1. 침입탐지시스템의 오용탐지 기법이 사용하는 6가지 방법론을 나열하고 해당 방법론에 대한 설명을 서술하시오.
2. 침입탐지 시스템 : 오용탐지 기법
3. 전문가시스템(Expert system)

: 공격에 관한 규칙 집합을 가지고 있어, 감사이벤트가 전문가 시스템 내에서 의미를가지는 사실로 변환이 되고, 추론엔진은 이 규칙들과 사실을 기반으로 침입을 판단.함. 감사자료의 추상화정도를 증가시킴. 감사자료를 체계적으로 탐색할수있게함. 전체적성능은 낮음. 늦은 처리 속도로 인해서 프로토타입에서만 사용됨.

대표적인 예, ASAX

1. 시그니처분석(Signature Analysis)

: 전문가시스템과 동일한 방식으로 지식을 획득하지만, 지식을 사용하는 방식이 다름.함. 효율적인 구현이 가능. 상업적인 침입탐지 제품에 응용되고 있음. 취약점에 대해 자주 갱신을 해줘야함.

1. 페트리넷(Petri-net) : 쿠마의 기존 패턴 매칭을 개선함.
2. 상태전이분석(State Transition Analysis) : 공격을 목표와 상태전이의 집합으로 기술하며, 상태전이 다이어그램으로 표현한 것으로 STAT라 부름.
3. 신경망(Neural Network) : 타당한 방법으로 새로운 입력, 출력상을 얻기위해 두 집합의 정보간 관련성을 학습하고 일반화하는데 사용되는 기법.
4. 유전 알고리즘(genetic algorithm) : 자연 선택의 원리와 자연계의 생물 유전학에 기본 이론을 두는 기법.