EXPLORACIÓN DE HERRAMIENTAS OSINT PARA LA RECOLECCIÓN DE INFORMACIÓN PÚBLICA

¿QUE ES OSINT?

Que es osint español se traduce como Inteligencia de Fuentes Abiertas. Se refiere al proceso de recopilar, analizar y usar información que está disponible públicamente para obtener conocimiento útil

¿PARA QUE SE USA OSINT?

- **Seguridad y defensa: para anticipar amenazas, monitorizar movimientos de grupos terroristas o criminales, y prevenir delitos mediante el análisis de información pública como noticias, redes sociales y documentos oficiale**

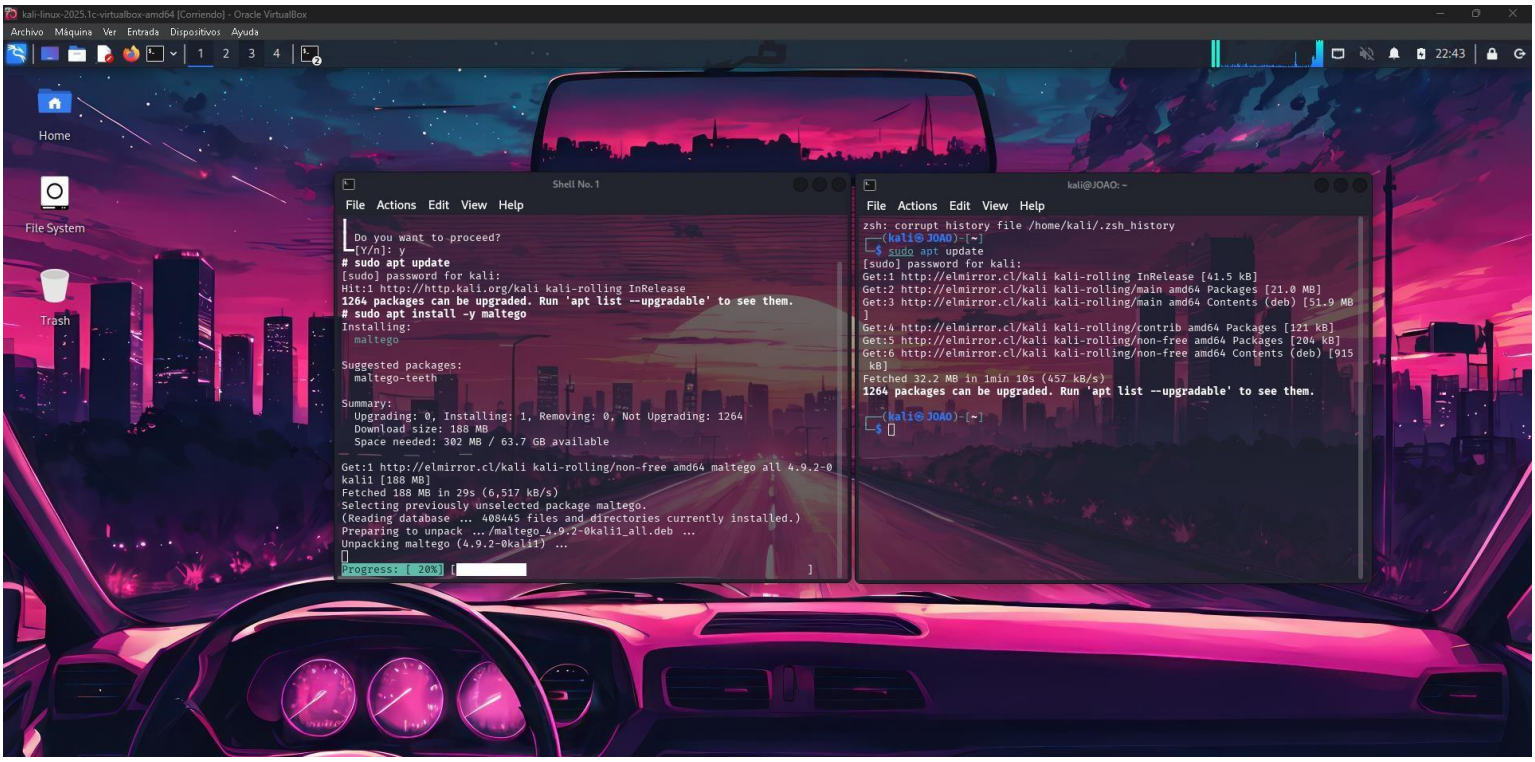
- **Empresas: para analizar la competencia, estudiar tendencias del mercado, evaluar reputación online y realizar auditorías internas, utilizando bases de datos públicas, informes financieros y redes sociales**

- **Ciberseguridad: para identificar vulnerabilidades, detectar amenazas, proteger datos sensibles y realizar pruebas de penetración (pentesting). OSINT ayuda a descubrir credenciales filtradas, configuraciones expuestas y posibles vectores de ataque antes que los ciberdelincuentes**

ALGUNAS HERRAMIENTAS SE USA PARA OSINT:

1. MALTEGO (KALI LINUX):

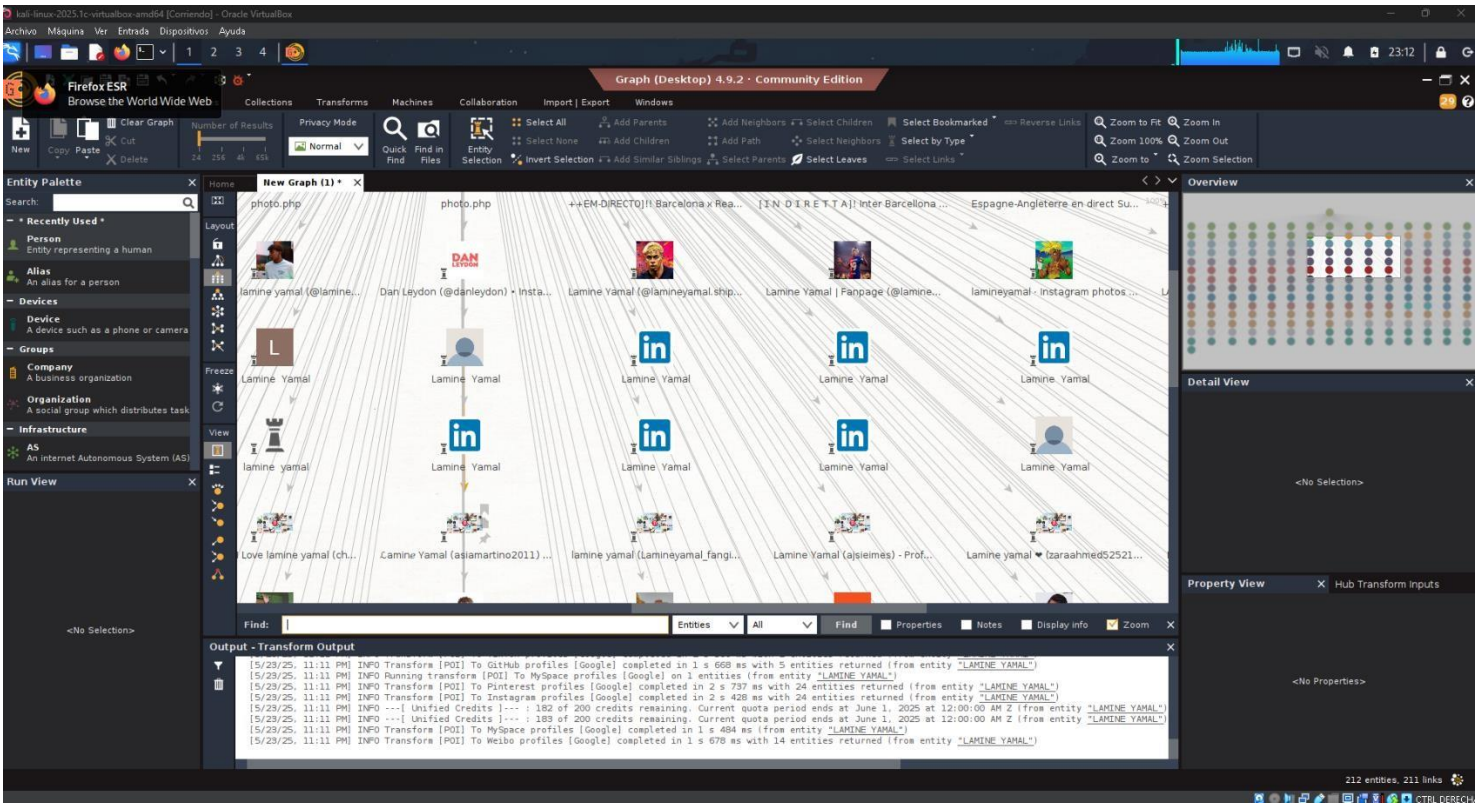
Maltego es una herramienta de inteligencia de fuentes abiertas (OSINT) que permite recopilar, analizar y visualizar información de diversas fuentes públicas para identificar relaciones y patrones entre personas, empresas, dominios, direcciones IP, correos electrónicos y otros datos relevantes



Una vez instalado maltego tenemos que registrarnos con un correo y una contraseña para que el mismo programa nos permita usar los trasformadores que nos ayudaran hacer una búsqueda.

