|  |
| --- |
|  |
| **Censys API 활용법과 API를 활용하는 오픈도구들 조사 및 실습** |
|  |

|  |  |  |
| --- | --- | --- |
|  | 팀명: | 모의해킹36기 |
|  | **이름:** | **구본혁** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**문서 정보 / 수정 내역**

|  |  |
| --- | --- |
| File Name | Censys API 활용 및 기타 도구 실습 |
| 원안작성자 | 구본혁 |
| 수정작업자 | 구본혁 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 수정 날짜 | 대표 수정자 | Revision | 추가/수정 항목 | 내 용 |
| 2022.7.23 | 구본혁 | 0.0 | 초안 작성 | 초안 작성 |
| 2022.7.24 | 구본혁 | 0.1 | 내용 추가 및 수정 | 본문 작성 및 api실습 |
| 2022.7.26 | 구본혁 | 0.2 | 오탈자 교정 | 오탈자 교정 |
| 2022.08.03 | 구본혁 | 0.3 | 그림 교체 | 피드백 수용 후 사진 교체 |
|  |  |  |  |  |
|  |  |  |  |  |

표 ‑ 문서 정보 / 수정 내역

목 차

[1 개요 6](#_Toc110428463)

[1.1 프로젝트 주제 6](#_Toc110428464)

[1.2 프로젝트 추진 배경 및 목표 6](#_Toc110428465)

[1.3 프로젝트 요약 6](#_Toc110428466)

[2 Censys 개요 7](#_Toc110428467)

[2.1 OSINT의 의미 7](#_Toc110428468)

[2.2 Censys란? 7](#_Toc110428469)

[2.3 Censys 기본옵션 7](#_Toc110428470)

[3 Censys API 활용법 9](#_Toc110428471)

[3.1 기본설정 9](#_Toc110428472)

[3.2 Python 소스코드 10](#_Toc110428473)

[4 Censys API를 활용한 오픈도구 조사 및 실습 12](#_Toc110428474)

[4.1 Censys-subdomain-finder 12](#_Toc110428475)

[4.1.1 사용법 13](#_Toc110428476)

[5 참고 문헌 14](#_Toc110428477)

[5.1 참조 링크 14](#_Toc110428478)

표 목차

[표 1‑1 문서 정보 / 수정 내역 2](#_Toc110428512)

[표 1‑1 프로젝트 주제 6](#_Toc110428513)

[표 1‑2 프로젝트 추진 배경 및 목표 6](#_Toc110428514)

[표 1‑3 프로젝트 요약 6](#_Toc110428515)

[표 2‑1 host dataset에서 검색 가능한 필드 8](#_Toc110428516)

[표 5‑1 참조 홈페이지 14](#_Toc110428517)

그림 목차

[그림 2‑1 censys검색화면 7](#_Toc110428494)

[그림 2‑2 censys ip 검색예시 8](#_Toc110428495)

[그림 3‑1 Censys 기본 설정 9](#_Toc110428496)

[그림 3‑2 Censys 검색을 위한 파이썬 파일 생성 10](#_Toc110428497)

[그림 3‑3 Python 소스코드(search) 결과 10](#_Toc110428498)

[그림 3‑4 Python소스코드(view) 11](#_Toc110428499)

[그림 3‑5 Python소스코드(view) 결과 11](#_Toc110428500)

[그림 4‑1 저장소 복제 12](#_Toc110428501)

[그림 4‑2 python3.9-venv 설치 12](#_Toc110428502)

[그림 4‑3 가상환경 활성화 12](#_Toc110428503)

[그림 4‑4 샘플 하위 도메인 검색 13](#_Toc110428504)

[그림 4‑5 구글 하위 도메인 검색 13](#_Toc110428505)

# 개요

## 프로젝트 주제

|  |
| --- |
| 1. OSINT 개념 잡기 2. Censys API를 활용하는 오픈도구 실습 |

표 ‑ 프로젝트 주제

## 프로젝트 추진 배경 및 목표

|  |
| --- |
| 1. OSINT 이해 2. Censys 이해 3. Censys API 활용 4. Censys API를 활용한 오픈도구 실습 |

