Virtual Honeynet을 이용한 신종공격 탐지 사례

김천석* · 강대권* · 엄익채**

The Case of Novel Attack Detection using Virtual Honeynet

Chun-Suk Kim* · Dae-Kwon Kang* · Ieck-Chae Euom**

요 약

전력, 수력, 원자력, 석유 등 국가에서 관리하는 중요핵심기반시설들은 대부분 SCADA(Supervisiory Control And Data Acquisition)시스템의 폐쇄망 형태로 운영되고 있다. 이러한 시스템들은 개방형 프로토콜 및 상용 운영체제 사용 등으로 인해 점차 IT에 대한 의존성이 증가되는 추세이다. 이러한 주요 시설들이 사이버 테러 및 해킹, 바이러스 등에 의해 원격 조작 및 통제되는 경우 심각한 위험에 빠질 수 있다.

본 논문에서는 주요기반시설 시스템에 대한 위협 및 취약성을 최소화하는 방법을 제시하고, 공격패턴이 알려지지 않은 Zero-Day Attack을 탐지하는 Virtual Honeynet의 시스템 구성과 공격 탐지 알고리즘, 탐지 사례 등에 대해 알아보고자 한다.

ABSTRACT

Most national critical key infrastructure, such like electricity, nuclear power plant, and petroleum is run on SCADA (Supervisory Control And Data Acquisition) system as the closed network type. These systems have treated the open protocols like TCP/IP, and the commercial operating system, which due to gradually increasing dependence on IT(Information Technology) is a trend. Recently, concerns have been raised about the possibility of these facilities being attacked by cyber terrorists, hacking, or viruses.

In this paper, the method to minimize threats and vulnerabilities is proposed, with the virtual honeynet system architecture and the attack detection algorithm, which can detect the unknown attack patterns of Zero-Day Attack are reviewed.

키워드

Virtual Honeynet, Honeypot, High-Interaction Honeypots
보안 메커니즘, 공격탐지 기술

Ⅰ. 서 론

최근 정보통신기술의 발전으로 인해 국가주요핵심기반시설(Critical Infrastructure)의 제어시스템이 개방형 프로토콜 적용 및 외부 시스템과의 연계 등이 이루어지고 있다. 이러한 점은 사이버 침해 및 공격에 따른 위협으로부터 안전하지 못한 점을 나타내고 있다[1]. 특히 기존의 보안 기술은 알려진 공격(well-known attack)만 탐지하기 때문에 신종 공격이 국가주요핵심기반시설을 공격하면 막대한 피해가 예상된다. 실례로 2007년 미국 Idaho National Laboratory는 미국 국토보안국의 SCADA 소프트웨어의 취약점

* 전남대학교 전자통신공학과(kim1000s@chonnam.ac.kr)
* 전남대학교 전자통신공학과(kang7233@kdn.com)
** 한전KDN 정보보호사업팀(ice@kdn.com)
접수일자 : 2012. 01. 06 심사(수정)일자 : 2012. 03. 15 게재확정일자 : 2012. 04. 07

을 이용하여 Power Grid 장비를 해킹할 수 있음을 시연하였으며, IOActive사의 보안전문가는 Smart Grid의 스마트 미터를 해킹하여 네트워크상의 스마트 미터에 Worm Virus가 신속하게 전파될 수 있음을 검증하였다[2]. 표 1은 기존 보안기술의 한계를 나타내고 있다. 이러한 기존 보안기술의 한계를 극복하기 위해 새로운 개념의 공격탐지기법이 연구되고 있으며 대표적으로 Sandbox, NBA(Network Behaviour Analysis), Honeynet, One way F/W(Firewall), CCM (Configuration & Change Management) 등의 기술들이 있으며 간략히 설명하면 다음과 같다. SandBox기술은 기존 AntiVirus는 알려진 시그니처(Signature) 즉 바이러스 패턴 문자열 매칭기반으로 공격을 탐지하는데 비해, Sandbox기술은 악성코드의 행위분석을 통하여 악성유무를 판단한다. NBA(Network Behaviour Analysis)는 네트워크 트래픽의 학습된 기준선(baseline) 대비 특정편차(deviation)기반 이상의 트래픽에 대한 악성유무를 판단한다. One Way F/W (Firewall)은 논리적인 접근제어기술로서, 물리적인 단방향 통신 보장 접근제어기술이다. CCM은 FIle또는 Configuration의 변경에 의한 무결성 여부를 판단하는 탐지 기술이다. Honeynet은 공격자의 기법, 의도, 도구, 방법 등을 알아내는 도구이다[3].

