개인정보 보호를 위한 네트워크 보안장비의 로그 가시화 방법 연구

심희연* · 김형종*

요 약

최근 들어 단순히 시스템에 남아있는 단서들을 분석하는 디스크 포렌식에서 공격자의 추적을 위해 시스템이 포함하는 네트워크의 침입 관련 정보를 분석하여 네트워크 포렌식의 연구가 활발해지고 있다. Firewall이나 IDS, 웹서버 로그의 상호 관계와 분석은 네트워크 포렌식 절차에서 중요한 역할을 한다. 이 연구는 네트워크 포랜식에서 개인정보 노출 감시를 위한 통합 GUI를 제시한다. 본 논문에서는 네트워크 포렌식을 위한 다양한 로그 정보들의 필요성을 제시하고 개인정보 누출을 모니터하는 보안 관리자를 위한 GUI를 설계한다.

An Log Visualization Method of Network Security Equipment for Private Information Security

Hee Youn Sim* · Hyung Jong Kim

ABSTRACT

Recently, network forensic research which analyzes intrusion-related information for tracing of attackers, has been becoming more popular than disk forensic which analyzes remaining evidences in a system. Analysis and correlation of logs from firewall, IDS(Intrusion Detect System) and web server are important part in network forensic procedures. This work suggests integrated graphical user interface of network forensic for private information leakage detection. This paper shows the necessity of various log information for network forensic and a design of graphical user interface for security managers who need to monitor the leakage of private information.

Key words : 네트워크 포렌식, 인터페이스, 침입탐지

* 서울여자대학교 컴퓨터학부

1. 서 론

컴퓨터 사용의 증가로 많은 분야에서 사용자에게 디지털 환경의 서비스를 제공하게 되었고, 오늘날 '언제어디서나 인터넷과 컴퓨터가 연결되어 존재하는' 유비쿼터스 시대에 도래하였다. 이러한 서비스 제공을 위해 사용자의 정보를 효율적으로 저장할 수 있는 DB사용이 급증하였고, 범죄양상 또한 디지털 환경에서 이루어지는 시스템 공격이나 해킹으로 인한 사용자의 정보유출과 같이 기존의 범죄양상과 다른 형태로 전개되고 있다.

디지털 포렌식은 디지털 환경의 범죄수사에 쓰이는 증거 수집 방법으로 많은 범죄수사에 사용되고 있으며 현재 많은 연구가 이루어지고 있다.

최근 들어 단순히 시스템에 남아있는 단서들을 분석하는 디스크 포렌식에서 시스템이 포함하는 네트워크의 침입 관련 정보를 얻고 분석해서 역추적 하는 네트워크 포렌식의 연구가 활발해지고 있다. 본 연구는 네트워크 포렌식의 사용자 인터페이스에 대한 설계를 제시하고 있다. 특히, 가용성이 높은 공개용 침입탐지 시스템, 방화벽 및 웹서버의 로그정보를 기반으로 포렌식을 실행하는 방안을 제시한다. 이러한 제안을 통해 포렌식의 이론적 접근을 통해 난해한 형태로 제시되는 것에 대한 일정 수준의 해법을 제시하는데 가치가 있다고 볼 수 있다.

본 논문의, 제 2장에서는 관련 연구로 로그가 저장될 포렌식 시스템에 대한 정의와 각 시스템별로 제공하는 기능들에 대해서 소개한다. 제 3장에서는 각 시스템에 저장되는 로그의 형태를 분석하고 역추적에 필요한 정보를 추출하여 포렌식 관리자에게 제공하는 인터페이스를 제시한다. 제 4장에서는 정상적인 행위와 비정상적인 행위의 시나리오를 제시하여 본 논문에서 제시한 인터페이스에 적용해 본다. 제 5장에서는 본 논문의 결론과 향후 연구에 대해 기술한다.

2. 연구 배경

2.1 네트워크 포렌식

컴퓨터 포렌식이란 컴퓨터를 매개로 이루어지는 범죄행위에 대한 법적 증거 자료를 확보하기 위해 컴퓨터시스템과 네트워크로부터 정보를 수집, 보존, 복구 및 분석하여 법정 증거물로서 제출할 수 있도록 하는 일련의 행위를 의미한다.

