
Fuente: Bing Chat AI

# LABORATORIO 2. OSINT Y NAVEGACIÓN SEGURA

**DEPARTMENTO DE INFORMÁTICA. UNIVERSIDAD DE OVIEDO**

**Seguridad de Sistemas Informáticos | 2023 – 2024** (V4.0 *"S-81 Isaac Peral"*)

# Contenido

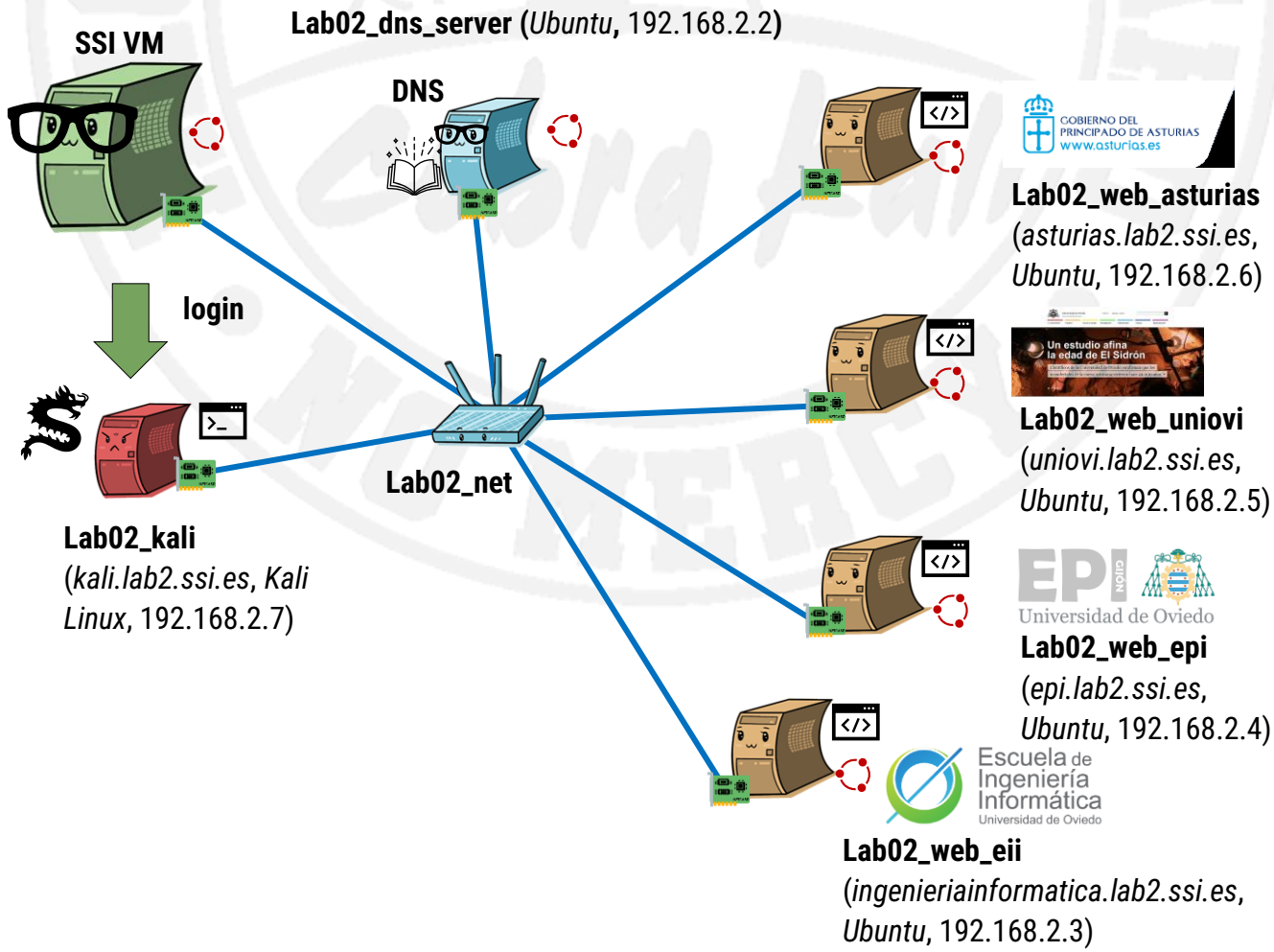
# Infraestructura de este laboratorio

**NOTA**: Antes de empezar, por favor asegúrate de la máquina virtual de la asignatura tiene una serie de paquetes instalados para que los laboratorios funcionen correctamente. Para ello **se necesita ejecutar lo siguiente**: `sudo apt install gnome-keyring gnupg2 pass`

En primer lugar, asegúrate de tener la estructura de carpetas `ssi_labs` que os damos dentro de tu máquina virtual. Este laboratorio (`lab_02`) consiste en una infraestructura compuesta por varios contenedores. No todas las actividades requieren el uso de todos ellos. Consulta el siguiente diagrama para entender el diseño de la infraestructura:

- **Una LAN interna**: (*lab02_net*, `192.168.2.0/24`)
- **4 servidores web distintos**
- **Un DNS**: proporciona nombres para cada servidor web en el dominio `lab2.ssi.es.`
- **Una máquina Kali** (`lab2_kali`) con varias herramientas instaladas solo para fines de **enumeración** que se describen en este documento. Esto también implica que no tienes que instalarlas. Esta máquina *Kali* es el punto de partida del laboratorio.

**IMPORTANTE: Asegúrate de haber leído y entendido las instrucciones del documento "*Infraestructuras automatizadas de SSI*" para entender cómo trabajar con este tipo de infraestructuras de laboratorios automatizados.**



# Bloque 1: Exploración de contenidos web

## Ejercicio L2B1_ROBOTS: Fichero robots.txt

### Descripción de la actividad / Aplicación práctica

Quieres saber si una web está revelando rutas “secretas” en este fichero público

### Resultados Esperados

Para completar esta actividad es necesario elegir cualquier web que prefieras y analizar su archivo `robots.txt`, determinando si puedes encontrar algo interesante o que comprometa la seguridad (y por qué).

### Otra información necesaria para su realización

Parte del ***Robot Exclusion Standard*,** este archivo se usa para indicar a los motores de búsqueda que siguen ese estándar que no indexen las URL correspondientes a ciertas entradas que se encuentran bajo la palabra clave `Disallow` en un archivo que se llama `robots.txt`. Estos archivos siempre son accesibles usando este patrón: `<URL de la web>/robots.txt`.

Algunos desarrolladores lo usan para que *Google* u otros motores de búsqueda no indexen contenido "sensible". El problema es que este archivo es público y accesible, por lo que los motores pueden leer su contenido y, por tanto, ¡tú también puedes! 😊. Puedes encontrar más información aquí: https://www.synopsys.com/blogs/software-security/robots-txt/

## Ejercicio L2B1_METADATOS: Metadatos de documentos

### Descripción de la actividad / Aplicación práctica

Necesitas saber si los documentos, imágenes, etc. de un sitio web están revelando demasiada información acerca de sus propietarios o autores.

### Resultados Esperados

Esta actividad se completará cuando elijas cualquier archivo local o descargado de los tipos aceptados y lo analices con la web o la herramienta `exiftool` mencionadas para ver si encuentras algo interesante. Puedes contestar a estas preguntas:

- *¿Qué harías si encuentras IPs?*
- *¿Qué harías si encuentras nombres de personas?*
- *¿Qué harías si encuentras nombres de aplicaciones? ¿Qué crees que podría revelar ese dato?*

## Otra información necesaria para su realización

Los metadatos son datos adjuntos a un archivo, **pero no como parte de su contenido, sino normalmente en sus cabeceras de archivo.** Los metadatos se pueden adjuntar a un archivo como texto sin cifrar o cifrado. Mucha gente ignora que los archivos pueden tener metadatos. Peor aún, **mucha gente tampoco sabe que muchos programas ponen automáticamente metadatos en los archivos que generan sin su consentimiento, o sin ser conscientes de ello**.

