

Ensayo de los resultados obtenidos

Del escaneo pasivo

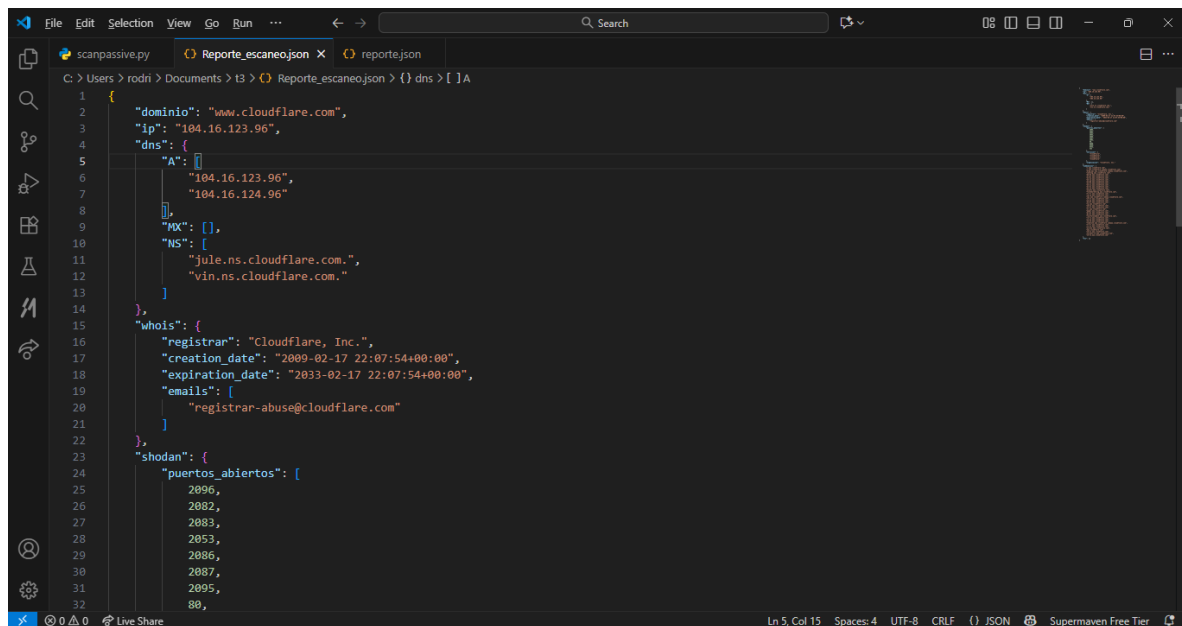
Funcionalidad del script:

Ejecutando el script pasivo de Python usando una url:

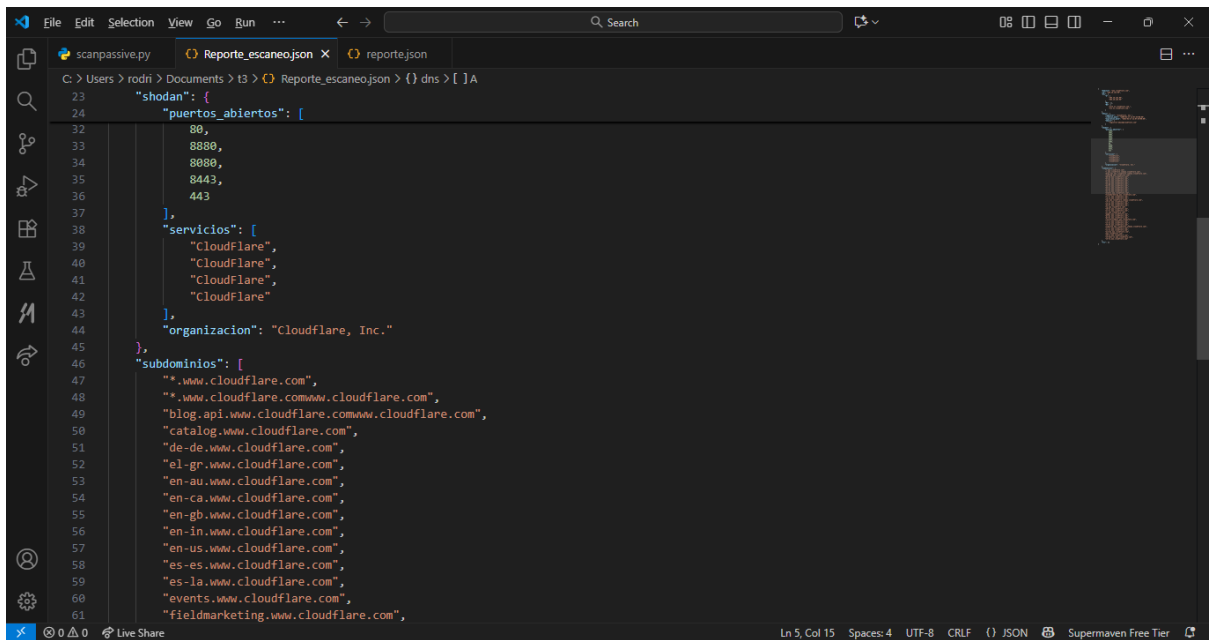
- Extraemos el dominio limpio
- Consulta registros DNS públicos
- Obtiene información WHOIS/RDAP
- Resuelve la IP y consulta Shodan
- Busca subdominios en certificados públicos
- Guarda todo en un archivo JSON

Datos obtenidos y sus usos en Ciberseguridad

Los resultados obtenidos nos lo dan en un archivo JSON



```
1 {
2   "dominio": "www.cloudflare.com",
3   "ip": "104.16.123.96",
4   "dns": {
5     "A": [
6       "104.16.123.96",
7       "104.16.124.96"
8     ],
9     "MX": [],
10    "NS": [
11      "jule.ns.cloudflare.com.",
12      "vin.ns.cloudflare.com."
13    ]
14  },
15  "whois": {
16    "registrar": "Cloudflare, Inc.",
17    "creation_date": "2009-02-17 22:07:54+00:00",
18    "expiration_date": "2033-02-17 22:07:54+00:00",
19    "emails": [
20      "registrar-abuse@cloudflare.com"
21    ]
22  },
23  "shodan": {
24    "puertos_abiertos": [
25      2096,
26      2082,
27      2083,
28      2053,
29      2086,
30      2087,
31      2095,
32      80,
```



```
23 "shodan": {
24   "puertos_abiertos": [
32     80,
33     8880,
34     8080,
35     8443,
36     443
37   ],
38   "servicios": [
39     "CloudFlare",
40     "CloudFlare",
41     "CloudFlare",
42     "CloudFlare"
43   ],
44   "organizacion": "Cloudflare, Inc."
45 },
46 "subdominios": [
47   "*.www.cloudflare.com",
48   "*.www.cloudflare.comwww.cloudflare.com",
49   "blog.api.cloudflare.comwww.cloudflare.com",
50   "catalog.cloudflare.com",
51   "de-de.www.cloudflare.com",
52   "el-gr.www.cloudflare.com",
53   "en-au.www.cloudflare.com",
54   "en-ca.www.cloudflare.com",
55   "en-gb.www.cloudflare.com",
56   "en-in.www.cloudflare.com",
57   "en-us.www.cloudflare.com",
58   "es-es.www.cloudflare.com",
59   "es-la.www.cloudflare.com",
60   "events.www.cloudflare.com",
61   "fieldmarketing.www.cloudflare.com",
```

Dominio e IP

Conseguimos la IP del dominio que es "104.16.123.96" esto nos pueden servir para identificar la infraestructura detrás del dominio, verificar si nos exponen o no su IP directa, y correlacionarlas con otras IPs con dominios.

