



LABORATORIO 3.1 - Make a profile for ekoparty.org using Censys

TEMA: *Discovery (OSINT)*

Objetivos:

- Buscar vulnerabilidades tecnológicas, versión de web server, subdominios, correos electrónicos.

Descripción / Escenario:

Durante la etapa de reconocimiento un buen Red Teamer hacer su tarea, la cual es

Recursos necesarios:

Máquina Virtual atacante: Kali Linux 2019.

Máquina Virtual objetivo: Windows 10 Pro.

Procedimiento:

Paso 1:

Generar API keys en www.censys.io

Loguearse en el portal y en la pestaña account dar click en la opción API.

Figura 1. Generación API keys Censys

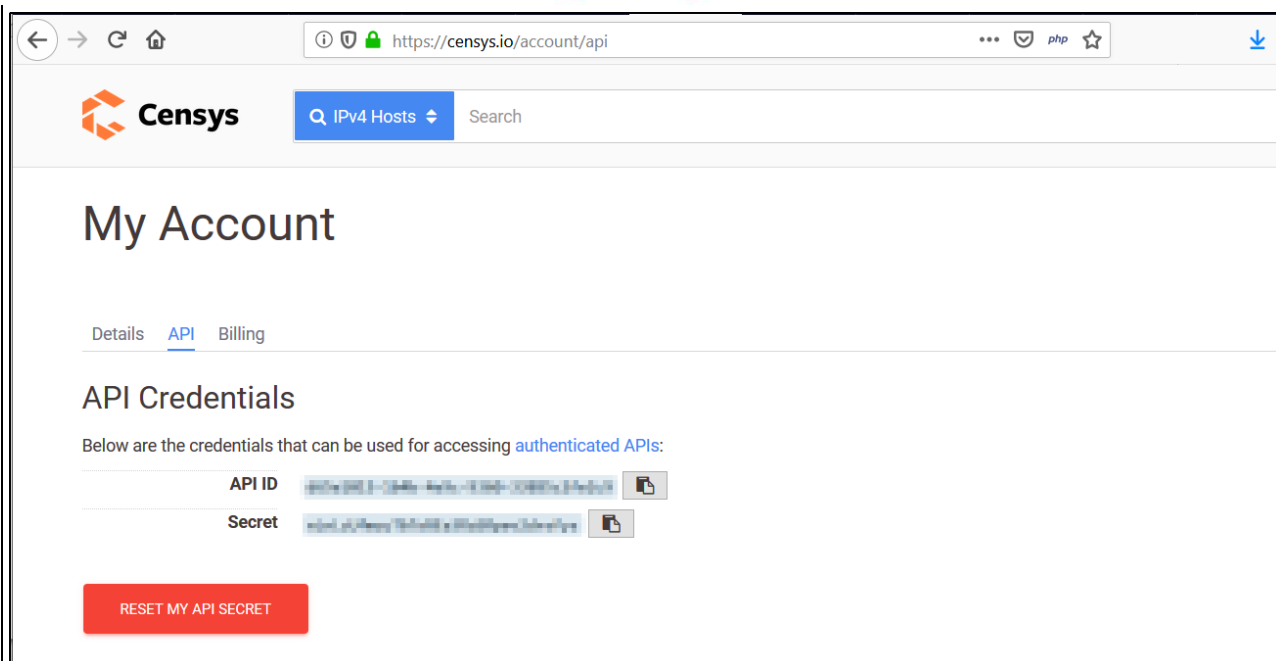


Figura 2. Generación API keys Censys

Paso 2:

Añadir las API keys de Censys en la variables de ambiente del OS, en este caso Kali Linux

```
#export CENSYS_API_ID=.....
#export CENSYS_API_SECRET=.....
```

Paso 3:

Descargar los script desde los siguientes enlace:

git clone --recursive <https://github.com/0xbharath/censys-enumeration>

git clone --recursive <https://github.com/christophetd/censys-subdomain-finder>

Paso 4:

Instalar todas las librerías requeridas

pip2.7 install -r requirements.txt

```
root@pwnag3:/opt/censys-enumeration# pip2.7 install -r requirements.txt
```

Figura 3. Instalación de las librerías en Python

pip2.7 install -r requirements.txt

```
root@pwnag3:/opt/censys-subdomain-finder# pip2.7 install -r requirements.txt
```