🔍 ***La importancia de estos (meta)datos puede variar desde información trivial a verdaderamente comprometedora. Hoy en día, muchos servicios eliminan automáticamente los metadatos de los archivos que subes (las redes sociales lo hacen), pero no debes confiar en que lo hagan siempre (¡pueden tener errores!). También pueden conservar los metadatos originales para su uso particular (marketing), aunque los eliminen de los archivos que se muestran al público. En resumen, debes eliminar los metadatos de los archivos que cargues usando los programas adecuados por si acaso*** 😊**.**

**FOCA** es un programa de *Windows* que extrae y analiza los metadatos de diferentes tipos de archivos, que también implementa búsqueda en dominios, servidores DNS, URL y documentos publicados. FOCA se puede descargar desde aquí: https://github.com/ElevenPaths/FOCA. Hay una versión gratuita de código abierto y una versión comercial. Desafortunadamente, requiere configurar una *base de datos SQL* (*SQLExpress* o *SQL Server)* que lleva tiempo y esfuerzo instalar.

Esto no forma parte de los objetivos de este curso, por lo que, en lugar de esta herramienta, vamos a utilizar una en línea más simple, que analiza los metadatos de documentos individuales y otros tipos de archivos: ***Metadata2Go*** (https://www.metadata2go.com/view-metadata).

Esta página web permite subir cualquier archivo de una lista de tipos de archivo aceptados y extrae sus metadatos para ver si hay algo útil o sospechoso en ellos. Si la web no admite el tipo de archivo, podemos usar una herramienta local llamada `exiftool` que veremos en el laboratorio 4 para otra cosa. En este laboratorio la usaremos simplemente para **leer los metadatos completos de un archivo** que nos hayamos descargado de la web (admite zips, imágenes de muchas clases, documentos *Office*, PDF...) haciendo uso de sus opciones: https://manpages.ubuntu.com/manpages/trusty/en/man1/exiftool.1p.html. Por favor instálala si no está ya en la MV.

# Bloque 2: Buscando entre contenido expuesto y pasado

## Ejercicio L2B2_GHACK: *Google Hacking*

### Descripción de la actividad / Aplicación práctica

Puedes usar el motor de búsqueda de *Google* para encontrar información comprometedora de cualquier objetivo en Internet

### Resultados Esperados

Esta actividad se completará cuando elijas un sitio web y realices algunas operaciones de búsqueda con la base de datos *Google Hacking Database* para familiarizarte con el proceso, analizando si encuentras algo sospechoso.

**NOTA**: Es más que probable que *Google* te pida verificar tu identidad con una *catpcha* tras usar 2 o 3 búsquedas de este tipo, para comprobar que no eres un *bot*.

### Otra información necesaria para su realización

*Google Hacking* es la capacidad de realizar ciertas operaciones de búsqueda manuales en *Google,* normalmente combinadas con el operador `site:`. También se aplica sobre otros buscadores, aunque cada motor de búsqueda usa sus propios operadores. Estas operaciones de búsqueda tienen como objetivo detectar vulnerabilidades, problemas de configuración o información que puedan provocar un ataque.

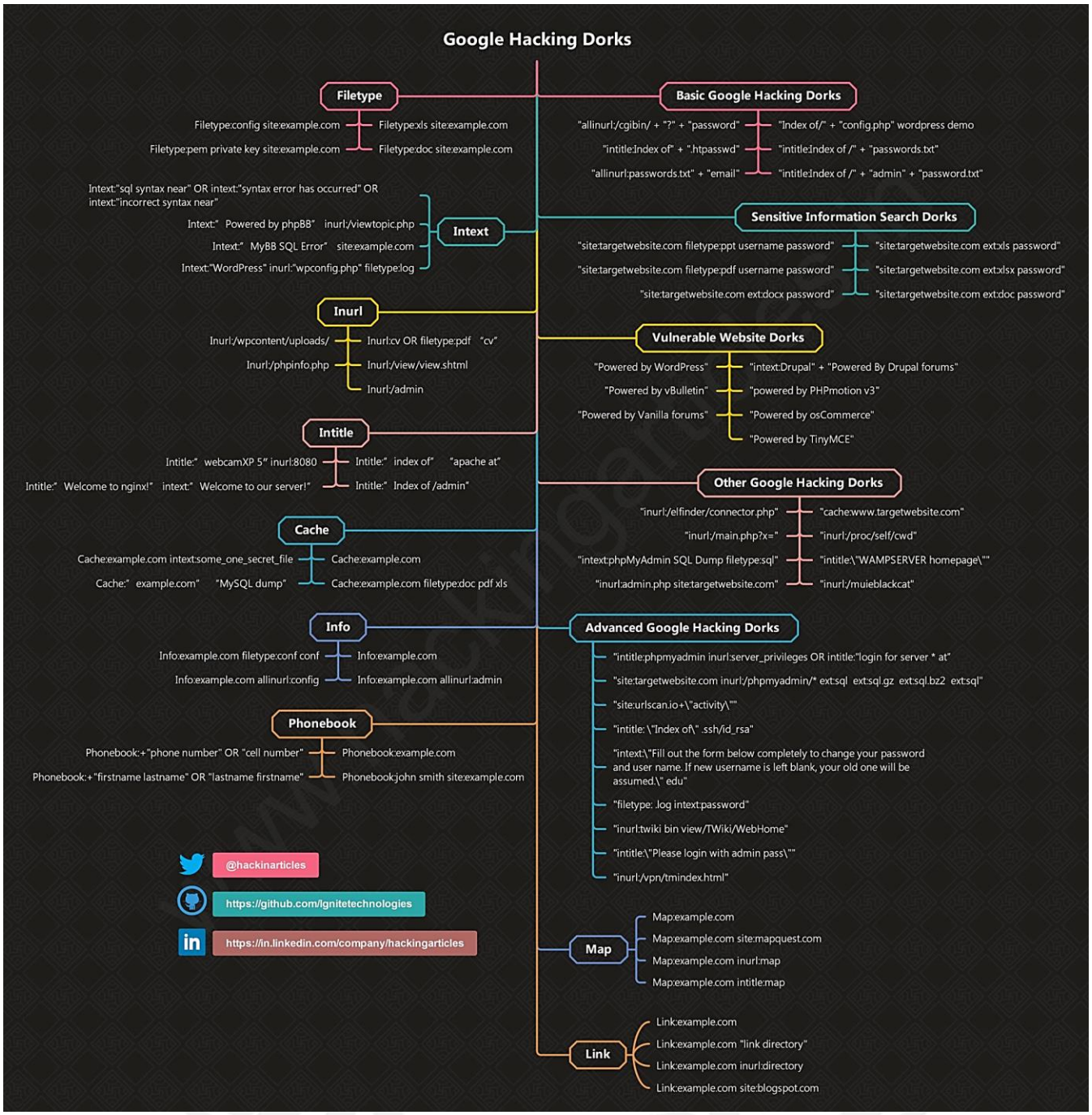
Hay muchas operaciones de búsqueda predefinidas que cubren diferentes tipos de ataques / procedimientos de recopilación de información en la ***Google Hacking Database*** **(GHDB):** https://www.exploit-db.com/google-hacking-database. El procedimiento para usar esta base de datos es:

- Elegir una categoría de búsqueda y una consulta
- Realizar la consulta sobre un objetivo concreto (utilizando el operador de búsqueda `site:`, https://support.google.com/websearch/answer/2466433?hl=es) y ver si el resultado coincide con el esperado, según la búsqueda elegida.

Hay una imagen con los pasos que requiere este procedimiento en el **primer seminario** del curso. Hay las siguientes categorías de búsquedas predefinidas

| | |
|---|---|
| Footholds | Files Containing Juicy Info |
| Files Containing Usernames | Files Containing Passwords |
| Sensitive Directories | Sensitive Online Shopping Info |
| Web Server Detection | Network or Vulnerability Data |
| Vulnerable Files | Pages Containing Login Portals |
| Vulnerable Servers | Various Online Devices |
| Error Messages | Advisories and Vulnerabilities |

También puedes encontrar direcciones con más ejemplos en el **primer seminario** y usar este *cheatsheet* como ayuda para hacer este ejercicio**:**




## Ejercicio L2B2_SHODAN: *Shodan*

### Descripción de la actividad / Aplicación práctica

Puedes usar el motor de búsqueda de máquinas *Shodan* para averiguar información acerca de cualquier dispositivo en Internet.

