산업테러 기반 3번째 강의

앞에서 다뤘던 센시스 웹서비스 api를 이용한 검색 활용

<https://github.com/gelim/censys>로 들어가야함.

칼리리눅스에서 실행 하면됨.

**명령어 : git clone http ~**

**Cd censys**

**Ls**

**Pip install -r requirements.txt //** 이러면 설치완료 된 것..

**Python censys\_io.py** – 센시스를 실행하는 것이다. // 센시스 api를 변수에 넣어줘라

My account – api에 가서 획득

**Export CENSYS\_API\_ID=**

**Pyhon censys\_io.py** 하면 동작이 되는 것을 알수있음.

-T TAGS 태그옵션 / -t HTML TITLE 아파치, 톰캣 이런것들 검색하면 되고 / -S HTTP\_SERVER

--limit LIMIT 결과값들에 대해서 제한하는 명령어

**Python censys\_io.py -t “Apache Tomcat” –limit 10** // 10800개의 결과값들이 나옴

**Pyhton censys\_io.py –html-title “Hacked by” –limit 20 –html** //해킹된 사이트에 대해 검사를 해서 520개 정도의 정보들이 나왔다. 🡪 /tmp/tmpKJLnpF의 사이트로 들어가보겠다.

다른 터미널 해서 **cd /tmp/tmpKJLnpF** – ls – 검색 하면 됨 .

**Firefox \*** //이렇게 하면 파이어폭스가 열리면서 여기있는 사이트들 다 오픈함.

**Python censys\_io.py –html-title “HFS” –limit 10 –html** //hfs의 타이틀이포함된 정보들 10개를 html로 저장하겠다. 라는 명령어 // 여기에 악성코드들이 많이 배포될 경우, 범죄자들이 많이 사용하는 경로이기 때문에

**Cd /tmp/tmpj\_S3Kw**

**Ls**

**Firefox \*** 이런식으로 검색해보면 파일들이 나옴. exe파일 .. rar 및 exe파일 같은 경우는 악성코드인지 아닌지 확인을 해봐야함 . 조심을 해야함. // 바이러스 토탈서비스나 세이프징 브라우즈 서비스나 결합을해서 활용할 수 있음.

**Python censys\_io.py –tags heartbleed –report location.country.raw**

//리포트정보를 뽑아내는데 하트블리드 취약점이 있는 것을 컨트리 기준으로 확인. /쇼단 컨트리랑 비슷한 느낌 facet랑 비슷한 . //75000개 하트블리드 취약점 노출되는 것을 볼 수 있다.

이런식으로 활용하는 것이 센시스 도구이다.