Suricata와 Elastic Stack, Kafka를 이용한 공격 패킷 분석 및 보안관제 시스템 구축

이다은, 이혜린, 조민규
성신여자대학교 융합보안공학과
성신여자대학교 컴퓨터공학과
영남대학교 컴퓨터공학과
storyda1@naver.com, lin7258@naver.com, inch1209@naver.com

Establish a security control system through attack packet analysis with Suricata, Elastic Stack, and Kafka

Da-Eun Lee, Hye-Rin Lee, Min-Gyu Jo
Dept. of Convergence Security Engineering, Sung-shin Women's University
Dept. of Computer Engineering, Sung-shin Women's University
Dept. of Computer Engineering, Yeung-nam University

요 약

코로나19 대유행으로 인해 전 세계가 원격으로 일상을 옮겨가면서 인터넷 트래픽량이 증가하고 보안 위협 또한 높아졌다. 높은 보안성이 요구되는 현 상황에 대응하기 위해 본 논문에서는 Suricata와 Elastic Stack, Kafka를 이용해 보안관제 로그 분석시스템을 구축하였다. 실시간으로 공격을 탐지하고 로그를 수집해 유의미한 데이터를 도출하여 시각화한다. 또한 시각화 한 대시보드를 제공함으로써 사용자는 공격의 위험도를 파악할 수 있고 앞으로의 공격을 대비할 수 있다.

1. 서론

코로나19 대유행으로 인한 봉쇄가 시작되고 전 세계가 원격으로 일상을 옮겨가면서 인터넷 트래픽이 30% 증가했다. 아카마이가 발표한 '인터넷 보안 현황 보고서: 불확실성에 적응하기'에 따르면 2020년에만 약 1,090억 건의 악성 DNS 쿼리가 관측됐다[1]. 트래픽 증가로 인해 각종 보안 이벤트 및 시스템 로그 등을 분석하고 차단할 수 있는 보안관제에 대한 중요성이 커지고 있다.

본 논문에서는 매년 증가하는 사이버 공격에 효과적으로 대응하기 위해 Suricata를 이용하여 공격 탐지 및 차단하기 위한 정책을 등록하고 Elastic stack을 이용해 로그를 수집하고 시각화한다. 또한 Apache Kafka를 이용해 기존 방식보다 빠르고 안정적으로 로그 데이터를 수집 및 분석할 수 있도록 한다. 시각화한 대시보드를 통해 트래픽 이상 유무를 빠르게 파악할 수 있는 보안관제 시스템을 제안한다. 이로써 앞으로의 공격을 대비할 수 있는 시스템을 제공하고자 한다.

2. 본론

2.1 보안관제 시스템 운영 현황

'2021 사이버 동향 보고서'에 따르면 기업에서 많이 사용하는 'Exchange Server'의 보안취약점이 발견되었다. 서버 내부에 접근하여 권한을 탈취하는 방법으로 공격한 것이다. PC에 설치된 백신과 KISA의 조치를 통해 큰 피해로 이어지지 않았지만 기업에서는 침해 여부 확인 방법조차 알지 못했다[2]. 이처럼 제로 데이 공격(Zero day Attack) 등 신규 보안 취약점으로 공격하거나, 사전에 규정된 취약점 이외의 공격은 효과적으로 조치하는 것이 어렵다. 기존의 보안관제 프로세스는 공격, 침해시도를 발견하면 공격을 분석하고 추후에 공격이 들어왔을 때 대응할 수 있도록 예방점검을 하며 공격에 대비한다[3]. 이는 식별할 수 없는 공격패턴이 정상 트래픽으로 위장하여 서버에 접근할 경우 실시간으로 알아차리지 못하여 그대로 공격에 노출되기 쉽다. 따라서 공격자의 접근 여부를 빠르게 판단할 수 있는 보안관제 시스템이 필요하다.

2.2 선행 연구

2.2.1 Suricata

Suricata는 IDS, IPS와 NSM 기능을 가진 오픈소스이다. Snort와 호환 가능하며 멀티 스레드 방식으로 동작하여 처리 속도가 빠르다는 특징이 있다.

2.2.2 Elastic Stack

Elastic Stack은 세 개의 오픈소스 Elasticsearch, Logstash, Kibana와 Beats가 추가된 형태이다.