표 1. 기존 보안 기술의 한계
Table 1. Limitations of existing security technologies

위협	대응 기술	한계	알려지지 않은 공격
취약점 발생	패치관리시스템(PMS)	▪ 단말 PC에 대한 보안패치 ▪ 패치제작 : 7 ~ 30시간 소요	▪ Zero-Day Attack ▪ Known Attack 변종 ▪ 목표(Targeted) 공격 ▪ 신종 Worm 공격 ▪ 미래 위협(Warhol, Flash Threat)
바이러스, 스팸	안티바이러스, 안티스팸	▪ 알려진 공격만 탐지 ▪ 시그니처 제작 : 7 ~ 30시간 소요	
외부해커	방화벽(F/W)	▪ 정책기반의 차단만 가능	
알려진 공격	침입탐지시스템(IDS)	▪ 알려진 공격의 탐지 또는 방지 ▪ 시그니처 제작 : 7 ~ 30시간 소요	
	침입방지시스템(IPS)		
	웹방화벽		
	ESM	▪ 보안이벤트에 대한 모니터링	
	TMS	▪ 보안이벤트에 대한 모니터링 ▪ 네트워크 트래픽(PPS, BPS)에 모니터링	

본 논문에서는 IPS(Intrusion Prevention System)의 공격패턴에 없는 신종공격자(공격코드)의 기법을 분석하며, ESM(Enterprise Security Management)의 대량 보안이벤트에서 Focusing할 데이터를 선별 분석할 수 있는 Virtual Honeynet의 시스템 구성 및 탐지 알고리즘, 탐지 사례에 대하여 알아보고자 한다.

II. Virtual Honeynet시스템 구성 및 탐지알고리즘

2.1 Virtual Honeynet 시스템 구성

Honeypot이란 네트워크 침해를 유도하고 이를 상세히 분석하여 공격자의 공격의도, 기법, 도구 등을 분석하여 신종 공격기법에 대한 분석 및 대응을 통하여 보안을 강화하기 위한 도구로 정의 할 수 있다. 또한 여러 Honeypot으로 구성된 Honeypot의 네트워크를 Honeynet이라고 한다. 본 논문에서는 가상화 기반의 유지관리 편의성이 향상되고 공격행위의 자동 분석 및 포렌직분석 연계 등이 지원되는 Virtual Honeynet시스템의 구성에 대해 논하고자 한다[4][5].

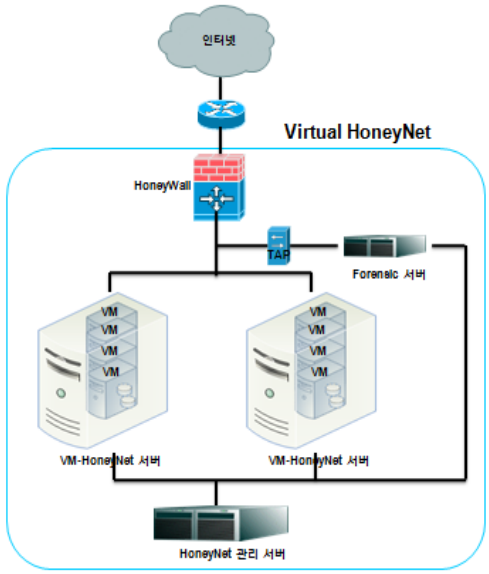

그림 1. Virtual Honeynet 시스템 구성도
Fig. 1 Configuration of Virtual Honeynet System

Virtual Honeynet은 그림 1과 같이 Honeywall, VM-Honeynet서버, Honeynet관리시스템, 포렌직시스템으로 구성이 되며 세부 기능은 아래와 같다.

2.1.1 HoneyWall

Honeywall은 인터넷망에서 연결되는 외부의 통신을 내부의 가상 Honeypot시스템으로 연결하며, 혹시 발생될 수 있는 내부 Honeypot의 외부에 대한 공격을 그림 2와 같이 사전에 차단하여 내부공격을 방어하도록 한다. 이를 위하여 기존의 보안기술인 방화벽과 침입탐지 기능을 수행한다.