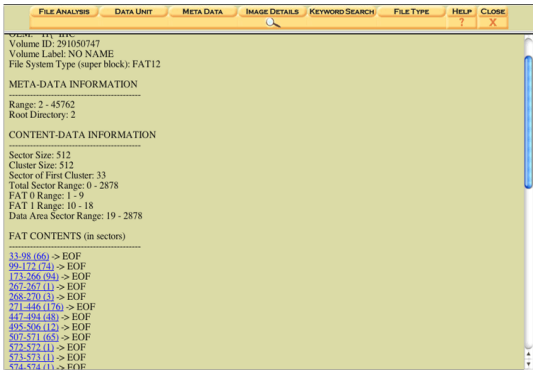
여기서 네트워크 포렌식은 침해사고가 발생 했을 때, 발생의 진원지를 파악하기 위해 네트워크 관련 자료를 수집하고, 저장해 두었다가 IP나 E-Mail, 로그 등을 분석하는 행위이다.

포렌식 시스템은 모든 로그를 수집하여 저장해 두었다가 포렌식 서버에서 분석을 수행하는 CIAYC (Catch It As You Can)시스템과, 내부 네트워크로 진입하는 패킷을 메모리로 가져와 먼저 분석을 진행하고 침입과 관련된 정보만을 저장하는 SLAL (Stop Look And Listen)시스템으로 분류된다.

기존의 네트워크 포렉식 도구들은 이 두 가지 방법 중 하나를 선택하여 사고가 발생 시 사고의 단서가 되는 정보를 추적하는 형태로 진행된다. 그러나 현실적으로 볼 때 네트워크 패킷을 추출하는 것은 침입탐지시스템, 방화벽, 웹서버로그 등의 기존 보안 시스템이 갖는 정보를 사용하는 경우, 선택의 여지가 있지 않은 것이 현실이다. 기존의 포렌식 도구들이 갖는 특성으로 다른 한 가지는 사고 발생의 단서가 되는 시스템의 모든 정보에 대해 이미지를 만들어 분석을 수행하는 것이다[9]. (그림 1)은 The Sleuth Toolkit을 기반으로 동작하는 사용자 인터페이스인 Autopsy의 사용자 인터페이스 중 분석 대상이 되는 파일 시스템의 자세한 내용을 확인하기 위한 인터페이스이다.

본 논문에서는 방화벽, 침입탐지시스템, 웹서버에서 생성되는 로그를 기반으로 수행할 수 있는 포렌식 기능을 제시하는 데에 그 목표를 두고 있다. 이러한 환경에서는 CIAYC 특성을 갖는 시스

템으로 모든 로그를 저장 후 모니터링 할 수 있으므로 개별적으로 분석이 가능하고, 실시간으로 탐지하지 못했던 비정상 행위를 찾을 수 있으며, 법정 대응에 대한 증거수집, 사후 관리 등을 제공해 줄 수 있다.



(그림 1) Autopsy의 파일시스템 이미지 자세히 보기

2.2 포렌식 데이터 수집대상 분석

본 연구 포렌식 도구가 활용되는 데이터 소스에 해당하는 방화벽, 침입탐지시스템 및 웹 로그는 수집이 용이한 특성을 갖는 것들이다. 특히 본 연구에서는 공개 소프트웨어의 로그 분석을 통해 이들 사이의 연결 관계를 제시하는 소프트웨어의 사용자 인터페이스를 설계하고자 한다. 다음은 각 장비가 갖는 주요 기능들이다.

방화벽의 주요기능은 다음과 같다.

- 외부의 침입으로부터 내부 망 보호
- IP 주소 및 port 번호를 이용하여 외부의 접속을 차단
- 사용자 인증에 기반을 두고 외부접속을 차단
- 상호 접속된 네트워크에 대한 트래픽 감시기록

침입탐지 시스템의 주요 기능은 다음과 같다.

- 탐지 대상에서 생산되는 사용내역이나 네트워크상의 패킷 등의 데이터 수집
- 수집된 데이터를 가공하여 침입 판정 및 로그 기록
- 가공된 데이터를 이용하여 침입여부 판정
- 자동으로 대응하거나 관리자에게 보고

웹서버의 주요기능은 다음과 같이 정리 할 수 있다.

- 인증, 정적 콘텐츠 관리
- HTTP, HTTPS 지원, 콘텐츠 압축
- 가상 호스팅, 대용량 파일 지원
- 대역폭 스로틀링, 통신기록

3. 로그 분석 및 인터페이스 제시

각 시스템(Firewall, IDS, Web Server)마다 남기는 로그의 형태와 정보의 종류는 다르지만 침입의 근원지를 파악하기 위한 역추적에 모두 필요한 정보는 아니다. 각 시스템의 로그의 형태를 파악하여 필요한 정보만 취함으로써 관리자나 로그 분석자에게 좀 더 빠르게 로그의 흐름을 파악할 수 있다.

