Snort 와 Suricata 를 활용한 내부망 공격 탐지 및 패킷 분석

김상유, 노우석, 이호재
수원대학교 정보보호학부
e-mail : rlatkddb706@naver.com

Packet Analysis with Snort & Suricata

Sang-yoo Kim, Woo-Suk No, Ho-Jae Lee
Dept. of Information Security, Suwon University

"본 논문은 2017 년 한이음 ICT 멘토링 프로젝트의 결과물입니다."

요 약

오픈소스 기반의 패킷 탐지 도구인 WireShark 를 활용하여, 패킷을 직접 캡쳐, 분석해보고 칼리 리눅스를 활용한 시나리오 기반의 모의해킹을 시도, Snort 와 Suricata 를 이용하여 공격적인 성향의 패킷을 탐지하여 로그를 데이터베이스화 시킨 후 사용자 편의에 맞도록 가시화(可視化)한다. 사용자는 가시화 된 로그를 통해 공격을 좀 더 빠르게 인지하여 대응하는 것이 가능하다.

1. 서론

IoT 를 비롯한 AI 와, 자율주행 등의 첨단 ICT 기술이 여러 산업 서비스들과 융합되어 제공됨에 따라, 인간의 삶의 질을 향상시켜주는 긍정적인 효과를 낳았지만, 신기술의 발전에 따른 보안 위협이 증가하여 안전성 우려 또한 높아지고 있다.

지난 2016 년 악성코드 'Mirai' 에 감염된 50 만개의 IoT 기기들로 인해 아마존·트위터·넷플릭스 등의 사이트가 DDOS 공격을 받게 되어, 마비가 된 사례가 있었으며, 최근엔 자동차 해킹 시연을 통해 키 없이 시동 걸기, 차량 급 발진과 같은 차량의 제어권 탈취가 가능하다는 것이 증명됨에 따라 정보보안은 일상생활에서 중요한 부분으로 자리 잡았다는 것을 알 수 있다. 이러한 이유로 정보보안시장의 규모는 점차 확장되어 정보보안 인력의 수요가 증가하고 있다.

제안된 연구내용은 정보보안 업무분야 중 하나인 보안관제 업무에 쓰이는 패킷 분석 도구와 실제 기업에서 사용 되어지는 보안솔루션인 Snort 와 Suricata 를 운용해보며 정리한 결과물이다.

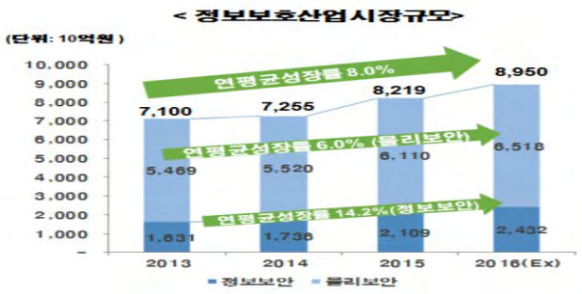

그림 1. 정보보호산업시장 규모의 확장

2.선행 연구

2.1 WireShark

패킷 탐지에 사용되는 Wireshark 는 여러 종류의 컴퓨터 플랫폼에서 동작할 수 있는 크로스 플랫폼으로, GTK + 위젯 툴킷을 이용하여 사용자 인터페이스를 제공하며, pcap(packet capture)을 이용하여 패킷을 포획한다.

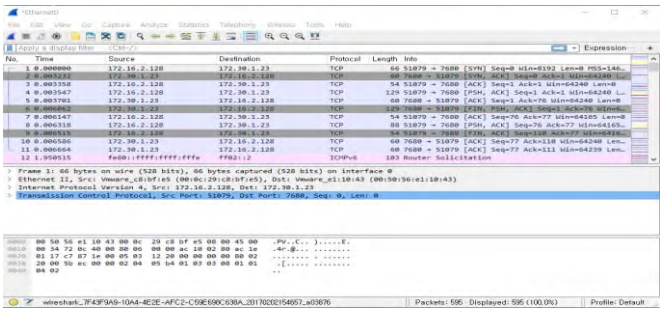

그림 2. WireShark 실행화면

2.2 Snort

Snort 는 “sniffer and more"라는 말에서 유래 되었으며, 1998 년 Sourcefire 의 CTO 인 Martin Roesch 가 발표했습니다. 처음에는 단순한 패킷 스니퍼 프로그램이었으나, 이후 현재의 IDS 와 같이 rule 을 이용한 분석 기능이 추가되고, 커뮤니티를 통하여 계속적인 기능 보안과 향상을 통해 지금과 같이 다양한 기능과 탁월한 성능을 갖춘 프로그램이 되었다.