En este caso usaremos el personaje LAMINE YAMAL donde podemos ver que no sale redes sociales, imágenes todo relacionado con las personas que estamos buscando

Es importante dar más información a maltego mientras más se haga relación con esa persona el resultado será mas efectivo ya que los trasformadores darán un resultado mas efectivo



Gracias a maltego podemos tener una información más precisa de una persona como una empresa ya nos permite hacer una búsqueda profunda es una herramienta muy poderosa

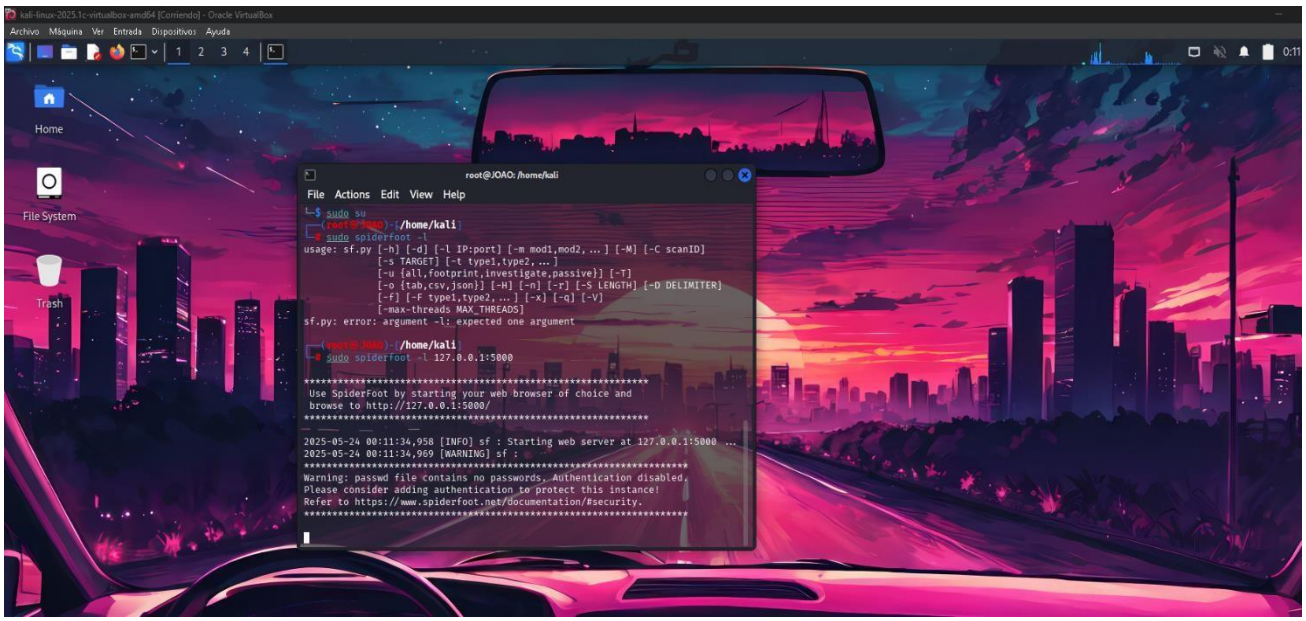
2. SPIDERFOOT (KALI LINUX):

SpiderFoot es una herramienta automatizada de OSINT (inteligencia de fuentes abiertas) diseñada para recopilar información pública sobre un objetivo específico, como una dirección IP, dominio, correo electrónico, nombre de usuario o persona, consultando más de 100 fuentes de datos abiertas Tenemos que instalarlo en Kali Linux para poder hacer los escaneos Pero en algunos Kali ya vine por defecto instalado solo sería cuestión de actualizarlo

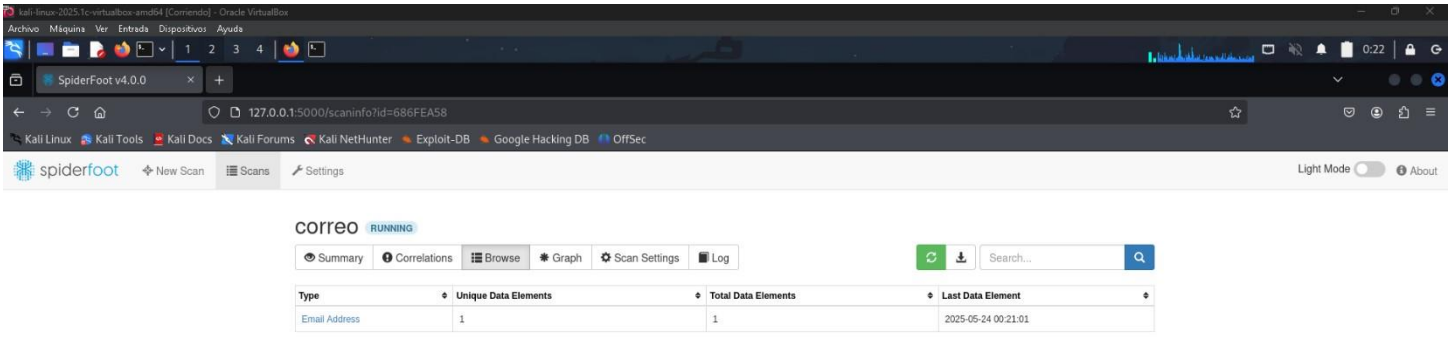
Una vez que tenemos el programa iremos a correrlo con el siguiente comando

Sudo spiderfoot -l la ip 127.0.0.1 La dirección IP 127.0.0.1 es una dirección especial llamada loopback luego el puerto 5000 se utiliza para que la aplicación web escuche y acepte conexiones entrantes desde el navegador

Una ves que ponemos eso el mismo programa nos dará una url donde podremos ingresar desde el navegador para poder hacer las pruebas de escaneo

