침입탐지스스템의 오용탐지 기법이 사용하는 6가지 방법론을 나열하고 해당 방법론에 대한 설명을 서술하시오.

서명 분석

지식 기반 접근 방식을 이용하는 침입 탐지 방법론으로서 침입 양상에 대하여 의미적인 단계를 부여하고 이에 대한 광범위한 정보를 축적한다. 감사증적으로부터 감사 사건을 직접 검색하여 감사 사건의 기록 순서, 기록 패턴 등을 축적된 정보와 비교하여 침입을 탐지한다.

전문가 시스템

서명 분석 방법론과 마찬가지로 지식 기반 접근을 이용한 탐지 방법론이다. 우선 순위 기반으로 수립된 규칙 집합과 감사 증적의 사건들을 비교하여 침입을 탐지한다.

상태 전이 분석

침입을 상태 전이의 집합으로 표현한 상태 전이 다이어그램을 통하여 침입 탐지 과정을 분석하는 방법론이다.

페트리 넷

퍼튜 대학교에서 개발한 지식 기반 침입 탐지 방법론이다. CPNs을 사용하여 침입탐지시스템의 행위를 모델링하고 있다. 복잡하고 분산된 시스템을 추상화한 모델을 정립하는데 매우 유용하며 침입탐지시스템을 모델링할 경우 개념적으로 단순화가 가능하고 도식적인 표현이 가능하다.