방화벽 로그를 이용한 침입탐지기법 연구

윤 성 종* · 김 정 호**

A Study on the Intrusion Detection Method using Firewall Log

Sung-Jong Yoon* · Jeong-Ho Kim**

Abstract

According to supply of super high way internet service, importance of security becomes more emphasizing. Therefore, flawless security solution is needed for blocking information outflow when we send or receive data. Large enterprise and public organizations can react to this problem, however, small organization with limited work force and capital can't. Therefore they need to elevate their level of information security by improving their information security system without additional money. No hackings can be done without passing invasion blocking system which installed at the very front of network. Therefore, if we manage isolation log effective, we can recognize hacking trial at the step of pre-detection. In this paper, it supports information security manager to execute isolation log analysis very effectively. It also provides isolation log analysis module which notifies hacking attack by analyzing isolation log.

Keywords : Firewall, Intrusion Detection System, Hacking

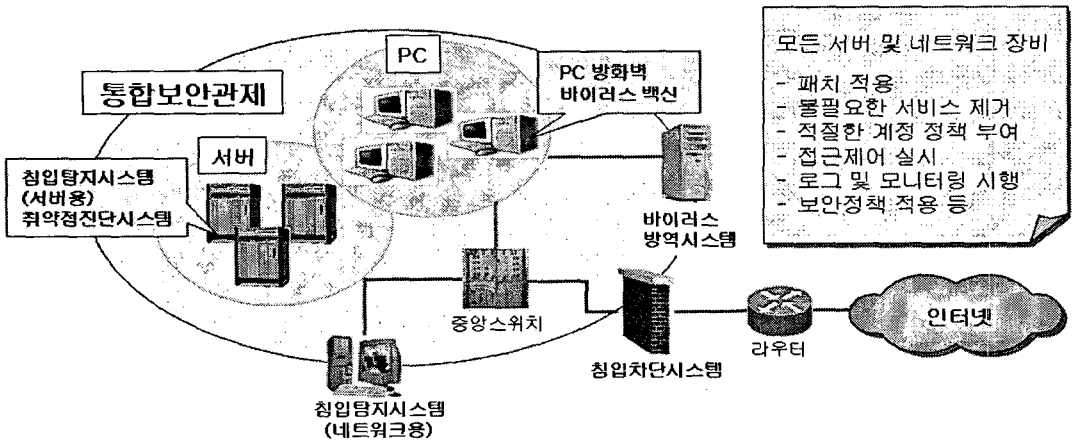
논문접수일 : 2006년 02월 02일 논문게재확정일 : 2006년 11월 24일

* 한밭대학교 정보통신전문대학원 컴퓨터공학과

** 교신저자, 한밭대학교 정보통신전문대학원 컴퓨터공학과 교수, (305-719) 대전 유성구 덕명동 산16-1, Tel : 042-821-1216, e-mail : jhkim@hanbat.ac.kr

1. 서 론

현대 사회의 기반구조가 시공간적 제한이 있는 실생활에서 제한요인의 영향을 받지 않는 인터넷 기반의 가상환경으로 전환되고 있다. 이에 따라 모든 사회적 인프라가 가상환경 안에 실환경과 동등한 수준으로 구축되고 사용자는 이를 활용하여 자신의 소요정보를 획득하고, 이용하는 것으로 사회가 변화하고 있다. 기업은 전자상거래를 통해 소비자에게 직접 다가가 상품을 판매하고 있으며, 정부 및 공공기관은 인터넷을 이용하여 전자민원을 해결하고, 민원인이 요구하는 정보를 웹에서 실시간으로 제공하고 있다. 이는 사용자가 자신의 집에서 모든 정보를 이용할 수 있는 편리함을 제공하면서, 정보제공자에게는 정보를 제공하기 위한 물리적인 장소 및 인원을 절감할 수 있어 비용 감소라는 긍정적인 역할을 하고 있다. 하지만, 모든 정보가 집중화되어 대단위로 이동하기 때문에 해킹과 같은 침해사고 발생시, 정보유출 및 유실에 따른 피해가 예전과는 비교할 수 없을 정도로 커지게 되었다. 해킹 피해를 예방하기 위해 다양한 방식의 정보보호체계가 구축되어 운영되고 있다. 현재, 많이 활용되고 있는 보호체계에는 <그림 1>에서와 같이 방화벽, 네트워크용 침입탐지시스템(NIDS), 침입방지시스템(IPS), 바이러스 방역시스템(AVS) 및 이를 통합 관리하는 통합관제시스템(ESM)이 있다. 그리고, 대규모 전산실이 아닌 곳에서 이러한 보호시스템을 구축하는 것은 비용대비 효과측면에서 낭비이기 때문에 중·소규모의 전산실에서는 방화벽과 NIDS를 병행운영하면서, AVS 구축하고 있다. 그런데, 보호체계에서 생성된 탐지 로그를 종합해주는 ESM을 구비하지 않을 경우 보호체계 관리자는 침입 이벤트를 점검하는데 상당한 부담을 가질 수밖에 없다. 특히, 대부분의 방화벽에서 보여지는 로그의 형태가 단순히 packet 차단내역을 목록 상태로 보여주기 때문에, 관리자가 침입시도를 인지하기 위해서는 별도의 통계 S/W를 이용해야 한다. 이는 침해상태를 바로 알려주는 IDS 로그와 비교해 볼 때에 상대적으로 덜 중요하게 인식되는 요인이 된다. 그러나, 다음과 같은 이유로 방화벽의 차단로그는 NIDS의 탐지로그와 같이 중요하게 관리되어야 한다. 첫째, NIDS는 방화벽을 통과한 packet을 대상으로 분석하기 때문에 방화벽에 의해 차단



〈그림 1〉 정보보호체계 설치 구성도

된 공격시도는 NIDS에 탐지되지 않는다. 둘째, NIDS는 순간 네트워크 소통량이 많을 경우 packet 처리량의 한계로 탐지율이 70~100% 정도에 머무르게 된다. 따라서, 방화벽에서 불필요 packet을 엄격하게 차단하고 선행 분석을 실시하여, NIDS의 packet 처리량을 안정적으로 낮춰 NIDS의 탐지율을 높일 수 있도록 해야 한다.