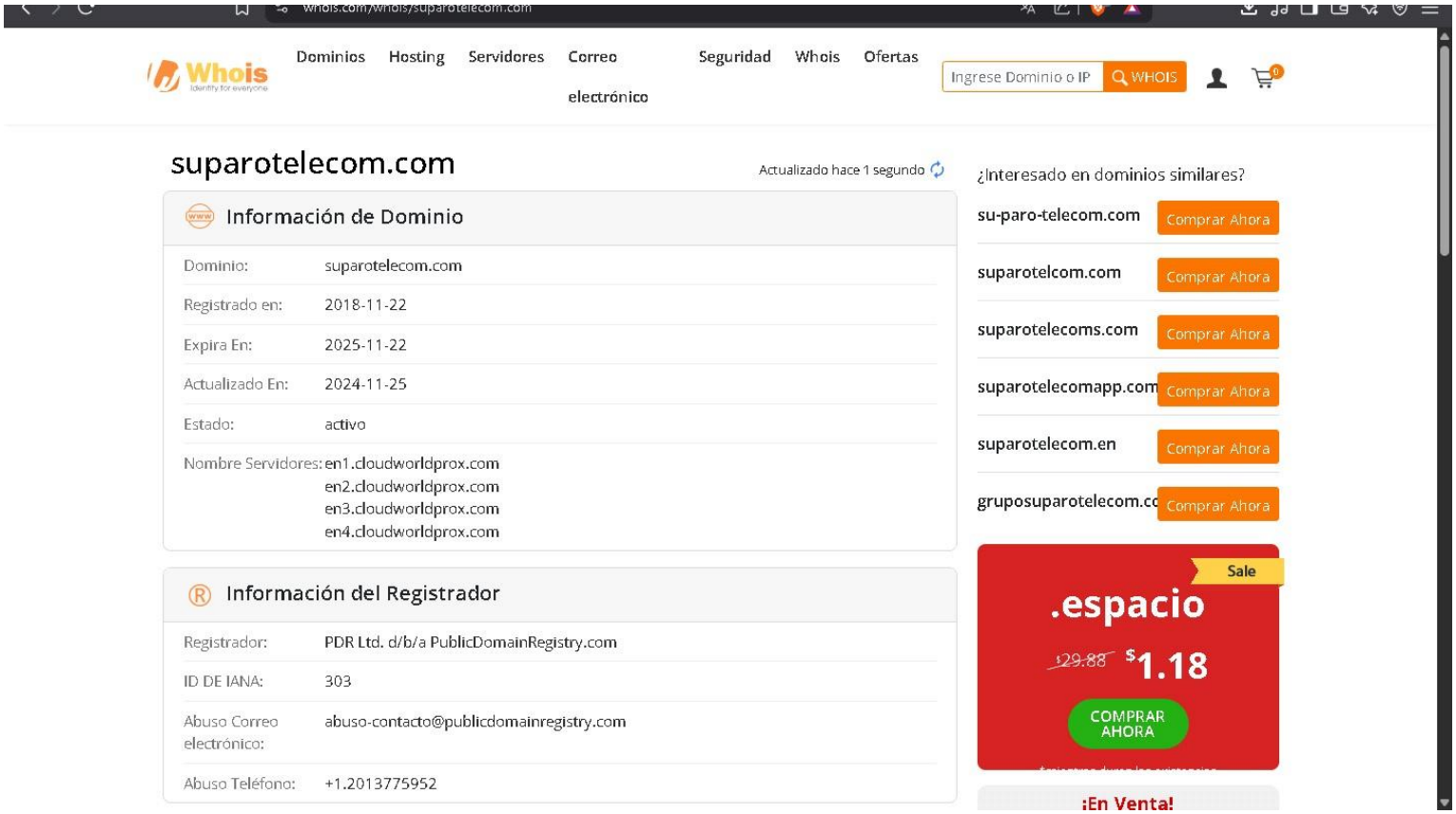


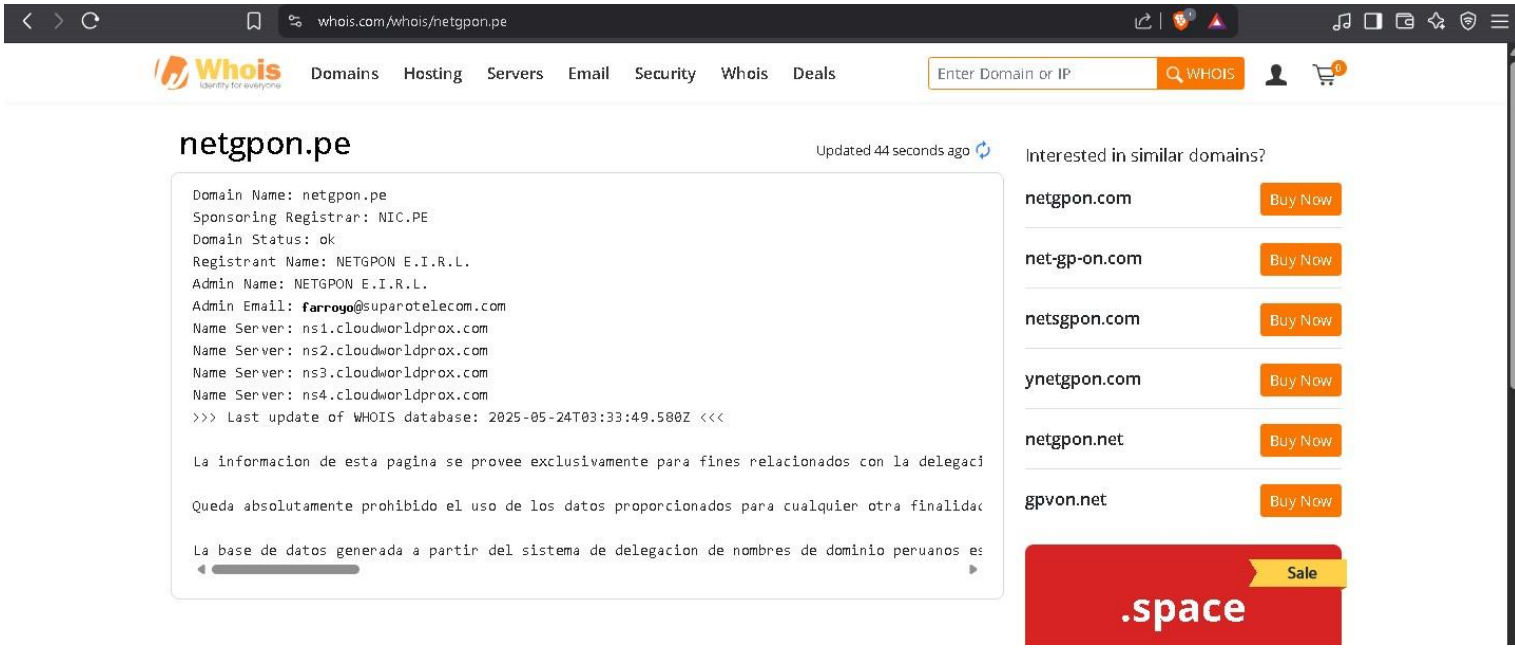
Una vez que entramos a navegador podemos escanear una ip, un numero de celular o un dominio y un correo en este ejerció yo lo hice con mi correo

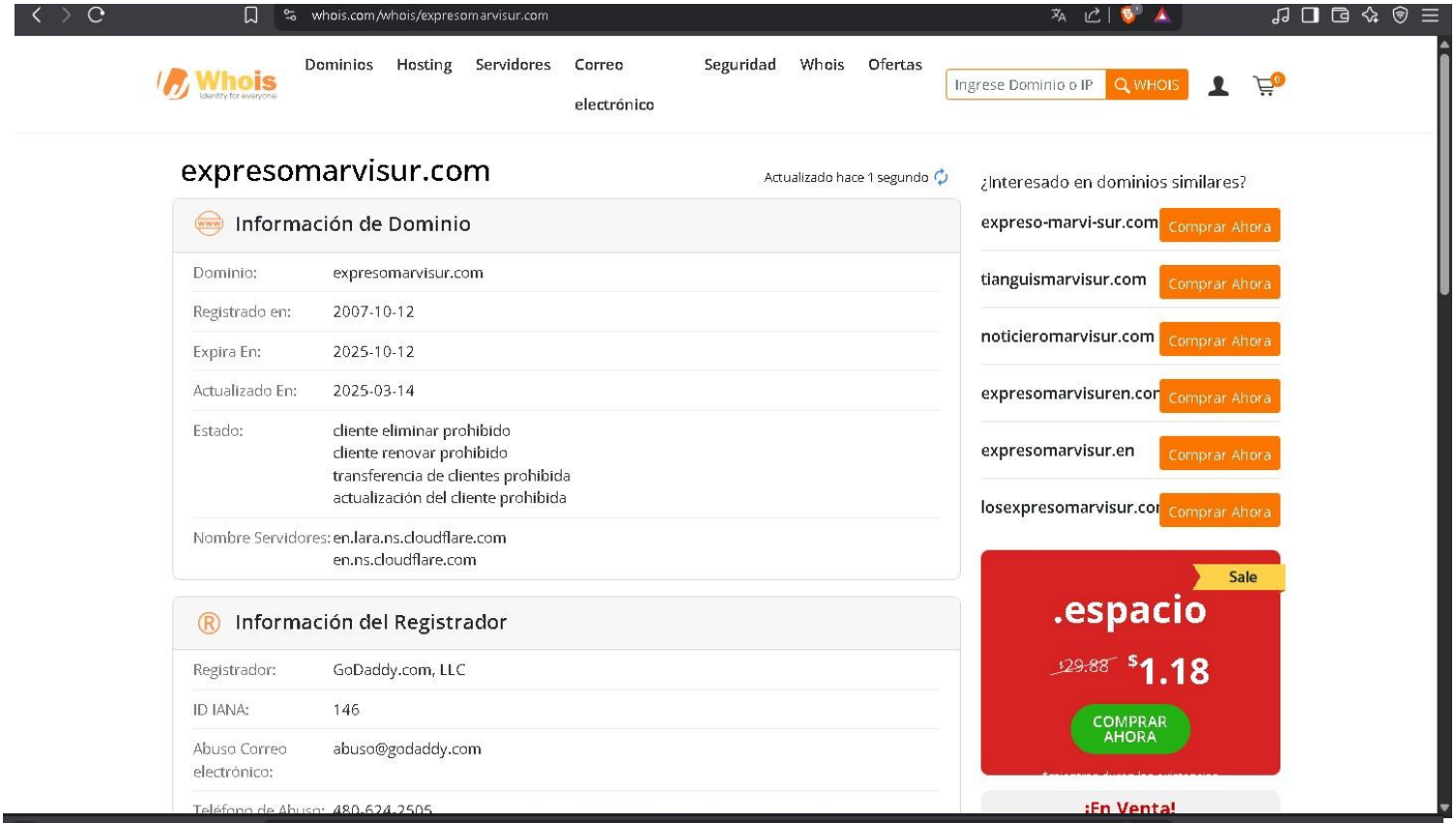


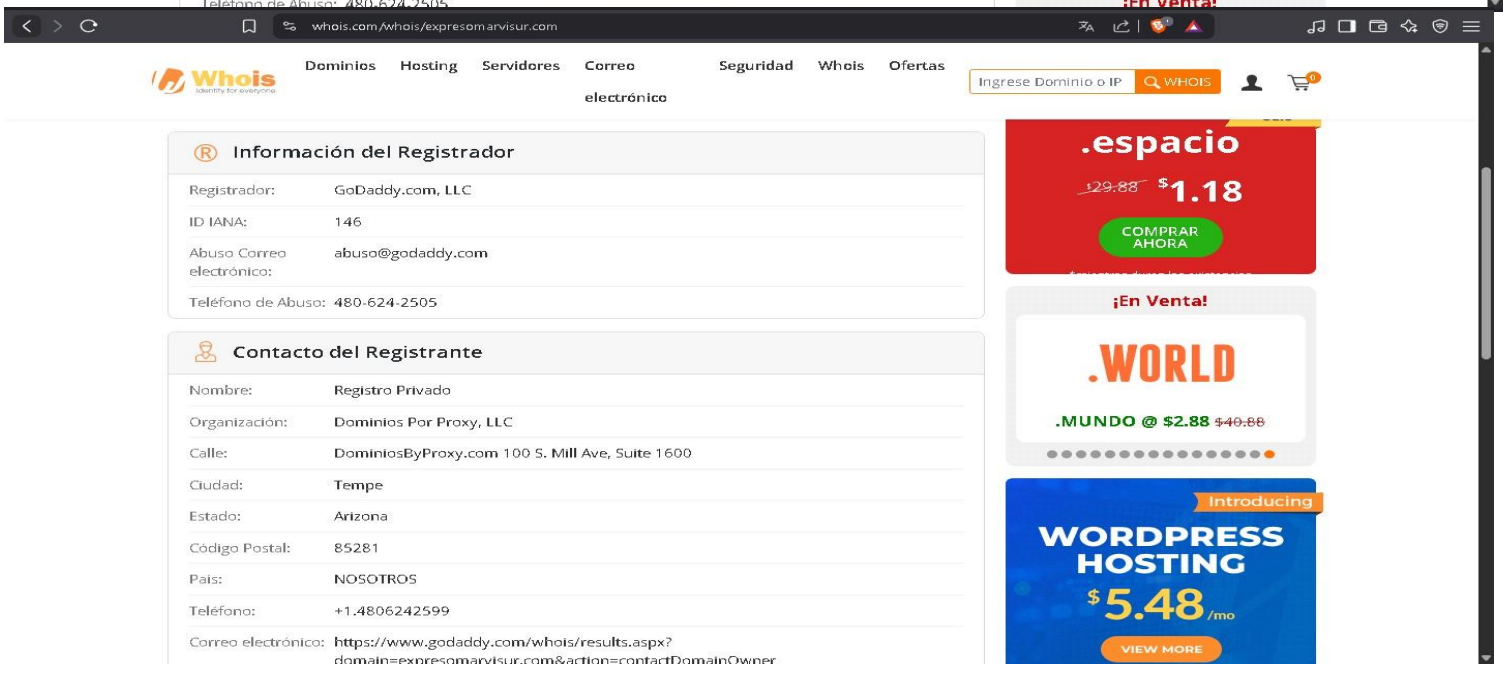
3. ¿Qué es WHOIS?

