情報保護學會論文誌
第14券 第4號, 2004. 8

자동화된 침해사고대응시스템에서의 네트웍 포렌식 정보에 대한 정의

박 종 성[a)†], 최 운 호[b)], 문 종 섭[a)‡], 손 태 식[a)]

고려대학교 정보보호대학원[a)], 금융결제원 금융 ISAC 정보보호기술팀[b)]

A Study on Network Forensics Information in Automated Computer Emergency Response System

JongSeong Park[a)†], UnHo Choi[b)], Jongsub Moon[a)‡], Taeshik Shon[a)]

Center for The Information Security Technologies, Korea University[a)],
Korea Financial Telecommunications & Clearings Institute[b)]

요 약

포렌식에 관한 연구는 현재까지 피해 컴퓨터에 남은 흔적을 수집하고 가공, 보관하는 시스템 포렌식에 치우쳐 있었다. 최근들어 단순히 피해 컴퓨터에 남은 흔적만을 분석하는 것이 아닌 컴퓨터 시스템이 속한 전체 네트웍에서 침입 관련 정보를 얻고 분석하려는 네트웍 포렌식에 대한 연구가 활발하다. 특히나 자동화된 침해사고대응시스템에서는 전체 네트웍에 대한 침입 흔적을 다루어야 하기 때문에 네트웍 포렌식의 중요성이 크다고 할 수 있다. 본 논문에서는 자동화된 침해사고대응시스템에서 네트웍 포렌식 정보로서 수집되어야 할 정보들을 정의하고 정의된 정보들을 가상의 침해사고 시나리오를 통해 확인한다.

ABSTRACT

Until now the study of computer forensics has been focused only system forensics which carried on keeping, processing and collecting the remained evidence on computer. Recently the trend of forensic study is proceeding about the network forensics which analyze the collected information in entire networks instead of analyzing the evidence on a victim computer. In particular network forensics is more important in Automated Computer Emergency Response System because the system deals with the intrusion evidence of entire networks. In this paper we defined the information of network forensics that have to be collected in Automated Computer Emergency Response System and verified the defined information by comparing with the collected information in experimental environments.

Keywords : *Network Forensic, Automated Computer Emergency Response System, ISAC*

Ⅰ. 서 론

최근 악의적인 해킹이나 산업 스파이에 의한 정보 유출 등의 컴퓨터 범죄가 날로 늘어남에 따라 사후 대처의 관점에서 컴퓨터 포렌식(Computer Forensics)에 대한 관심이 급증하고 있다. 현재까지의 포렌식은 사이버 경찰청과 같은 수사 기관에서 아동 포르노나 인터넷 사기 등의 증거 확보 및 분석을 위해 사용되어 왔다. 그렇기 때문에 시스템 포렌식에 대한 연구만이 활발히 이루어졌다.[1-3]

하지만 현재는 인터넷의 급속한 발달과 함께 하루에도 수백만건의 해킹시도가 기록되고 있으며, 방대

접수일 : 2004년 5월 14일 ; 채택일 : 2004년 7월 26일
* 본 연구는 대학 IT연구센터 육성 지원 사업에 의해 수행되었습니다.
† 주저자 : p19j78s@korea.ac.kr
‡ 교신저자 : jsmoon@korea.ac.kr

한 양의 기록들에 대한 분석의 어려움은 실제적인 침해사고에 대한 확인을 어렵게 한다. 이러한 대규모 환경에서 효과적으로 침해사고에 대처하기 위해 자동화된 침해사고대응시스템이 제안되었고 국가기관 및 민간기업에서는 실제 구축에 들어간 상태이다.[4]

자동화된 침해사고대응시스템에서도 사후 대처를 위해 포렌식 기술을 이용한 정보 수집, 분석, 보관에 대한 연구를 진행하고 있다. 또한 자동화된 침해사고대응시스템에서는 시스템 및 소규모 네트웍이 아닌 방대한 네트웍의 침입을 다루어야 하기 때문에 네트웍 포렌식의 효과적 사용이 불가피하다. 네트웍 포렌식 정보는 시스템 포렌식 정보처럼 사건에 대해 침입의 확실한 정보를 제공하지는 않지만 침입 정보를 보충하고 정보에 대한 신뢰성을 제공하는 역할을 한다. 즉, 시스템내의 로그를 통해 손쉽게 컴퓨터 범죄자를 확인할 수 있다 하더라도, 컴퓨터 범죄와 관련된 각종 정보보호 장비 및 네트웍 장비의 정보를 통해 종합적인 컴퓨터 범죄 재현과 연관 정보들의 신뢰성을 키우는 작업이 필요하다.[5,6]

본 논문에서는 먼저 2장에서 자동화된 침해사고대응시스템에서의 네트웍 포렌식에 대한 개요를 통해 자동화된 침해사고대응시스템과 네트웍 포렌식에 대해 살펴본 후, 3장에서 자동화된 침해사고대응시스템에서 수집되어야 하는 네트웍 포렌식 정보를 정의한다. 마지막으로 4장에서 네트웍 포렌식 정보에 대해 증명하고 결론을 맺는다.

II. 자동화된 침해사고대응시스템에서의 네트웍 포렌식 개요

2.1 자동화된 침해사고대응시스템

자동화된 침해사고대응시스템은 개인이나 민간의 IT 정보, 회사의 정보보호관련 취약성 정보 등을 원격지에서 상호 간에 공유함과 동시에, 해킹, 바이러스, 사이버 테러 등의 비인가된 접속을 포함하는 침해 사고에 종합적으로 대응할 수 있도록 구성된 정보공유 및 분석센터(ISAC/S : Information Sharing & Analysis Center/System) 형태의 전사적 통합보안관제시스템(ESM) 및 이들 ISAC 및 ESM간의 정보 공유를 위한 신뢰정보공유네트웍(Trusted Information Sharing Network)을 말한다.

따라서, 자동화된 침해사고대응시스템은 시스템에 위협이 되는 광범위한 침해사고요소(해킹, 바이러스, 웜, 사이버테러, 네트웍 스파이, 정보전 등의 침해사고 및 취약성 정보)에 관한 정보를 자동으로 수집/분류하고, 해당 조직별로 필요한 방식으로 정보를 가공/분석하여 이용할 수 있으며, 축적된 정보보호관련

