


Censys API 활용법과 API 를 활용하는 오픈도구들 조사 및 실습

팀 명 : 모 의 해 킹 3 6 기

이 름 : 구 본 혁

2022-08-03


	Censys API 활용 및 기타 도구 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.3	2022.08.03	

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 1-1 문서 정보 / 수정 내역

	Censys API 활용 및 기타 도구 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.3	2022.08.03	

목 차

1	개요	6
1.1	프로젝트 주제	6
1.2	프로젝트 추진 배경 및 목표	6
1.3	프로젝트 요약	6
2	CENSYS 개요	7
2.1	OSINT의 의미	7
2.2	CENSYS란?	7
2.3	CENSYS 기본옵션	7
3	CENSYS API 활용법	9
3.1	기본설정	9
3.2	PYTHON 소스코드	10
4	CENSYS API를 활용한 오픈도구 조사 및 실습	12
4.1	CENSYS-SUBDOMAIN-FINDER	12
4.1.1	사용법	13
5	참고 문헌	14
5.1	참조 링크	14


	Censys API 활용 및 기타 도구 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.3	2022.08.03	

표 목차

표 1-1 문서 정보 / 수정 내역	2
표 1-1 프로젝트 주제	6
표 1-2 프로젝트 추진 배경 및 목표	6
표 1-3 프로젝트 요약	6
표 2-1 host dataset에서 검색 가능한 필드.....	8
표 5-1 참조 홈페이지	14



	Censys API 활용 및 기타 도구 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.3	2022.08.03	

그림 목차

그림 2-1 censys검색화면	7
그림 2-2 censys ip 검색예시	8
그림 3-1 Censys 기본 설정	9
그림 3-2 Censys 검색을 위한 파이썬 파일 생성	10
그림 3-3 Python 소스코드(search) 결과	10
그림 3-4 Python소스코드(view)	11
그림 3-5 Python소스코드(view) 결과	11
그림 4-1 저장소 복제	12
그림 4-2 python3.9-venv 설치	12
그림 4-3 가상환경 활성화	12
그림 4-4 샘플 하위 도메인 검색	13
그림 4-5 구글 하위 도메인 검색	13

	Censys API 활용 및 기타 도구 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.3	2022.08.03	

1 개요

1.1 프로젝트 주제

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

표 1-1 프로젝트 주제

1.2 프로젝트 추진 배경 및 목표


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

표 1-2 프로젝트 추진 배경 및 목표

1.3 프로젝트 요약

1. Censys API 활용법과 API를 활용하는 오픈도구 조사 및 실습

표 1-3 프로젝트 요약

	Censys API 활용 및 기타 도구 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.3	2022.08.03	

2 Censys 개요

2.1 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.

2.2 Censys란?

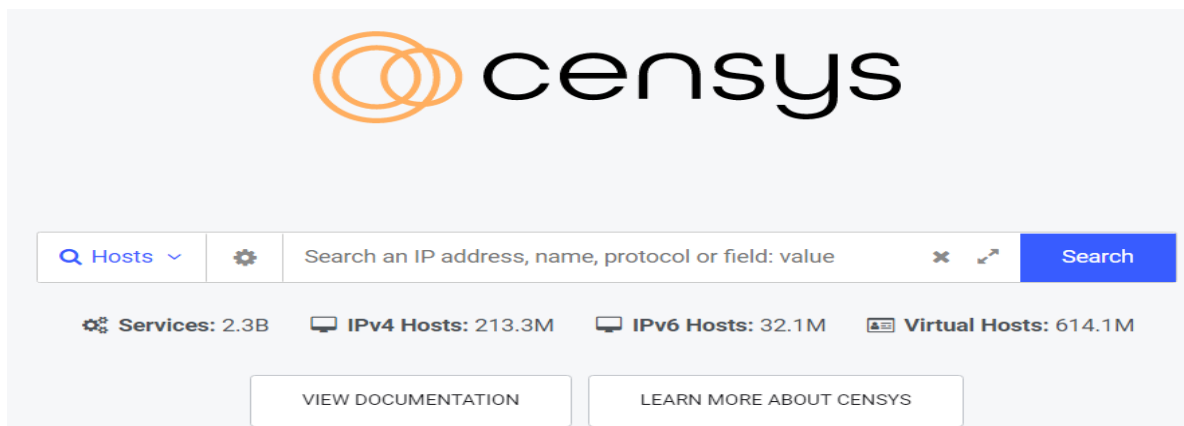



그림 2-1 censys검색화면

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.