Los registros DNS (A,MX,NS)

```
"A": [
  "104.16.123.96",
  "104.16.124.96"
],
"MX": [],
"NS": [
  "jule.ns.cloudflare.com.",
  "vin.ns.cloudflare.com."
```

Esto nos dan información sobre servidores web, correos y DNS, nos serviría para detectar subdominios activos y servicios expuestos, verificar si el correo está protegido, e identificar proveedores externos.

WHOIS/RDAP

```
"whois": {  
  "registrar": "Cloudflare, Inc.",  
  "creation_date": "2009-02-17 22:07:54+00:00",  
  "expiration_date": "2033-02-17 22:07:54+00:00",  
  "emails": [  
    "registrar-abuse@cloudflare.com"
```

Son los datos de registro del dominio como fechas, registrados y correos, estos nos sirven para ver la ambigüedad y expiración del dominio, identificamos los posibles correos expuestos para ingeniería social, y podemos verificar si el dominio usa privacidad de WHOIS.

SHODAN

```
"shodan": {  
  "puertos_abiertos": [  
    2096,  
    2082,  
    2083,  
    2053,  
    2086,  
    2087,  
    2095,  
    80,  
    8880,  
    8080,
```

8443,

443

"servicios": [

"CloudFlare",

"CloudFlare",

"CloudFlare",

"CloudFlare"

],

"organizacion": "Cloudflare, Inc."

Es la información pública sobre la IP del dominio (puertos, servicios, banners) nos sirve para detectar puertos expuestos innecesarios, identificar versiones vulnerables de software, evaluar si la IP pertenece a una organización conocida o a un proveedor inseguro.

Subdominios

"subdominios": [

"*.www.cloudflare.com",

"*.www.cloudflare.comwww.cloudflare.com",

"blog.api.www.cloudflare.comwww.cloudflare.com",

"catalog.www.cloudflare.com",

"de-de.www.cloudflare.com",

"el-gr.www.cloudflare.com",

"en-au.www.cloudflare.com",

"en-ca.www.cloudflare.com",

"en-gb.www.cloudflare.com",

"en-in.www.cloudflare.com",
"en-us.www.cloudflare.com",
"es-es.www.cloudflare.com",
"es-la.www.cloudflare.com",
"events.www.cloudflare.com",
"fieldmarketing.www.cloudflare.com",

Los subdominios son los que encontramos en certificados TLS públicos, nos sirve para descubrir servicios internos o secundarios, podemos detectar posibles vectores de ataque por subdominios olvidados

Tareas defensivas y uso del reporte

Reconocimientos pasivos OSINT - Identificar superficie expuesta sin interacción directa.

Auditoria de configuración - Validar prácticas seguras en DNS, TLS, WHOIS.

Análisis de configuración – Evaluar antigüedad, proveedor y exposición pública.

