컴퓨터 보안_01

실습 2주차

동국대학교 CSDC Lab.
실습조교 김선규, 최연우

2023.03.15 (Wed.)

Index

Review

1주차 실습 주요 이슈

dongguk UNIVERSITY

➢ JTR

- 환경 구성에 대한 어려움
- 패스워드 크래킹

※ apple, b4n4n4에 대한 비밀번호는 대부분 구하였음

※ P@ssw0rd 비밀번호는 2명을 제외하고 최대 60시간 까지 JTR을 돌려도 구할 수 없었음.

➢ Hash Suite

- Hash Suite 파일 다운로드

※ Windows 보안의 바이러스 및 위협 방지 설정 및 기타 백신 프로그램으로 인한 다운로드 불가 이슈

- Import local accounts 불가

※ Windows 보안의 바이러스 및 위협 방지 설정 및 기타 백신 프로그램으로 인한 Import 불가

※ Free version은 비밀번호 최대 6자리까지밖에 지원하지 않아 8자리 패스워드 P@ssw0rd는 모두 구할 수 없었음.

실습 강좌 소개

➢ 실습 진행 방법

- 간단한 이론 복습 및 해당주차 실습문제 설명
- 실습 후 보고서를 작성하여 다음주 화요일 자정(23:59) 까지 E-Class에 제출(이메일 제출 불가, 반드시 E-Class를 통해 제출)
- 실습 과제 제출 기한 엄수 (제출기한 이후로는 0점 처리)

➢ 실습 보고서 [1/2]

- 실습 문제에 대한 요구 사항 파악, 해결 방법 등 기술
- 프로그램 설계 / 알고리즘
  - 해결 방법에 따라 프로그램 설계 및 알고리즘 등 기술
  - 문제 해결 과정 및 핵심 알고리즘 기술
- 결과 / 결과 분석
  - 결과 화면을 캡쳐 하여 첨부, 해당 결과가 도출된 이유와 타당성 분석
- 소감
  - 실습 문제를 통해 습득할 수 있었던 지식, 느낀 점 등을 기술

실습 강좌 소개

➢ 실습 보고서 [2/2]

- 제출 방법
  - 보고서를 작성하여 E-Class “과제” 메뉴를 통해 제출
    - “이름_학번_실습주차.zip” 형태로 제출 (e.g. : 홍길동_2022123456_실습1주차.zip)
    - 파일명에 공백, 특수 문자 등 사용 금지
    - 보고서 파일은 한글, 워드 작성이 상관 없으나 .pdf 로 변환하여 제출

- 유의사항
  - 보고서의 표지에는 학과, 학번, 이름, 담당 교수님, 제출일자 반드시 작성
  - 정해진 기한 내 제출
    - 기한을 넘길 시 0점 처리
    - E-Class가 과제 제출 마지막 날 오류로 동작하지 않을 수 있으므로, 최소 1~2일 전에 제출
    - 당일 E-Class 오류로 인한 미제출은 불인정
  - 보고서를 자신이 작성하지 않은 경우 실습 전체 점수 0점 처리

Brute Force Attack (무작위 대입 공격)?

dongguk UNIVERSITY

➢ Brute Force Attack (무작위 대입 공격) ?

- 암호문의 암호 키를 찾기 위해 모든 경우의 수를 무작위로 대입하여 암호를 푸는 공격 방법

비밀번호 길이	경우의 수(영문+숫자조합)	경우의 수(특수문자포함)
6	61,474,519	156,238,908
7	491,796,152	1,473,109,704
8	3,381,098,545	11,969,016,345
9	20,286,591,270	85,113,005,120
10	107,518,933,731	536,211,932,256
11	508,271,323,092	3,022,285,436,352
12	2,160,153,123,141	15,363,284,301,456
13	8,308,281,242,850	70,907,466,006,720
14	29,078,984,349,975	298,824,321,028,320
15	93,052,749,919,920	1,155,454,041,309,500
16	273,342,452,889,765	4,116,305,022,165,110

[Fig 1. 암호를 풀기위한 대입 경우의 수]

[Fig 2. John the Ripper]

Brute Force Attack 구현하기

dongguk UNIVERSITY

➢ 과제 내용

- 4 ~ 8자리 패스워드를 무작위 생성한다.

- 무작위 패스워드 생성 시 유형을 선택할 수 있다. (숫자, 알파벳, 숫자+알파벳, 숫자+알파벳+특수문자)
  ※ 사용자에게 입력을 받거나, 소스코드 내에서 설정 가능

- 모든 경우의 문자를 생성하여 패스워드를 찾을 때 까지 비교한다.
  ※ 생성한 모든 경우의 문자 = Key 값
  ※ Key 값은 패스워드와 달리 유형 구분 없이 모든 경우의 문자를 생성

- 찾을 때 까지 소요된 시간을 기록하여 분석한다.

- 각 케이스 별로 100회 테스트할 수 있도록 한다.
  ※ 프로그래밍 언어 자유, 보고서 분량 자유

Q & A

Thank you