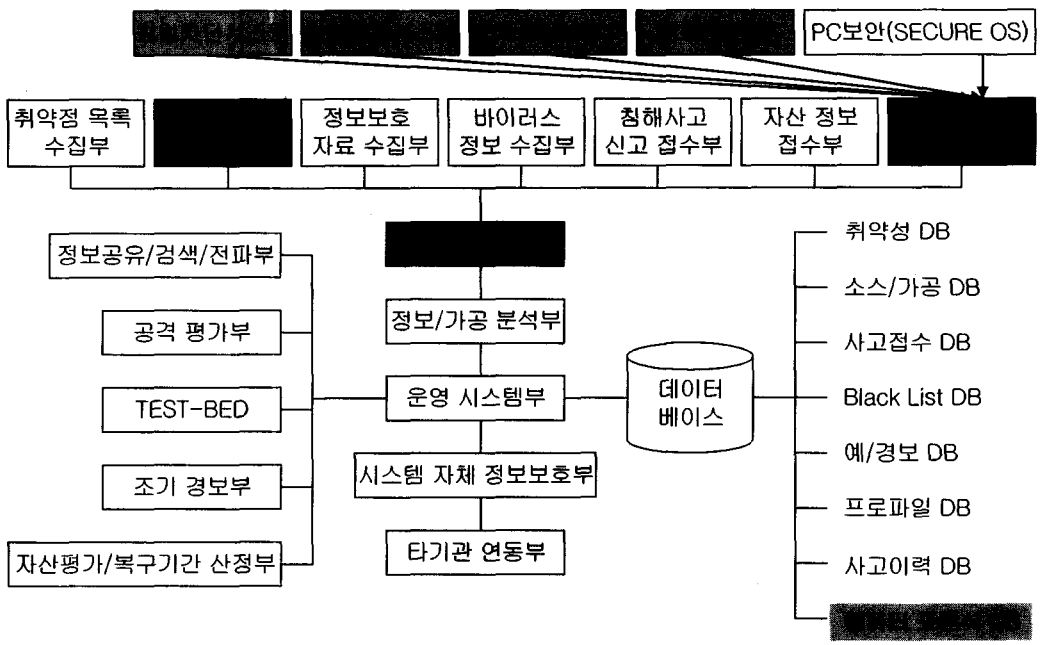


그림 1. 자동화된 침해사고대응시스템

정보의 안전한 공유 및 제공, 각 침해사고에 대한 공격평가와 조기 경보가 가능하며, 새로운 침해사고 및 공격방법에 대한 테스트(시뮬레이션)를 수행함으로써 효율적인 침해사고대응이 가능한 종합적인 침해사고 대응시스템과 그 운용방법의 구현을 목표로 한다.

그림 [1]은 이러한 자동화된 침해사고대응시스템의 전체구성도를 보이고 있다.[7] 자동화된 침해사고 대응시스템은, 웹, 전화, 전자메일, 팩스 등과 같은 통신망을 통하여 보호가 필요한 보호대상이 되는 컴퓨터 시스템 및 네트워크, 어플리케이션, 인터넷 서비스 등에 관련된 보안정보를 수집하고 원시 데이터를 저장하는 정보수집/관리분야와, 지식기반의 분석 알고리즘을 이용하여 수집된 보안정보를 가공 및 분석하고 분석 결과를 저장·관리하는 정보 가공/분석분야와, 가공/분석된 보안정보를 등급별로 분류/관리하고, 하나 이상의 보호대상 시스템 또는 다른 분야 시스템으로 전달하는 정보 공유/검색/전파분야와 필요한 보안정보를 소정 형식으로 출력하는 디스플레이분야(Wallscreen 혹은 다량의 모니터세트를 의미)를 포함하는 운영시스템분야와, 자동화된 침해사고대응시스템의 자체 정보보호를 위한 시스템 자체 정보보호분야와, 취약성 정보를 저장하는 취약성 데이터베이스와 원시 보안정보 및 가공/분석된 정보를 저장하는 소스/가공 DB를 포함하는 데이터베이스분야, 및 다른 분야 시스템과의 신뢰성이 있는 정보 공유를 위한 타기관 연동분야를 포함한다.[8]

자동화된 침해사고대응시스템에서 포렌식이 응용되는 부분은 그림 [1]에서 진하게 표시되었다. 침해사고대응시스템의 정보보호 관련 이벤트 수집부는 침입차단시스템, 침입탐지시스템, 가상사설망, 네트워크 장비의 정보들을 모은다. 그리고 취약점 결과 수집부는 해당 네트워크 상에 존재하는 알려진 취약점을 검색하고 수집한다. 정보보호관련 이벤트 수집부와 취약점 결과 수집부의 정보들은 정보수집/관리부의 정보로 통합되며 운영시스템부에 의해 포렌식 정보로 분류된 정보들만이 컴퓨터 포렌식 DB에 저장된다.

본 논문은 자동화된 침해사고대응시스템의 전체적인 모델 중 정보 수집부에 대해 다룬다. 그리고 전체 정보 수집부의 다양한 정보 중 포렌식 측면의 수집 정보에 초점을 맞춘다.

2.2 네트워 포렌식

네트워 포렌식은 침해사고 확인을 시발점으로 침해와 관련된 네트워 이벤트(Event)를 수집·분석·저장하는 일련의 과정이다. 네트워 포렌식의 목적은 침해당시의 상황 재구성을 통해 증거자료에 대한 신뢰성을 제공하는데 있다.

네트워 포렌식은 일반적으로 두 가지 형태로 분류된다[9].

- "Catch-it-as-you-can" systems

내부 네트워으로 진입하는 모든 패킷을 저장소(storage)에 저장하고 저장소의 정보를 이용하여 포렌식 분석서버에서 분석을 진행한다. 이 시스템은 많은 저장 공간을 필요로 한다.

- "Stop, look and listen" systems

내부 네트워으로 진입하는 패킷을 메모리로 가져와 먼저 분석을 진행하고 침입과 관련된 정보들만 저장소에 저장하는 방법이다. 적은 저장 공간을 필요로 하나 실시간 패킷 분석을 위해 빠른 처리가 필요하다.

기존의 네트워 포렌식에 대한 이러한 분류는 중형 전산망에서는 적합하지만 여러 정보보호장비로부터 수백만건의 로그정보들이 기록되는 자동화된 침해사고대응시스템에서는 의미가 없다. 그 이유는 첫째로 기존의 네트워 포렌식이 하루 수백만건의 로그 정보를 실시간으로 분석하고 현재상황을 파악해야 하는 현재의 환경에서 고려되지 않았기 때문이며, 둘째로 "여러 정보보호장비 및 네트워 장비의 연관성 분석을 통한 침해정보의 신뢰성 획득"이라는 개념이 고려되지 않았기 때문이다.

결국, 자동화된 침해사고대응시스템에서의 네트워 포렌식은 여러 정보보호장비 및 네트워 장비의 방대한 로그 및 상태정보 뿐만아니라 취약점 정보들을 수집하여 대용량의 데이터베이스에 저장하고, 이 정보들의 연관성을 분석하고, 분석된 정보를 안전하게 보전하여 실제 수사 과정이나 법적인 증거자료로서 사용하는 일련의 과정이다.

본 논문에서는 자동화된 침해사고대응시스템의 네트워 포렌식 연구에 있어 가장 기본이 되는 정보수집 단계에서 수집되어야 할 정보를 정의한다. 본 논문은 자동화된 침해사고대응시스템을 필요로 하는 대규모 전산망에서 고려되었다.

2.3 네트워 포렌식 정보의 범위(SCOPE)

본 논문에서는 네트워 포렌식 정보를 다음과 같이

정의한다. "네트워의 뼈대 역할을 하는 네트워 장비(Router, Switch 등)와 침입자로부터 네트워을 감시 및 보호하는 정보보호장비(Firewall, Monitering Server, IDS, VPN, 취약점 서버 등)에 의해 획득된 정보". 서버 시스템 자체의 로그정보 및 상태정보 혹은 시스템에서 동작하고 있는 모니터링 정보나 보안 로그 정보는 제외된다. 즉, 순수히 네트워 장비나 정보보호장비로서의 역할을 수행하는 시스템의 정보를 네트워 포렌식 정보로 정의한다.