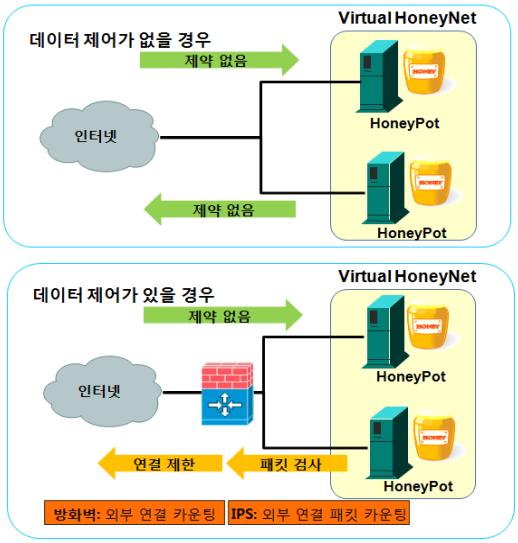

그림 2. Honeywall 기능
Fig. 2 The role of honeywall

2.1.2 VM-Honeynet서버

VM-Honeynet서버는 Honeynet내부에 다양한 종류의 OS 및 버전과 어플리케이션이 존재하여야 풍부한 공격자 정보를 수집할 수 있다. 따라서 VM-Honeynet서버에는 이러한 설치 및 관리를 효율적으로 하기 위한 Agent가 존재하며 이러한 Agent들은 외부 공격자의 침투나 공격 정보를 수집하여 Honeynet관리서버로 전송하는 역할도 수행한다. 이때 VM-Honeynet서버 자체는 완벽하게 보호되어 있어야 하며, 실제 공격받거나 감염되는 주체는 내부의 가상머신(Virtual machine)으로 국한된다. 이를 위해 그림 3과 같은 VM-Honeynet서버는 보안이 강화된 운영체제를 사용한다[4][5].

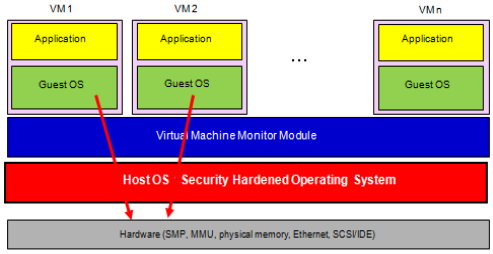

그림 3. VM-Honeynet서버 구성도
Fig. 3 Configuration of VM-Honeynet server

2.1.3 Honeynet관리시스템

Honeynet관리시스템은 그림 4와 같이 Virtual Machine들을 중앙관리하며 가상머신의 에이전트 관리 및 상관분석을 통한 봇(Bot)감염 행위 분석 및 모델링을 한다. 또한 포렌직 서버와의 상관분석(Correlation)을 통한 의심 행위 상세분석을 한다.

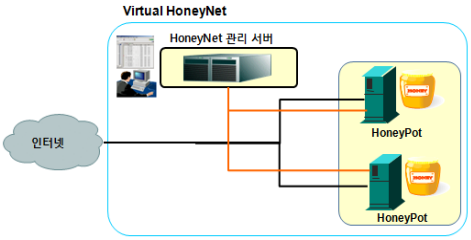

그림 4. Honeynet관리시스템
Fig. 4 Honeynet management system

2.1.4. 포렌직 시스템

Honeynet 네트워크상의 데이터 캡춰는 네트워크 포렌직(Forensic)서버에 의해 수행된다. Honeynet으로 유입 또는 유출되는 모든 네트워크 통신 내용을 캡춰하기 위해서 외부와 통신하는 Honeynet의 최전방 HoneyWall의 인입선에 네트워크TAP장비와 함께 설치되어 Honeynet과 외부의 모든 통신 패킷 내용을 캡춰하여 해당 내용을 분석할 수 있는 기능을 제공한다.