Elasticsearch는 Apache Lucene 기반의 모든 유형의 데이터를 위한 검색, 분석 엔진이다. 가변 검색 및 실시간에 가까운 저장, 검색, 분석을 제공한다.

Logstash는 실시간 파이프라인 기능을 가진 오픈소스 데이터 수집 엔진이다. 여러 소스에서 동시에 데이터를 수집하여 변환 후 전송이 가능하다.

Kibana는 Elasticsearch에서 색인된 데이터를 검색 및 필터링하고, 시각화할 수 있는 오픈소스 프론트엔드 애플리케이션이다.

Beats는 서버 에이전트로 설치하여 다양한 유형의 데이터를 Elasticsearch 또는 Logstash에 전송하는 오픈소스이며, Filebeat, Metricbeat 등 여러 종류의 beat가 있다. 본 논문에서는 Filebeat를 사용한다.

2.2.3 Wireshark

Wireshark는 오픈소스 패킷 분석 프로그램이다. Qt 위젯 툴킷을 이용하여 사용자 인터페이스를 제공하며, pcap 파일 형식을 가진다. 다양한 UNIX 계열 운영체제와 Windows에서 동작이 가능하다.

2.2.4 Kafka

Kafka는 오픈소스로 Publish-Subscribe 모델을 구현한 분산 메시징 시스템이며, 대용량 실시간 로그 처리에 특화되어 있다.

2.2.5 DVWA

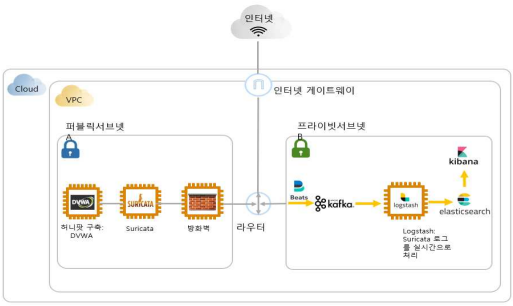
DVWA는 취약하게 만든 웹 환경으로 구성되어 있으며, 웹 모의해킹을 진행하기 위해 사용된다. 본 논문에서는 DVWA를 이용해 허니팟을 구성하였다.

2.3 연구 내용

2.3.1 연구목표

기존의 보안관제 시스템과 비교하여 빠르고 안전하게 실시간 로그 데이터를 수집 및 분석할 수 있는 시스템을 설계 및 구축한다. 외부망/내부망 위치를 고려하여 구성한다. 모의 공격 시도 후 패킷 분석을 바탕으로 Suricata rule을 작성하여 공격을 탐지하고, 방대한 양의 로그를 빠르고 안정적으로 처리하기 위해 Elastic stack과 Kafka를 함께 이용한다. 실시간으로 수집되는 로그들을 보기 쉽게 시각화하여 대중들도 쉽게 사용할 수 있도록 한다.

2.3.2 연구흐름도



(그림 1) 보안관제 시스템 구성도

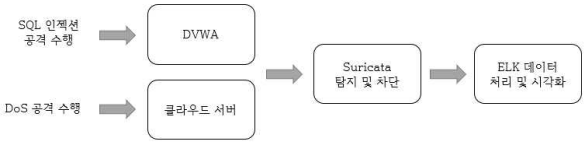
AWS의 VPC(Virtual Private Cloud)를 이용해 외부에서 접근할 수 있는 Public 망과 외부에서 접근할 수 없는 Private 망으로 나눈 환경을 구성하였다.

DVWA를 이용한 허니팟은 외부에서 접근할 수 있는 Public망에 두고, Suricata를 통해 탐지 및 차단을 진행하였다. 탐지에 있어 Snort, Suricata 두 가지 선택지가 존재했지만, IP, TCP, UDP, ICMP 이외의 프로토콜을 탐지할 때 포트 번호에 의지하는 Snort와 달리 프로토콜 자체를 파악할 수 있으며 멀티 스레드 방식으로 처리 성능이 비교적 더 빠른 Suricata를 본 논문에 사용하였다[4].

Suircata를 통해 Public망에 저장되는 대용량의 로그들을 Filebeat 및 Kafka를 이용해 실시간으로 Private망 내부에 있는 Logstash에 전달해 준다. 전달된 데이터는 미리 설정한 필터링을 통해 전처리가 이루어지고, Elasticsearch에 전송 및 저장된다. Kibana는 Elasitcsearch의 실시간에 가까운 검색 기능을 통해 데이터들을 가져오고, 보기 쉬운 대시보드 구성을 통해 시각화한다.