2.4 네트웍 포렌식 정보의 연구 동향

기존의 네트워 포렌식에 대한 연구는 중·소 규모 네트워에서의 포렌식 정보 수집, 연구, 보관에 치중되어 왔다. 주요연구 분야로는 포렌식 정보의 안전한 수집과 정보의 연관성에 대한 분석 및 정리, 분석된 정보의 안전한 보관에 대한 내용이 주를 이루었다.[10-13] 하지만 아직까지 중·소 규모 네트워에서의 네트워 포렌식 정보에 대한 정의 조차도 명확한 연구가 이루어지지 못했다. 이는 중·소 규모 네트워에서의 네트워 포렌식 정보는 특별한 정의가 필요없는 즉각적으로 알 수 있는 정보로 여겨져 왔기 때문에 단지 이를 안전하게 수집하는데만 관심이 모아졌고 네트워 포렌식 정보 보다는 더 상세한 정보를 지니는 시스템 포렌식 정보의 정의와 획득이 관심이 모아져 왔기 때문이다.

그러나 최근들어 대형 대응 시스템들의 필요성이 대두됨에 따라 현 네트워의 위험 수위를 판단하고 이에 재빨리 대처하기 위해 네트워 포렌식에 대한 연구가 활발히 이루어지고 있는 실정이다. 이러한 연구는 유럽의 CSIRT 와 CERT에서 활발히 이루어지고 있다.[14] 하지만 네트워 포렌식 대한 연구 중 초기에 수집되어야 할 네트워 포렌식 정보에 대한 정의는 가장 기초적인 작업이며 중요한 작업임에도 불구하고 연구의 흔적을 찾을 수 없었다.

III. 자동화된 침해사고대응시스템을 위한 네트웍 포렌식 정보 정의

본 논문에서는 현재까지 포렌식 정보의 주류를 이루었던 시스템 포렌식 정보가 아닌 기본적인 시스템 포렌식 정보에 정확성과 신뢰성을 제공해 줄 수 있는 네트워 포렌식 정보를 정의한다. 날로 급증하는 해킹과 바이러스 등의 정보화 역기능을 해소하기 위해 수요가 급증하고 있는 자동화된 침해사고대응시스템에서 반드시 수집되어야 하는 네트워 포렌식 정보를 정의하는데 초점을 맞춘다.

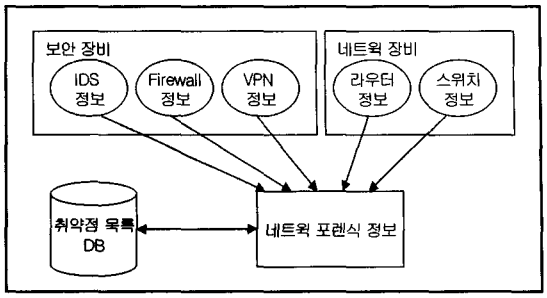


그림 2. 네트웍 포렌식 정보

그림 [2]는 자동화된 침해사고대응시스템에서 수집될 네트워 포렌식 정보의 전체 그림을 보이고 있다. 네트워 포렌식 정보는 크게 정보보호장비의 정보, 네트워장비의 정보, 취약점 정보를 이용한다. 정보보호장비의 정보에는 방화벽, 가상사설망, 침입탐지시스템 각각의 정보가 포함된다. 물론 더 다양한 정보보호장비에 대해 고려되어야 하지만 본 논문에서는 가장 일반적인 정보보호장비만을 다루도록 한다. 그리고 네트워 장비의 정보에는 라우터와 스위치의 정보를 포함한다. 취약점 정보는 취약점 스캐너에 의해 사전에 조사되어진 내부 네트워의 취약점을 말한다.

표 [1]에서 자동화된 침해사고대응시스템에서 수집되어야할 상세한 네트워 포렌식정보를 보이고 있다. 정보보호장비 및 네트워 장비의 네트워 포렌식 정보는 시간정보와 버전정보, 설정정보와 정책정보, 로그정보라는 3개의 주제로 분류된다. 그 중 시간정보와 버전정보는 모든 장비들에서 공통적으로 수집되어야 하는 정보이다. 해당 시스템의 시간정보는 각 시스템의 증거수집 시간을 명시하고 이후 시간 동기화에 사용될 수 있다. 해당 시스템의 버전정보는 시스템의 버전차이에 따른 성능 및 기능 차이를 고려하는데 사용된다.

설정정보와 정책정보 및 로그정보의 정보에 대해서는 이후의 소절에서 상세히 설명하도록 한다.

3.1 네트웍 장비 - 라우터(Router)

라우터의 설정정보와 정책정보에 대해 알아보자.

· Routing 정보 : 라우터의 라우팅 프로토콜

표 1. 네트워 포렌식 정보의 정의

	· Time · Version	· Time · Version	· Time · Version	· Time · Version	· Time · Version	· Time · Version
	· Port · Trunk · Vlan · 스위치 IP주소 · 설정된 터미널 및 터미널패스워드 · 스위치자체 패스워드	· Routing · ARP · Netstat · Interface · 설정된 터미널 및 터미널패스워드 · 라우터자체 패스워드	· 탐지정책 · 통제정책	· 연결정책	· 탐지정책	· 네트워상의 취약점 정보
	· Local Log	· Local Log · Netflow Log	· Local Log · Filtering Log	· Local Log · Connection Log	· Detection Log	

(Routing Protocol) 및 라우팅 테이블에 대한 정보를 포함한다. 침해 당시의 네트워 흐름을 파악할 수 있고 정보보호장비의 우회 가능성도 확인할 수 있다.

- ARP 정보 : 내부 네트워에 존재하는 호스트들의 IP 주소를 MAC 주소로 연결시키는 정보이다. 침해 당시, ARP Cache에 등록된 IP 주소와 MAC 주소 확인을 통해 네트워 상황파악이 가능하다. 또한 ARP Cache 정보는 ARP Spoofing 이나 Redirection 공격에 의해 변조될 가능성이 존재하기 때문에 확인이 필요하다.
- NETSTAT 정보 : 라우터에서 제공하는 네트워 서비스의 목록을 보여준다. 침해 당시, 라우터가 허용했던 서비스를 통해 침해상황재현에 이용할 수 있다.
- 라우터의 Interface 정보 : 라우터에 연결된 각 인터페이스(INTERFACE)들의 IP 주소와 서브넷팅(SUBNETTING)에 대한 정보이다. 침해 당시의 네트워 상황파악이 가능하다.
- 설정된 터미널 및 터미널 패스워드 정보 : 라우터에서 열려진 터미널에 대한 정보와 터미널 접속시의 패스워드 정보이다. 당시의 외부연결 가능성을 확인할 수 있다.
- 라우터 자체에 대한 패스워드 설정 여부 : 라우터의 설정을 변경하기 위해 Enable모드로 이동할 때의 입력 패스워드정보로 라우터 자체를 침해하는 공격에 대한 상황재현 정보로 사용된다.
- 라우터의 Access-List 정보 : 라우터에 설정된 패킷 필터링(Filtering)에 대한 규칙 정보로 라우터의 필터링여부와 필터링시의 정책 확인을 통해 침해 당시 네트워 상황파악이 가능하다.

라우터의 로그정보는 크게 두 가지로 분류 된다.

