통합보안관리 시스템에서 내부 보안을 향상시킨 보안 솔루션 구조의 설계 및 구현

Design and Implementation of Security Solution Structure to Enhance Inside Security in Enterprise Security Management System

강민균, 김석수
한남대학교 멀티미디어학과

Min-Gyun Kang(card7s@paran.com), Seok-Soo Kim(sskim@hannam.ac.kr)

요약

인터넷의 보급으로 인해 기업의 전산화가 발전함에 따라, 바이러스, 전산망 침해 등 정보화의 역기능도 크게 증가하고 있다. 따라서 오늘날, 기업 보안의 중요성이 매우 강조되고 있다. 이렇게 보안의 중요도가 높아짐으로 인하여 보안 솔루션도 함께 발전하고 있다. 보안 솔루션은 기존 단일 체제에서 통합 보안 관리 시스템으로 발전하고 있으며 통합보안관리 시스템에서 중요한 것은 각 보안 솔루션의 기능과 정책의 적합한 설계이다. 기존의 보안 정책은 외부의 침입으로 부터의 보안을 중요시 해왔으나 현재는 내부의 보안도 그 중요도가 높아지고 있다. 이를 위하여 새로운 구조의 통합 보안관리 시스템을 구축해야 한다. 본 논문에서는 침입탐지차단 시스템을 활용하여 내부보안을 강화한 통합 보안 관리 시스템을 제안, 구현하였으며. 내·외부의 IP와 ID접근을 실험하여 그 결과를 분석하였다.

■ 중심어 : | 통합보안관리 | 보안 솔루션 | 기업 네트워크 |

Abstract

Corporation's computerization developed by diffusion of internet, and dysfunction of information is increasing greatly with virus, computing network infringement. Therefore, the today, corporation security is more and more emphasized. Security solution by that importance of security rises so is developing together. Security solution is developing to ESM system in existing single system and important thing is function of each security solution and optimizing design of policy. Existent security policy taking a serious view security from external invasion but security of interior the importance rise the today. Accordingly, must construct ESM system of new structure for this. This paper proposes and embodied integration security administration system that solidify interior security utilizing IDS. Experiment external IP and ID access and analyzed the result.

■ keyword : | Enterprise Security Management | Security Solution | Enterprise Network |

* 본 연구는 2005 산학협동재단 학술연구비사업 지원으로 수행되었습니다.

접수번호 : #050518-002
접수일자 : 2005년 05년 18일
심사완료일 : 2005년 08월 23일
교신저자 : 강민균, e-mail : card7s@paran.com

I. 서 론

컴퓨터 하드웨어의 발전과 데이터 전송의 필요성이 대두 되면서부터 인터넷은 발전하였다. 이러한 인터넷은 연구적 성향에서 상업적 성향으로 좀 더 일반화 되면서 많은 사람들이 이용하게 되었다. 이러한 상업적 발전은 전자상거래(Electronic Commerce), 홈뱅킹(Home Banking) 등 여러 가지의 서비스들로 개발되어 사용자가 크게 증가하고, 인트라넷 구축을 통한 기업이나 교육기관 등 사회 전 분야에 걸쳐서 전자기록 및 자료 이용이 보편화됨에 따라 이를 악용하는 불건전 정보 유통 및 정보 범죄와 같은 정보화의 역기능 또한 크게 증가하고 있다[1].

이러한 인터넷의 취약점인 정보범죄의 유형은 전산망 침해행위, 전자기록 위·변조, 각종 음란물 유통, 통신상의 명예훼손, 바이러스 제작 유포 등이 있으며, 이러한 행위들은 외부에서 내부로의 침입을 기반으로 하고 있다[2].

이러한 침입을 막기 위하여 보안 시스템을 운영하고 있는데, 현재 보안 시스템은 방화벽 시스템(Firewall System) 과 침입방지시스템(Intrusion Detection System)이 대표적이다. 하지만 침입의 유형이 매우 다양화 되면서 침입에 대한 탐지 및 대응이 매우 복잡해지고 보안제품에 따라 기능 및 제어가 어려워지고 있다. 그로인해 다양한 보안솔루션에 대한 보안 관리자들의 통합보안관리가 요구되었고 이러한 요구를 충족시키기 위하여 다양한 보안솔루션의 통합관리 시스템의 개발이 중요한 과제로 대두 되었다[3].