따라서 본 논문에서는 방화벽 관리자의 침입 인지율 향상을 위해 방화벽 차단로그 분석결과를 기반으로 스캔, DOS 등의 네트워크 공격행위의 인지를 NIDS에 앞서 탐지해 안정적인 네트워크 운영을 보장하고자 한다.

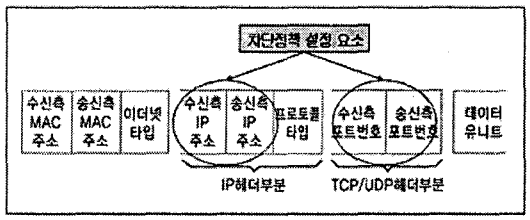
2. 방화벽 기능

방화벽은 외부로부터 불법적인 접근이나 해커의 공격으로부터 내부 네트워크를 방어하기 위해 내부 네트워크와 외부 네트워크 사이의 통로에 설치하여 두 네트워크간의 traffic을 제어하기 위한 목적으로 구성된 시스템 혹은 시스템들의 네트워크라고 말할 수 있다. 즉, 외부 네트워크에서 내부 네트워크로 액세스하기 위해서는 방화벽을 통과하여야만 내부 네트워크로 진입할 수 있도록 한 후, 네트워크 traffic 중 적법하다고 인증된 traffic만 통과시킴으로써 외부의 침입으로부터 다음과 같이 내부 네트워크를 안전하게 보호한다.

- 내부의 취약한 네트워크 구성요소를 보호
- 외부로부터 내부로의 불법적인 행동에 대한 내부망의 보호

방화벽은 관리자가 사전에 설정한 통제 정책에 따라 내/외부간 네트워크 traffic을 제어한다. 이를 통해 방화벽의 가장 중요한 기능인 외부 네트워크로부터의 내부 네트워크 보호를 수행한다.

방화벽의 통제 요소인 차단정책 설정 주요 요소로는 <그림 2>에서 보는바와 같이 '수신측 IP주소', '수신측 포트번호'와 '송신측 IP주소', '송신측 포트번호'가 있으며, 이외에도 사용자 등급, 접속시간 등이 사용될 수 있다.



<그림 2> packet 내용

지금까지 언급한 방화벽의 주요기능은 다음과 같이 정리할 수 있다[이만영, 2005].

- 외부의 침입으로부터 내부 네트워크 보호
- 비인가 된 서비스 접속 허용 및 차단
- 내/외부간 네트워크 사용자 통제
- 내/외부간 네트워크 traffic 감시

<표 1>은 일반적인 방화벽의 기능을 표로 나타낸 것이다[채규혁, 1998].

<표 1> 방화벽의 기능

기 능	IP차단	Port차단	암호화	Traffic감시
포함유무	○	○	△	○

3. 차단로그를 활용한 공격정보 해석

3.1 차단 정책 설정

방화벽의 차단정책은 <그림 2>의 packet 내용 중에서 '수신측 IP주소', '수신측 포트번호'와 '송신측 IP주소', '송신측 포트번호'를 이용하여 만들어지게 되며, 사용자 등급 및 접속시간 등이 추가로 사용된다.

일반적인 차단정책은 <표 2>과 같이 '출발지 IP' 등을 비롯하여 총 8개의 요소를 사용하여

작성되게 되며, 각각의 설정 요소는 아래와 같다.

• 출발지 IP

packet 내용 중 '송신측IP'에 해당한다. 특정 출발지를 지정할 경우에는 해당되는 IP를 기입하고, 모든 외부유입에 대해 설정할 경우에는 'any'로 기입한다.

• 출발지 PORT

포트번호란 네트워크 서비스 사용시 이용되는 서비스 번호로 '출발지 PORT'는 packet 내용 중 '송신측 포트번호'에 해당한다. 출발지에서 사용되는 특정 서비스를 지정할 경우에는 해당되는 포트번호를 기입하고, 서비스가 불확실하거나 모든 서비스에 대해 설정할 경우에는 'any'로 기입한다.

• 도착지 IP

packet 내용 중 '수신측IP'에 해당한다. 특정 도착지를 지정할 경우에는 해당되는 IP를 기입하고, 모든 내부 네트워크에 대해 설정할 경우에는 'any'로 기입한다.

• 도착지 PORT

'도착지 PORT'는 packet 내용 중 '수신측 포트번호'에 해당한다. 도착지에서 제공하는 특정 서비스를 지정할 경우에는 해당되는 포트번호를 기입하고, 제공하는 서비스가 불확실하거나 모든 서비스에 대해 설정할 경우에는 'any'로 기입한다.

• 프로토콜

통신에 사용되는 프로토콜의 종류를 지정하는 부분으로 프로토콜 종류를 알 경우에는 'TCP', 'UDP', 'ICMP' 중 하나를 선택하고, 불확실하거나 모든 프로토콜에 대하여 설정할 경우에는 'any'로 기입한다.

• 허용 여부

packet이 방화벽을 통과할지 차단될지를 결정하는 부분으로, '허용'과 '차단' 중 사용자가 의도하는 것을 선택하여 기입한다.

• 허용 시간

차단정책이 적용되는 시간을 지정하는 부분으로 'any'로 지정할 경우 24시간을 의미하며, 관리자가 원하는 시간대를 기입할 수도 있다.

<표 2>에서와 같이 차단정책 내용을 기록한 것을 해석하면 다음과 같다[이만영, 2005].