오픈 소스로 개발중인 패킷 캡처 라이브러리인 libpcap 을 사용하여 패킷을 캡처하고, 수집된 패킷이 사전에 정의된 Snort 공격 룰과 비교하여 만약 매

칭 되었을 경우 syslog 를 통해 로그를 남기거나 특정 디렉토리의 특정 파일 또는 database 남기도록 할 수 있다.

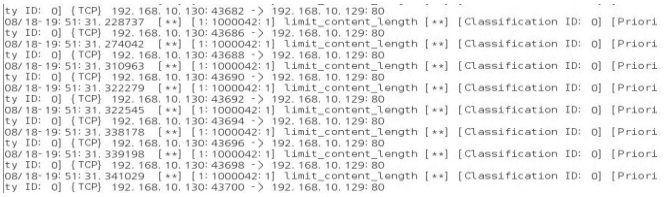

그림 3. 텍스트 기반의 Snort 로그

2.3 Suricata

Suricata 는 OISF(Open Information Security Foundation)에서 개발 한 것으로, Suricata 가 나오기 전까지는 Snort 가 Open Source 기반의 IDS 로 오랜 시간 입지를 굳혀왔지만, 트래픽 양이 점점 증가하면서 대용량 트래픽의 실시간 처리에 대한 이슈가 부각되면서 단일 스레드만 지원해서 대용량 트래픽을 실시간으로 처리하기 어려운 Snort 를 대신해 Suricata 가 주목받기 시작하였다.

Suricata 는 기존 Snort 에서 사용하던 시그니처를 그대로 사용할 수 있도록 완벽 호환하며, Snort 룰 포맷을 몰라도 스크립트 언어(lua)로 시그니처 작성이 가능하다. 또한 대용량 트래픽을 실시간으로 처리하기 위해서 멀티 코어, 멀티 스레드를 완벽히 지원가능하다는 장점을 가지고 있다.

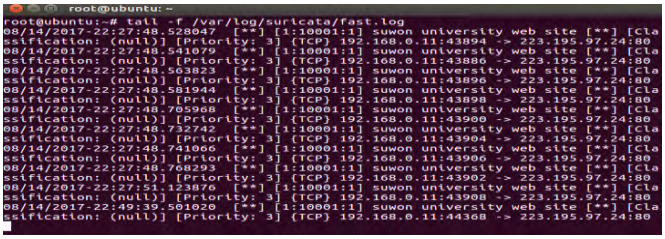

그림 4. 텍스트 기반의 Suricata 로그

2.4 Kali Linux

칼리 리눅스(Kali Linux)는 정보 보안을 테스트하기 위한 오픈소스 리눅스 배포판인 백트랙의 후속버전으로 이 안에는 백트랙처럼 수많은 해킹과 관련된 도구와 설명서들이 있다.

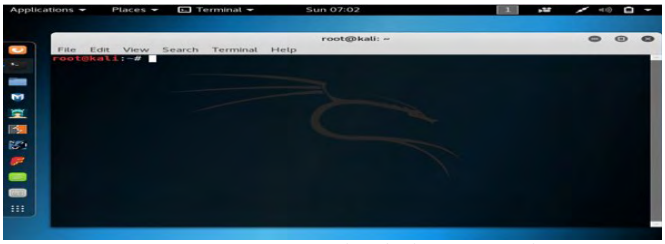

그림 5. Kali Linux 의 터미널 실행화면

3.연구 내용

3.1 연구목표

기존 연구에 사용되어진 도구들은 모두 텍스트 기반의 로그들을 남긴다. 짧은 시간 내에도 셀 수 없이 많은 패킷이 캡쳐 되므로 사용자가 텍스트 기반의 로그를 모두 살펴보며 판단하기가 어렵다. 보안관제 서비스 특성 상 실시간 탐지가 필요하므로 사용자가 로그를 쉽고 빠르게 판단하기 위해선 GUI 환경의 패킷 가시화가 필요하다.

3.2 연구 흐름도

3.2.1 Snort

가상 OS 소프트웨어인 VMWare 를 활용하여 Centos 7 가상 운영체제와 Kali linux 를 실행한다. Kali linux 를 활용하여 Centos 7 운영체제에 모의 공격을 실시, Centos 7 에서는 WireShark 를 활용하여 공격성 패킷을 캡처 및 분석을 한다. 분석한 결과를 바탕으로 Rule 을 추가한 후 barnyard2 와 연동하여 Snort 를 실행한다. 이 때 발생한 로그는 MySQL 에 저장되어지므로 BASE 를 통해 MySQL 에 저장되어있는 로그 DB 를 실시간으로 읽어들여 가시화하는 기능을 한다.

