Open IDS 및 CVE 기반의 OpenIOC가 결합된 CTI 프레임워크 설계

윤경찬, 유지훈, 신동일, 신동규
세종대학교 컴퓨터 공학과
keoungchan@gamil.com, yoojihoon@sju.ac.kr, dshin@sejong.ac.kr, shindk@sejong.ac.kr

Design of CTI framework that combines Open IDS and CVE based OpenIOC

Keoungchan Yoon, Jihoon Yoo, Dongkyoo Shin
*Dept. of Computer Engineering, Se-jong University

요 약

정보통신 기술의 발달로 무분별한 사이버 공격에 노출되어 있기 때문에 정보보안의 기술이 중요해지고 있다. 이중 침입 탐지 시스템은 방화벽과 더불어 시스템 및 네트워크 보안을 위한 대표적인 수단으로, 현재까지 네트워크 기반인 NIDS와 호스트 기반인 HIDS에 대한 많은 연구가 이루어졌다. 이러한 침입탐지에 대한 CTI(Cyber Threat Intelligence)를 공유하기 위해 다양한 CTI 프레임워크를 사용하여 CTI 정보를 공유하는 연구가 진행되고 있다.

이에 본 논문에서는 CVE기반의 OpenIOC와 Snort 및 OSSEC에서 생성된 Raw Data를 결합하여 새로운 CTI 프레임 워크를 제안한다. 제안된 시스템을 테스트하기 위해서는 CVE 분석을 기반으로한 Kali Linux로 공격을 진행한다, 이를 통해 생성된 데이터는 시간이 지남에 따라 축적된 데이터를 저장 및 검색을 위해 대규모 분산 처리 시스템과도 결합이 필요할 것으로 예상되며 추후 딥러닝 기술을 활용하면 지능형 지속 위협을 분석하는데 용이할 것으로 예상된다.

1. 서론

전 세계적으로 인터넷이 활성화 된 21세기는 정보통신 기술의 발달로 무분별한 사이버 공격에 노출되어 있기 때문에 정보보안기술이 더욱 중요해지고 있다. 이에 따라 정보보호 서비스 및 보호 기술에 대한 수요가 확대되고 있으며, 이중 침입탐지 시스템(IDS, Intrusion Detection System)은 방화벽(Firewall)과 더불어 시스템 및 네트워크 보안을 위한 가장 대표적인 수단이다. 침입 탐지 시스템은 네트워크 기반의 NIDS(Network based Intrusion Detection System)와 호스트 기반인 HIDS(Host based Intrusion Detection System)으로 구분되며, NIDS의 경우 네트워크 공격인 DoS, Port Scan 등의 네트워크 트래픽 공격 탐지와 관련해서 많은 연구가 주를 이룬다 [1, 2]. 이에 반해 호스트 기반의 HIDS는 시스템 내부에서 발생되는 시스템 호출, 이벤트 로그 등의 시스템 내부 행위 및 로그에 대한 분석을 통해 이상 여부를 탐지한다. 이와 더불어 사이버 공격에 대한 위협정보를 공유하기 위해 CTI(Cyber Threat Intelligence)플랫폼을 사용하여 최신의 공격과 기존 운영 체제의 취약성에 관련된 위협 정보를 수집 및 분석하여 공유하는 연구가 진행되고 있다 [3].

본 논문에서는 Raw Data와 OpenIOC가 결합된 CTI 프레임워크를 제안한다. 이 프레임워크는 CVE(Common Vulnerabilities and Exposures)기반의 OpenIOC와 연관된 오픈 IDS(Snort, OSSEC) 규칙을 설정하고, 해당 원시(Raw) 데이터를 생성하기 위해서 위협 도구로 Kali Linux를 사용한다.

2. 관련 연구

Satyendra Kumar Patel, Abhilash Sonker 는 네트워크 보안을 개선하기 위해 규칙 기반의 Snort을 제안하였다. 해당 연구에서는 Port Scan 공격을 실시간을 감지하기 위해 자체적으로 EPSDR (Efficient Port Scan Detection) 규칙을 생성하였다. 이러한 새로운 EPSDR 기반 IDS는 새로운 오탐을 줄이는 데 좋은 성과를 달성했다 [4].

RaviTeja Gaddam ,Dr. M. Nandhini는 Snort를 통해 생성된 대량의 트래픽을 처리하기 위하여, 여러 가지 문제를 극복하기 위해 즉각적인 정보에 반응하는 계층 기반 설계를 구상하였다. 이 설계를 통합하기 위하여 Snort 코드를 재구성 한 다음 Kali Linux 환경에 수정된 Snort를 배포하여 성능 평가를 진행하는 방식을 제안하였다 [5].

Guangming Yang 외 3명은 트래픽이 많이 발생되는 네트워크 환경에서 침입 탐지의 효율성을 높이기 위해 시그니처 커스텀 마이징 방법을 제안하였다. 이 방법은 취약성 스캐너, 상태보고서, 서명 선택, 호스트로 구성되고 CVE번호 선택과 포트 선택의 방식으로 구성된다. 해당 연구에서는 불필요한 경고를 줄이고 탐지 효율을 향상시킨 것을 볼 수 있었다 [6].