Es una aplicación en línea que nos permite hacer un escaneo a un dominio, ip los resultados son los siguientes



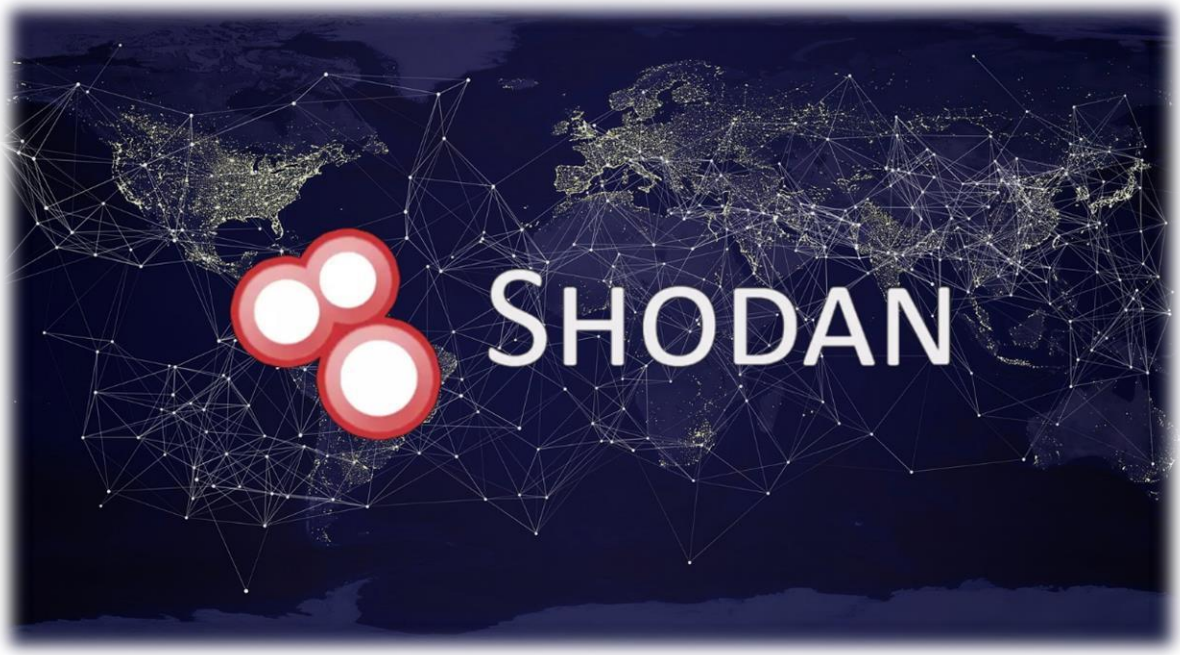

whois.com/whois/netgpon.pe
Whois
Domains Hosting Servers Email Security Whois Deals
Enter Domain or IP
WHOIS
netgpon.pe
Updated 44 seconds ago
Domain Name: netgpon.pe
Sponsoring Registrar: NIC.PE
Domain Status: ok
Registrant Name: NETGPON E.I.R.L.
Admin Name: NETGPON E.I.R.L.
Admin Email: farroyo@suparotelecom.com
Name Server: ns1.cloudworldprox.com
Name Server: ns2.cloudworldprox.com
Name Server: ns3.cloudworldprox.com
Name Server: ns4.cloudworldprox.com
>>> Last update of WHOIS database: 2025-05-24T03:33:49.580Z <<<
La informacion de esta pagina se provee exclusivamente para fines relacionados con la delegaci
Queda absolutamente prohibido el uso de los datos proporcionados para cualquier otra finalidac
La base de datos generada a partir del sistema de delegacion de nombres de dominio peruanos es
Interested in similar domains?
netgpon.com Buy Now
net-gp-on.com Buy Now
netsgpon.com Buy Now
ynetgpon.com Buy Now
netgpon.net Buy Now
gpvon.net Buy Now
Sale
.space


whois.com/whois/expresomarvisur.com
Whois
Dominios Hosting Servidores Correo electrónico Seguridad Whois Ofertas
Ingrese Dominio o IP
WHOIS
expresomarvisur.com
Actualizado hace 1 segundo
Información de Dominio
Dominio: expresomarvisur.com
Registrado en: 2007-10-12
Expira En: 2025-10-12
Actualizado En: 2025-03-14
Estado: cliente eliminar prohibido
cliente renovar prohibido
transferencia de clientes prohibida
actualización del cliente prohibida
Nombre Servidores: en.lara.ns.cloudflare.com
en.ns.cloudflare.com
Información del Registrador
Registrador: GoDaddy.com, LLC
ID IANA: 146
Abuso Correo electrónico: abuso@godaddy.com
Teléfono de Abuso: 480-624-2505
¿Interesado en dominios similares?
expreso-marvi-sur.com Comprar Ahora
tianguismarvisur.com Comprar Ahora
noticieromarvisur.com Comprar Ahora
expresomarvisuren.cor Comprar Ahora
expresomarvisur.en Comprar Ahora
losexpresomarvisur.cor Comprar Ahora
Sale
.espacio
$29.88 $1.18
COMPRAR AHORA

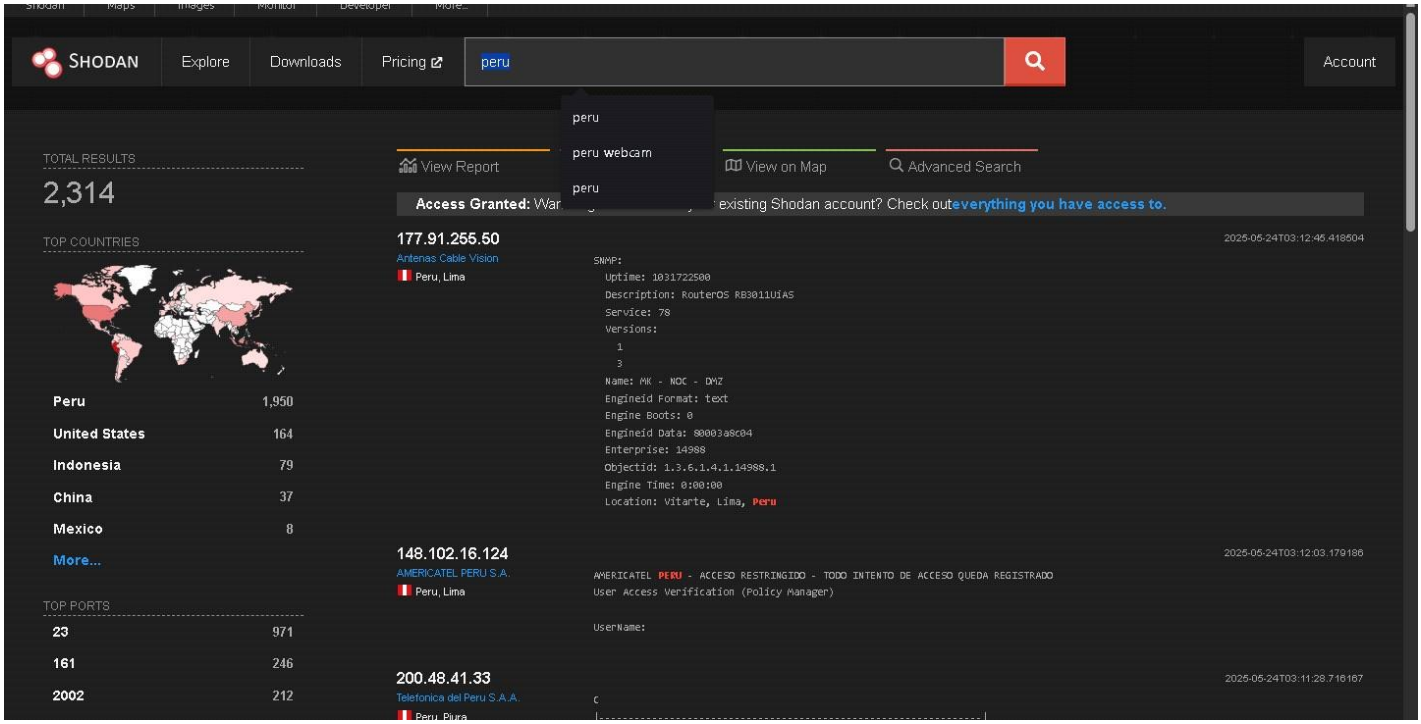

whois.com/whois/expresomarvisur.com
Whois
Dominios Hosting Servidores Correo electrónico Seguridad Whois Ofertas
Ingrese Dominio o IP
WHOIS
Información del Registrador
Registrador: GoDaddy.com, LLC
ID IANA: 146
Abuso Correo electrónico: abuso@godaddy.com
Teléfono de Abuso: 480-624-2505
Contacto del Registrante
Nombre: Registro Privado
Organización: Dominios Por Proxy, LLC
Calle: DominiosByProxy.com 100 S. Mill Ave, Suite 1600
Ciudad: Tempe
Estado: Arizona
Código Postal: 85281
País: NOSOTROS
Teléfono: +1.4806242599
Correo electrónico: https://www.godaddy.com/whois/results.aspx?domain=expresomarvisur.com&action=contactDomainOwner
.espacio
$29.88 $1.18
COMPRAR AHORA
¡En Venta!
.WORLD
.MUNDO @ $2.88 $40.88
Introducing
WORDPRESS HOSTING
$5.48 /mo
VIEW MORE