본 논문은 이러한 통합보안관리 시스템을 구축하기 위한 보안 솔루션의 구조에 대하여 연구하였다. 이를 위하여 기존 통합보안관리 시스템을 분석해 보고 이를 기반으로 좀 더 보안을 강화할 수 있는 통합보안관리 시스템을 제시하게 되었고 이러한 시스템을 직접 테스트해 보았다. 이를 테스트하기 위하여 리눅스 기반의 로그분석을 통한 IDS을 이용하였으며 사내 네트워크를 가상IP체계를 사용하여 설계한 후 테스트를 하였다.

II. 관련 연구

1. 침해행위와 공격

침해행위란 해킹이나 정보의 위변조를 통해서 시스템에 침입하거나 데이터의 위변조로 인한 정보의 손실 등을 말하며 공격이란 시스템을 마비시키거나 시스템이 정상적으로 유지될 수 없도록 방해하는 행위 등을 말한다. 일반적으로 인터넷에서 침해행위나 공격을 하기 위해서는 먼저 정보를 수집해야 한다. 공격의 대상이 되는 곳의 시스템에 대한 정보, OS에 대한 정보, 보안 솔루션이나 기타 네트워크 장비에 대한 정보를 수집하여 대상의 취약점을 분석해야한다. 이러한 과정을 거친 후 시스템 침입을 하게 되는데 실제 개별 시스템에 침입하는 과정으로, 정보수집에서 수집한 정보를 바탕으로 가장 취약한 부분을 공격하게 된다. 이렇게 침입을 하거나 공격을 들어왔을 경우 이 상태에서 끝나는 경우도 있지만 대부분 공격 전이를 하게 된다. 공격전이란 공격 대상에서 다른 공격대상을 찾고 이를 다시 공격하는 것으로 이렇게 되는 경우는 더욱 공격에 대한 탐지를 하기 힘들어진다. 이러한 공격을 막기 위해서 일반적으로 침입탐지 시스템 또는 침입차단 시스템 또는 이를 혼합한 침입탐지차단시스템 등 여러 가지 보안 시스템을 선택하여 보안을 강화할 수 있다[4][5].

2. 통합 보안 관리 시스템 개념

통합 보안관리 시스템(ESM : Enterprise Security Management)이란 침입 차단 시스템, 침입 탐지 시스템, 가상 사설망 등 이 기종 보안 솔루션을 중앙에서 통합 관리하는 시스템으로 솔루션 간 상호 연동을 통해 전체 IT 시스템에 대한 보안 정책 수립이 가능한 시스템이다[6].

통합 보안 관리 기술 수준은 현재 개발사 제품에 대한 모니터링 기능이 구현되어 있지만, 앞으로는 보안 프로토콜의 표준화를 통해 다른 곳에서 개발한 제품을 포함한 이기종 보안 시스템에 대한 모니터링 기능을 가지도록 발전할 것이며, 수집된 자료를 분석하여 보안 사건에 대한 리포팅 기능과 함께 각 보안시스템에

대한 세부 정책관리 기능이 가능한 단계로 발전할 것으로 예상되고 있다. 통합 보안 관리를 위한 보안 표준 프로토콜로는 체크포인트사의 Firewall-1/VPN을 중심으로 컨텐츠 보안, 인증 및 권한 관리, 침입 탐지 시스템, 사건 분석 및 리포팅, 디렉토리 서버분야의 프레임워크 파트너를 구성하는 OPSEC과 IETF의 IDS 상호연동 메시지 표준을 구축하고 있는 IDWG 워킹그룹이 대표적이다.

통합 보안관리 시스템은 워크플로우에 따라 사용자 및 정책 관리자와 취약성 및 위협 평가로 분류할 수 있다[3,6-8]. 보안 관리의 중요성이 강조되면서 점차 도입하는 기업이 늘고 있는 통합 보안 관리 솔루션이 다양한 이기종 보안 솔루션을 중앙 집중 관리하고, 보안 솔루션 이벤트의 상호간 연관성 분석을 통해 오 탐지를 최소화하는 방향으로 발전하고 있다. 자원 낭비를 줄이고 효율적인 중앙 집중 관리를 가능하게 한다.

비즈니스의 활성화와 더불어 정보시스템은 내·외부자에 의해 노출되고 있다. 이에 따라 기업의 신뢰도와 서비스 가용성이 더불어 위협받고 있는 게 사실이다.

