자동화된 침해사고대응시스템에서의 네트웍 포렌식 정보에 대한 연구

박종성[0], 문종섭*, 최운호**

*고려대학교 정보보호기술연구센터, **금융결제원 금융ISAC실 정보보호기술팀장*
p19i78s@korea.ac.kr, ismoon@korea.ac.kr, tiger@kftc.or.kr

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

JongSeong Park[0], Jong-sub Moon, UnHo Choi

요 약

포렌식에 관한 연구는 현재까지 시스템에 남은 흔적을 수집하고 가공, 보관하는 시스템 포렌식에 치우쳐 있었다. 최근들어 단순히 시스템에 남은 흔적만을 분석하는 것이 아닌 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 포렌식을 위해 수집되어야 할 정보들을 정의한다. 자동화된 침해사고대응시스템의 여러 장비들과 정보들 중 컴퓨터 범죄 발생시 증거(Evidence)가 되는 포렌식로 수집되어야 할 항목들을 제시하고 필요성에 대해 언급할 것이다.

1. 서 론

최근 악의적인 해킹이나 산업 스파이에 의한 정보유출 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.

하지만 사이버 경찰이 전체 인터넷 망에서 일어나는 컴퓨터 범죄를 다룰 수 없고 인터넷 내에서의 정보의 중요성이 커짐에 따라 자체적인 자동화된 침해사고대응시스템의 구축을 통한 컴퓨터 범죄 예방 및 사후 대처가 준비되고 있는 실정이다. 이러한 자동화된 침해사고대응시스템에서는 사후 대처를 위해 포렌식 기술을 이용한 정보 수집, 분석, 보관에 대한 연구를 진행하고 있다. 자동화된 침해사고대응시스템에서는 전체 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.

본 논문에서는 네트웍 포렌식의 의미와 관련 연구 동향을 살펴 본 후, 자동화된 침해사고대응시스템에서 수집되어야 하는 네트웍 포렌식 정보를 정의한다. 본 논문의 구성은 다음과 같다. 2장에서는 네트웍 포렌식의 개요와 연구동향에 대해 살펴보고 3장에서는 네트웍 포렌식을 위한 수집되어야 할 정보들을 정의한다.

2. 네트웍 포렌식의 의미 및 범위

2.1 네트웍 포렌식

네트웍 포렌식은 컴퓨터 범죄 발생 시, 범죄자를 찾아내고 보안 사고의 원인을 찾기 위해 네트웍 이벤트(Event)을 수집하고 기록하고 분석하는 일련의 과정이다.

네트웍 포렌식은 일반적으로 두 가지 형태로 분류된다.

· "Catch-it-as-you-can" systems

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

기존의 네트웍 포렌식에 대한 이러한 분류는 중형 전산망 초점이 맞추어져 있고 여러 가지 정보보호장비를 갖추고 있는 자동화된 침해사고대응시스템에서는 의미가 없다.

자동화된 침해사고대응시스템에서의 네트웍 포렌식은 여러 정보보호장비 혹은 네트웍 장비 및 취약점 정보들을 수집하여 저장하고 연관성을 분석하는 절차이고 가공된 포렌식 정보를 실제 수사 과정이나 법적인 증거자료로서 사용하는 경우가 자주 발생는 특화된 시스템이기 때문이다.

2.2 네트웍 포렌식 정보의 범위(SCOPE)

본 논문에서는 네트웍 포렌식 정보를 네트웍을 유지하기 위한 네트웍 장비(Router, Switch 등)와 침입자로부터 네트웍을 감시 및 보호하는 정보보호장비(Firewall, Monitering Server, IDS, VPN, 취약점 서버 등)에 의해 획득된 정보로 정의한다. 서버 시스템 자체의 로그정보 및 상태정보 혹은 시스템에서 동작하고 있는 모니터링 정보나 보안 로그 정보는 제외된다. 즉, 순수히 네트웍 장비나 정보보호장비로서의 역할을 수행하는 시스템의 정보를 네트웍 포렌식 정보로 정의한다.

2.3 네트웍 포렌식 정보의 연구 동향

기존의 네트웍 포렌식에 대한 연구는 중·소 규모 네트웍에서의 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. 하지만 아직까지 중·소 규모 네트웍에서의 네트웍 포렌식 정보에 대한 정의 조차도 명확한 연구가 이루어지지 못했다. 이는 중·소 규모 네트웍에서의 네트웍 포렌식 정보는 특별한 정의가 필요없는 즉각적으로 알 수 있는 정보로 여겨져왔기 때문에 단지 이를 안전하게 수집하는데만 관심이 모아졌고 네트웍 포렌식 정보보다는 더 상세한 정보를 지니는 시스템 포렌식 정보의 정의와 획득이 관심이 모아져왔기 때문이다.

