네트워크 자원의 로그 분석을 통한 보안 위협 탐지

김진홍* · 이행곤** · 조인준*

*배재대학교, **한국전자통신연구원

The detection of threats using loging data analing of network resource

Jin-Hong Kim* · Haeng-Gon Lee** · In-June Jo*

*Paichai University, **KISTI

E-mail : {jhkim, injune}@pcu.ac.kr, null@kisti.re.kr

요 약

정부, 기관(연구기관, 교육기관 등) 심지어 일반 개인 생활에서 인터넷의 활용도가 증가하면서 네트워크 장비의 중요성은 한층 강조되고 있다. 현재 네트워크 장비의 보안은 방화벽, 침입탐지장치에 의존하고 있으나, 이 장비들은 잘 알려진 공격을 기준으로 패턴 매핑 방식으로 검출한다. 따라서 잘 알려지지 않은 공격에는 취약하다.

본 논문에서는 네트워크 보안장비를 위회한 보안위협이 탐지될 경우 네트워크 자원에서 발생하는 로그를 실시간으로 수집하여 관리함으로써 침해사고 시 그 원인을 분석할 수 있는 근거자료를 확보하고, 실시간 로그 분석을 통해 신속한 보안 위협의 탐지 및 해결방안을 제공한다.

키워드

로그분석, 보안위협탐지, 방화벽, 라우터, 네트워크 보안

Ⅰ. 서 론

국내 인터넷 서비스는 1998년 도입된 이래 세계에서 유래가 없는 속도로 가입자 수의 증가로 전세계 인터넷 시장을 주도하였다. 이러한 국내 인터넷의 폭발적인 성장 배경에는 인터넷 이용자의 수요 증가와 정부의 적극적인 인터넷 보급정책 그리고 ADSL/Cable Modem 등 망 사업자의 치열한 경쟁의 상호작용 결과이다. 이러한 국내 인터넷 시장의 빠른 성장에 힘입어 이제 인터넷이 보편적인 사용 환경으로 정착하였고, 경제·사회적 필수 서비스로 자리 잡게 되었다.

그러나, 인터넷의 발전과 함께 악의적인 목적으로 인터넷을 사용하는 공격자들이 증가하게 되었고, 인터넷은 커다란 공격의 발판된 것이다. 현재 네트워크 장비 보호는 방화벽이나 침입탐지장치가 설치되어 있으나 이 장비들은 잘 알려진 공격에만 보안이 가능하기 때문에 보안상의 취약점이 노출되었다. 따라서 이러한 취약점에 의하여 국내는 2003년 1월 25일날 모든 네트워크망을 마비시킨 사이버 테러가 발생하였고, 극심한 사회적 혼란을 초래하게 되었다. 다양하게 증가하는 공격을 방어하기 위한 장비인 방화벽과 침입탐지장치의 성능이 미흡하다는 것이다. 따라서 고도화되는 공격의 피해를 최소화하기 위하여 네트워크 장비 로그를 체계적으로 분석하고, 분석된 결과를 네트워크 관리자에게 전달하여 네트워크 자원과 보안 위협에 대한 안정성 제공을 위한 서비스가 절실히 필요한 상황이다.

본 논문은 고도화되는 공격의 피해를 최소화하기 위하여 네트워크 장비에서 발생하는 로그를 체계적으로 분석하여 보안위협요소를 도출하고, 분석된 결과를 네트워크 관리자에게 제공하는 시스템을 개발하여 네트워크 자원과 보안 위협에 대응할 수 있도록 한다.

Ⅱ. 본 론

1. 네트워크 위협요소

전통적인 공격모델의 변화는 미국에서 보안 시스템이 보편화되면서 이를 극복하고자 하는 공격자들의 노력에서 시작된다. 즉, 공격자와 방어자의 뚫고 막는 경쟁으로 인한 것이다. 현재의 보안 모델에서는 일반적으로 공격자가 항상 우세하며 방어자는 알려진 공격방법에만 대응하는 방식의 사이클을 가진다. 또한 인터넷이 실세계의 중요한 일부가 되면서 "사이버테러", "사이버범죄" 또한 구체화, 조직화 되는 것도 전통적인 공격모델의

변화에 큰 영향을 주고 있다.