〈표 2〉 차단정책 내용

순번	출발지IP	출발지 PORT	도착지 IP	도착지 PORT	프로토콜	허용 여부	허용 시간
1	any	any	1.1.1.1	80	TCP	허용	any
2	2.1.*.*	any	any	any	TCP	차단	any
3	3.1.*.*	any	any	any	TCP	허용	any
4	any	any	any	any	any	허용	any
:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:
99	any	any	any	any	any	차단	any

- 순번 1 : 외부의 모든 IP는 내부 1.1.1.1의 TCP 80번 Port에 24시간 접근이 허용된다.
- 순번 2 : 외부 IP 2.1.1.1~2.1.255.255는 내부의 모든 TCP 서비스에 대한 접근이 24시간 차단된다.
- 순번 3 : 외부 IP 3.1.1.1~3.1.255.255는 내부의 모든 TCP 서비스에 대한 접근이 24시간 허용된다.
- 순번 4 : 외부의 모든 IP는 내부의 모든 서비스에 대한 접근이 24시간 허용된다(즉, 모든 외부 유입 허용).
- 순번 99 : 외부의 모든 IP는 내부의 모든 서비스에 대한 접근이 24시간 차단된다(즉, 모든 외부 유입 차단).

방화벽을 통과하려는 packet은 위와 같이 차단정책과 packet의 해더 정보를 각각 비교한다. 만약, 2번행의 내용과 해더정보가 같다면 해당 packet은 버려지게 되고, 1번 또는 3번행과 같다면 방화벽을 통과해서 내부로 들어오게 된다.

일치하지 않는 packet의 경우에는 마지막 행인 99번에 의해 차단되어 버려지게 된다. 차단정책 설정시 가장 주의해야 할 점은 모든 외부 유입을 허용하는 정책을 입력하면 안 된다는 것이다. <표 2>에서와 같이 외부 유입을 모두 허용하는 4번행을 입력한 후 추가로 입력한 5번행~99번행의 정책은 그 효력을 상실하게 되기 때문에, 방화벽 관리자는 차단정책 중간에 이와 같은 내용이 입력되지 않도록 주의 깊게 살펴보아야 한다. <그림 3>은 실제 방화벽의 차단로그를 보여주는 화면을 저장한 그림으로, '차단시간', 'packet종류', '허용여부', '방향성', '발신지주소', '수신지주소', '발신지포트', '수신지포트'의 항목이 저장되는 것을 볼 수 있다.

번호	시간	패킷종류	허용여부	방향성	발신지주소	수신지주소	발신지포트	수신지포트
257	2005/09/14 14:05:44	ICMP	차단	외부=>내부	67.2.1.27	48.1.1.14	3	
258	2005/09/14 14:05:44	UDP	차단	외부=>내부	48.16.1.176	48.1.2.79	1029	53
259	2005/09/14 14:02:24	ICMP	차단	외부=>내부	67.8.1.13	54.12.12.111	3	
260	2005/09/14 14:00:27	TCP	차단	외부=>내부	8.153.1.230	54.6.1.14	1661	80
261	2005/09/14 14:00:27	TCP	차단	외부=>내부	8.153.1.230	54.6.1.15	1662	80
262	2005/09/14 14:00:27	TCP	차단	외부=>내부	8.153.1.230	54.6.1.13	1660	80
263	2005/09/14 14:00:27	TCP	차단	외부=>내부	8.153.1.230	54.6.1.20	1667	80
264	2005/09/14 14:00:27	TCP	차단	외부=>내부	8.153.1.230	54.6.1.21	1668	80
265	2005/09/14 14:00:27	TCP	차단	외부=>내부	8.153.1.230	54.6.1.16	1665	80
266	2005/09/14 14:00:27	TCP	차단	외부=>내부	8.153.1.230	54.6.1.19	1666	80
267	2005/09/14 14:00:27	TCP	차단	외부=>내부	8.153.1.230	54.6.1.15	1663	80
268	2005/09/14 14:00:27	TCP	차단	외부=>내부	8.153.1.230	54.6.1.17	1664	80
269	2005/09/14 14:00:27	ICMP	차단	외부=>내부	67.3.1.9	54.6.5.252	3	
270	2005/09/14 14:00:27	ICMP	차단	외부=>내부	5.5.1.249	54.5.7.107	8	
271	2005/09/14 14:00:27	ICMP	차단	외부=>내부	67.3.1.9	54.6.6.23	3	
272	2005/09/14 14:13:23	TCP	차단	외부=>내부	48.2.126.12	54.9.12.63	2253	80
273	2005/09/14 14:03:53	TCP	차단	외부=>내부	54.2.4.42	54.8.1.1.98	2167	2186
274	2005/09/14 14:05:16	ICMP	차단	외부=>내부	67.2.1.27	48.1.1.14	3	
275	2005/09/14 14:05:49	UDP	차단	외부=>내부	48.16.1.176	48.1.2.79	1029	53
276	2005/09/14 14:02:28	ICMP	차단	외부=>내부	67.8.1.13	54.12.12.111	3	
277	2005/09/14 14:00:32	TCP	차단	외부=>내부	48.2.1.63	50.1.1.30	40759	34454
278	2005/09/14 14:00:32	TCP	차단	외부=>내부	8.153.1.230	54.6.1.22	1669	80
279	2005/09/14 14:00:32	ICMP	차단	외부=>내부	67.3.1.9	54.6.5.252	3	
280	2005/09/14 14:13:23	TCP	차단	외부=>내부	48.2.126.12	54.9.12.63	2253	80

〈그림 3〉 차단로그 내용

3.2 차단로그를 활용한 공격유형 분석

네트워크에서 소통되는 packet 중에서 해킹 공격에 사용되는 유해 packet은 '출발지 IP주소', '도착지 IP주소', '도착지 Port'의 3가지 필드를 기준으로 분석하여 탐지할 수 있다. 이와 같이 방화벽 차단로그를 분석하기 위해서는 먼저, 분석모듈에서 탐지할 수 있는 공격유형을 사전에 정의해야 할 필요가 있다. 이것은 전체 공격유형을 파악한 뒤에 분류해야 하는데, 본 논문에서는 전체 공격유형을 정의하기 위해서 한국전자통신연구원에서 개발한 상황인식 기반의 침입탐지 방법인 NASA (Network Attacks Situation Analysis)를 사용하여 전체 공격유형을 파악하였다[정연서 외 2인, 2001]. NASA는 {공격명(a), 출발지IP(s), 도착지IP(t), 도착지Port(p)}의 속성 집합을 이용하여 3개 레벨, 10가지의 상황을 정의한다. 3개 레벨은 다음과 같다. 레벨 1은 속성 3가지가 결합된 상황이며, 레벨 2는 속성 2가지, 레벨 3은 속성 1가지에 의한 상황이다. 이를 바탕으로 발생 가능한 상황 10가지를 정의하면 다음과 같다.