2.2 Virtual Honeynet 공격 탐지 알고리즘

VM-Honeynet에서는 Honeywall에서의 통신요약데이터, IDS이벤트 그리고 Guest OS 및 어플리케이션 침해정보, 네트워크 기반의 OS정보가 발생한다. 이러한 다양한 정보들을 자동으로 인식하여 Fusion하고

이들 간의 연관성을 분석함으로써, 보다 효율적으로 VM-Honeynet데이터를 분석할 수 있으며 보다 포괄적인 침입분석이 가능하다. 그림 5와 같이 시스템 로그와 IDS정보들을 Honeynet Datastore에서 상관분석 처리한다. 봇 탐지를 위하여 상관분석이 사용되며 시스템 감염행위 및 분석을 위한 모델링을 사용하고 있다. 공격 패턴은 [외부 IP : 내부 IP : 내부 포트 : 패킷 길이]로 표현을 한다. 예들 들어 1-1-m-1패턴은 외부 고정IP, 내부 고정IP에 가변 내부포트 및 고정길이의 패턴을 의미하며 포트 스캔의 의미를 가진다. 그림 6은 포트 스캔 공격을 시각화 한 것이다. 표 2는 공격패턴의 종류이다[3].

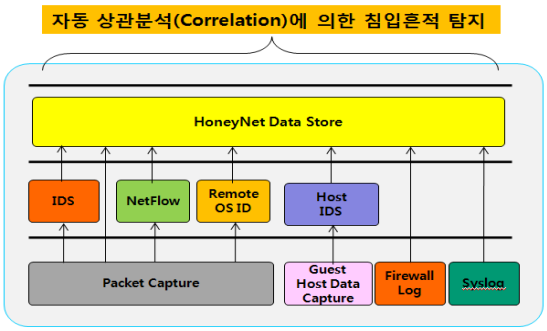

그림 5. 자동 상관분석에 의한 공격 탐지
Fig. 5 Attack detection using correlation

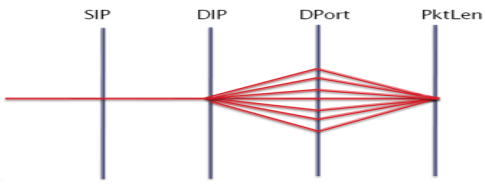

그림 6. 공격형태(port scan)
Fig. 6 Attack type (port scan)

표 2. 공격 패턴의 종류
Table 2. Categories of attack type

패턴 종류	설 명
1-1-m-1	내부 포트만 변경됨
1-m-1-1	내부 IP만 변경됨
1-m-1-0	내부 IP만 변경되는데 패킷 길이가 48byte 미만
m-1-1-1	외부 IP만 변경됨
m-m-1-1	외부 IP와 내부 IP가 변경됨
m-1-m-1	외부 IP와 내부 포트가 변경됨
1-m-m-1	내부 IP와 내부 포트가 변경됨
m-m-m-1	외부 IP와 내부 IP, 내부 포트 모두 변경됨
1-1-1-1	모두 고정된 형태의 패턴

서버 Honeypot과 클라이언트 Honeypot의 주요기능 차이는 표 3과 같다.

2.2.1 서버 Honeypot 공격탐지 알고리즘

서버 Honeypot의 상관분석 및 공격탐지 프로세스는 그림 7과 같다. 기본 데이터는 주어진 단위시간(5분)동안 서버 Honeypot에 들어온 이벤트이다. 외부 IP에서 n개 이상의 동일 이벤트가 발생할 시는 이를 축약하며, 동일한 외부 IP에서 여러 서버 Honeypot의 동일한 포트로 이벤트가 발생할 때는 스캐닝이 의심된다. 다양한 외부 IP에서 여러 서버 Honeypot의 동일한 포트로 이벤트가 발생할 시는 웜 전파를 의심하며, 다양한 외부IP에서 여러 서버 Honeypot의 다양한 포트로 동일 공격 내용의 이벤트 발생 시는 봇 전파를 의심한다[3].