2.4 시나리오

본 논문의 대략적인 모의공격 시나리오는 (그림 2)와 같다. DoS 공격으로는 Ping of Death와 TCP SYN Flooding 공격을 진행한다.



(그림 2) 모의 공격 가상 시나리오

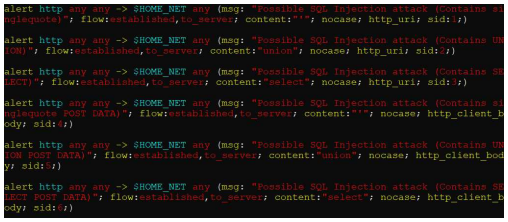
2.5 연구 결과

2.5.1 SQL Injection 공격

SQL Injection은 응용 프로그램 보안 상의 허점

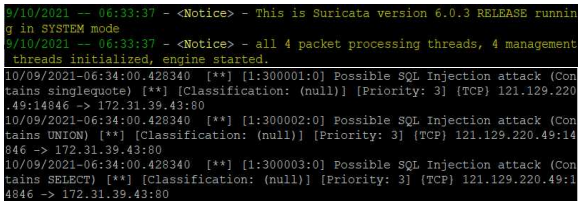
을 이용해 악의적으로 SQL문을 주입하고 실행하여 데이터데이스가 비정상적으로 동작하도록 조작하는 행위이다. SQL injection 공격의 종류는 작은 따옴표(')와 or 연산자를 활용한 공격, UNION 명령어를 활용한 공격, 논리적 에러를 이용한 공격, Blind SQL Injection 공격 등이 있다.

공격 기법들을 분석하여 SELECT, UNION 등 특정 내용이 포함된 패킷을 탐지할 수 있도록 Suricata rule을 작성한다.



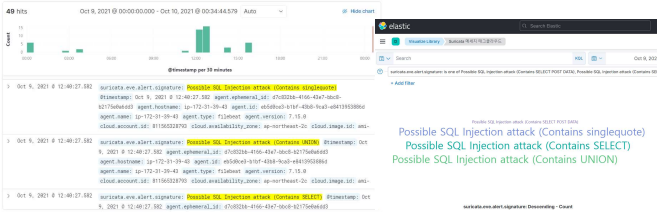
(그림 3) Suricata rule 작성(SQL Injection)

Suricata를 실행하고 DVWA에서 모의 공격을 수행한 결과 SQL Injection 공격 패킷을 탐지하였다.



(그림 4) Suricata 실행과 공격 탐지 로그

수집한 로그 데이터를 ELK로 분석하고, Kibana에서 필터링을 통해 발생한 SQL Injection 공격 유형에 대해 태그 클라우드로 시각화하였다. 이를 통해 SQL Injection 공격 유형에 따른 발생량을 빠르게 분석할 수 있다.



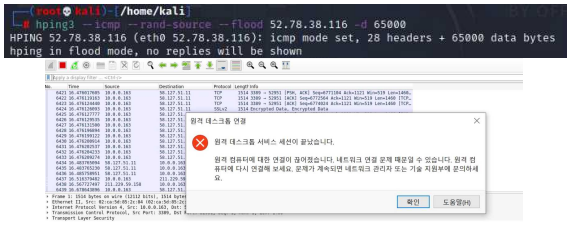
(그림 5) ELK 분석 및 Kibana 필터링을 통한 시각화

2.5.2 DoS 공격

서비스 거부 공격(DoS)은 시스템을 악의적으로 공격해 해당 시스템의 리소스를 부족하게 하여 정상적으로 서비스할 수 없도록 가용성을 떨어뜨리는 공격이다.

가. Ping of Death 공격

Ping of Death 공격은 규정 이상 크기의 ICMP 패킷을 공격 대상에게 전송해 시스템을 마비시키는 공격이다. 크게 만들어진 패킷은 공격 대상 네트워크에 도달하는 동안 작은 조각으로 쪼개져 수신측에서 다시 재집합한다. 재집합 과정에서 큰 패킷 사이즈로 인해 버퍼 오버플로우가 발생하고 라우터 성능에 높은 부하를 야기한다. 모의 공격 수행 시 약 3초 후에 버퍼 오버플로우가 발생하였다.