III. 통합 보안 관리 시스템 구조 설계

1. 통합보안관리 시스템 의 필요성과 보완 요구점

최근 정보통신부가 조사한 '정보보호 실태조사'에 따르면 국내 기관들의 정보보호 투자비율은 선진국에 비해 크게 부족하다. 특히 보안 솔루션의 도입 패턴을 두고 볼 때, 통합 보안 관리와 취약점 분석 등 침해 사고에 대한 예방 부분에 있어서는 그 준비가 매우 저조한 것으로 나타났다. 2003년 발생했던 1.25 인터넷 대란이나 복합적인 사이버 침해 사고들의 원인이 관리자가 시의 적절하게 대응하지 못했기 때문이라는 사실을 감안하면 심각한 문제가 아닐 수 없다.

하지만 현실적으로 각 보안 솔루션들을 운영하면서 상호연관성 분석을 통해 이상 징후를 찾아낼 수 있는 수준의 정보보호 전담조직 및 전문 인력을 갖추기란 쉽지 않다. 방화벽, 침입탐지시스템, 가상사설망(VPN), 안티 바이러스와 같은 다양하고 전문화된 보안 솔루션의 도입은 증가하는 반면, 보안 솔루션에 대한 전문지식 보유 인력은 여전히 부족하기 때문이다. 그렇다고 보안만 전담하는 관리자를 두면 사전 방지 및 대응 조치가 가능한 것도 아니다. 각 보안 솔루션이 처리하는 방대한 양의 보안 이벤트와 분석 작업은 결코 수작업으로 처리할 성질의 것이 아니다.

보안 관리의 중요성이 강조되면서 점차 도입하는 기업이 늘고 있는 통합 보안 관리 솔루션은 다양한 이기종 보안 솔루션을 중앙집중 관리하고, 보안 솔루션 이벤트의 상호간 연관성 분석을 통해 오탐지(False Positive)를 최소화하는 기능을 갖고 있다. 또한 기업의 보안 관리자들이 행하는 단순하고 반복적인 업무(모니터링/로그 분석, 보고서 산출)의 자동화로 정보보호정책 및 지침 수립 등의 중요도 높은 업무에 집중할 수 있게 도와 기업의 비즈니스 연속성을 확보한다[7][8].

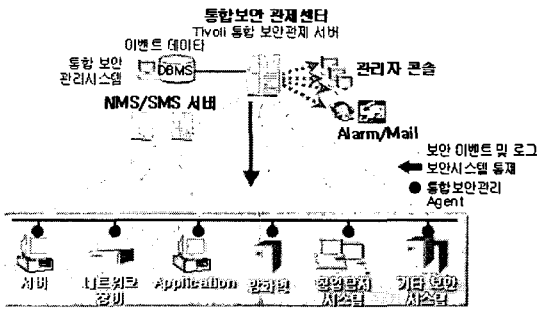

그림 1. 통합보안관리시스템 구조도

하지만 이러한 통합 보안 시스템을 보면 [그림 1]과 같이 구조를 이루고 있다. 이 구조를 볼 때 앞에서 말한 것과 같이 내외부적으로 보안을 이루어야 하는데 있어서 현재 구축되어지는 통합 보안 시스템은 외부적으로는 기업에 맞는(네트워크 속도, 보안의 중요도) 보안 정책을 수립할 수 있지만 내부적으로는 상당한 위험에 노출 되어져 있다. 이러한 내부적 노출을 방지하기 위하여 내부 서버에 한 번 더 보안 시스템을 구축하는 구조를 이루어야 한다. 외부적인 침입에 의해서만 보안이 철저하고 내부 침입에 대비하지 않는다면 기업 내 구성원의 해킹이나 구성원의 사소한 실수로 인하여

구성원 컴퓨터가 노출이 되어 진다면 외부적으로 철저히 보안을 이룬다 하더라도 무용지물이 된다.