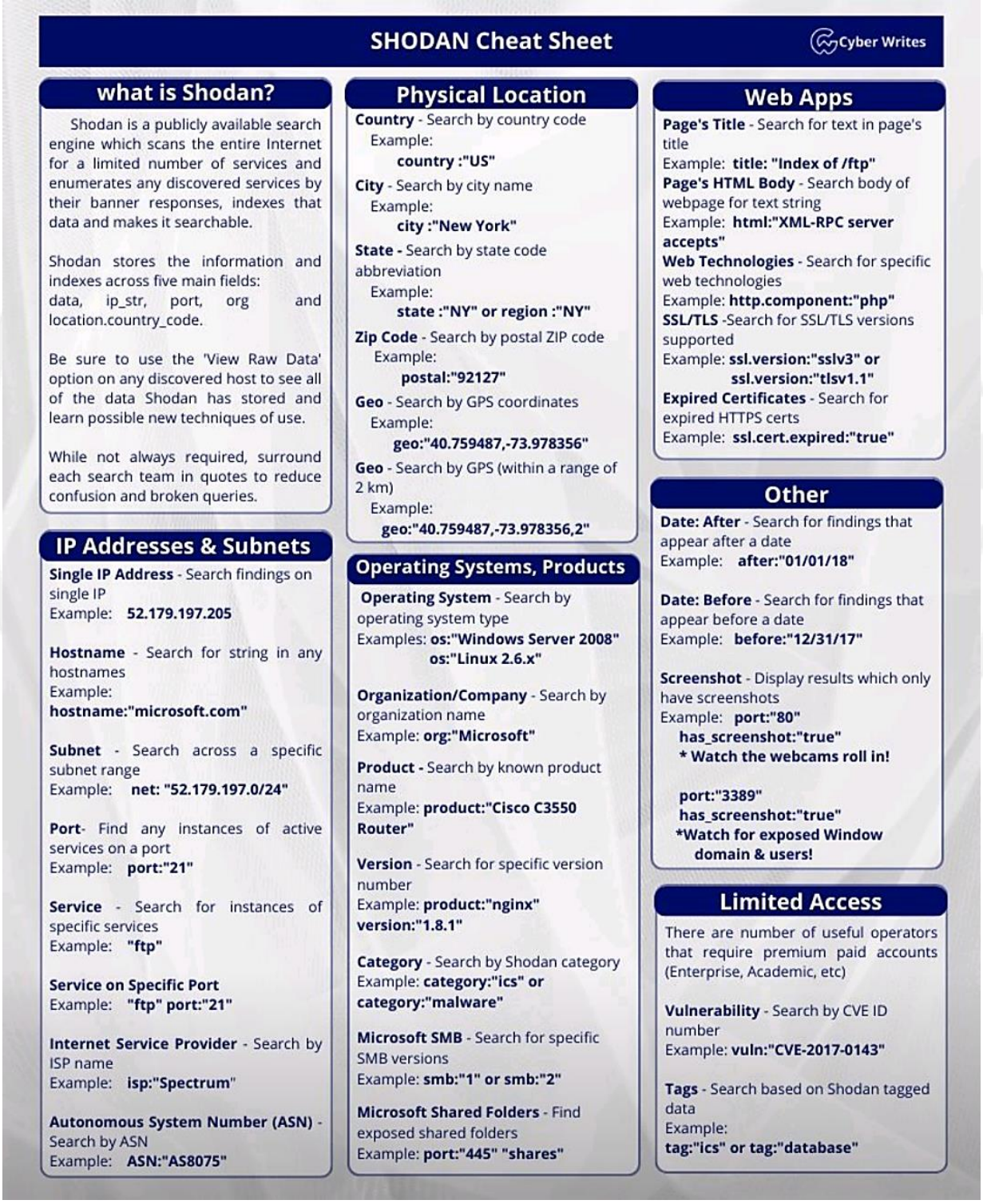
### Resultados Esperados

Esta actividad se completará cuando puedas hacer una petición en *Shodan* sobre una sola URL o IP, analizando la salida que se obtiene y por qué crees que su información puede ser un peligro para el objetivo.

🔍 ***Tienes más libertad si creas una cuenta gratuita, pero no es necesaria para hacer este ejercicio si te limitas a IPs individuales.***

## Otra información necesaria para su realización

*Shodan* (http://www.shodanhq.com/) es un buscador capaz de encontrar dispositivos en lugar de páginas web: *routers*, servidores, cámaras de grabación CCTV, semáforos, .... Se pueden encontrar más detalles sobre su funcionalidad y uso en el primer **seminario** (también incluye URLs con ejemplos de uso). También puedes usar este *cheatsheet* para realizar este ejercicio:



**SHODAN Cheat Sheet** — Cyber Writes

**what is Shodan?**

Shodan is a publicly available search engine which scans the entire Internet for a limited number of services and enumerates any discovered services by their banner responses, indexes that data and makes it searchable.

Shodan stores the information and indexes across five main fields: data, ip_str, port, org and location.country_code.

Be sure to use the 'View Raw Data' option on any discovered host to see all of the data Shodan has stored and learn possible new techniques of use.

While not always required, surround each search team in quotes to reduce confusion and broken queries.

**IP Addresses & Subnets**

**Single IP Address** - Search findings on single IP
Example: **52.179.197.205**

**Hostname** - Search for string in any hostnames
Example: **hostname:"microsoft.com"**

**Subnet** - Search across a specific subnet range
Example: **net: "52.179.197.0/24"**

**Port**- Find any instances of active services on a port
Example: **port:"21"**

**Service** - Search for instances of specific services
Example: **"ftp"**

**Service on Specific Port**
Example: **"ftp" port:"21"**

**Internet Service Provider** - Search by ISP name
Example: **isp:"Spectrum"**

**Autonomous System Number (ASN)** - Search by ASN
Example: **ASN:"AS8075"**

**Physical Location**

**Country** - Search by country code
Example: **country :"US"**

**City** - Search by city name
Example: **city :"New York"**

**State** - Search by state code abbreviation
Example: **state :"NY" or region :"NY"**

**Zip Code** - Search by postal ZIP code
Example: **postal:"92127"**

**Geo** - Search by GPS coordinates
Example: **geo:"40.759487,-73.978356"**

**Geo** - Search by GPS (within a range of 2 km)
Example: **geo:"40.759487,-73.978356,2"**

**Operating Systems, Products**

**Operating System** - Search by operating system type
Examples: **os:"Windows Server 2008"** **os:"Linux 2.6.x"**

**Organization/Company** - Search by organization name
Example: **org:"Microsoft"**

**Product** - Search by known product name
Example: **product:"Cisco C3550 Router"**

**Version** - Search for specific version number
Example: **product:"nginx" version:"1.8.1"**

**Category** - Search by Shodan category
Example: **category:"ics" or category:"malware"**

**Microsoft SMB** - Search for specific SMB versions
Example: **smb:"1" or smb:"2"**

**Microsoft Shared Folders** - Find exposed shared folders
Example: **port:"445" "shares"**

**Web Apps**

**Page's Title** - Search for text in page's title
Example: **title: "Index of /ftp"**
**Page's HTML Body** - Search body of webpage for text string
Example: **html:"XML-RPC server accepts"**
**Web Technologies** - Search for specific web technologies
Example: **http.component:"php"**
**SSL/TLS** -Search for SSL/TLS versions supported
Example: **ssl.version:"sslv3" or ssl.version:"tlsv1.1"**
**Expired Certificates** - Search for expired HTTPS certs
Example: **ssl.cert.expired:"true"**

**Other**

**Date: After** - Search for findings that appear after a date
Example: **after:"01/01/18"**

**Date: Before** - Search for findings that appear before a date
Example: **before:"12/31/17"**

**Screenshot** - Display results which only have screenshots
Example: **port:"80"**
**has_screenshot:"true"**
*** Watch the webcams roll in!**

**port:"3389"**
**has_screenshot:"true"**
***Watch for exposed Window domain & users!**

**Limited Access**

There are number of useful operators that require premium paid accounts (Enterprise, Academic, etc)

**Vulnerability** - Search by CVE ID number
Example: **vuln:"CVE-2017-0143"**

**Tags** - Search based on Shodan tagged data
Example:
**tag:"ics" or tag:"database"**

# Ejercicio L2B2_CENSYS: *Censys*

## Descripción de la actividad / Aplicación práctica

Puedes usar el motor de búsqueda de máquinas *Censys* y otras herramientas auxiliares para averiguar información acerca de cualquier dispositivo público en Internet

## Resultados Esperados

Esta actividad se completará cuando puedas usar *Censys* para escanear un rango de IP o red (por ejemplo, un rango que pertenezca a Uniovi). A continuación, se deben hacer las siguientes operaciones:

