**Python para Hacking ético**

**UD1: Reconocimiento**

**Apuntes**

**Junio 2022-2023**

AURKIBIDEA

[**1. Qué es el reconocimiento 1**](#_heading=h.1fob9te)

[**2. Reconocimiento pasivo 1**](#_heading=h.wd6rck282yqf)

[2.1. Redes sociales 1](#_heading=h.ro25me6nllcm)

[2.2. Búsquedas en Internet 2](#_heading=h.fty7j22mgxbj)

[2.2.1. Geolocalización 2](#_heading=h.qmu23udokab2)

[2.3. Bases de datos WHOIS 2](#_heading=h.x3c39jkctb17)

[**3. Reconocimiento activo 3**](#_heading=h.7gatewfbn5cg)

[3.1. Shodan 3](#_heading=h.ate6d44x2sk)

[3.2. DNS 4](#_heading=h.4e75empr07i)

[3.2.1. Registros más comunes 4](#_heading=h.8i4lmi8fpk0s)

[3.2.2. Transferencia de zona 4](#_heading=h.e1lm95pjav1y)

[3.3. Análisis de metadatos 5](#_heading=h.bqxwlbwlno91)

[**4. Bibliografía 6**](#_heading=h.8m7hrgahhyly)

# Qué es el reconocimiento

Un test de intrusión puede dividirse en cuatro fases: reconocimiento (*footprinting*), enumeración (*fingerprintig*), explotación y post-explotación. El presente capítulo se centrará en la primera de esas cuatro fases.

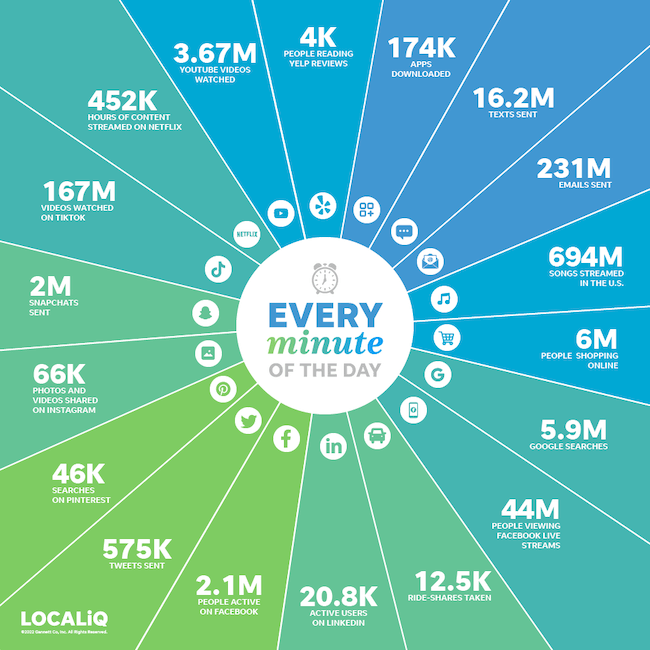
Lo primero a tener en cuenta es que en esta fase la fuente de información es toda Internet. De ahí se puede conseguir una gran cantidad de información que habrá que saber filtrar debidamente.

# Reconocimiento pasivo

Con el reconocimiento pasivo se buscará información sobre el objetivo sin establecer ninguna conexión directa con él; es decir, utilizando toda la información que podamos encontrar en Internet sobre él.

## Redes sociales

Esto es lo que hoy en día está ocurriendo en [Internet durante un minuto](https://localiq.com/blog/what-happens-in-an-internet-minute/).



Uno de los ingenieros sociales más reputados de la actualidad indica que la ingeniería social asienta sus éxitos en otros cuatro principios sobre las personas: todos queremos ayudar; el primer movimiento es siempre de confianza hacia el otro; no nos gusta decir "no"; a todos nos gusta que nos alaben.

Desde el punto de vista del pentester, uno de los mayores inconvenientes de las redes sociales es que suelen requerir un registro previo y un mínimo de interacción para obtener algo de información. Otro problema será discernir si esa información es o no veraz, ya que en las redes sociales hay muchas fuentes no fiables.

A continuación, se muestran algunas herramientas muy interesantes relacionadas con OSINT (inteligencia de fuentes abiertas):

*tinfoleak*

[Herramienta](https://tinfoleak.com/) que te proporciona un dossier con información sobre cualquier cuenta de twitter. Sólo tienes que introducir el nombre de la cuenta e indicar una cuenta de correo electrónico en la que, pasados unos minutos (ten paciencia), recibirás un enlace al informe.

*crosslinked*

Herramienta que simplifica los procesos de búsqueda de LinkedIn para recopilar nombres de empleados válidos de una organización que cuenten con perfil en la red social y que anuncien en ella dónde trabajan o han trabajado.

En [este anexo](https://docs.google.com/document/d/1dB2N5me2fnVqv8w6JN6Y1FD_jv0ILbEmQIkNHGkZm_w/edit#) hay una pequeña práctica para comprender su funcionamiento.

