

Práctica 3: Recolección de información en fuentes abiertas I y II

Práctica 4: Escaneo y enumeración de activos

Seguridad en los Sistemas Informáticos

Grupo 9

Juan Antonio Pozo Orozco
José Manuel Gallardo del Águila
Jose Luis Venega Sánchez

CURSO 2024/25

Índice general

Capítulo 1

Práctica 3.1: Recolección de información en fuentes abiertas I

1.1. Ejercicio 1

Accederemos al enlace cuya dirección es:

`http://www.cs.fsu.edu/~langle/CIS4385-2015-1/2015-01-logs-test/auth.log.`

Conteste a las siguientes preguntas:

- ¿A qué tipo de archivo estamos accediendo, y para qué sirve en los sistemas?
Estamos accediendo a un fichero '.log' de una base de datos MySQL.
- ¿Qué información útil podríamos obtener de este archivo si nuestra finalidad fuera maliciosa?
Podríamos obtener credenciales de usuarios o direcciones IPs que podamos encontrar en el propio fichero.

Ahora, accederemos al enlace `http://ftp.rinotel.com/Software/Linux/proftpd.conf.`

Conteste a las siguientes preguntas:

- ¿A qué tipo de archivo estamos accediendo, y para qué sirve en los sistemas?
Estamos accediendo a un fichero de configuración ".conf", ya que en el dork estamos haciendo uso del parámetro **filetype .conf**.
- ¿Qué información útil podríamos obtener de este archivo si nuestra finalidad fuera maliciosa?

Tenemos un archivo de configuración '.conf' de un servicio *PROFTPD*, el cual corre bajo el protocolo *FTP*, por lo que podemos encontrar información sobre si la *TLS* está activada o no, o si podemos iniciar sesión con una conexión anónima.

Por último, accedemos al dork con título: *filetype username putty*. Haremos clic en el enlace que aparece, cuya URL es *http://asanovich.free.fr/COMPASS/4-1.log*.

Conteste a las siguientes preguntas:

- ¿A qué tipo de archivo estamos accediendo, y para qué sirve en los sistemas?
Estamos accediendo a un fichero de configuración de un dispositivo de red, el cual probablemente sea un switch.
- ¿Qué información útil podríamos obtener de este archivo si nuestra finalidad fuera maliciosa?
Podemos encontrar versión del software del propio switch, configuraciones y autenticación de usuarios, entre otros.

1.2. Ejercicio 2

Accedemos a la siguiente URL *https://open-bitbucket.nrao.edu/projects/CASA/repos/casa-pkg/browse/configuration/jenkins/warp/users/ville/config.xml?at=67d6e09964459b6f0d7004b36efbaedcee575b3f*

- ¿Qué tipo de archivo nos devuelve el uso de este dork?
Nos devuelve archivos de tipo XML (observable en *filetype:xml*)
- ¿Qué información útil podríamos obtener de este archivo si nuestra finalidad fuera maliciosa?
Si un atacante accediera a este archivo tendría toda la información relacionada con el email y contraseña (mediante su hash) del usuario Ville Suoranta (líneas 29 y 32).

Ahora, accedemos a

https://github.com/ptorres27/AnalyzeTorresPersonalWebsite/blob/master/proftpdpasswd

- ¿Qué información contienen estos archivos y para qué podría sernos útil dicha información si tuviéramos una intención maliciosa?
Estos archivos pueden contener información sensible, como nombres de usuarios y contraseñas (hasheadas) como podemos ver en la Figura 1.4.

1.3. Ejercicio 3

Seleccionamos la categoría “Web Server Detection” en Google Hacking Database, y buscamos el dork cuyo título es `intext:”Powered by phpSQLiteCMS”—intitle:”phpSQLiteCMS - A simple & lightweight CMS”`. Al hacer esto llegaremos a un resultado de Google y accedemos a varios enlaces devueltos por la búsqueda para detectar qué tipo de información nos devuelve la búsqueda realizada. Conteste a las siguientes preguntas:

- *¿Qué información importante estamos obteniendo a raíz del uso de este dork? Estamos obteniendo distintos sitios webs que usan phpSQLiteCM. phpSQLiteCMS es de código abierto y por tanto, esto permite encontrar algunas vulnerabilidades con mayor facilidad.*

A continuación, usaremos el dork con título "PHP CreditsConfigurationPHP Core.^{ext}:php inurl:info. Haremos clic sobre el enlace con dirección <http://61.216.3.97/info.php>. Conste a las siguientes preguntas:

- *¿A qué estamos accediendo exactamente?*
Estamos accediendo a la configurador del servidor PHP 61.216.3.97.
- *¿Qué información útil podemos obtener de aquí si nuestras intenciones fueran maliciosas?*
Obtenemos mucha información que podría ser útil desde un punto de vista malicioso, como versión de PHP, esto nos permite buscar las vulnerabilidades conocidas para dicha versión, información acerca del sistema operativo, que igualmente nos ayudaría a encontrar vulnerabilidades para dicha versión de SO, se pueden ver las extensiones de PHP habilitadas (curl, MySQL, etc.), se muestra también la ruta del fichero de configuración inicial (php.ini) y algunas más.
En definitiva al disponer de tanta información sobre la implementación de este servidor, cualquier atacante podría intentar encontrar vulnerabilidades.

Finalmente, usaremos el dork cuyo título es: `inurl:phpsysinfo/index.php?disp=dynamic`. Esto nos devolverá un resultado y accedemos al enlace:

`http://phpsysinfo.sourceforge.net/phpsysinfo/index.php?disp=dynamic`. Conteste a las siguientes preguntas:

- *¿A qué estamos accediendo exactamente?*
Estamos accediendo a la información del sistema que aloja dicha dirección.
- *¿Qué información útil podemos obtener de aquí si nuestras intenciones fueran maliciosas?*
Desde un punto de vista malicioso podemos rescatar bastante información útil, por ejemplo, podemos ver la dirección IP del servidor, información acerca del sistema como el kernel o el SO, el tiempo de actividad (el tiempo que no ha sido reiniciado), procesadores, información acerca de la memoria, entre otras. Como en el caso anterior, en definitiva, se muestra demasiada información que puede ser utilizada desde un punto de vista atacante para buscar y explotar vulnerabilidades del sistema.

1.4. Ejercicio 4

Accederemos al enlace cuya URL `https://uftm.edu.br/proplan/index.php?option=com_content&view=article&id=110:gtm1-divulgacao-da-uftm&catid=16:cev`.

- *A qué tipo de información estamos accediendo?*
Estamos accediendo a un mensaje de error 'RuntimeException' de una aplicación Joomla.
- *¿Qué información importante obtendríamos de este resultado, si nuestra intención fuera maliciosa?*
Podemos hacer uso de esto para conocer detalles de la base de datos, como por ejemplo, las tablas de la misma, con el fin de conocer la propia estructura de la base de datos y relizar consultas para obtener información sensible.

Ahora, accedemos al enlace con URL `https://eportal.pwc.ca/siteminderagent/forms/smpwservices.fcc`.

- *¿A qué tipo de información estamos accediendo?*
Como podemos ver, estamos accediendo a un panel de información de como deben de ser las contraseñas de ese sitio web.

- *¿Qué información importante obtendríamos de este resultado, si nuestra intención fuera maliciosa?* Podemos saber la composición de las contraseñas de la web, podemos hacer esto para poder filtrar las potenciales contraseñas para realizar un ataque de fuerza bruta y acceder al servicio web.

1.5. Ejercicio 5

Vamos a la URL

`https://www.jeeptelevision.com/fotoeventi/index.php?folder=c2ljaWxpYQ=`

- *¿A qué nos da acceso dicho enlace?*
Al sistema de ficheros de una máquina (directorio /home).
- *¿Qué acciones podemos realizar usando este enlace?*
Tener acceso a la información del sistema, modificar y subir archivos.
- *Desde el punto de vista de un ataque malicioso, ¿cómo podríamos sacar partido de este enlace?*
El simple hecho de tener acceso a los archivos puede resultar un ataque si se tratase de información confidencial, también podríamos modificar los archivos sin estar autorizados e incluso subir archivos maliciosos al sistema.

1.6. Ejercicio 6

De los dorks que encontramos en el enlace usaremos dos, el primero será el que tiene como título `allinurl: drive.Google.com/open?id=`. Con este tipo de dork podríamos acceder, por ejemplo, al enlace con URL:

`https://drive.google.com/file/d/0ByO02CwASGN0d0hNbWM4OEc5ZmM/view?resourcekey=0-OrCfpNOoo9q7fbXmsMIHQQ.`

Conteste a las siguientes preguntas:

- *Exactamente, ¿a qué estamos accediendo?*
Como podemos observar estamos accediendo al solucionario del examen de oposición del Cuerpo de Ingenieros de Caminos, Canales y Puertos de 2007.
- *¿Qué utilidad podemos encontrarle a este dork?*
Podemos encontrar ejercicios resueltos para estudiar para una convocatoria

actual, o tratar de buscar otros exámenes más recientes de la misma manera que hemos encontrado este.

A continuación, usaremos el dork cuyo título es `filetype:txt "gmail" – "hotmail" – "yahoo" -robots site:gov – site:us`. Accederemos al enlace:

<https://www.sec.gov/Archives/edgar/data/921669/000092847508000248/dfan14a070708.txt>.

Conteste a las siguientes preguntas:

- *¿Qué estamos viendo?*
Estamos viendo un *"proxy statement"* [?] de Carl C.Icahn, en este Carl C.Icahn discute por cambios en la junta directiva de *"Yahoo!"*
- *¿Qué información útil podemos obtener de este enlace?*
Podemos sacar información interna de la organización y las estrategias que se van a seguir.
- *¿Por qué podríamos considerar esta información sensible?*
Por el mismo motivo que en la pregunta anterior, se puede sacar información interna la cual puede afectar negativamente a la empresa ya sea por revelación de decisiones privadas, pérdida de la confianza en dicha empresa, etc. estas acciones pueden hacer que el valor de la empresa disminuya gravemente. También otras empresas competidoras con dicha información pueden aprovecharla para fortalecerse y superar a *Yahoo!*.

1.7. Ejercicio 7

Haciendo uso de dorks de Shodan, encuentre las IP correspondientes a 2 equipos con servicio MQTT (Message Queuing Telemetry Transport) en la ciudad de Logroño de la organización "arsys.es".

Hacemos uso de los parámetros: **org**, **country**, **city**, para especificar la empresa, el país y la ciudad a donde buscar, respectivamente.

1.8. Ejercicio 8

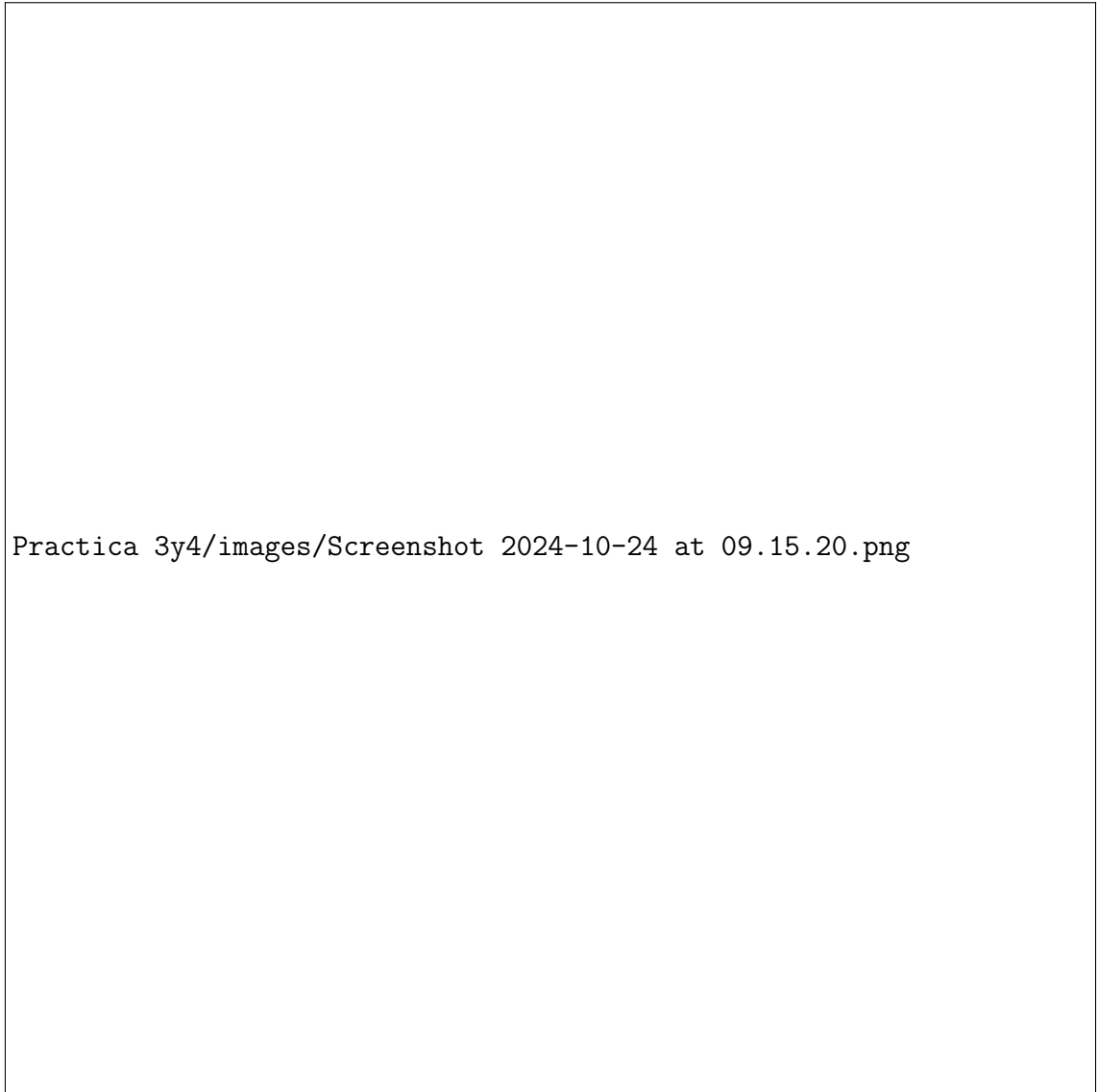
Haciendo uso de Shodan, encuentre el número de equipos del Nuclear Physics Institute de Moscu con el puerto Telnet a la escucha.