표 ‑ 프로젝트 추진 배경 및 목표

## 프로젝트 요약

|  |
| --- |
| 1. Censys API 활용법과 API를 활용하는 오픈도구 조사 및 실습 |

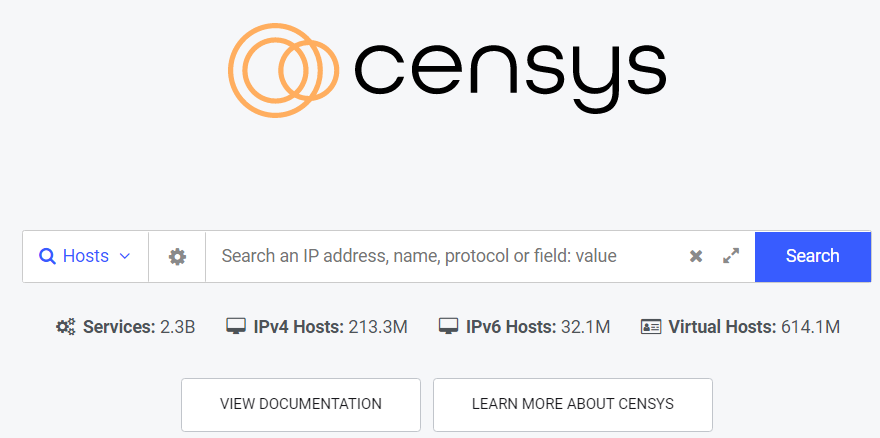
표 ‑ 프로젝트 요약

# Censys 개요

## OSINT의 의미

OSINT는 Open Source Intelligence의 약자로, Open Source와 군대에서 첩보활동인 Intelligence가 합쳐져 탄생하였다. OSINT는 공개된 출처에서 합법적으로 정보를 얻는 전반적인 과정을 의미한다. OSINT는 사이버 보안 분야에서 활발하게 사용된다. 취약점 진단 및 모의해킹, 악성코드 분석, 포렌식, 침해사고조사 및 대응에서 OSINT는 꼭 필요하다고 할 수 있다.

## Censys란?

그림 ‑ censys검색화면

Censys는 2013년 Michagan대학교 연구팀이 만든 Python기반의 취약점 검색엔진이다. Censys는 공개된 취약점을 찾는데 중점을 둔다. 그리고 수집한 정보에 대한 결과 분석 및 취약점에 대한 보안 조치를 할 수 있다. Censys는 포트 스캔을 기반으로 웹 서버, 디바이스, 네트워크, 스위치, 라우터, IOT, 산업IOT 등을 검색할 수 있고, Zmap 스캔방식으로 전 세계를 대상으로 스캔을 수행한다. Censys는 알려진 프로토콜을 대상으로 스캔한다. 하트블리드 등을 포함한 웹 취약점이 적용되는 시스템에 대한 정보를 확인할 수 있으며, 여기서 발견된 정보는 Censys 검색엔진을 통해 조회할 수 있다. 또한, IP나 인증서로도 점검할 수 있다.

## Censys 기본옵션

Censys api활용 전 기본옵션을 알아보자. censys기본 필드는 다음과 같다.

|  |  |
| --- | --- |
| Host information | 호스트 정보 |
| Host operating system | 호스트의 운영체제 정보 |
| Host location | 호스트의 위치정보 |
| Host autonomous system | 호스트 자동화 시스템 정보 |
| Host DNS | 호스트 DNS정보 |
| Service information | 서비스 정보 |
| TLS | TLS정보 |

표 ‑ host dataset에서 검색 가능한 필드

표 2‑1은 censys에서 주로 사용하는 필드이다. 이것 말고도 ampq, software 등 다양한 필드가 존재하며 총 16개 필드가 존재한다. 검색 시 사용가능한 옵션이 뜨고 검색 속도도 빠르다.

