침입탐지 방법론

* 오용 탐지
1. 전문가 시스템(Expert System) – 공격에 관한 규칙 집합을 가지고 있어 감사 이벤트가 전문가 시스템 내에서 의미를 가지는 사실로 변환되고, 추론 엔진은 규칙들과 사실을 기반으로 침입을 판단함. 감사 자료에 의미를 부여함으로써 감사 자료에 추상화 정도를 증가 시킴.
2. 시그니처 분석(Signature Analysis) – 전문가 시스템과 동일한 방식으로 지식을 획득하지만, 지식을 사용하는 방식이 다름. 공격에 대한 의미적 기술은 감사 자료에서 곧바로 검색이 가능한 형태의 정보로 변경됨. 이 기법은 공격에 관한 기술이 낮은 수준인 경우 시행됨. 아주 효율적인 구현이 가능하여 상업적인 침입 탐지 기법에 응용되고 있음.
3. 페트리넷(Petri-net) – 코마의 기존 패턴 매칭 방법을 개선한 것으로 침입에 관한 시그니처를 표현하기 위해 칼라 페트리넷, CPN을 사용하였음. CPN은 일반성, 개념적 단순성, 그래프 표현성 등의 장점을 가지고 있음.
4. 상태전이분석(State Transition Analysis) – 공격을 목표와 상태 전이의 집합으로 기술하며, 상태 전이 다이어그램으로 표현한 것으로 일반적으로 STAT라 부름. 처음 설계되고 도구로 개발된 것이 92년 개발한 USTAT이며, 멀티 호스트로 확정한 것이 NSTAT.
5. 신경망(Neural Network) – 타당한 방법으로 새로운 입력 출력상을 얻기 위해 두 집합의 정보 간 관련성을 학습하고, 일반화하는 데 사용되는 알고리즘 기법. 지식 기반 침입 탐지 방식에서 공격을 학습하고, 감사 스트림에서 탐색하는 데 사용될 수 있음. 입력과 출력 간의 관계를 알 수 있는 믿을 만한 방법이 없으므로, 공격을 추론하거나 설명할 수 없어 주로 비 정상 행위 탐지 기법으로 많이 연구되었으나, 최근에는 지식 기반 프로파일을 구성하여 오용 탐지 기법으로도 사용됨.
6. 유전알고리즘(genetic algorithm) – 자연 선택의 원리와 자연계의 생물 유전학의 기본 이론을 두며, 모든 생물은 주어진 다양한 환경 속에 적응함으로써 살아남는다는 다윈의 적자생존의 이론을 기본개념으로 함.