1.9. Ejercicio 9

Haciendo uso de Shodan, encuentre el nombre de la organización que más servidores de Minecraft hostea en la actualidad. Una vez hecho esto encuentre la IP de los servidores de este conocido juego en la provincia de Sevilla.

El nombre de la organización que más servidores de Minecraft hostea es BisectHosting con un total de 11500 servidores.

La IPs de las organizaciones con sevidores de Minecraft de Sevilla son:



Practica 3y4/images/Screenshot 2024-10-24 at 09.15.20.png

Figura 1.1: Fragmento del contenido del archivo.log

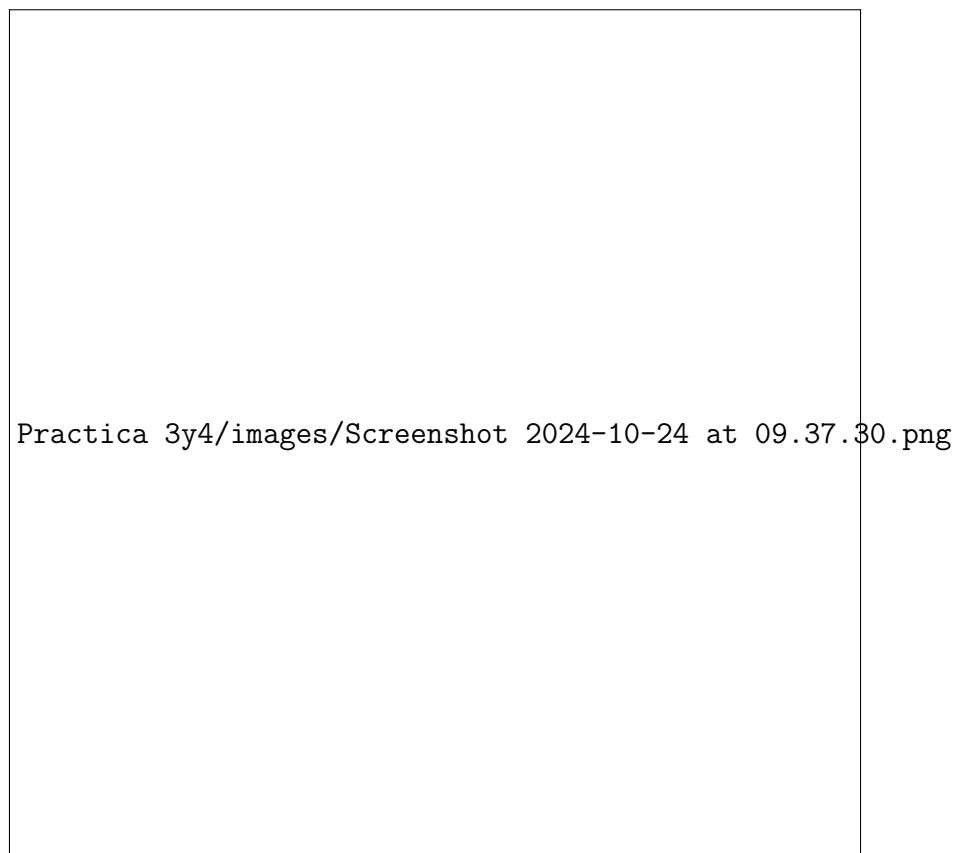


Figura 1.2: Contenido del fichero.conf



Figura 1.3: Parte del contenido de la configuración de un switch

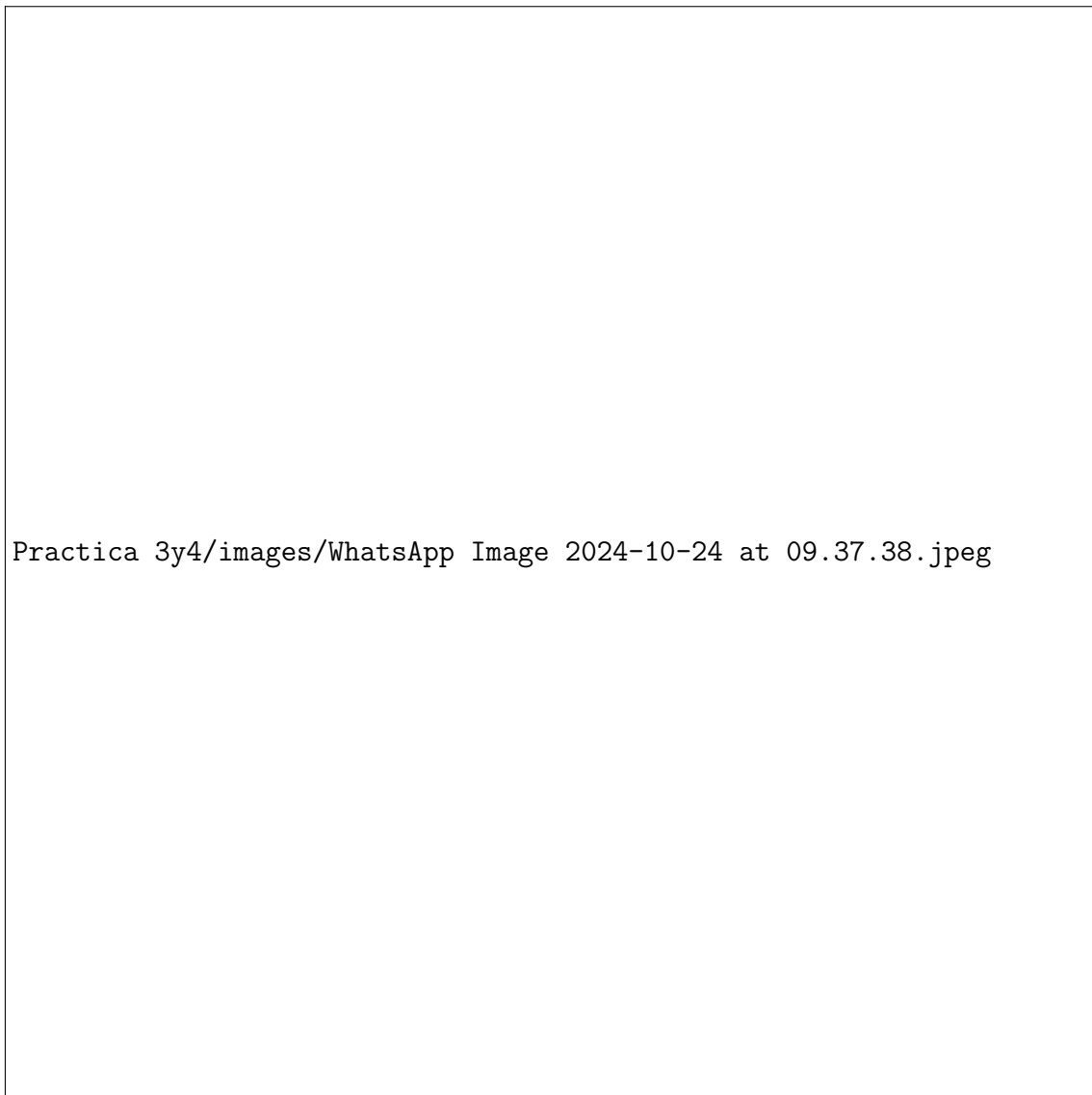


Figura 1.4: Contenido del archivo XML.

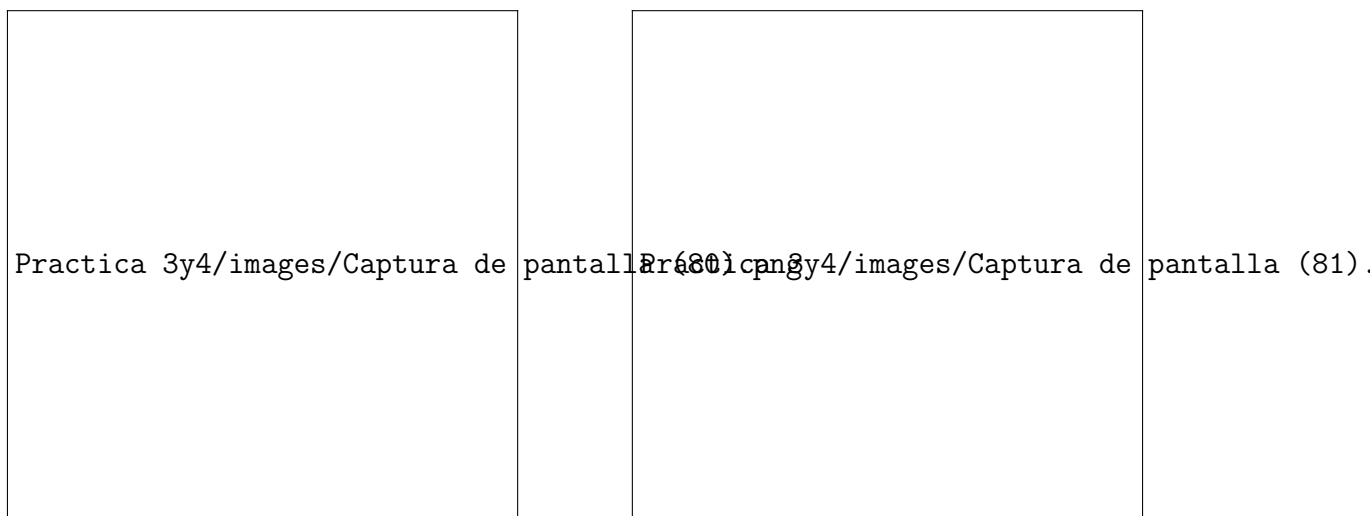


Figura 1.5: Búsqueda en Google Hacking Database

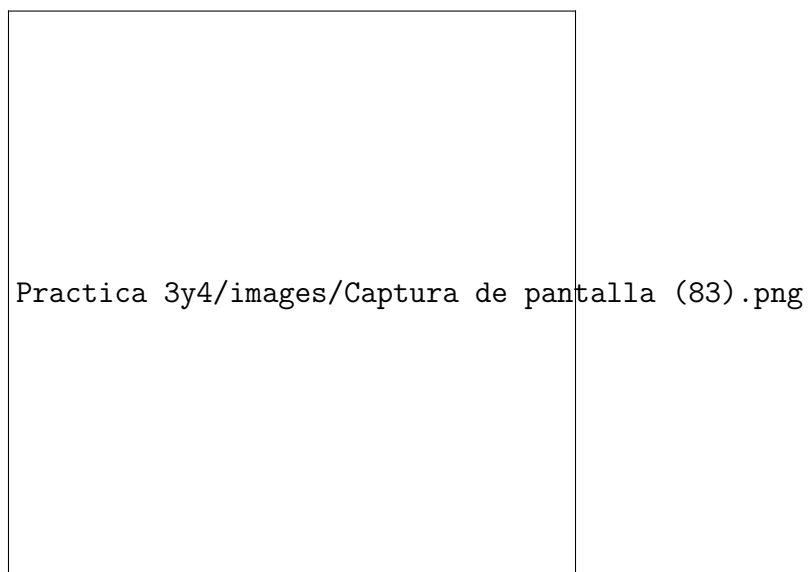
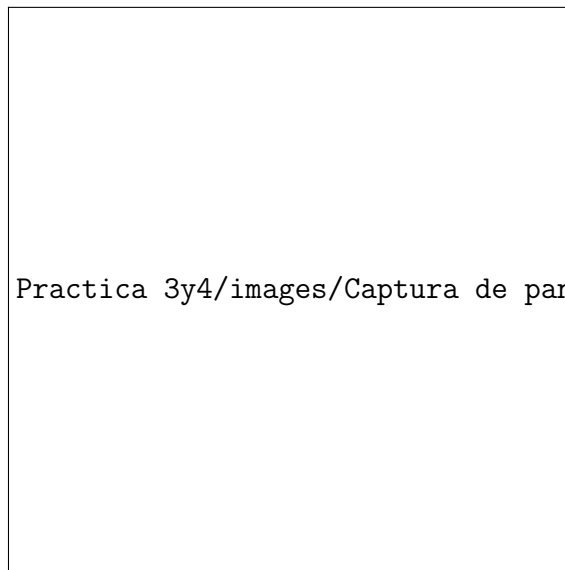
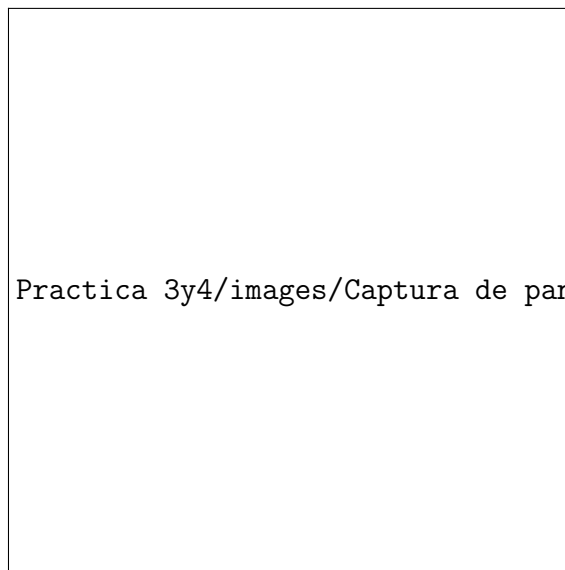