- *Se debe analizar la salida que proporciona y la información que se muestra sobre cada host.*
- *Se debe analizar la información para determinar por qué podría ser peligrosa desde el punto de vista de un ataque.*
- *Dado que a Censys le falta el mapa de geolocalización que aporta Shodan, se debe lograr la misma funcionalidad combinando la web https://www.iplocation.net/ y Google Maps (que admite coordenadas de latitud y longitud)*

## Otra información necesaria para su realización

***Censys*** es como *Shodan,* pero presenta la información de una manera más estructurada. Permite hacer operaciones de búsqueda basadas en los datos que obtiene de los servidores que analiza en todo Internet. **El primer seminario** ofrece más detalles al respecto. Puedes encontrar ejemplos de uso aquí:

- https://search.censys.io/search/examples?resource=hosts
- https://support.censys.io/hc/en-us/articles/360059720271-Search-2-0-Example-Host-Queries

También puedes usar este *cheatsheet* para ayudarte a hacer este ejercicio:

# Cheatography

## Censys Search Cheat Sheet

by himajedi via cheatography.com/196419/cs/41272/

### IP Addresses and Subnets

| | |
|---|---|
| Single IP (*supports IPv4 and IPv6*) | 8.8.8.8 or ip:8.8.8.8 |
| Subnet by CIDR | ip: "23.0.0.0/8" |
| Subnet by IP Range | ip: [1.12.0.0 to 1.15.255.255] |
| Hostname | dns.names:"*.zip" |
| Autonomous System # (ASN) | autonomous_system.asn:16509 |
| Autonomous System Name | autonomous_system.name:"AMAZON-02" |
| IPv6 hosts | ip: "2001::/3" or labels:ipv6 |

### Ports, Protocols, and Software

| | |
|---|---|
| Port | services.port:22<br>services.port:[20 to 25]<br>services.port:{20,21,22} |
| Number of open ports on host | service_count: [1 to 20] |
| Service / Protocol | services.service_name:SSH |
| Transport protocol | services.transport_protocol:TCP |
| Software by product and/or vendor | services: (software.vendor:"Apache" AND software.product:"HTTPD") |
| Software by URI / CPE | services.software.cpe =`cpe:2.3:o:mikrotik:routeros:*:*:*:*:*:*:*:*` |
| Banner grab | services.banner:"HTTP/" |

### Geography

| | |
|---|---|
| Country | location.country:"United States" |
| City | location.city:"Ann Arbor" |
| State | location.province:"Michigan" |
| GPS Coordinates | (location.coordinates.latitude=41.85003 AND location.coordinates.longitude=-87.65005) |

**Pro tip:** Use Map To Censys to draw a box over the geographic area of interest and click "Open in Search" to see hosts in the area

### Labels

| | |
|---|---|
| search by label | labels:`<la bel -na me>` |

**Some useful host labels:** scada, c2, login-page, open-dir, network.device, cryptocurrency, managed-file-transfer, ipv6. See a breakdown of common labels here

### Handy Censys Search CLI JQ filters

| | |
|---|---|
| List of IP addresses | '.[].ip' |
| Banners | '.[] \| .ip as $ip \| .services[] \| [ $ip, .transport_protocol, .port, .service_name, .banner ]' |

Usage: `censys search <qu ery> | jq <fi lte r>`

### Web Entities (HTTP/S)

| | |
|---|---|
| HTML Title | services.http.response.html_title:"dashboard" |
| Response Body | services.http.response.body:"login" |
| HTTP Status code | services.http.response.status_code=200 |
| Server header | services.http.response.headers.Server:"nginx" |
| Certificate Issuer | services.tls.certificates.leaf_data.issuer.organization:"Let's Encrypt" |
| Certificate Subject Common Name | services.tls.certificates.leaf_data.subject.common_name:`*.hero kua pp.com` |
| TLS version (*Highest negotiated version*) | services.tls.version_selected:"TLSv1_1" |
| Favicon MD5 Hash | services.http.response.favicons.md5_hash:* |

### Use Case Examples

| | |
|---|---|
| Hacked web servers | services: (service_name:"HTTP" and http.response.html_title:"hacked by") |
| U.S. Government or Military hosts | dns.names: *.gov or dns.names:* .mil or name: *.gov or name:* .mil |
| Hosts serving login pages with port 22 open | services.port:22 and labels:`login-page` |
| Servers in Russia running remote access protocols | location.country:"Russia" and labels:`remote -access` |
| Filter out hosts with 100+ ports open | services.truncated: false |
| Compromised MikroTik routers | services.service_name: MIKROTIK_BW and "HACKED" |

**Pro tip**: Get more results by including virtual hosts -- click the gear icon and toggle **Virtual Hosts: INCLUDE**

By **himajedi**
cheatography.com/himajedi/

Published 14th November, 2023.
Last updated 2nd December, 2023.
Page 1 of 2.

# Ejercicio L2B2_WAYBACK: *The Wayback Machine*

## Descripción de la actividad / Aplicación práctica

Puedes usar el motor de búsqueda *Internet Archive* (aka "*Wayback Machine*") para averiguar información acerca de sitios web publicados en el pasado en muchos dominios de Internet

## Resultados Esperados

Esta actividad se completará cuando puedas usar la *Wayback Machine* para

- **Localizar la lista de URL históricas de cualquier sitio web que elijas**, cualquier archivo interesante que prefieras y las diferentes versiones históricas de cualquier documento o página web que estuviera en el sitio. Una vez que puedas hacer eso, también debes pensar en lo que esto podría significar desde el punto de vista de la seguridad (las preguntas al final del laboratorio pueden ayudarte a analizarlo).
- **Localizar post antiguos de una cuenta pública de la red social** que quieras de un personaje público. Tú eliges la fecha. *¿Crees que la Wayback Machine puede localizar post que se hayan borrado tiempo después de haberse publicado?*

## Otra información necesaria para su realización

*(**NOTA**: La Wayback Machine es masiva, y por tanto es bastante lenta muchas veces. No es tu conexión o tu ISP, es que es así, y no puedes hacer nada para evitarlo, lo sentimos 😊)*

🔍 ***La mayoría de las personas (¡incluyendo bastantes administradores web!) están acostumbradas a buscar contenido comprometedor en las páginas web para eliminarlo, pero no incluyen el contenido comprometedor que ESTABA allí, pero ya no, o eliminan el contenido sin tener en cuenta que puede quedar archivado en la Wayback Machine. Este contenido puede resultar muy útil para los atacantes, y esta sección de laboratorio le enseñará cómo lidiar con él.***

Hay una página web de referencia para conocer la "historia" de cualquier sitio web en Internet y su nombre es "***The Wayback Machine***" (también conocido como *The Internet Archive):* https://archive.org/web/. Este sitio web es un archivo masivo de contenidos pasados ordenandos por fecha que fueron mostrados por cualquier sitio web público que estuvo activo en Internet, pero también tiene usos "hacker".

Por ejemplo, puedes inspeccionar **TODAS las URL** que se han extraído de un dominio en particular utilizando una consulta como esta: http://web.archive.org/web/*/<URL>/* (por ejemplo. http://web.archive.org/web/*/http://www.uniovi.es/* ). Ten en cuenta que la carga de URLs es asíncrona, por lo que puede tardar un tiempo. No te preocupes si inicialmente te encuentras una tabla vacía (para Uniovi, generalmente tarda 30s en cargarse).

Una vez que tenemos la lista histórica de URL de un sitio, podemos utilizar esta información para obtener información muy interesante sobre el mismo. Puedes encontrar más detalles aquí: https://www.elladodelmal.com/2013/04/hacking-con-archivecom-wayback-machine.html

- La tabla de URL se puede procesar con código para extraer todas las URL, o las **URL de un determinado tipo** que pueden ser interesantes para un determinado propósito. Por ejemplo, puedes extraer imágenes o documentos para inspeccionar su contenido (¡o metadatos! 😉 😉. Esto

también se puede hacer en la página web *de Wayback Machine,* ya que tiene un cuadro de texto de filtrado.

100,000 URLs have been captured for this domain.