2. 내부보안을 향상시킨 통합보안관리 시스템

제안된 통합보안관리 시스템의 보완을 알고리즘으로 표현하면 다음과 같은 구조를 형성한다.

```
main()
{  while(end connection)
       {   N_data = P_filter(internal_network);
        S_data = P_filter(server);
       D_module(N_data);
       D_module(S_data);
       }
          return 0; }
D_module(DATA)
{       connection DB;
            txtcutlist =  reader["Cut_list"];
            txtuser_list =  reader["User_list"];
            query = "insert into web_log values('access_data')";
            stmt.executeQuery(query);
            if (txtcutlist ==access_data)
            {  A_Module(); }
            else if (txtuser_list ==access_data)
            {  A_Module();  } }
P_filter(log_file)
{  fin = new BR(new FR(log_file));
       while( fin != null{
       tokenizer.parseToken(line);
       line = fin.readLine();
       tokenizer.storeToken();
       file.close();
       clearlog.clear(logpath);
       conf.close();
   return line; }
A_Module()
{  mail_send("Warning message");
   sms_send("Warning message");
   consol_call("Warning message");}
```

* N_data : Network data, S_data : Server data, D_module : depensive module,
A_Module : Alarm Module, P_filter : Packet filter, A_data : Access data,
BR : Buffer Reader, FR : File Reader

A. N_data와 S_data에 각각 전체 네트워크와 내부 네트워크에서 발생하는 패킷들을 P_filter모듈에 의해서 필터링한다.

B. 필터링한 데이터를 D_module에서 기존 차단 데이터와 비교하여 일치할 경우 방어하거나 차단한다.

C. 차단할 데이터가 발생할 경우 이를 관리자에게 A_module를 통하여 통보한다.

D. 이러한 후에 다시 필터링한 데이터를 기존 사용자와 비교하여 사용허가가 없는 데이터일 경우 네트워크에서 차단시킨다.

E. A-B까지를 연결이 없을 때까지 계속해서 반복하여 실시간 검색을 시도한다.

[그림 2]는 앞에서 제시한 알고리즘을 구조도로 표현한 것이다.

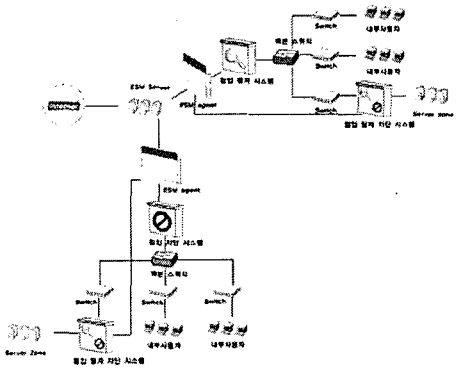

그림 2. 제안하는 통합보안관리 시스템 구축 구조도

[그림 2]에서 기업에 맞는 보안정책에 따라 선택적으로 가상사설망, 침입 탐지시스템, 방화벽 중 선택을 하거나 내부적으로 침입 탐지시스템 또는 방화벽을 필요에 따라 선택을 하여 구축을 할 수는 있지만 통합 보안 관리 에이전트를 기점으로 하여 통합 보안 관리 에이전트 안의 시스템은 모두 구축을 하는 것이 내외부적으로 보안에 안전하다는 것을 알 수 있다. 이 시스템에 있어서 보안에 대한 안정성 평가는 사용하는 보안 시스템과 통합 보안 관리에 따른 보안정책에 따라 달라질 것이다.

Ⅳ. 제안하는 통합보안관리 시스템 구현

1. 성능평가 설정

보안 관리의 중요성이 강조되면서 점차 도입하는 기업이 늘고 있는 통합 보안 관리(ESM) 솔루션이 다양한 이기종 보안 솔루션을 중앙 집중 관리하고, 보안 솔루션 이벤트의 상호간 연관성 분석을 통해 오탐지를

최소화하는 방향으로 발전하고 있다. 자원 낭비를 줄이고 효율적인 중앙 집중 관리를 가능하게 한다. 비즈니스의 활성화와 더불어 정보시스템은 내·외부자에 의해 노출되고 있다. 이에 따라 기업의 신뢰도와 서비스 가용성이 더불어 위협받고 있는 게 사실이다[6].

내부적 노출을 방지하기 위하여 내부 서버에 한 번 더 보안 시스템을 구축하는 구조를 이루어야 한다. 외부적인 침입에 의해서만 보안이 철저하고 내부 침입에 대비하지 않는다면 기업 내 구성원의 해킹이나 구성원의 사소한 실수로 인하여 구성원 컴퓨터가 노출이 되어 진다면 외부적으로 철저히 보안을 이룬다 하더라도 무용지물이 된다. 이를 막기 위하여 내부의 보안을 강화하는 구조를 [그림 2]에서 설명한 바 있다.

