***규칙-기반 침입탐지(오용 침입탐지)***

- 시스템 로그, 네트워크 입력정보, 알려진 침입방법, 비정상적인 행위 패턴 등의

특징을 비교하여 탐지하는 방법이다.

- 기존의 침입방법을 데이터베이스에 저장해 두었다가 사용자 행동 패턴이 기존의

침입 패턴과 일치하거나 유사한 경우 침입이라 판단한다.

- 새로운 공격이나 침입 방법이 출현하였을 경우에 그에 맞는 공격 패턴을 생성하여 추가한다.

시그니처 예

- 루트(root) 사용자 이름으로 Telnet 로그인 시도

- 시스템 프로그램 복제 시도

- 패스워드 파일 복제 시도

장점

1. 오탐률(False Positive)이 낮음

2. 전문가 시스템(추론 기반 지식 베이스) 이용

3. 트로이목마, 백도어 공격 탐지 가능

단점

1. 새로운 공격 탐지를 위해 지속적인 공격 패턴 갱신 필요

2. 패턴에 없는 새로운 공격에 대해서는 탐지 불가능(Zero day Attack)

False Positive

- 합법적인 사용자를 침입자로 판단 (침입자의 행동을 높게 잡았을 경우)

- 침입이 아닌 합법적인 사용도 침입으로 오인

False Negatives

- 침입자를 합법적인 사용자로 판단(침입자의 행동을 좁게 잡았을 경우)

-침입을 하였는데도 침입인지 모름

저는 이 부분을 예를 들어 뭐든 행동을 하는 즉, 합법이든 불법이든 행동으로 잡았기에

False Positive로 생각 행동조차 하지 않으면 Negative로 외우고 있습니다.

보안에선 안 하는 것보다 일단 하는 게 나으니깐요.

또 저는 제로데이 공격 같은 경우 Postitive는 잡으니깐 이상 탐지

반대로 오용 탐지는 못 잡기 때문에 Positive가 낮고(융통성이 좋다고 생각)

그리고 오용 탐지 이렇게 외우고 있습니다.

최대한 외구기 쉽게요 나중에야 이제 개념이 완전히 정리가 되겠지만 이전에 외우려고 할 때는 잘 안되더라고요

이 부분이 Positive가 낮고 이상 탐지는 높고 이 부분이 잘 안 외워져서 이렇게 외웠습니다.

***통계적 변형(행위 기반) 탐지 (비정상 행위 침입탐지 / 이상 탐지)***

- 관찰된 사건들을 정상적인 행위에 대한 정의들과 비교하여 심각한 수준의

일탈 행위를 식별하는 과정

-- 시스템과 사용자의 정상적인 행위 패턴을 프로파일로 생성하고 시스템상에 행위가

프로파일 범위를 벗어날 경우 침입으로 탐지 정상적인 행위를 한 데이터를

기반으로 기준을 작성함(i/o사용량, 로그인 횟수, 패킷량 등등)

- 정량적인 분석, 통계적 분석 이용

장점

1. 인공지능 알고리즘 사용으로 스스로 판단하여 수작업의 패턴 업데이트 불필요

2. 오용 탐지 기법보다 데이터베이스 관리가 용이하고 알려지지 않은 공격

(Zero day Attack) 탐지가 가능

3. 침입 이외에 시스템 운용상의 문제점 발견할 수 있음.

단점

1. 오탐률(False Positive)이 높음

2. 정상과 비정상 구분을 위한 임계치 설정이 어려움

***대응방법***

1. 수동적 대응 방법

- 대량의 정보를 수집하는 형태를 취하거나 필요한 경우에 권한을 가진 사용자들에게

보다 엄격한 조치를 취할 수 있도록 통보하는 형태(대부분의 IDS가 사용)

- 주로 침입을 피하거나 무시하는 방법, 상세한 분석, 조치를 취할 수 있도록 도움이 되는

정보를 수집하는 이벤트 기록방법 또는 전자우편 SNMP 트랩 등을 이용하여 침입과 관련된

정보를 보안 관리자에게 보고하는 방법 등이 있다.

SNMP 트랩

- 만일 비정상적인 무엇인가를 찾아내면 관리자에게 경고 메시지를 송신하는 것

2. 능동적 대응 방법

- 침입에 대해 가장 빨리 실행할 수 있는 행동으로 침입에 대한 손실을 줄일 수 있게 함

- 신중한 고려와 정확한 검증이 없다면 혼란을 방생시키거나 서비스를 제공할 수 없는 오경보 발생.