그림 6. Snort 로그 가시화 흐름도

3.2.2 Suricata

공격 환경 구축과 패킷 캡처 및 분석 과정은 Snort 구축과 같다. Suricata 로 탐지 및 차단한 패킷의 로그를 MySQL 로 DB 화하고, Logstash 를 이용하여 생성된 로그 DB 를 수집한다. 수집한 로그 DB 들은 전처리를 거쳐 Elasticsearch 로 자동으로 업로드 시키게 되고, 수집된 로그 DB 를 index 에 저장하여 관리한다. index 에 저장된 로그 DB 들을 Kibana 를 사용하여 검색 및 분석, 시각화를 실시한다.

그림 7. Suricata 로그 가시화 흐름도

3.3 시나리오 기반 실습

3.3.1 SLOW HTTP POST DOS - Snort

Slow Http Dos 공격은 HTTP POST 메소드를 이용하여 서버로 전달할 대량의 데이터를 장시간에 걸쳐 분할 전송하며, 서버는 POST 데이터를 모두 수신하지 않았다고 판단하여 연결을 장시간 유지하므로 가용량을 소비하게 되어 다른 클라이언트의 정상적인 서비스를 방해하는 서비스 거부 공격이다.

Kali linux 에서 FORM 을 이용해 HTTP POST 를 전송하는 웹페이지를 공격하기 위해서 R-u-dead-yet(RUDY)를 활용하여 공격을 실행한다.

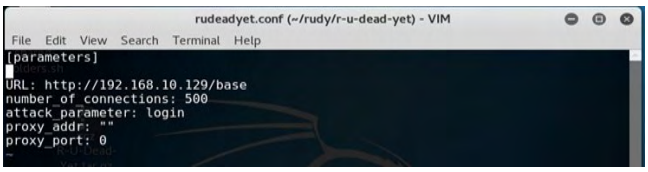

그림 8. RUDY 에 공격대상 등록

그림 8 은 rudeadyet.conf 에 공격대상의 Web-server 의 parameters 를 등록하는 과정이다. 공격대상의 URL 을 호출하여 설정되어 있는 쿠키정보가 있다면 헤더의 Content-Length 를 크게 설정하여 Connetction 수 만큼 Client 를 생성하여 서버를 지연시킨다.

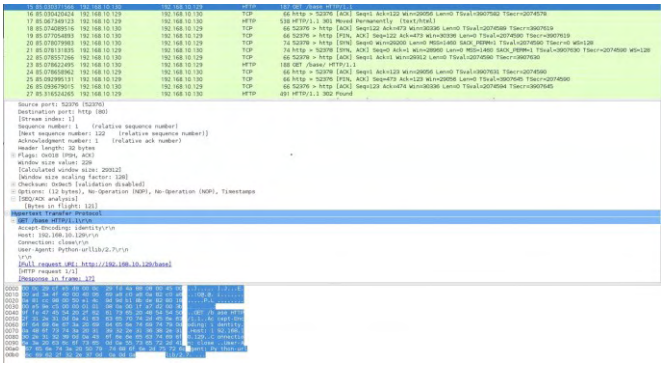

그림 9. WireShark 패킷분석 (Slow HTTP POST)

패킷을 분석하면 POST 공격은 쿠키정보를 세팅하기 위해서 희생자의 URL 을 호출하는데, 이때 사용되는 GET 패킷을 보면 User-Agent 가 Python-urlib/2.7 로 되어있는 것을 알 수 있다. 이 결과를 바탕으로 그림 10. 과 같이 Snort 에 rule 을 추가한다.

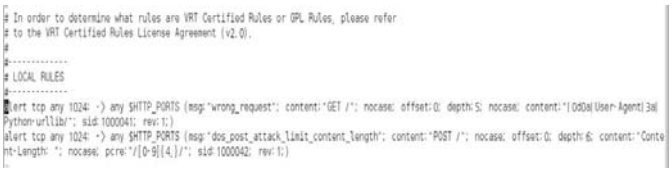

그림 10. Snort rule 추가 (Slow HTTP POST)

Snort 를 효율적으로 출력하기 위해서 barnyard2 를 연동한 후 Snort 를 실행할 경우 그림 11.처럼 추가한 Rule 에 일치하는 패킷이 찍힌 것을 확인할 수 있다.