전통적인 공격기법 변화의 가장 큰 원동력은 방어자의 보안수준 향상이다. 파이어월 및 침입탐지시스템(IDS, Intrusion Detection System)의 보편화는 전통적인 공격기법에 매우 효과적인 대응수단을 제공한다. 그리고 여러 국가의 CERT 간의 공조체계도 공격자의 활동범위를 좁혀가고 있다. 하지만 이러한 장벽을 극복하고 성공적으로 시스템에 침입하기 위한 기술 및 도구들이 최근 몇 년간 지속적으로 개발되고 있다. 대표적인 도구로는 hping, Firewalk, Loki Project, pcap, libnet 등을 들 수 있다. 그리고 이러한 변화 중 주목을 끌만한 것은 바로 98년 중반에 공개된 백오러피스이다. 이러한 기술 및 도구들의 등장은 새로운 공격기법의 패러다임으로 가는 과도기이며, 기반 기술이 된다.

2. 네트워크 보안 기술 개발 동향

지금까지는 침입차단시스템과 침입탐지시스템, 바이러스 백신 등과 같은 단일 기능을 갖춘 보안 시스템들이 주로 개발되어, 단순하게 주소 위주의 차단 정책과 탐지 후 보고 등 수동적인 대응에 의존하여 왔다. 최근 갈수록 복잡해지고 다양화되어 가는 악성 침해 기법들을 차단하기 위해서 보다 새로운 형태의 보안 시스템들이 나타나고 있다.

또 다른 추세로서 네트워크 장비에 보안 기능들이 직접 탑재되는 임베디드 보안 형태가 자리잡아 가고 있으나, 대부분의 기능이 소프트웨어적으로 개발되어 네트워크의 고속화 추세에 뒤따르지 못하는 문제점들이 있다. 최근 이를 해결하기 위해 전용 칩을 탑재하는 등 성능 향상에 초점을 맞춘 하드웨어형 장비들이 개발되고 있다. 또한, 다양한 보안 장비들을 상호연계한 종합적인 네트워크 보안 서비스를 제공할 수 있도록, 통합보안관리 시스템과 연계하거나, 침입 탐지시 이를 직접 차단할 수 있도록 단일 플랫폼에 다양한 기능들을 탑재한 통합보안제품 등 아래와 같은 다양한 추세가 있다.

2.1 보안 라우팅 장비(Secure Router)

네트워크 장비 업체들이 자사의 스위치나 라우터 기술을 이용하여 하드웨어 기반의 보안 장비를 내놓고 시장 공략에 적극 나서고 있다. 시장분석 자료에 의하면 네트워크 장비 개발 업체들의 보안 장비 점유율이 점차 상위권으로 이동하는 것을 알 수 있다.

스위치나 라우팅 장비를 취급하는 업체에서는 자사의 고성능 네트워킹 장비에 방화벽과 VPN기능을 추가하는 형태와, 패킷 필터링은 물론, 침입탐지와 콘텐츠 필터링의 기능(layer2~layer7)까지 제공하기도 한다. 그리고 SSL 가속기나 VPN 가속보드 등을 탑재하여 고속처리를 제공하고 있다.

2.2 통합보안시스템

최근 하나의 플랫폼에 다양한 보안 기능을 탑재한 통합보안시스템들이 출시되고 있다. 보안 시스템은 단독으로 동작하기보다는 다른 기능을 갖는 보안 시스템들과 연계되어 동작할 때, 보다 많은 효과를 가져 올 수 있으며, 비용 절감 효과와 관리의 편이성을 확보할 수가 있다. 이러한 통합보안시스템에는 자사의 보안 시스템들을 탑재하는 경우와 자사의 고성능 플랫폼에 타사의 보안 소프트웨어를 탑재하는 경우, 두 가지로 크게 나누어 볼 수 있다.

한 장비 내에 모든 기능을 포함시킬 경우, 장비의 성능 제한과 장비 내에 설치된 성격이 각기 다른 보안 솔루션의 전문성과 각 모듈간의 상호 연동 동작에 대한 성능은 아직 제대로 검증되지 않았지만, 용이한 설치와 관리를 장점으로 들 수 있어, 점차 중소 규모의 네트워크에 도입이 활성화될 것으로 전망되고 있다.