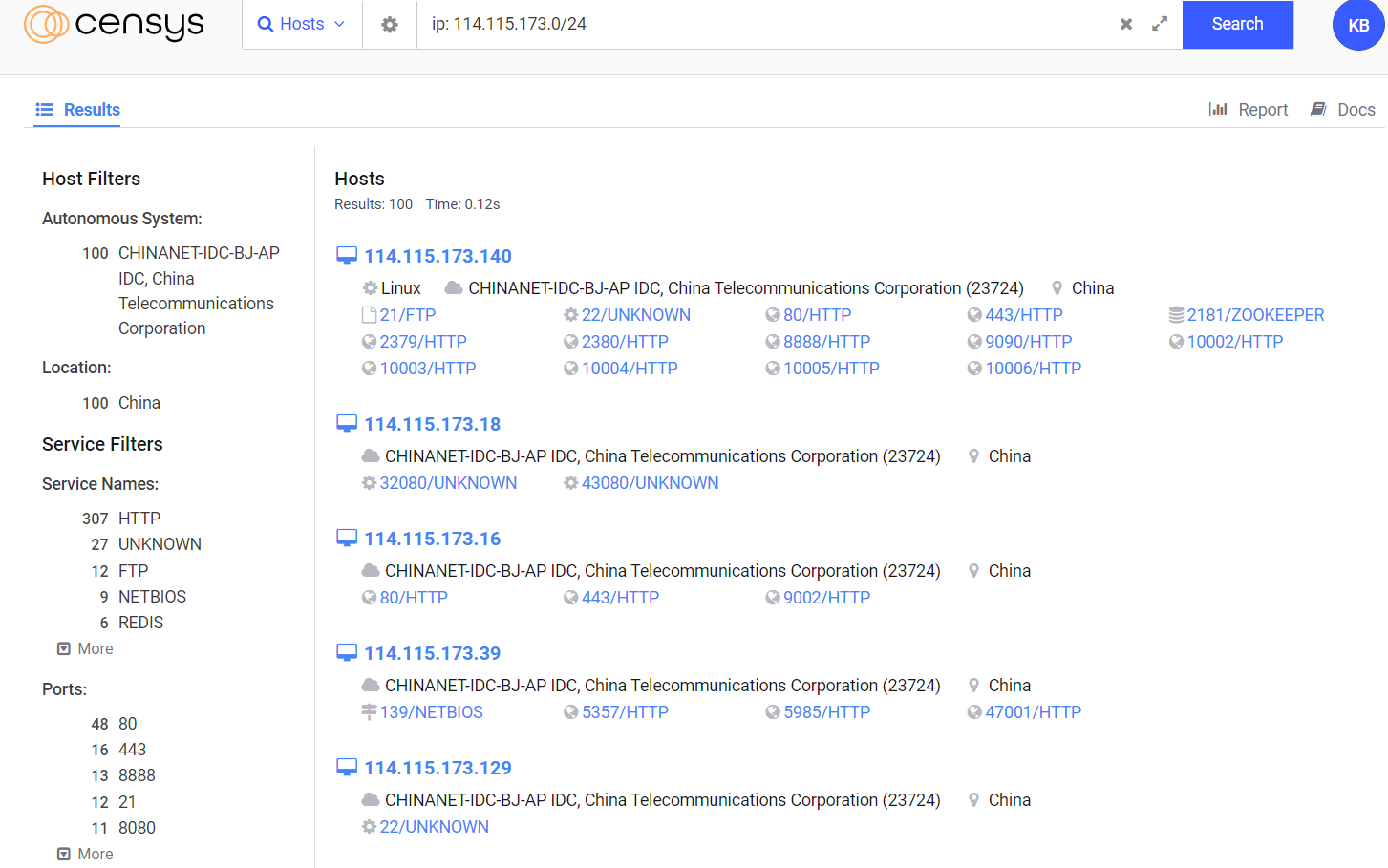


그림 ‑ censys ip 검색예시

그림 2‑2는 Host information중 ip path 를 이용하여 검색한 결과이다.