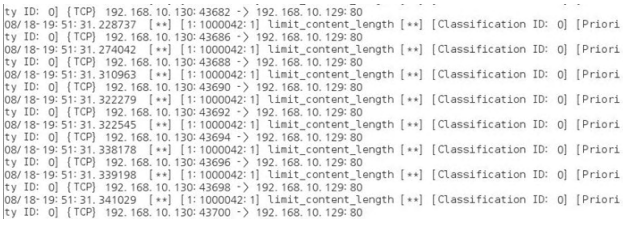

그림 11. Barnyard2 연동 후 검출된 패킷 로그

그림 12. 는 Snort 의 탐지결과를 BASE 로 가시화(可視化) 시켜 탐지된 패킷을 상세히 표시하였다.

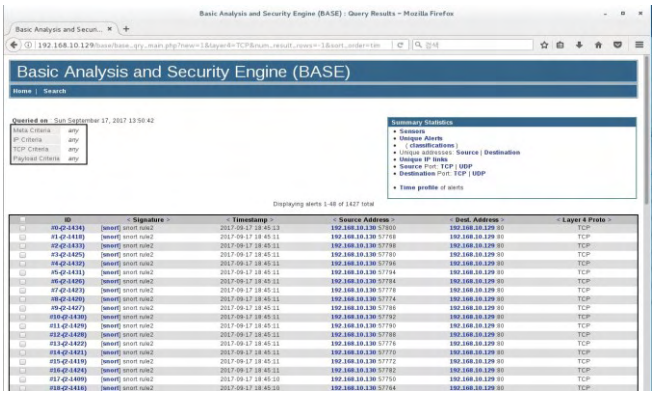

그림 12. 검출된 패킷 로그 BASE 연동

3.3.2 SLOW HTTP POST DOS - Suricata

Suricata 의 경우 앞서 언급한 Snort 와 과정이 동일하다. 패킷 로그 가시화(可視化)시 Snort 와 다른 Kibana 를 활용하여 출력하였다.

그림 13. 검출된 패킷 로그 Kibana 연동

3.3.3 ICMP Redirection - Snort

ICMP Redirection 공격은 ICMP Redirect 패킷(Type 5)이 라우터를 통하여 호스트에게 최적의 경로라고 알려주는 것을 이용하여 공격자가 대상의 라우터를 속여 라우팅 테이블을 변경하여 특정한 트래픽이 의도치 않은 경로로 경유하도록 만드는 공격이다.

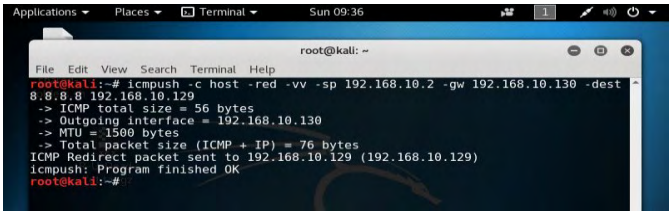

그림 14. ICMP Redirection 실행

Kali linux 에서 Type 5 와 Code 1 을 이용해 패킷을 만들어서 공격 대상에 전달해 공격을 실행을 위해 Icmpush 툴을 사용한다.

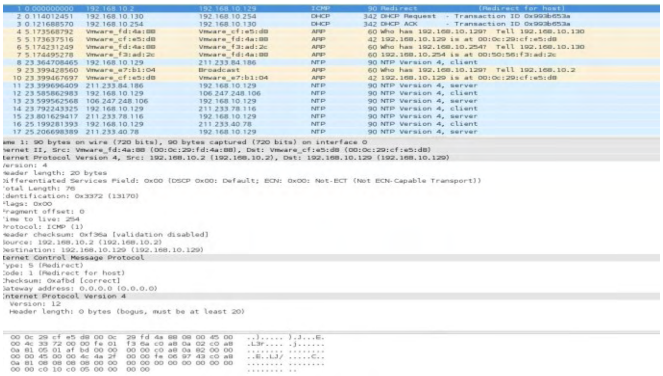

그림 15. WireShark 패킷분석 (ICMP Redirection)

패킷을 분석하면 ICMP Redirect 패킷(Type 5)이 검출된다. 그림 16. 과 같이 Snort rule 에 type5 를 탐지할 수 있는 룰을 추가한다.