Figura 1.6: Acceso a uno de los sitios webs



Practica 3y4/images/Captura de pantalla (84).png

Figura 1.7: Acceso al sitio web



Practica 3y4/images/Captura de pantalla (85).png

Figura 1.8: Acceso al sitio web

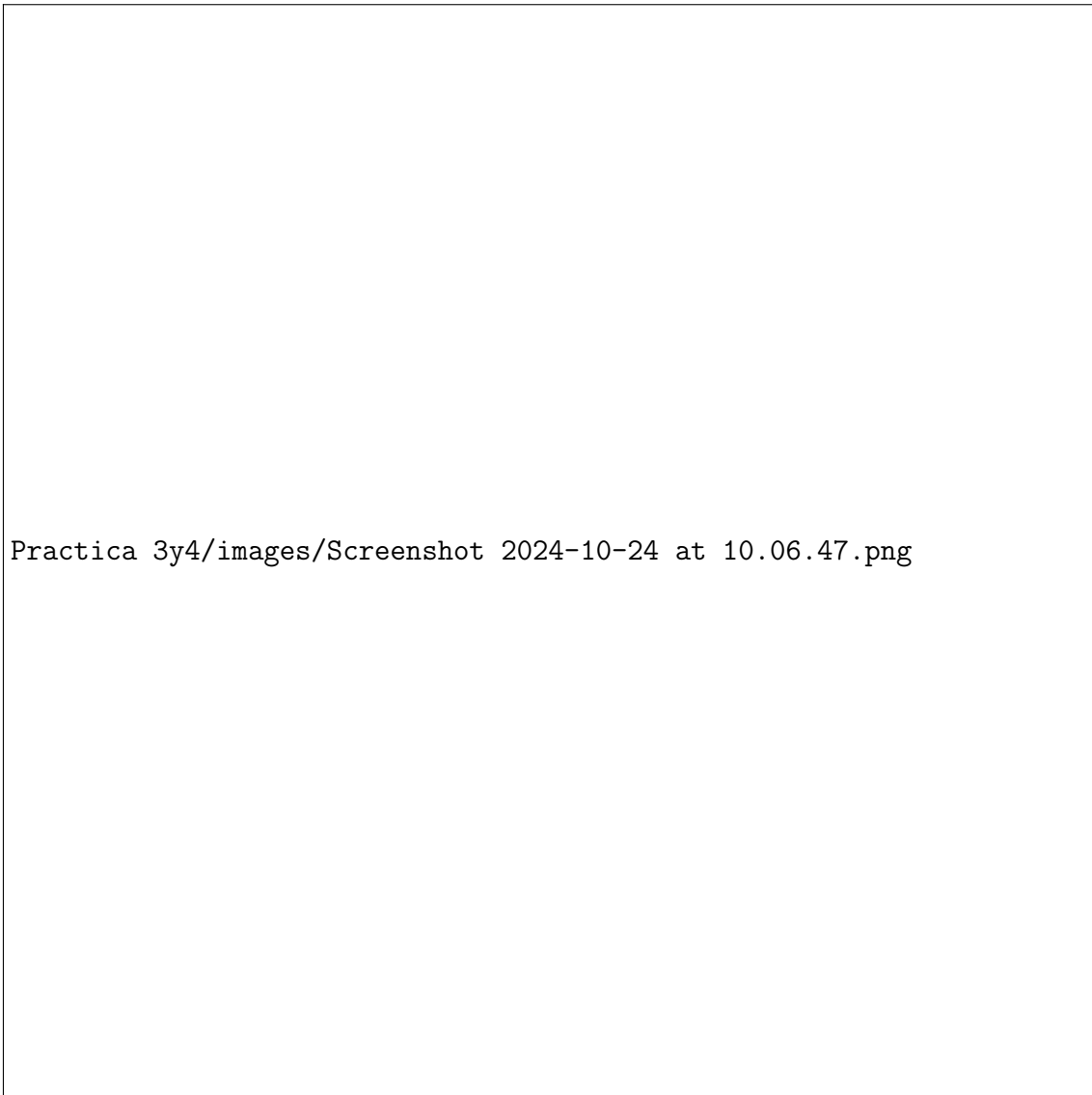


Figura 1.9: Código de error al que accedemos.

Figura 1.10: Panel con información de como debe de ser las contraseñas

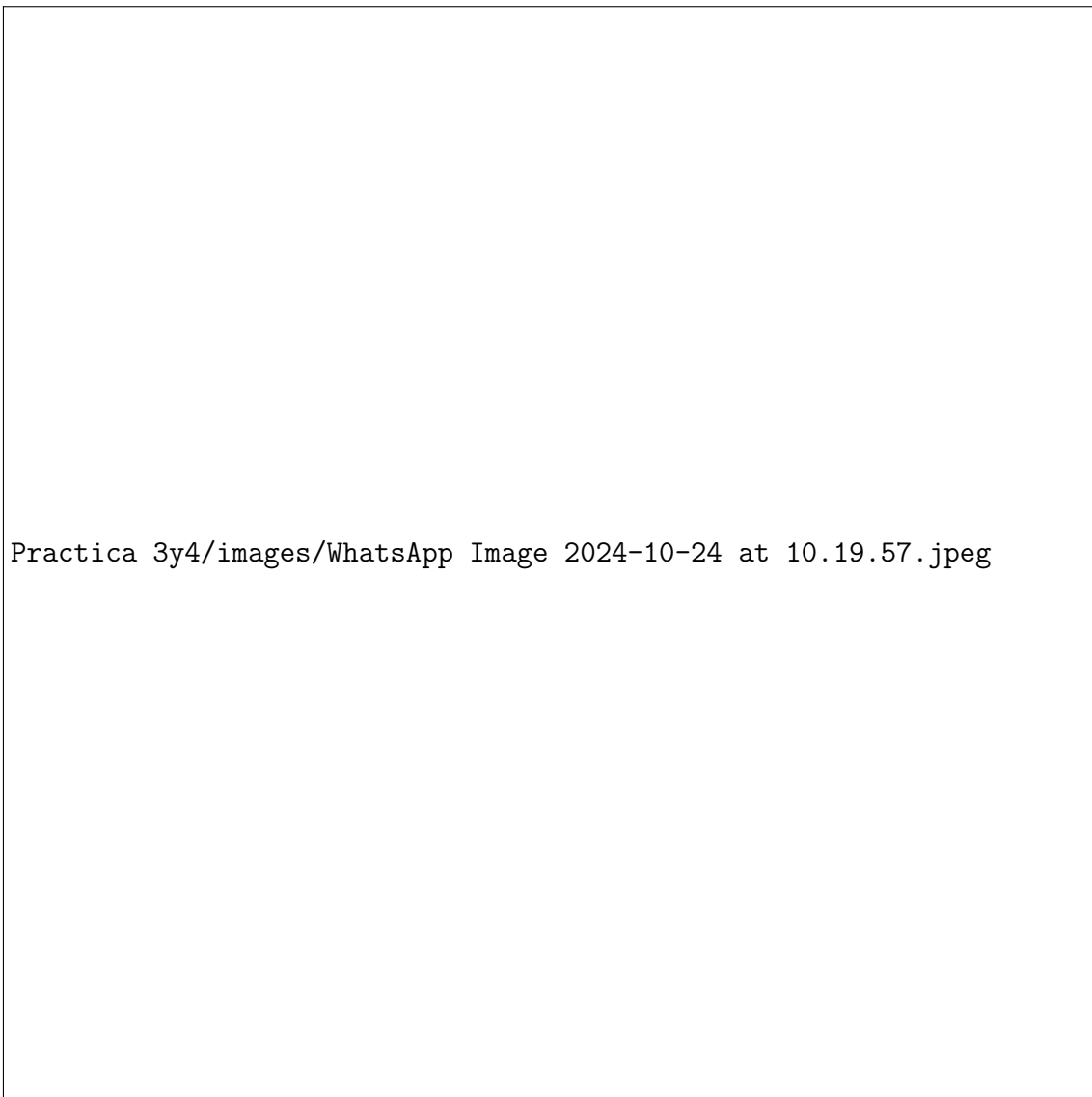
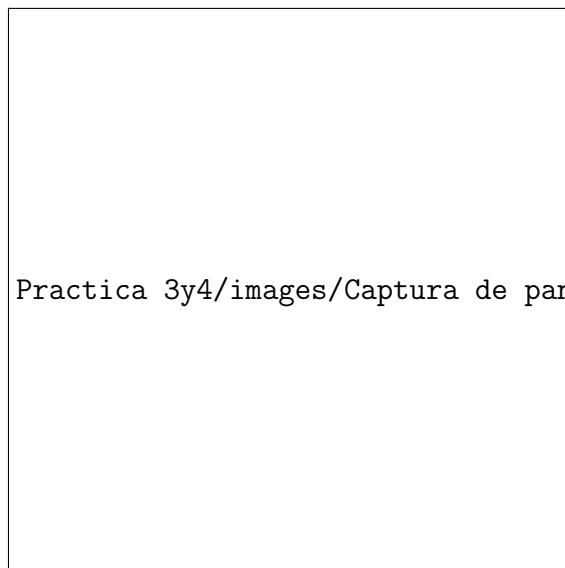


Figura 1.11: Directorio /home de un servidor.