이를 직접적으로 구현해 보기 위하여 기업에서 사용하는 실제 네트워크를 구축하는 것에는 무리가 있어 소규모 네트워크를 구축한 후 침입탐지를 위한 보안 솔루션을 가지고 구축을 해보았다.

2. 웹 로그 분석

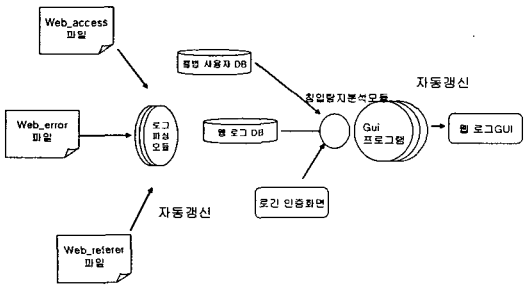

그림 3. Http 프로토콜 로그분석 모듈

웹 서버에서 시스템에 어느 사이트로부터 접속하였으며, 어느 파일이 다운로드 되었는지에 대한 사항이 access_log 파일에 기록되고, 존재하지 않는 파일에 대한 접근 등 에러에 대한 내역은 error_log에 기록하고 있다. [그림 3]은 이러한 로그파일을 '로그파싱모듈'을 이용하여 필요한 데이터를 데이터베이스에 저장하여 관리자에게 정보를 제공하게 되는 과정을 계략적으로 표현한 것으로 모듈 구조도이다[9][10].

3. 텔넷 로그 분석

wtmp 파일은 사용자들의 로그 정보를 가지고 있다. 사용자들의 로그인, 로그아웃 히스토리를 모두 가지고 있고, 시스템의 shutdown, booting 히스토리까지 포함되어 있다. [그림 4]는 이러한 wtmp 파일을 '로그파싱모듈'을 이용하여 관리자에게 정보를 제공하게 되는 과정을 계략적으로 표현한 것으로 모듈 구조도이다[11].

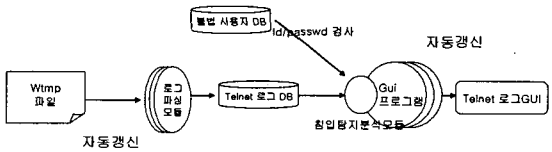

그림 4. Telnet 로그 분석 모듈

이 두 가지 침입탐지 모듈과 탐지된 IP또는 호스팅 주소를 차단할 수 있는 차단 모듈을 이용하여 침입탐지 솔루션을 구현하였다. 또한 실시간 경고를 하기 위하여 웹에서 볼 수 있도록 웹 솔루션을 채택하였고 관리자가 실시간으로 침입 상태를 확인할 수 있다.

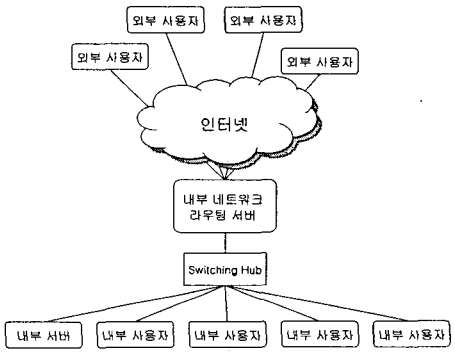

그림 5. 물리적 연결 구조도

[그림 5]와 같이 물리적 연결을 한 후 내부 네트워크 라우팅 서버에 침입탐지 솔루션을 설치한 경우(이하: A시스템)와 내부 네트워크 라우팅 서버와 내부 서버에 침입탐지 솔루션을 설치한 경우(이하: B시스템)를 구현하여 실질적인 성능 테스트를 하였다. 물론 이렇게 구현한 ESM이 실제 ESM과 같은 성능을 가질 수

는 없지만 ESM의 장점인 통합 시스템 모니터링과 실시간 경고를 볼 수 있다.

실험에 제한적이기 때문에 보안정책을 활용하여 여러 가지 보안 솔루션을 활용한 통합 보안 관리 시스템을 구축할 수는 없었지만 통합 보안 관리 시스템의 양대 산맥인 침입 탐지 시스템과 방화벽을 이용하여 구축하였다.

