실습 과제 1 - 하트블리드(HeartBleed)

1. 하트블리드 취약점이 무엇인지 조사

하트블리드(HeartBleed) : 정해진 규격의 네트워크 보안 프로토콜을 범용 라이브러리로 구현하기 위해 만들어진 OpenSSL 라이브러리 1.0.1 버전에서 발견된 매우 위험한 취약점

- OpenSSL 을 구성하고 있는 TLS/DTLS 의 HeartBeat 확장규격에서 발견됨.
    - TLS 는 전송 계층 보안을 뜻하는 용어로 개인 정보 보호 및 안전한 전송을 위해 이메일을 암호화하는 표준 인터넷 프로콜
    - DTLS 는 데이터그램 형식의 콘텐츠를 애플리케이션끼리 주고받을 때 안전하게 전송할 수 있도록 하는 통신 프로토콜 (SSL, TLS 기술 토대)
    - HeartBeat 는 서버와 클라이언트 사이에 문제가 없는지 또는 안정적인 연결을 유지하기 위한 목적으로 신호를 주고 받을때 사용하는 확장규격
- 해당 취약점을 이용하면 서버와 클라이언트 사이에 주고받는 정보들을 탈취
- 강력한 암호화를 제공하기 때문에 이메일, 금융권에서 애용 → 더욱 문제
- 클라이언트는 서버에게 특정 정보와 해당 정보의 길이를 보내줌 → 서버는 전달받은 정보와 그 정보의 길이가 일치할 때만 응답해야 하는데 이 길이 검증을 하지 않음 → 서버는 모자란 길이만큼 자신의 메모리 정보를 채워서 응답함 → 정보 유출
- 한 번에 많이 유출되는건 아니고 1 회 정보 요청량이 64KB 이지만 반복될 수록 조금씩 조금씩 새어나감

2. 하트블리드 취약점으로 인해 발생한 해킹 사례 조사

- 2014 년 4 월 14 일 캐나다 국세청 하트블리드 해킹으로 인해 사회보장번호 900 여개가 도난된 사건
- 영국 150 만명 회원수를 보유한 육아 관련 사이트 '맘스넷' 의 가입자 정보 해킹 사건

3. 하트블리드 기반 해킹 사례를 이용해 해당 사례의 취약점, 위협, 위험은 무엇이었는지 정의해

- 취약점 : 국세청 서버가 클라이언트의 요청에 대한 길이 검증을 하지 않았고 저장되어 있던 사회보장정보 나 개인정보에 대한 암호화를 하지 않은 것
- 위협 : 서비스 서버에 요청을 보낼때 보내는 정보의 길이와 다른 길이를 보내주는 행위를 반복적으로 함. 탈취하고자 하는 정보를 입력하는 란에 아무 정보나 입력하고 서버에 요청 보내는 데이터의 길이를 늘려 반복적으로 요청함
- 위험 : 개인 정보 도난 및 유출