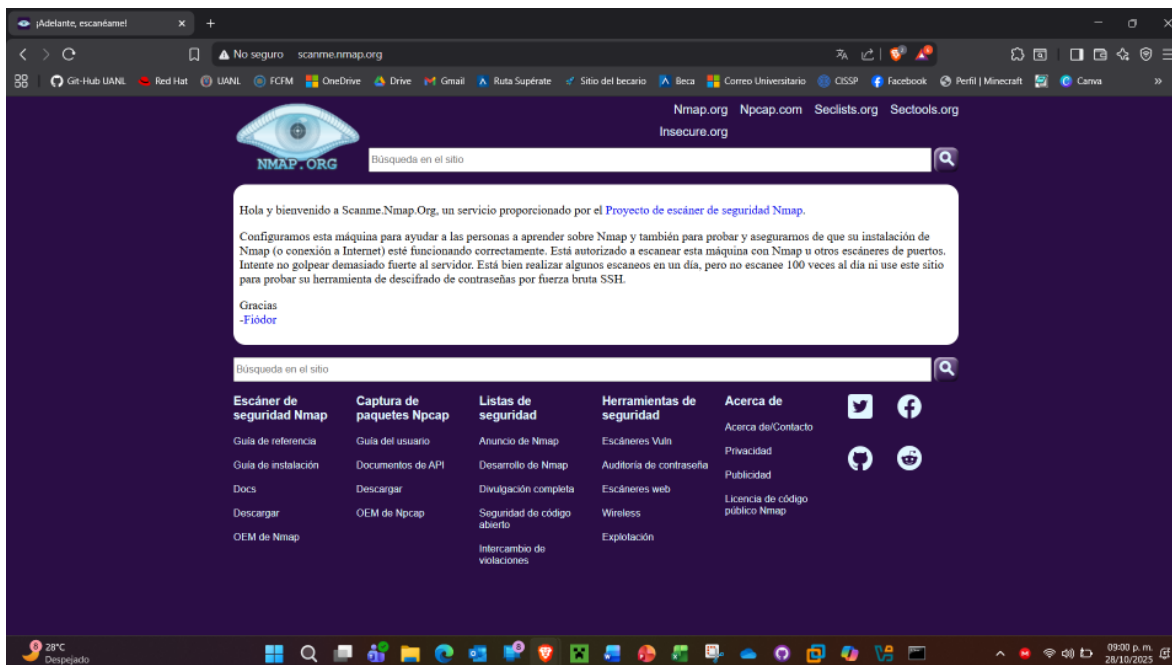
Detección de vectores ocultos – Descubrir subdominios y servicios no documentados.

Documentación ética – Generar evidencia para informes o presentaciones.

Comparación entre dominios – Benchmarking de seguridad y exposición.

Ensayo de los resultados obtenidos del escaneo activo

Autorización explícita de la página web para realizar escaneos contra ella.



Envío de un paquete para comprobar que el host esté activo.

Se envió un paquete a la página web scanme.nmap.org para comprobar que la página esté activa, pero lo que descubrimos es que nos manda este mensaje, “WARNING: MAC address to reach destination not found. Using broadcast.” e inmediatamente después nos dice que el host está inactivo.

La dirección MAC no se encontró en mi red local, pero el ping que se envió a la página web posiblemente fue recibido, pero no regresó ningún resultado por algún firewall que se tenga, dándonos un falso negativo.

```
----- Menú de la tarea activa -----
1) Verificación de que el host esté activo
2) Escaneo de puertos activos y sus respectivos servicios/versiones
3) Salir
Ingrese una opción: 1

¿Está completamente seguro de ejecutar esta tarea?
* Presione "y" si está seguro
* Presione cualquier otra tecla si no lo está

>> y
Comprobando conexión con: scanme.nmap.org

WARNING: MAC address to reach destination not found. Using broadcast.
El host scanme.nmap.org no está activo
```

Comprobación de puertos abiertos

Cuando realizamos las conexiones con socket, pudimos detectar 2 puertos abiertos, de la lista de “posibles puertos” que le dimos al script. Los cuales fueron el 22 y el 80, el 22 nos indica que tiene abierto el SSH para poder tener acceso a la Shell del servidor siempre y cuando se conozca la contraseña y el 80 siempre está activo en servidores web porque es el http, nos da un indicio de que la página no está muy segura, para ello debería de tener abierto el puerto 443, que en este caso está cerrado.

```
El puerto: 21 (FTP) está CERRADO
El puerto: 22 (SSH) está ABIERTO
El puerto: 25 (SMTP) está CERRADO
El puerto: 80 (HTTP) está ABIERTO
El puerto: 110 (POP3) está CERRADO
El puerto: 143 (IMAP) está CERRADO
El puerto: 443 (HTTPS) está CERRADO
El puerto: 3389 (RDP) está CERRADO
```