본 연구의 핵심 포렌식 활용 대상 보안 시스템은 Suse Firewall, Snort, Apache Web Server이다. 이들은 본 연구의 공개용 소프트웨어를 통한 포렌식이라는 목적에 부합되는 도구들이며, 실 운영 환경에서 활용이 가능한 동시에, 포렌식에 활용할 가능한 자세한 로그정보를 제공해 주는 특성을 갖는다.

3.1 Suse Firewall 로그

본 연구에서 다루는 방화벽의 로그 는 위의 (그림 2)와 같은 형태로 이루어져 있다. 로그를 통해 알 수 있는 정보는 트래픽이 들어온 시간과 들어오거나 나가는 인터페이스, 출발지 주소와 목적지 주소 그 외에 포트 정보 등을 알 수 있다. 여기서

역추적에서 중요하게 쓰일 정보들은 다음과 같다.

- 출발지 주소와 포트 : 침입을 하거나 공격을 했을 경우 공격자의 IP주소를 파악하거나 공격의 종류를 파악 한때
- 목적지 주소와 포트 : 침입을 하거나 공격을 했을 경우 공격 대상인 시스템을 파악하고 시스템의 취약점을 판단하거나 공격의 종류를 파악할 때.
- 시간 : 사용자가 주로 접속하는 시간, 역추적에서 경로 파악할 때.

```
18 : 23 : 36 IN = eth0 OUT = eth1 SRC = 192.168.0.11
DST = 203.246.40.46 LEN = 40 TOS = 0x00 PREC
= 0x00 TTL = 127 ID = 787 DF PROTO = TCP
SPT = 1175 DPT = 80 WINDOW = 0 RES = 0x00
ACK RST URGP = 0
18 : 23 : 36 IN = eth0 OUT = eth1 SRC = 192.168.0.11
DST = 203.246.40.46 LEN = 40 TOS = 0x00 PREC
= 0x00 TTL = 127 ID = 786 DF PROTO = TCP
SPT = 1169 DPT = 80 WINDOW = 0 RES = 0x00
ACK RST URGP = 0
```

(그림 2) Firewall에서 나오는 로그 형태

3.2 Snort 로그

Snort의 로그 는 위의 (그림 3)과 같은 형태로 이루어져 있다. 로그를 통해 알 수 있는 정보는 트래픽이 들어온 시간과 공격의 종류, 출발지 주소와 목적지 주소 그 외에 포트 정보 등을 알 수 있다. 여기서 역추적에서 중요하게 쓰일 정보들은 다음과 같다.

- 공격의 종류 : IDS에서 rule에 의해 탐지된 공격을 파악할 때.
- 출발지 주소와 포트 : 침입을 하거나 공격을 했을 경우 공격자의 IP주소를 파악하거나 공격의 종류를 파악 한때
- 목적지 주소와 포트 : 침입을 하거나 공격을 했을 경우 공격 대상인 시스템을 파악하고 시스템의 취약점을 판단하거나 공격의 종류를 파악할 때.
- 시간 : 사용자가 주로 접속하는 시간, 역추적에서 경로 파악할 때.

```
[**] SCAN nmap TCP [**]
03/27-01 : 57 : 52.780526 172.16.4.80 : 39002 ->
172.16.2.34 : 21
TCP TTL : 58 TOS : 0x0 ID : 28513 IpLen : 20
DgmLen : 60
***A**** Seq : 0x580E33D1 Ack : 0x0 Win :
0x1000 TcpLen : 40
TCP Options (5) => WS : 10 NOP MSS : 265
TS : 1061109567 0 EOL
[**] SCAN nmap TCP [**]
03/27-01 : 57 : 52.780621 172.16.4.80 : 39004 ->
172.16.2.34 : 1
TCP TTL : 58 TOS : 0x0 ID : 19632 IpLen : 20
DgmLen : 60
***A**** Seq : 0x580E33D1 Ack : 0x0 Win :
0x1000 TcpLen : 40
TCP Options (5) => WS : 10 NOP MSS : 265
TS : 1061109567 0 EOL
```

(그림 3) Snort에서 나오는 로그 형태

3.3 Apache 로그

```
61.79.100.140 - - [12/Feb/2004 : 09 : 00 : 00 +0900]
"GET /kr/images/4wd/left_menu/l_sub_08.gif
HTTP/1.1" 304 -
21.120.128.117 - - [12/Feb/2004 : 09 : 00 : 00
+0900] "GET /kr/images/mypage/td_space.gif
HTTP/1.1" 200 67
61.79.100.140 - - [12/Feb/2004 : 09 : 00 : 00 +0900]
"GET /kr/images/4wd/left_menu/l_sub_09.gif
HTTP/1.1" 304 -
```