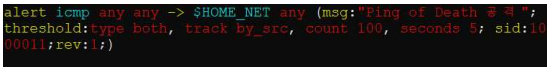


(그림 6) 공격 수행 시 버퍼 오버플로우 발생

Kibana에서 시각화한 그래프를 분석한다. 그 결과 일반적으로 5초당 100개 이하의 패킷이 들어온 반면, 버퍼 오버플로우 발생 직전에는 5초 내로 200개 이상의 ICMP 패킷이 들어온 것을 알 수 있다.

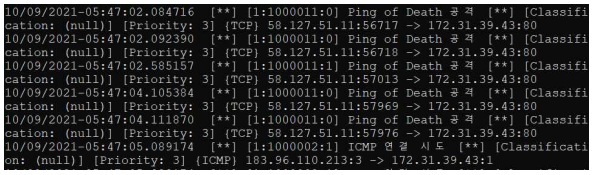
(그림 7) ELK를 활용한 Ping of Death 공격 분석

threshold 옵션을 이용하여 특정 네트워크에서 5초 내로 100개의 과도한 패킷을 보낸다면 Ping of Death 공격으로 탐지하는 Suricata rule을 작성한다.



(그림 8) Suricata rule 작성(Ping of Death)

클라우드 서버에 모의 공격 수행 시 침입 탐지 시스템이 정상적으로 악의적인 패턴을 탐지하는지 실험을 진행한다. 그 결과 Suricata에서 실시간으로 공격을 탐지하여 다음과 같이 출력했다.



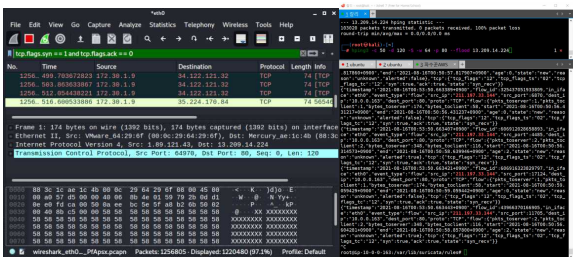
(그림 9) Suricata 공격 탐지 로그

나. TCP SYN Flooding 공격

TCP SYN Flooding 공격은 DoS 공격의 대표적인 공격 유형 중 하나이다. TCP SYN Flooding 공격은 3-Way-Handshake의 취약점을 이용한다. 공격 대상에서 SYN 연결 요청만 보내고 응답을 보내지 않으면 공격 대상은 연결 요청에 LISTEN 상태를 일정 시간 동안 유지한다. 따라서 TCP의 연결 가능한 자원을 모두 소진하고 외부 사용자는 TCP 연결

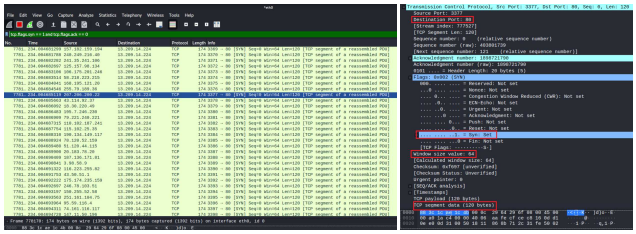
을 할 수 없게 된다.

hping3으로 공격 대상에게 무분별한 SYN 패킷을 전송하여 TCP SYN Flooding 공격을 수행한다.



(그림 10) TCP SYN Flooding 공격 과정

Wireshark에서 패킷을 필터링하고 분석한 결과는 다음과 같다. 과다한 SYN 패킷이 발생되는 것을 볼 수 있으며 모두 TCP 패킷의 Flags 값으로 S를 저장하고 있다.