Filter results (i.e. '.txt'): pdf

| URL | MIME TYPE | FROM | TO | CAPTURES | DUPLICATES | UNIQUES |
|---|---|---|---|---|---|---|
| http://www.uniovi.es/-/defecto.pdf | text/html | Jun 16, 2013 | Jul 15, 2013 | 2 | 0 | 2 |
| http://www.uniovi.es/-/file.pdf | text/html | Jun 16, 2013 | Jul 15, 2013 | 2 | 0 | 2 |
| http://www.uniovi.es/-/preistabelle.pdf | text/html | Jun 16, 2013 | Jul 15, 2013 | 2 | 0 | 2 |
| http://www.uniovi.es/-/presitabelle.pdf | text/html | Jun 16, 2013 | Jul 15, 2013 | 2 | 0 | 2 |
| http://www.uniovi.es/aal/archivos_pdf/neutro_materia.pdf | text/html | Jun 6, 2011 | Dec 15, 2018 | 7 | 6 | 1 |
| http://www.uniovi.es/accesoyayudas/estudios/373/Oficio+de+Adjunto+Plantilla+Solicitud.pdf/5412a9a3-9730-40a4-8 | text/plain | Sep 4, 2014 | Sep 4, 2014 | 1 | 0 | 1 |
| http://www.uniovi.es/accesoyayudas/tramites/tramite/-/asset_publisher/v9UAvM9qJpFc/content/wwww.uniovi.es/documents/31582/243104/INSTANCIA+VICERRECTOR+ESTUDIANTES_131028.pdf/d7cdc975-d56c-404f-b5a0-ef50be637791 | text/html | Sep 8, 2014 | Sep 8, 2014 | 1 | 0 | 1 |
| http://www.uniovi.es/Alfonso_Garcia_Leal/1993478.pdf | text/html | Jan 19, 2012 | Apr 12, 2012 | 2 | 1 | 1 |
| http://www.uniovi.es/Areas/Mecanica.Fluidos/becasempleo/investigacionaerodinamica_paniaguaSMALL.pdf | unk | Nov 11, 2014 | Nov 11, 2014 | 1 | 0 | 1 |
| http://www.uniovi.es/Areas/Mecanica.Fluidos/docencia/_asignaturas/maquinas_de_fluidos/Lecc6_r1.pdf | unk | Apr 12, 2017 | Apr 12, 2017 | 1 | 0 | 1 |
| http://www.uniovi.es/Areas/Mecanica.Fluidos/docencia/_asignaturas/maquinas_de_fluidos/Presenta_Leccion3.pdf | unk | Apr 12, 2017 | Apr 12, 2017 | 1 | 0 | 1 |
| http://www.uniovi.es/Areas/Mecanica.Fluidos/docencia/_asignaturas/mecanica_de_fluidos/05_06/8.%20FLUJO_CONDUCTOS.pdf | unk | Jul 29, 2015 | Jul 29, 2015 | 1 | 0 | 1 |

- También puedes obtener el contenido de **archivos interesantes** de una página web. Por ejemplo, el archivo `robots.txt`
- **Historial de cualquier archivo del sitio web**: La columna de la tabla "URL" muestra el número de copias diferentes que cualquier archivo ha tenido a lo largo del tiempo. Esto significa que podemos localizar cualquier versión de cualquier archivo que haya sido indexado. Puedes iterar a través de ellos en la vista de calendario una vez que hagas clic en el archivo

Saved **4 times** between June 28, 2012 and July 11, 2013.

1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 **2013** 2014 2015 2016 2017 2018

**JAN**

| | | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 27 | 28 | 29 | 30 | 31 | | |

**FEB**

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | 1 | 2 | |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | | |

**MAR**

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | 1 | 2 | |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | | | | | | |

**APR**

| | | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 | | | | |

**MAY**

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 29 | 30 | 31 | |

**JUN**

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |

**JUL**

| | | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 | 31 | | | |

**AUG**

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |

# Bloque 3: Inspección de IPs y dominios

## Ejercicio L2B3_DOMINIOS: Descubrimiento de subdominios

### Descripción de la actividad / Aplicación práctica

Necesitas saber si un dominio concreto tiene subdominios registrados

### Resultados Esperados

Esta actividad se completará cuando puedas enumerar todos los subdominios de `uniovi.es` con cualquiera de las herramientas proporcionadas basadas en web. Las herramientas de línea de comandos deben usarse en el dominio incluido en la infraestructura de este laboratorio, `lab02.ssi.es`.

🔍 ***Recomendamos utilizar al menos una de las herramientas de línea de comandos y uno de los sitios web proporcionados para obtener una mejor comprensión de cómo realizar esta actividad. NO ES NECESARIO probar todas las herramientas mencionadas.***

### Otra información necesaria para su realización

Los nombres de dominio son muy curiosos porque normalmente la mayoría de la gente conoce el principal pero, la mayoría de las veces, hay **subdominios secundarios** que no son tan populares, solo conocidos por algunas personas, o simplemente olvidados. En cualquier caso, suponen más vectores de enumeración, y ahí reside el potencial de descubrir más cosas sobre un objetivo. Hay muchas maneras de descubrir esta información automáticamente. Estos son algunos de ellos:

- `knockpy` (https://github.com/guelfoweb/knock). *Herramienta Python* diseñada para enumerar subdominios en un dominio de destino a través de una lista de palabras. En *Ubuntu* puedes instalarlo con `sudo apt install knockpy` y ejecutar un escaneo básico con `./knockpy <objetivo>`. En el `README` de su repositorio puedes encontrar instrucciones de uso detalladas.
- `dnsenum` (https://github.com/fwaeytens/dnsenum): Por ejemplo. `dnsenum uniovi.es`. Si no se proporciona un parámetro `-f`, de forma predeterminada será `/usr/share/dnsenum/dns.txt` o un archivo `dns.txt` en el mismo directorio que `dnsenum.pl`

🔍 ***NOTA: Algunos estudiantes han informado que `dnsenum` puede congelar sus laboratorios cuando se arranca. Si es tu caso, cancela rápidamente la operación (CRTL+C) y usa otra herramienta. Esto se debe a un problema de instalación de VirtualBox, pero no hemos podido averiguar su origen exacto, ya que no os pasa a todos.***

## dnsenum 1.2.6 Cheatsheet (ingenieriainformatica.uniovi.es)

**multithreaded perl script to enumerate DNS information of a domain**

https://github.com/fwaeytens/dnsenum

### GENERAL USAGE

```
dnsenum [Options] <domain>
```

### NOTES

If no -f tag supplied will default to /usr/share/dnsenum/dns.txt or the dns.txt file in the same directory as dnsenum.pl

### OPTIONS

#### GENERAL OPTIONS

- **--dnsserver <server>**: Use this DNS server for A, NS and MX queries.
- **--enum**: Shortcut option equivalent to --threads 5 -s 15 -w.
- **-h, --help**: Print this help message.
- **--nocolor**: Disable ANSIColor output.
- **--noreverse**: Skip the reverse lookup operations.
- **--private**: Show and save private ips at the end of the file domain_ips.txt.
- **--subfile <file>**: Write all valid subdomains to this file.
- **-t, --timeout <value>**: The tcp and udp timeout values in seconds (default: 10s).
- **--threads <value>**: The number of threads that will perform different queries.
- **-v, --verbose**: Be verbose: show all the progress and all the error messages.

#### GOOGLE SCRAPING OPTIONS

- **-p, --pages <value>**: The number of google search pages to process when scraping names, the default is 5 pages, the -s switch must be specified.
- **-s, --scrap <value>**: The maximum number of subdomains that will be scraped from Google (default 15).

#### BRUTE FORCE OPTIONS

- **-f, --file <file>**: Read subdomains from this file to perform brute force. (Takes priority over default dns.txt)
- **-r, --recursion**: Recursion on subdomains, brute force all discovered subdomains that have an NS record.
- **-u, --update <a|g|r|z>**: Update the file specified with the -f switch with valid subdomains.

| | |
|---|---|
| a (all) | Update using all results. |
| g | Update using only google scraping results. |
| r | Update using only reverse lookup results. |
| z | Update using only zonetransfer results. |

```
operario@kali:~$ dnsenum uniovi.es
dnsenum VERSION:1.2.6

-----   uniovi.es   -----

Host's addresses:
__________________

uniovi.es.                              1216     IN    A        156.35.233.105

Name Servers:
_____________

enol.si.uniovi.es.                      172800   IN    A        156.35.14.2
chico.rediris.es.                       6186     IN    A        162.219.54.2
zeus.etsimo.uniovi.es.                  1800     IN    A        156.35.23.24
sun.rediris.es.                         3781     IN    A        199.184.182.1
solid.net.uniovi.es.                    1800     IN    A        156.35.11.170

Mail (MX) Servers:
__________________

mx02.puc.rediris.es.                    30       IN    A        130.206.19.162
mx02.puc.rediris.es.                    30       IN    A        130.206.19.130
mx01.puc.rediris.es.                    30       IN    A        130.206.19.162
mx01.puc.rediris.es.                    30       IN    A        130.206.19.130

Trying Zone Transfers and getting Bind Versions:
________________________________________________

Trying Zone Transfer for uniovi.es on enol.si.uniovi.es ...
AXFR record query failed: REFUSED

Trying Zone Transfer for uniovi.es on chico.rediris.es ...
AXFR record query failed: REFUSED
```

#### WHOIS NETRANGE OPTIONS:

- **-d, --delay <value>**: The maximum value of seconds to wait between whois queries, the value is defined randomly, default: 3s.
- **-w, --whois**: Perform the whois queries on c class network ranges. **Warning**: this can generate very large netranges and it will take lot of time to perform reverse lookups.