- 레벨 1 : $\{a, s, t\}^{1-1}$, $\{s, t, p\}^{1-2}$
- 레벨 2 : $\{s, t\}^{2-1}$, $\{a, s\}^{2-2}$, $\{a, t\}^{2-3}$, $\{s, p\}^{2-4}$, $\{t, p\}^{2-5}$
- 레벨 3 : $\{a\}^{3-1}$, $\{s\}^{3-2}$, $\{t\}^{3-3}$

침입경보 속성 값을 확인하여 현재 침입상황이 어떤 클래스에 해당하는지를 평가해야 한다. 평가과정은 레벨 1 → 레벨 2 → 레벨 3 순서를 따른다. 즉, 레벨 1에 해당하는 상황이 존재하지 않는 경우에 레벨 2에 해당하는 상황이 존재하는가를 평가한다. 마찬가지로, 레벨 3의 경우는 레벨 1과 레벨 2에 해당하는 상황이 존재하지 않을 때, 평가된다. 그러므로 상위 레벨에 대한 평가가 성공할 경우에는 하위 레벨에 대한 평가는 수행되지 않는다. 동등 레벨에 대한 평가결과에는 영향을 받지 않는다. 이와 같이, 평가 과정을 거쳐 확정된 상황 클래스는 <표 3>과 같다. 본 논문에서는 <표 3>의 상황 클래스 정의 중에서 방화벽의 차단로그를 통하여 탐지할 수 있는 공격상황인 (1-2), (2-1), (2-4), (2-5)를 선별하여 각각의 상황을 <표 4>과 같이 정리하였다.

<표 4>의 차단로그를 통해 탐지 가능한 공격유형을 공격 형태별로 설명하면 아래와 같다.

〈표 3〉 NASA에서 표현한 상황 클래스 정의

공격상황	공격명	출발지IP	도착지IP	도착지Port	설 명
1-1	O	O	O		특정 공격자가 특정 대상에 대해 동일 공격을 반복적으로 시도하는 상황
1-2		O	O	O	특정 공격자가 특정 대상의 특정 서비스에 대해 다양한 공격을 반복적으로 시도하고 있는 상황
2-1		O	O		특정 공격자가 특정 대상에 대해 다수의 공격을 시도하고 있는 상황
2-2	O		O		특정 대상에 대해 동일 공격이 반복적으로 시도되고 있는 상황
2-3	O	O			특정 공격자가 특정 공격을 반복적으로 시도하고 있는 상황
2-4		O		O	특정 공격자가 불특정 다수의 특정 서비스에 대해 공격을 시도하고 있는 상황
2-5			O	O	특정 대상의 특정 서비스가 다수로부터 다양한 공격을 받고 있는 상황
3-1	O				특정 공격자가 다양한 공격을 지속적으로 시도하고 있는 상황
3-2		O			특정 대상으로 다양한 공격자로부터 다양한 형태의 공격이 시도되고 있는 상황
3-3			O		네크워크 상에 특정 공격이 지속적으로 시도되고 있는 상황

• 공격 / 피해가 명확한 공격

하나의 공격방법을 가지고, 지속적으로 공격하는 경우에 해당하며, 공격자 IP와 피해자 IP 그리고, 도착지 포트번호가 일정한 특성을 보인다.

• Port Scan

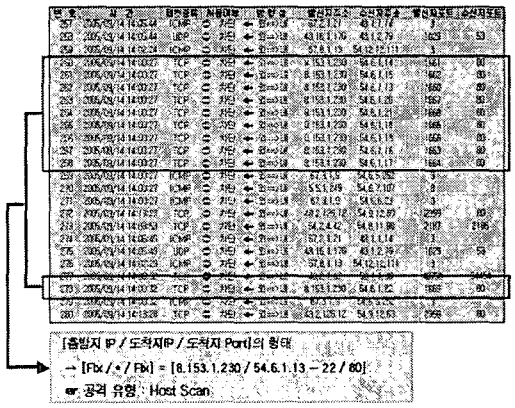
해킹 대상 서버에서 취약한 서비스를 찾기 위해 실시하는 해킹의 기초단계로서, 공격자가 해킹대상 서버에서 제공하고 있는 서비스를 검색하는 공격이다. 이 공격은 공격자와 피해자가 일정하고 대신 검색하는 서비스 포트가 변하는 특성을 보인다.

• Host Scan

취약한 서비스를 가지고 있는 서버를 찾기 위해 실시하는 공격으로, 공격대상 네트워크에서 취약한 서비스를 제공하는 서버를 검색하는 공격이다. 이 공격은 공격자 IP와 검색하는 포트번호가 일정한 반면, 피해자 IP가 변하는 특성을 보인다.

• DOS

서버에서 제공할 수 있는 서비스 제공 능력을 초과하여 한 번에 많은 양을 요청할 때 다른 정상적인 서비스를 제공에 장애를 초래하는 공격이다. 이 공격은 하나의 공격자가 하나의 해킹대상서버의 취약한 서비스를 대상으로 공격하는 경우에 해당하며, 공격자 IP와 피해자 IP가 일정한 반면, 도착지 포트번호가 변하는 특성을 보인다.



