침입 탐지와 차단 시스템 01분반 질문 &
답변 보고서

정보보호학과 2021111703 최유진

Ⅰ. Brute Force Attack – 변혜빈, 백유진

Q. intruder 설정하실 때 'Cluster Bomb'유형으로 attack type을 설정하셨는데 'Cluster Bomb' 공격 유형이 무엇인지, 이것이 다른 브루트 포스 공격 유형들과 어떻게 다른지 알 수 있을까요?

A. 총 4가지 공격 유형이 있는데, cluster bomb attack type의 경우, 페이로드를 어떻게 설정하냐에 따라 나뉘어진다. 이 실습의 경우, 유저네임과 패스워드 2개의 페이로드를 설정해야한다. 두 개의 공격을 조정할 수 있는 것으로 정해야 하는데, 나머지 3개는 한 개에 대한 변수를 공격하거나 한 개에 대한 변수에 대해서도 브루트포스 공격 처리 방식이 달라서 cluster bomb이 이 실습 공격 유형에 잘맞는다고 판단하여 cluster bomb으로 설정했다.

***답변에 대한 생각**

Burp Suite라는 웹 보안 도구에서 'intruder' 기능을 사용할 때, 'Cluster bomb' 공격 유형은 두 개 이상의 payload set을 동시에 대상으로 하는 공격 유형이기 때문에 위의 공격처럼 유저네임과 패스워드와 같이 두 가지 변수를 동시에 대상으로 하는 시나리오에서 사용하는 것은 적절하고 타당성이 있다고 생각이 된다. 다만, 다른 유형으로는 'sniper', 'battering ram', 'pitchfork' 가 있는데 이 부분에 대한 보충적인 설명이나 구체적으로 어떤 공격에 주로 사용하기 좋은지 등에 대한 부분이 답변됐다면 더 좋았을 것이라는 아쉬움이 있다.

Ⅱ. RUDY – 김주미, 장지은

Q. 하신 공격실습에서는 10초 즈음에 가용 서비스가 현저하게 줄어들었다고 하셨는데, 혹시 공격이 실질적으로 통하기 시작하는 시간을 줄일 공격자가 원하는대로 늘리거나 줄일 수 있나요?

A. slowhttptest 툴에서는 옵션으로 content-length 값을 설정할 수 있다. 디폴트 값인 4096으로 실습을 진행했는데, 이 값을 만약 대략 1000 정도로 줄이면 하나의 공격에 대해서 서버와 연결되어있는 시간이 줄어들고, 반대로 10000 정도로 늘리면 하나의 공격에 대해 서버와 연결되어있는 시간이 늘어나게 될 것이다. 이렇게 하나의 연결이 서버와 연결되어있는 시간을 조절함으로서, 총 공격 시간을 조절할 수 있겠다.

***답변에 대한 생각**

'slowhttptest'라는 툴을 사용하여 시간을 조절하는 방법을 정확하게 설명해준 것 같다. content-length 값을 조절하여 연결을 유지하는 시간을 늘리거나 줄일 수 있다는 부분에 대해 정확하게 설명해준 것 같다. slowhttptest는 몇 가지의 매개변수를 사용하여 공격을 더욱 세밀하게 조정할 수 있는데, 값에 대한 부분과 같이 초당 연결 요청 수를 정의하는 –r옵션이나 헤더 값을 조정하여 추가로 연결을 유지하는데 필요한 시간을 조정하게 할 수 있는 –i옵션처럼 세밀한 부분에 대한 부분도 같이 답변을 받았으면 더 좋았을 것 같다.