(그림 4) Apache에서 나오는 로그 형태

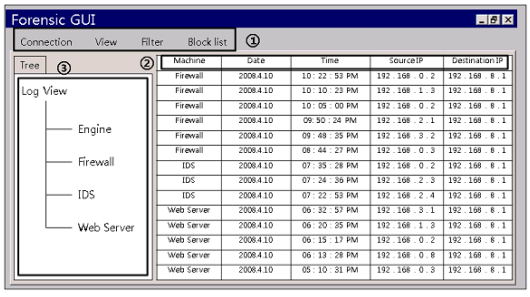
Apache의 로그는 위의 (그림 4)와 같은 형태로 이루어져 있다. 로그를 통해 알 수 있는 정보는 웹서버에 접속한 시간과 출발지 주소와 목적지 주소 그 외에 사용자 ID, 경로 정보, 오류형태 등을 알 수 있다. 여기서 역추적에서 중요하게 쓰일 정보들은 다음과 같다.

- 사용자 ID : IP 이외에 사용자를 파악할 때.
- 출발지 주소 : 침입을 하거나 공격을 했을 경우 공격자의 IP주소를 파악할 때.

- 목적지 주소 : 침입을 하거나 공격을 했을 경우 공격 대상인 시스템을 파악 할 때.
- 오류형태 : 페이지의 오류의 원인을 파악할 때.
- 시간 : 사용자가 주로 접속하는 시간, 역추적에서 경로 파악할 때.

3.4 인터페이스

위에서 파악했던 로그 형태를 바탕으로 로그를 종합 관리하는 인터페이스를 제시한다. 대략적인 인터페이스는 아래 (그림 5)와 같다.



(그림 5) 인터페이스 중 View

① : 메뉴

메뉴에는 Connection과 View, Filter, Block list로 나뉘며 Connection은 관리자나 로그 분석자 이외의 사람에게는 로그를 볼 수 있는 권한을 주지 않기 위한 기능이다. 로그인 전에는 나머지 메뉴들은 비활성화 되어있으며 로그를 볼 수 있는 View나 특정 IP를 검색 할 수 있는 Filter, 침입을 시도 했던 사용자나 주의가 필요한 사용자를 추가할 수 있는 Block list의 기능을 제공한다. 위의 (그림 5)는 시스템들의 로그를 사용자에게 제공하는 기본적인 모습이다.

② : 시스템마다 가시화되는 정보

위의 (그림 4)와 같이 가시화 되는 정보는 Table 형태로 제공된다. 각각의 종목별로 정렬이 가능하며 ③에서 보이는 트리구조를 클릭 할 때마다 제공되는 로그의 정보는 밑의 그림과 같다.

Machine	Date	Time	SourceIP	DestinationIP

(그림 6) 기본적인 로그형태

(그림 6)은 기본적인 로그형태로 각 시스템에서 공통으로 보여주는 로그의 정보들을 보여준다. 시스템을 구분하기 위해 시스템의 종류를 함께 보여주며 이는 침입자나 사용자가 어떠한 경로를 통해 접속하였는지 파악을 돕는다.

Error	Date	Time	SourceIP	Destination IP	URL	Error Content

(그림 7) Web Server 로그 형태

(그림 7)은 ③의 트리구조 중 Web Server 로그에 해당한다. Web Server는 로그 파일이 Access_Log와 Error_Log로 나뉜다. Access_Log는 일반적으로 사용자의 방문기록을 나타내며 방문시간과 방문 경로 등을 알 수 있고 Error_Log는 Web Server의 오작동에 대한 모든 정보를 볼 수 있다. 두 종류의 로그의 내용을 모두 제공해야 하기 때문에 Access_Log에서 알 수 있는 기본적인 정보들과 Error_Log에서 필요한 중요한 정보 Error 여부와 Error Content가 추가하여 사용자에게 두 가지 종류의 로그를 같이 제공한다.

accept	Date	Time	Protocol	SourceIP	S Port	Destination IP	D Port

(그림 8) Firewall 로그 형태

(그림 8)은 ③의 트리구조 중 Firewall에 해당하는 부분으로 패킷이 Filtering 되었는지 여부를 알 수 있는 Firewall의 가장 중요한 부분인 accept와 그밖에 접속시간과 출발지 주소의 정보와 도착지 정보의 주소로 이루어져 있다.