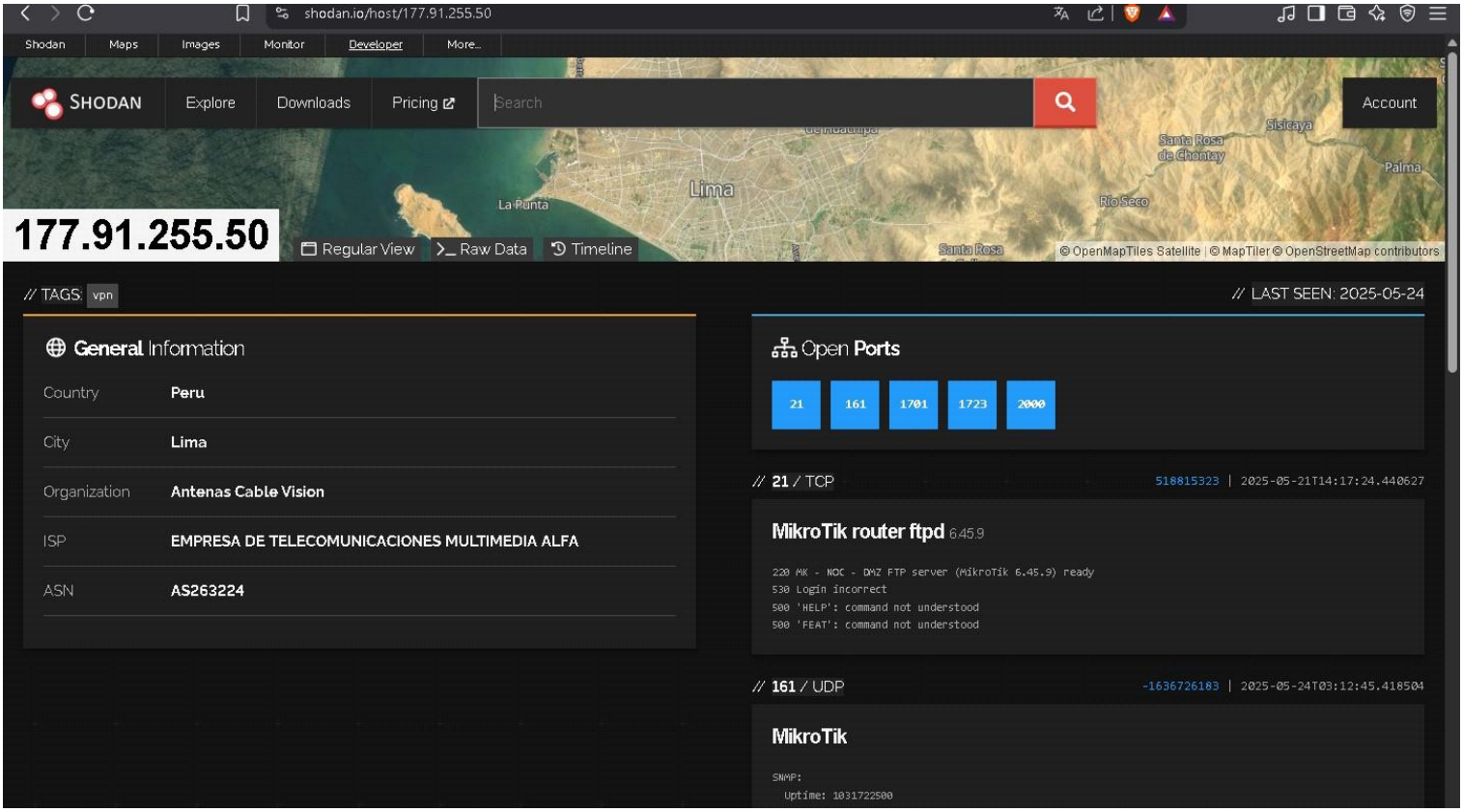
4. QUES ES SHODAN

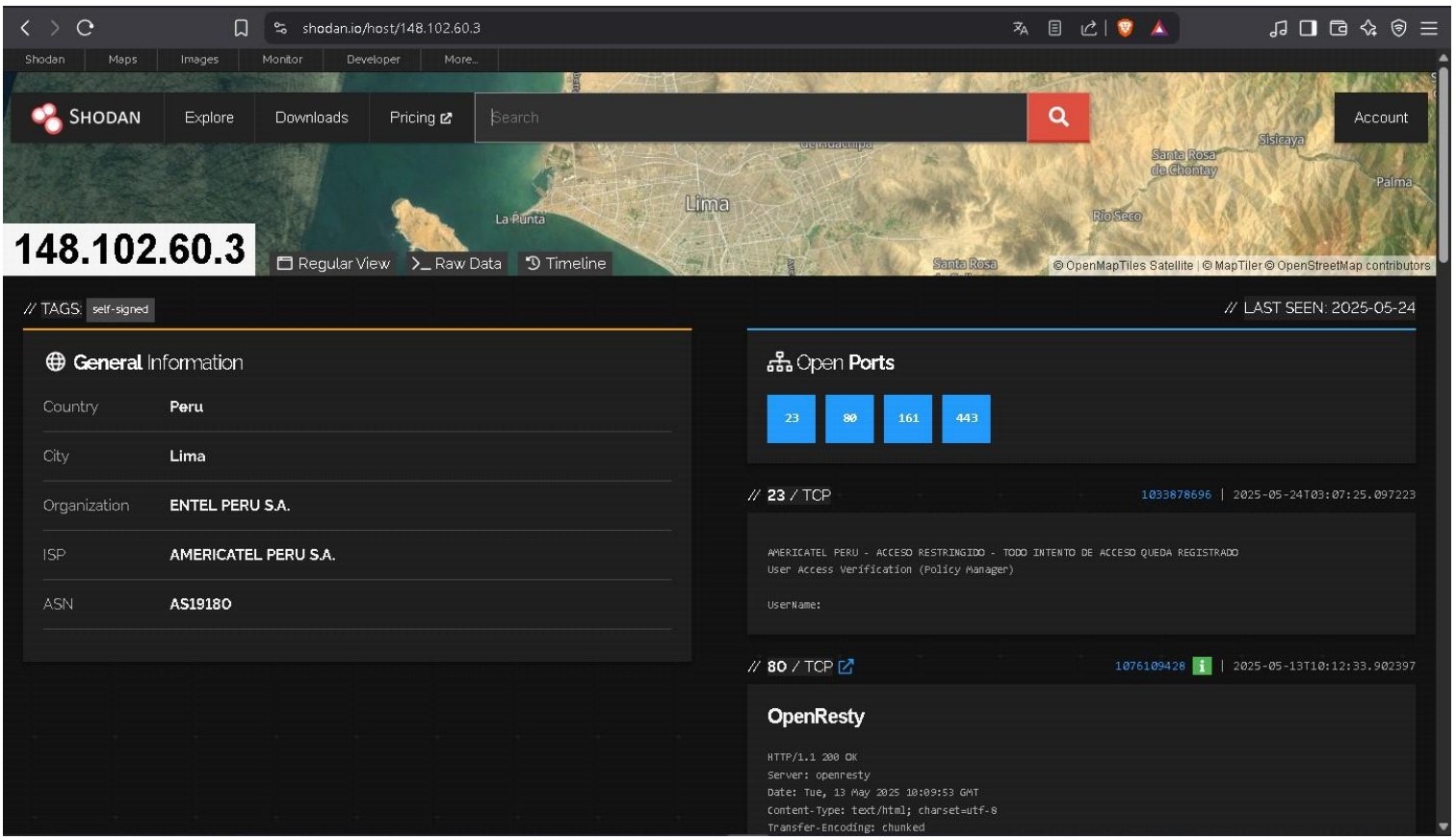
Shodan es un motor de búsqueda especializado que, a diferencia de Google u otros buscadores tradicionales que indexan páginas web, se dedica a **buscar y recopilar información sobre dispositivos conectados a Internet** como servidores, cámaras IP, routers, impresoras, sistemas industriales y otros dispositivos IoT

