Miguel Casares Martínez

Anonimización del entorno de trabajo

Índice

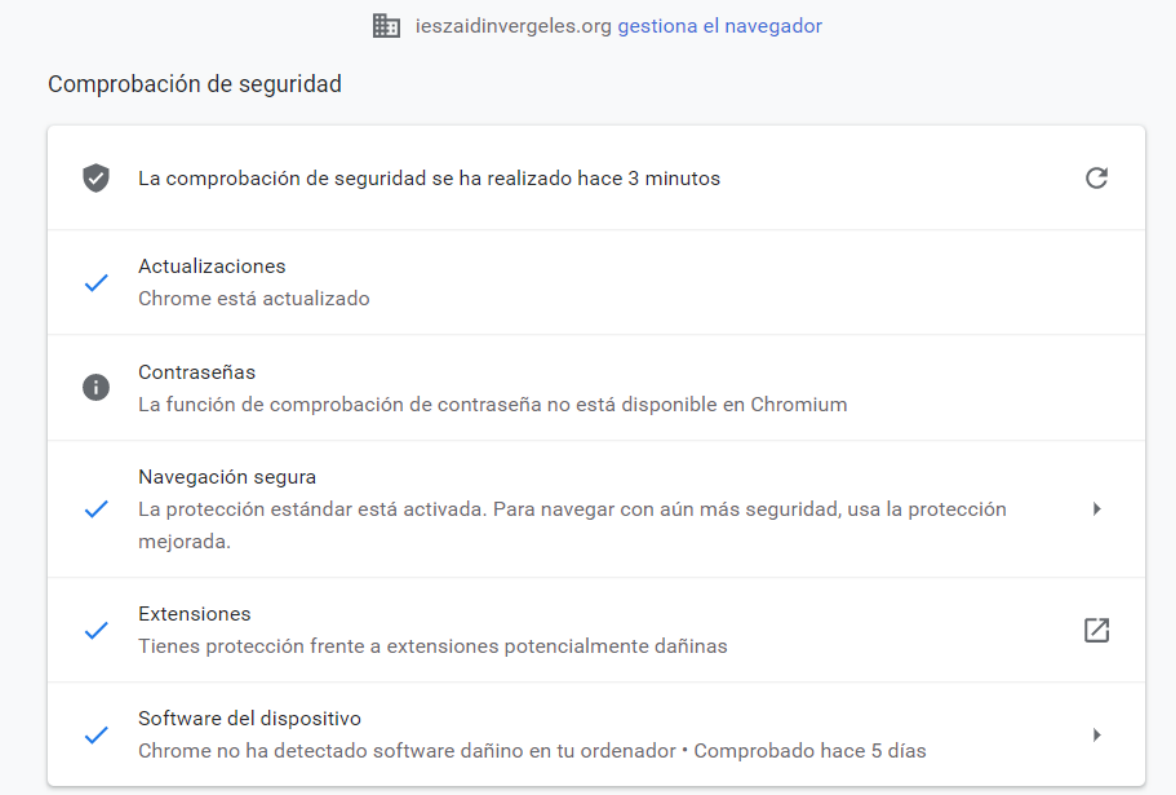
Ejercicio 1: Valoración de privacidad de información y conexiones.

Descripción:

Antes de comenzar la recogida de información y de anonimizar nuestro entorno de trabajo, es necesario valorar el estado actual de nuestra privacidad, tanto en los equipos informáticos que usamos como en nuestra información personal que puede encontrarse públicamente. Se utilizarán las utilidades y herramientas vistas en la unidad (test de privacidad del navegador, egosurfing, CONAN Mobile), y cualquier otra herramienta que descubras y pueda ser de utilidad.

a) Estado de anonimización de nuestros equipos.

Analizando el PC, vamos a la configuración del navegador, en mi caso normalmente uso Chrome:
En la comprobación de seguridad, aparentemente vemos que está todo correcto.



Ahora nos vamos a una página especializada para analizar nuestro navegador.

En mi caso he elegido la página de la EFF (Electronic Frontier Foundation), una organización sin ánimo de lucro dedicada a preservar los derechos digitales.

Link: https://coveryourtracks.eff.org/

Allí nos da bastante información, entre otra, que el navegador no está bloqueando los anuncios y nos pueden rastrear el tráfico, además el navegador tiene una huella digital única.