- 로컬로그 정보 : 라우터 자체의 설정오류나 장치상의 문제를 기록하고 ACL(Access Control List)에 의해 접속이 거부된 패킷(Packet) 정보를 기록한다. 로컬로그는 라우터 자체에 대한 공격여부를 파악하거나 침해당시 ACL에 의해 차단된 패킷정보를 이용해 당시 공격상황을 파악할 수 있다.
- 패킷 모니터링(Netflow log) 로그 정보 : 라우터를 경유하는 네트워 트래픽 중 라우터와 연동되는 NetFlow에 의해 기록되는 정보이다. 패킷 모니터링 로그는 라우터를 거치는 모든 패킷정보를 기록해 두기 때문에 이 후 침입자의 흔적을 찾기 위한 원천정보로 사용된다.

3.2 네트워 장비 - 스위치(switch)

스위치의 설정정보와 정책정보에 대해 알아보자.

- 스위치의 포트정보 : 전체 스위치 포트 중 현재 사용중인 포트와 사용중이지않은 포트의 정보를 지닌다. 스위치의 포트정보를 통해 침해당시의 네트워구성을 파악할 수 있다.
- Vlan(virtual LAN) 정보 : 하드웨어적이 아닌

소프트웨어적으로 스위치 포트의 전달(Broadcast) 영역을 나누기 위한 설정정보이다. 총 36개의 포트를 12개 씩 3 소그룹(sub-group)으로 나눈다면 해당 소그룹에 속한 호스트 간에만 스위치를 통한 데이터 교환이 가능하다. VLAN 정보를 통해 침해당시의 네트웍 구성을 파악할 수 있다.

- Trunk 정보 : Vlan으로 나누어진 스위치간 서브넷(subnet)영역으로 통신할 수 있게 하는 Trunk 서비스의 설정과 관련된 정보이다. Trunk 정보를 통해 침해사고 당시 스위치간의 연결을 통한 네트웍을 구축했었는지 확인할 수 있다.
- 스위치의 IP 주소정보 : 스위치로의 원격접속을 위해 설정하는 스위치의 IP주소정보이다. 스위치의 IP 주소정보가 설정되었다면 악의적 사용자의 원격접속을 통한 설정정보 변경을 의심해볼 수 있다.
- 설정된 터미널 및 터미널 패스워드 정보 : 스위치의 열려진 터미널에 대한 정보와 터미널 접속시의 패스워드 정보로서 당시의 외부연결 가능성을 확인할 수 있다.
- 스위치 자체에 대한 패스워드 설정 여부 : 스위치의 설정을 변경하기 위해 Enable모드로 이동할 때의 입력 패스워드정보로 스위치 자체를 침해하는 공격에 대한 상황재현 정보로 사용된다.
- 스위치의 로컬로그정보 : 스위치 종료, 시작, 재시작과 관련된 내용들이 기록된다. 로컬로그는 스위치 자체에 대한 공격여부를 파악하거나 스위치의 상태를 파악하는데 이용한다.

3.3 정보보호장비 - 방화벽(Firewall)

방화벽은 악의적인 공격자로부터 내부의 서버나 호스트들을 지키기 위한 보안관으로서의 역할을 한다. 내부로 접속하는 모든 네트웍 트래픽은 방화벽(firewall)을 통해서 접속하도록 허용하고 방화벽에서는 지나는 모든 네트웍 패킷의 IP 주소와 포트번호 그리고 연결상태를 기준으로 해당 패킷을 허용할지 거부할지를 결정한다.

- 방화벽의 통제정책 : 통제정책은 방화벽을 통한 출입의 허락(Allow)과 거부(Deny) 조건에 대한 목록정보로 방화벽의 동작(Operation)에 대한 기준이 되는 정보이다. 방화벽은 통제정책에 따라 동작하기 때문에 침해당시의 방화벽 동작상태를 알기위해 반드시 필요하다.
- 방화벽의 로그 정보 : 방화벽의 로그정보는 자체의 하드웨어적인 오류 혹은 설정 상의 오류에 대한 기록을 남기는 로컬로그정보와 접속이 거부되거나 허가된 패킷의 로그기록을 남기는 필터링(Filtering) 로그정보로 나뉜다. 방화벽의 필터링 로그정보는 침해당시의 허락되거나 거부된 패킷을 조사함으로써 침해사고에 대한 직접적인 정보를 제공한다.

3.4 정보보호장비 - 가상사설망(VPN)

가상사설망(VPN)은 가상사설망 게이트웨이(gateway) 대 게이트웨이 혹은 게이트웨이 대 원격 사용자(remote user) 간의 안전한 데이터 교환을 위해 패킷을 캡슐화 하여 보내는 기술이다. 자동화된 침해사고대응시스템에서는 공유 정보의 안전한 통신을 위해 가상사설망을 사용한다.

- 가상사설망의 연결정책(Policy)정보 : 외부에서 접속하는 신뢰된 사용자와 관련된 연결정보의 목록을 지닌다. 이 정보에는 신뢰하는 사용자의 IP 주소 영역범위와 호스트명 등을 포함한다. 가상사설망의 연결정책(Policy)정보는 가상사설망의 신뢰사용자 연결동작(Operation)에 대한 기준정보로서 침해당시 가상사설망의 운영상황을 확인할 수 있다.
- 가상사설망의 로그정보 : 가상사설망의 로그정보에는 중요 동작(activity)이 발생하거나 운영(SA 형성 혹은 Policy 적용, 캡슐화 혹은 역캡슐화 과정) 중에 오류가 발생할 경우 기록되는 로컬로그정보와 신뢰된 상대방과의 터널연결과 관련된 정보를 기록하는 연결로그정보가 있다. 연결로그정보는 상대 호스트의 IP 주소, 약속된 인자값(알고리즘, 킷값)을 포함한다. 침해당시 내부로 접근이 허락된 사용자는 침해사고의 유력한 용의자가 될 수 있기 때문에 가상사설망의 연결로그정보는 기본적인 네트웍 포렌식 정보이다.

3.5 정보보호장비 - 침입탐지시스템(IDS)

침입탐지시스템(IDS)는 공격자의 침입을 탐지하

여 관리자에게 알려주거나 관련 로그를 기록하는 시스템이다. 자동화된 침해사고대응시스템에서는 네트워 전체의 침해 상황을 파악하고 대처하기 위해 침입탐지시스템을 사용한다.

- 침입탐지시스템의 탐지정책 : 침입탐지시스템이 오용 탐지 기법의 시스템일 경우, Signature 룰이 탐지정책이 된다. 반면 비정상 탐지 기법의 시스템일 경우, 정상에 대한 기준(Profile)이 탐지정책이 된다. 침입탐지시스템의 탐지정책은 침입탐지에 대한 기준정보로서 침해당시 침입탐지시스템의 탐지정책에 따라 탐지로그정보가 기록되기 때문에 확인이 필요한 네트워 포렌식 정보이다.
- 침입탐지시스템의 탐지(Detection)로그정보 : 탐지로그정보는 침입탐지시스템의 탐지정책에 근거해 탐지된 악의적 사용자의 공격과 관련된 로그기록이다. 침입탐지시스템의 탐지로그정보는 침해공격에 대한 즉각적인 공격패킷 분석을 통해 기록된 침입정보이기 때문에 침해사고에 대한 직접적인 정보를 제공한다.