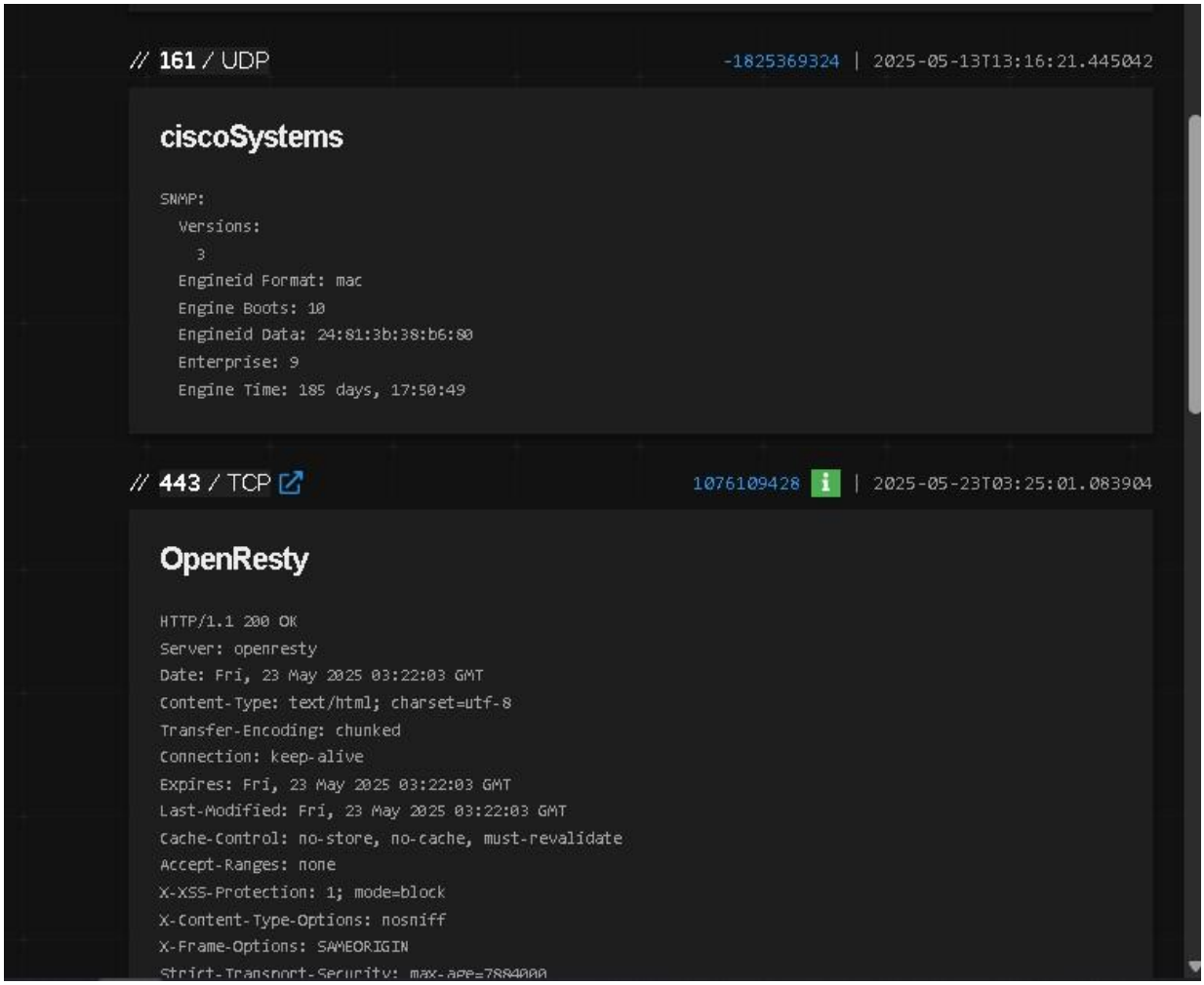


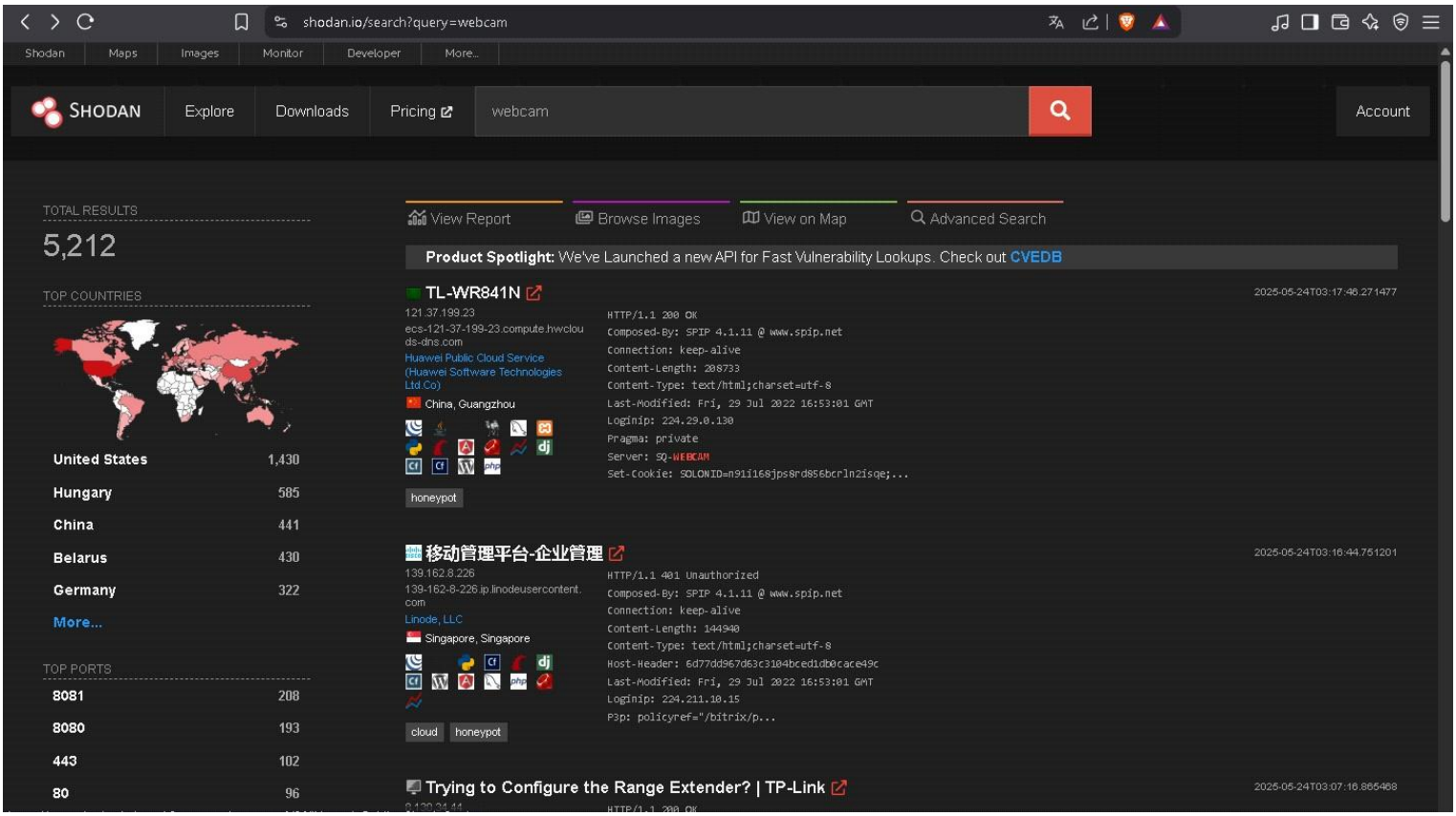
Puedes encontrar muchos servicios vulnerables puertos abiertos como servidores o servicios de empresas que no tienen seguridad o como cámaras web que no están bien configuradas o como routers




shodan.io/host/177.91.255.50
Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Downloads
Pricing
Search
Account
177.91.255.50
Regular View
Raw Data
Timeline
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors
// TAGS: vpn
// LAST SEEN: 2025-05-24
General Information
Country Peru
City Lima
Organization Antenas Cable Vision
ISP EMPRESA DE TELECOMUNICACIONES MULTIMEDIA ALFA
ASN AS263224
Open Ports
21
161
1701
1723
2000
// 21 / TCP
518815323 | 2025-05-21T14:17:24.440627
MikroTik router ftpd 6.45.9
220 MK - NOC - DMZ FTP server (MikroTik 6.45.9) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
// 161 / UDP
-1636726183 | 2025-05-24T03:12:45.418504
MikroTik
SNMP:
Uptime: 1031722500

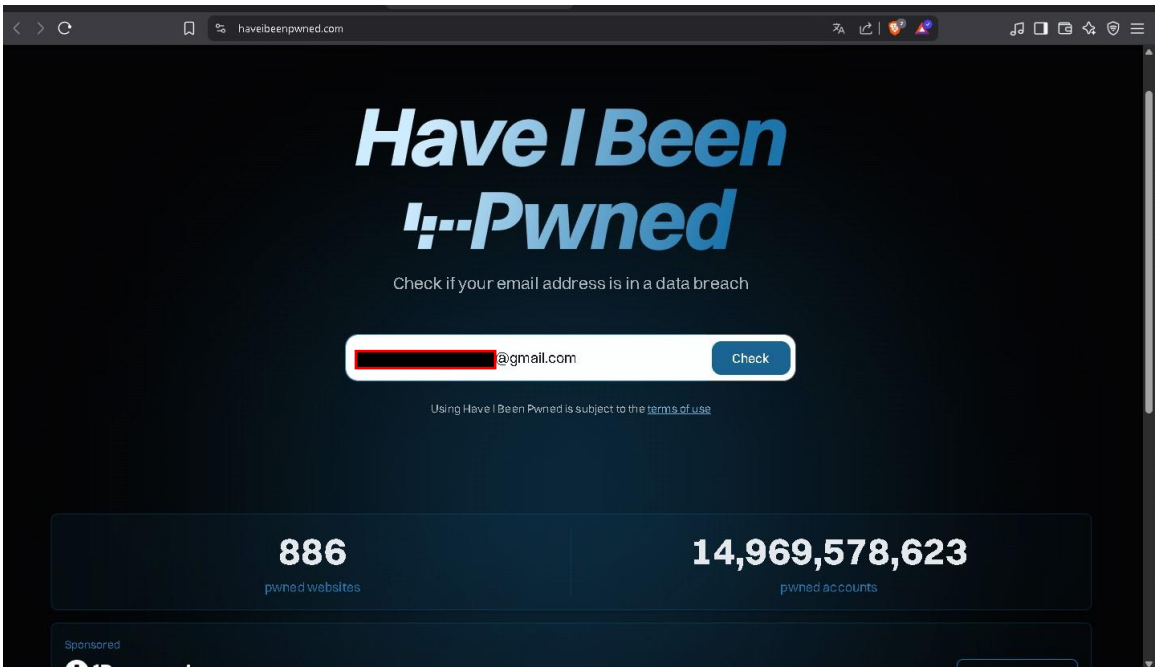

shodan.io/host/148.102.60.3
Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Downloads
Pricing
Search
Account
148.102.60.3
Regular View
Raw Data
Timeline
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors
// TAGS: self-signed
// LAST SEEN: 2025-05-24
General Information
Country Peru
City Lima
Organization ENTEL PERU S.A.
ISP AMERICATEL PERU S.A.
ASN AS19180
Open Ports
23
80
161
443
// 23 / TCP
1033878696 | 2025-05-24T03:07:25.097223
AMERICATEL PERU - ACCESO RESTRINGIDO - TODO INTENTO DE ACCESO QUEDA REGISTRADO
User Access Verification (Policy Manager)
UserName:
// 80 / TCP
1076109428 | 2025-05-13T10:12:33.902397
OpenResty
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 13 May 2025 10:09:53 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked





5. HAVE I BEEN:

es un servicio web que permite a los usuarios verificar si su dirección de correo electrónico o datos personales han sido comprometidos en alguna filtración de seguridad o brecha de datos.