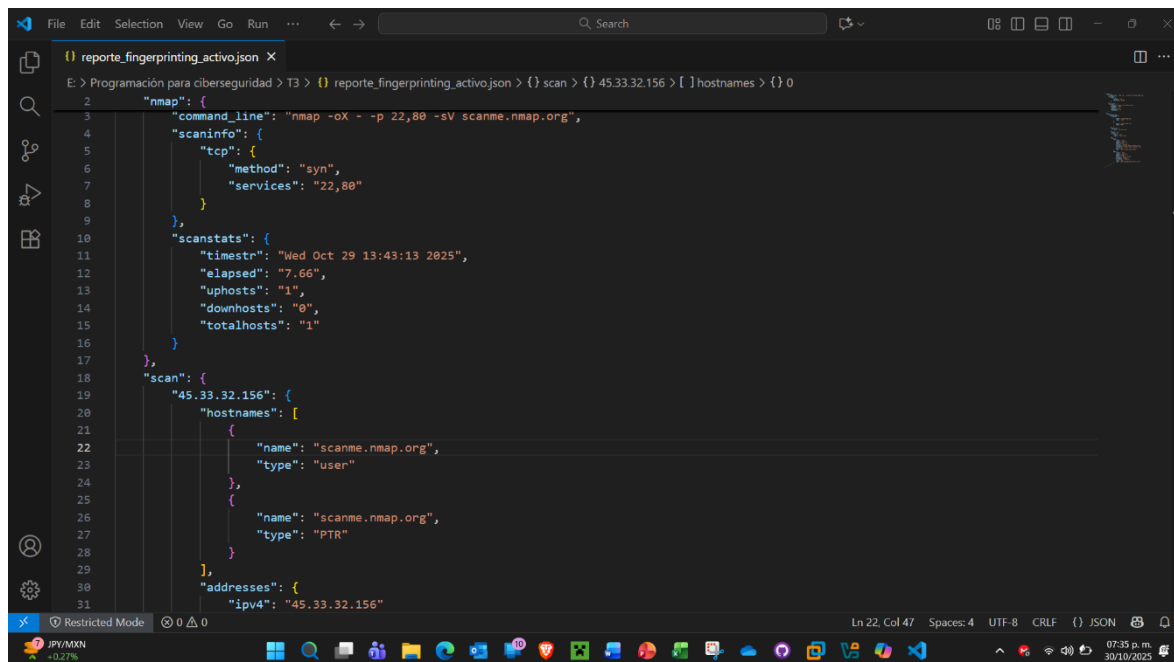
Descubrimiento de servicios y versiones de cada puerto abierto

Realizamos un escaneo con nmap, usando tcp hacia los puertos 22 y 80.