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

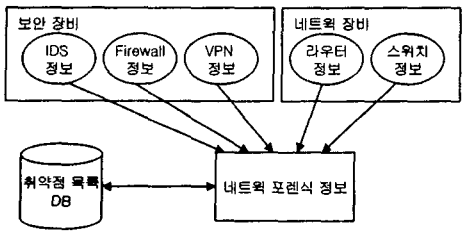

그림 (1) 네트워 포렌식 정보

3. 자동화된 침해사고대응시스템을 위한 네트워 포렌식 정보

본 논문에서는 현재까지 포렌식 정보의 주류를 이루었던 시스템 포렌식 정보가 아닌 시스템 포렌식 정보에 기본적인 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(1)는 자동화된 침해사고대응시스템에서 수집될 네트워 포렌식 정보의 전체 그림을 보이고 있다.

본 절에서는 먼저 네트워 장비에서 수집되어야 할 포렌식 정보를 언급하고 그 후 정보보호장비에서 수집되어야 할 포렌식 정보를 다룬다.

3.1 네트워 장비 - 라우터(Router)

라우터는 인터넷이라는 거대한 네트워 망을 유지해주는 뼈대 역할을 한다. 인터넷 망을 통해 주고받는 모든 정보는 라우터를 거쳐서 상대방에서 전송되고 응답 또한 라우터를 거쳐 수신된다.

포렌식 관점에서 중요한 정보라 할 수 있는 컴퓨터 범죄와 관련된 정보들도 라우터를 거치게 된다. 또한 라우터는 내부망(intranet)과 외부망(Extranet)의 중계점(chock-point) 역할을 하며 내부 정보보호장비들과의 최초 연결 지점이기도 하다.

라우터에서 보장되어야 하는 네트워 포렌식 정보는 다음과 같다.

- 라우터의 상태 정보와 설정 정보
- 라우팅 프로토콜과 라우팅 테이블 정보
- 라우터의 ARP Cache 정보
- 라우터의 local 로그 정보와 네트워 트래픽 로그 정보

라우터의 상태 정보와 설정 정보는 라우터의 설정 정보와 사건 발생시의 시각, 버전(VERSION)정보를 포함하고 컴퓨터 범죄(Digital Crime)가 일어났던 때의 당시 상황 재현을 위해 중요한 정보이다. 라우팅 프로토콜과 라우팅 테이블 정보는 공격자의 정보보호장비 우회 가능성을 확인할 수 있는 정보이다. 그림[2]는 CISCO 라우터의 라우팅 프로토콜과 라우팅 테이블 정보를 보이고 있다. 또한 라우터의 ARP Cache 정보는 라우터에서 정보를 송신할 때 생기는 근접 호스트의 MAC address 정보 이므로 ARP Spoofing 이나 redirection 공격에 의해 변조되지 않았는지 확인해야 한다. 마지막은 라우터에 남는 로그 정보로 크게 두 가지로 분류 할 수 있다. 그 첫 번째는 라우터 자체의 설정오류나 장치 상의 문제를 기록하고 ACL(Access Control List)에 의해 접속이 거부된 패킷(Packet) 정보를 기록하는 local 로그이고 두 번째는 라우터를 경유하는 네트워 트래픽 중 라우터와 연동되는 NetFlow에 의해 기록되는 패킷 모니터링 정보이다.

3.2 네트워 장비 - 스위치(switch)

스위치(switch)는 내부망에서 호스트들 간의 네트워을 형성하는 중계기의 역할을 한다. 스위치는 단순히 신호를 전달해주는 역할을 하는 허브와는 달리 전송될 메시지를 MAC address 와 일치하는 port 로 전달해주는 데이터링크(Data Link)계층 장비이다.

스위치에서 보장되어야 하는 네트워 포렌식 정보는 다음과 같다.

- 스위치 상태 정보 및 설정 정보
- MAC table

```
Router#show ip route

Gateway of last resort is 192.168.1.33 to network 0.0.0.0

211.106.165.0 255.255.255.192 is subnetted, 1 subnets
C211.106.165.64 is directly connected, Ethernet0
192.168.1.0255.255.255.252 is subnetted, 1 subnets
C192.168.1.32 is directly connected, Serial1
S*0.0.0.0 0.0.0.0 [1/0] via 192.168.1.33
```

그림 (2) 라우팅 프로토콜과 라우팅 테이블 정보(CISCO 장비)

- VLAN(virtual LAN)