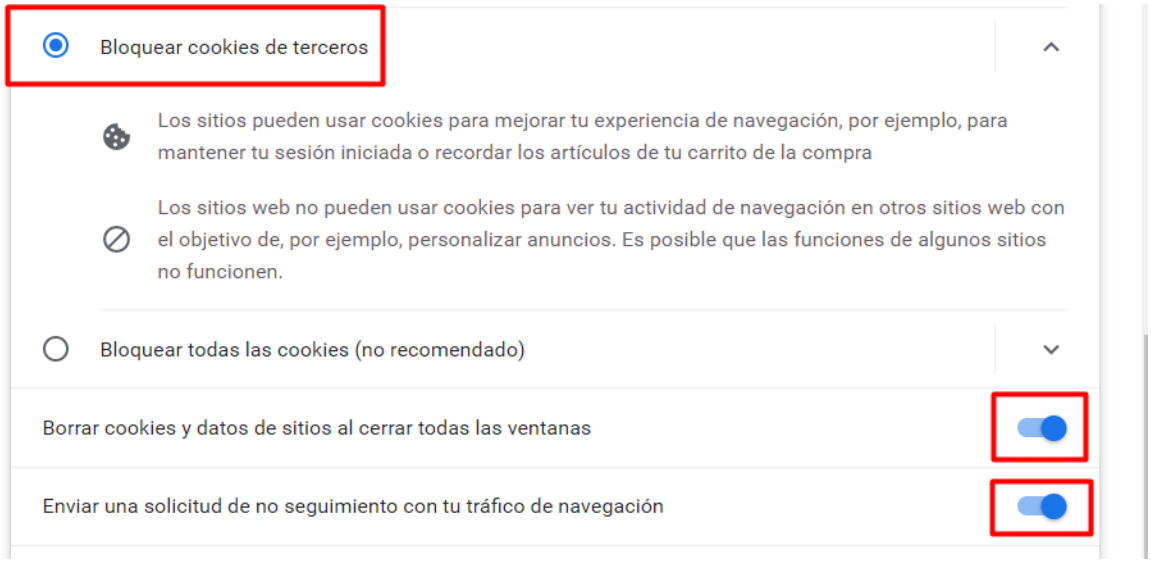
Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

Our tests indicate that you are not protected against tracking on the Web.

IS YOUR BROWSER:

Blocking tracking ads?	No
Blocking invisible trackers?	No
Protecting you from fingerprinting?	Your browser has a unique fingerprint

Nos vamos al navegador y en la configuración activamos más opciones de seguridad, como no seguir mi tráfico de navegación:

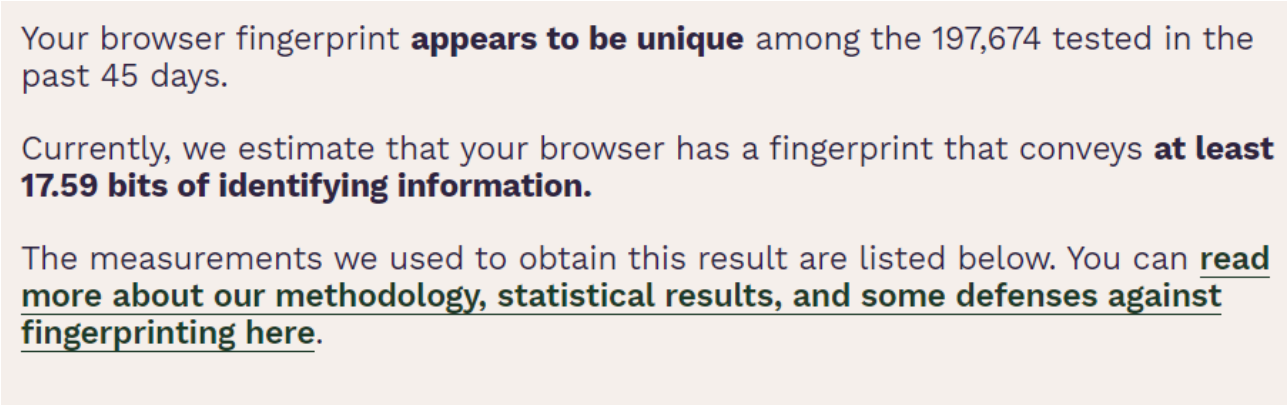


Volvemos a hacer el test y vemos resultados:

