SW보안 개론 과제 및 실습 소개

Jaewoo Shim

Mar. 07. 2018

목차

- ❖ 과제 개요
- ❖ 팀프로젝트 소개
- ❖ 과제 및 실습 소개
  - 소프트웨어 취약점 및 보호기법 실습
  - 네트워크 트래픽 캡쳐(wireshark)
  - SQL Injection 실습
- ❖ 결론

과제 개요

- 이론 수업과 병행하여 학부생의 이해를 도울 수 있도록 함
- 운영체제, 네트워크, 데이터베이스와 같은 분야의 기본지식을 스스로 익힐 수 있는 기회를 제공하므로써 보안과의 연관성을 이해
- 불법으로 다뤄질 수 있는 공격 기법 등의 지식을 모의 환경을 직접 구축하여 실습하므로써 공격자의 공격 패턴을 이해

팀프로젝트 소개

- **악성코드 분석 – lightAidra**
  - 소스코드가 없는 바이너리를 분석할 수 있는 역량을 익히기에는 현실적으로 어려움이 있음
  - 소스코드가 있는 악성코드를 대상으로 분석을 수행 – 2000줄 정도

- **소스코드 다운로드 가능 : https://github.com/eurialo/lightaidra**

- **3 ~ 4명의 팀으로 수행하는 것을 권장**
- **팀원 구성 후 조교에게 전달 : 3월 14일(수) 까지**
- **제안서 제출 : 4월 4일(수) 까지**
- **4주간 수행 후 결과 보고서 제출 : 5월 2일(수) 까지**

팀프로젝트 소개 - 제안서

- **양식 및 분량 – 자유**
- **팀 별로 1부 제출**
- **제안서에 반드시 포함되어야 하는 내용**
  - 팀명
  - 팀원 이름/학번/이메일 - 팀장이 누구인지 표기
  - 분석을 수행할 환경
  - 분석에 사용할 도구
  - 일정(간트차트)

팀프로젝트 소개 - 보고서

- **양식 및 분량 – 자유**
- **팀 별로 1부 제출**
- **보고서에 반드시 포함되어야 하는 내용**
  - 제안서에 기입했던 내용들
    - 환경과 도구는 분석 시 다르게 이용했을 경우 실제 사용한 내용을 작성
  - 소스코드 분석 내용(소스코드 주석달아 제출하지 마세요 - **감점**)
    - 각 *.c 파일의 역할 – 무슨 기능을 하는지?
    - 각 함수의 역할 – “~기능을 수행하는 함수이다.”
  - 컴파일 후 실행 내용
    - 어떤 기능을 수행하는 악성코드인지?
    - 어떤 식으로 동작하는지?(자세하게)
      - 이 기능을 어떤 분석환경을 어떻게 갖추어 어떻게 실행시켜 확인했는지?
  - 결론
    - 이 악성코드는 어떤 환경에서 무슨 기능을 수행하는 악성코드다.
    - 내가 보안 담당자라면 어떻게 해당 악성코드를 탐지 및 차단할 것인지?

과제 및 실습 소개

❖ 소프트웨어 취약점 및 보호기법 실습

- 버퍼 오버플로우 / 포맷스트링 버그 취약점 설명
- 버퍼 오버플로우 취약점 공격 실습
  - 실습환경은 구축중

❖ 과제 – 2주

- 다수의 버퍼오버플로우 취약점이 존재하는 소스코드와 실행파일을 제공
  - bof.c, bof
- 다수의 포맷 스트링 버그 취약점이 존재하는 소스코드와 실행파일을 제공
  - fsb.c, fsb
- 소스코드를 분석해서 취약점을 찾은 뒤 **패치**해오기
  - 기능을 없애버리거나, 정상 기능을 하지 못하도록 패치할 경우 **감점**
- **[가산점]** 패치 전 버퍼오버플로우 실행파일을 대상으로 공격을 성공하여 쉘 획득 시 가산점 제공
- **자신이 수행한 사항을 보고서로 작성하여 제출**
- 과제 나가는 날짜 : **3월 19일**
- 과제 제출 날짜 : **4월 4일**

과제 및 실습 소개

- ❖ 네트워크 트래픽 캡처
  - http 와 https 통신을 수행하는 각각의 웹서버를 대상으로 패킷을 캡쳐
  - 암호화의 상태를 확인해보는 수업
  - 간단한 TCP/IP관련 네트워크 지식을 미리 공부해보고 wireshark의 사용방법을 아는 것이 과제의 의도

- ❖ 과제 – 1주
  - 자신의 컴퓨터에 간단한 https 웹서버 구축(가상환경 추천)
  - Wireshark 프로그램을 이용하여 서버와의 통신을 캡처
  - wireshark를 이용하여 캡처한 https 트래픽을 복호화해오기
    - 자기가 통신한 트래픽을 복호화해오면 됩니다.
  - 자신이 수행한 사항을 보고서로 제출
  - 과제 나가는 날짜 : **5월 9일**
  - 과제 제출 날짜 : **5월 16일**

과제 및 실습 소개

- **SQL Injection 실습**
  - **데이터베이스를 대상으로 공격을 수행하여 내부 정보를 조회해보는 공격 실습**
  - **WebGoat를 이용**

- **과제 – 2주**
  - **WebGoat에 있는 문제 2문제 풀어오기**
  - **자신의 풀이방법을 보고서로 제출**
  - 과제 나가는 날짜 : **5월 28일**
  - 과제 제출 날짜 : **6월 15일**

QnA

- 조교 이름 : 심재우
- 이메일 : tlawodn94@gmail.com
- 연구실 : 미디어센터 505호 / 부재 시 504호

Thank You !