Ensayo de los resultados obtenidos

Del escaneo pasivo

Funcionalidad del script:

Ejecutando

python scanpassive.py https://www.cloudflare.com

-Extraemos el dominio limpio

-Consulta registros DNS publicos

-Obtiene informacion WHOIS/RDAP

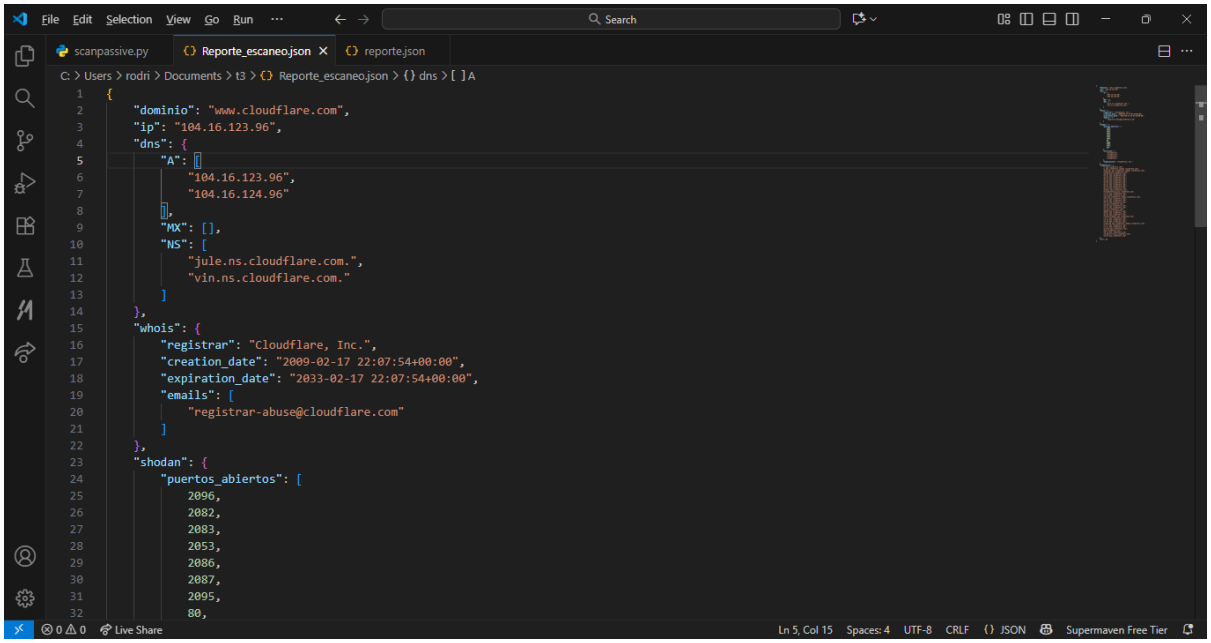
-Resuelve la IP y consulta Shodan

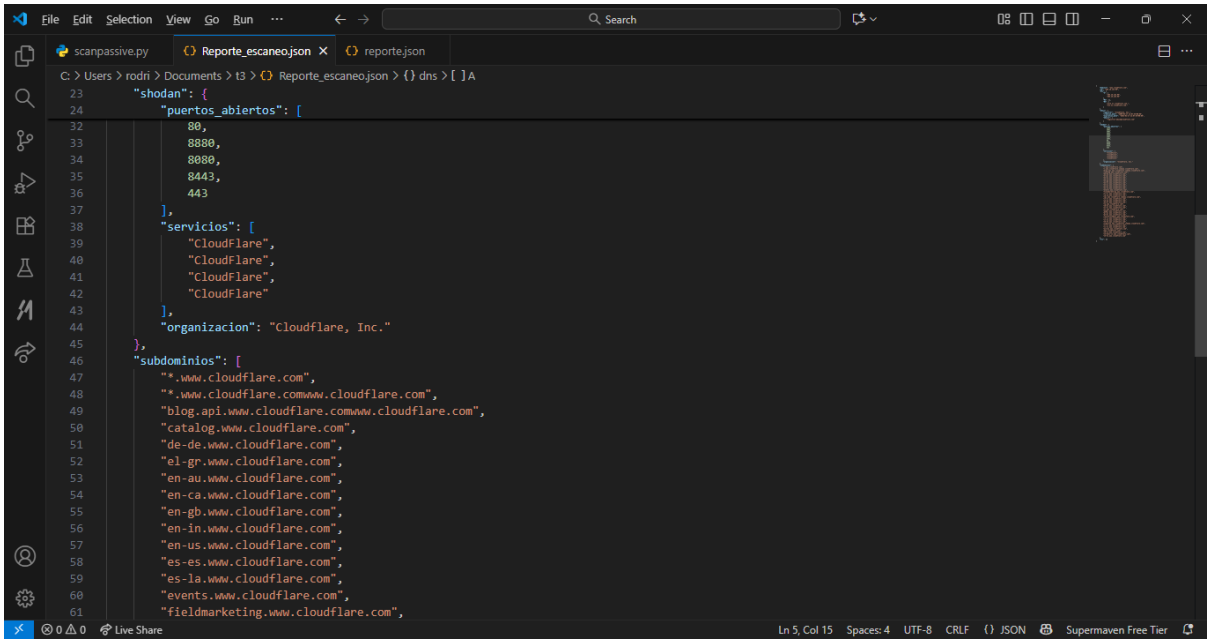
-Busca subdominios en certificados publicos

-Guarda todo en un archivo JSON

Datos obtenidos y sus usos en Ciberseguridad

Los resultados obtenidos nos lo dan en un archivo JSON





Dominio e IP

Conseguimos la IP del dominio que es "104.16.123.96" esto nos pueden servir para identificar la infraestructura detras del dominio, verificar si nos exponen o no su IP directa, y correlacionarlas con otras IPs p 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 informacion sobre servidores web, correos y dns, nos serviria para detectar subdominios activos y servicios expuestos, verificar si el correo esta 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, estoy nos sirven para ver la ambiguedad y expiracion del dominio, identificamos los posibles correos expuestos para ingeneria 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 informacion publica 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 organizacion conocida o a un proovedor 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 publicos, nos sirve para descubrir servicios internos o secundarios, podemos detectar posibles vectores de ataque por subdominios olvidados

Tareas defensivas y uso del reporte

Reconocimientos pasivo OSINT - Identificar superficie expuesta sin interaccion directa

Auditoria de configuracion - Validar practicas seguras en DNS, TLS, WHOIS

Analisis de configuracion – Evaluar antiguedad, proveedor y exposicion publica

Deteccion de vectores ocultos – Descubrir subdominios y servicios no documentados

Documentacion etica – Generar evidencia para informes o presentaciones

Comparacion entre dominios – Benchmarking se seguridad y exposicion