2.3 바이러스 월(viruswall)

바이러스 관련 제품은 예전의 경우에는 감염된 파일의 치료 목적으로 개인용 컴퓨터에 설치되어 왔으나, 최근에는 운영체제와 상관없이 네트워크를 통한 파일 다운로드, 웹 다운로드, 응용 프로그램의 실행, 메일 수신 등의 다양한 수단을 통해 급속한 속도로 전 세계 컴퓨터 시스템을 마비시키고 있으며, 무선 단말기기의 확산과 더불어 무선 인터넷으로의 확산이 예상되고 있다.

최근 웜 바이러스 등 새로운 네트워크형 바이러스 형태의 공격에 대응하기 위해, 데스크탑 제품에서 메일 서버나 파일서버에 설치하여 바이러스의 감염으로부터 방어하거나, 게이트웨이 형태로 설치하여 네트워크로 유입되는 바이러스를 방지할 수 있는 게이트웨이용 네트워크 방어 시스템을 개발하고 있다.

2.4 침입방지시스템(Intrusion Prevention System : IPS)

침입방지시스템은 접근제어목록에 따른 접근제어와 탐지 후 통보라는 수동적인 방어 개념의 침입차단시스템이나 침입탐지시스템과는 달리 이상징후가 탐지되면 이를 자동적으로 사전에 차단하는 보안 솔루션이다. 몇몇 회사에서는 차세대 침입탐지 시스템으로 명명하고 있으며, 패킷 필터링과 Stateful Inspection, 접근제어, 침입탐지 등 다양한 기술들이 복합적으로 포함되어 있다.

침입방지시스템은 크게 두 가지 형태로 볼 수 있는데, 한가지는 특정 서버나 호스트에 설치되어 서버의 운영체제나 자원들, 혹은 해당 어플리케이션을 보호하는 형태로 허가되지 않은 시스템 콜이나 API의 실행, 자원의 불법 접근, 유해한 프로그램의 실행 등을 커널과 사용자 사이에서 사전에 탐지 차단하여 보호를 하게 된다. 다른 경우는 네트워크 상에서 해당 유해 패킷을 탐지 시에 즉시 폐기시키는 보안 솔루션이다. 즉, 망에 스니핑

모드가 아닌 인-라인(in-line) 형태로 연결되어서 비정상적인 트래픽을 망 내부로 유입되지 않도록 사전에 폐기시키는 대응 기능을 갖추고 있다.

기존의 시스템들은TCP Reset과 방화벽 signaling으로 대응 처리를 하고 있지만 공격을 정지시킬 수 없으며 복구과정이 필요하다는 단점이 있다. 이에 반해 침입방지시스템과 같은 능동형 보안 시스템은 처리과정 중에 패킷을 폐기하므로 해당 호스트에 트래픽이 도달되지 않아 한층 더 강화된 보호 효과를 가져 올 수 있을 것이다. 그러나 침입탐지시스템이나 침입방지 시스템 모두 침입이 아닌데도 불구하고 침입으로 간주하는 False Positive를 최소화 시키는 것이 관건이 될 것으로 보인다.

2.5 통합보안관리시스템 (Enterprise Security Management : ESM)

통합보안관리는 보안 제품의 네트워크 적용한 이후, 적절한 보안정책에 따른 유지관리, 침해 유형 모니터링 등의 목적으로 사용되는 시스템이다. 분산된 보안 시스템과 네트워크 노드에 에이전트를 설치하고 중앙관리모듈에서 이를 제어하는 개념으로 설계된다. 처음 업체별 독자적인 API를 사용하던 움직임에서 벗어나 국제표준화 기구들에 의한 제안된 로그 및 프로토콜 표준을 채용하는 방향으로 전환되고 있어서, 점차 이기종간에 자유로운 연동이 가능한 시스템으로 발전하고 있다. 이외에도 보안기능뿐만 아니라 시스템의 자원관리와 접근허가, 인증 등의 서비스들과 통합하거나, 기존의 서비스관리시스템(SMS)과 네트워크관리시스템 (NMS)과의 연동하는 형태로 개발 진화되고 있다.

