침입탐지시스템의 오용탐지기법이 사용하는 6가지 방법론

1. 전문가시스템

공격에 관한 규칙집합을 가지고 감사이벤트가 전문가적인 시스템 내에서 의미를 포함하는 내용으로 변환이 되어 침입여부가 판단되며, 감사자료에 의미를 두어 그 자료의 추상화정도를 증가시킬 수 있다. 이 접근방식은 알려진 부족한 부분을 이용하려는 시도들에 관한 증거를 찾기 위해 자료를 체계적으로 탐색할 수 있도록 한다. 하지만 전문가 시스템의 전체적 효율은 낮은 정도이며 처리속도가 늦어 프로토타입에서만 이용되어진다.

1. 시그니처 분석

전문가시스템과 같은 방법으로 지식획득에 기반한다. 하지만 지식을 사용하는 방법은 다르다. 공격에 대한 기술이 곧바로 자료에서 검색이 가능한 모양의 정보로 변경이 되면서 공격에 관한 수준이 낮은 수준일 때 실행되어진다. 이 방법은 아주 효율적인 효과가 가능하기에 상업적 침입탐지 제품에 활용되고 있지만, 새롭게 발견되는 부분에 대해서는 자주 갱신을 해주어야 하는 것이 단점이라고 할 수 있다.

1. 페트리넷

95년 쿠마의 기존 패턴 매칭방법을 개선한 것으로 침입에 관한 시그너쳐를 표현하기위해서 CPN을 사용하였다. CPN은 기념성, 일반적 단순성, 그래프 표현성 등의 장점을 가지고 있다. CPN의 일관성으로 복잡한 시그너쳐들도 쉽게 작성은 되어지지만 복잡한 시그너쳐를 감사자료와 비교하는 작업은 많은 계산비용을 요구된다는 것이 단점이다.

1. 상태전이분석

공격을 목표와 상태전이의 집합으로 기술하며 상태전이 프로그램으로 표현한 것으로 일반적으로 SDAT라고 부른다.

1. 신경망

타당한 방법으로 새로운 입력 출력상을 얻기 위해 두 정보간 관련성을 연결하고 일반화 시키는 것에 사용되는 알고리즘 기법이다. 이론적으로 지식기반 침입탐지방식에서 공격학습후에 감사 프로그램에서 탐색하는 것으로 사용된다. 입력과 출력 간에 관계를 알 수 있는 믿을 만한 방법이 없으므로 신경망은 공격을 추론하거나 설명이 어려워서 주로 비정상행위탐지기법으로 많이 연구되었으나, 지식기반 프로파일을 구성하여 오용탐지기법으로 최근에는 사용되어지고 있다.

1. 유전 알고리즘

모든 생물은 주어진 다양한 형태의 환경에 적응함으로 살아간다는 다윈의 적자생존의 이론을 기본개념으로 하며, 자연선택의 원리와 자연계의 생물유전학에 기본이론을 둔다.