Attack Type	Date	Time	SourceIP	S Port	Destination IP	D Port

(그림 9) IDS 로그 형태

(그림 9)는 ③의 트리구조 중 IDS에 해당하며 사용자의 비정상적인 행위만을 탐지하기 때문에 공격자의 공격행위와 접속시간, 그밖에 공격자의 주소 정보, 공격대상의 주소 정보로 이루어져 있다.

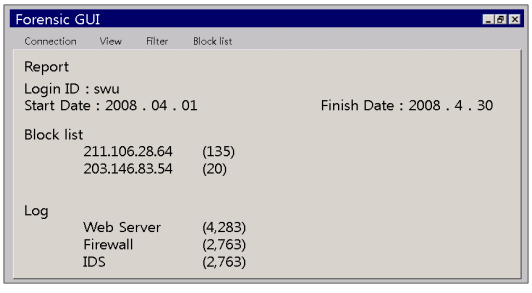
Alert	Date	Time	SourceIP	Destination IP

(그림 10) Engine 로그 형태

(그림 10)은 ③의 트리구조 중 Engine에 해당하는 로그 형태이다. Engine은 정보를 접근할 수 있는 유일한 시스템이며 사용자에게 보내지는 Alert는 Confirm, Warring, Invaded 이렇게 3가지이다. 이중 정보의 침입의 위협을 느끼거나 침입을 당했을 때 발생하는 Warring과 Invaded Alert는 비정상적인 행위를 하는 사용자일 가능성이 높기 때문에 로그의 구분이 필요하며 그 외에 접속시간과 출발지 주소와 도착지 주소의 형태로 이루어져 있다.

③ : Tree 구조

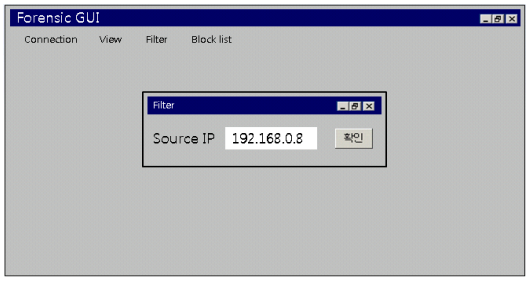
Forensic DB가 가지고 있는 로그들의 출처로 종합적인 로그를 보여줄 뿐 아니라 각 시스템마다 로그를 따로 보여주는 기능을 한다.



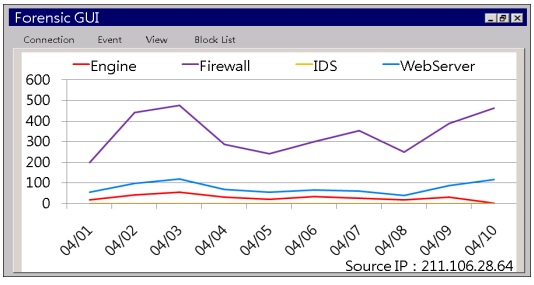
(그림 11) 인터페이스 Report

Connection 후에 보여 지는 Report로 관리자 ID와 Forensic 시스템에 저장된 로그들의 전반적인 내용을 포함한다. Block list는 관리자가 저장한 IP 주소로 주의하고 관찰해야 하는 IP를 저장한 것으로 Block list에 저장된 IP의 접속횟수를 보여준다.

(그림 12), (그림 13)에서 보이는 것과 같이 Log는 각 시스템에 저장된 로그의 개수를 의미한다. View 메뉴의 서브 메뉴로 특정 Source IP에 대한 통계 자료를 그래프로 표현하여 사용자의 접속 패턴이나 공격자일 경우 어느 경로를 통하여 공격하는지 추측할 수 있도록 도와준다.



(그림 12) Source IP Filtering

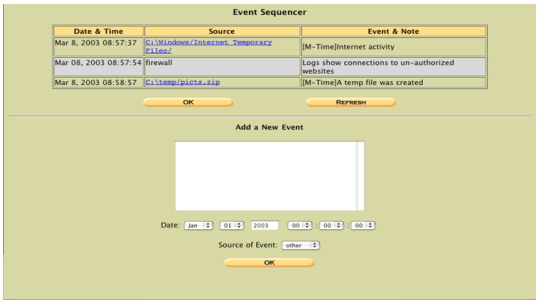


(그림 13) Filtering 된 Source IP Graph

3.5 사용자 인터페이스 비교

본 연구의 내용과 대표적인 오픈 소스 포렌식 인터페이스 환경인 Autopsy와 비교하고자 할 때 가장 대표적인 화면 구성이 (그림 14)라고 할 수 있다. 이 그림에서는 단순히 방화벽 또는 침입탐지시스템의 로그정보를 시간 순서에 맞게 나열하는 것만을 수행한다.