3.6 취약점 정보

취약점 정보는 취약점 스캐너에 의해 수집된 해당 네트워 및 호스트시스템들의 전체 취약점 목록[15]이다. 이러한 취약점 정보는 자동화된 침해사고대응시스템에서 취약점 데이터베이스 내에 저장되어 있다.

침해사고는 해당 시스템들의 취약점에 의해 발생하기 때문에 침해당시의 네트워이나 시스템의 취약점 정보는 중요한 포렌식 정보가 된다.

IV. 침해사고 시나리오를 통한 네트워 포렌식 정보에 대한 증명

본 절에서는 앞서 정의한 네트워 포렌식 정보를 증명한다. 앞서 정의한 네트워 포렌식 정보가 실제로 침해사고를 유추할 수 있는 포렌식 정보인지를 확인하는 과정이다. 침해사고의 원인이 되는 몇 가지 공격기법을 통해 정보보호장비 혹은 네트워 장비에 남는 침해흔적을 확인하는 방법을 사용한다. 이러한 침해흔적의 확인을 통해 앞 절에서 정의한 네트워 포렌식 정보의 증명이 가능하다. 본 절의 테스트 방법은 다음과 같다.

1. 침해공격과 흔적정보의 수집에 대한 시나리오(가설)를 세운다.
   - 침해공격에 대한 시나리오를 세운다.
   - 수집될 네트워 포렌식 정보에 대한 시나리오를 세운다.
2. 시나리오에 따라(가설대로) 침해공격을 시도하고 흔적정보를 수집한다.
   - 시나리오에 따라 공격을 진행한다.
   - 시나리오에 따라 네트워 포렌식 정보를 수집한다.
3. 수집된 흔적정보를 분석하고 침해공격 당시 상황을 유추한다.
   - 수집된 네트워 정보를 분석하여 침해공격 당시의 상황을 유추한다.
   - 초기 공격 시나리오와의 일치여부를 확인한다.

결국, 수집된 네트워 포렌식 정보의 분석을 통해 유추된 침해공격(3번)과 초기 시나리오에서 정의한 침해공격(1번)이 일치한다면 네트워 포렌식 정보에 대한 증명이 가능하다. 본 증명은 이론적인 침해공격 및 정보수집 시나리오를 통해 얻은 포렌식 정보와 실제테스트를 통해 얻은 포렌식 정보의 연계성을 확인하는 방식을 이용한다.

표 [1]에서 정의된 모든 정보에 대해 테스트가 이루어져야 하지만, 본 절에서는 대표적인 3가지 공격기법에 대해서 테스트를 진행하고 관련된 네트워 포렌식 정보를 증명한다. 또한 본 테스트는 정의된 모든 네트워 포렌식 정보를 언급하기 보다는 침해공격을 유추하기에 가장 적합한 각 정보보호장비의 로그정보와 네트워 상황을 파악할 수 있는 스위치와 라우터의 중요 설정정보를 중심으로 네트워 포렌식 정보를 증명한다. 기타 각 정보보호장비 및 네트워 장비의 시간 및 버전 정보, 정책정보들은 직접적으로 침해공격을 유추하지 못하기 때문에 증명부분에선 제외되지만 로그정보를 뒷받침하는 정보들로서 포렌식적 개념에 비추어 이론적인 합의가 이루어졌다고 본다.

4.1 테스트 준비 사항

테스트를 위한 네트워은 그림 [3]과 같다. 그리고 테스트에 사용된 장비는 다음과 같다.

- Cisco 7200 Series VXR
- Switch Catalyst 6000 Series
- Switch Catalyst 8500 Series
- Secure Works Firewall (Firewall)

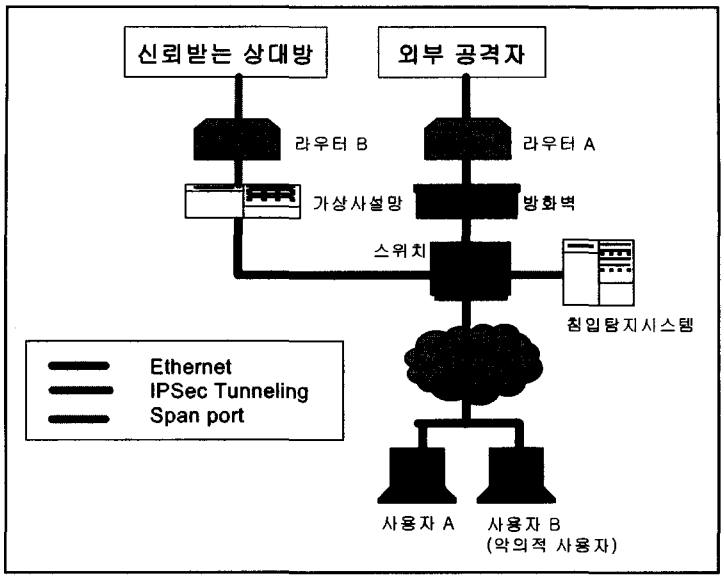


그림 3. 테스트 네트웍 환경

- Secure Works Firewall (VPN)
- Snort IDS

테스트에 사용된 각 장비 및 호스트 컴퓨터의 IP 주소는 다음과 같다.

- 외부공격자 : 211.241.48.123
- 신뢰받는 상대방 : 211.241.48.124
- 라우터 A : serial1 - 211.241.83.253
  ether0 - 192.168.83.253
- 라우터 B : serial1 - 211.241.83.250
  ether0 - 192.168.83.250
- 방화벽 : 211.241.83.97
- 가상사설망 : 211.241.83.99
- 침입탐지시스템 : 211.241.83.105
- 사용자 A : 211.241.83.108
- 사용자 B(악의적 사용자) : 211.241.83.109

테스트에 사용된 공격기법은 다음과 같다.

- 내부에서의 침해공격 : WINSMURF
- 외부에서의 침해공격 : XMAS 스캔, NT NULL SESSION
- 신뢰된 통로를 통한 연결 : BACKDOOR subseven

4.2 첫 번째 시나리오

4.2.1 시나리오 생성

- 침해공격에 대한 시나리오 : 공격자(사용자 B)는 내부의 사용자 A에게 SMURF flooding 공격을 시도한다. SMURF flooding 공격은 서비스거부공격의 일종으로 사용자 A에게 과도한 응답 UDP패킷을 보내게 된다. 방화벽에 의해 차단되기 때문에 외부로는 나가지 못한다.
- 수집될 네트웍 포렌식 정보에 대한 시나리오 : SMURF flooding 공격에 의한 영향 범위는 그림 [4]와 같고 공격에 대한 수집정보는 공격의 영향권 내에 속하는 다음의 정보들이다.

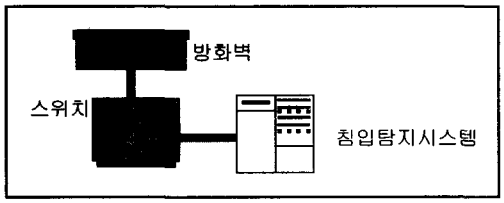


그림 4. SMURF flooding 공격에 의한 영향 범위

- 스위치의 포트정보 및 VLAN 정보
- 방화벽의 필터링 로그
- 침입탐지시스템의 탐지로그

침입탐지시스템과 방화벽에 SMURF 공격과 관련된 로그정보가 남게 되고 연관성을 지니게 된다. 또한 침해사고 당시의 내부 네트웍 상황을 파악하기 위해 스위치의 포트(Port)정보 및 Vlan 정보를 확인한다.