## Búsquedas en Internet

### Geolocalización

Desde el punto de vista del hacking ético, la geolocalización puede ser una herramienta útil en la fase de reconocimiento durante un proceso de pruebas de penetración. En esta fase, el objetivo es recopilar información sobre el sistema o red que se está evaluando, y la geolocalización puede proporcionar información valiosa sobre la ubicación física del sistema y sus activos en línea.

Por ejemplo, la geolocalización puede ayudar a identificar la dirección IP y la ubicación física de los dispositivos de red que se utilizan en el sistema, lo que puede ser útil para identificar posibles vectores de ataque. Además, la geolocalización también puede proporcionar información sobre la ubicación del servidor del objetivo, lo que puede ser útil para identificar posibles vulnerabilidades geográficas específicas y diseñar un plan de prueba más efectivo.

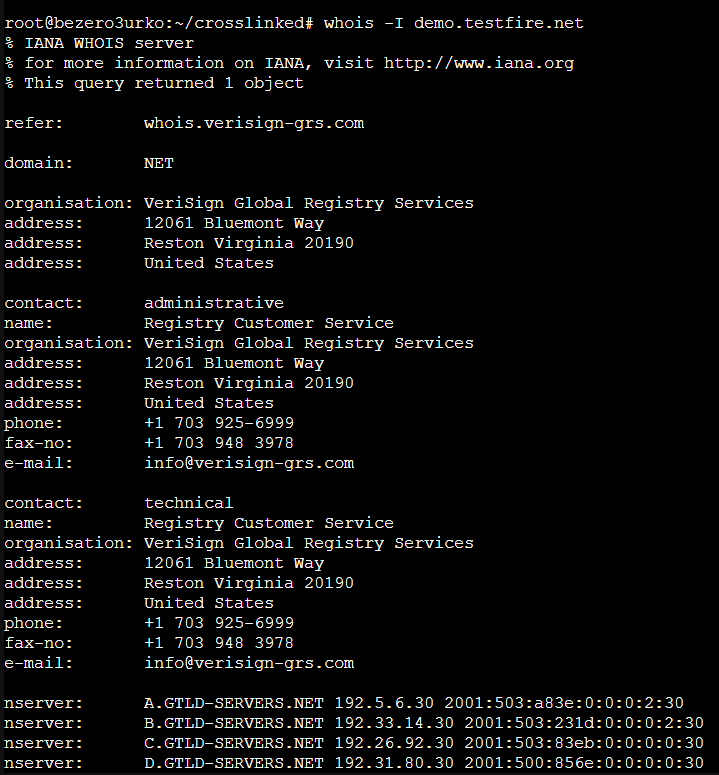
## Bases de datos WHOIS

Cuando una organización registra un dominio, tiene que proporcionar cierta información de la empresa, del propietario y del personal técnico del dominio; esa información queda registrada en “registradores”, entidades que la guardan en bases de datos; parte del contenido de éstas queda accesible. Sin embargo, desde el año 2018, al registrar el dominio se pide consentimiento para mostrar datos personales en las búsquedas; sin ese permiso, los datos no se mostrarán en una consulta Whois.

El servicio *Whois* es un protocolo TCP usado para realizar consultas y obtener datos sobre un dominio. Hay páginas web que proporcionan la opción de realizar consultas Whois: Icann/Lookup (no permite búsquedas sobre dominios *.es*), [DomainTools](https://www.domaintools.com/) (permite buscar dominios, incluso los de TLD *.es*), [www.dominios.es/dominios](http://www.dominios.es/dominios) (sólo para dominios *.es*).

También se pueden realizar consultas a través de la línea de comandos. En el caso de sistemas *Windows*, habrá que descargarse alguna herramienta; por ejemplo, la herramienta *whois* de la suite *sysinternals*, que proporciona Microsoft gratis. En la mayoría de las distribuciones GNU/Linux, en cambio, se encuentra por defecto (si no lo estuviera, bastaría para instalarlo con ejecutar el siguiente comando: sudo apt-get install whois).

La ejecución desde la línea de comandos es muy sencilla; basta con escribir la palabra *whois* seguida del dominio que nos interese. Es recomendable (y a veces indispensable) incluir el parámetro -I en el medio. Así, la consulta, antes de llegar al servidor autoritativo para la petición, consultará a [whois.iana.org](https://www.iana.org/whois).



# Reconocimiento activo

## Shodan

Existen motores de búsqueda que van más allá de los relacionados con buscadores. Son capaces de encontrar dispositivos conectados a Internet, lo cual puede ofrecernos una entrada para conocer direcciones IP de servidores o routers; también podemos lograr el acceso a cámaras de vigilancia o a dispositivos OT que han sido conectados sin reparar en su seguridad.

Uno de los más existosos es [Shodan](https://www.shodan.io/). La cantidad de información que puede mostrarnos con un par de clics es impresionante. Se pueden hacer búsquedas por IP (simplemente escribiendo la IP en la búsqueda); pero, además, si no tenemos tan claro el objetivo, con el comando *port* se pueden hacer búsquedas de puertos abiertos, y con ellos hacernos una idea de los servicios que están accesibles. Por otro lado, no sólo se pueden hacer búsquedas ideadas completamente por nosotros, sino que también se puede hacer uso de búsquedas predefinidas, a pesar de que algunas de ellas estarán inaccesibles fuera de la versión de pago.