2.6 침입감내시스템(Intrusion Tolerant System : ITS)

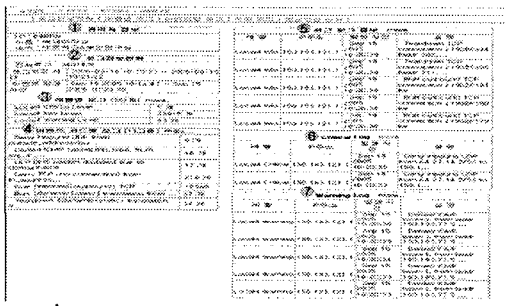
대부분의 기존 보안 장비들은 침입의 방지와 탐지에만 관심을 두고 개발되었다. 고장 감내 시스템의 경우에는 침입이 성공되었다 하더라도 시스템의 중요 서비스의 지속적인 제공을 목표로 무결성과 가용성을 염두에 두고 연구 개발되고 있는 보안 시스템이다.

3. 로그분석 시스템

현재 국내 네트워크 침입 차단 장치보안은 방화벽이나 침입탐지장치를 사용한다. 만약 이 장치의 공격패턴을 우회한 방법 침입될 경우 1.25사태가 다시 발생할 수 도 있을 것이다. 따라서 외부 침입을 조기에 파악하여 실시간으로 상황을 전달하기 위하여 본 논문에서는 네트워크 로그를 실시간으로 제공받아 분석하고, 분석된 결과를 인터넷 웹 환경으로 서비스를 제공한다. 관리자는 언제 어디서든 로그파일을 웹 환경에서 제공하고, 취약점을 실시간으로 분석하여 제공받을 수 있다.

3.1 로그분석

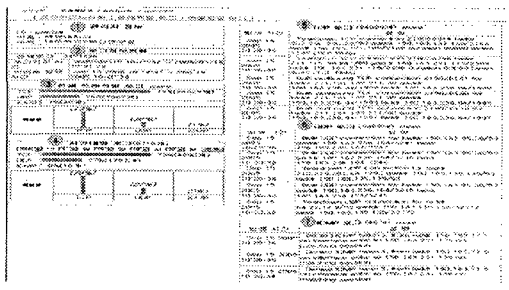
[그림 3-1]는 제공받은 로그정보의 분석 결과이다. '①' 관리자 정보에서는 관리자 아이디와 이름 소속등을 알려주고, '②' 로그정보현황에서는 제공받은 로그 저장및 이벤트 발생시간을 알려준다. '③' 레벨별 로그에서는 로그정보를 분석하여 위험 및 취약한 로그의 수를 제공한다. '④' 이벤트 코드별 로그의 경우 이벤트별로 로그정보를 분석하여 서비스를 제공한다. '⑤' 최근 로그정보의 경우 가장 최근에 분석한 로그정보의 이벤트 발생시간을 분석하여 서비스한다. '⑥' Critical log의 경우 위험수위에 있는 로그정보들을 분석하여 서비스한다. 마지막으로 '⑦'의 경우 위험수위에 있는 로그들을 분석한 결과이다. 따라서 정당한 관리자의 경우 메인으로 로그정보 분석 결과의 서비스를 제공한다.



[그림 3-1] 네트워크 로그정보현황

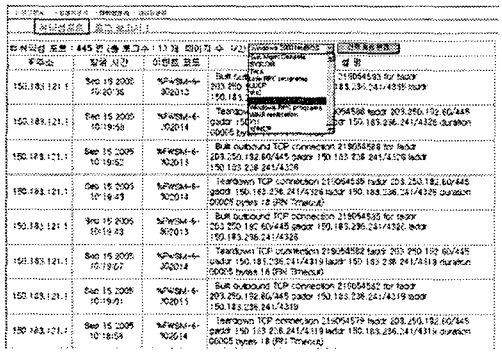
3.2 트래픽분석

[그림 3-2]의 트래픽 정보 현황은 네트워크 로그에서 발생된 트래픽을 종류별로 분류한 것이다. '①' 관리자 정보는 관리자의 아이디와 소속을 제공하고 있으며, '②' 로그정보현황에서는 제공된 로그가 언제였는지를 알려준다. '③'전체 트래픽별 로그의 경우 로그를 모두 분석하여 전송방법에 따라 "TCP/UDP/ICMP"를 %로 구분하였다. '④' 시간대별 로그의 경우 특정시간대를 기준으로 메시지 전송방법의 비율을 측정하였다. '⑤', '⑥', '⑦' 의 TCP, UDP, ICMP 로그에서는 메시지별 로그들을 수집하여 관리자가 분석하기 편리하도록 서비스를 제공하였다.