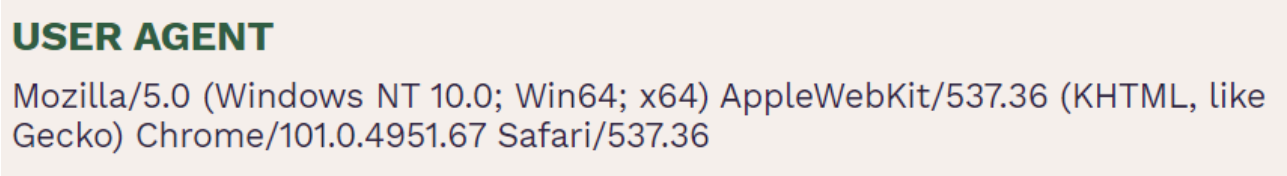
Vemos que hemos ganado algo de seguridad, aunque no es completa, ya que nada más usando Chrome ya tenemos un cierto riesgo.

Analizando más los resultados vemos que aparece mucha información, me sorprendió bastante la página.

Vemos cuantos bits de información puede ser usada del navegador:



En el reporte entran apartados como la zona horaria, el agente que usa el navegador hasta el tipo de fuentes:



Por ejemplo en este apartado vemos que se pueden ver los ajustes de la ventana de Chrome y que los trackers podrían usar para sustituirla y engañarnos:

SCREEN SIZE AND COLOR DEPTH

1536x864x24

WHAT IS THIS?

The dimensions of your current browser window, and its color depth.

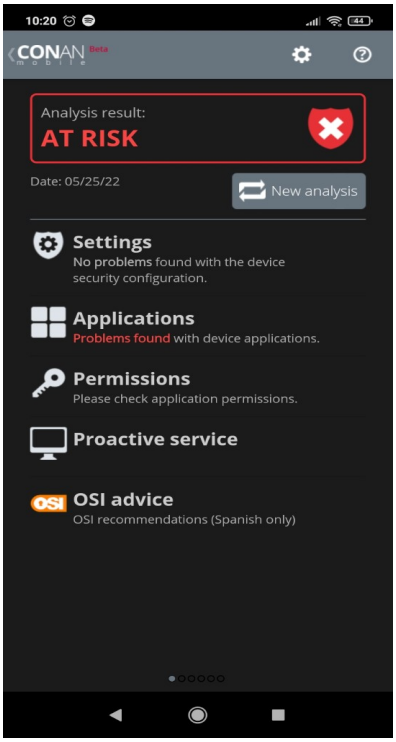
HOW IS THIS USED IN YOUR FINGERPRINT?

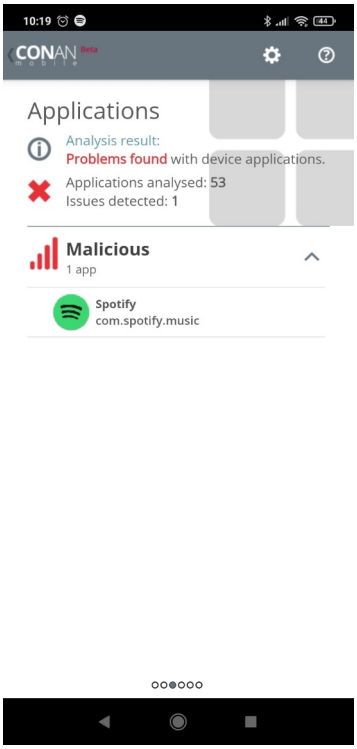
While this metric can supplement other information, it's often too 'brittle' to be usable by trackers because users can easily change their browser window dimensions.

Bits of identifying information: ***4.29***
One in x **browsers have this value:** ***19.54***