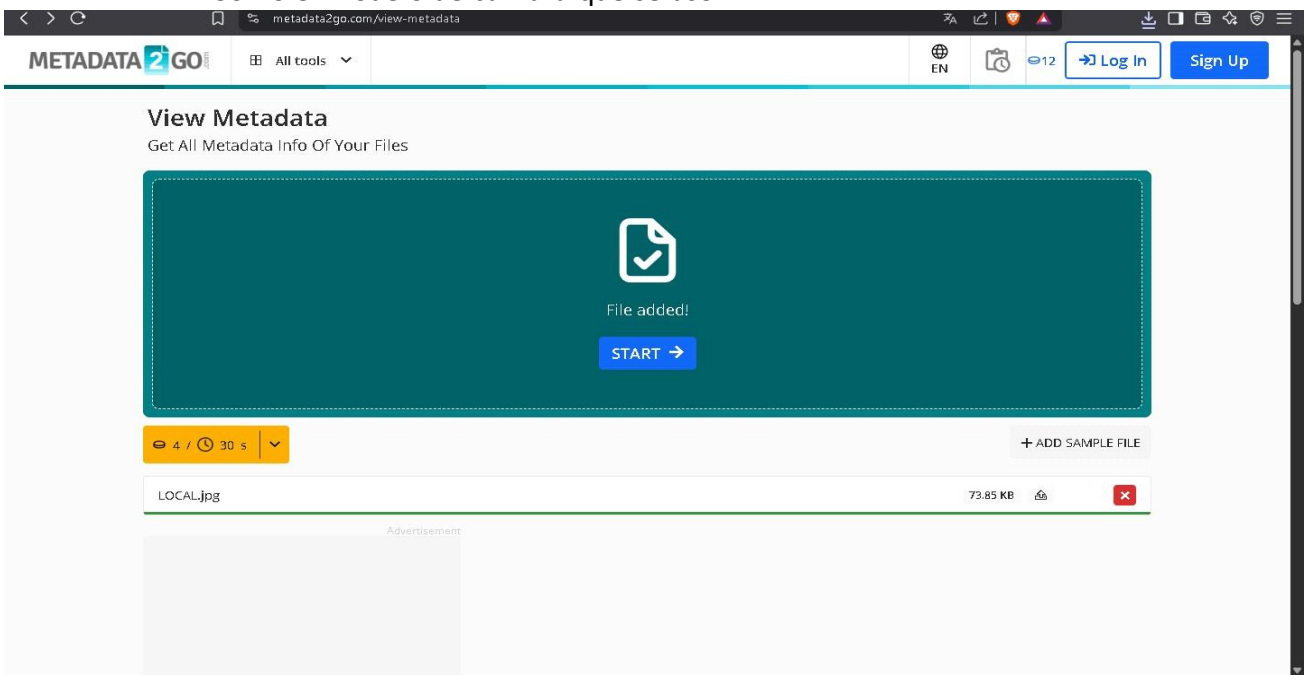


Como podemos ver nos sale que nuestro correo ha sido filtrado algunos datos nos da la información cuando fue que pagina fue la que hiso la filtración de esos datos.

Hice la prueba de un segundo correo donde tuve resultado que tuve dos ataques de intento de fishing

¿Qué son los metadatos de fotos?

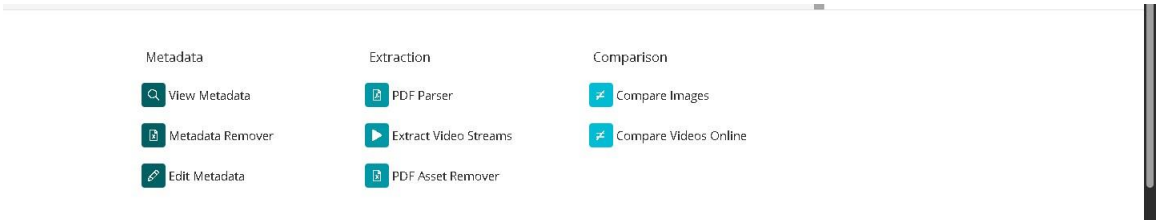
- Son datos **sobre la propia imagen**, como la fecha y hora en que se tomó la foto, el modelo y marca de la cámara o smartphone, los ajustes usados (ISO, apertura, velocidad de obturación), la resolución, el tamaño y el formato del archivo
- Donde en algunas ocasiones podemos obtener la geolocalización de donde fue la foto
- Como el modelo de cámara que se uso



Esta herramienta nos ayudara hacer un diagnóstico breve sobre una imagen como el tamaño que tipo de archivo es datos que son de la imagen.

checksum	6f669ba1fb59c44c2a38a699c1e456a4
file_name	LOCAL.jpg
file_size	76 kB
file_type	JPEG
file_type_extension	jpg
mime_type	image/jpeg
jfif_version	1.01
resolution_unit	None
x_resolution	1
y_resolution	1
image_width	960

OJO: es importante remover los metadatos de nuestras fotos porque esa información que brinda las imágenes en manos equivocas es un arma muy poderosa ya que en internet sabrán mucha información nuestra como en redes sociales o alguna página web.

