# Suricata, iptables, OSSEC, Elastic Stack을 활용한 실시간 공격 탐지 및 차단 : 통합 보안 솔루션 구축

서지윤[1], 오승준[2], 장휘영[3], 임정락[3]
[1]이화여자대학교 스포츠과학과
[2]한신대학교 정보통신학과
[3]동의대학교 정보통신공학과
[1]1210ji1210@gmail.com,[2]dhtmd009@naver.com,[3]{gnldud15,koreaman159}@naver.com

# Real-Time Threat Detection and Prevention with Suricata, Iptables, OSSEC, and the Elastic Stack

Seo Ji-Yun[1], Oh Seung-Jun[2], Jang Hwi-Young[3], Lim Jeong-Rak[3]
[1]Dept. of Sports Science, Ewha Womans University
[2]Dept. of Information and Communication, Hanshin University
[3]Dept. of Information and Communication Engineering, Dong-Eui University

요 약

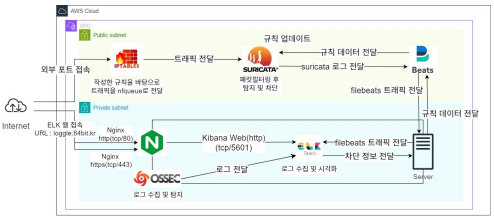
최근 사이버 공격의 급증으로 기존 보안 솔루션의 한계가 드러나고 있다. 본 논문에서는 Suricata, iptables, OSSEC를 통합하여 사이버 공격을 실시간으로 탐지하고 적시에 차단하는 효율적인 보안 솔루션을 제안한다. 또한 Elastic Stack을 활용하여 로그 데이터를 분석 및 시각화하여 보안 상황을 직관적으로 파악하고 신속한 대응을 가능하게 한다. 모의 공격 시나리오를 통해 시스템의 성능을 평가하였으며, 그 결과 본 솔루션이 네트워크와 시스템의 보안을 강화하고 운영 효율성을 향상시킴을 확인하였다.

## 1. 서론

최근 사이버 공격의 빈도는 대기업뿐만 아니라 중소기업, 1인 기업, 인터넷 방송인 등 일반인에게까지 확대되고 있으며, 그 심각성이 매년 커지고 있다. 대기업은 방어 시스템이 잘 갖춰져 있는 편이지만, 개인과 소규모 기업은 기초 보안만으로는 효과적인 대응이나 분석이 어려워 공격자의 주요 표적이 될 수 있다. 본 연구는 이러한 문제를 해결하기 위해 Suricata, iptables, OSSEC, Elastic Stack을 통합하여 사이버 위협을 실시간으로 탐지하고 적시에 차단하는 보안 솔루션을 개발하는 것을 목표로 한다. 이 솔루션은 AWS 클라우드 환경에서 Public, Private으로 시스템을 분리하여 보안성과 성능을 최적화하였다.

## 2. 본론

### 2.1 S/W 주요기능 및 연구 흐름도




(그림 1) 연구 흐름도

본 시스템에서 Public은 Suricata가 외부 트래픽을 모니터링하고, iptables가 위협을 차단하며, Beats는 Suricata의 로그 데이터를 ELK 스택으로 전달한다. Private 에서는 OSSEC이 비정상 활동을 감지하고, Logstash가 데이터를 처리한다. Elasticsearch는 로그 데이터를 저장·검색하며, Kibana는 이를 시각화해 Suricata의 실시간 수집된 데이터로 보안 상황을 쉽게 파악할 수 있게 한다. TLS 1.3과 SSL/TLS로 데이터 전송 보안을 강화하고, Elasticsearch 로그는 AES-256으로 암호화된다. 그림 1은 Suricata와 iptables가 트래픽을 실시간 모니터링·대응하는 과정을 보여준다.

### 2.2 시나리오

초기 단계에서는 시스템이 외부에서 발생하는 다수의 자동화된 봇 공격을 인지하지 못하거나 방어하지 못하는 취약한 상황을 가정하였다. 1차 목표는 이러한 자동화된 공격을 실시간으로 탐지하고 대응하는 것이었으며, 이후 2차 목표는 실제 악의적인 해커가 이러한 공격을 발판으로 시스템에 침입하려는 시도를 설정하였다. 이 단계에서는 해커의 침입 시도를 탐지하고 즉각적으로 차단하는 효과를 확인하였다.

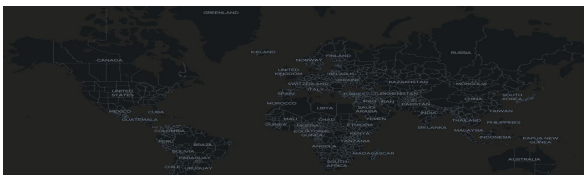
### 2.3 연구 결과

#### 가. Suricata


(그림 2) Suricata rule 작성

Suricata는 네트워크의 주요 프로토콜인 ICMP와 SSH에 대해 맞춤형 suricata.rules를 생성하여 외부 네트워크 연결 시도를 효과적으로 모니터링하고 탐지한다. ICMP는 네트워크 스캐닝과 시스템 접근 확인에 자주 사용되며, SSH는 원격 접속의 주요 채널로 활용된다. 이를 통해 발생하는 잠재적 위협을 탐지하고 방어하는 데 중요한 역할을 수행한다.

