**호스트 기반 IDS** : 하나의 호스트의 특성과 그 안에서 발생하는 이벤트들을 감시하면서 의심가는 활동을 탐지 해낸다.

**​**

**네트워크 기반 IDS :** 네트워크 특정 세그먼트에서 관찰되는 네트워크 트래픽을 감시하고 네트워크, 전송 , 응용 프로토콜을 분석함으로써 이상활동을 탐지해낸다.

​

**분산 또는 하이브리드 IDS** : 센서들과 호스트 와 네트워크 기반 IDS들로 부터 오는 정보들을 전부 합쳐서 침입 활동을 분석한다.

​

**​**

**분석 방법**

**​**

**1. 이상탐지 :** 오랜 기간 동안 수집된 합법적인 사용자들의 행동패턴 데이터를 이용한다.

관찰된 행동이 높은 confidence로 합법적인 사용자의 행동이라고 판단할 수 있는지를 통계학적인 테스트를 이용해서 판단.

​

**2. 오용탐지:** 특정 행동이 침입자의 것인지 아닌지를 판단하기 위해서 몇가지 규칙과 공격 패턴을 정의한다.

​

실무에서는 많은 공격 패턴에 대응 하기 위해서 두가지 방식을 혼용해서 사용한다.

​

​

**이상탐지**

​

이상탐지는 훈련 단계에서는 모니터링 시스템의 정상적인 행동으로부터 수집된 데이터를 분석하여 정상적인 행동을 정의한다. 탐지 단계에서는 정상적인 행위에서 벗어났는지를 비교하여 탐지를 한다.

​

- **통계** : 단변량, 다변량 또는 관측된 매트릭스 시간을 관찰하여 분석하는 방법

-**지식기반** : 전문가 시스템을 사용하여 정상적인 모델의 동작을 규칙으로 만들고 관찰된 행동과 서로 비교하여 탐지하는 방식

-**기계학습** : 데이터 마이닝 기법을 사용하여 자동으로 적합한 분류를 결정하는 방식.

​

​

**호스트 기반 침입탐지**

​

호스트 기반 침입 탐지 시스템은 취약하거나 민감한 시스템에 보안 소프트웨어의 특별한 레이어를 추가하여 이루어진다. 즉 데이터베이스 서버 및 관리 시스템이 여기에 해당된다.

​

HIDS는 의심스러운 동작을 검출하기 위한 다양한 방법으로 시스템의 활동을 감시한다.

​

호스트 기반 탐지 시스템의 주요 장점은 외부와 내부 모두를 감지할 수 있다는 것이다. 어떤 것은 네트워크 IDS와 방화벽에서 외부와 내부 모두 사용하지 못한다.

​

데이터 소스와 센서

-시스템 호출 추적

-감사 기록

-파일의 무결성 체크

-레지스트리 접근

​

​

**이상탐지 기반 HIDS**

​

이상 탐지 기반 HIDS의 주 업무는 유닉스와 리눅스 시스템에서 수집된 데이터를 가지고 이루어진다. 초기 버전은 회계기록이나 감사 기록을 사용하여 탐지를 하며 , 시스템 호출 추적 기반으로 탐지한다.

​

시스템 호출은 핵심 커널 기능을 접근하는 프로그램이며, 운영체제의 하부 레벨의 상호작용을 말한다.

따라서 프로세스의 활동이 정상인지 비정상인지의 판단을 위해 세부적인 프로세스 활동에 관한 정보를 제공한다.

​

​

**오용 탐지 또는 휴리스틱 호스트 기반 탐지 시스템**

​

호스트 기반 휴리스틱 또는 시그니처 탐지 방식은 주로 안티 멜웨어나 안티 바이러스 프로그램으로 많이 사용되고 잇다.

윈도우 시스템과 메일, 방화벽 웹프록시와 네트워크 기반 침입 탐지 시스템에서 흔히 사용되고 있다.

이들은 오용 탐지 데이터베이스나 휴리스틱한 규칙으로 악의적인 행동을 파악하여 잘 알려진 형태의 악의적인 소프트웨어를 탐지한다.

​

오용탐지 또는 휴리스틱 규칙에 부합되지 않는 제로데이 공격을 탐지할 수 는 없다.

​

**네트워크 기반 침입탐지**

​

**네트워크 센서의 종류**

1. inline센서 - client 에서 server 로 전달하기 위해선 무조건 inline 센서를 거쳐야 함

장점 : 이상한 데이터 차단 가능

단점 : 센서가 죽으면 통신 불가능

​

2. passive센서 - 망에 영향을 주지 않고 복사된 패킷을 보고 관리자에게 표시해줌

장점 : 고장나도 망 연결에 영향을 미치지 않음

단점 : 자동 차단 안됌

​

​

**NIDS센서의 배포**

​

위치 선정은 네트워크 상황에 따라 변화가 많음

​

가장 이상적인 부분은 각각의 구간 모두에 센서를 장착하는 것 (비용 부담)

​

가장 효율 적인 부분은 스위치와 라우터 사이

​

​

**침입 탐지 기술**

- 응용계층 정찰과 공격

- 전송계층 정찰과 공격

- 네트워크계층 정찰과 공격

- 예상외 응용서비스

- 정책 위반

**이상 탐지 기술**

- 서비스 거부 공격

- 스캐닝

- 웜

**[출처]** [침입 탐지](https://blog.naver.com/zxc991019/222338037431)|**작성자** [연구하는 연선비](https://blog.naver.com/zxc991019)