표 3. 서버허니팟과 클라이언트 허니팟
Table 3. Server honeypot, client honeypot

항목	서버 허니팟	클라이언트 허니팟
트래픽 형 태	외부에서 들어오는 트래픽을 탐지	내부에서 외부로 서비스 요청
주요공격 탐지패턴	스캐닝이나 웜, DoS 공격의 패턴 탐지	좀비 공격이나 C&C, DDoS 공격 등 탐지
특 징	TCP/UDP의 모든 포트를 모니터링 하고 있다가 한번 이상 동일 포트로 발생하는 서비스 요청 탐지	사용자가 이메일에 첨부된 URL이나 첨부파일을 수행하여 감염되는 것과 동일하게 감염시켜 발생되는 트래픽 패턴 탐지

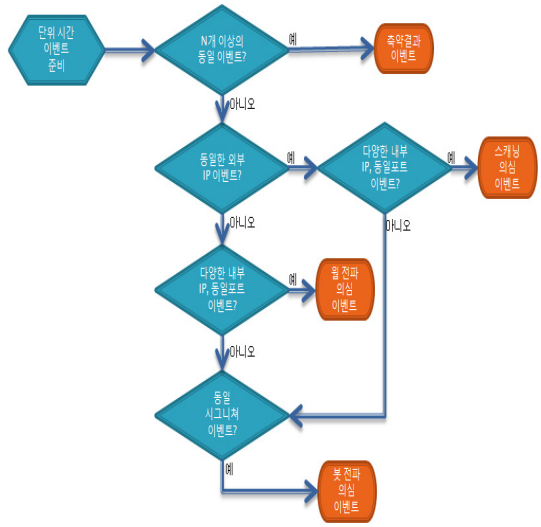

그림 7. 서버 허니팟의 공격탐지 프로세스
Fig. 7 Attack detection process of server honeypot

2.2.2 클라이언트 Honeypot 공격탐지 알고리즘

클라이언트 Honeypot에서는 주어진 단위시간(5분) 동안 클라이언트 Honeypot에 들어오거나 나가는 기대되지 않은 트래픽을 분석한다. 탐지프로세스는 그림 8과 같다. 동일한 외부IP에서 하나 이상의 클라이언트 Honeypot의 동일한 포트로 트래픽이 발생할 시는 봇의 C&C (Command & Control)서버로 의심이 되며, 하나 이상의 내부 IP에서 동일한 외부IP로 트래픽이 발생할 시는 분산 서비스 공격(Distributes denial of service)이 의심된다. 하나 이상의 내부 IP에서 다양한 외부IP로 트래픽이 발생되면 봇 전파가 의심된다[3].

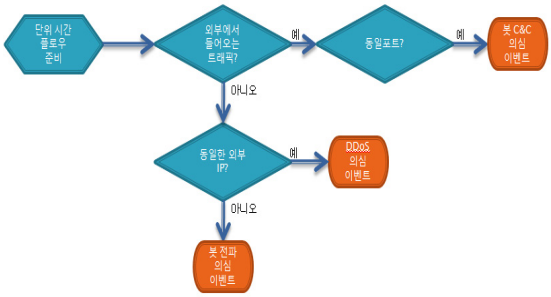

그림 8. 클라이언트 허니팟의 공격탐지 프로세스
Fig. 8 Attack detection process of client honeypot

외부 및 내부간의 유입되는 트래픽에 대한 공격탐지 프로세스는 다음과 같다. 첫째, TCP/UDP의 64,000개의 모든 포트를 모니터링 및 한 번 이상 동일 포트로 시도하는 공격의도 확인(Attack-intention)기반의 공격정보를 수집한다. 둘째, 송신IP-송신포트-수신IP-수신포트의 관계 분석을 통한 Scan, DDoS등의 네트워크 행위 기반 공격 탐지를 한다[3].

III. 공격탐지사례

3.1 DoS공격 행위 탐지

Testbed에 Virtual Honeynet시스템을 설치한 후 운영한 결과, 그림 9와 같이 Virtual Machine에서 KT DNS로의 트래픽이 짧은 시간 동안 많은 트래픽이 유발되었다. 58.227.23.107 호스트에서 KT DNS로 반복Query하는 것을 볼 수 있다.

