학과: 정보보호학과 학번: 2021111703 이름: 최유진

#1 침입탐지와차단시스템의 필요성과 특징

근래에 오기까지 점차 인터넷 기술이 다양하게 발전하면서 일상이 편리해짐과 동시에 이러한 인터넷 시스템에 수많은 침입 시도가 발생했다. 인터넷 기술이 발전하는 만큼, 시스템을 침입하려는 이들의 기술 또한 발전하고 다양해졌다. 이러한 상황 속에서 늘어가는 보안 위협으로부터 크게는 국가와 기업이 작게는 개인이 다양한 보안 위협으로부터 개인과 조직을 보호하고 지키기 위해 침입 탐지와 차단 시스템이 필요하다.

침입탐지와차단시스템의 필요성을 서술하기 전에 이 기술의 특징을 먼저 살펴보면 다음과 같다. 우선, 침입 탐지 시스템을 '탐지'만을 수행하기 때문에 탐지 시스템이 같이 필요하다. 침입 탐지 시스템은 Intrusion Detection System, 약자로 IDS라고 불린다. 크게 설치 위치와 목적에 따라 호스트 기반 IDS와 네트워크 기반 IDS로 나뉜다. 침입 차단 시스템은 방화벽이라고 하는데, 네트워크에서 보안을 높이기 위한 일차적인 방법으로, 서로 다른 네트워크를 지나는 트래픽을 정해진 보안 정책 및 규칙 집합을 기반으로 트래픽을 허용하거나 차단하는 기능을 수행하는 시스템이다. 침입 탐지 시스템과 침입 차단 시스템 모두 외부 공격과 내부 공격, 권한이 부여되지 않은 액세스 등에 대한 보안 위협을 감지하는 특징을 가진다. 또한, 시스템이 실시간으로 공격을 탐지하고, 보안 위협을 감지하는 즉시 경고 및 알림을 제공하는 특징을 가진다. 그뿐만 아니라, 침입 탐지와 차단 시스템은 공격 및 차단에 대한 로그와 보고서를 생성한다는 특징을 가진다. 이들이 생성한 로그와 보고서를 통해 개인 및 조직은 보안 위협을 추적하거나 대응 방법을 개선하는 것이 가능해진다.

이렇게 다양한 특징을 가지는 침입탐지와차단시스템이 필요한 이유는 다음과 같다고 생각한다. 우리는 4차 산업혁명을 거쳐 거의 모든 것이 인터넷으로 연결된 세상 속에 살고 있다. 1~2년 전, kt가 먹통이 되었을 때, 당시 e-class를 통한 시험은 모두 미뤄졌고, 사람들이 스마트폰 통신을 사용할 수 없어 지하철에 공중전화 앞에 긴 줄이 늘어섰었다. 카드 단말기를 사용하는 식당가는 점심 장사를 공쳤고, 그 밖에도 많은 불편을 겪었다. 통신사 통신망 하나 먹통 되었다고 말이다. 이렇게 인터넷이 제대로 작동하지 못한 것은 고작 1시간 반 남짓인데, 많은 이들의 일상이 마비됐었다. 만약, 해커나 사이버범죄로부터 인터넷이 공격당한다면 어떻게 될까? 아마 통신망이 잠깐 마비된 것과는 비교도 되지 않을 만큼 큰 손해를 입을 것이다. 복구에도 무수한 비용과 시간이 들어갈 것이다. 특히, 북한을 필두로 하여 타 국가로부터의 해킹 공격 시도가 무수히 이루어지는 한국으로서는 이들의 침입을 탐지하고 사전에 차단하여 방지하지 않는다면 범국가적으로 큰 손실을 보는 것을 면치 못할 것이다. 그럴 뿐만 아니라, 각 기업과 조직은 중요한 데이터를 보유하고 있다. 그들이 침입자에게 당한다면, 기업과 조직, 기관의 중요 데이터만이 아니라 그 기업과 조직 및 기관의 서비스를 이용하고 있는 많은 개인에게도 영향을 미칠 것이다. 주요 기관인 보건복지부의 전산망이나 데이터가 침해당한다고 생각해보자. 대한민국에서 건강보험에 가입해있는 모든 사람의 기록이 그냥 무방비하게 노출되는 것이다. 그들의 이름, 나이, 성별, 거주지, 주민등록번호, 가족관계, 진료기록 등 개인의 주요한 데이터가 모두 그대로 개방되는 것이다. 개인정보보호가 중요시 되는 요즘 시기에 개인들의 정보를 보호하기 위해서라도 침입탐지와차단시스템은 꼭 필요하다. 그리고 설령, 주요한 기관이나 기업, 조직이 아니라고 할지라도 침입이 불러오는 피해가 어떤 정도일지, 그 영향이 어디까지일지 우리는 짐작하기 어렵다. 따라서 미리 보안 위협과 침입을 탐지해내고 그들을 차단해내어 더 큰 보안 위협을 미연에 방지하고 지속해서 침입을 관리하기 위해서 침입탐지와차단시스템은 반드시 필요하다.