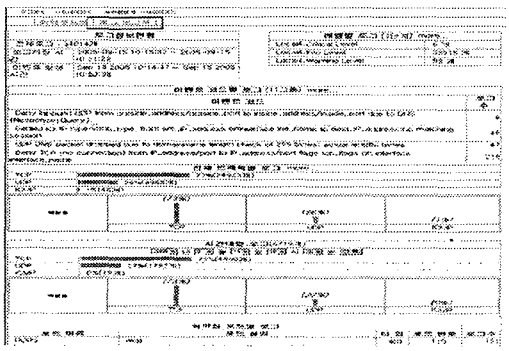
[그림 3-2] 트래픽 정보 현황

3.3 취약점 분석



[그림 3-3] 취약성 포트 리포트

[그림 3-3]과 같이 제공받은 로그정보의 취약점을 분석하여 관리자에게 서비스를 제공한다.



[그림 3-4] 로그 보고서

[그림 3-4]의 로그보고서는 로그 분석결과 및 트래픽 분석 그리고, 취약점 분석결과의 핵심 내용을 한눈에 파악할 수 있게 정리하여 서비스를 제공한다. 로그분석에서는 로그정보현황과 레벨별 로그 그리고, 이벤트 코드별 로그를 정리하여 서비스를 제공하였고, 트래픽분석에서는 데이터 전송방법에 따라 전체 또는 시간별로 사용량을 서비스하였다. 마지막으로 제공된 로그의 취약점 리포트를 근거로 분류하여 관리자가 파악하기 쉽게 서비스를 제공하였다.

III. 결 론

현재 국내 네트워크 보안은 방화벽이나 침입탐지장치와 같은 장비를 설치하였다. 그러나 이 장치들은 알려진 공격기법을 보호할 수 있기 때문에 공격패턴을 우회한 침입방법이 확산될 경우 1.25사태와 같은 대 혼란이 다시 발생할 수 도 있다. 따라서 외부 침입을 조기에 파악하여 실시간으로 상황을 전달하는 실시간 로그분석 시스템이 절실히 필요하였다.

본 논문은 네트워크 자원에서 발생하는 로그를 실시간으로 수집 및 관리하여 실시간 로그 분석을 통해 신속한 보안 위협의 탐지 및 해결방안을 제시하였다.

참고문헌

[1] Cisco Systems, Inc, "Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module System Message Guide", 2004.

[2] SANS Institute, "The Twenty Most Critical Internet Security Vulnerab - ilities The Experts Consensus", October, 2003.

[3] Bruce Schneier, "Applied Cryptography", WILEY, 1996.

[4] 최용락, 소우영, 이재광, 이임영, "통신망정보보호", 그린, p 456~p469, 1995.

[5] 올리프 커치, 테리 도슨, "리눅스 네트워크 관리자 가이드", O'REILLY, 2001.

[6] 이영무, "투덜이 PHP 4", 가메 출판사, 2001.

[7] 박재진, "PHP Bible ver. 4", 영진출판사, 2001.

[8] 김종호, 이승재, "IP 라우팅 프로토콜", 사이버출판사, 2003.

[9] Matt Kolon, "지능형 로지컬 라우터 서비스", Juniper Networks, October, 2004.

[10] 정연서, 류걸우, 남택용, 손승원, "사이버 위협에 대한 보안 솔류션 기술 동향", IITA 기술정책정보단, October, 2002.

[11] 이현우, "네트워크 공격기법의 패러다임 변화와 대응방안", October, 2001

[12] 손승원, "네트워크 보안 기술의 현재와 미래", 2005.

[13] 김사혁, "차세대네트워크(NGN) 수요 및 산업의 변화", March, 2005.