※ 과제

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

1. 전문가 시스템(Expert Systems)

서명 분석 방법론과 마찬가지로 지식 기반 접근을 이용한 탐지 방법론이다.

우선 순위 기반으로 수립된 규칙 집합(rule set)과 감사 증적의 사건들을 비교하여 침입을 탐지한다.

감사 데이터에 대한 추상적인 단계를 부여하며 각 공격 유형에 대한 지식들을 규칙 집합으로 표현한다.

2. 시그니처 분석(Signature Analysis)

지식 기반 접근(knowledge based approach) 방식을 이용하는 침입 탐지 방법론으로서 침입 양상에 대하여 의미적인 단계를 부여하고 이에 대한 광범위한 정보를 축적한다.

감사 증적으로부터 감사 사건을 직접 검색하여 감사 사건의 기록 순서, 기록 패턴 등을 축적된 정보와 비교하여 침입을 탐지한다.

상용 침입탐지시스템 제품에 자주 적용되는 방법론이다.

3. 페트리 넷(Petri-nets)

지식 기반 침입 탐지 방법론이다. 복잡하고 분산된 시스템을 추상화한 모델을 정립하는데 매우 유용하며 페트리 넷을 이용하여 침입탐지시스템을 모델링 할 경우 개념적으로 단순화가 가능하고 도식적인 표현이 가능하므로 복잡한 침입탐지시스템의 행위들의 집단화(gathering), 분류(classification), 상관 관계(correlation) 등을 매우 효과적으로 설명할 수 있다.

4. 상태 전이 분석(State Transition Analysis)

침입을 상태 전이의 집합으로 표현한 상태

전이 다이어그램(state transition diagram)을 통하여 침입 탐지 과정을 분석하는 방법이다.

5. 신경망(Neural Network)

수학적 모델로서의 뉴런이 상호 연결되어 네트워크를 형성할 때 이를 신경망이라 한다.

신경망은 각 뉴런이 독립적으로 동작하는 처리기의 역할을 하기 때문에 병렬성이 뛰어나고,

많은 연결선에 정보가 분산되어 있기 때문에 몇몇 뉴런에 문제가 발생하더라도

전체 시스템에 큰 영향을 주지 않으므로 결함 허용(fault tolerance) 능력이 있으며, 주어진 환경에 대한 학습 능력이 있다.

6. 유전 알고리즘(Genetic algorithm)

진화의 핵심 원리인 자연 선택과 유전자의 개념을 이용한 최적화 기법.

주어진 문제에 대한 해답(solution)을 무작위로 생성한 뒤 이 해답 집단을 진화시켜 좋은 해답을 찾는다.