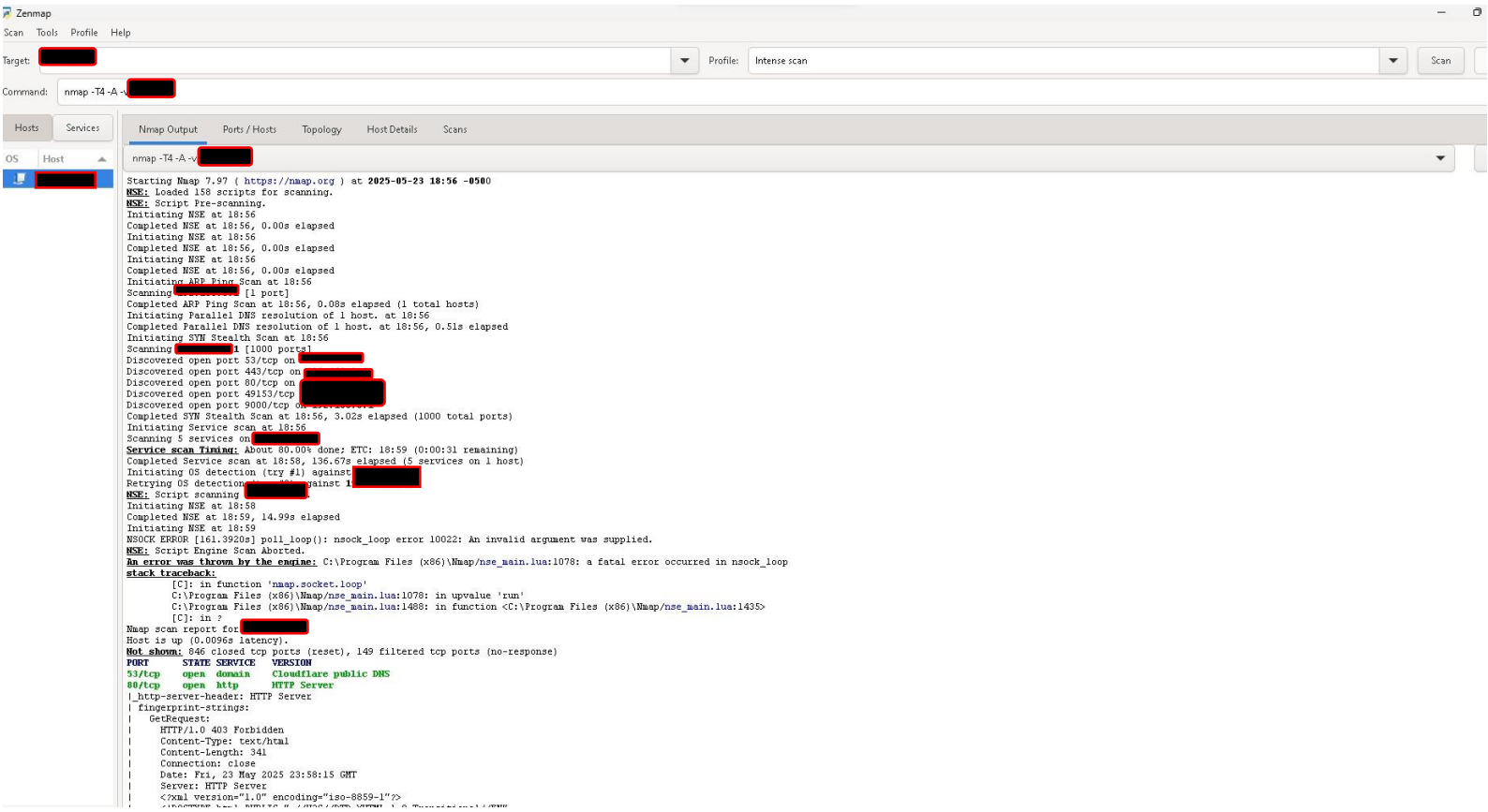


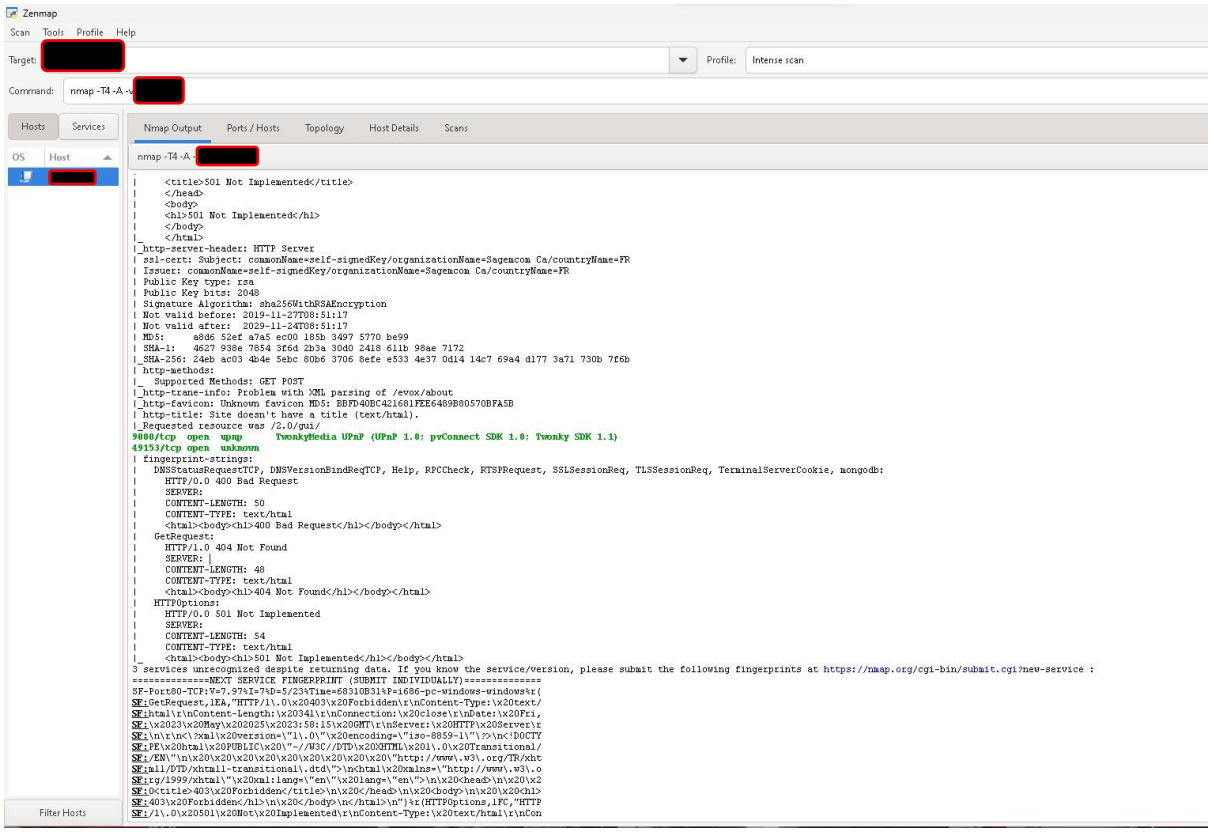
ACONTINUACION UN PEQUEÑO EJERCIO:

UN USUARIO ESTA PRESENTADO LENTITUD EN SERVICIO DE INTERNET QUIERE SABER SI ES SU PROVEDOR, PERO EL TIENE UNA CONTRASEÑA SEGURA A PESAR DE ESO EL USUARIO QUIERE SABER EL MOTIVO DE QUE SU RED TIENE ALGUNOS PROBLEMAS PUEDE SER LA LATENCIA O MUCHOS DISPOSITIVOS CONECTADOS IREMOS DESAROLLANDO ESTE CASO.

Usaremos el zenmap

Es una herramienta de escaneo de redes Nmap es una potente utilidad de línea de comandos para descubrir dispositivos, puertos abiertos, servicios y vulnerabilidades en una red, Zenmap facilita su uso al ofrecer una interfaz visual intuitiva que permite ejecutar escaneos sin necesidad de manejar comandos complejos.





En este escaneo pudimos detectar que los certificados HTTP 443 estaban caducados de igual manera podemos detectar una vulnerabilidad que seria

```
|_Requested resource was /2.0/gui/
9000/tcp  open  upnp       TwonkyMedia UPnP (UPnP 1.0; pvConnect SDK 1.0; Twonky SDK 1.1)
49153/tcp open  unknown
| fingerprint-strings:
```

Es importante estar contrastantemente monitoreando nuestras redes para saber que todo tenga actualizado y en orden para mejor seguridad ya que hoy en día todo es vulnerable y existen muchos ataques

PODEMOS REVISAR NUESTRA RED DESDE NUESTRO DISPOSITIVO MOVIL:

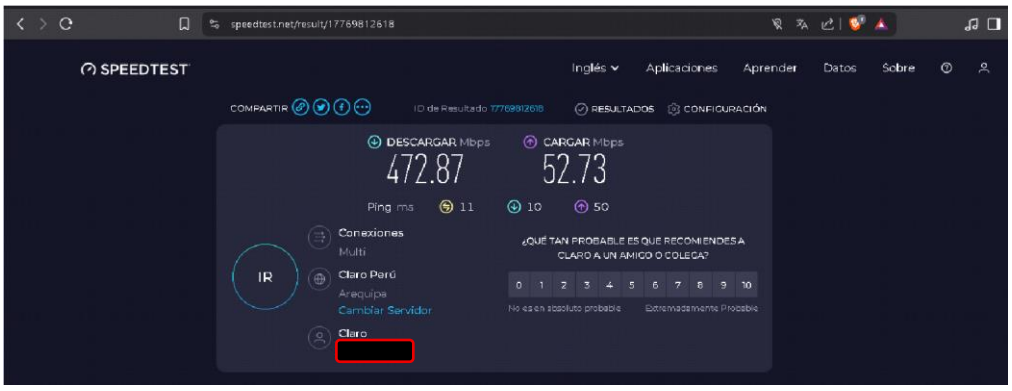
FING: ESCANEO DE RED

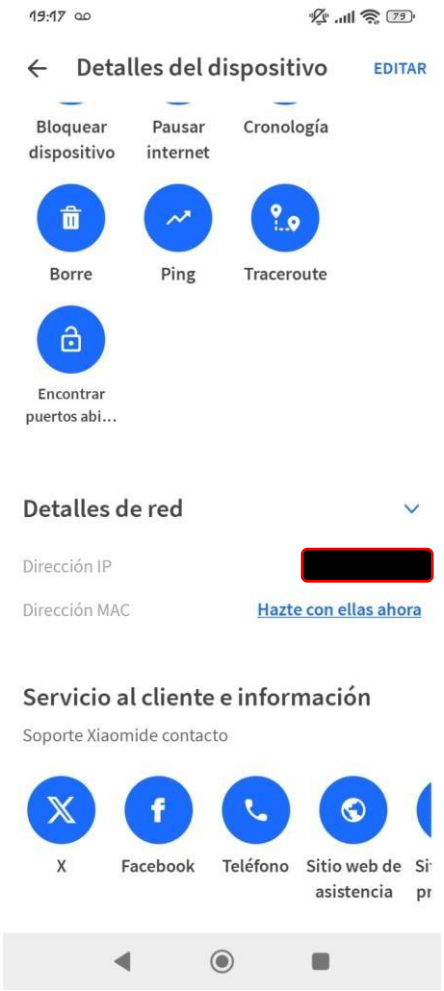
Nos permite saber cuántos dispositivos están conectados a nuestra red como speedtest


18:39
ZONA_ROJA
RECARGAR
Dispositivos
Red
Seguridad
Internet
3 dispositivos no
Tipo
WiFi
SSID
ZONA_ROJA
BSSID
Banda
2.4 GHz
Señal
-54 dBm
Canal
Ch #9
WPS habilitado
Si
Seguridad
WPA2
Velocidad de enlace
72 Mbps
CERRAR
dispositivos nuevos están deshabilitadas
Recibe una notificación cada vez que se incorpore un nuevo dispositivo a tu red.


19:17
Detalles del dispositivo
EDITAR
Redmi 14C
Xiaomi / Redmi 14C
El dispositivo está en línea desde 33m
Redmi 14C
Modelo
Marca
Xiaomi
Modelo
Redmi 14C
Android 15 REL
Sistema operativo
android
Marca
Google
Nombre
Android
Versión
Android
Administrar este dispositivo


19:18
02:00:00:00:00:00
RECARGAR
Dispositivos
Red
Seguridad
Internet
Última prueba de velocidad
ahora
Descargar
33,9 Mbps
Desde Lima, PE
Subida
31,3 Mbps
Para Lima, PE
Latencia
227 ms
Para Lima, PE
Probar ahora
ESTE DISPOSITIVO MÓVIL REALIZARÁ LA PRUEBA
Claro Tendencia
Según la velocidad, las opiniones de los usuarios y las interrupciones generalizadas
Rendimiento de velocidad
Tendencia estable
Opinión de los usuarios
Tendencia estable


speedtest.net/result/17769812618
SPEEDTEST
Inglés
Aplicaciones
Aprender
Datos
Sobre
COMPARTIR
RESULTADOS
CONFIGURACIÓN
DESCARGAR Mbps
472.87
CARGAR Mbps
52.73
Ping ms
11
10
50
Conexiones
Multi
Claro Perú
Arequipa
Cambiar Servidor
Claro
IR
¿QUÉ TAN PROBABLE ES QUE RECOMIENDES A CLARO A UN AMIGO O COLEGA?
0 1 2 3 4 5 6 7 8 9 10
No es en absoluto probable
Extremadamente Probable



CONCLUSION:

El uso de OSINT se ha consolidado como una herramienta esencial tanto en la ciberseguridad como en otras áreas estratégicas como el análisis empresarial y la inteligencia militar. A través del uso de herramientas como Maltego, SpiderFoot, Shodan y WHOIS, es posible obtener una gran cantidad de información pública que, correctamente analizada, puede prevenir ataques, detectar vulnerabilidades y fortalecer la postura de seguridad digital.

Además, los ejercicios prácticos demostraron cómo incluso usuarios comunes pueden utilizar estos recursos para diagnosticar problemas en sus redes o investigar incidentes de seguridad. Sin embargo, este poder debe usarse con responsabilidad, siempre respetando los marcos éticos y legales.

En conclusión, dominar las técnicas OSINT no solo mejora la capacidad de defensa ante amenazas, sino que también desarrolla una mentalidad crítica y proactiva ante los desafíos actuales del ciberespacio. La formación continua en este campo es fundamental para cualquier profesional de la seguridad informática.