# Censys API 활용법

Censys API는 웹 인터페이스와 같은 데이터에 대한 프로그래밍적 접근이 가능하다. 엔드 포인트는 <https://censys.io>가 호스팅하며 API ID와 API Secret 기본 http인증으로 이용 가능하며 계정마다 임계치 검색 비율이 존재한다.

Censys 라이브러리 특징으로는 다음과 같다.

〮censys데이터검색

〮검색 대용량 인증서 조회

〮대용량 데이터 다운로드

〮Censys ASM의 자산, 이벤트, 시드

〮Command Line Interface

## 기본설정

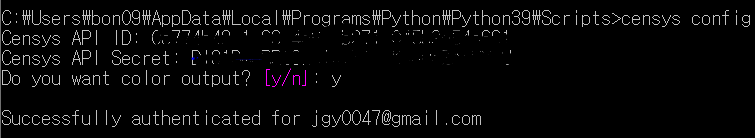


그림 ‑ Censys 기본 설정

Censys API를 사용하려면, 자격 증명을 위한 API ID와 API Secret를 입력한다. ‘censys config’명령어를 입력하여 API ID와 Secret을 입력하면, 자신이 가입한 이메일로 인증이 성공했다는 메시지가 나온다. ID와 비밀키는 제3자에게 노출되지 않도록 비식별화 하였다.

## Python 소스코드

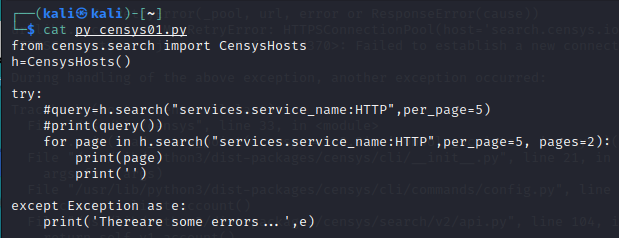


그림 ‑ Censys 검색을 위한 파이썬 파일 생성

python 코딩을 통해 Censys 검색을 이용할 수 있다. python 소스코드는 Censys API를 이용하여 원하는 검색 결과를 출력하고 관리할 수 있다.

이제 python 소스코드를 활용한 Censys 검색을 할 것이다. Censys.search.v2 패키지는 Certs 인덱스와 상호 작용하는 CensysCerts와 호스트 인덱스와 상호 작용하는 CensysHosts를 제공한다. 이 중 CensysHosts를 사용하여 py\_censys01.py를 작성하였고 작성 결과는 그림 3‑2와 같다.