Figura 4. Instalación de las librerías en Python



Paso 5:

Ejecutar el script (censys_subdomain_finder.py) hacia el dominio ekoparty.org desde la ubicación donde fue descargado

python censys_subdomain_finder.py ekoparty.org

```
root@pwnag3:/opt/censys-subdomain-finder# python censys_subdomain_finder.py ekoparty.org
[*] Searching Censys for subdomains of ekoparty.org
[*] Found 12 unique subdomains of ekoparty.org in ~2.5 seconds

- hacktheprinter.ekoparty.org
- ww2.ekoparty.org
- ekol3.ekoparty.org
- mail.ekoparty.org
- oc.ekoparty.org
- www.ekoparty.org
- ekoparty.org
- cfp.ekoparty.org
- blog.ekoparty.org
- d3v.ekoparty.org
- ctf.ekoparty.org
- www.cfp.ekoparty.org
```

Figura 5. Resultado ejecución de script (censys_subdomain_finder.py)

Paso 6:

Ejecutar el script (censys_enumeration.py)

Primero crear el archivo dominio.txt y que este contenga ekoparty.org

echo "ekoparty.org" > dominio.txt

python2.7 censys_enumeration.py --verbose dominio.txt

```
root@pwnag3:/opt/censys-enumeration# python2.7 censys_enumeration.py --verbose dominio.txt
```

Figura 5. Resultado ejecución de script (censys_enumeration.py)

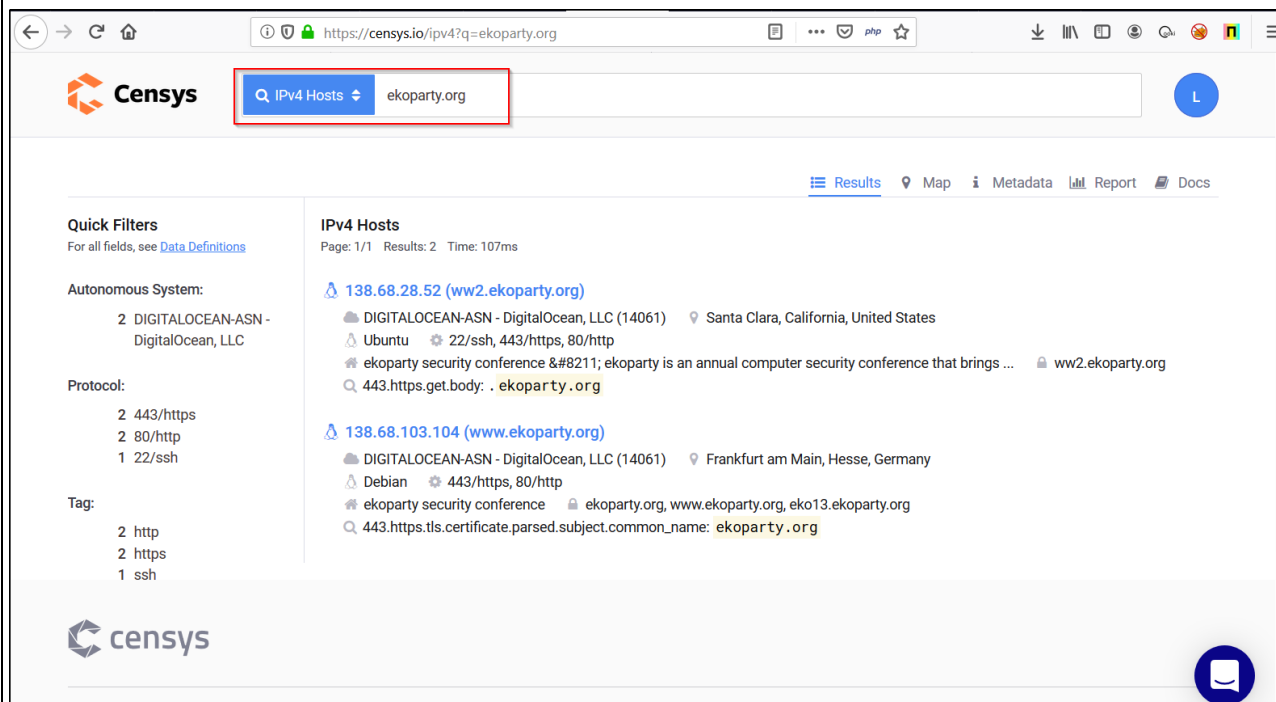
```
root@pwnag3:/opt/censys-enumeration# python2.7 censys_enumeration.py --verbose dominio.txt
[+] Extracting certificates using Censys
[+] Extracting emails belonging to ekoparty.org from SSL/TLS certificates
[!] Did not find any email addresses
[+] Extracting sub-domains for ekoparty.org from certificates
[*] Total unique subdomains found for ekoparty.org: 12
blog.ekoparty.org
cfp.ekoparty.org
ctf.ekoparty.org
d3v.ekoparty.org
ekol3.ekoparty.org
ekoparty.org
hacktheprinter.ekoparty.org
mail.ekoparty.org
oc.ekoparty.org
ww2.ekoparty.org
www.cfp.ekoparty.org
www.ekoparty.org
[+] Results written to JSON file : /opt/censys-enumeration/json_results
root@pwnag3:/opt/censys-enumeration#
```