〈그림 4〉 침입차단 로그 유형 분석

〈표 4〉 차단로그를 통해 탐지 가능한 공격 유형

NASA 공격상황	공격형태	필드 구성			설 명
		출발지IP	도착지IP	도착지Port	
1-2	공격/피해가 명확한 공격	Fix	Fix	Fix	특정 공격자가 특정 대상의 특정 서비스에 대해 다양한 공격을 반복적으로 시도하고 있는 상황
2-1	Port Scan	Fix	Fix	*	특정 공격자가 특정 대상에 대해 다수의 공격을 시도하고 있는 상황
2-4	Host Scan	Fix	*	Fix	특정 공격자가 불특정 다수의 특정 서비스에 대해 공격을 시도하고 있는 상황
2-5	DOS	*	Fix	Fix	특정 대상의 특정 서비스가 다수 로부터 다양한 공격을 받고 있는 상황

지금까지 살펴본 4가지 공격 유형을 기반으로 <그림 3>의 차단로그를 분석할 수 있다. <그림 4>에서 보이는 바와 같이 차단로그의 260~268번을 살펴보면, 출발지 IP가 '8.153.1.230'로 고정되어 있고, 도착지 포트번호도 '80번'으로 고정되어 있는 것을 볼 수 있다. 이렇게 출발지 IP와 도착지 포트번호가 일정한 가운데 도착지 IP주소가 '54.6.1.13'에서 '54.6.1.22'로 변한 것을 볼 수 있다. 이것을 <표 4>의 공격유형과 비교하여 살펴보면, 아래와 같이 Host Scan의 공격 특성과 같음을 알 수 있다.

- 출발지 IP : 8.153.1.230 ⇒ FIX
- 도착지 IP : 54.6.1.13~22 ⇒ 변동
- 도착지 포트번호 : 80 ⇒ FIX

따라서, 해당 차단로그를 통해 Host Scan 발생한 것을 알 수 있다.

3.3 차단로그 분석규칙 정의

방화벽 차단로그에서 Host Scan 등의 공격상황을 안정적이고 신속하게 탐지해내기 위해서는 시스템적으로 차단로그 분석을 수행한다. 그리고, 시스템적으로 차단로그 분석을 수행하기 위해서는 정형화된 차단로그 분석규칙이 요구된다. 본 논문에서 탐지하고자 하는 공격형태는 일정한 행위 패턴을 가지고 공격을 수행한다. 그렇기 때문에, 이를 토대로 하여 분석규칙을 수립할 수 있다. 앞서 <그림 4>의 차단로그 분석예시에서 알 수 있듯이, Host Scan은 출발지 IP와 도착지 포트번호가 고정적이면서 도착지 IP가 변하는 공격형태를 지니고 있다. 차단로그 분석 규칙은 이러한 공격형태를 이용하여 정의할 수 있다. 본 논문에서 탐지하려는 공격에 대한 차단로그 분석규칙은 다음과 같이 정의될 수 있다.

(1) 공격/피해가 명확한 공격

- 특정 출발지에서 공격대상 서버의 취약한 서비스에 지속적으로 공격을 시도하는 행위
- 출발지의 IP와 Port가 일정한 가운데, 도착지 IP와 Port도 일정한 차단로그
- 반복되는 수가 10회 이상일 때 공격으로 분류

```
Source : srcip = FIX, srcport = FIX
Destination : dstip = FIX, dstport = FIX
공격인정 최소값 = 10
```

(2) Port Scan

- 공격대상으로 정해진 서버에서 제공하는 모든 서비스를 찾는 행위
- 출발지의 IP와 Port가 일정한 가운데, 도착

지 IP는 일정한 반면 Port가 변하는 차단 로그

- 반복되는 수가 20회 이상일 때 공격으로 분류

Source : srcip = FIX, srcport = FIX Destination : dstip = FIX, dstport = RANDOM 공격인정 최소값 = 20

(3) Host Scan

- 내부 네트워크의 여러 서버 중 취약점이 있는 서비스를 운영하는 서버를 찾는 행위
- 출발지의 IP와 Port가 일정한 가운데, 도착지 Port는 일정한 반면 IP가 변하는 차단 로그
- 반복되는 수가 20회 이상일 때 공격으로 분류

Source : srcip = FIX, srcport = FIX Destination : dstip = RANDOM, dstport = FIX 공격인정 최소값 = 20

(4) DOS

- 외부 네트워크의 여러 출발지에서 특정서버의 취약한 서비스에 접근이 집중됨으로써, 정상적인 서비스 제공이 방해 받는 상황
- 출발지의 IP와 Port가 변하는 가운데, 도착지 IP와 Port가 일정한 차단로그
- 반복되는 수가 100회 이상일 때 공격으로 분류

Source : srcip = RANDOM, srcport = RANDOM Destination : dstip = FIX, dstport = FIX 공격인정 최소값 = 100

이렇게 정의한 4가지 공격 유형에 대한 분석규칙 이외에도 차단로그를 이용하여 Worm Scan 탐지 등과 같은 차단로그 분석규칙도 정의할 수 있다.

(5) Worm Scan

- 외부 네트워크에서 내부 네트워크에 Worm을 전파시키기 위하여 서버 또는 PC에서 운영중인 취약한 서비스를 찾는 행위
- 출발지의 IP와 Port, 도착지 IP가 변하는 가운데, 도착지 Port가 <표 5>의 Worm Port Group에 속하는 차단로그
- 반복되는 수가 10회 이상일 때 공격으로 분류

Source : srcip = RANDOM, srcport = RANDOM Destination : dstip = RANDOM, dstport = Worm Port Group 공격인정 최소값 = 10

지금까지 정의한 공격 유형별 분석규칙 이외에도 시스템을 관리하는 관리자의 필요에 따라 분석규칙을 정의할 수 있다. 예를 들어 내/외부 네트워크에 위치한 중요 서버에 대한 감시가 필요할 때에는 주요 IP 및 Port에 대한 분석규칙을 정의하여 적용함으로써 활용할 수 있다.

<표 5> Worm Port Group

Port	Worm 목록
25	Netsky 등
135	Blaster, Lovgate 등
139	Netlog, Qaz, Deborms, Moega 등
445	Agobot, Randex, Polybot, 등
445	Sasser, Korgo, Spybot, Janx 등
1080	MyDoom 등
1434	Slammer 등
2745	Bagle 등
3410	OptixPro, Mockbot 등
5000	Bubbel, ICKiller, Rald, Bobax 등
6129	Mockbot. Dameware 등

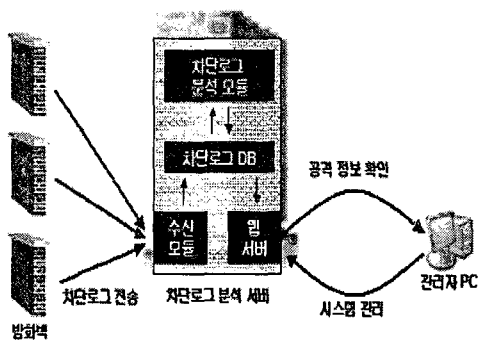
3.4 차단로그 분석체계 구성

방화벽 차단로그를 통해 공격을 탐지하기 위해서 3.3에서 정의한 분석규칙에 따라 공격이 의심되는 packet를 분류하여 관리해야 한다. 그리고, 이렇게 관리된 packet 정보를 필요에 따라 추출하여 조합함으로써 공격을 탐지할 수 있다.