#### REVERSE LOOKUP OPTIONS:

- **-e, --exclude <regexp>**: Exclude PTR records that match the regexp expression from reverse lookup results, useful on invalid hostnames.

#### OUTPUT OPTIONS:

- **-o --output <file>**: Output in XML format. Can be imported in MagicTree (www.gremwell.com)

- https://dnsdumpster.com/: Sitio web que nos permite localizar subdominios de un dominio determinado.
- https://searchdns.netcraft.com/: Otra web que nos permite localizar subdominios de un dominio determinado.
- https://www.virustotal.com: Si vamos a "Buscar", damos un nombre DNS (por ejemplo, uniovi.es) y realizamos un escaneo de detección de URLs como el que vimos anteriormente, la pestaña "Detalles" también muestra sus subdominios asociados.
- https://crt.sh/: Darle un nombre de dominio (por ejemplo, uniovi.es) también nos da subdominios asociados.

Por último, es posible que algunos de estos dominios puedan estar, como decíamos, **abandonados.** En este caso tenemos dos opciones:

- Un dominio **verdaderamente abandonado** (sin contenido)
- Un **dominio no mantenido** (contenidos potencialmente vulnerables, versiones antiguas de los servicios, sin parchear, sin fijar...).

Estas no son las únicas herramientas que pueden hacer este trabajo, pero cubren la mayoría de los casos de uso. `Knockpy` y `dnsenum` requieren instalación, pero están disponibles en los paquetes estándar de *Kali Linux*. Puedes encontrarlos instalados en el contenedor *Kali* de la infraestructura del **Laboratorio 2**.

## Ejercicio L2B3_RANGO_IP: Analizar un rango de IPs

### Descripción de la actividad / Aplicación práctica

Necesitas saber el rango de IPs asignado a cualquier dominio de Internet

### Resultados Esperados

Esta actividad se completará cuando pueda verificar el rango de IP asignado a `uniovi.es` o cualquier organización `.com` que quieras

### Otra información necesaria para su realización

Una vez que conocemos los dominios DNS y subdominios de cualquier organización, podemos buscar en sus rangos de IP públicas asignadas para saber cuáles son las posibles IPs a inspeccionar, en busca de máquinas o servicios expuestos pertenecientes a esta organización. Para sitios `.com`, podemos consultar https://whois.arin.net. Para ello, podemos introducir el nombre de la organización (por ejemplo, "Microsoft", "Yahoo") en el cuadro de texto *SEARCH WHOIS-RWS* y desplazarnos hacia abajo para ver los rangos de IP que esta organización tiene asignados.

Para dominios `.es` podemos utilizar www.nic.es para el mismo fin. Pulsando en los detalles de un dominio (*"Ver datos"*) nos muestran los servidores DNS que sirven a las diferentes redes asignadas a la organización, de las que podemos extraer fácilmente IPs y rangos IP.

## Ejercicio L2B3_NMAPSCAN: Escaneos en LAN con *nmap*

### Descripción de la actividad / Aplicación práctica

Necesitas inspeccionar una red de área local (LAN) en busca de máquinas "vivas"

### Resultados Esperados

Esta actividad se completará cuando puedas localizar hosts activos en la LAN mencionada y sus nombres DNS. Puedes contestar a esta pregunta: *¿Entiendes la relación que hay entre las tres actividades de este bloque (Dominio->Subdominios->Rangos de IPs de cada subdominio->nmap) y que te permitiría hacer?*

### Otra información necesaria para su realización

El propósito de esta actividad es localizar todas las máquinas activas en una red LAN (¡no en Internet!). Para ello la **infraestructura del laboratorio 2** tiene una red LAN construida. Esto extiende la actividad del **Laboratorio 1**, que solo determina si un servidor está "vivo". Usa un *list scan* de este *cheatsheet* para ver si también se obtienen los nombres DNS de los hosts vivos.

