버와 에이전트는 쓰레드 기반으로 작동되도록 리눅스 기반으로 구현하였다. 점검 서버는 데몬 형태로 항상 백그라운드에서 작동되도록 구현했으며, 에이전트는 관리자의 편리를 위하여 GUI로 구현하였다. 각 모듈들을 자세히 보면, 점검 쓰레드 모듈은 공격 payload가 없는 공격 패킷을 생성하여 점검을 실시하며, 정보보호제품 이벤트 분석 쓰레드 모듈은 이를 탐지하고 대응하는 정보보호제품의 이벤트를 받아 분석을 하여 올바르게 작동하는지 체크를 한다.

또한, 서버와 에이전트는 3단계 점검 시나리오에서 가상의 공격대상의 역할을 수행하며, 각 항목별로 점검을 할 때마다 서로 동기화되도록 구현하였다. 이렇게 함으로써, 점검에 대한 탐지, 대응, 차단에 대한 정보를 정확하게 얻을 수 있다.



(그림 5) 서버/에이전트 기반 점검도구 구성



(그림 6) 네트워크 보안시스템 점검 도구

2.3 실험

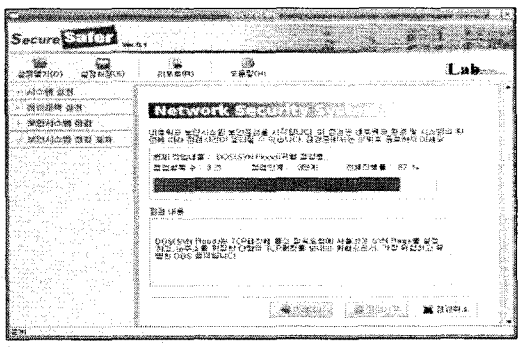
본 논문에서 구현한 점검도구는 소규모 학교 망에서 실험 분석하였다. 점검 대상 보안장비는 다음 <표 3>과 같다.

점검 도구의 실험은 점검이 올바르게 이루어지고 있는 확인하게 위해서 점검하는 동안 보안장비들을 실시간으로 모니터링 하여 점검 도구와 비교

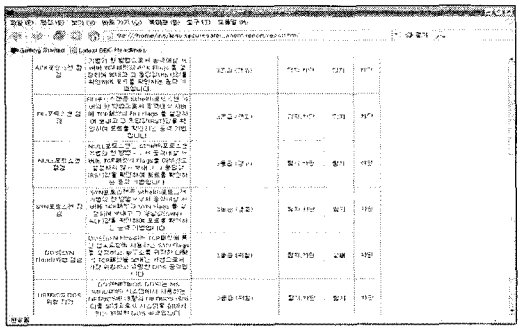
분석하였으며, 또한, 점검 도중의 네트워크 패킷을 캡쳐 하고 모니터링 하여 점검이 올바르게 이루어지고 있는지 확인하였다.

〈표 3〉

구 분	항 목
보안장비	상용 IDS : 1대 공개 IDS : 1대(snort) 상용 방화벽 : 1대 공개 방화벽 : 1대(linux 이용)



(그림 7) 네트워크 보안시스템 점검



(그림 8) 네트워크 보안시스템 점검 결과

4. 결론 및 향후 계획

본 논문에서는 네트워크 보안시스템을 올바르고 효과적으로 점검할 수 있는 방법을 제안하고 구현하였다. 또한 구현한 점검도구를 소규모 네트워크 보안시스템에서 실험하고 그 결과를 분석하였다. 3단계 점검 시나리오와 공격 payload가 없는 점검 방법은 네트워크 보안시스템을 정확하고 효과적으로 점검할 수 있다. 하지만, 실제 공격 코드를 구하고 이를 분석하여 payload가 없는 점검 코드를 만드는데 많은 노력과 시간이 필요한 것은 사실이다. 평균 새로운 위협이 발생되었을 때 이를 분석하고 만드는데 3~4일 정도가 소요된다. 물론 이러한 방법이 비효과적이라고 생각될 수 있지만, 기존의 보안전문가가 취약성 점검도구와 단일 보안장비 점검 도구를 이용하는 방법과 비교해 보면 인적, 경제적, 시간적으로 많은 비용을 줄일 수 있을 뿐만 아니라, 더 정확하게 점검할 수 있다는 것이다.

본 논문에서는 보안장비를 침입탐지 시스템과 침입차단 시스템으로 제안하여 구현, 실험하였지만 향후, VPN, VirusWall과 같이 다양한 보안장비를 갖춘 네트워크 보안시스템을 점검할 수 있도록 보완 개발할 예정이다.

참 고 문 헌

[1] 문호성 외, "보안정책 서버의 경보 데이터 분석 모듈 설계 및 구현", 한국정보처리학회 춘계학술발표논문집, 2002

[2] 박준홍, 남길현, "대규모 조직에 적합한 계층적 구조의 통합 보안관리 시스템에 관한 연구", 한국정보보호학회지 학술대회지, 2001.

[3] 손우용, 송정길, "통합보안 관리시스템의 침입탐지 및 대응을 위한 보안 정책 모델", 한국컴퓨터정보학회논문지, 제9권, 제5호, 2004.

[4] 이영석, "능동 네트워크 기반의 능동 보안 관리 시스템", 한국통신학회논문지, 제29권, 제4C호, pp. 559-569, 2004.

[5] Judy Novak, Stepahn Northcutt, "Network INstrusion Detectiom", New Riders Publishing,

2003.

[6] Randy Heffner, "Enterprise Application Security Integration", IT Trends 2002, December 2001.

[7] Michael O'neill, "Unix System in a Large Enterprise Environment-Axent ESM", SANS Institute Information security Reading Room, June 2001.

김 점 구

광운대학교 전자계산학과(이학사)
광운대학교 전자계산학과(이학석사)
한남대학교 컴퓨터공학과(공학박사)
(주)제성프로젝트 연구원
(주)시사컴퓨토피아 인터넷사업본부장
현재 남서울대학교 컴퓨터학과 교수