본 논문에서는 차단로그 정보를 DB저장하여 관리하고, 이렇게 저장된 차단로그를 대상으로 SQL 질의문을 적용하여 공격유형을 분석하는 기법을 제시하였다.

3.4.1 체계 구성도

본 논문에서 제안한 체계구성은 <그림 5>과 같다. <그림 4>와 같은 차단로그를 '분석서버'의 '수신모듈'로 전송하고, '수신 모듈'은 전송받은 로그를 '차단로그 DB'에 저장한다. DB에 저장된 차단로그는 '차단로그 분석모듈'에 의해 공격유형이 판별되고, 공격으로 판별된 정보는 다시 '차단로그 DB'에 저장되어 관리자가 웹 서버를 통해 볼 수 있도록 설계하였다. 그리고, 복수의 방화벽을 운영하는 전산실의 경우에는 각각의 방화벽의 차단로그를 수집하여 통합 분석할 수 있도록 하였다.



〈그림 5〉 로그분석체계 구성도

3.4.2 차단로그 분석모듈

차단로그 분석모듈은 3.3에서 정의한 분석규칙을 기반으로 동작되는데, 이를 위해서는 packet 분석을 위한 정보를 관리해야 할 필요가 있다. 본 논문에서는 각 공격유형에 해당하는 packet 정보를 DB를 통해 관리하였고, packet 정보를 저장하는 DB 테이블은 <표 6>와 같이 구성했다.

〈표 6〉 공격 유형에 따른 테이블 구성

DB 테이블	출발 IP	도착 IP	도착 Port	탐지 가능 공격 유형
TYPE_0	O	O	O	공격자 IP 및 대상 IP/Port가 명확한 공격
TYPE_1	O	O		Port Scan
TYPE_2	O		O	Host Scan
TYPE_3		O	O	DOS

공격 유형 분석을 위한 DB테이블은 다음과 같이 생성했다.

- TYPE_0 테이블은 전체 차단로그DB 중 TCP와 UDP packet을 대상으로 출발지 IP, 도착지 IP, 그리고 도착지 Port를 추출하여 저장한다.

```
TYPE_0 : insert into TYPE_0_table
select Protocol_type, 출발지IP, 도착지IP,
도착지 Port, sum(packet_num),
sum(packet_size) from 차단로그 DB
group by Protocol_type, 출발지 IP,
도착지 IP, 도착지 Port;
```

- TYPE_1 테이블은 전체 차단로그DB 중 TCP와 UDP packet을 대상으로 출발지 IP와 도착지 IP를 추출하여 저장한다.

```
TYPE_1 : insert into TYPE_1_table
select Protocol_type, 출발지 IP, 도착지 IP,
sum(packet_num), sum(packet_size)
from 차단로그 DB group by Protocol_type,
출발지 IP, 도착지 IP;
```

- TYPE_2 테이블은 전체 차단로그DB 중 TCP와 UDP packet을 대상으로 출발지 IP와 도착지 Port를 추출하여 저장한다.

```
TYPE_2 : insert into TYPE_2_table
select Protocol_type, 출발지 IP, 도착지 Port,
sum(packet_num), sum(packet_size)
from 차단로그 DB group by Protocol_type,
출발지 IP, 도착지 Port;
```

- TYPE_3 테이블은 전체 차단로그DB 중 TCP와 UDP packet을 대상으로 도착지 IP와 도착지 Port를 추출하여 저장한다.

```
TYPE_3 : insert into TYPE_3_table
select Protocol_type, 도착지 IP, 도착지 Port,
sum(packet_num), sum(packet_size)
from 차단로그 DB group by Protocol_type,
도착지 IP, 도착지 Port;
```

위와 같이 구성된 테이블을 대상으로 아래와 같이 SQL문을 실행하여 Host Scan, DOS, Port Scan의 공격을 탐지할 수 있다.

- Port Scan 공격 차단 유무 확인 : TYPE_1 테이블에서 출발지 IP가 20개 이상인 도착지 IP를 추출한다.

```
select 도착지IP, count(출발지IP) as cnt
from TYPE_1_table group by 도착지IP
having count(출발지IP) > 20 order by
cnt desc;
```

- Host Scan 차단 유무 확인 : TYPE_2 테이블에서 도착지 IP가 20개 이상인 출발지 IP를 추출한다.

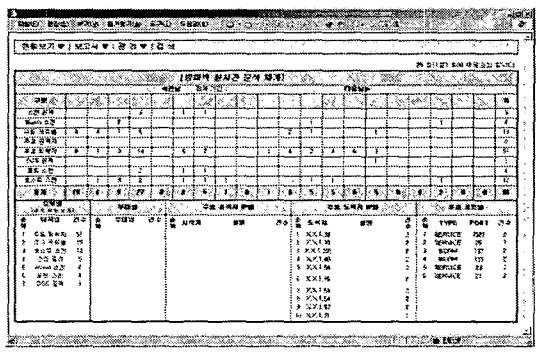
```
select 출발지IP, count(도착지IP) as cnt
from TYPE_2_table group by 출발지IP
having count(도착지IP) > 20 order by
cnt desc
```

- DOS 차단 유무 확인 : TYPE_3 테이블에서 도착지 Port가 100개 이상인 도착지 IP를 추출한다.

```
select 도착지IP, count(도착지Port) as cnt
from TYPE_3_table group by 도착지IP
having count(도착지Port) > 100 order by
cnt desc
```