스위치의 상태 정보 및 설정 정보에는 스위치의 시간 정보와 버전 정보, 패스워드 등록 유무, IP address, SNMP 서비스 등의 제공 서비스 목록이 포함된다. 그리고 MAC table 에는 switch 의 각 port에 물려있는 호스트(host)들의 MAC address와 port 의 정보를 유지하고 있다. MAC address 변조는 공격은 스위치의 취약점을 이용하는 공격자의 대표적인 방법이다. 마지막으로 VLAN (virtual LAN)은 하드웨어적이 아닌 소프트웨어적으로 스위치 포트의 전달(Broadcast) 영역을 나누는 정보이다. 총 36개의 port를 12개 씩 3 소그룹(sub-group)으로 나눈다면 해당 소그룹에 속한 호스트 간에만 스위치를 통한 데이터 교환이 가능하다. VLAN은 컴퓨터 범죄 수사 시 공격자를 유추할 수 있는 범위를 줄여줄 수 있다.

3.3 정보보호장비 - 방화벽(Firewall)

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

방화벽에서 보장되어야 하는 네트워 포렌식 정보는 다음과 같다.

- 방화벽의 상태 정보 및 설정 정보
- 방화벽의 로그

방화벽의 상태 정보와 설정 정보에는 방화벽의 시간 정보와 버전(version)정보가 포함된다. 방화벽의 로그 정보는 자체의 하드웨어적인 오류 혹은 설정 상의 오류 외에 접속이 거부된 패킷의 로그 기록을 남긴다. 그림(3)은 대표적 방화벽인 CHECK POINT 사의 방화벽 로그 기록이다.

3.4 정보보호장비 - 가상사설망(VPN)

가상사설망(VPN)은 VPN 게이트웨이(gateway) 혹은 게이트웨이(gateway) 대 원격 사용자(remote user) 간의 안전한 데이터 교환을 위해 패킷을 캡슐화 하여 보내는 기술이다.

자동화된 침해사고대응시스템에서는 공유 정보의 안전한 통신을 위해 가

```
19-May-00 17:31:59 drop inbound udp scan.wins.bad.guy
MY.NET.29.8 netbios-ns netbios-ns 78
19-May-00 17:32:09 drop inbound udp scan.wins.bad.guy
MY.NET.29.9 netbios-ns netbios-ns 78
19-May-00 17:32:20 drop inbound udp scan.wins.bad.guy
MY.NET.29.10 netbios-ns netbios-ns 78
----- snipped -----
19-May-00 18:15:18 drop inbound udp scan.wins.bad.guy
MY.NET.29.252 netbios-ns netbios-ns 78
19-May-00 18:15:29 drop inbound udp scan.wins.bad.guy
MY.NET.29.253 netbios-ns netbios-ns 78
19-May-00 18:15:39 drop inbound udp scan.wins.bad.guy
MY.NET.29.254 netbios-ns netbios-ns 78rt to
```

그림 (3) 방화벽 로그(CHECK POINT FIREWALL-1)

```
[**] NMAP TCP ping [**]
03/21-13:33:51. 880120 209.67.78.202:1029 -> 211.49.132.23:80
TCP TTL:46 TOS:0X0 ID:19678
******A* Seq: 0xE4F00003 Ack: 0x0 Win: 0xC00

[**] Large ICMP payload [**]
03/21-14:30:40. 110169 209.67.78.202 -> 211.49.132.23
ICMP TTL:255 TOS:0X0 ID:5487 DF
ID:7564 Seq:0 ECHO
```

그림 [4] SNORT 의 Alert 이벤트 정보

상사설망(VPN)을 사용한다. 가상사설망은 안전한 통신을 위해 통신 양단간에 암호화 터널을 생성하고 이 터널을 통해 메시지를 주고 받는다.

가상사설망(VPN)에서 보장되어야 하는 네트워 포렌식 정보는 다음과 같다.

- VPN 의 상태(Status) 정보
- 가상사설망의 보안 협상(SA) 정보
- 가상사설망의 정책(Policy) 정보
- 가상사설망의 로그(log) 정보

가상사설망의 보안 협상(SA)은 정보를 공유하는 상대방과 약속된 인자(parameter) 값들을 지닌다. SA에 올라있는 정보 공유자들은 일단 인가된 이들이다. 하지만 이들은 내부로의 접근이 자유로의 허락되므로 컴퓨터 범죄 발생시 SA 에 등록된 정보 공유자들의 정보는 수집되어야 한다. 가상사설망의 정책(Policy) 정보는 컴퓨터 범죄 발생 시점의 내부 접근 호스트들에 대한 정보를 제공하므로 수사 시 참고할 수 있다. 가상사설망의 로그(log) 정보는 중요 작업(activity)가 발생하거나 SA 형성 시 혹은 Policy 적용 시 그리고 캡슐화 혹은 de-캡슐화 과정 중에 오류가 발생할 경우 기록된다.

