취약점 점수를 활용한 패턴 기반 IDS 검출 내용 정제 방법

김종범 [1], 정지환 [2], 최성곤 [2*]
[1] 엑사비스㈜, 충북대학교 [2]

jbkim@xabyss.com, dean987@naver.com, *choisg@cbnu.ac.kr

A Pattern-based IDS detection refining method using vulnerability score

Kim Jong Beom[1], Jeong Ji Hwan[2], Seong Gon Choi[2]
[1]Xabyss inc., [2]Chungbuk Univ.

요 약

기존 패턴 기반 IDS 를 활용하는 환경에서, 기존 방법 사용 시 과도하게 검출 로그가 많이 발생하여 보안 이벤트 식별이 쉽지 않은 문제가 존재한다. 본 논문에서는 사용자가 중요한 보안 이벤트를 더욱 손쉽게 식별하도록 하기 위해 CVE(Common Vulnerabilities and Exposures)의 점수를 이용하여 불필요하게 많이 식별되는 검출 로그를 정제하였고, 이를 통해 보안 담당자가 중요 보안 이벤트를 손쉽게 식별할 수 있다.

Ⅰ. 서 론

본 논문에서는 기존 네트워크 보안장비의 일종인 IDS, 그 중 패턴 기반의 IDS 를 사용하는 환경에서 발생하는 보안 이벤트 식별에의 불편을 해결하기 위해 취약점 점수를 활용하였다.

기존 패턴 기반 검출 환경에서는 검출을 위한 패턴에 일치하게 되면 검출 내용의 중요도 및 심각성과 상관없이 모든 내용을 검출 메시지로 출력한다. 따라서, 하루 수많은 검출 메시지가 발생하는 네트워크 환경에서는 중요한 취약점 발생 여부와 그렇지 않은 사소한 접근 알림 등을 분류하여 점검하기 쉽지 않아 추가적인 분류 작업이 필요한 문제가 존재한다.

따라서, 본 논문에서는 이러한 문제를 해결하기 위해 CVE(Common Vulnerabilities and Exposures)에 매겨진 점수를 활용하여[1] 검출 내용을 취약점 점수를 참조해 위험도에 따라 구분하여 정제하였으며, 이를 통해 중요한 보안 취약점 관련 이벤트만을 확인할 수 있도록 하였다.

Ⅱ. 본 론

최근 네트워크 보안에 대한 관심이 높아지며 다양한 네트워크 보안 시스템들이 등장하고 많은 보안 관리자들이 실제 네트워크에 보안 시스템을 적용하고 있다. 또, 2020 년부터 코로나에 의해 시작된 원격근무 문화로 인한 원격 접속 환경에서의 보안 취약점을 악용한 공격이 다수 발견되며, 기업 등 근무환경 내의 네트워크 보안에 대한 필요성이 대두되었다.

원격근무로 인하여 네트워크 구조 또한 서서히 변화되어, 사내 인트라넷으로 업무를 진행하던 이전과는 다르게 네트워크 외부에서 원격 접속을 통해 내부로 접근해 업무를 진행하는 사례가 많아졌다. 이런 변화에 맞추어, 네트워크를 공격하기 위한 시도 또한 원격 접속 트래픽을 노리는 공격으로 그 트렌드가 서서히 변화되었다. 이러한 비정상적인 트래픽을 차단하고 방어하기 위하여 트래픽의 이상 유무를 파악하는 네트워크 보안 장비들이 다수 기업에서 도입되었다[2].

전통적으로 네트워크에 설치되어 보안 위협을 검사하기 위한 보안 장비 중 트래픽의 이상 유무를 식별하기 위해 IDS 를 많이 사용한다. IDS 는 침입 탐지 시스템(Intrusion Detection System)의 준말로, 트래픽 내의 위협 유무를 탐지하는 보안장비이다. IDS 는 크게 패턴 기반 IDS 와 이상행위 기반 IDS 로 분류된다.