### 나. Kibana(GeoIP)



(그림 3) Suricata에서 탐지한 IP 위치표기

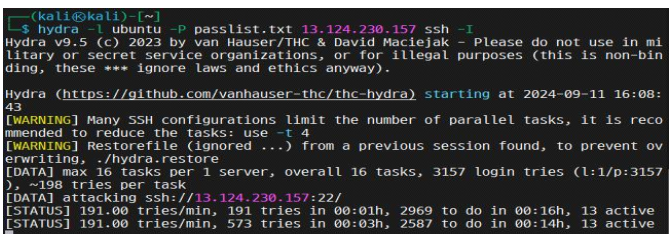
Kibana 대시보드에서 GeoIP는 외부에서 공격하는 IP 출처와 집중 지역을 시각적으로 파악할 수 있다. 이를 바탕으로 특정 지역에서 발생하는 위협에 대한 정확한 대응 전략을 수립할 수 있다.

### 다. DDoS 공격(ICMP Flooding)


(그림 4) 외부(미국IP, 홍콩IP)에서의 ICMP Flooding공격

Suricata를 통해 분석한 결과, 여러 외부 IP에서 다수의 ICMP 요청이 확인되었으며, 특정 IP는 2,652회의 패킷을 보냈다. 이는 전형적인 DDoS 패턴으로, ICMP Flood를 통해 서버 자원을 소진시키고 서비스 거부 상태를 유발하려는 시도로 분석된다.

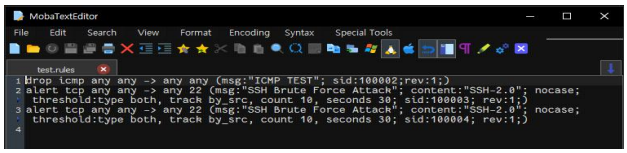
### 라. SSH 사전 대입 공격




(그림 5) Kali에서의 SSH 사전 대입 공격과정

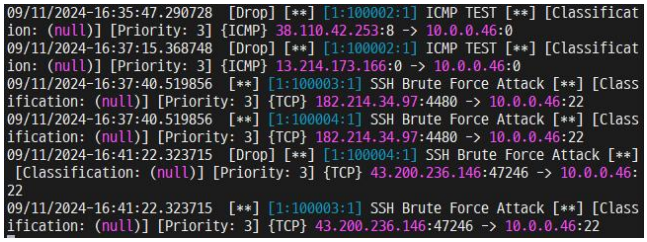
Kali Linux에서 Hydra를 이용해 SSH 사전 대입 공격을 시도하였으며, 3,157개의 로그인 시도를 통해 시스템의 보안 취약성을 검증하였다.

### 마. 침입 방지 시스템(IPS)




(그림 6) ICMP실시간 차단

Suricata의 IPS 기능을 활성화하여, 탐지된 악의적인 IP 트래픽을 실시간으로 차단하는 시스템을 구현하였다. IDS에서 수집된 IP를 기반으로, Suricata의 rules 파일에서 drop 규칙을 적용해 ICMP Flooding의 외부 위협을 자동으로 차단하였다.




(그림 7) SSH 사전 대입 공격 실시간 차단

Suricata는 다수의 SSH 로그인 시도를 실시간으로 탐지하고, Drop 규칙을 적용하여 악의적인 트래픽을 차단하였다. 이는 공격이 감지된 즉시 대응이 이루어져 시스템 자원을 보호할 수 있었음을 보여준다.

## 3. 결론

본 연구에서는 Suricata, iptables, OSSEC, Elastic Stack을 통합하여 다양한 사이버 공격을 탐지하고 차단하는 보안 솔루션을 구현하였다. SSH 사전 대입 공격 및 ICMP Flooding 시나리오를 통해 실시간 위협을 탐지하고 차단하는 효과를 입증하였다. 이러한 공격은 눈에 보이지 않게 지속적으로 발생할 수 있어 실시간 탐지 시스템의 중요성이 매우 크다. 탐지 시스템이 없으면 공격을 인지하지 못할 수 있으므로, 실시간 위협 감지 및 대응이 가능한 보안 시스템 구축이 필수적임을 확인하였다. 또한, AWS KMS를 통해 암호화 키를 주기적으로 갱신하고, 정기적인 보안 감사와 모니터링으로 시스템 보안을 강화하였다.

## 참고문헌

[1] 과학기술정보통신부 한국인터넷정보원(2024), 2024 사이버보안 위협과 분석 및 전망(1p)

[2] 이다은, 이혜린, 조민규, "Suricata와 Elastic Stack, Kafka를 이용한 공격 패킷 분석 및 보안관제 시스템 구축" ACK 2021년 논문집(28권 2호 1144p)

※ 본 논문은 과학기술정보통신부
대학디지털교육역량강화 사업의 지원을 통해
수행한 ICT멘토링 프로젝트 결과물입니다.