침입탐지시스템의 개념

- IDS는 IntrusionDetectionSystem의 약자입니다. 해석하면 말 그대로 침입탐지시스템입니다.

- 어떤 침입탐지시스템인지에 따라서 역할이 다르지만 (N-IDS,H-IDS) 하는 일은 이상행동을 탐지하고 알리는 역할을 합니다.

- 탐지 알고리즘에는 오용탐지기법과 비정상행위탐지기법이 있습니다.

​

오용탐지 (Misuse)

- 비정상 행위(시그니처 패턴)를 정하고 그 행위를 탐지한다.

장점 : 비정상행위탐지에 비해 속도가 빠르다.

단점 : 정해진 비정상 행위만 탐지가능하기 때문에 새로나온 패턴의 공격을 탐지할 수 없다.

​

비정상 행위탐지 (Anomaly)

- 정상 행위에 대한 자료값,통계 등을 통해 이에 벗어나는 행동을 탐지한다.

장점 : 새로나온 패턴의 공격을 감지할 수 있다.

단점 : 오용탐지에 비해 속도가 느리다.

N-IDS

- IDS의 앞에 N(Network)이 붙어서 네트워크 기반의 IDS 입니다.

- 여러 위치에 배치될 수 있지만 1순위로 배치되는 위치는 FireWall(방화벽)의 뒤에 배치됩니다.

- N-IDS는 성능이 우선입니다. 외부망으로부터의 엄청난 데이터들을 다 검사해야하므로 성능이 좋고 속도가 빨라야 합니다. 그러므로 주로 오용탐지기법을 사용합니다.

- 미러링 방식과 인라인 방식이 있습니다.

​

- 네트워크 기반이므로 네트워크 외부망 ( 간단히 인터넷이라 표현했지만 라우터 등의 게이트웨이를 뜻합니다. ) 에서 들어오는 데이터들이 FireWall을 거쳐서 들어오고 바로 IDS를 만나는 구조입니다. IDS가 정상으로 탐지해야 스위치를 통과해 네트워크 망으로 갈 수 있습니다. 즉, 외부의 데이터는 무조건 IDS를 거쳐서 들어가야 합니다. 장점은 침입자의 공격을 사전에 대응할 수 있다는 것이고, 단점은 서비스가 느리다는 것입니다. 모든 데이터가 IDS의 검사를 받아야 하므로 당연히 느립니다.

반면, N-IDS(네트워크기반 침입탐지시스템)의 미러링 방식은 외부의 데이터가 무조건 IDS를 거쳐서 들어가는 것이 아니라 일단은 스위치를 거치고 네트워크 망에 진입할 수 있습니다. 그리고 그 데이터를 스위치와 미러링한 IDS장비에서 탐지를 하고 만약 공격이라 판단되면 연결을 끊는 것입니다.

장점은 속도가 빠르다는 것입니다. 모든 데이터가 IDS의 검사를 받고 통과하려면 사용자에게 서비스하는 속도가 느려지기 때문에 일단 통과를 시키고 미러링을 통해 보안관제를 하는 것입니다. 따라서, 서비스 사용자는 끊김없이 서비스를 사용할 수 있습니다.

단점은, 일단 통과를 시키고 사후 대처를 하는 것이기 때문에 해커의 공격을 허용했다는 것입니다. 이를 보완하기 위해서 허니팟을 설치하기도 합니다.

​

H-IDS

- H-IDS는 H(Host)이므로 호스트 기반의 침입탐지시스템입니다.

- N-IDS에서는 탐지할 수 없었던 트로이 목마, 버퍼 오버플로우 등의 호스트 기반의 공격들을 탐지할 수 있습니다.

- 모든 로그와, 통계 등을 세밀하게 분석하므로 속도가 느립니다.(주로 비정상행위탐지기법을 사용함) 그러므로 모든 호스트 ( pc, 서버 등 )에 설치하는 것은 비효율적입니다. 따라서 철저한 보안이 필요한 중요한 호스트에 설치합니다.

​

N-IDS와 H-IDS의 연계방식

N-IDS와 H-IDS를 따로 쓰는것은 아닙니다. 네트워크 기반과 호스트 기반에서 모두 침입탐지를 해야하며, 서로 연계하는 방식을 사용합니다.

현재 네트워크를 통한 침입을 탐지하기 위한 N-IDS와 중요한 호스트에 H-IDS가 설치되어 있습니다. 중요 호스트에서의 IDS는 실시간으로 분석을 하며 탐지를 합니다. 만약 비정상행위를 탐지하여 해커의 공격을 알아냈다면 이 정보를 N-IDS에 등록합니다. 따라서 H-IDS가 분석한 내용을 네트워크기반에서 사전에 오용탐지를 할 수 있습니다. 이런 식의 연계방식은 IDS의 속도문제를 효율적으로 해결할 수 있고, 실시간으로 탐지하기 용이하다는 장점이 있습니다.