4.2.2 테스트 진행

- 침해공격 시나리오에 따라 공격을 진행한다.
- 수집 시나리오에 따라 정보를 수집한다. 수집정보는 표 [2]와 같다.

4.2.3 수집된 정보의 분석

수집된 정보에 대한 분석 및 분석결과는 표 [2]와 같다. SMURF flooding 공격에 대한 시나리오와 분석결과가 일치하기 때문에 수집될 네트웍 포렌식 정보로 정의한 스위치의 포트정보 및 VLAN 정보, 방화벽의 필터링 로그, 침입탐지시스템의 탐지로그정보는 올바른 네트웍 포렌식 정보이다.

4.3 두 번째 시나리오

4.3.1 시나리오 생성

- 침해공격에 대한 시나리오 : 외부의 공격자는 사용자 A가 NETBIOS 서비스(Tcp 139)를 제공하고 있는지 확인하기 위해 NMAP을 사용한 XMAS 스캔을 시도한다. 스캔의 결과 NETBIOS 서비스가 제공된다는 것을 안 공격자는 NT NULL SESSION을 연결한다.
- 수집될 네트웍 포렌식 정보에 대한 시나리오 : 외부에서의 XMAS 스캔 및 NT NULL SESSION 공격에 의한 영향 범위는 그림 [5]와 같고 공격에 대한 수집정보는 공격의 영향권내에 속하는 다음의 정보들이다.

- 스위치의 포트정보 및 VLAN정보
- 라우터 A의 Routing 및 Netstat 정보
- 방화벽의 필터링 로그

표 2. SMURF flooding 공격에 대한 분석정보

<table>
<tr><th colspan="2">정보</th><th>네트웍 포렌식 정보</th></tr>
<tr><td rowspan="2">방화벽</td><td>로그정보</td><td>e1000g2 rtip 거부 시작 2004/04/23 18:43:26 UDP 211.241.83.108:520
255.255.255.255:520 cno=0 nno=0 PKT=0 SIZE=0 (FRAG: PKT=0 SIZE=0)
e1000g2 rtip 거부 종료 2004/04/23 18:43:29 UDP 211.241.83.108:520
255.255.255.255:520 cno=0 nno=0 PKT=1 SIZE=0 (FRAG: PKT=0 SIZE=0)</td></tr>
<tr><td>분석결과</td><td>2004/04/23 18:43:26과 18:43:29에 각각 브로드캐스트영역(255.255.255.255)으로의 UDP 패킷이 거부되었다.</td></tr>
<tr><td>침입탐지시스템</td><td>로그정보</td><td>[**] UDP smurf [**] 04/23-18:43:26, 371260 211.241.83.108:520 -> 255.255.255.255:520 UDP TTL:255 TOS:0X0 ID:23372 ******S* Seq: 0xA1300402 Ack: 0x0 Win: 0xC00</td></tr>
<tr><td></td><td>분석결과</td><td>2004/04/23-18:43:26에 211.241.83.108:520 -> 255.255.255.255:520으로의 UDP smurf 공격이 탐지되었다.</td></tr>
<tr><td>스위치</td><td>포트정보 및 VLAN 정보</td><td>Port Name Status Vlan Duplex Speed Type
---- ---------- ---------- ---------- ------ ----- ----------
4/1 connected 1 auto auto 10/100BaseTX
4/2 connected 1 auto auto 10/100BaseTX
4/3 notconnect 1 auto auto 10/100BaseTX
4/4 notconnect 1 auto auto 10/100BaseTX
4/5 notconnect 1 full 100 10/100BaseTX
4/6 notconnect 1 full 100 10/100BaseTX
4/7 notconnect 1 half 100 10/100BaseTX
4/8 notconnect 1 half 100 10/100BaseTX
6/1 monitor 1 full 1000 1000BaseSX
6/2 connected 1 full 1000 1000BaseSX
6/3 connected 1 full 1000 1000BaseSX</td></tr>
<tr><td></td><td>분석결과</td><td>4/1과 4/2 포트가 내부 호스트와 연결되어있고 6/2가 방화벽과 6/3이 가상사설망과 연결되었으며 6/1이 침입탐지시스템과 연결되어있다. 스위치는 하나의 서브그룹을 지닌다.(by Vlan)</td></tr>
<tr><td colspan="3">flooding 공격을 시도한다.</td></tr>
</table>

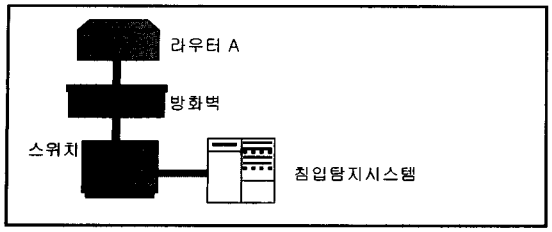


그림 5. XMAS 스캔 및 NT NULL SESSION 공격의 영향범위

- 침입탐지시스템의 탐지로그

방화벽과 침입탐지시스템에 NETBIOS 공격과 관련된 정보가 기록된다. 그리고 당시의 네트웍 상황을 파악하기 위해 라우터 A의 라우팅 테이블과 제공 서비스 정보, 스위치의 포트(Port)정보 및 Vlan 정보를 확인해야 한다.

4.3.2 테스트 진행

- 침해공격 시나리오에 따라 공격을 진행한다.
- 수집 시나리오에 따라 정보를 수집한다. 수집정보는 표 [3]과 같다.

4.3.3 수집된 정보의 분석

수집된 정보에 대한 분석 및 분석결과는 표 [3]와 같다. XMAS 스캔 및 NT NULL SESSION 공격에 대한 시나리오와 분석결과가 일치하기 때문에 수집될 네트웍 포렌식 정보로 정의한 스위치의 포트정보 및 VLAN 정보, 라우터 A의 Routing 및 Netstat 정보, 방화벽의 필터링 로그, 침입탐지시스템의 탐지로그정보는 올바른 네트웍 포렌식 정보이다.

4.4 세 번째 시나리오

4.4.1 시나리오 생성

- 침해공격에 대한 시나리오 : 신뢰받는 상대방은 가상사설망을 통해 내부 네트웍에 접속하고 사전에 사용자 A에 설치되어 대기상태에 있는 Subseven이라는 백도어(Back-Door)에 통제신호를 보낸다. 이 통제신호를 통해 사용자 A의 호스트 컴퓨터를 제어할 수 있다.
- 수집될 네트웍 포렌식 정보에 대한 시나리오 : 신뢰된 사용자의 백도어 공격에 의한 영향 범위는 그림 [6]과 같고 공격에 대한 수집정보는 공격의 영향권 내에 속하는 다음의 정보들이다.