V. 성능 평가

앞에서 이야기한 A시스템과 B시스템을 실제 침입에 따른 테스트를 하였다. 그 결과 다음과 같은 분석을 얻을 수 있었다.

표 1. A시스템 테스트 목록

HOST	Web log	ID	Telnet log
total	256	total	132
203.247.63.144	175	root	28
203.247.63.145	45	test1	23
203.247.63.146	7	test2	31
203.247.63.147	5	test3	17
203.247.63.148	1	test4	13
192.168.0.3	15	test5	20
192.168.0.5	8		

[표 1]은 A 시스템에 총 7대의 컴퓨터가 웹으로의 침입을 시도한 횟수와 6가지 아이디로 텔넷을 통하여 접속을 시도한 횟수이다. 이를 통하여 특정 IP를 가진 컴퓨터가 접근을 시도할 경우 데이터 접속횟수와 데이터 전송량 평균 데이터 전송량을 분석하여 침입을 확인하고 이를 차단할 수 있도록 했다.

표 2. B시스템 테스트 목록

HOST	Web log	ID	Telnet log
total	330	total	158
203.247.63.144	275	root	45
203.247.63.145	16	test1	20
203.247.63.146	1	test2	35
203.247.63.147	1	test3	23
203.247.63.148	25	test4	14
192.168.0.3	12	test5	21
192.168.0.5	1		

[표 2]는 B 시스템에 총 7대의 컴퓨터가 웹으로의 침입을 시도한 횟수와 6가지 아이디로 텔넷을 통하여 접속을 시도한 횟수이다.

[그림 6]과 [그림 7]은 웹 로그에 대한 A와 B 시스템의 실험 데이터를 그래프로 표현한 것이다. A 시스템에서는 IDS가 전체 입력 데이터를 전부 검출해 내지 못하고 lose 데이터가 발생하였다. B시스템에서는 손실되는 데이터 없이 모든 데이터가 검색이 가능했다.

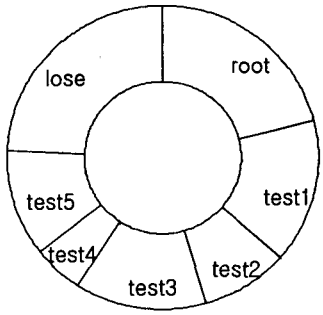

그림 6. A 시스템 웹 로그 분석

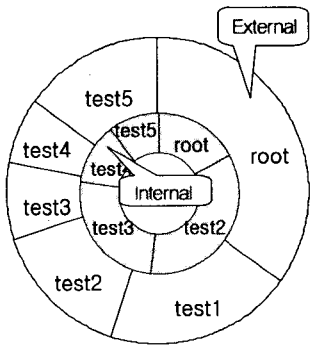

그림 7. B 시스템 웹 로그 분석

[그림 8]과 [그림 9]는 텔넷 로그 분석을 통한 A, B 시스템의 성능평가를 그래프로 표현한 것으로 이 데이터에서는 앞의 웹 로그 분석처럼 실제 손실 데이터가 있는지는 알 수 없다 하지만 앞에서 입력 데이터를 제공한 [표 1]과 [표 2]를 참고로 아래의 데이터 값들을 비교해서 본다면 A시스템에서 데이터를 제대로 검출 못한 사실을 알 수 있다. 또한 [그림 9]에서는 각각 외부와 내부에서 검색된 데이터가 있으며 이로 인해 앞

에서 제시한 [표 2]의 데이터들이 모두 검출된 것을 알 수 있다.

