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

오용탐지- 비정상 행위(시그니처 패턴)를 정하고 그 행위를 탐지한다.

오용 탐지 기법은 새로운 침입 유형이 있으면 새로운 침입 유형에 대한 탐지 자체가 취약한 단점이 있습니다. 이미 발견되고 정립된 공격 패턴을 미리 입력해 두고, 거기에 해당하는 패턴을 탐지하는 기법이다 --> 오용 탐지 기법.

알려진 공격 이외에는 탐지할 수가 없어 새로운 공격에는 비효율적이다 --> 오용 탐지 기법

다른 말로 Signature Base 나 Knowledge Base라 불린다. --> 오용 탐지 기법

여기에서 Signature는 ‘침입 서명’을 의미하는 것입니다.

이미 알려져 있는, Knowledge base.

시그니처 오용과 남용.

오용 탐지 기법의 단점은 : 미탐율이 높다. 새로운 공격을 찾아내질 못해서 미탐율이 높다.

-전문가 시스템

-키 모니터링

-상태 전이 분석

-패턴 매칭