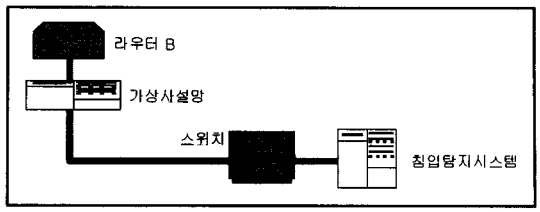


그림 6. 신뢰된 사용자의 백도어 공격에 의한 영향 범위

- 스위치의 포트정보 및 VLAN정보
- 라우터 B의 Routing 및 Netstat 정보
- 가상사설망의 연결로그
- 침입탐지시스템의 탐지로그

가상사설망과 침입탐지시스템에는 백도어 공격과 관련된 로그정보가 기록된다. 또한 침해사고 당시의 내부 네트웍 상황을 파악하기 위해 라우터와 스위치의 정보를 확인해야한다.

4.4.2 테스트 진행

- 침해공격 시나리오에 따라 공격을 진행한다.
- 수집 시나리오에 따라 정보를 수집한다. 수집정보는 표 [4]와 같다.

4.4.3 수집된 정보의 분석

수집된 정보에 대한 분석 및 분석결과는 표 [4]와 같다. 신뢰받는 상대방의 백도어 공격에 대한 시나리오와 분석결과가 일치하기 때문에 수집될 네트웍 포렌식 정보로 정의한 스위치의 포트정보 및 VLAN 정보, 라우터 B의 Routing 및 Netstat 정보, 가상사설망의 연결로그, 침입탐지시스템의 탐지로그정보는 올바른 네트웍 포렌식 정보이다.

VI. 결론 및 향후 연구 방향

자동화된 침해사고대응시스템에서 포렌식은 잦은 보안 사고의 사후 대처를 위해 필수적인 부분이고 특히나 네트웍 포렌식은 전체 네트웍에서 일어나는 침해 정보를 기록하기 때문에 수사시의 사건재구성을 용이하게 하고 침해흔적에 대한 신뢰성을 보장해 주는 중요 부분이다. 본 논문에서는 자동화된 침해사고대응시스템에서 수집되어야 하는 네트웍 포렌식 정보

표 3. XMAS 스캔 및 NT NULL SESSION 공격에 대한 분석정보

방화벽	로그정보	e1000g2 rtip 허용 시작 2004/04/23 19:52:57 TCP 211.241.48.123:2891 211.241.83.108:139 cno=0 nno=0 PKT=1 SIZE=64 (FRAG: PKT=0 SIZE=0) e1000g2 rtip 허용 시작 2004/04/23 19:52:58 TCP 211.241.83.108:139 211.241.48.123:2891 cno=0 nno=0 PKT=1 SIZE=60 (FRAG: PKT=0 SIZE=0) --- e1000g2 rtip 허용 시작 2004/04/23 19:56:54 TCP 211.241.48.123:3012 211.241.83.108:139 cno=0 nno=0 PKT=1 SIZE=48 (FRAG: PKT=0 SIZE=0) e1000g2 rtip 허용 시작 2004/04/23 19:56:54 TCP 211.241.83.108:139 211.241.48.123:3012 cno=0 nno=0 PKT=1 SIZE=48 (FRAG: PKT=0 SIZE=0) e1000g2 rtip 허용 시작 2004/04/23 19:56:54 TCP 211.241.48.123:3012 211.241.83.108:139 cno=0 nno=0 PKT=1 SIZE=40 (FRAG: PKT=0 SIZE=0) e1000g2 rtip 허용 시작 2004/04/23 19:56:55 TCP 211.241.48.123:3012 211.241.83.108:139 cno=0 nno=0 PKT=1 SIZE=140 (FRAG: PKT=0 SIZE=0)
	분석결과	2004/04/23 19:52:57에 211.241.48.123에서 사용자A(211.241.83.108)로 TCP 139번 연결시도가 있었다. 4분 뒤인 2004/04/23 19:56:54에 211.241.48.123에서 사용자A(211.241.83.108)로 TCP 139번 연결이 이루어졌다.
침입탐지 시스템	로그정보	[**] SCAN XMAS [**] 04/23-19:52:57, 758320 211.241.48.123:2891 -> 211.241.83.108:139 TCP TTL:46 TOS:0X0 ID:13512 12UAPRSF Seq: 0xA2800504 Ack: 0x0 Win: 0xC00 [**] NETBIOS NT NULL session [**] 04/23-19:56:55, 758320 211.167.71.86:4875 -> 211.241.83.108:139 TCP TTL:64 TOS:0X0 ID:26611 ...AP... Seq: 0x9b7d17be Ack: 0xf8c2077d Win: 0xffff
	분석결과	2004/04/23 19:52:57에 211.241.48.123에서 사용자A(211.241.83.108)로 XMAS SCAN 공격이 이루어졌다. 4분 뒤인 2004/04/23 19:56:54에 211.241.48.123에서 사용자A(211.241.83.108)로 NETBIOS NT NULL session공격이 이루어졌다.
라우터	라우팅정보	Gateway of last resort is 192.168.31.98 to network 0.0.0.0 192.168.83.0 255.255.0.0 is subnetted, 1 subnets C 192.168.83.253 is directly connected, Ethernet0 211.241.83.253 255.255.255.252 is subnetted, 1 subnets C 211.241.83.253 is directly connected, Serial1 S* 0.0.0.0 0.0.0.0 [1/0] via 211.241.83.254
	NETSTAT 정보	Proto Recv-Q Send-Q Local Address Foreign Address (state) tcp 0 0 *.23 *.* LISTEN udp 0 0 *.161 *.* udp 0 0 *.69 *.*
	분석결과	라우터는 내부의 ether0 인터페이스에 192.168.83.253주소를 사용하고 외부와의 통신을 위한 serial1 인터페이스에 211.241.83.253주소를 사용한다. 해당 라우터는 211.241.83.254를 통해 통신하도록 정적라우팅이 설정되어 있다. 라우터는 Telnet(23), SNMP(161), TFTP(69) 서비스를 지원하고 있으며 Telnet 서비스만이 대기상태에 있다.
스위치	설정정보	첫 번째 시나리오의 설정정보와 동일하다.