3. CTI 프레임워크 구성

본 연구에서 제안한 CTI 프레임워크 구성은 그림 1에 나타내었으며, 핵심 어플리케이션은 아래에서 설명한다. CVE기반의 OpenIOC와 연관된 공개 IDS(Snort, OSSEC) 규칙을 설정하고, 해당 원시 데이터를 생성하기 위해서 위협 도구로 Kali Linux를 사용하며, 원시 데이터 및 관련정보를 Anomali STAXX에 축적하여 CTI Feed를 구성한다.

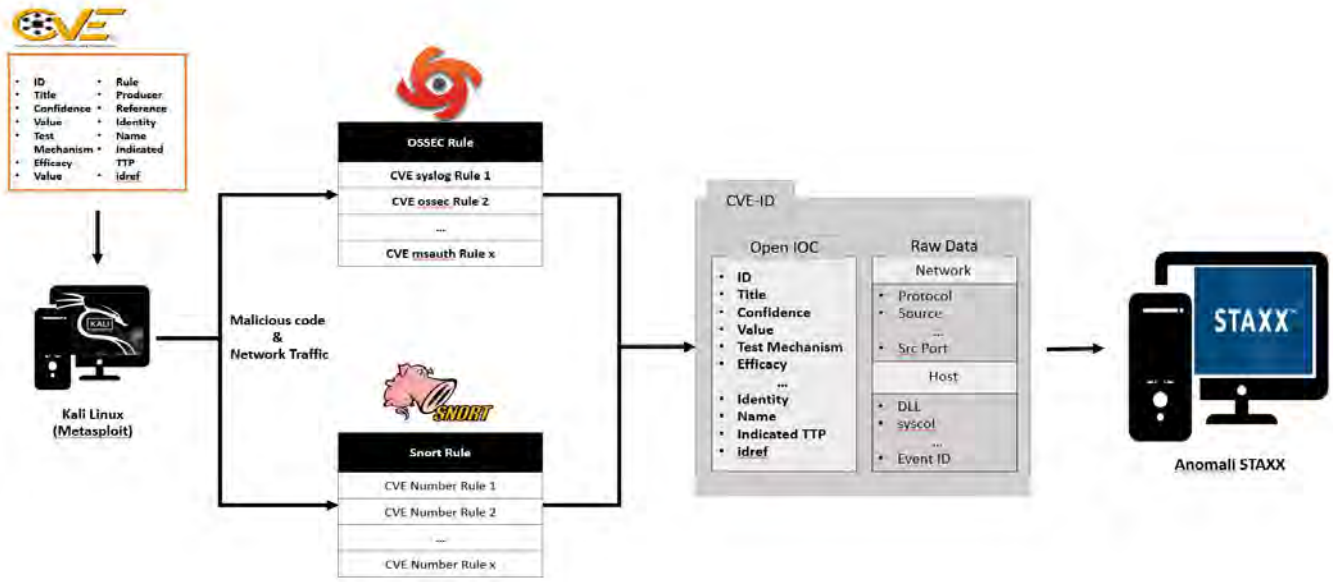
3.1 CVE (Common Vulnerabilities and Exposures)

CVE는 알려진 취약점을 식별하는 방식을 표준화하는 것으로 표준 ID를 통해 다양한 CVE 정보 소스에서 특정 위협에 대한 기술적 정보를 찾아 활용하는데 사용한다. CVE의 구성요소를 그림 2에 나타내었다. 본 논문에서는 Snort와 OSSEC에서 나온 RAW데이터와 CVE 기반의 OpenIOC를 매핑시키는 것이 목표이다.

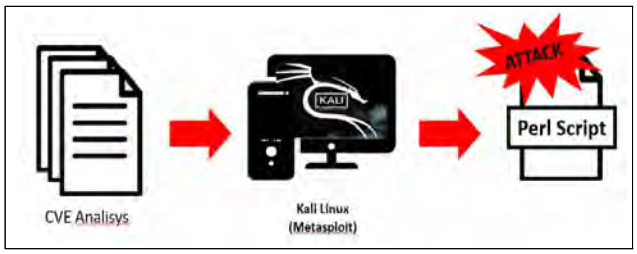
(그림 2) CVE 구성요소

3.2 Kali Linux(Metasploit)

Kali Linux는 침투 테스트를 위해 만들어진 데비안 계열의 리눅스로, 취약점과 관련한 모든 메타 데이터를 관리하는 프레임워크인 MetaSploit를 통해 보안 취약점 분석에 많이 사용된다. 본 연구에서는 이 MetaSploit 및 Perl Script기반의 취약점 공격을 통해 Open IDS에 원시 데이터를 생성하는데 사용한다. 그림 3은 Kali Linux의 취약점 공격 구조를 나타낸다.