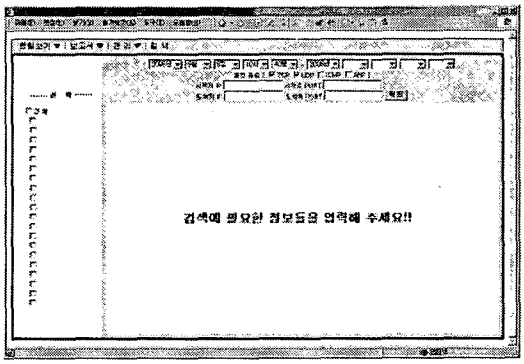
3.4.3 차단로그 분석 결과

위의 방식으로 방화벽에서 차단로그가 저장된 차단정보를 분석할 수 있는데, 이것은 차단로그 분석서버에서 수행하게 되고, 웹 서버를 통해 관리자에게 보이게 된다. 관리자는 <그림 6>와 같이 웹 브라우저를 통하여 원격에서 차단로그 분석결과를 알 수 있다. 관리자는 이를 통해 일정기간 동안의 Scan공격, Worm Scan, DOS 공격이 발생한 건수를 파악 할 수 있다. 더불어, 이 공격에 대한 주요 출발지 IP와 도착지 IP를 함께 제공하여, 해킹 피해가 예상되는 관리대상을 정확하게 식별할 수 있도록 정보를 제공한다. 만약, 여러대의 방화벽을 운영하는 조직에서 이 기법을 확대적용 할 경우에는 각 방화벽에서 차단된 로그를 종합하여 분석할 수도 있다. 그리고, 각 공격에 대한 세부적인 시간, IP등에 대한 세부적인 정보를 파악할 수도 있는데, 이같은 상세한 공격행위를 검색하고자



〈그림 6〉 차단로그 분석 결과 화면

할 때에는 <그림 7>의 차단로그 검색기능을 활용하여 찾을 수 있다.



〈그림 7〉 차단로그 검색 화면

앞서 <그림 4>의 차단로그 중 출발지 IP가 '8.153.1.230'인 것에 대한 Host Scan을 검색하면, <그림 8>과 같은 결과를 얻을 수 있다. 이 결과를 보면 출발지 IP '8.153.1.230'인 Host Scan 시도 1994건 있었다는 것을 알 수 있다.

방화벽 로그 상세 분석

집계 시간 : 2005-09-14 06:00 ~ 2005-09-14 16:55

선택 유형 : 호스트 스캔 차단

시작지 IP	도착지 IP 차단 횟수	시작지 IP	도착지 IP 차단 횟수
8.153.1.230	1994	48.2.1.84	63
48.2.1.84	1583	8.153.1.7	56
48.2.1.84	390	54.3.1.72	52
48.2.1.84	191	54.1.41.55	44
22.9.1.78	141	8.153.6.6	42
48.2.1.92	---	48.2.1.84	39
48.2.1.84			38

〈그림 8〉 차단로그 분석 결과

그리고, '8.153.1.230'에서 어느 서버를 대상으로 Scan을 시도했는가를 알고자 할 때에는 <그림 9>과 같은 세부 차단정보도 얻을 수 있다. 로그 상세정보를 보면, '8.153.1.230'에서 Host Scan을 시도한 도착지 IP가 '54.6.1.1'부터 '54.6.1.104'임을 알 수 있다. 또한, Scan하는 도착지 Port가 80번인 것을 보아 웹 서비스를 제공하는 서버를 찾고 있는 것을 알 수도 있다.

방화벽 로그 상세 정보

총 1994회 차단

패킷 종류	시작지 IP	도착지 IP	도착지 PORT	패킷갯수	패킷크기합
TCP	8.153.1.230	54.6.1.1	80	3	144
TCP	8.153.1.230	54.6.1.10	80	3	144
TCP	8.153.1.230	54.6.1.100	80	3	144
TCP	8.153.1.230	54.6.1.101	80	3	144
TCP	8.153.1.230	54.6.1.102	80	3	144
TCP	8.153.1.230	54.6.1.103	80	3	144
TCP	8.153.1.230	54.6.1.104	80	2	96
TCP					96

〈그림 9〉 세부 차단정보

방화벽 차단로그를 이용하여 탐지할 수 있는 공격유형은 차단로그 DB를 얼마나 잘 관리하고 분석하느냐에 달렸으며, 본 논문에서는 여러 공격중 Scan 및 DOS 공격에 초점을 맞추어 분석모듈을 구성하였다. 차단로그 분석체계를 시스템 운영자 측면에서 바라볼 경우에는 정상서비스가 방화벽에 의해 차단되고 있는 것을 인지하는 도구로 활용될 수 있다. 서버에서는 서비스를 제공하지만, 방화벽 차단정책을 수정하지 못해서 정상적인 외부 서비스 요청이 방화벽에 의해 차단되는 경우가 있기 때문에, 관리자는 이 체계를 지속적으로 감시함으로서, 심각한 서비스 장애가 발생하는 것을 조기에 인지하여 초치할 수 있다. 그리고, 네트워크 관리자는 네트워크 장비간에 시스템 관리를 위해 소통되는 packet의 추이를 지켜볼 수 도 있다.

3.5 기존 로그분석모듈과의 비교

지금까지 로그를 통해서 해킹 등의 침해상황을 탐지하고자 할 때 사용되는 프로그램으로는 'Logchek', 'Swatch', 'Colorlog' 등이 사용되어 왔다. 이들 프로그램은 시스템에서 운영중 생성되는 시스템 로그 파일을 분석하여 기존에 관리자가 입력한 유형과 비교하는 방식으로 동작한다. 이들 프로그램은 본 논문에서 제안한 기법과는 분석대상, 분석방식에서 차이가 있으나 로그파일을 통해서 해킹 시도를 탐지하고자하는

사용목적에서는 같다고 볼 수 있기에, <표 7> 에서와 같이 기존에 사용된 로그분석S/W와 본 논문에서 제안한 기법을 비교하였다.