표 4. 신뢰된 사용자의 백도어 공격에 대한 분석정보

가상사설망	로그정보	- IKE 로그 2004-04-23 20:25 IPSEC P2 connection "IPSEC000-Tunnel" (211.241.48.124→211.241.83.99) established 2004-04-23 20:25 pf_key_v2_set_spi: protocol:ESP encryption_alg:3DES_CBC authentication:SHA1 encap_mode:TUNNEL dst:211.241.83.99 2004-04-23 20:25 ADD flow (dst 211.241.83.99, 211.241.48.124 <-> 211.241.83.99) - 가상사설망 allow 로그 2004-04-23 20:56:55,FW,211.241.48.124:27374/tcp,211.241.83.108:5012,0,0,VPN 2004-04-23 20:56:57,FW,211.241.83.108:5012/tcp,211.241.48.124:27374,0,0,External
	분석결과	2004-04-23 20:25에 211.241.48.124→211.241.83.99 간에 IKE 프로토콜에 따른 신뢰된 연결이 이루어진다. 그 후 2004-04-23 20:56:55에 신뢰된 연결을 통해 211.241.48.124호스트에서 사용자A로 연결을 맺는다.
침입탐지시스템	로그정보	[**] BACKDOOR subseven 22 [**] 04/23-20:56:55, 7612380 211.241.48.124:27374 -> 211.241.83.108:5012 TCP TTL:64 TOS:0X0 ID:13219 ...AP... Seq: 0x3b11170b Ack: 0x72c6781c Win: 0xffff
	분석결과	2004-04-23 20:25에 신뢰된 사용자 211.241.48.124가 사용자A(211.241.83.108)에게 subseven 백도어에 대한 제어신호를 보낸다.
라우터	라우팅정보	Gateway of last resort is 192.168.31.98 to network 0.0.0.0 192.168.83.0 255.255.0.0 is subnetted, 1 subnets C 192.168.83.250 is directly connected, Ethernet0 211.241.83.250 255.255.255.252 is subnetted, 1 subnets C 211.241.83.250 is directly connected, Serial1 S* 0.0.0.0 0.0.0.0 [1/0] via 211.241.83.251
	NETSTAT정보	Proto Recv-Q Send-Q Local Address Foreign Address (state) tcp 0 0 *.23 *.* LISTEN udp 0 0 *.161 *.* udp 0 0 *.69 *.*
	분석결과	라우터는 내부의 ether0 인터페이스에 192.168.83.250주소를 사용하고 외부와의 통신을 위한 serial1 인터페이스에 211.241.83.250주소를 사용한다. 해당 라우터는 211.241.83.251를 통해 통신하도록 정적라우팅이 설정되어 있다. 라우터는 Telnet(23), SNMP(161), TFTP(69) 서비스를 지원하고 있으며 Telnet 서비스만이 대기상태에 있다.
스위치	설정정보	첫 번째 시나리오의 설정정보와 동일하다.

를 정의하고 실제 공격테스트를 통해 이 정보들에 대한 증명을 진행하였다.

본 논문에서는 네트웍 포렌식에 대한 가장 기초적인 부분인 수집정보의 정의를 다루었지만, 이후에는 네트웍 포렌식 분야에 관한 다양한 연구가 필요할 것이다. 먼저 자동화된 침해탐지대응시스템에서 침해사고의 유·무를 판단하는 침해사고판단시스템에 대한 연구가 필요하다. 이 연구는 IDS처럼 침해의 가능성이 아닌 각 시스템에서 일어난 실제 침해사고를 판단하여야 한다. 그리고 자동화된 침해탐지대응시스템 내에서 포렌식 정보를 안전하게 수집하고 보관하기 위한 기술과 절차에 대한 연구도 필요하다. 포렌식

정보가 안전하게 수집되었다면 획득된 포렌식 정보를 관리자가 단순하고 명확하고 확인할 수 있도록 분석하고 정리해주는 알고리즘에 대한 연구도 있어야 한다. 마지막으로 분석과 정리가 이루어진 포렌식 정보를 자동화된 침해사고대응시스템내의 다른 각 단위 시스템들과 응용하여 최대의 효과를 얻어내는 것에 대한 연구가 필요할 것이다.

참 고 문 헌

[1] Henry B. Wolfe, "Electronic Evidence Gathering", DEAKIN UNIV, Seventh Australasian Conference on Information Security and Privacy, 2002

[2] Allan H. Magee, Michael J. Hittel, "Securing and preserving the scene of an electrical accident", GM Worldwide Facilities Member, Industrial and Commercial Power Systems Technical Conference. IEEE, 2001.

[3] Keith J. Jones, "incident response: Performing Investigations on a Live Host", computer forensic consultant for Foundstone, The Magazine of Usenix & Sage, pp. 26-31, November, 2001.

[5] Rik Rarrow, "Correlating Log File Entries", The Ohio State University Incident Response Team, The Magazine of Usenix & Sage, pp. 38-44, November, 2000.

[6] Brad Powell, "forensics lite", Sun Microsystems, The Magazine of Usenix & Sage, pp. 32-42, November, 2001.

[7] 최운호, "종합 침해사고 대응시스템의 전체 구성", 금융결제원

[8] 최운호, "국가 사이버상황실(CyberWaroom) 구축연구", 금융결제원

[9] 한민옥, 국가 사이버테러 대응체계 가동", 디지털타임스, 16, December, 2003

[10] Melisa LaBancz, "Network Forensics", networkSecurity.com, IT Journalist, April, 2002.

[11] Vicka Corey, Charles Peterman, Sybil Shearin, Michael S.Greenberg, and James Van Bokkelen, "Network Forensics Analysis", Sandstorm Enterprises, IEEE Internet Computing Magazine, November 2002.

[12] Liu Jiqiang, Han Zhen, Lan Zengwei, "Secure audit logs server to support computer forensics in criminal nvestigations", Department of Computer Science, Northen Jiaotong University, Proceeding of IEEE TENCON, 2002

[13] J. Philip Craiger, Alex Nicoll, Bline Burnham, "An Applied Cource in Network Forensics", Department of Computer Science & Nebraska University Consortium for Information Assurance, Secure and Dependable Systems Workshop, September 23-25, 2002.

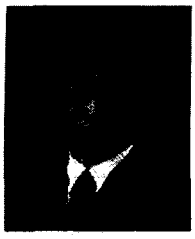
[14] Kulesh Shanmugasundaram, Nasir Memon, "ForNet:A Distributed Forensic Network", Polytechnic UNIV, Digital Forensic Research Workshop, 2002.

[15] Renaud Deraison and Jordan Hrycaj, "nessus: the free network security scanner", Nessus project, The Magazine of Usenix & Sage, pp. 45-48, November, 2000.

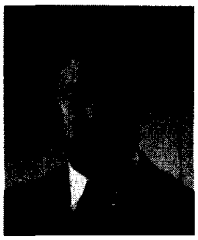
[16] Eoghan Casey, "HANDBOOF OF Computer Crime Investigation", ACDEMIC PRESS, 2003

[17] Stephen Northcutt, Mark Cooper, Matt Fearnow, Karen Frederick, "Intrusion Signatures and Analysis" New Riders, January 2001.

〈著者紹介〉



박 종 성 (Jong-Seong Park)
2002년 2월 : 경남대학교 졸업(공학사)
2003년 2월~현재 : 고려대학교 정보보호대학원 석사과정
〈관심분야〉 네트워크 · 시스템보안, 컴퓨터 포렌식



최 운 호 (Un-Ho Choi)
1990 광운대학교(학사)
1995 광운대학교 대학원 전자계산학과(석사)
2000 광운대학교 대학원 컴퓨터과학과(박사과정 수료)
〈관심분야〉 조기경보, 블랙리스트, 관제센터 운영, 침해사고신고 자동화 등

손 태 식 (TaeShik Sohn)
2000년 2월 : 아주대학교 정보 및 컴퓨터 공학부 졸업(공학사)
2002년 2월 : 아주대학교 정보통신공학과 졸업(공학석사)
2002년 3월~2004년 2월 : 고려대학교 정보보호대학원 박사수료
2002년 8월~현재 : 고려대학교 정보보호기술연구센터
2004년 2월~현재 : Visiting Researcher, University of Minnesota
〈관심분야〉 네트워크 · 시스템보안, 인터넷프로토콜 보안

문 종 섭 (JongSub Moon)
1981년 2월 : 서울대학교 계산통계학과 학사
1983년 2월 : 서울대학교 계산통계학과 석사
1992년 2월 : Illinois Institute of Technology 박사
1993년~현재 : 고려대학교 전자 및 정보공학부 교수
고려대학교 정보보호대학원 겸임 교수
〈관심분야〉 IDS, 신경망, 생체인식, 운영체제