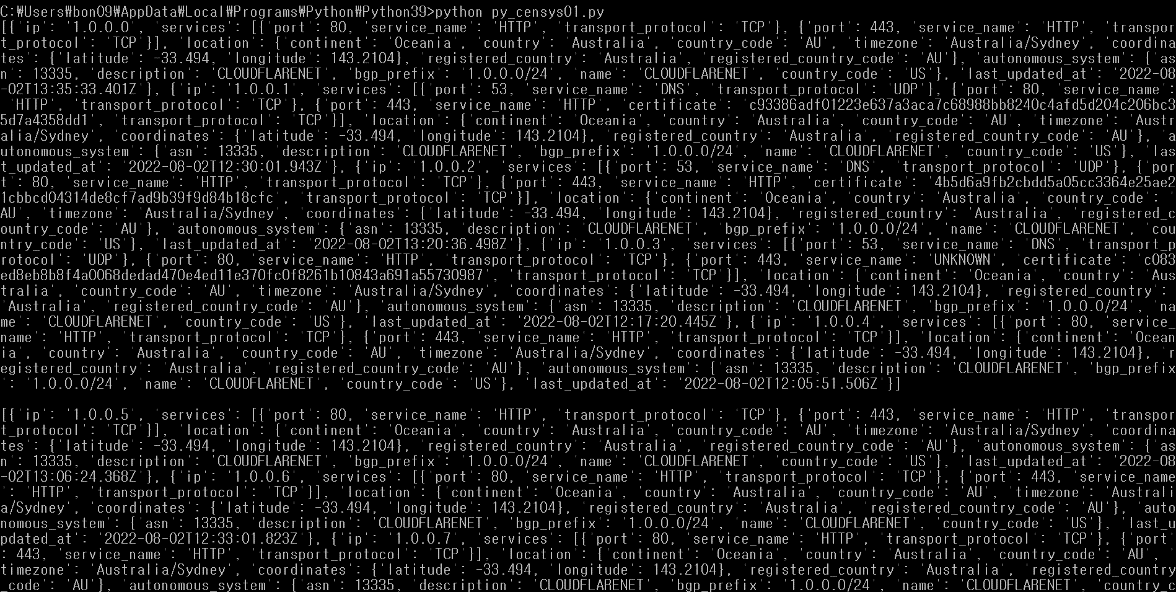


그림 ‑ Python 소스코드(search) 결과

py\_censys01.py의 결과는 그림 3‑3와 같다.

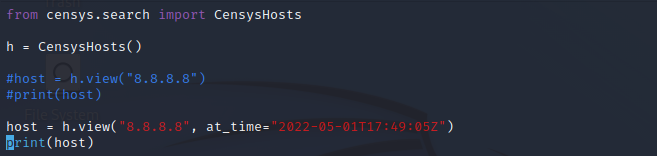


그림 ‑ Python소스코드(view)

