과제 3 서버 분석

과제 3

- **제출 마감일 : 11월 19일 (일요일) 11:59pm**
- **eClass 과제방에 제출**
- **제출 양식**
  - 결과를 포함한 보고서 (PDF), 프로그램 코드
- **개인 과제**

1. 로그 분석

로그 분석하기

- 웹서버, DB서버가 설치된 리눅스 서버를 운영하였다.
- 리눅스 서버에 쌓인 로그를 분석하여 내 서버에 어떤 일들이 있었는지 설명한다.
- 로그는 var/logs 이외에도 DB서버의 로그와 웹서버의 로그는 다른 공간에 생성될 수도 있다.
- 로그 분석을 통해 각종 서버 프로그램에 접속 시도들을 확인할 수 있다.
- 서버를 켜놓은 기간이 길수록 더 많은 시도들이 있다.

1. 로그 분석

분석 내용

- 로그인 실패 이력, 로그인시 시도한 계정 정보
- SSH 접속 시도
- 웹서버 접속 시도 및 접속 의도, 접속하여 빼간 정보들
- DB 서버 접속 시도, 시도한 계정 정보 등

1. 로그 분석

- **이후로는 서버를 더 이상 사용하지 않으니 서버 종료 또는 계정 종료할 것(11월 20일 이후)**
  - 종료 : 서버를 제거함. 요금이 더 이상 과금되지 않음
    - free tier는 1년간 무료 사용이 가능하지만, 서버를 켜두었다는 사실을 잊고 있으면 1년 후부터 매달 요금이 과금
    - 과금되는 부분이 없는지 잘 확인할 것
  - 계정 종료 : 계정 자체를 삭제함. 계정이 남아있으면 카드 번호가 등록되어 있으므로 언제든 과금 사유가 발생하면 과금
    - 계정을 유지하면 언제든 사용이 가능하지만, 계정을 노리는 해커들이 많고, 계정을 해킹당할 경우 수천 만원 이상의 큰 피해가 발생할 수 있음 (봐달라고 하면 1회는 봐주기도 함)
    - 다른 사이트와 같은 계정 정보를 쓸 경우 해킹 소지가 있음

2. 서버 분석 프로그램 작성하기

서버 정보를 수집하는 프로그램 작성

- 서버의 IP를 입력하면 이 IP에 존재하는 서버와 서버 프로그램을 분석하여 운영체제, 웹서버 유무, SSH 유무, 데이터베이스 유무 및 버전 등을 조사하여 결과를 출력하는 프로그램을 작성한다.
- 해당 서버에 열려있는 포트에 접속을 해야만 정보 수집이 가능하다.

작성 언어 : 무관하나 파이썬으로 쉽게 가능

- 서버에 접속한 후 얻을 수 있는 정보로 분석 및 결과를 표시하는 것까지 프로그램에 포함되어야 한다.

2. 서버 분석 프로그램 작성하기

- **자신이 할 수 있는 프로그래밍을 이용해 서버 분석 프로그램 만들기**
  - 이것을 진행하려면 소켓 프로그래밍을 알아야 한다.
  - 소켓 프로그래밍을 검색하여 적절한 코드를 찾는다.
    - 소켓 프로그래밍은 서버와 클라이언트쪽 코드가 다른데, 우리는 클라이언트쪽을 사용한다.
    - 소켓은 입력된 데이터를 서버로 전달하고, 서버쪽 반응을 가져오는 역할만 수행한다. 서버로 연결 또는 서버로 간단한 정보를 보내고 그 응답을 수집하여 서버를 분석한다.
    - 소켓은 존재하지 않은 서버, 존재하지 않는 포트를 접속하려 시도하면 일정 시간(대략 15초)동안 블록되기도 한다. 그것은 불가피한 상황이므로 대기해야 한다.

2. 서버 분석 프로그램 작성하기

- **테스트할 수 있는 서버의 IP**
  - 서버 1 : is1.xtc.co.kr(3.38.104.136)
  - 서버 2 : is2.xtc.co.kr(15.164.244.73)
- **2개의 테스트 서버를 분석하여 정보를 표시한다.**
- **참고로 2개의 서버는 Linux 또는 Windows이고, Linux 종류도 한 배포판으로 고정된 것은 아니다.**
  - 서버에는 모두 다른 서버 프로그램이 구동중이므로 포트 검색 및 연결을 통해 서버의 종류와 버전을 찾아야 한다.
  - 웹서버 프로그램은 Apache일수도, IIS 일수도 있다.
  - DB 프로그램은 MySQL일수도, MSSQL일수도, 없을 수도 있다.

2. 서버 분석 프로그램 작성하기

서버 분석 프로그램의 활용

- 지금은 3개의 테스트용 서버만 사용하지만, ip 영역대를 입력 받아 서버를 찾는 기능까지 포함하면 더 강력한 서버 분석 프로그램이 될 수 있다.
  - 예) 3.34.56.0 ~ 3.34.56.255 의 모든 서버를 검색
- 지금은 제한된 포트/서버 프로그램만 확인하지만, 다양한 포트/서버 프로그램에 대응하면 더 많은 정보를 수집할 수 있다.

2. 서버 분석 프로그램 작성하기

- **실행 예)**

  IP를 입력하세요 : ***3.34.56.78***

  분석 결과

  OS : Ubuntu Linux 20.X

  웹서버 : Apache 2.4

  DB : 없음

  SSH : 버전 3.4