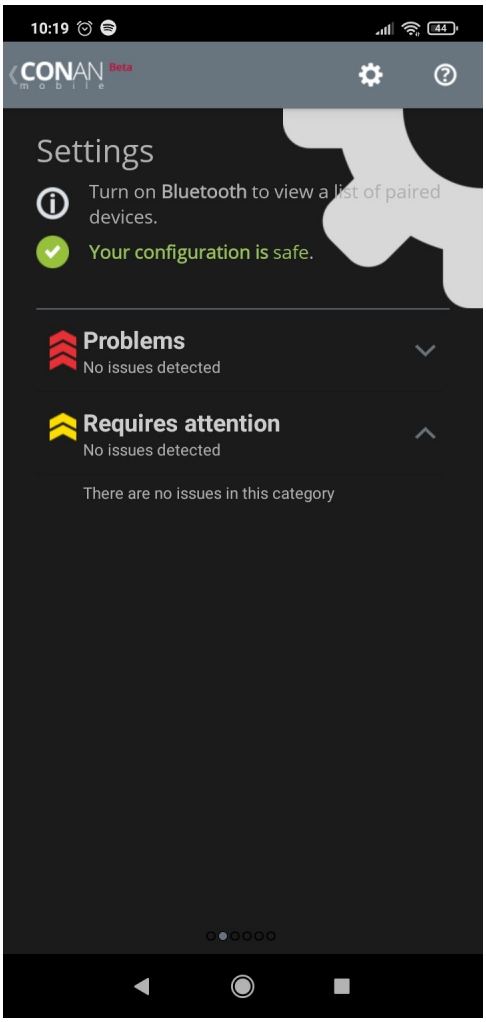
Analizando nuestro dispositivo móvil, instalamos la app Conan mobile, del Incibe:

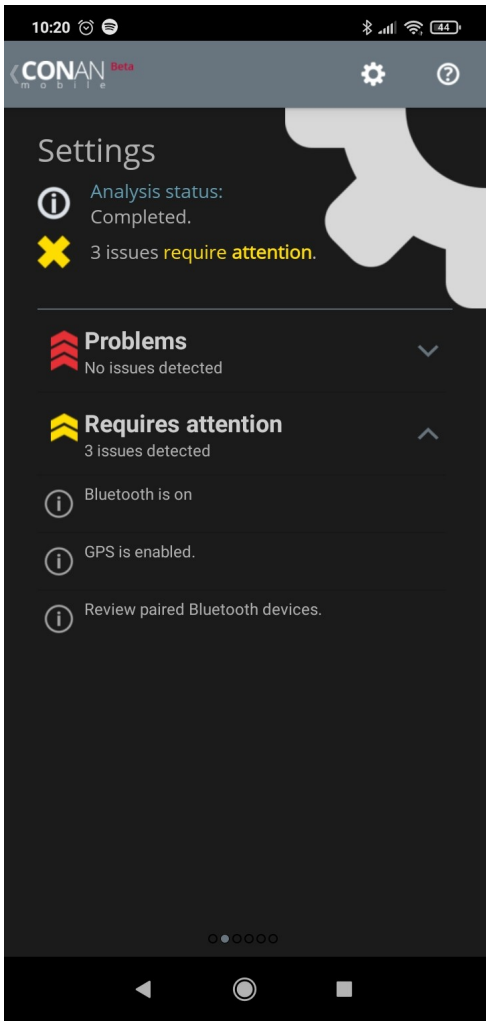
Vemos que nos aparece un riesgo de aplicaciones, una apk de Spotify. Obviamente sabemos que no es recomendable y que tiene agujeros de seguridad, lo demás parece correcto.





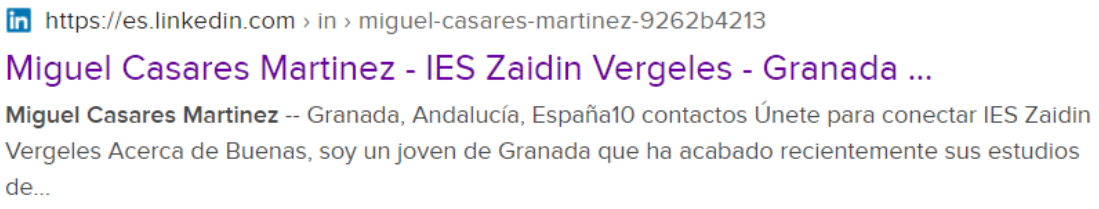
En el apartado settings nos aparecerá riesgo si activamos el bluethoot o el GPS, yo por mi parte los suelo tener desactivados, luego hago una prueba activandolos.

