과 정 명 : 전사원이 알아야 할 랜섬웨어와 악성코드 예방법
교육기간 : 2021-02-25 ~ 2021-03-26
작 성 자 : 이숙영

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

▶ 침입탐지시스템이란?

컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템으로 오용탐지 기법과 비정상행위 탐지 기법이 있음.

▶ 침입탐지시스템의 오용탐지 기법이 사용하는 6가지 방법론

① 전문가시스템(Expert System)

공격에 관한 규칙집합을 가지고 있어 감사 이벤트가 전문가 시스템 내에서 의미를 가지는 사실로 변환되고 추론엔진은 이 규칙과 사실을 가지고 침입을 판단하는 방법
단점은 성능이 낮고, 처리속도가 늦음.

② 시그니처 분석(Signature Analysis)

전문가시스템과 동일한 방식으로 지식을 획득하지만 활용하는 방식이 다름.
공격에 관한 기술이 저수준인 경우 사용되고, 효율적인 구현이 가능하여 상업적인 침입탐지 제품에 사용
단점은 새로 갱신된 취약점에 대해 잦은 갱신을 해야 함.

③ 페트리넷(Petri-net)

침입에 관한 시그니처를 구현하기 위하여 칼라 페트리넷과 CPN을 사용
일반성, 개념적 단순성, 그래프표현성의 장점을 지님.
복잡한 시그니처를 감사자료와 비교하는 것은 많은 비용 소모

④ 상태전이분석(State Transition Analysis)

공격을 목표와 상태전이의 집합으로 기술하며 상태전이 다이아그램으로 표현
네트워크 기반 침입탐지 시스템이 NET STAT임.

⑤ 신경망(Neural Network)

타당한 방법으로 새로운 입력 출력상을 얻기 위해 두 집합의 정보간 관련성을 학습하고 일반화 하는 데 사용하는 알고리즘 시스템

⑥ 유전 알고리즘(genetic Algorithm)

자연선택의 원리와 자연계의 생물유전학의 기본이론을 두며, 모든 생물은 주어진 다양한 환경속에 적응하여 살아남는다는 다윈의 적자생존 이론을 적용