〈표 7〉 기존 로그분석S/W과의 비교

S/W명	로그분석방식	분석대상로그
제안기법	패턴분석 연관관계분석	방화벽 차단로그
Logchek	패턴분석	시스템 로그파일
Swatch	패턴분석	시스템 로그파일
Colorlog	패턴분석	시스템 로그파일

위의 비교 내용을 살펴보면, 로그분석방식에서 기존의 S/W는 패턴분석방식을 이용하는 반면 제안기법은 이에 덧붙여 연관관계분석을 사용하고 있음을 볼 수 있다. 이렇게 연관관계분석이 추가적으로 수행됨으로서 관리자가 미처 입력하지 못한 침입형태에 대한 탐지가 가능해져, 운영 편리성의 향상을 기대할 수 있게 되었다. 하지만, 본 논문에서 제안한 기법은 방화벽 차단로그를 기반으로 동작하기 때문에 네트워크영역에서 발생되어지는 공격 유형에 대한 탐지만을 수행할 수 있다. 외부의 패킷이 네트워크에 진입한 이후에 발생하는 행위에 대한 탐지는 할 수 없기 때문에 독립적으로 운영하기에는 한계가 있다. 이러한 이유로 본 논문에서 제안한 기법은 기존의 로그분석S/W을 대체하는 프로그램이 아니라 상호 보완적으로 운영되는 프로그램으로 봐야 할 것이다.

4. 결론 및 향후 연구과제

본 논문에서는 방화벽의 차단로그를 분석함으로서 네트워크 공격행위를 조기에 인지할 수 있는 기법을 제안했다. 방화벽은 정보보호 시스템 중에서 침입탐지시스템과 더불어 가장 많이 운영되고 있는 정보보호 시스템이다. 하지만, 침입탐지시스템이 능동적으로 공격을 탐지하는 것에 비하여, 방화벽은 사전에 입력한 정책에 의해 패킷을 걸러냄으로서 수동적으로 내부망을 보호해왔다. 그래서, 지금까지 방화벽은 해킹 예방과 네트워크 운영측면에서 주로 관심의 대상이 되어왔다. 이로 인해 방화벽의 차단로그는 다른 정보보호시스템에 비하여 소홀이 관리되어 왔다. 본 논문에서는 이렇게 관리된 방화벽의 차단정보를 공격유형별로 정의한 분석규칙을 통해 재가공함으로서 특정 유형의 공격행위를 탐지해 낼 수 있는 기법을 제안했다. 방화벽에서 공격행위를 탐지함으로 인하여, 방화벽에 의해 걸러져 다른 정보보호시스템이 탐지하지 못한 미탐지 공격행위를 찾아낼 수 있게 되었다. 전산실 관리자는 기존에 운영하던 침입탐지시스템과 더불어 방화벽에서도 Scan/DOS/Worm 등의 공격을 추가적으로 인지할 수 있게 되어 한층 강화된 정보보호 수준을 기대할 수 있게 되었다. 그리고, 차단로그 분석은 정보보호측면 뿐만 아니라, 시스템 관리와 네트워크 관리분야에서도 활용될 수 있다. 시스템 관리자는 조직의 중요 서버에 대한 접근 차단 기록을 통해 서비스 지원 상태를 검증할 수 있고, 네트워크 관리자는 네트워크 장비간의 packet 소통 추이와 불필요 packet의 대량유입을 감시할 때 활용할 수 있다.

본 논문에서는 공격유형 탐지를 위한 방화벽 차단로그 분석을 DB Query문을 이용하여 수행했다. 이러한 분석기법은 대용량의 로그를 실시간으로 분석할 때와 Agobot 웜과 같이 Scan Port가 80/135/139/445/3127번로 다양한 공격을 탐지할 때에는 제한이 따른다. 이러한 제한사항을 해결하기 위해서는 수집된 데이터들간의 상관관계를 분석하여 새로운 정보를 추출하는 기법에 대한 연구가 필요하다. 현재, 관련분야로

불규칙한 데이터에서 새로운 특징을 추출할 수 있는 데이터 마이닝의 연관규칙(association rule) 기법이 있으며, 이를 활용한다면 더욱 강력한 차단로그 분석이 가능할 것으로 본다.

참 고 문 헌

[1] 국가보안기술연구소, "테이터마이닝을 이용한 침입 이벤트 분석 기술", 2004.

[2] 국가사이버안전센터, *방화벽 관리 및 침입기록 분석 방법*, 2005.

[3] 소진, 이상훈, "연관 규칙을 이용한 네트워크 기반 침입 탐지 패턴생성 기술", 한국정보과학회논문지, 2002.

[4] 유일선, 조경산, "네트워크 취약점 검색공격에 대한 개선된 탐지시스템", *정보처리학회논문지*, 10. 2001.

[5] 이동영, 서광현, 정태명, "인터넷 정보보호 알파에서 오메가까지", 영진닷컴, 2002.

[6] 이만영, *최신 정보보호개론*, 홍릉과학출판사, 2005.

[7] 이재광, 이용준, 박성열, "인터넷 방화벽과 네트워크 보안", 이한출판사, 1996.

[8] 정연서, 류걸우, 장종수, "네트워크 보안을 위한 ESM 기술 동향", ETRI, 주간기술 동향 통권 제1026호, 2001.

[9] 조기준, 김훈희, "해킹과 방어 완전실무", 구민사, 2001.

[10] 채규혁, "인터넷 방화벽 구축하기", 한빛미디어, 1998.

□ 저자소개

윤 성 종

연세대학교에서 전산학 학사 학위를 취득하였으며, 한밭대학교에서 컴퓨터공학 석사학위를 취득하였다. 주요 관심분야는 정보보호정책, 침입차단 및 탐지 모델 등이다.

김 정 호

경북대학교에서 전자공학 학사, 전자공학과 석사, 단국대학교에서 컴퓨터공학과 박사)를 취득하였다. 전자통신연구소에서 근무하였다. 현재는 한밭대학교 정보통신컴퓨터공학부의 교수이며, 주요관심분야는 컴퓨터네트워크, 프로토콜 공학, 유무선통합망 서비스 등이다.

◈ 이 논문은 2006년 02월 02일 접수하여 1차 수정을 거쳐 2006년 11월 24일 게재확정되었습니다.