이 중 패턴 기반 IDS 는 시그니처 기반 IDS 라고도 불리며, 미리 지정된 패턴(Indicators of Compromise, IoC)과 네트워크 트래픽을 비교하며 패턴에 일치하는 내용을 찾아내는 방식으로 위협을 찾아내는 IDS 를 말한다. 지정된 패턴에는 네트워크 공격에 사용되는 문자열, 악성 파일로 보고된 해시, 악의적 활동을 하는 것으로 식별된 도메인 정보 등이 포함될 수 있다.

패턴 기반 IDS 의 경우 모든 트래픽을 모니터링하는 특성 때문에 In-line 방식의 IDS 뿐만 아니라 미러링되어 저장된 트래픽의 회귀검사용으로 적합하며, 이는 실시간 네트워크 보안장비단에서 처리하지 못하고 통과된 트래픽들을 재검사하는데 주로 사용된다[3].

패턴 기반 IDS 는 패킷을 순차적으로 모두 검사하며 보유하고 있는 모든 패턴 중 일치하는 것이 있는지를 확인한다. 이러한 특성 때문에 위험도가 높은 취약점 뿐만 아니라 단순 접근 감지 등의 보안 이벤트 등도 식별되어 검출되는 보안 이벤트가 많고, 따라서 보안 이벤트 중 위험도가 높은 취약점을 파악하는 데 불편함이 있다는 단점이 있다.

이를 해결하기 위해 본 논문에서는 기존 패턴 기반의 IDS 를 사용해 보안 이벤트를 검출하고 있는 환경에, 취약점 데이터베이스인 CVE(Common Vulnerabilities and Exposures) 데이터베이스에 포함된 취약점의 점수를 적용하여 검출되는 보안 이벤트의 위험도에 따라 그 표시를 정제하는 방법을 제안한다.

Ⅲ. 기술 구현 및 검증

실제 패턴 기반의 IDS 를 활용하고 있는 네트워크 환경에서, 본 논문이 제안하는 방법을 적용하기 이전의 보안 이벤트 종류의 수와 적용한 이후의 보안 이벤트

종류의 수를 비교하여 실제 보안 담당자가 얼마나 효율적으로 보안 이벤트를 식별할 수 있는지를 확인할 것이다.

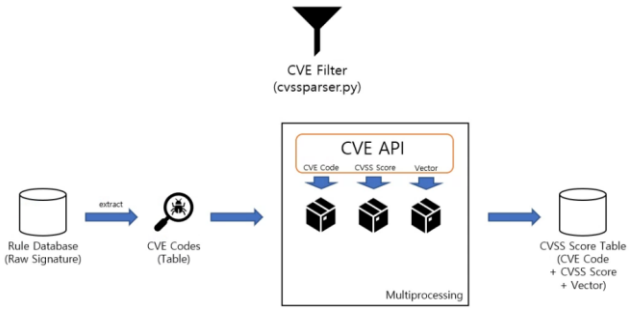
기술 구현은 한국지능정보사회진흥원(NIA)가 제공하는 초연결 지능형 연구개발망(KOREN)을 활용하며, 해당 망에서 발생하는 다수의 보안 위협이 포함된 실험용 트래픽을 패턴 기반의 IDS 로 검사할 것이다[4].

검사에 활용할 패턴 기반의 IDS 는 Suricata 를 사용한다. Suricata 는 Snort 를 계승한 오픈 소스 IDS 엔진이며, inline 기능을 통해 IPS 로도 동작할 수 있다. 또한, 실시간 트래픽 모니터링 외에 오프라인에 pcap 형태로 저장된 트래픽 또한 검사할 수 있어 동일한 패킷을 재검사할 때 유용하다[5]. 본 논문에서는 동일한 패킷을 재검사할 때 보여지는 보안 이벤트의 종류를 비교하기 때문에 Suricata 를 사용하는 것이 적합하다.

패턴 기반 IDS 에서 트래픽을 검사하기 위해서는 탐지를 위한 패턴이 포함된 탐지룰이 필요하다. 본 논문에서는 취약점뿐만 아니라 기타 보안 이벤트 또한 검출하기 위해 약 6 만개의 패턴을 포함하는 proofpoint 社의 Emergingthreats Pro 탐지룰 세트를 사용할 것이다[7].