Source	sport	Destination	dport	Protocol	Info
17:21:14.491389 58.227.23.107	137	58.227.23.255	137	NBNS	Name query NB WWW.IF.EE<00>
17:21:14.522074 58.227.23.107	1788	168.126.63.1	53	DNS	Standard query A www.starman.ee
17:21:14.522153 58.227.23.107	1789	168.126.63.1	53	DNS	Standard query A www.online.if.ee
17:21:14.522208 58.227.23.107	1790	168.126.63.1	53	DNS	Standard query A www.if.ee
17:21:14.569297 58.227.23.107	1831	168.126.63.1	53	DNS	Standard query A www.if.ee
17:21:14.569408 58.227.23.107	1830	168.126.63.1	53	DNS	Standard query A www.online.if.ee
17:21:14.569471 58.227.23.107	1829	168.126.63.1	53	DNS	Standard query A www.starman.ee
17:21:14.575722 168.126.63.1	53	58.227.23.107	1788	DNS	Standard query response, Refused
17:21:14.575728 168.126.63.1	53	58.227.23.107	1790	DNS	Standard query response, Refused

그림 9. 트래픽 분석 화면1
Fig. 9 Packet flow1

Virtual Honeynet시스템의 상관분석엔진은 이 형태를 “Zombie attack - single destination” 공격으로 탐지하였다. 해당 패킷에 대해 Deep Packet Inspection한 결과 Allaple worm으로 판명이 되었다. Allaple worm은 C&C서버 접속 없이 특정 웹사이트에 대하여 DoS공격을 하는 Worm으로서 20,80,97,443포트를 이용하여 DoS공격을 수행한다. 하지만 Worm이 KT DNS서버에 특정 웹사이트의 DNS query하였으나 KT DNS서버가 query를 거부함으로서 Allaple worm은 해당 사이트들의 IP주소를 구하지 못하게 되어 실제로는 DoS공격을 수행하지는 못하였다. 이러한 Worm이 국내 일반PC에 대량으로 감염될 경우, KT DNS서버에 부하를 주어 자칫 1.25대란과 유사한 공격피해를 유발할 수 있다. 추가적인 분석 결과 Allaple worm은 또한 무작위로 ICMP공격을 수행한다. 그림10에서 보는 바와 같이 내부 Virtual machine에서 다수의 외부 호스트로 ICMP 패킷을 보내는 행위들이 탐지되었다.

20:17:01.809458	58.227.23.107	216.69.54.175	ICMP	Echo (ping) request
20:17:01.831368	58.227.23.107	216.69.188.185	ICMP	Echo (ping) request
20:17:01.859897	58.227.23.107	216.69.30.234	ICMP	Echo (ping) request
20:17:01.859944	58.227.23.107	216.69.42.37	ICMP	Echo (ping) request
20:17:01.859991	58.227.23.107	216.69.85.178	ICMP	Echo (ping) request
20:17:01.860035	58.227.23.107	216.69.7.206	ICMP	Echo (ping) request
20:17:01.860078	58.227.23.107	216.69.185.106	ICMP	Echo (ping) request
20:17:01.860121	58.227.23.107	216.69.87.63	ICMP	Echo (ping) request
20:17:01.860164	58.227.23.107	216.69.66.98	ICMP	Echo (ping) request
20:17:01.860206	58.227.23.107	216.69.36.84	ICMP	Echo (ping) request
20:17:01.860250	58.227.23.107	216.69.77.136	ICMP	Echo (ping) request
20:17:01.860301	58.227.23.107	216.69.211.86	ICMP	Echo (ping) request
20:17:01.861953	58.227.23.107	216.69.112.27	ICMP	Echo (ping) request
20:17:01.895386	58.227.23.107	216.69.32.32	ICMP	Echo (ping) request
20:17:01.937857	58.227.23.107	216.69.161.68	ICMP	Echo (ping) request
20:17:01.951557	216.69.101.66	58.227.23.107	ICMP	Echo (ping) reply
20:17:01.972754	58.227.23.107	216.69.76.147	ICMP	Echo (ping) request
20:17:02.020700	58.227.23.107	216.69.206.203	ICMP	Echo (ping) request
20:17:02.061542	58.227.23.107	216.69.31.63	ICMP	Echo (ping) request
20:17:02.090716	58.227.23.107	216.69.249.123	ICMP	Echo (ping) request
20:17:02.126143	58.227.23.107	216.69.249.91	ICMP	Echo (ping) request

그림 10. 트래픽 분석 화면 2
Fig. 10 Packet flow2

위 탐지 사례에서 보는 바와 같이, Virtual Honeynet에서는 Allaple Worm의 이러한 행위를 Signature없이도 행위기반으로 탐지한 것을 볼수 있다. 위 탐지 사례는 IPS나 TMS에 해당 Worm에 대한 Signature가 없을 경우에는 공격 탐지가 불가능한 공격으로서 Virtual honeynet의 행위기반 탐지능력을 보여 준다.