Practica 3y4/images/WhatsApp Image 2024-10-24 at 10.20.22.jpeg

Figura 1.12: Caption

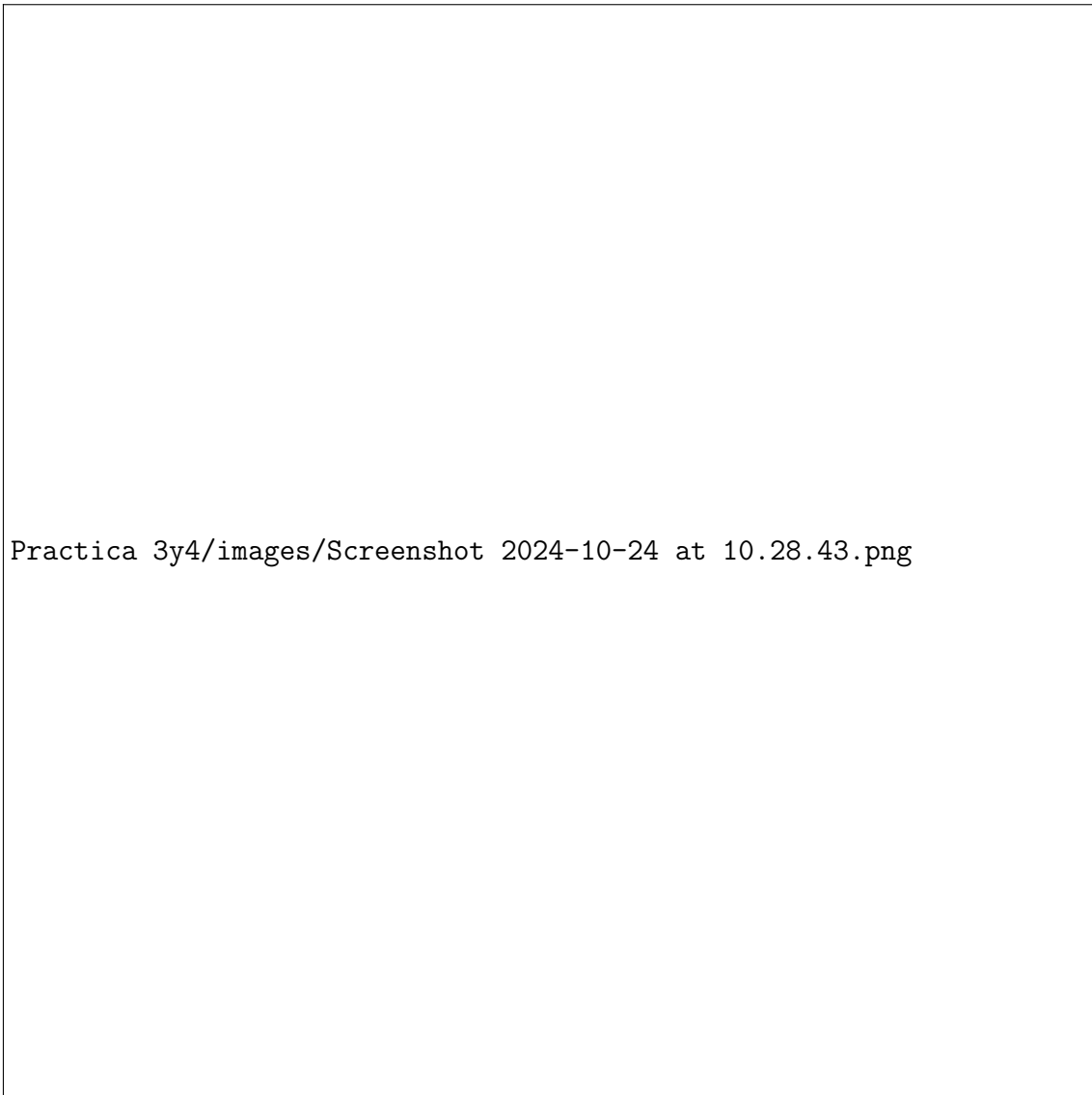


Practica 3y4/images/Captura de pantalla (86).png

Figura 1.13: Captura del sitio encontrado

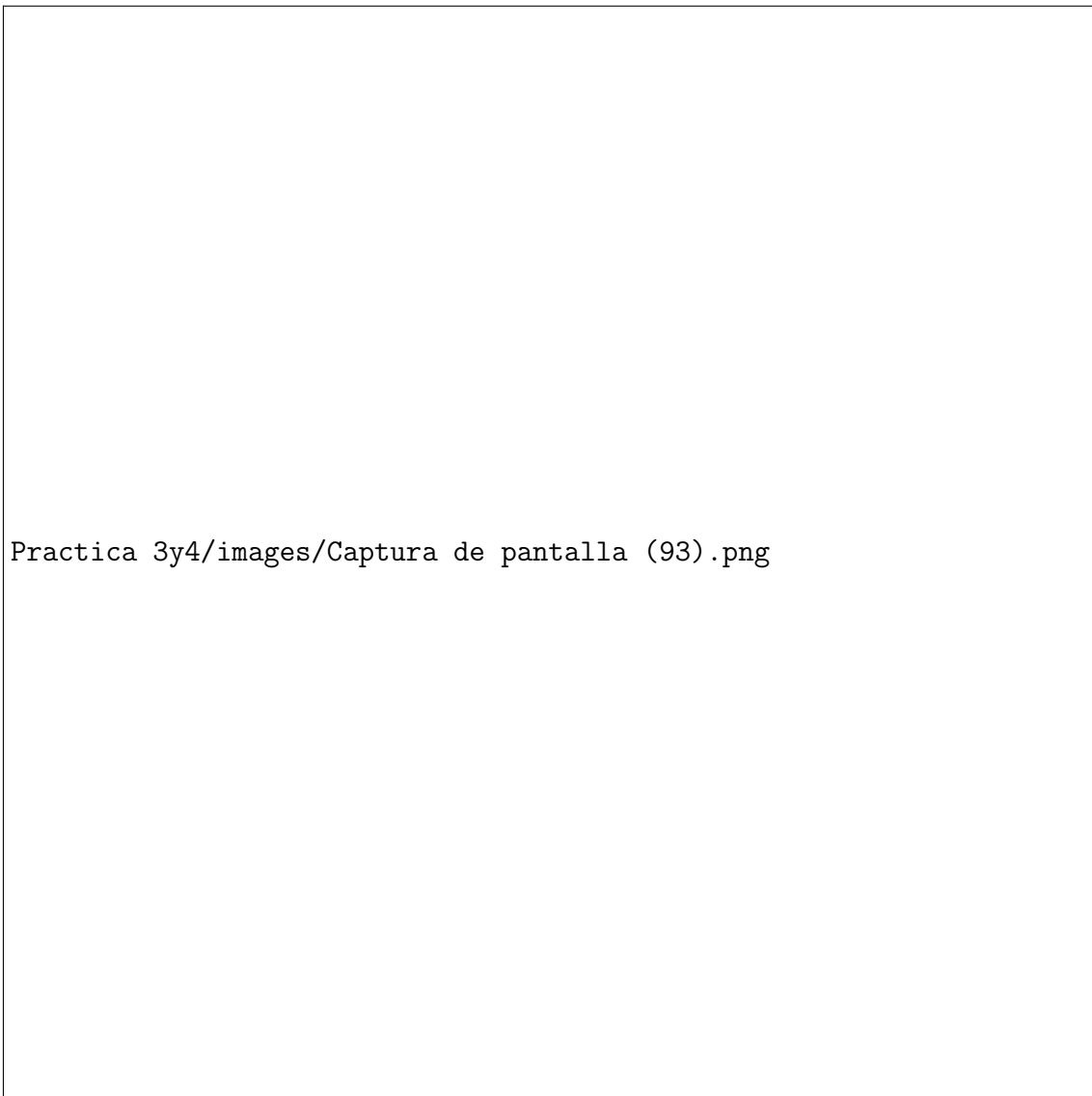


Figura 1.14: Imágenes del proxy statement



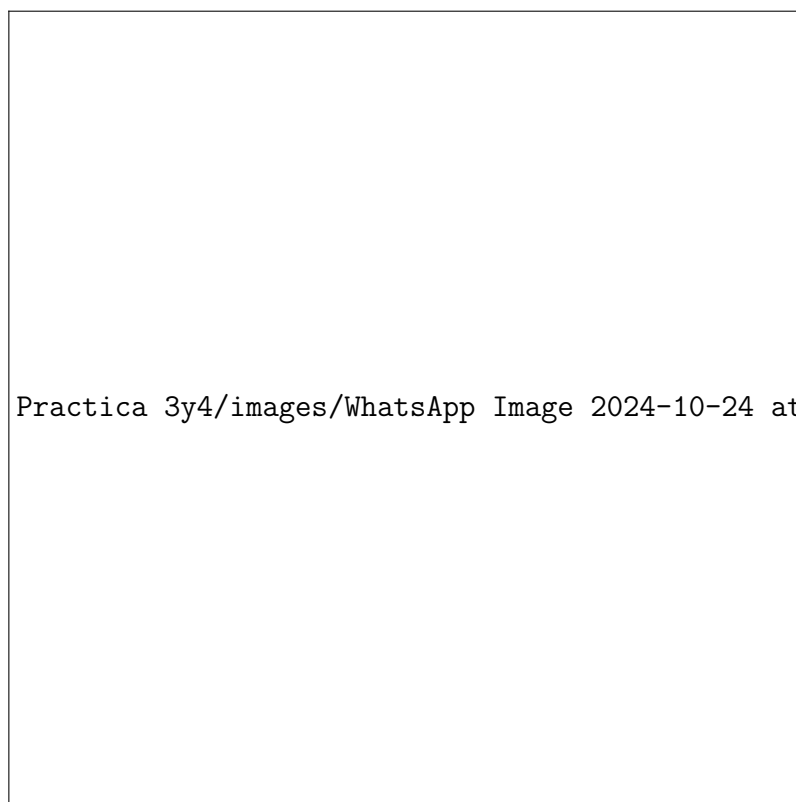
Practica 3y4/images/Screenshot 2024-10-24 at 10.28.43.png

Figura 1.15: Búsqueda en Shodan.



Practica 3y4/images/Captura de pantalla (93).png

Figura 1.16: Búsqueda del Institute for Nuclear Research de Moscú con el puerto Telnet a la escucha



Practica 3y4/images/WhatsApp Image 2024-10-24 at 10.48.04.jpeg

Figura 1.17: Búsqueda de la organización con más servidores.

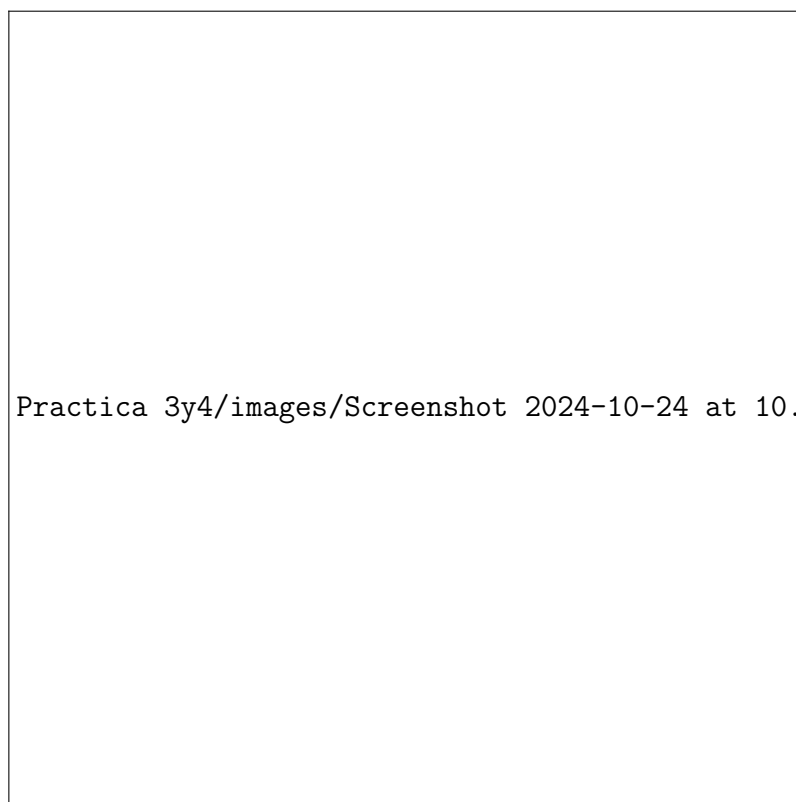
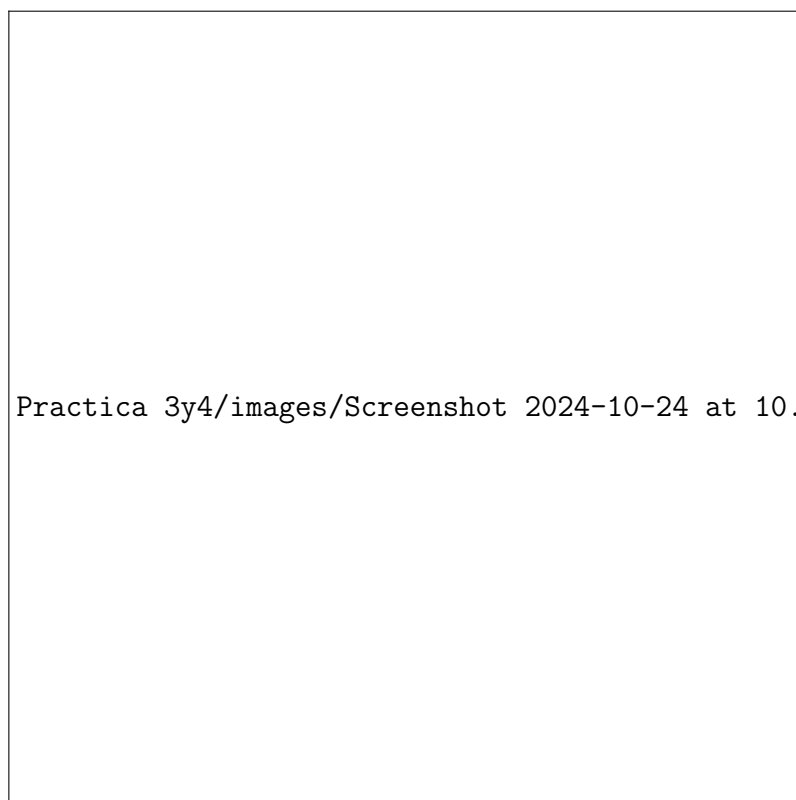


Figura 1.18: Búsqueda en Shodan I



Practica 3y4/images/Screenshot 2024-10-24 at 10.52.16.png

Figura 1.19: Búsqueda en Shodan II

Capítulo 2

Práctica 3.2: Recolección de información en fuentes abiertas II

2.1. Ejercicio 1

Usando *DNSDumpster* [?] haga un análisis de los subdominios de *cadiz.es*

- ¿Qué ISP aloja la mayoría de las webs?