2.3 Censys 기본옵션

Censys api활용 전 기본옵션을 알아보자. censys기본 필드는 다음과 같다.

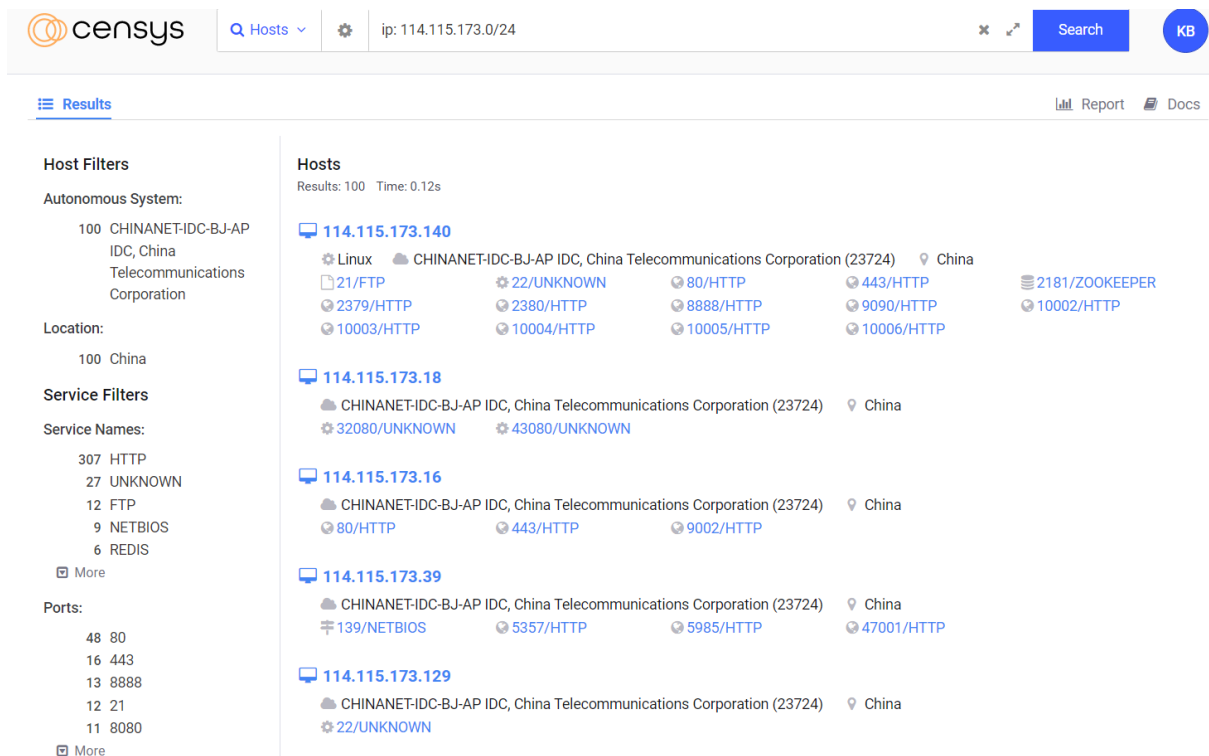
Host information	호스트 정보
Host operating system	호스트의 운영체제 정보
Host location	호스트의 위치정보
Host autonomous system	호스트 자동화 시스템 정보

	Censys API 활용 및 기타 도구 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.3	2022.08.03	

Host DNS	호스트 DNS정보
Service information	서비스 정보
TLS	TLS정보

표 2-1 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.