3.2 Port Scan 행위 탐지

외부의 테스트PC에서 Honeypot측으로 nmap을 이용하여 Port Scan을 시도하면 Virtual Honeynet에서는 "Single-Source-Spoofed DoS[1-1-1-1] worm으로 판단하며, 그림 11과 같이 패턴을 시각화하여 보여준다.

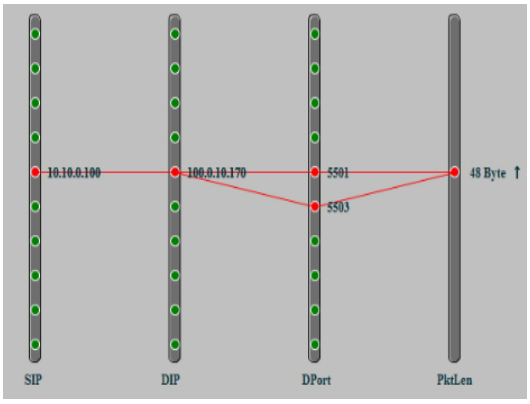

그림 11. Port scan행위 시각화 분석 화면
Fig. 11 Visual analysis of port scan

3.3 Multi-Get Request 행위 탐지

외부의 테스트PC에서 내부 여러대의 Honeypot 웹서버로 80포트를 이용한 Get방식의 Request행위를 그림 12와 같이 시행하였다.

```
--- 100.0.10.100 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.244/0.252/0.259/0.008 ms
CMC-MB13:~ mcchae$ ping 100.0.10.168
PING 100.0.10.168 (100.0.10.168): 56 data bytes
64 bytes from 100.0.10.168: icmp_seq=0 ttl=63 time=4.857 ms
64 bytes from 100.0.10.168: icmp_seq=1 ttl=63 time=0.373 ms
^C
--- 100.0.10.168 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.373/2.615/4.857/2.242 ms
CMC-MB13:~ mcchae$ GET http://100.0.10.168
-bash: GET: command not found
```

```
CMC-MB13:~ mcchae$ wget http://100.0.10.168
--2011-09-06 12:04:47--  http://100.0.10.168/
Connecting to 100.0.10.168:80... failed: Connection refused.
CMC-MB13:~ mcchae$ wget http://100.0.10.168
--2011-09-06 12:04:51--  http://100.0.10.168/
Connecting to 100.0.10.168:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 30 [text/html]
Saving to: `index.html'

100%[======================================================>

2011-09-06 12:04:52 (1.30 MB/s) - `index.html' saved [30/30]

CMC-MB13:~ mcchae$ vi index.html
CMC-MB13:~ mcchae$
CMC-MB13:~ mcchae$
CMC-MB13:~ mcchae$
CMC-MB13:~ mcchae$ cat index.html
```

그림 12. Multi-Get request 실행
Fig. 12 Launched Multi-Get request

Virtual honeynet에서는 위의 Multi-Get Request 행위를 이상행위로 판단하여 그림 13과 같이 "Packet injected" 이상 행위를 보여주고 있으며 실제 Packet 내용도 볼 수가 있다.

TimeStamp	위...	경고내용	로그	소스IP	목적지IP
2011/09/06 10:13:59	6	Packet Injected	18 bytes attack string from 10.1	10.10.0.100	100.0.10.169
2011/09/06 10:13:59	6	Packet Injected	18 bytes attack string from 10.1	10.10.0.100	100.0.10.169
2011/09/06 10:13:59	6	Packet Injected	18 bytes attack string from 10.1	10.10.0.100	100.0.10.170
2011/09/06 10:13:59	6	Packet Injected	18 bytes attack string from 10.1	10.10.0.100	100.0.10.168
2011/09/06 10:13:59	6	Packet Injected	18 bytes attack string from 10.1	10.10.0.100	100.0.10.170