El ISP que más se usa es el denominado **ACENS.AS**:

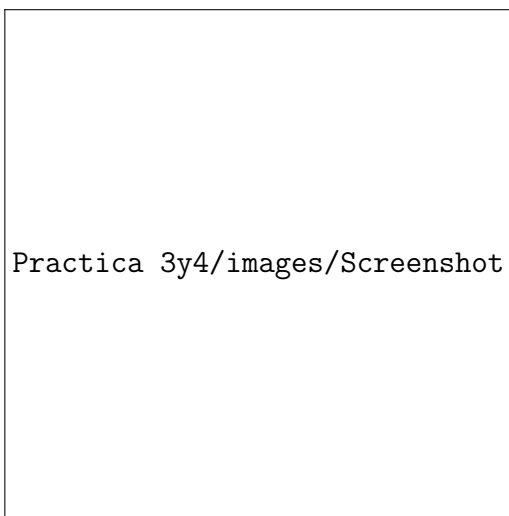


Figura 2.1: Interfaz principal de DNS-Dumpster

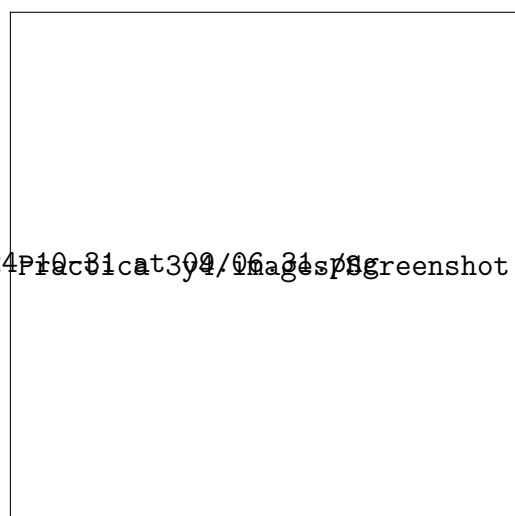


Figura 2.2: Resultado de búsqueda de los subdominios cadiz.es

2.2. Ejercicio 2

Usando la herramienta *DNS Trails* [?] liste los subdominios de *diariodecadiz.es* y responda a las siguientes preguntas:

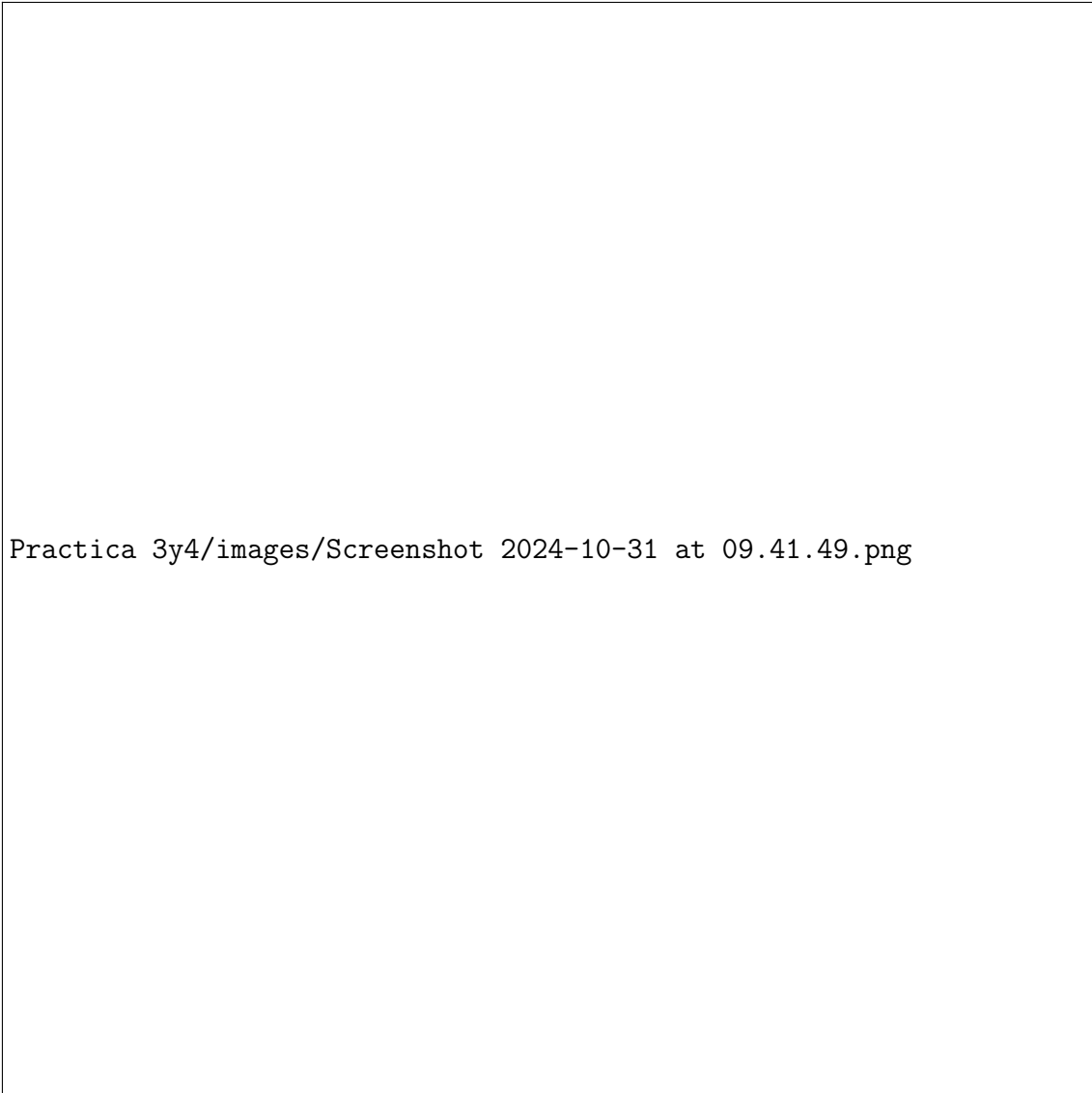


Figura 2.3: Interfaz principal

- ¿Cuántos subdominios encontramos?
Encontramos 29 subdominios, como podemos ver en las figuras:



Figura 2.4: Resultado de búsqueda del dominio.

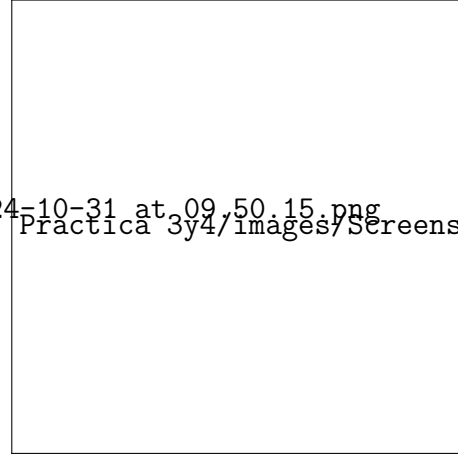


Figura 2.5: Algunos subdominios

- *¿Quién provee el hosting a la página principal?*
Como podemos ver en la Figura 2.6, el dominio de la página principal `diariodecadiz.es` es **Amazon**.

- ¿Qué subdominio es una redirección a un panel de login?
Finalmente, en la *Figura 2.8* podemos ver que el dominio `https://panelcontrolhosting.com/` contiene lo siguiente:

2.3. Ejercicio 3

Haciendo uso de Whois Lookup, conteste a las siguientes preguntas:

- *¿Qué información podemos obtener sobre el dominio cadizturismo.com?*

Podemos obtener bastante información como; la ip, el id de IANA, la ubicación, los cambios (hosting), etc.

- *¿Quién es el registrador de cadiz.com?*

El registrador es *BRANDON GRAY INTERNET SERVICES*, que operaba como *NameJuice.com*, era un operador de registro de nombres de dominio acreditado por ICANN con sede en Markham, Ontario.

2.4. Ejercicio 4

Haciendo uso de la información encontrada a través de la extensión Wappalyzer, conteste a las siguientes preguntas:

- *¿Qué versión de Apache se usa en directorio.uca.es?*
La dirección dada usa Apache Tomcat y Apache HTTP Server 2.4.37.
- *¿Qué versión de PHP se usa en formulagades.com?*
Usa la versión de PHP 8.1.18.
- *¿Qué proxy está usando https://esingenieria.uca.es/?*
Está usando Nginx.

2.5. Ejercicio 5

-

2.6. Ejercicio 6

■

2.7. Ejercicio 7

■

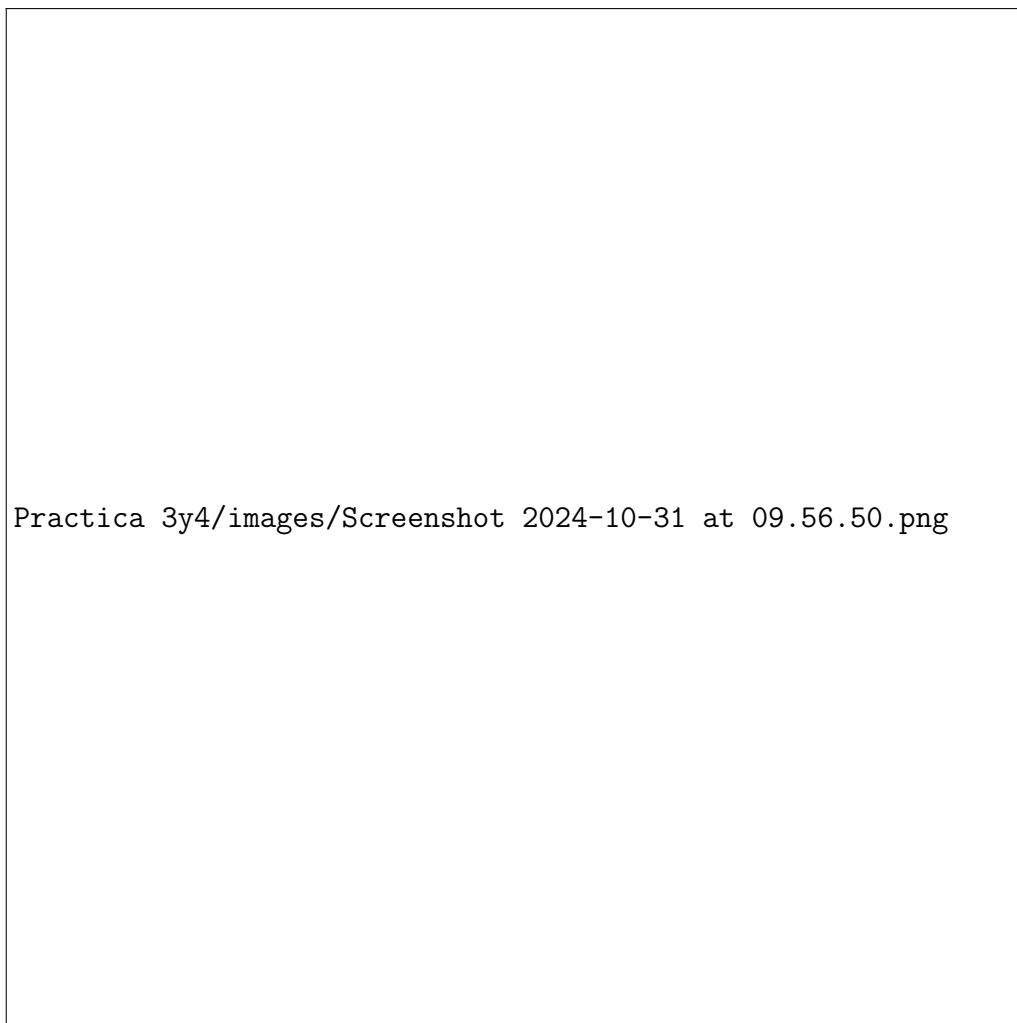
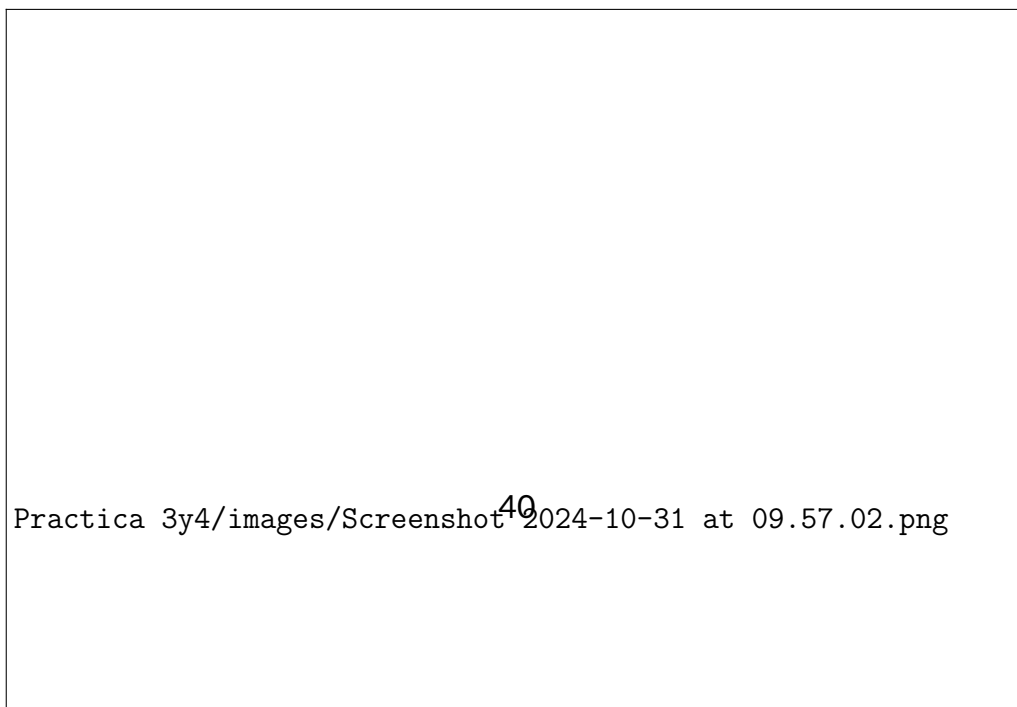