그림 16. Snort rule 추가 (ICMP Redirection)

barnyard2 를 연동하여 Snort 탐지 결과를 출력하면 그림 17. 과 같이 출력되는 것을 확인할 수 있다.

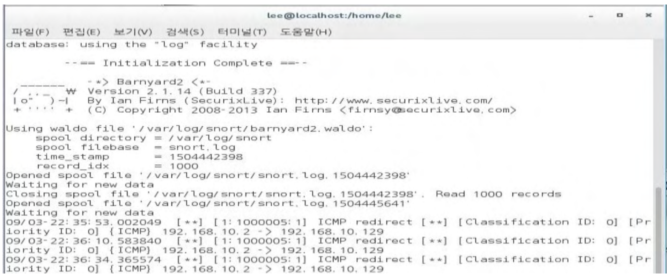

그림 17. Barnyard2 연동 후 검출된 패킷 로그

그림 18. 은 Snort 의 탐지결과를 BASE 로 가시화 시킨 것이다.

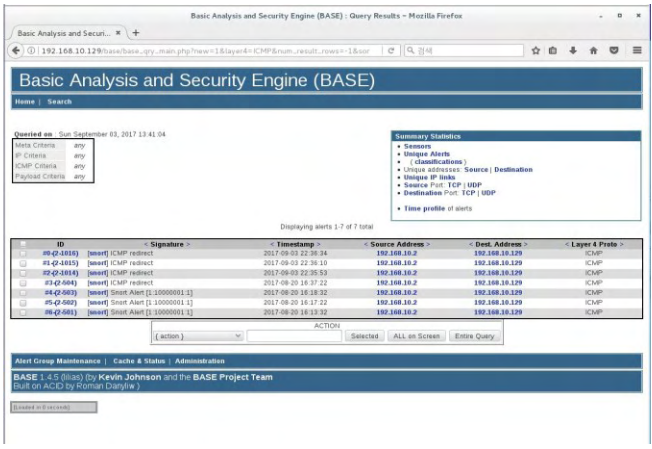

그림 18. 검출된 패킷 로그 BASE 연동

3.3.4 ICMP Redirection - Suricata

Suricata 의 경우 앞서 언급한 Snort 와 과정이 동일하다. 패킷 로그 가시화(可視化)시 Snort 와 다른 Kibana 를 활용하여 출력하였다.

그림 19. 검출된 패킷 로그 Kibana 연동

4. 결론

IDS 와 IPS 는 보안 솔루션으로써 가장 널리 알려져 있으며 다양한 형태로 존재한다. 이미 국내,외 많은 상용제품들이 나와 있고, 공개 S/W 중에서도 활용 가능한 IDS, IPS 들이 많이 있다. 그 중에서도 가장 대표적인 IDS, IPS 인 Snort 와 Suricata 는 비용이 들지 않고 다른 오픈 소스 보안 솔루션들과 연동하여 구현할 시 시중에서 판매되는 고가의 상용 보안 솔루션들에 뒤쳐지지 않을 만큼 강력하고 사용자 편의에 맞는 툴 들을 제공하므로 자본이 넉넉하지 않은 중소기업에서 활용하기에 알맞은 솔루션이라 생각한다.

5. 활용 방안

Snort 와 Suricata 를 Database 와의 연동을 통해 실무에서 사용하는 보안시스템을 구축하는데 기초로 사용될 수 있으며, 윈도우에서 일부러 보안이 취약한 서버를 만들어 허니팟 시스템으로도 구현이 가능하다. 더 나아가 허니팟 시스템을 기반으로 Application 을 만들어 사용자에게 침입한 여러 해킹 공격들에 대한 패턴을 기록하고 수집하여 보안성을 강화해 나갈 수 있다. 그 외에도 IDS 패턴매칭과 heuristics 기술의 전문성을 바탕으로 새로운 알고리즘도 발명 할 수 있으며 Deep Learning 기술을 활용하여 새로운 보안솔루션을 개발하기 위한 API 로 사용할 수 있다. 또한 취합된 로그 DB 들을 활용하여 새로운 보안 솔루션과 소프트웨어들을 무궁무진하게 개발할 수 있다.

참고문헌

[1] 김상유, 오픈소스 IDS/IPS Snort 와 Suricata 의 탐지 성능에 대한 비교 연구, 디지털산업정보학회 논문지, 2016

[2] 노우석, International Journal of Future Generation Communication and Networking, 보안공학연구지원센터, 2016

[3] 이호재, A Designing Method of Digital Forensic Snort Application Model, 한국사이버테러정보전학회, 2010 년