그림 13. Packet Injected 행위 탐지
Fig. 13 Detection of packet Injected behaviour

Ⅳ. 결 론

Virtual honeynet을 이용하여, 기존의 보안기술에서 탐지하지 못했던 은닉기법을 사용한 악성코드를 다중 호스트의 통신 Flow비율 특성을 상관 분석하여봇넷(Botnet)의 Target공격 및 C&C서버와의 이상행위를 탐지하였다. 오늘날 DDoS와 같은 인터넷 공격은 봇넷 등을 이용한 Large Scale공격의 양상을 보이고 있으며 사회적 또는 국가적 차원의 문제가 되고 있으며, 사이버테러 및 사이버 전쟁 등에도 널리 사용되고 있다. 특히 봇넷은 은닉기법을 사용하므로 기존의 알려진 공격패턴을 사용하는 안티바이러스와 같은 악성코드 탐지 툴 및 침입탐지 또는 침입방지 시스템에서 탐지가 불가능하다. 따라서 이러한 Large Scale 공격

의 효율적인 탐지를 위해서는 다중 호스트 통신 특성을 상관 분석하여, 이들 공격의 target, C&C서버와의 통신 등의 공격행위를 탐지할 수 있다. Virtual Honeynet은 봇넷과 같은 시그니처에 의해 탐지 불가능한 악성 코드에 의한 네트워크의 행위에 대해서 전문가의 판단을 요구하는 종래의 시그너쳐 방식 대신에 다중 호스트로 유입되거나 다중 호스트로부터 유출되는 패킷들의 통신 비율의 행위를 상관분석함으로써 보다 신속하게 네트워크의 이상 행위 및 봇넷을 탐지할 수 있는 효과가 있다. 향후 바이러스와 웜의 특성을 이용하여 감염 속도를 최대화 한 혼합형 보안위협(Blended threat)분야에 Virtual honeynet의 행위 탐지기반 기법의 탐지 효용성에 대한 검증이 필요한 부분이다.

참고 문헌

[1] 김인중, "중요핵심기반시설(SCADA)에 대한 보안관리연구", 한국통신학회논문지, 30권, 8C호, pp.838-848, 06, 2005.

[2] 방송통신위원회, 2010 국가정보보호백서, 행정안전부, 4월, 2010년.

[3] 강대권, "Virtual Honeynet을 이용한 신종공격 탐지기술 개발", 한국전자통신학회논문지, 5권, 4호, pp.406-411, 2010.

[4] Honeynet Project, Know Your Enemy :Honeynets, http://www.honeynet.org,2006

[5] The Honeynet Project. http://www.honeynet.org.

[6] Wikipdeia, Comparison of platform virtual machines, http://en.wikipedia.org/wiki/Comparison_of_platform virtual_machines

[7] E.Alata,Lessons learned from the deployment of a high-interaction honeypot, IEEE Computer Society,2006

[8] Sebek. https://projects.honeynet.org/sebek/

[9] HFlow, https://projects.honeynet.org/hflow/

[10] G. Bednarski et el, "Understanding Network Threats through Honeypot Deployment", CMU, pp 273-306, 2004.

[11] Ricky M,Understanding Virtual Honeynets, magam, 2004.

[12] 김영진, "SCADA시스템의 안전성 확보방안에 관한 연구", 한국정보보호학회논문지, 19권, 6호, pp.146-149, 2009.

저자 소개

김천석(Chun-Suk Kim)

1980년 9월 광운대학교 전자공학과(공학사)
1982년 9월 건국대학교 대학원 전자공학과(공학석사)
1998년 경남대학교 대학원 전자공학(공학박사)
1982년 11월~현재 전남대학교 전자통신공학과 교수
※ 관심분야 : 수중통신, 정보통신분야

강대권(Dae-Kwon Kang)

1984년 2월 광운대학교 전자통신공학과 졸업(공학사)
1988년 8월 한양대학교 산업대학원 전자공학과 졸업(공학석사)
2012년 1월 현재 전남대 전자통신공학과 박사과정
현재 한전KDN(주) 전력 IT연구원 송변전IT연구그룹
※ 관심분야 : 정보보호, 전력IT컨설팅

엄익채(Ieck-Chae Euom)

2003년 8월 전남대학교 컴퓨터정보공학과 졸업(공학사)
2003년 8월~2007년 9월 LG이노텍 신뢰성S/W Lab
2007년 10월~현재 한전KDN 정보보호사업팀
저서 : Start Up! 웹마스터 (2002, 웅보출판사)
※ 관심분야 : 인프라 가상화 분야 정보보호