Q. 와이어샤크에서 TOS에 해당하는 ECN은 혼잡 알림을 위해 사용된다고 했는데, 어떻게 혼잡 알림을 주는가? (답변에서 굵게 처리된 부분은 피드백을 반영한 부분입니다.)

A. ECN은 Explicit Congestion Notification의 약자로, '명시적 혼잡 알림'이라는 뜻이다. ECN 방법은 통신 혼잡이 발생한 초기에 혼잡이 발생했음을 명백하게 알려주기 때문에 통신 혼잡을 판단하는 정확한 방법이라고 할 수 있습니다. ECN은 TCP와 IP에 모두 관여하는데, 질문에 나와있듯이 TOS 필드에 있는 2개의 비트 공간을 ECN에 사용합니다. **여기서 TOS는 Time of Service의 약자로, TOS 필드는 IP 패킷 헤더에 포함되는 필드 중 하나입니다.** ECN 2개의 비트 중에서 1개의 비트는 라우터가 정체를 겪어 혼잡하다는 것을 나타내기 위해 사용됩니다. 그리고 남은 한 비트는 발신 호스트가 송신자와 발신자가 모두 ECN을 사용할 수 있다고 라우터에게 알리는 데 사용됩니다. ECN은 세그먼트의 손실 원인을 밝혀 혼잡을 회피하는 방식에 속합니다. ECN은 라우터나 게이트웨이에서 버퍼가 어느 정도 차서 폐기가 예상되면 세그먼트에 ECN 마킹을 해주어 송신 TCP에게 통신 혼잡을 알립니다. **이때, 마킹은 ECN 시스템 내에서 우선순위를 부여하는 것을 뜻합니다.** 이렇게 통신 혼잡을 빠르게 알게 된다면, 송신 TCP에서는 전송 속도를 낮추어 즉각적인 대응을 통해 혼잡 정도를 완화할 것이라고 생각됩니다. 이렇게 명백하게 알림을 통한 이러한 방법으로 혼잡 정도를 낮추는 식의 용도로 ECN이 혼잡 알림을 위해 사용된다고 봅니다.
[피드백]
정보보호학과 2021111345 원가은
와이어샤크를 다뤄본 적은 있으나 TOS에 대해서 있다는 정도만 알고 ECN의 개념에 대해서는 몰랐었는데, ECN의 사용방식과 과정을 처음 알게 된 사람도 쉽게 이해할 수 있도록 답변을 달아놓은 것이 좋았다. 또한 ECN의 혼잡알림이 송신 TCP에 어떠한 영향을 주는지까지 알 수 있어 유익했고, 내용의 흐름이 전반적으로 글읽기에 용이했다.

정보보호학과 2021111335 손예은
명시적 혼잡 알림인 ECN의 정의와 사용될 때의 각각이 어떻게 사용되는지 알 수 있었다. 또, 통신 혼잡이 일어났을 때 혼잡 정도를 낮추기 위해 어떻게 대응할지에 대해 알 수 있었다. 그래서 통신 혼잡이 발생했을 때 이렇게 동작하겠구나를 생각할 수 있었다. 특히 ECN의 각각의 비트에서 라우터와 관련해 어떻게 사용되고 동작하는지 잘 알려준 것 같다. 그렇지만 TOS나 마킹 등 조금 새로운 용어에 대해 설명을 해줬으면 좋겠다고 생각했다.

[출처]
남수만, 『강의소개』, 침입탐지와차단시스템 강의자료(2023) , p13-14.

보안바라기, 2019년 1월 31일 https://catchingitsecure.tistory.com/4

이계영, 임재걸, 장익현, "정보통신 : ECN 마킹을 위한 최적의 Threshold"(2005), p1-2.

Kick_snare, 2022년 11월 5일 https://uzun.dev/167

ChatGPT, https://chat.openai.com/