3.5 정보보호장비 - 침입탐지시스템(IDS)

침입탐지시스템(IDS)는 공격자의 침입을 탐지하여 관리자에게 알려주거나 관련 로그를 기록하는 시스템이다. 침입탐지시스템은 송·수신되는 패킷을 모니터링하는 수집부와 해당 패킷이 침입인지 판단하는 판단부 해당 침입에 대해서 관리자에게 경고를 주거나 로그를 기록하는 대응부로 이루어진다. 침입에 대한 탐지를 네트워 전체를 대상으로 하느냐 아니면 호스트를 대상으로 하느냐에 따라 네트워 침입탐지시스템(NIDS)와 호스트 침입탐지시스템(HIDS)로 분류할 수 있고 탐지 기법에 따라 signature를 이용하는 오용 탐지(Misuse Detection)과 비정상 탐지(Anomaly Detection)으로 분류된다.

자동화된 침해사고대응시스템에서는 네트워 전체의 침해 상황을 파악하고 대처하기 위해 네트워 침입탐지시스템의 사용이 용이하다.

침입탐지시스템(IDS)에서 보장되어야 하는 네트워 포렌식 정보는 다음과 같다.

- 침입탐지시스템(IDS)의 상태 정보
- 침입탐지시스템(IDS)의 정책 정보
- 침입탐지시스템의 이벤트 로그와 로그 정보

침입탐지시스템의 상태정보는 시간 정보와 버전(version)정보를 포함한다. 침입탐지시스템의 정책정보는 오용 탐지 기법의 시스템일 경우, signature 를을 말하고, 비정상 탐지 기법의 시스템일 경우, 정상에 대한 기준을 말한다. 침입탐지시스템은 공격의 탐지와 함께 이를 관리자에게 알리기 위한 이벤트 로그와 정확히 공격으로 판단되지는 않지만 네트워 상황 판단을 위해 유용한 정보이거나 이 후의 필요성을 위해 기록해 두는 로그 정보를 가진다. 그림 [4]는 SNORT에서 기록된 로그정보를 보이고 있다.

3.6. 정보보호장비 - 취약점 스캐너

취약점 스캐너는 네트워 전체의 취약점과 각 호스트 시스템들의 취약점을 분석하는 도구이다. 포트 탐지(Port Scanning) 이나 해당 서비스 접속시

```
Nessus Scan Report----------------SUMMARY
- Number of hosts which were alive during the test : 9
- Number of security holes found : 54
- Number of security warnings found : 113
- Number of security notes found : 303

TESTED HOSTS
10.163.155.2 (Security holes found)
10.163.156.1 (Security holes found)

+ 10.163.155.2 :
. List of open ports :
  o ftp (21/tcp) (Security notes found)
  o http (80/tcp) (Security warnings found)
  o snmp (161/udp) (Security hole found)
  o general/tcp (Security warnings found)
```

그림 [5] NESSUS의 취약점 분석 결과

의 응답정보를 분석하여 취약점을 판단한다. 이러한 취약점 스캐너는 취약점 탐지 지점에 따라 네트워 취약점 탐지시스템과 시스템 취약점 시스템으로 나뉜다.

사실 취약점 스캐너는 엄밀히 따져 정보보호장비에 속하지는 않는다. 하지만 자동화된 침해사고대응시스템에서 다른 정보보호장비들 만큼이나 포렌식 정보로서 중요하다. 그림 [5]는 대표적 네트워 취약점 분석 도구인 NESSUS의 취약점 분석 결과를 보인다.

4. 결론

자동화된 침해사고대응시스템에서 포렌식은 잦은 보안 사고의 사후 대처를 위해 필수적인 기술이고 특히나 네트워 포렌식 기술은 전체 네트워의 침해 정보를 유지하고 시스템 내의 침해 흔적에 추가적인 정보와 정보의 신뢰성을 제공해 준다. Off-line 의 범죄 수사와 마찬가지로 On-line 의 범죄수사에서도 침입자의 모든 흔적은 이후의 침해 유추나 증거자료로서 쓰일 수 있기 때문에 각 정보보호장비와 네트워 장비 내에 남은 침입자의 흔적을 수집하고 분석, 기록하는 네트워 포렌식이 중요하다 하겠다.

본 논문에서는 자동화된 침해사고대응시스템에서 수집되어야 할 네트워 포렌식 정보에 대해 정의해 보았다. 이후에는 수집된 네트워 포렌식 정보의 분석을 통해 정보들의 연관성을 파악하고 응용방안에 대해 고민해 보아야 할 것이다.

참 고 문 헌

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

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

[3] 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.

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