Figura 2.6: Encontramos el subdominio del panel de login



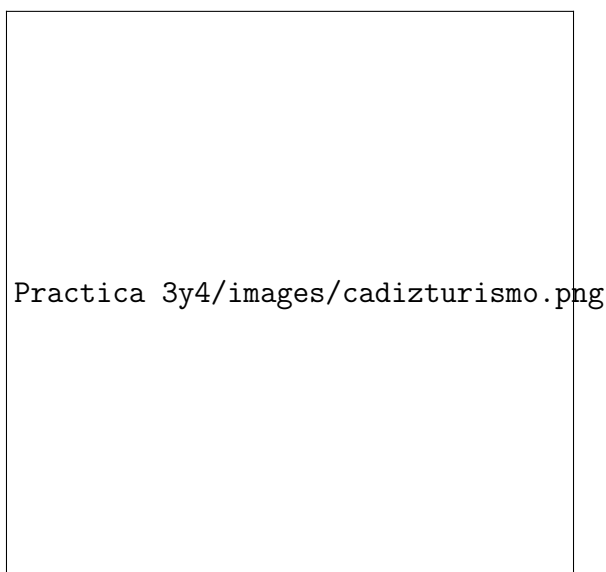


Figura 2.8: Uso de Whois Lookup para cadizturismo.com

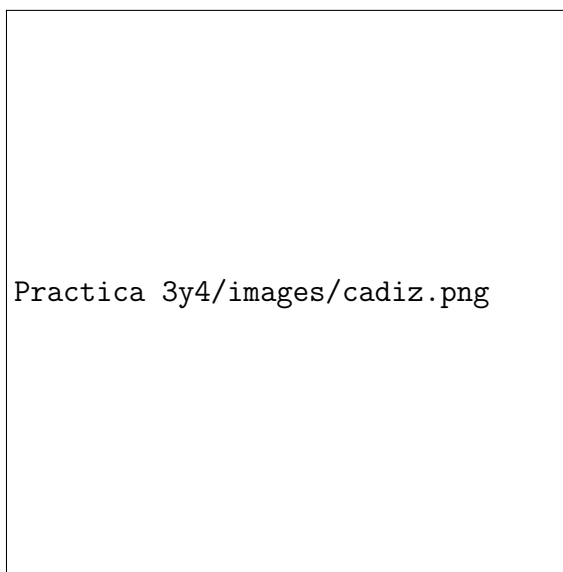
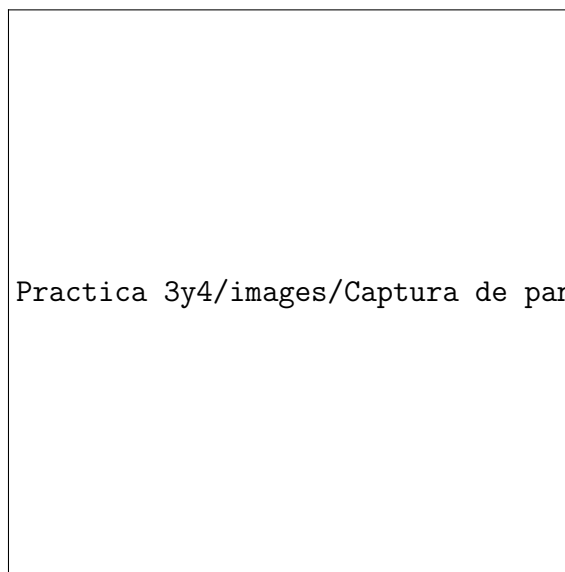


Figura 2.9: Uso de Whois Lookup para cadiz.com



Practica 3y4/images/Captura de pantalla 2024-10-31 112257.png

Figura 2.10: Ejemplo de uso de Wappalyzer

Capítulo 3

Práctica 4: Escaneo y enumeración de activos

3.1. Ejercicio 1

Ejecute la siguiente orden: `tcpping www.diariodecadiz.com`

- Describa la salida que ha obtenido.
- ¿En qué se diferencia de un ping tradicional?

Vemos que tcpping realiza conexiones TCP mientras que ping hace uso del protocolo ICMP.

Ahora seleccione una dirección IP de su red local, puede ser un ordenador portátil, un teléfono móvil, o cualquier otro que tenga a mano.

- ¿Qué ocurre si hacemos tcpping a esa dirección? Justifique su respuesta.

Vemos que al ser un dispositivo que está en local y no una página web la latencia es mucho menor así como el alcance de red, además vemos que los firewalls de los dispositivos locales no son tan restrictivos que los de una web.

- ¿Qué información útil le proporcionaría tcpping desde el punto de vista de la seguridad?

Desde una perspectiva de la seguridad, este comando puede proporcionarnos información valiosa como la detección de servicios activos, verificación

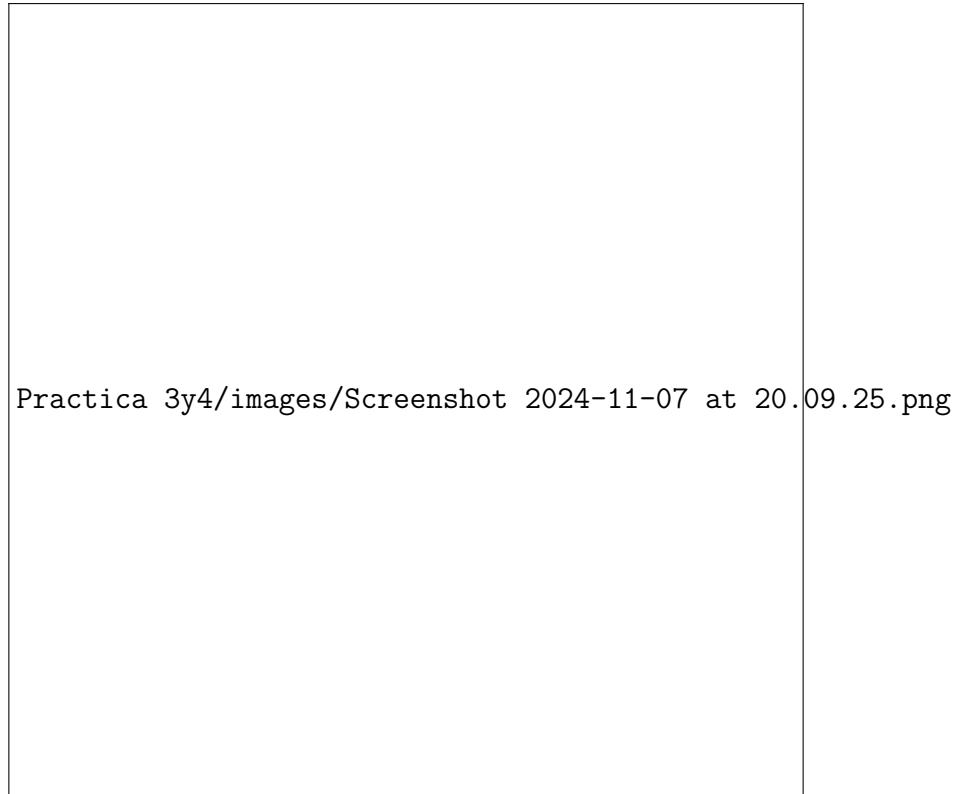


Figura 3.1: Uso con una página web

de configuración de algún firewall, la latencia y el rendimiento de la red, entre otros.

3.2. Ejercicio 2

Accedemos a la siguiente máquina de TryHackme [?]

- Acceda a la documentación de Nmap [?]. Describa la sintaxis completa con las opciones del comando `nmap`.

```
nmap [<Scan Type>...] [<Options>] {<target specification>}
```

- Realice un escaneo en modo *half-scan* de la máquina objetivo.

Un escaneo denominado *half-scan* es aquel donde no se completa el saludo de 3 vías, por tanto, para poder realizarlo haremos uso de la opción `-sS`,

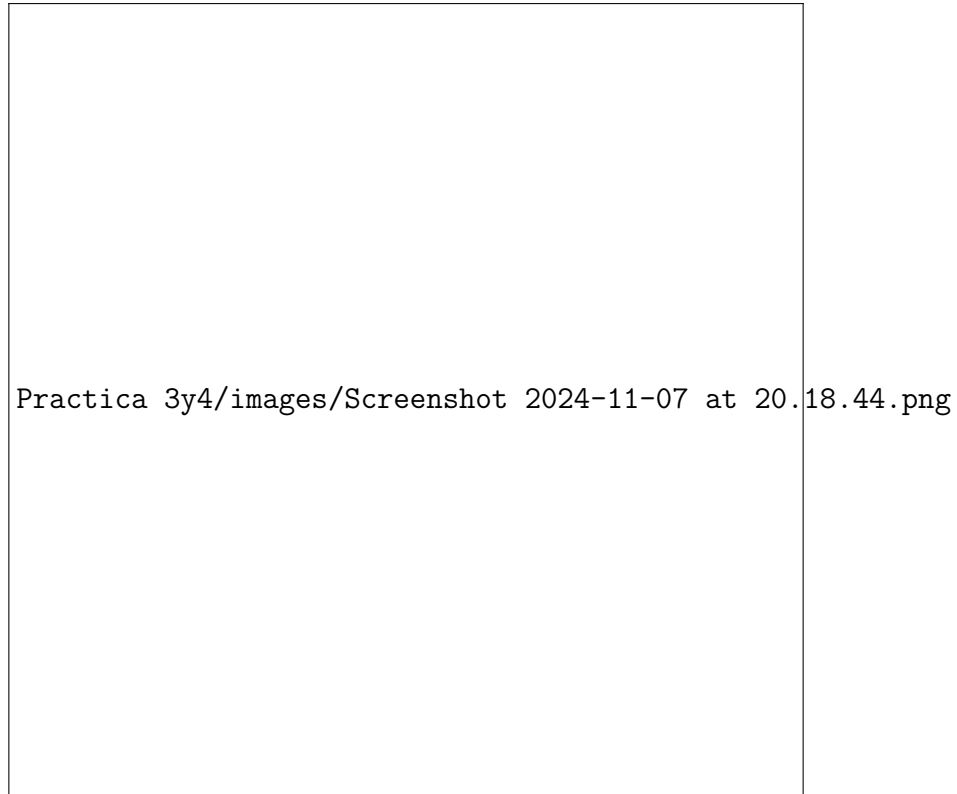


Figura 3.2: Uso con un dispositivo en local

además con `-p-` especificamos todo el rango de puertos abiertos. Todo esto lo podemos ver en <https://nmap.org/book/synscan.html>

Ahora, lo ponemos en práctica frente a la IP de la máquina víctima dada por la plataforma:

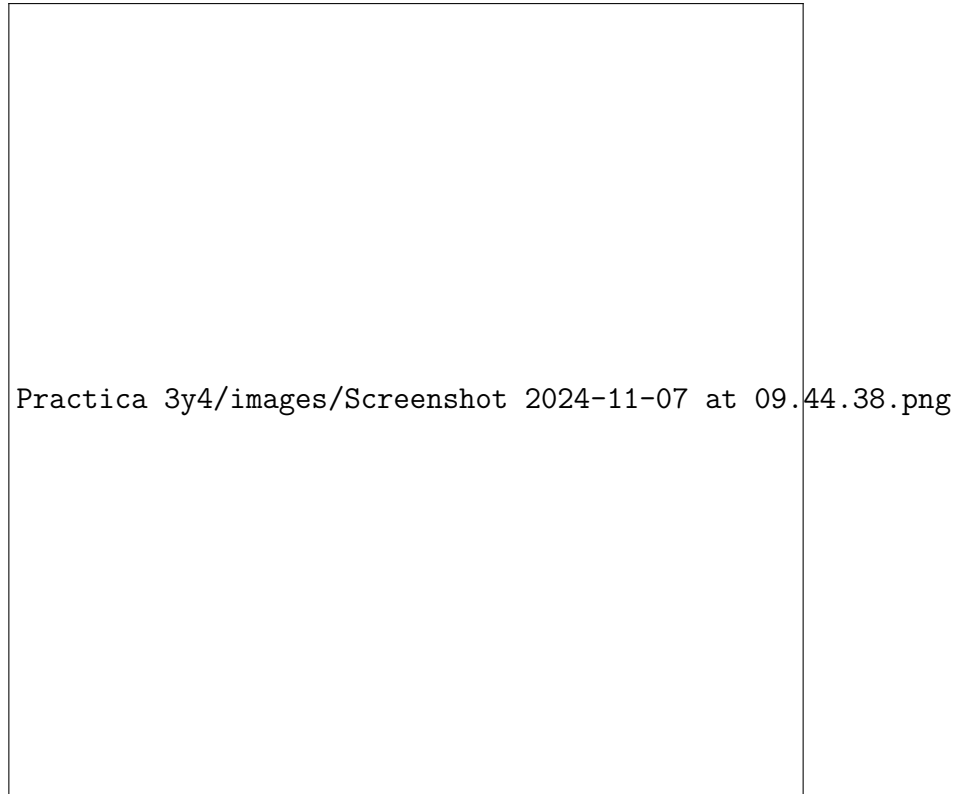
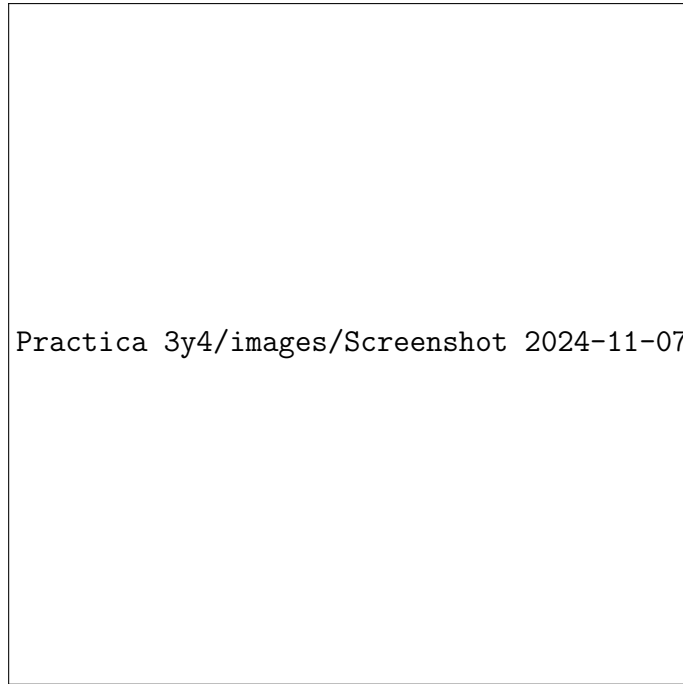


Figura 3.3: Búsqueda del tipo escaneo

- *Realice un escaneo tipo connect que permita detectar el sistema operativo de la máquina objetivo.*

Ahora, volvemos a buscar en la misma web el nuevo escaneo. En este caso el parámetro será `-sT`, donde realiza una conexión *TCP* con el servidor. A diferencia de la opción anterior, es decir `-sS`, el escaneo si realiza el saludo de 3 vías del protocolo *TCP*.

Lo ponemos en práctica:



Practica 3y4/images/Screenshot 2024-11-07 at 09.46.03.png

Figura 3.4: Resultado del half-scan de Nmap

- *Realice un escaneo en modo half-scan que permita detectar el sistema operativo, la versión de los servicios y la obtención de banners de la máquina objetivo.*

Para poder realizar este tipo de ataque, vamos a hacer uso de las opciones `-sS` para un ataque de tipo *half-scan*, el parámetro `--script` donde le especificamos que queremos los *banners* y la opción `-sV` para obtener la versión (esto, al igual que los escaneos anteriores lo busqué en la web de Nmap):

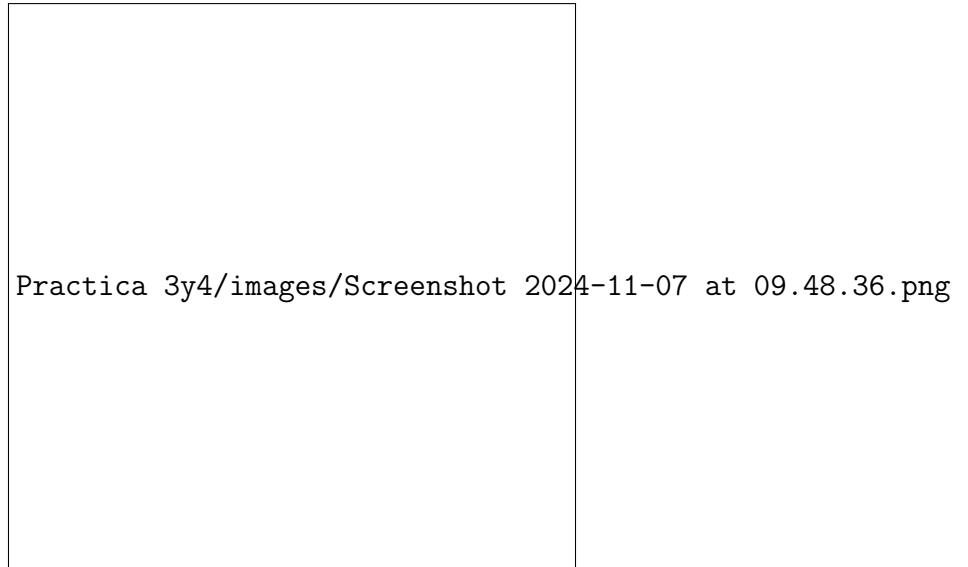


Figura 3.5: Búsqueda del escaneo

3.3. Ejercicio 3

Describe y explique los resultados obtenidos tras ejecutar el comando nmap en Kali Linux junto con las opciones necesarias para realizar:

- *Un escaneo en modo half-scan del servidor scanme.nmap.org.*
- *Un escaneo tipo connect que permita detectar el sistema operativo del servidor scanme.nmap.org.*

Obtenemos los puertos abiertos y su servicio.

En este caso no se puede obtener el sistema operativo con certeza pero nos da una aproximación. De igual manera que en caso anterior, obtenemos los puertos abiertos y sus servicios.

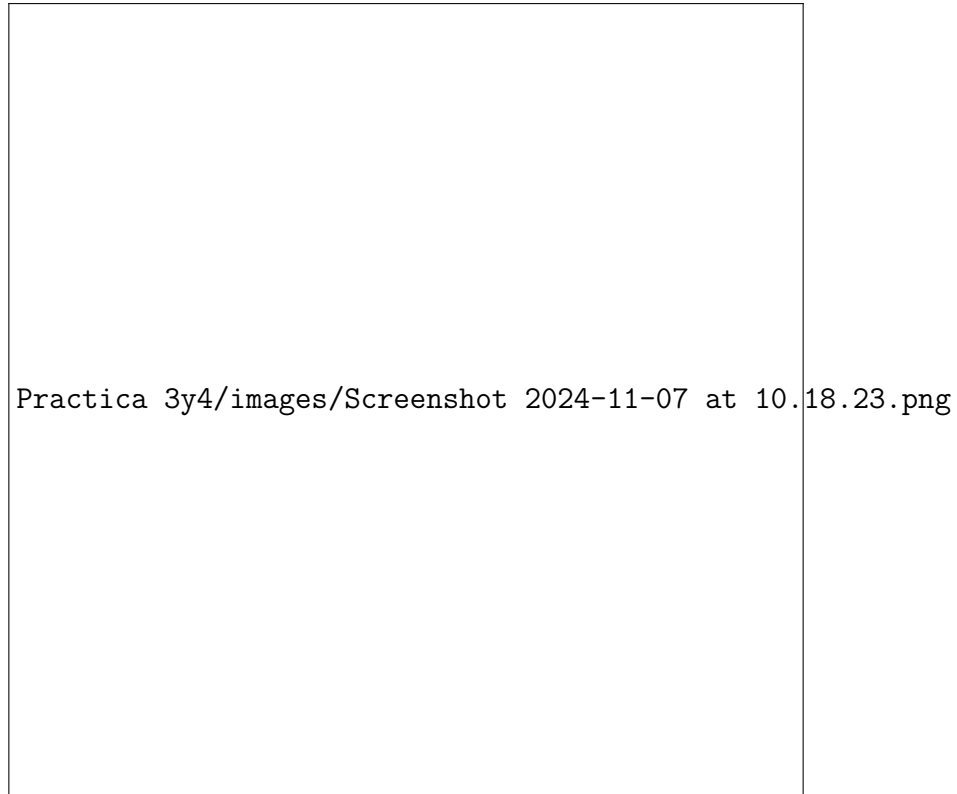


Figura 3.6: Resultado del escaneo connect.

- *Un escaneo en modo half-scan que permita detectar el sistema operativo, la versión de los servicios y la obtención de banners del servidor scanme.nmap.org.*

obtenemos lo mismo que en la primera consulta, pero ahora tenemos la versión de algunos puertos y de igual forma, se muestran, algunos banners.

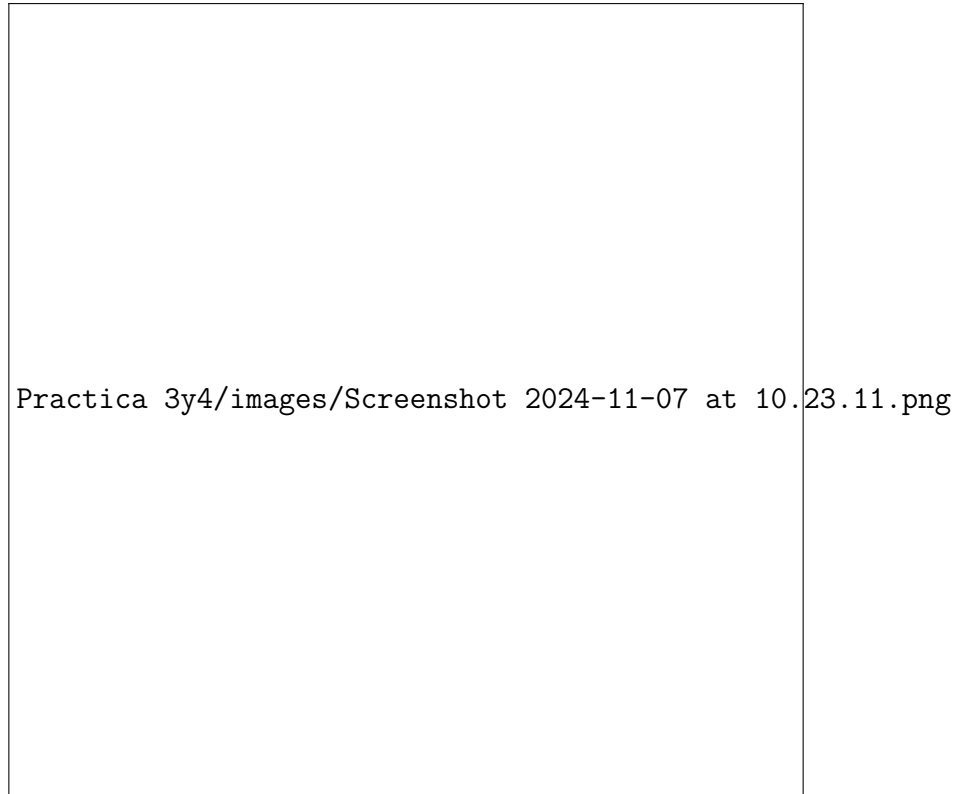


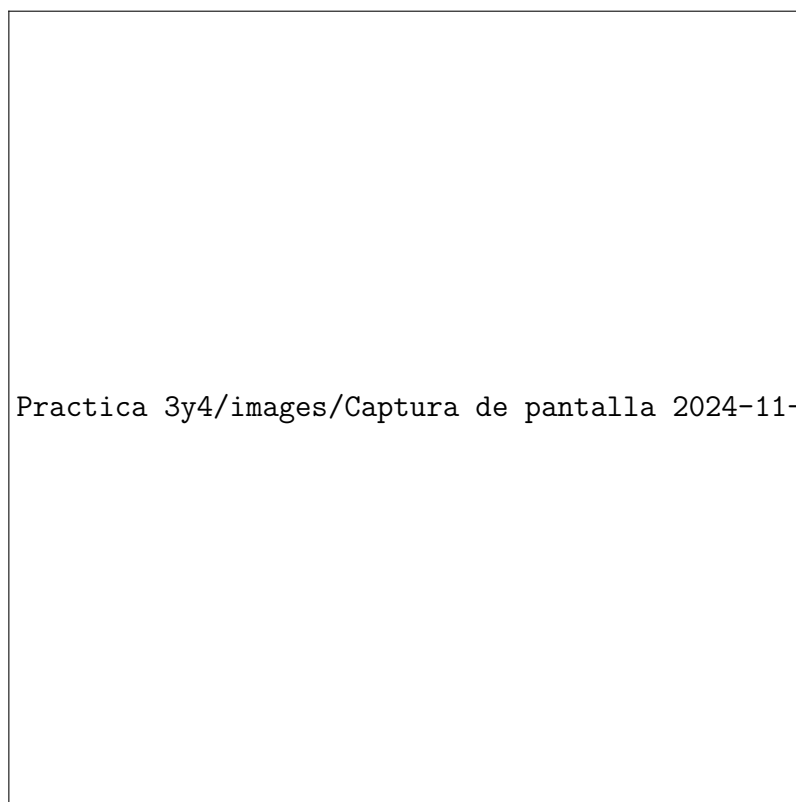
Figura 3.7: Escaneo que nos devuelve las versiones de los protocolos