## Nmap 7.80 Cheatsheet series (ingenieriainformatica.uniovi.es)

***Part 1: Reconnaissance (Basic)***

https://nmap.org/

```
operario@kali:~$ nmap -sn 192.168.20.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 18:38 CEST
Nmap scan report for 192.168.20.10
Host is up (0.00085s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
```

```
operario@kali:~$ sudo nmap -PS22,80 192.168.20.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 18:42 CEST
Nmap scan report for 192.168.20.10
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:67:7A:EF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

### GENERAL USAGE

nmap [Scan Type(s)] [Options] {target specification}

### NOTES

*Target specifications can be host names, IP addresses, ranges, networks, etc. (scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254)*

*Use these options to locate "alive machines" (sometimes only returns that, sometimes they also return some port / service information)*

### TARGET SPECIFICATION

**-iL <inputfilename>**: Input from from file a list of hosts/networks

**-iR <num hosts>**: Choose random targets

**--exclude <host1[,host2][,host3],...>**: Exclude hosts/networks

**--excludefile <exclude_file>**: Exclude list from file

### RECONOISSANCE EXAMPLES

*nmap -sn scanme.nmap.org*

*sudo nmap -PS22,80 scanme.nmap.org*

*sudo nmap --traceroute scanme.nmap.org*

### HOST DISCOVERY OPTIONS (WAYS TO CHECK "ALIVE" MACHINES)

**--dns-servers <serv1[,serv2],...>**: Specify custom DNS servers

**-n/-R**: Never do DNS resolution/Always resolve [default: sometimes]

**-PE/PP/PM**: ICMP echo, timestamp, and netmask request discovery probes

**-Pn**: Treat all provided hosts as online -- skip host discovery

**-PO[protocol list]**: IP Protocol Ping

**-PS/PA/PU/PY[portlist]**: TCP SYN/ACK, UDP or SCTP discovery to given ports

**-sL**: List Scan - simply list targets to scan

**-sn**: Ping Scan - disable port scan

**--system-dns**: Use OS's DNS resolver

**--traceroute**: Trace hop path to each host

# Bloque 4. Privacidad y seguridad en la navegación

## Ejercicio L2B4_PRIVACIDAD: *Blacklight*: Inspector de privacidad de la web

### Descripción de la actividad / Aplicación práctica

Necesitas saber hasta qué punto cualquier sitio de Internet **usa datos acerca de tu navegación** para su propio provecho

### Resultados Esperados

Esta actividad se completará cuando puedas usar *Blacklight* para inspeccionar cómo cualquier sitio que elijas está recopilando tus datos y analizar los resultados. Puedes contestar a estas preguntas:

- *¿Has detectado trackers en webs de organizaciones públicas (Gobiernos, Universidades...)?*
- *¿Cómo se comportan las tiendas típicas de Internet?*
- *¿Y los periódicos?*

### Otra información necesaria para su realización

*Blacklight* (https://themarkup.org/blacklight) escanea y descubre tecnologías específicas de seguimiento de usuarios (*tracking*) de cualquier sitio web. Esto significa que revela quién está obteniendo sus datos al navegar por un sitio y, por tanto, quien los usará para luego servirte anuncios basados (supuestamente) en tus gustos.

## Ejercicio L2B4_NAVEGAR: Crear un entorno de navegación seguro y verdaderamente privado en tu máquina virtual

### Descripción de la actividad / Aplicación práctica

Puedes crear un entorno de navegación web más seguro para tu día a día

### Resultados Esperados

Esta actividad se completará cuando tu navegador seguro esté operativo y puedas navegar a páginas web con todos los complementos mencionados activos. Puedes contestar a estas preguntas:

- *¿Consideras adecuado montar todas estas medidas de seguridad en una máquina virtual que uses solo para navegar?*
- *¿Crees que es buena idea combinar todo esto (máquina virtual incluida) con el NextDNS del laboratorio anterior de cara a la seguridad?*

## Otra información necesaria para su realización

*(**NOTA:** Seguro no significa privado. Tus intentos de conexión seguirán siendo registrados por los servidores de destino, y también registrarán tu IP. Para lograr un cierto grado de* privacidad de *navegación necesitas otras herramientas (como ToR), pero eso será más adelante 😊 )*

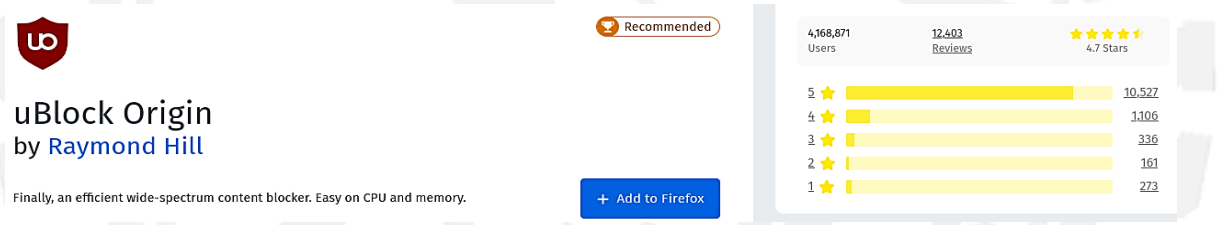
El propósito de esta sección es luchar contra las técnicas que has descubierto con *Blacklight,* ya que la cantidad de datos recopilados por un sitio web puede ser problemática en ciertos escenarios de uso. Aparte de eso, es muy útil tener un entorno de navegación más seguro en caso de que accidentalmente navegues por una página web maliciosa o troyanizada, con anuncios maliciosos u otras amenazas web. De esta manera, puedes navegar de una manera más segura **si usas los siguientes complementos del navegador**.

🔍 ***Al combinarlo con usar una "máquina virtual para navegación por Internet", obtienes un entorno de navegación notablemente más seguro (especialmente si es Linux).***

Usaremos *Firefox* como ejemplo de navegador, pero los mismos complementos también están disponibles en otros navegadores (también en versiones móviles). Esto también conecta con el tema de introducción de la teoría.

Para tratar con extensiones de navegador, debes considerar las cosas que se están permitiendo:

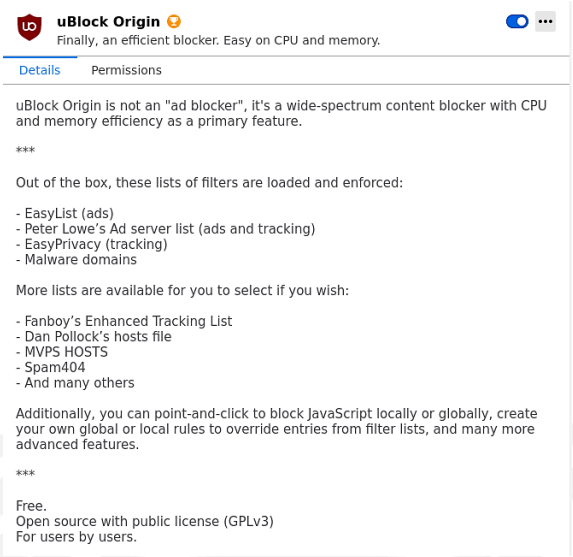
- **Hay extensiones maliciosas**: para evitar problemas, instala solo las *recomendadas* (inspeccionadas por el fabricante del navegador), con alta puntuación y muchas recomendaciones de usuario.




- Ten cuidado con las extensiones que piden demasiados permisos o permisos no razonables.
- Las extensiones normalmente se instalan utilizando una opción específica del navegador *(Complementos)* o un *market* (*Google Chrome Store),* no de una web externa.

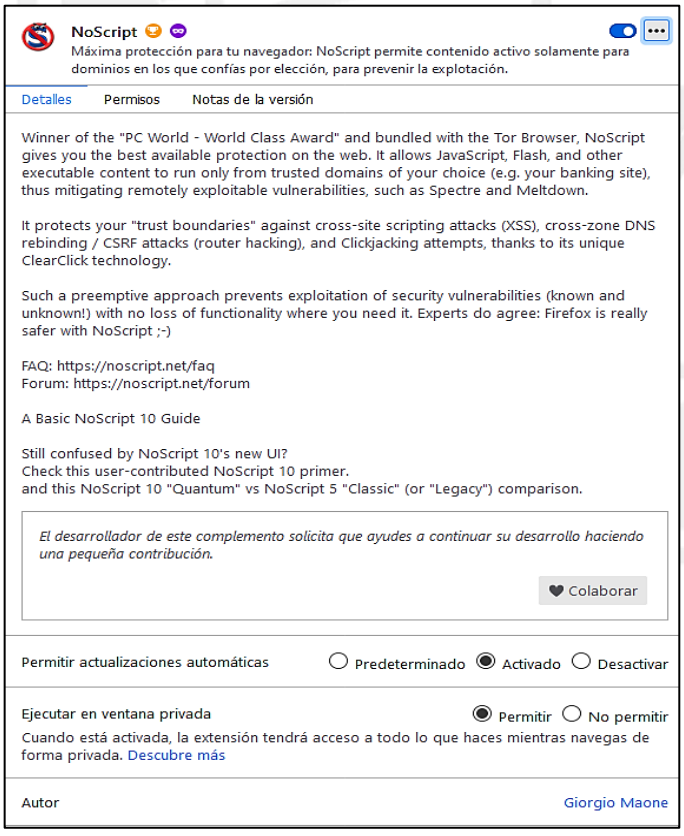
Una vez dicho esto, se recomienda instalar extensiones que se ocupen de:

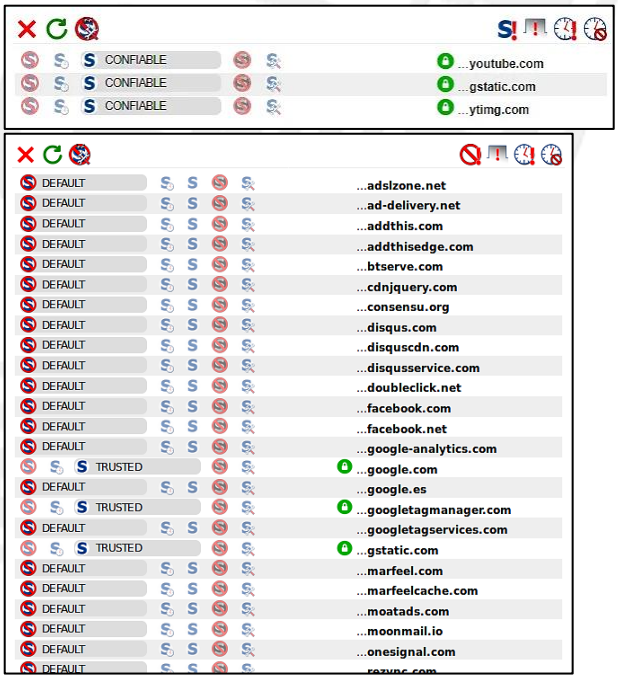
- **Anuncios:** ya que pueden ser molestos y/o maliciosos, incluso siendo una fuente de ingresos legal para los propietarios de páginas. ***uBlock Origin*** es el complemento recomendado.




- **Bloqueadores de *scripts***: Usar *JavaScript* en páginas web es común y legítimo, pero a veces los *scripts* se usan con fines maliciosos. Para evitar esto, se recomienda la extensión ***NoScript***. No solo bloquea *scripts*, sino que también identifica el uso de *scripts* maliciosos en páginas web. Sin embargo, su uso requiere "entrenamiento", ya que inicialmente bloquea la mayoría de los *scripts* en una página web, quedando muchas veces inutilizable (o haciendo que su contenido sea invisible).

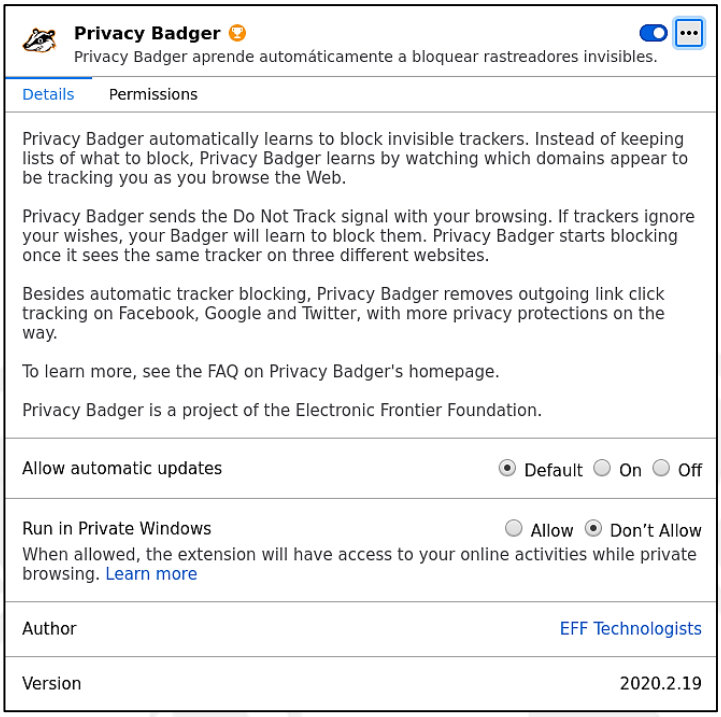
🔍 ***Puedes ir desbloqueando orígenes de scripts hasta que la página sea lo suficientemente utilizable para lo que quieres hacer. ¡No desbloquees anuncios o dominios maliciosos obvios! Normalmente, debes comenzar con orígenes de scripts que tengan el mismo nombre DNS que la página que estás viendo. Este tipo de "entrenamiento" se almacena entre sesiones, por lo que solo necesitas hacerlo una vez por página web.***