(그림 1) 제안된 프레임 워크 흐름도



(그림 3) Kali Linux의 취약점 공격 구조

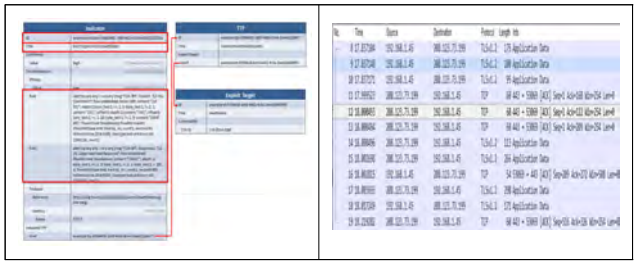
3.3 OSSEC (Open Source HIDS Security)

OSSEC는 오픈 소스 기반의 호스트 침입탐지 시스템이다. OSSEC는 로그를 분석 가능한 로그 분석 엔진이 있고, 중앙 집중식 아키텍처로 구성된 플랫폼이기 때문에 여러 시스템을 관리하기 용이하다. 본 연구에서는 호스트 기반 침입 탐지에서 발생될 수 있는 원시 데이터를 CVE와 매핑시키는 것이 목적이다.

(그림 4) OSSEC 구성요소

3.4 Snort

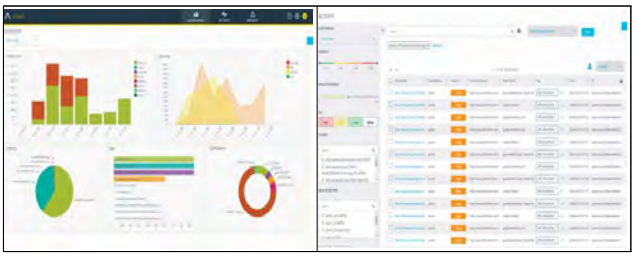
Snort는 실제 취약점 탐지를 기반으로 하고 IP 네트워크에서 프로토콜 분석 실시간 트래픽 분석 작업 등을 수행하여 다양한 공격을 탐지하는 네트워크 기반의 침입 탐지 시스템이다. 본 연구에서는 Snort Rule을 활용해 CVE 분석을 기반으로 생성된 Kali Linux의 공격을 스캔하여 축적된 Raw Data와 CVE 기반의 OpenIOC와 매핑을 시키는 것이 목표이다.



(그림 5) Snort Rule

3.5 Anomali STAXX

Anomali STAXX는 STIX/TAXII 서버에 연결하여 위협 피드를 발견 및 구성하고 위협 정보를 폴링 가능하게 한다. 또한 사용자에게 IOC(Indicator of Compromis)연구 도구를 제공한다. 본 연구에서는 CVE 기반의 데이터와 OSSEC 및 Snort가 매핑된 데이터를 Anomali STAXX에 정보를 축적하여 CTI Feed를 구성하는 것이 목표이다.



(그림 6) Anomali STAXX

4. 결론

본 연구를 통해서 OSSEC 및 Snort에서 생성된 Raw Data와 CVE 기반의 OpenIOC를 매핑한 CTI를 축적할 수 있는 프레임 워크를 제안할 수 있었다. 제안된 프레임 워크는 시간이 지남에 따라 축적된 CTI정보들을 처리하기 위해서 대규모 분산 처리 시스템을 통해 효율적인 저장 및 검색을 필요 할 것으로 예상하며, 추후 축적된 데이터를 딥러닝 기술을 이용하여 지능형 지속 위협(APT, Advanced Persistent Threat)을 분석 하는데 활용 가능할 것으로 예상한다.

ACKNOWLEDGMENT

"본 연구는 국방과학연구소의 지원으로 수행되었습니다(위탁연구계약번호:UD200014ED)"

참고문헌

[1] ROESCH, Martin, et al. Snort: Lightweight intrusion detection for networks. In: Lisa. 1999. p. 229-238.

[2] SABOOR, Amtul; AKHLAQ, Monis; ASLAM, Baber. Experimental evaluation of Snort against DDoS attacks under different hardware configurations. In: 2013 2nd National Conference on Information Assurance (NCIA). IEEE, 2013. p. 31-37.

[3] KIM, Eunsoo, et al. CyTIME: Cyber Threat Intelligence ManagEment framework for automatically generating security rules. In:

Proceedings of the 13th International Conference on Future Internet Technologies. 2018. p. 1-5.
[4] PATEL, Satyendra Kumar; SONKER, Abhilash. Rule-based network intrusion detection system for port scanning with efficient port scan detection rules using snort. International Journal of Future Generation Communication and Networking, 2016, 9.6: 339-350.
[5] GADDAM, RaviTeja; NANDHINI, M. An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment. In: 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE, 2017. p. 10-15.
[6] YANG, Guangming, et al. Research of intrusion detection system based on vulnerability scanner. In: 2010 2nd International Conference on Advanced Computer Control. IEEE, 2010. p. 173-176.