Los filtros básicos que soporta Shodan son:

* *city*: permite especificar la ciudad.
* *country*: para indicar el país mediante sus iniciales.
* *geo*: para indicar las coordenadas geográficas a partir de los datos de latitud y longitud.
* *hostname*: para indicar el nombre de la máquina.
* *port*: puerto
* *before*/*after*: permite indicar un rango de fechas para acotar la búsqueda.

## DNS

### Registros más comunes

La información referente al protocolo DNS es almacenada en registros. Estos son algunos de ellos:

* **A**: se usa para treducir un nombre de equipo en una dirección IPv4.
* **CNAME**: se utilizan para crear alias de los nombres de equipos, de tal manera que a estos equipos se les pueda hacer referencia con más de un nombre. Por ejemplo: *ftp* y *www*.
* **NS:** define cuál será el servidor (o servidores) de nombres asociados al dominio.
* **MX**: identifica los servidores de correo de un dominio.
* **PTR**: se usa al revés que el registro A: traduce una IP en un nombre de dominio.
* **SOA**: indica que un servidor es autoritativo para una zona. Son muy importantes en las transferencias de zona.
* **TXT:** sirve para incluir texto; por ejemplo, para guardar información del propietario.

Si queremos obtener información sobre un DNS, podemos utilizar muchas herramientas. *Kali* trae instaladas muchas: *dnsdict*, *dnsenum*, *dnsmap*, *dnsrecon*, *dnsrevenum6*, *dnstrcker*…

### Transferencia de zona

Podemos tener un servidor DNS secundario además del primario; el secundario posee una copia de los datos recogidos en el primario. Esto ocurre gracias a que el servidor secundario solicita una transferencia de zona al primario, y éste, si está correctamente configurado, la efectúa. Esto tiene la ventaja de que la información de nuestro servidor DNS queda inmediatamente replicada, pero puede suponer un problema de seguridad grave si esa transferencia está abierta a petición de cualquier solicitante, que es lo que ocurre muchas veces.

De hecho, en un software específico como es BIND, muy utilizado en sistemas GNU/Linux para configurar servicios DNS, es muy común no haber tenido en cuenta este asunto, que es lol que ocurre cuando el archivo */etc/bind/named.conf.local* está configurado de manera básica. La manera de limitar este problema es incluir una sentencia en dicho archivo (tanto en la zona directa como en la inversa) que no permita las transferencias de zona más que hacia la IP del servidor secundario (o hacia ninguna, si no hubiera un secundario). La sentencia en cuestión es *allow-transfer*.

Supongamos que en la red 10.10.10.0/24 tenemos un servidor DNS secundario en la IP 10.10.10.233. La sentencia que tendríamos que incluir en la configuración del servidor DNS es:

*allow-transfer {10.10.10.233;};*

Habrá que agregar esa línea debajo de cada línea “*notify yes;* “.

Por lo tanto, desde el punto de vista del hacker ético, si tuviéramos acceso al servidor DNS primario, podríamos configurarlo para que las transferencias de zona estuvieran permitidas hacia donde nos interesara.

## Análisis de metadatos

Los metadatos son información adicional que no está visible directamente a la hora de abrir un documento. Esa información, de diversa índole, puede ser de gran utilidad para el pentester. Algunos de los metadatos que se pueden obtener están relacionados con: la aplicación usada para generarlos, nombres de usuario, fecha de creación y modificación, direcciones de correo electrónico, ruta en la que se ubica el archivo…

Los metadatos son necesarios en las organizaciones ya que ayudan a mantener el orden y control de los archivos, pero pueden suponer una fuga importante de información. Evidentemente, el primer paso para obtener los metadatos, es obtener los propios archivos deseados, para poder extraer de ellos la información deseada.

Exif (Exchangeable Image File Format) es un estándar de metadatos utilizado principalmente en fotografía digital. Los datos EXIF son los metadatos relacionados con dicho estándar: datos de configuración de la cámara, fecha y hora de la toma de la imagen, ubicación geográfica… Por poner un ejemplo cotidiano, si tomamos una foto con un dispositivo configurado para que su geolocalizacion esté compartida y su ubicación activada, ésta aparecerá entre los datos EXIF, pudiendo ser una información valiosísima para un atacante.

# Bibliografía

HERRERO PÉREZ, L. (2022).  *Hacking ético.* Madrid*.* Ra-Ma.

GONZÁLEZ PÉREZ, P. (2020). *Ethical Hacking*. Madird. 0xWORD.

GONZÁLEZ PÉREZ, P, SÁNCHEZ GARCÉS, G. y SORIANO de la CÁMARA, J.M. (2020). *Pentesting con Kali*. Madrid. 0xWORD

ALONSO, C. [*Un informático en el lado del Mal*](https://www.elladodelmal.com/)

CHANDEL, R. [*Hacking articles*](https://www.hackingarticles.in/)