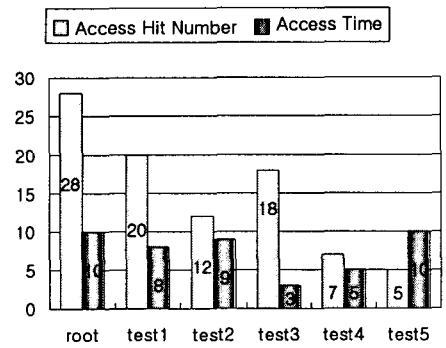

그림 8. A 시스템 텔넷 로그 분석

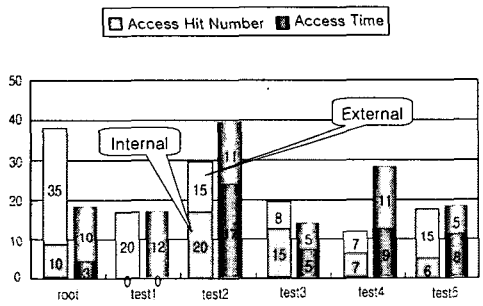

그림 9. B 시스템 텔넷 로그 분석

VI. 결 론

본 논문에서는 Firewall System에서 IDS를 거쳐 통합 보안 관리시스템 구조로 발전해 나가는 보안 시스템에 대하여 발전 과정과 발전 방향을 분석하였으며 보안 시스템의 가장 근본적인 목표인 내외부적 보안을 강화하고 보안 시스템 구축을 최종점인 통합 보안 관리 시스템 구축에 있어서 효율적이며 기업에게 맞는 어떠한 보안정책에도 적용할 수 있는 보안 시스템 체계 구조도를 제시하였으며 이를 직접 구현해보고 테스트를 거쳐 내부적으로 보안이 향상되었음을 알 수 있었다. 그러나 보안 시스템의 추가로 인하여 비용이 증가하는 단점이 발생할 수 있으며 서버의 네트워크 속도의 저하가 있을 수도 있다. 하지만 이러한 것은 기업의 보안 정책에 의해서 해결이 가능할 것이다. 향후 침입차단방법은 급격히 발전하는 해킹 및 바이러스에 대해 실시간 차단 및 침입정보의 철저한 분석으로 비슷한 유형의 패킷이나 침입에 대해 정보를 미리 파악하여 침입을 차단할 수 있어야 하며 대용량 데이터 처리 시 네트워크속도가 현저히 저하되지 않도록 트래픽 양을 분산시킬 수 있는 침입차단 방법을 구성해야 할 것이다.

참 고 문 헌

[1] 김병구, 정태명, "침입탐지 기술의 현황과 전망", 정보과학회지, 제18권, 제1호, 2000(1).

[2] 김익수, 김명호, "실시간 침입탐지 및 차단을 위한 시스템", 정보과학회지, Vol.29, No.1, 2002(4).

[3] 손우용, "통합보안관리 시스템에서 우선순위 기반의 보안정책 수립 모델", 한남대학교, 박사 학위 논문, 2004(7).

[4] 한국정보보호진흥원, "해킹바이러스 통계 및 분석 월보", 정보보호뉴스, 2003(5).

[5] 하영길, "인터넷의 정보보안 기술에 대한 연구", 情報保護學會誌, Vol.13, No.6, 2003.

[6] 정연서, 박배욱, 손승원, 오창석, "안전한 인터넷을 위한 보안관리 시스템 설계", 韓國컴퓨터情報學會論文誌 제7권, 제3호, 2002(12).

[7] 최현희 ,정태명, "통합보안관리시스템을 위한 보안정책 일반화에 관한 연구", 정보처리 학회 논문지, 제9-C권, 제6호, 2002(12).

[8] 이동영, 김동수, 정태명, "이종의 보안시스템 관리를 위한 정책 기반의 통합보안관리시스템의 계층적 정책모델에 관한 연구", 정보처리 학회 논문지, 제 8-C권, 제5호, 2001(12).

[9] http://www.faqs.org/rfcs/rfc2616.html

[10] http://www.w3.org/Protocols/HTTP/ietf-http-ext/

[11] http://rfc.net/rfc854.html

저 자 소 개

강 민 균(Min-Gyun Kang) 준회원

- 2003년 8월 : 한남대학교 컴퓨터공학과 공학사
- 2003년 8월~현재 : 한남대학교 대학원 공학석사

<관심분야> : 정보보호, 컴퓨터 네트워크, XML

김 석 수(Seok-Soo Kim) 종신회원

- 1991년 2월 : 성균관대학교 대학원 공학석사
- 1991년 2월~1996년 5월 : 정풍물산(주) 중앙연구소 주임연구원
- 1997년 4월~1998년 1월 : (주)한국탑웨어 책임연구원
- 2002년 2월 : 성균관대학교 대학원 공학박사
- 1998년 3월~2000년 2월 : 경남도립거창전문대학 교수
- 2000년 3월~2003년 2월 : 동양대학교 컴퓨터공학부 교수
- 2003년 3월~현재 : 한남대학교 정보통신멀티미디어학부 교수

<관심분야> : 멀티미디어, 정보통신, 웹솔루션, 정보보호, 원격교육 플랫폼 및 컨텐츠