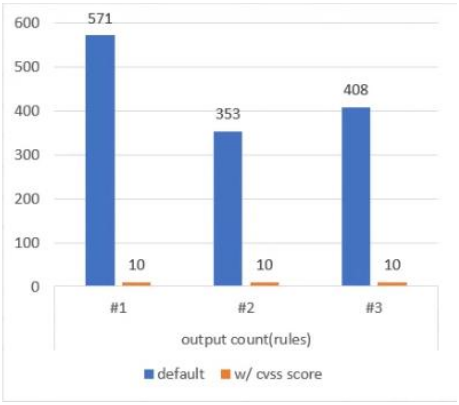
구현 기술을 검증하기 위해 KOREN 네트워크에서 1 일간 네트워크 트래픽을 수집하고, 해당 네트워크 트래픽을 Suricata IDS 로 검사한 결과와 본 논문에서 제안하는 기술을 적용한 후의 검사 결과를 비교할 것이다.

취약점 점수 정보를 IDS 에서 활용하기 위해, CVE Database 로부터 CVSS Score(취약점 점수)를 획득하여야 한다. 이를 위해 CVSS Score 를 파싱하여 DB 에 저장하는 아래 <그림 1>의 구조를 가진 python script 를 작성하였다.



<그림 1> CVSS parser script 동작 구조

CVSS parser script 로 취약점 점수를 수집한 뒤, 1 일간 수집하여 검사가 이미 진행되었던 네트워크 트래픽을 재검사하고 취약점 점수를 반영하여 보안 이벤트의 종류를 정제한 뒤 그 양을 비교하였다.



<그림 2> 보안 이벤트 종류 수 비교

<그림 2>는 취약점 점수를 통한 검출 내용 정제 방법을 적용한 결과를 나타낸다. 매일 수백건 이상 발견되던 보안 이벤트가 방법 적용 이후 10 건으로 줄어들어 보안 담당자가 실제 위험도가 높은 보안 이벤트만을 빠르게 식별하고 확인할 수 있게 된다.

Ⅳ. 결론

본 논문에서는 패턴 기반의 IDS 에서 발생하는 보안 이벤트를 취약점 점수에 따라 분류하여 검출 내용을 그 위험도에 따라 분류하여 제공하는 방법을 제안하였다.

제안하는 방법을 통해 기존 수백가지 이상의 보안 이벤트가 발생하는 네트워크 환경에서, 위험도가 높은 취약점 정보를 추려 사용자에게 제공함으로써 보안 담당자가 불필요하게 많이 출력되는 검출 로그를 전부 확인할 필요 없이 중요 보안 이벤트만을 손쉽게 식별할 수 있다.

본 논문에서 제안하는 방법을 적용하면 SIEM 등의 타 보안장비와 연결하여 보안 위협을 모니터링하는 과정에서도 또한 조금 더 정교한 메시지 로그를 수집하여 활용함으로써 오탐 및 과탐을 감소시킬 수 있으며, 보안 사고 발생 시에도 또한 간소화된 보안 이벤트 종류로 인해 침해 내용 파악/대응에 도움이 될 수 있을 것이다.

*교신저자: 최성곤(choisg@cbnu.ac.kr)

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 지역지능화혁신인재양성(Grand ICT 연구센터) 사업의 연구결과로 수행되었음" (IITP-2022-2020-0-01462). 또한, 이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(2019R1A2C1006167).

참 고 문 헌

[1] NIST, "Vulnerability Metrics," (https://nvd.nist.gov/vuln-metrics/cvss).

[2] KISA, "2022 년 상반기 사이버 위협 동향 보고서," 2022.

[3] Jang Hyeon Jeong et al, "Feedback System to Minimize Damage by Zero-Day High-Volume Attack based on NIDPS," 한국통신학회 학술대회논문집, 2020.

[4] NIA, "초연결 지능형 연구개발망 소개," (https://koren.kr).

[5] Suricata Official Webpage [Online], (https://suricata.io)

[7] proofpoint, "ET Pro Ruleset,"[Online], (https://www.proofpoint.com/us/threat-insight/et-pro-ruleset).