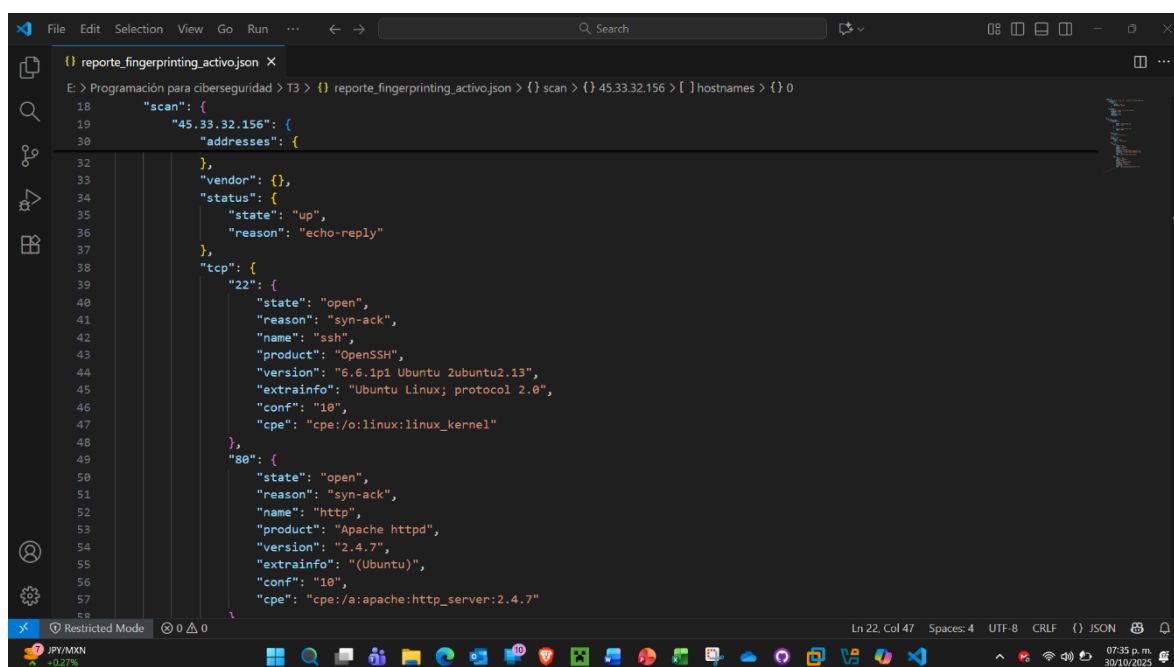
Antes de mostrar los hallazgos de los servicios/versiones de los puertos, encontramos información, como la dirección ip, que es "45.33.32.156", el nombre del host, que es "scanme.nmap.org", el tiempo que se tardó en hacer el escaneo, que fue 7.66 segundos, así como el comando basado en nmap que se ejecutó "nmap -oX - -p 22,80 -sV scanme.nmap.org".

Del puerto 22 encontramos que su estado es “abierto” por qué se recibió una respuesta, el servicio es OpenSSH y la versión usada es "6.6.1p1 Ubuntu 2ubuntu2.13".

En el caso del puerto 80, igualmente se le encontró “abierto” porque se recibió una respuesta, el servicio es “Apache httpd” y la versión es "2.4.7 Ubuntu".



```
1  "nmap": {
2    "command_line": "nmap -oX - -p 22,80 -sV scanme.nmap.org",
3    "scaninfo": {
4      "tcp": {
5        "method": "syn",
6        "services": "22,80"
7      }
8    },
9    "scanstats": {
10     "timetr": "Wed Oct 29 13:43:13 2025",
11     "elapsed": "7.66",
12     "uphosts": "1",
13     "downhosts": "0",
14     "totalhosts": "1"
15   },
16   "scan": {
17     "45.33.32.156": {
18       "hostnames": [
19         {
20           "name": "scanme.nmap.org",
21           "type": "user"
22         },
23         {
24           "name": "scanme.nmap.org",
25           "type": "PTR"
26         }
27       ],
28       "addresses": {
29         "ipv4": "45.33.32.156"
30       }
31     }
32   }
33 }
```



```
18  "scan": {
19    "45.33.32.156": {
20      "addresses": {
21        "ipv4": "45.33.32.156"
22      },
23      "vendor": {},
24      "status": {
25        "state": "up",
26        "reason": "echo-reply"
27      },
28      "tcp": {
29        "22": {
30          "state": "open",
31          "reason": "syn-ack",
32          "name": "ssh",
33          "product": "OpenSSH",
34          "version": "6.6.1p1 Ubuntu 2ubuntu2.13",
35          "extrainfo": "Ubuntu Linux; protocol 2.0",
36          "conf": "10",
37          "cpe": "cpe:/o:linux:linux_kernel"
38        },
39        "80": {
40          "state": "open",
41          "reason": "syn-ack",
42          "name": "http",
43          "product": "Apache httpd",
44          "version": "2.4.7",
45          "extrainfo": "(Ubuntu)",
46          "conf": "10",
47          "cpe": "cpe:/a:apache:http_server:2.4.7"
48        }
49      }
50    }
51  }
52 }
```