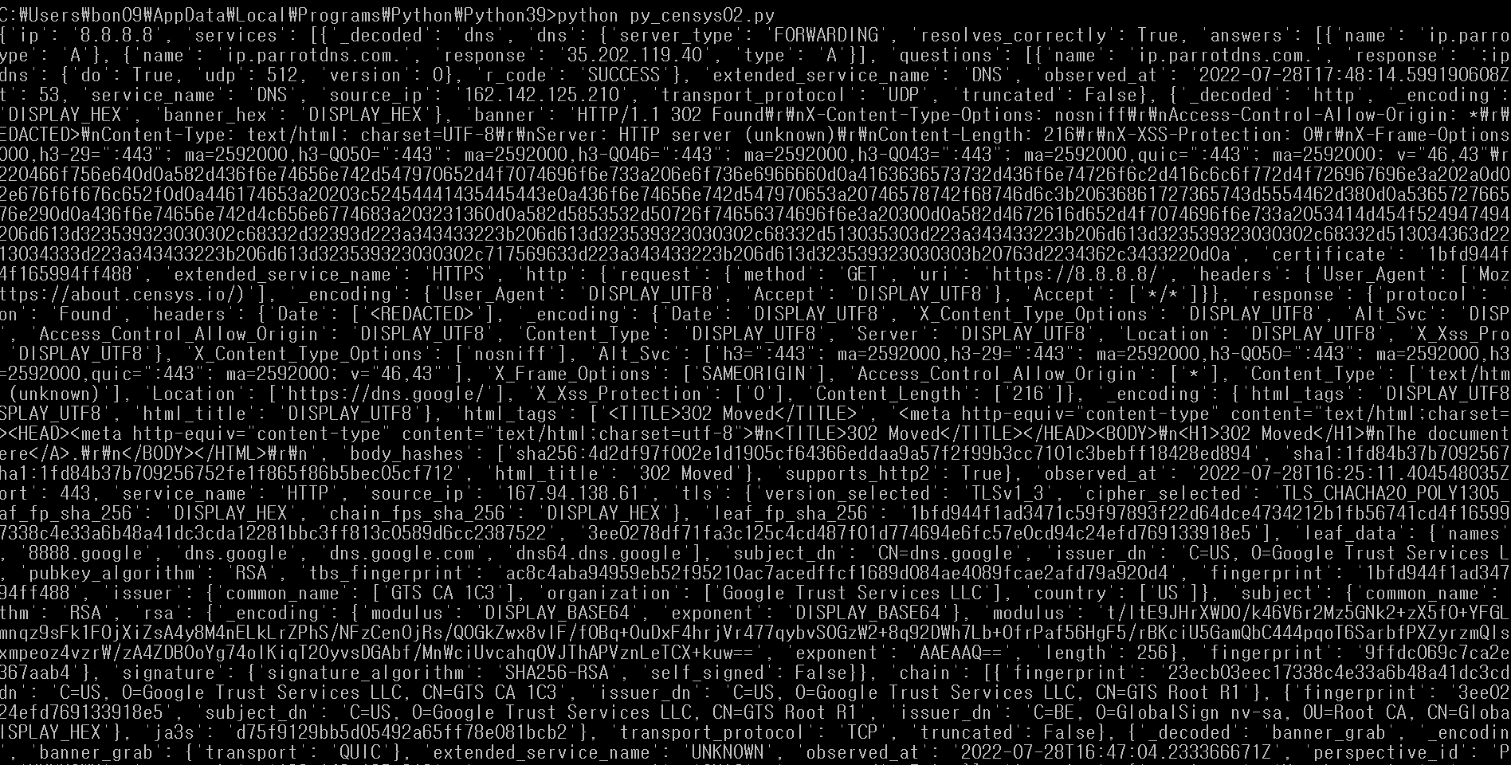


그림 ‑ Python소스코드(view) 결과

그림 3‑4 코드는 특정 호스트 및 해당 서비스를 가져오는 것으로, CensysHosts에 있는 정보를 가져와 View를 수행하는 것이다. 필터 at\_time이라는 변수에 적힌 시간대에 8.8.8.8(구글DNS) 호스트의 상세정보를 출력한다는 의미를 담고 있다. 그림 3‑4의 결과는 그림 3‑5과 같으며, 7일 기준으로 보여준다.

〮search함수 원형

**search(*query:***[***str***](https://docs.python.org/3/library/stdtypes.html#str)**, *per\_page:***[***Optional***](https://docs.python.org/3/library/typing.html#typing.Optional)***[***[***int***](https://docs.python.org/3/library/functions.html#int)***] = None*, *cursor:***[***Optional***](https://docs.python.org/3/library/typing.html#typing.Optional)***[***[***str***](https://docs.python.org/3/library/stdtypes.html#str)***] = None*, *pages:***[***int***](https://docs.python.org/3/library/functions.html#int)***= 1*, *\*\*kwargs:***[***Any***](https://docs.python.org/3/library/typing.html#typing.Any)**)**

〮view함수 원형

**view(*document\_id:***[***str***](https://docs.python.org/3/library/stdtypes.html#str)**, *at\_time:***[***Optional***](https://docs.python.org/3/library/typing.html#typing.Optional)***[***[***Union***](https://docs.python.org/3/library/typing.html#typing.Union)***[***[***str***](https://docs.python.org/3/library/stdtypes.html#str)***,***[***datetime.date***](https://docs.python.org/3/library/datetime.html#datetime.date)***,***[***datetime.datetime***](https://docs.python.org/3/library/datetime.html#datetime.datetime)***]] = None*)**

매개변수:

# Censys API를 활용한 오픈도구 조사 및 실습

## Censys-subdomain-finder

Censys API를 사용한 오픈소스 도구로는 Censys-subdomain-finder가 있다. Censys-subdomain-finder는 Censys에 있는 인증서 투명성 로그를 사용하여 하위 도메인을 열거하는 도구이다.

초기 설정은 외부 변수 export를 사용하여 CENSYS\_API\_ID와 CENSYS\_API\_SECRET에 자신의 censys API ID와 SECRET값을 넣어줘야 한다. 주의해야할 점이 있다면, 이 도구를 사용하기 위해서 꼭 가상환경 ‘virtualenv’가 필요하다는 것이다.