본 연구에서는 이상 현상이 발생한 이후에 로그 전체를 종합해서 볼 수 있는 인터페이스를 제공하기 때문에 Autopsy와 비교할 때 좀 더 현재 시점에서의 관리가 가능한 형태라고 할 수 있다.



(그림 14) Autopsy의 시간순서별 로그 제시 화면

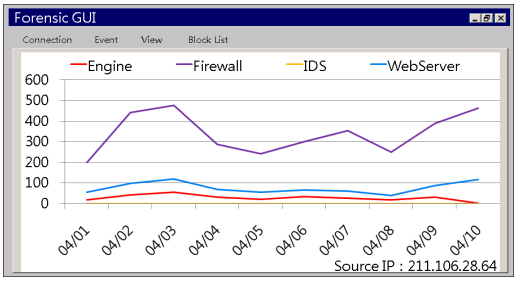
4. 시나리오

지금부터 정상인 접근과 비정상적인 접근의 시나리오를 구분하여 인터페이스의 차이를 살펴보고 비정상적인 접근의 로그를 분석해보도록 하겠다.

4.1 정상 사용자의 시나리오

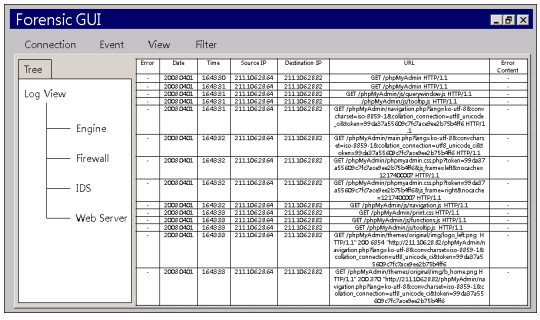
사용자 A는 자신에게 권한이 있는 정보를 접근하기 위하여 Engine B에 접속하기 위하여 Web server에 접속한다. 사용자 A는 자신에게 권한이 있는 정보만 접근할 수 있으며 사용자 A는 정책에 맞게 B에 접속한다.

위의 시나리오와 같이 사용자 A가 정상적인 행위만을 한다면 인터페이스로는 Firewall과 Web server, Engine에서 사용자 A의 로그를 확인 할 수 있다.



(그림 15) 정상 사용자에 대한 Graph

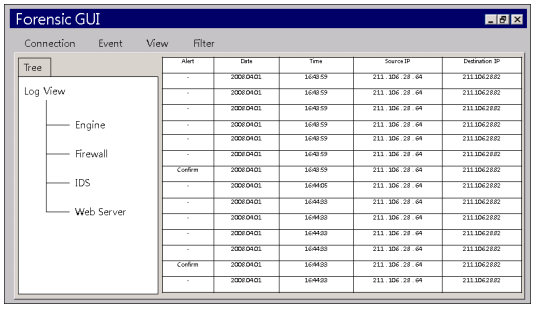
(그림 15)는 사용자 A의 행위들의 로그를 그래프로 표현한 것이다. 공격이나 비정상적인 행위를 탐지하여 로그를 수집하는 IDS는 위의 시나리오대로 정상적인 행위를 하는 사용자의 경우에는 나타나지 않으며 각 로그들의 패턴이 서로 비례하게 나타난다.



(그림 16) 정상 사용자에 대한 Web Server Logs

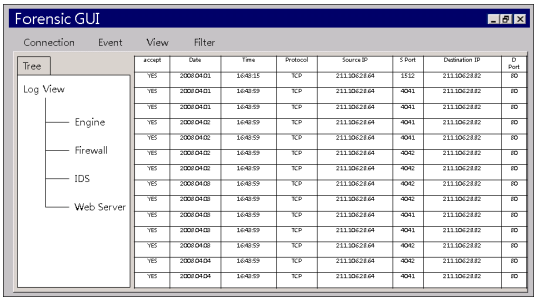
위의 (그림 16)은 정상사용자가 웹서버에서 하는 행위에 대한 로그를 수집하여 보여 준다.

Access_Log에 해당하여 Error여부와 Error Content에 해당하는 로그 정보가 없으며 정상사용자의 Web Server 방문 경로 등을 알 수 있다.



(그림 17) 정상 사용자에 대한 Firewall Logs

(그림 17)에서는 Firewall에서 수집된 A의 로그를 확인 할 수 있다. 인터페이스를 통하여 거의 모든 패킷들이 accept가 되었음을 확인 할 수 있으며, 정상적인 패킷들이라는 것을 확인 할 수 있다.