Figura 6 Resultado ejecución script (censys_enumeration.py)

Paso 7

Ingresar nuevamente a <https://www.censys.io>

Escribir [ekoparty.org](https://www.censys.io) y presionar enter para iniciar una búsqueda



The screenshot shows the Censys search interface. The search bar contains 'ekoparty.org'. The results are displayed under the 'IPv4 Hosts' tab. Two results are shown:

- 138.68.28.52 (ww2.ekoparty.org)**: DIGITALOCEAN-ASN - DigitalOcean, LLC (14061), Santa Clara, California, United States. Running Ubuntu 22/ssh, 443/https, 80/http. ekoparty security conference – ekoparty is an annual computer security conference that brings ... ww2.ekoparty.org. 443.https.get.body: . ekoparty.org
- 138.68.103.104 (www.ekoparty.org)**: DIGITALOCEAN-ASN - DigitalOcean, LLC (14061), Frankfurt am Main, Hesse, Germany. Running Debian 443/https, 80/http. ekoparty security conference ekoparty.org, www.ekoparty.org, eko13.ekoparty.org. 443.https.tls.certificate.parsed.subject.common_name: ekoparty.org

Figura 7 resultado búsqueda ekoparty.org en censys.io

Posteriormente procedemos a investigar cada IP asociada y podemos apreciar la versión de SSh que está corriendo, la versión de apache, los resultados de whois

22.ssh.v2.banner.comment	Ubuntu-4ubuntu0.3
22.ssh.v2.banner.raw	SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
22.ssh.v2.banner.software	OpenSSH_7.6p1
22.ssh.v2.banner.version	2.0
22.ssh.v2.metadata.description	OpenSSH 7.6p1
22.ssh.v2.metadata.product	OpenSSH
22.ssh.v2.metadata.version	7.6p1
22.ssh.v2.selected.client_to_server.cipher	aes128-ctr
22.ssh.v2.selected.client_to_server.compression	none
22.ssh.v2.selected.client_to_server.mac	hmac-sha2-256
22.ssh.v2.selected.host_key_algorithm	ecdsa-sha2-nistp256
22.ssh.v2.selected.kex_algorithm	curve25519-sha256@libssh.org
22.ssh.v2.selected.server_to_client.cipher	aes128-ctr
22.ssh.v2.selected.server_to_client.compression	none
22.ssh.v2.selected.server_to_client.mac	hmac-sha2-256
22.ssh.v2.server_host_key.ecdsa_public_key.b	WsY12Ko6k+ez671VdpiGvGudBrDMU7D20848PifSYEs=
22.ssh.v2.server_host_key.ecdsa_public_key.curve	P-256
22.ssh.v2.server_host_key.ecdsa_public_key.gx	axfR8uEsQkf4vObly6RA8ncDfYE6zOg9KE5RdiYwpY=
22.ssh.v2.server_host_key.ecdsa_public_key.gy	T+NC4uAaf5u05+tkfA+aE5u0M1d4uV70u77AaDe0l1f1-

Figura 7 versión de SSH y sistema operativo obtenido del banner ssh en la búsqueda en censys.io

Comentarios:



Open-Sec

They run automated tools, We have Pentesters



RED TEAM :
BREAKING SECURITY FOR REAL