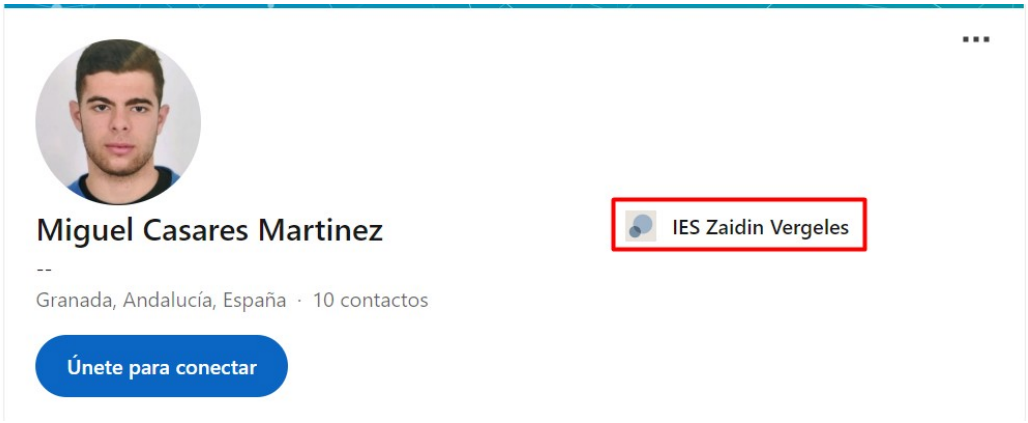


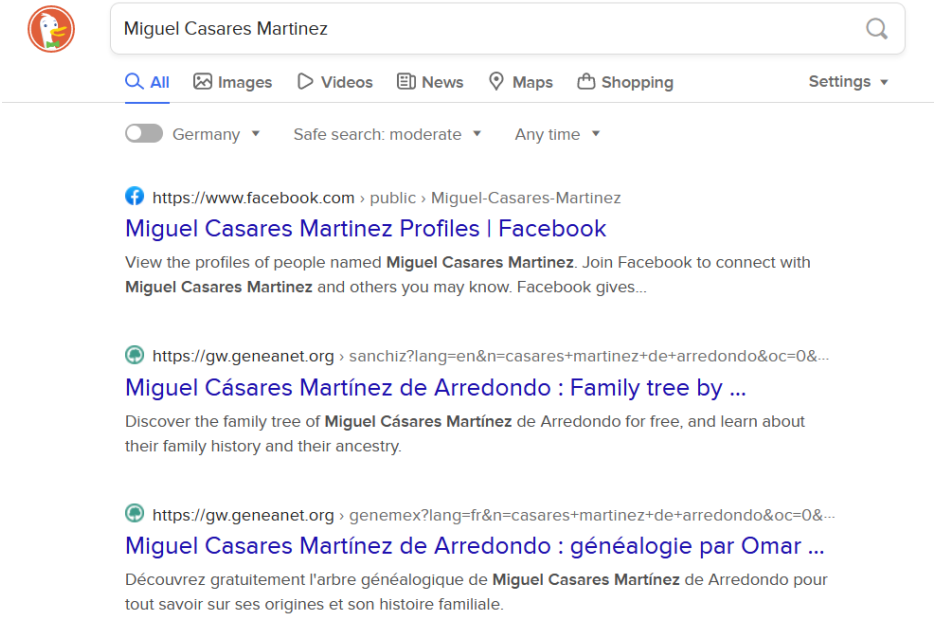


b) Estado de privacidad de nuestra información pública.

Procedemos a buscar nuestro nombre con DuckDuckGo. Observamos que salen tanto nuestro facebook (no lo uso), como nuestro Linkedin. En nuestro propio Linkedin podemos sacar información como donde hemos estudiado y que soy de Granada, además de la foto de perfil. El resto de links información de gente que se llama igual.

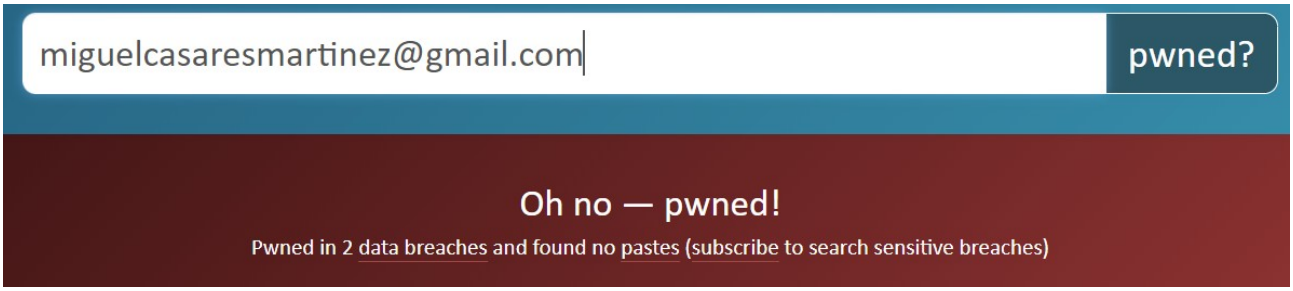






Por lo demás no encontramos nada en el Facebook ya que es una cuenta creada sin fotos ni información. Pero vemos que ya hemos conseguido datos valiosos, es decir tenemos datos expuestos en la red.