3.4. Ejercicio 4

Una vez instalada la herramienta *Furious* en Kali Linux, realice un escáner de tipo connect a la web oficial de la universidad:
uca.es

Una vez realizado, responda a las siguientes preguntas:

- ¿Cuál es la dirección del host?
La dirección del host es 150.214.80.210
- ¿Tiene algún puerto abierto? En caso afirmativo, ¿cuál?
Sí, tiene abierto el puerto 80 ligado al servicio http
- ¿Qué comando ha utilizado para realizar un escaneo de este tipo?
Hemos utilizado el comando **sudo ./main -s connect uca.es**



Practica 3y4/images/Captura de pantalla 2024-11-07 164902.png

Figura 3.8: Escaneo half-open

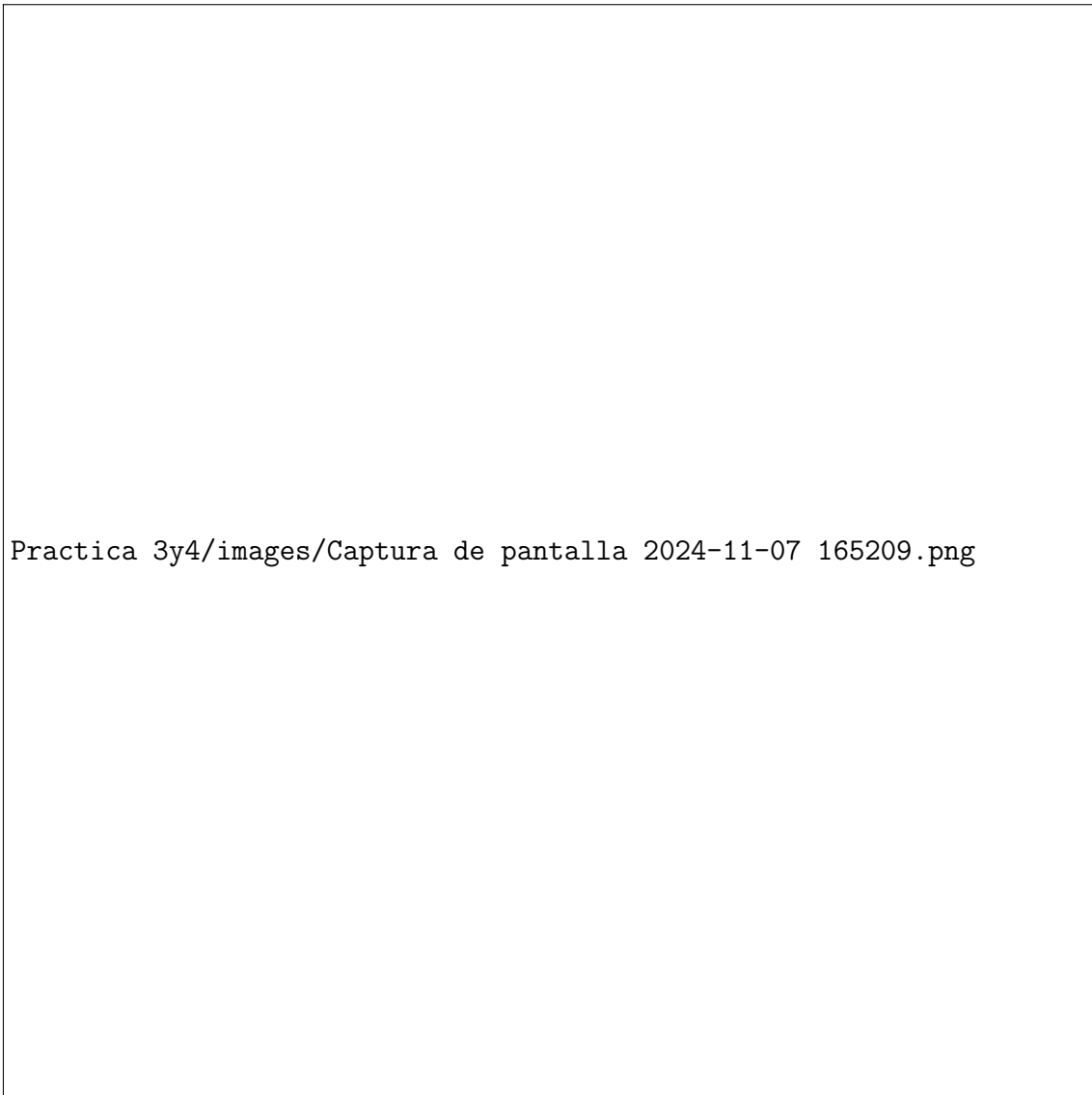


Figura 3.9: Escaneo Connect() con SO

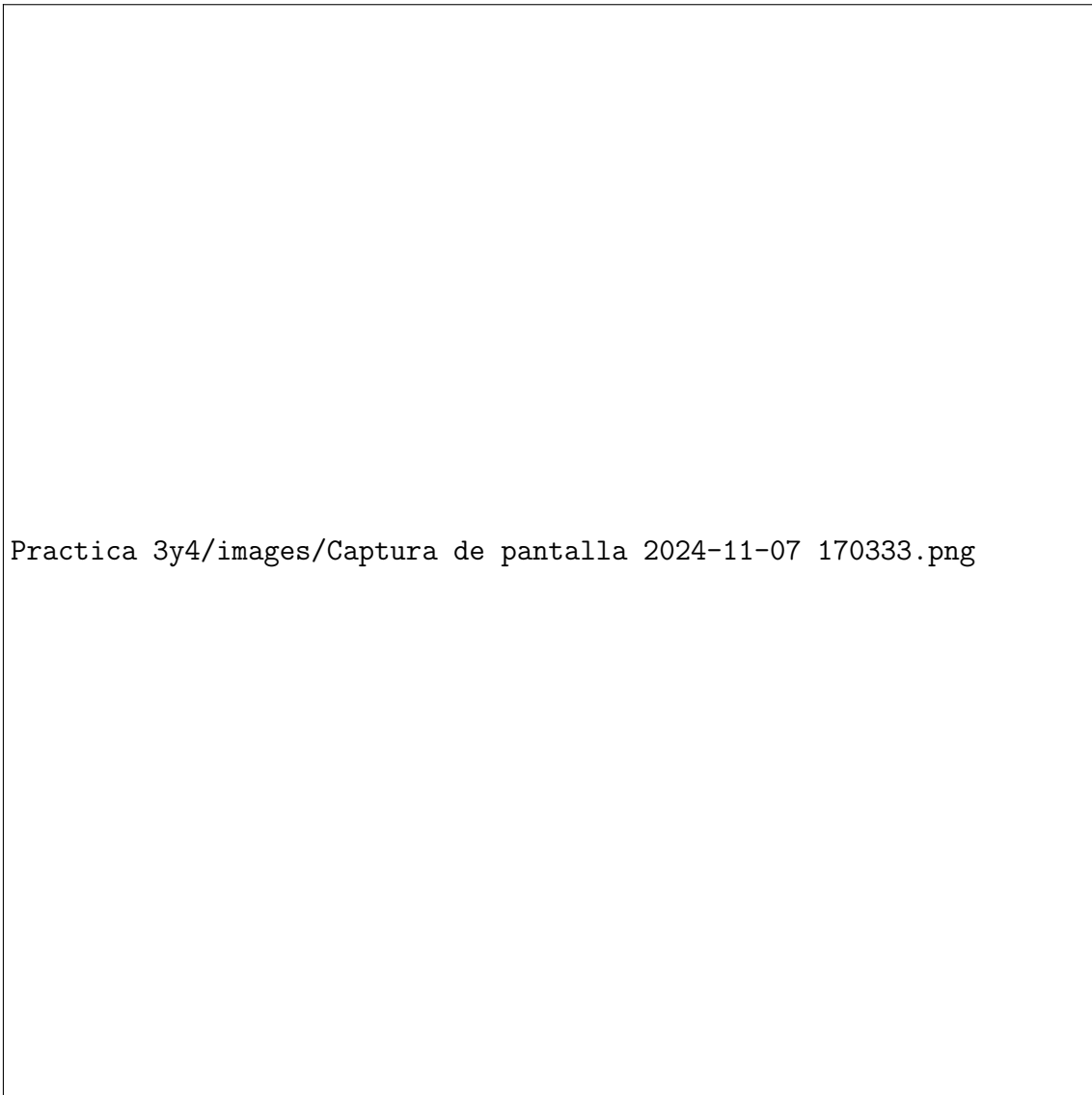
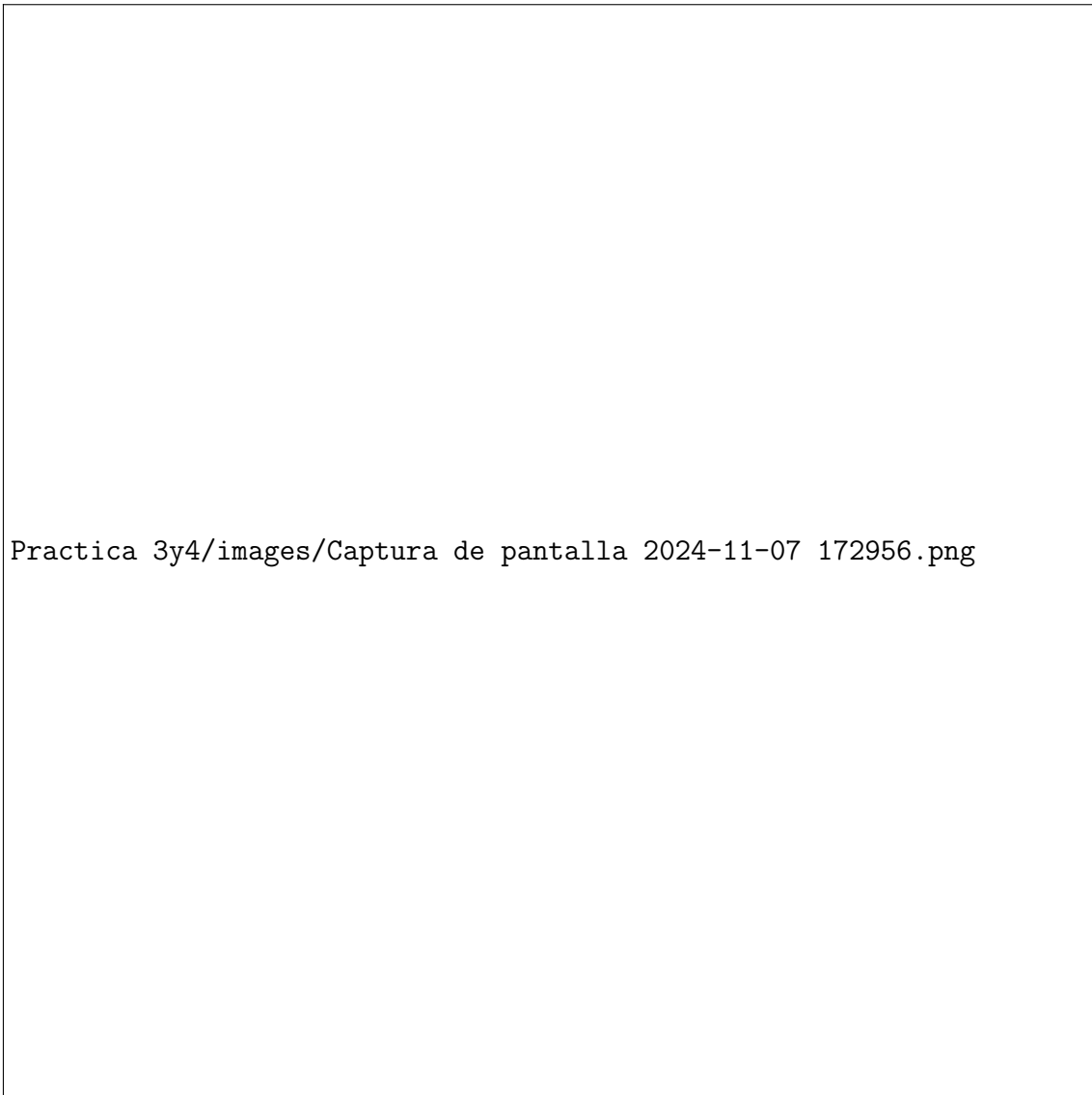


Figura 3.10: Escaneo half-open con SO, versión de servicios y banners



Practica 3y4/images/Captura de pantalla 2024-11-07 172956.png

Figura 3.11: Uso de Furious para escaneo de uca.es