The screenshot shows the Censys search results for the IP range 114.115.173.0/24. The interface includes a sidebar with filters and a main results section. The filters include Hosts, Autonomous System (CHINANET-IDC-BJ-AP), Location (China), Service Filters (HTTP, UNKNOWN, FTP, NETBIOS, REDIS), and Ports (80, 443, 8888, 21, 8080). The main results section lists several IP addresses with their associated services and locations.

IP Address	Services	Location
114.115.173.140	Linux, CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation (23724), 21/FTP, 22/UNKNOWN, 80/HTTP, 443/HTTP, 2379/HTTP, 2380/HTTP, 8888/HTTP, 9090/HTTP, 10003/HTTP, 10004/HTTP, 10005/HTTP, 10006/HTTP, 2181/ZOOKEEPER, 10002/HTTP	China
114.115.173.18	CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation (23724), 32080/UNKNOWN, 43080/UNKNOWN	China
114.115.173.16	CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation (23724), 80/HTTP, 443/HTTP, 9002/HTTP	China
114.115.173.39	CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation (23724), 139/NETBIOS, 5357/HTTP, 5985/HTTP, 47001/HTTP	China
114.115.173.129	CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation (23724), 22/UNKNOWN	China

그림 2-2 censys ip 검색예시

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

	Censys API 활용 및 기타 도구 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.3	2022.08.03	

4 Censys API를 활용한 오픈도구 조사 및 실습

4.1 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.

```
(kali@kali)-[~]
$ git clone https://github.com/christophetd/censys-subdomain-finder.git
Cloning into 'censys-subdomain-finder' ...
remote: Enumerating objects: 71, done.
remote: Counting objects: 100% (37/37), done.
remote: Compressing objects: 100% (25/25), done.
remote: Total 71 (delta 16), reused 27 (delta 11), pack-reused 34
Receiving objects: 100% (71/71), 21.16 KiB | 3.02 MiB/s, done.
Resolving deltas: 100% (33/33), done.
```

그림 4-1 저장소 복제

'git clone'을 통해 자신이 사용하고자 하는 깃허브의 저장소를 복제한다.

```
(kali@kali)-[~/censys-subdomain-finder]
$ sudo apt install python3.9-venv
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libpython3.9 libpython3.9-dev libpython3.9-minimal libpython3.9-stdlib libssl3 python3.9 python3.9-dev
  python3.9-minimal
Suggested packages:
  python3.9-doc binfmt-support
The following NEW packages will be installed:
  libssl3 python3.9-venv
```

그림 4-2 python3.9-venv 설치


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

```
(kali@kali)-[~/censys-subdomain-finder]
$ source venv/bin/activate

(venv)-(kali@kali)-[~/censys-subdomain-finder]
$
```

그림 4-3 가상환경 활성화

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

	Censys API 활용 및 기타 도구 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.3	2022.08.03	

4.1.1 사용법

```
(venv)-(kali@kali)-[~/censys-subdomain-finder]
$ python censys-subdomain-finder.py example.com
[*] Applying non-commercial limits (1000 results at most)
[*] Searching Censys for subdomains of example.com
```

그림 4-4 샘플 하위 도메인 검색


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

```
(venv)-(kali@kali)-[~/censys-subdomain-finder]
$ python censys-subdomain-finder.py google.com -o subdomains.txt
[*] Applying non-commercial limits (1000 results at most)
[*] Searching Censys for subdomains of google.com
[*] Found 523 unique subdomains of google.com in ~4.9 seconds

- ppsebastian.printer.corp.google.com
- cmn2-uatc-scan.hot.corp.google.com
- accolade-color.printer.corp.google.com
- irc.corp.google.com
- alt1.gmr-smtp-in.l.google.com
- cbf-dc-7.corp.google.com
- vmgol0463.vm.corp.google.com
- irc1-1.hot.corp.google.com
- physics-color.corp.google.com
- waymopl21xdev2.corp.google.com
- jonsnow-color.printer.corp.google.com
```

그림 4-5 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.

	Censys API 활용 및 기타 도구 실습			모의해킹 36기
	Category	문서 버전	문서 최종 수정일	
	Report	0.3	2022.08.03	

5 참고 문헌

5.1 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 5-1 참조 홈페이지