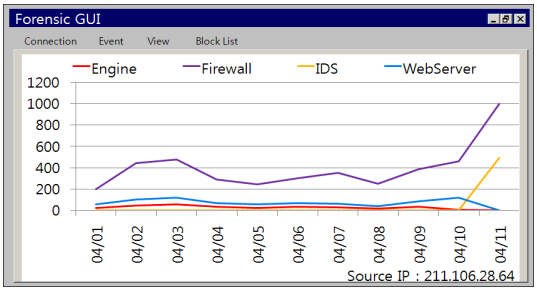
(그림 18) 정상 사용자에 대한 Engine Logs

Engine에서 발생하는 Alert는 3가지인데 Alert 종류(Confirm, Warning, Invaded) 중에서 사용자의 권한에 타당한 행위만을 하는 사용자는 Alert가 Confirm만 발생한다. 인터페이스에서 어떤 Alert가 발생 하였는지에 따라 정상적인 사용자인지 비정상적인 사용자인지 구별할 수 있다.

4.2 비정상 사용자의 시나리오

공격자 A는 Engine B의 서비스를 방해하기 위해 TCP의 취약점을 악용하는 X-MAS SCAN 공격을 1회 시도한다.

위와 같은 공격으로 Firewall과 IDS에 많은 로그가 수집될 뿐 아니라 IDS는 Alert를 발생시킨다.



(그림 19) 비정상 사용자에 대한 Graph

(그림 19)는 사용자 A의 행위들의 로그를 그래프로 표현한 것이다. 각 시스템의 로그의 패턴이 비슷한 성향을 보이다가 4/11에서 로그가 없었던 IDS의 로그가 나타나며 Firewall과 비슷한 로그 개수가 비례하게 나타나고 있다. 일단 IDS가 로그를 수집한 것은 비정상적인 행위를 탐지 한 것이기 때문에 어떠한 공격인지는 알 수 없지만 A가 B에게 공격이 이루어졌음을 확인 할 수 있다.

accept	Date	Time	Protocol	Source IP	S Port	Destination IP	D Port
YES	2008.04.11	16:43:15	TCP	211.106.28.64	1512	211.106.28.82	80
YES	2008.04.11	16:43:16	TCP	211.106.28.82	80	211.106.28.64	1512

(그림 20) 비정상 사용자에 대한 Firewall Logs

2008년 4월 11일 16시 43분경에 사용자A(211.106.28.64)가 Engine B(211.106.28.82)에게 연결 시도가 있었음 알 수 있다.

Attack type	Date	Time	Source IP	S Port	Destination IP	D Port
SCAN XMAS	2008.04.11	16:43:15	211.106.28.64	1512	211.106.28.82	80

(그림 21) 비정상 사용자에 대한 IDS Logs

2008년 4월 11일 16시 43분경에 사용자 A(211.106.28.64)가 Engine B(211.106.28.82)에게 X-MAS SCAN 공격이 이루어 졌음을 알 수 있다.

Scanning이란 시스템에서 제공하는 서비스를 비롯해 각종 정보를 수집하기 위한 행위이며 앞의 시나리오에서 사용한 X-MAS SCAN은 Stealth SCAN에 속한다.

Stealth SCAN은 SYN 패킷만을 검사하는 Firewall이나 IDS의 취약점을 이용하여 원하는 정보를 얻는 방법이다.

Scanning으로 수집되는 정보들은 시스템의 서비스들, 시스템의 기종, 접속 가능한 IP주소, 운영체제 등이며 X-MAS SCAN은 UNIX 호스트에서만 동작하고 OPEN SCAN과 같이 세션이 맺어지지 않기 때문에 공격대상 시스템에 로그가 남지 않는다는 특징이 있다.

이러한 Scanning은 해킹을 하기 전 해커가 공격대상에 대한 사전 정보를 얻기 위해 수행하는 과

정(1단계 : Foot Printing 2단계 : Scanning 3단계 : Enumeration)중 2단계에 속한다.

즉, X-MAS SCAN은 공격대상을 침해하는 행위는 아니지만 시스템에 해킹을 하기 전 행위로 볼 수 있기 때문에 이러한 행위는 앞으로 시스템에 저장된 개인정보들이 침해되고 유출 될 수 있는 행위를 유추 할 수 있다.