- **Privacidad:** ***Privacy Badger*** es la extensión recomendada, ya que evita que las páginas web rastreen tu historial de navegación y creen un perfil de tus comportamientos de navegación. También

bloquea redes sociales populares, los intentos de seguimiento de sitios web *(Facebook, Google, Twitter...)* e implementa otras medidas que protegen la privacidad del usuario.




# Ejercicio L2B4_PWDFILTRADAS: *Have I been pwnd?*

## Descripción de la actividad / Aplicación práctica

Necesitas saber si la clave de cualquier de tus cuentas de un servicio de Internet **ha sido potencialmente filtrada** en alguno de las muchas filtraciones de datos que ocurren hoy día

## Resultados Esperados

Esta actividad se completará cuando inspecciones cualquier cuenta de correo electrónico que quieras saber si es parte de una fuga de datos conocida. Puedes además pensar en posibles usos de esta herramienta que atenten contra la privacidad. Por ejemplo, *¿Qué crees que podría pasar si pones el email de alguien que conoces y sale que se ha filtrado en sitios como Tinder?*

## Otra información necesaria para su realización

*Have I been pwnd?* (https://haveibeenpwned.com/) es un sitio web que **almacena y permite consultar fugas de datos de usuarios**. Acepta nombres de cuentas de correo electrónico, e indica si este nombre de cuenta se ha filtrado en alguna de las bases de datos de usuarios conocidas que han sido robadas. Por tanto, si la cuenta de correo electrónico consultada está dentro de una de las múltiples bases de datos de usuarios robadas que maneja, te indicará el sitio cuyos usuarios han sido robados, cuándo y otros detalles sobre la fuga de datos asociada.

🔍 ***Debido a la probabilidad de usar la misma contraseña y correo electrónico en varios sitios, es muy importante verificar esto para evitar que un robo en un sitio facilite también intrusiones en otros sitios.***

# ✍️ Insignias y Autoevaluación

**NOTA:** Tienes una versión de esta tabla de insignias en formato editable disponible en el *Campus Virtual*. Puedes usar este archivo para crear un documento en el formato que desees y tomar notas extendidas de tus actividades para crear un log de lo que has hecho. Recuerda que el material que elabores se puede llevar a los exámenes de laboratorio.

| Nivel de insignia | Desbloqueado cuando | ¿Desbloqueado? |
|---|---|---|
|  | Puedes encontrar y analizar cualquier archivo `robots.txt` | |
|  | Responde a esta pregunta: *¿Cuáles crees que serán los problemas de seguridad que un `robots.txt` mal escrito podría provocar?* | |
|  | Puedes analizar los metadatos de cualquier archivo individual de un tipo adecuado que encuentres. Puedes responder a esta pregunta: *¿Por qué los metadatos pueden ser una amenaza para la seguridad?* | |
|  | Puedes analizar una única URL o IP utilizando *Shodan* e interpretar los resultados. También puedes responder a esta pregunta: *¿qué parte de los resultados enlaza con algo que vimos en el laboratorio anterior, y puede indicar un problema grave con la página web?* | |
|  | Puedes buscar todas las direcciones URL históricas de un dominio. | |
|  | Puedes responder a esta pregunta: *¿qué problemas de seguridad pueden aparecer si tenemos un archivo histórico de los diferentes contenidos de un archivo `robots.txt`?* | |
|  | Puedes responder a esta pregunta: *¿por qué los subdominios son interesantes desde el punto de vista de la seguridad? ¿Qué podría suceder si un subdominio (y su contenido) ha sido olvidado durante mucho tiempo?* | |
|  | Puedes analizar cómo un sitio web recopila datos de usuario y trata la privacidad mediante *Blacklight*. | |
|  | Puedes comprobar si una contraseña ha sido potencialmente comprometida en una fuga de datos y responder a esta pregunta: *¿qué debes hacer si encuentras tu email en una de estas intrusiones documentadas?* | |
|  | Puedes utilizar *Censys* para analizar los hosts de una red e interpretar los resultados, tanto de una red como de cualquier host individual. También puedes responder a esta pregunta: *¿puedes encontrar los servicios que se ejecutan en los hosts? ¿Cómo puedes encontrar si algunos son vulnerables?* | |
|  | Sabes cómo utilizar la base de datos de *Google Hacking* contra un objetivo concreto. | |
|  | Responde a esta pregunta: *¿Qué tipo de problema de seguridad crees que encontrar contenido que estaba alojado en el pasado podría suponer en un sitio web?* | |
|  | Puedes localizar subdominios de cualquier dominio mediante una de las herramientas proporcionadas y analizar la información del dominio que muestran. | |

| | | |
|---|---|---|
|  | Puedes localizar las redes IP de cualquier dominio *.com* o *.es* | |
|  | Puedes geolocalizar una IP cualquiera y responder a la siguiente pregunta: *¿Te parece que esta geolocalización es precisa?* | |
|  | Puedes localizar hosts activos en redes LAN | |
|  | Puedes configurar un entorno de navegación privado y seguro | |
|  | Puedes responder a esta pregunta: *¿Qué sucede si en lugar de un correo electrónico tuyo, decides investigar correos electrónicos de otras personas? ¿Qué sucede si el correo electrónico se notifica como comprometido?* | |
|  | Puedes responder a esta pregunta: Si soy capaz de encontrar cualquier imagen o documento que está (o estaba) en cualquier sitio web, *¿qué podemos hacer con estos archivos que pueda revelarme más información? ¿Qué sucede si puedo encontrar el historial de versiones de cualquiera de estos archivos? ¿Qué tipo de información puede proporcionar?* | |
|  | Puedes responder a esta pregunta: Si soy capaz de encontrar cualquier versión de cualquier página web de que una vez fue parte de un sitio web, *¿qué podemos hacer con estos archivos que pueda revelarme más información? ¿Crees que esto podría permitir localizar posibles vulnerabilidades?* | |
|  | Puedes responder a esta pregunta: Imagina que por error dejo en una página web un comentario comprometedor (por ejemplo, indicando un nombre de producto y / o versión, parte del código de servidor en un comentario ...). *¿Qué debemos hacer para eliminar realmente el problema de seguridad que esto podría suponer?* | |
|  | Puedes responder a esta pregunta: Es un hecho que los escaneos UDP son muy lentos, especialmente en WAN / Internet. También se sabe que `nmap` generalmente escanea por defecto sólo los puertos más utilizados en todo el mundo (una lista finita de puertos conocidos). Sabiendo esto, si quieres crear un servicio UDP "oculto" que sea muy difícil de localizar, *¿qué harías?* | |
|  | **He visto cosas que no creerías**: Conoces múltiples técnicas de enumeración y OSINT para extraer mucha información sobre máquinas, empresas y personas que puedes utilizar para investigarlas. | |