산업테러기반 2번째

센시스 : 쇼단보다 훨씬 많은 데이터를 가지고 있을 정도의 서비스 / 실무에서 악성코드 파일확인 할 경우 및 해킹을 당한 사이트 and 포트정보 확인 목적으로 사용중.

사용방법도 쇼단과 비슷하다.

장점 : 자세한 옵션들이 나온다. 여기서 ip정보를 찍으면 80.http.get.headers.server: 이렇게 하면 우리가 80포트를 사용하고있는 헤더 서버정보에 어떤 정보를 들어가있는지 찾아라 ! 라는 명령어

80.http.get.headers.server: apache : 아파치를 헤더 서버정보로 사용하고 있는 80포트

포트 정보 / 위치 정보 / 배너 그랩 정보들이 나온다. // 디테일 정보도 똑같이 관련된 정보들이 나옴.

22.ssh. .. 이런 것들이 하나의 옵션이다.

아파치를 사용하고 한국에서 사용하고 있는 것을 검색해라 !/ /뭐이런것들도 있음

Protocols: (“23/telnet” or “21/ftp”) - 23이나 21프로토콜을 사용하는 것들을 검색

즉, 이러한 태그들을 찾고 싶다 한다면은

80.http.get.body: wordpress 워드프레스가 본문에 들어가있는 것을 찾는 것

\\\\ 센시스에서 report로 들어가고 tags.raw라고 검색하면 센시스 쪽에서 검색을 했을 때, 태그정보들이 나온다. (센시스 기준으로)

Heartbleed와 mongodb들이 있다. 한번 검색해보면 tags; “mongodb”라고 찍히고 관련 정보들이 똑같이 나옴. – 쇼단보단 간략하게 나옴.

그래서 센시스에서 주제에 맞게 검색해서 정보를 크롤링 가능하다는 말인듯.

명령어 가이드를 찾아보고 이것을 활용해서 과제 하라.

다음시간은 censys 오픈 도구들에ㄷ대해서 살펴볼것이다.