5. 결 론

포렌식 분야는 디지털 수사에서 필수적인 요소이며 그 중 네트워크 포렌식은 시스템에 침입의 흔적을 수집하고 유지하기 때문에 각 시스템이 갖는 취약점을 파악 할 수 있으며, 침해 당시를 유추할 수 있다. 모든 네트워크 장비들과 시스템에서 침입흔적이 남기 때문에 디지털 수사에서 중요한 역할을 한다 할 수 있다.

본 논문에서는 디지털 수사에서 쓰이는 네트워크 포렌식 위해 수집된 로그들의 특징을 파악하고 역추적에 필요한 정보들을 추출하여 제공하는 종합 로그 인터페이스를 제시해 보았다.

이후에는 앞에서 제시한 인터페이스를 구현하기 위해서 먼저 각 시스템의 수집된 로그만으로도 사용자행위를 재구성 할 수 있는 네트워크 구성에 대한 연구가 진행 될 것이다. 또한 다양한 공격 시나리오를 제시하여 공격 전 후에 대한 각 행위의 연관관계를 파악하고 수집 될 수 있는 로그에 행위의 연관관계를 적용할 수 있을지에 대한 연구도 수행할 것이다. 실제 자신의 정보를 변경해서 공격하는 여러 행위들에 대한 전 후 로그에 위에서 파악한 패턴을 적용하여 여러 사용자들의 로그 중에 실제 사용자를 유추할 수 있는지에 대한 실험과 함께 각 행위에 대한 연관관계가 로그에 적용 시킬 수 있다면 인터페이스에서 이를 가시화 할 수 있도록 지속적인 연구를 수행할 것이다.

참 고 문 헌

[1] 정익래, 홍도원, 정교일, “디지털 포렌식 기술 및 동향”, 한국전자통신연구원, 2007.

[2] 김혁준, 이상진, “분석 사례를 통해 본 네트워크 포렌식의 동향과 기술”, 정보보호학회지, 2008.

[3] 박종성, 문종섭, 최운호, “자동화된 침해사고 대응시스템에서의 네트웍 포렌식 정보에 대한 연구”, 한국정보과학회 2004년도 봄 학술발표논문집, 2004.

[4] 고병수, 박영신, 최용락, “컴퓨터 포렌식스를 지원하는 보안 감사/추적 모듈 설계”, 한국컴퓨터정보학회, 2004.

[5] 전용희, 장종수, “비정상 트래픽 공격 유형 분석”, 정보보호학회지, 2007.

[6] 강민석, 윤가영, 최광희, 정의훈, “실시간 해킹 패턴을 이용한 침입 탐지 시스템의 구현”, 한국인터넷 정보학회 2005 정기총회 및 추계학술발표대회, 2005.

[7] 정우식, “IDS/Firewall/Router 통합 로그 분석기 설계”, 한국컴퓨터정보학회, 2003.

[8] 정강용, 박나연, “웹 서버의 로그파일 분석에 의한 웹 서비스 활용에 관한 연구”, 한국컴퓨터정보학회, 2000.

[9] The Sleuth Toolkit “http://www.sleuthkit.org”.

[10] Ricardo Kleber Martins Galvao, “Computer Forensics with The Sleuth Kit and The Autopsy Forensic Browser”, International Journal of Forensic Computer Science, Vol. 1, No. 1, pp. 41-44, 2006.

[11] CARRIER, Brian. File Activity Timelines. Available online on September/2006 at URL http://www.sleuthkit.org/sleuthkit/docs/ref_timeline.html.

[12] CARRIER, Brian. The FAT File System - Sleuth Kit Implementation Notes (SKINs). Available online on September/2006 at URL

http://www.sleuthkit.org/sleuthkit/docs/skins_fat.html.

[13] CARRIER, Brian. The NTFS File System - Sleuth Kit Implementation Notes (SKINs). Available online on September/2006 at URL http://www.sleuthkit.org/sleuthkit/docs/skins_ntfs.html.

[14] CARRIER, Brian. The Sleuth Kit Informer - Issue #13 - UNIX Incident Verification with Autopsy. Available online on September/2006 at URL http://www.sleuthkit.org/informer/sleuthkit-informer-13.txt.

심 희 연

2005년～서울여자대학교
컴퓨터학부 재학

김 형 종

1996년 성균관대학교
정보공학과(공학사)
1998년 성균관대학교 대학원
정보공학과(공학석사)
2001년 성균관대학교 대학원
전기전자및컴퓨터학과
(공학박사)
2001년～2007년 한국정보보호진흥원 수석연구원
2004년～2006년 미국 카네기멜론대학 Visiting Researcher
2007년～현재 서울여자대학교 컴퓨터학부 전임강사