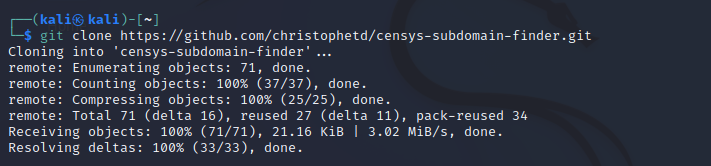


그림 ‑ 저장소 복제

‘git clone’을 통해 자신이 사용하고자 하는 깃허브의 저장소를 복제한다.

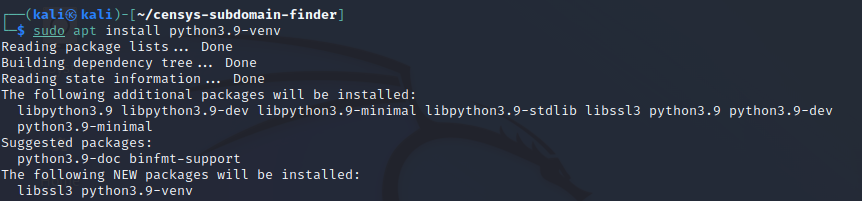


그림 ‑ python3.9-venv 설치

censys-subdomain-finder을 사용하기 위해 필요한 가상환경을 만들기 위해 python3.9-venv 설치한다.

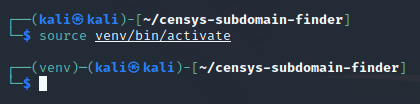


그림 ‑ 가상환경 활성화

‘source 가상 환경 경로/bin/activate’을 입력하여 가상 환경을 활성화하고, ‘pip install -r requirements.txt’로 필요한 라이브러리를 설치한다.

### 사용법

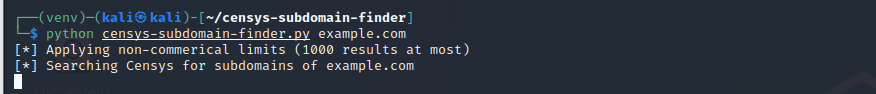


그림 ‑ 샘플 하위 도메인 검색

‘python censys-subdomain-finder.py example.com’을 입력하여 해당 주소의 하위 도메인을 확인할 수 있다.

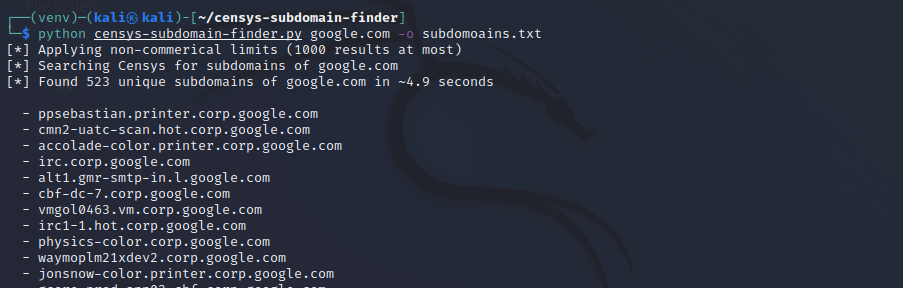


그림 ‑ 구글 하위 도메인 검색

‘python censys-subdomain-finder.py google.com -o subdomains.txt’를 입력하여 구글의 하위 도메인을 검색하고 검색 결과를 subdomains.txt파일로 저장한다.

# 참고 문헌

## 참조 링크

|  |
| --- |
| 참조 홈페이지 |
| <https://censyspython.readthedocs>  <http://www.kshieldjr.org/rsrh_rpt_det.do?id=163.io/en/stable/censys.search.v2.html#censys.search.v2.api.CensysSearchAPIv2.search>  <https://github.com/christophetd/censys-subdomain-finder>  <https://pypi.org/project/censys> |

표 ‑ 참조 홈페이지