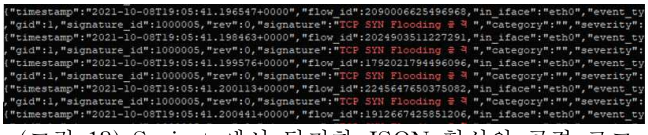
(그림 11) Wireshark 패킷 분석

TCP 프로토콜을 이용하고 80번 포트를 목적지로 하는 패킷 중 flags 값이 S로 설정되어있고 1초당 10개의 SYN 패킷이 발생되면 TCP SYN Flooding 공격으로 탐지하는 Suricata rule을 작성한다.

```
alert tcp any any -> $HOME_NET 80 (msg: "TCP SYN Flooding 공격 ";
flags:S; flow: stateless; threshold:type threshold, track by_dst,
 count 10 seconds 1; sid:1000005;)
```

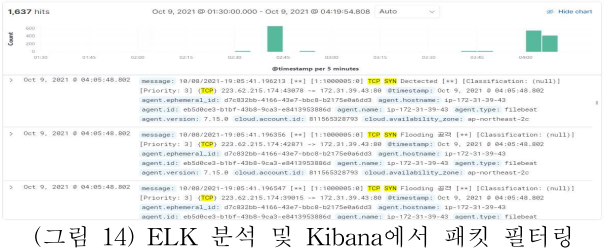
(그림 12) Suricata rule 작성(TCP SYN Flooding)

클라우드 서버에 모의 공격을 수행하고 Suricata가 악의적인 패킷을 탐지하는지 확인한다.



(그림 13) Suricata에서 탐지한 JSON 형식의 공격 로그

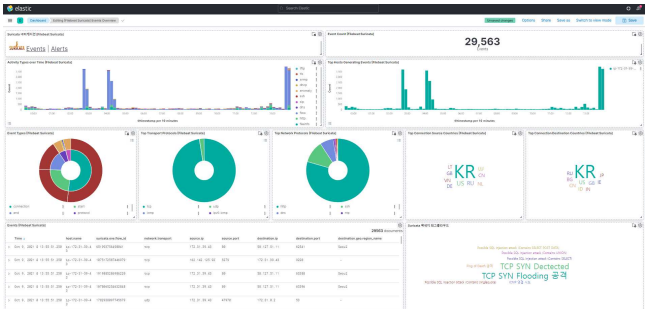
Kibana에서 SYN 패킷을 필터링하여 분석한다. 1초 이내에 200개 이상의 TCP SYN 패킷이 발생하였으며 Suricata에서 수립한 rule로 인해 TCP SYN flooding 공격을 탐지 및 차단 가능하며 Elastic stack을 이용해 실시간 공격 분석이 가능하다.



(그림 14) ELK 분석 및 Kibana에서 패킷 필터링

2.6 로그 데이터 시각화

시나리오 공격을 수행하여 수집한 로그 데이터를 Kibana로 시각화한 결과이다. 이로써 보안 이벤트 및 시스템 로그를 실시간으로 모니터링하고 분석, 대응할 수 있다.



(그림 15) Kibana 로그 데이터 시각화

3. 결론

본 논문에서는 DVWA, 클라우드 서버에 모의 공격을 수행하여 Wireshark로 패킷을 수집, 분석하고 분석 결과를 기반으로 공격을 탐지 및 차단하는 정책을 Suricata에 등록하였다. 정책을 통해 로그를 수집하고 ELK를 이용해 공격 이벤트를 분석하여 시각화하였다. 네트워크 모니터링과 분석, 대응이 실시간으로 가능한 보안관제 로그 분석시스템을 구축함으로써 공격으로부터 유의미한 데이터를 도출해 공격을 탐지 및 차단하고 앞으로의 공격을 대비할 수 있다. 향후 연구 방향으로는 패킷 간의 연관 관계를 분석하고 AI 알고리즘을 적용하여 네트워크 비정상 행위를 탐지할 수 있는 보안 시스템을 연구할 예정이다.

참고문헌

[1] 이상우, “코로나19 이후 인터넷 트래픽 30% 증가... 공격자는 이 혼란을 노렸다”, 보안뉴스, 2021.03.11.

[2] KISA, 2021년 사이버 위협 동향 보고서, 2021.07

[3] 이제국, 조인준, “다중 검색엔진을 활용한 보안관제 모델 개선방안”, 한국콘텐츠학회논문지 21(1), pp284-291, 2021

[4] 정명기, 안성진, 박원형 “Snort와 Suricata의 탐지 기능과 성능에 대한 비교 연구”, 융합보안 논문지 제14권 제5호, 2014. 09

- 본 논문은 과학기술정보통신부
정보통신창의인재양성사업의 지원을 통해
수행한 ICT멘토링 프로젝트 결과물입니다 -