Después de esto analizamos nuestra dirección de correo en HaveIbeenPwned, para saber si en algún momento nuestros datos han sido filtrados:



Vemos que hemos sido expuestos a algunas brechas de seguridad, entre otras, esta de PhoneHouse en 2021:

Dependiendo del tipo de usuarios registrados, se filtró hasta en algunos casos fechas de nacimiento, números de teléfono o incluso direcciones físicas. Afectó a mas de 3 millones de personas. Ahí tenemos otra vía por la que nos podrían encontrar datos personales.

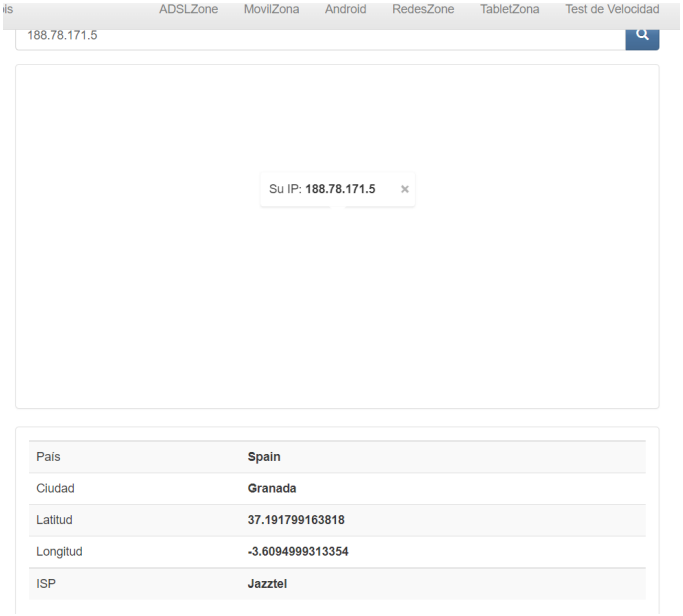
Ejercicio 2: Conexiones privadas mediante Tor.

Descripción:

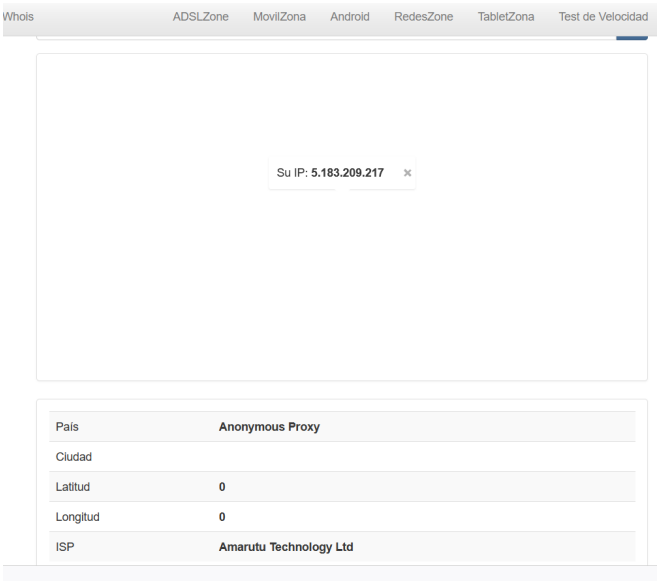
En este segundo ejercicio vas a realizar diferentes pruebas de conexión empleando la red anónima Tor.

a) Navegación outproxy e inproxy con Tor Browser. Compara la IP pública que tendrías utilizando un navegador habitual con respecto a usar Tor Browser, ¿hay diferencias? Conéctate a una web de tu elección e indica cuál es el circuito de nodos Tor que se está empleando. Conéctate al dominio .onion de DuckDuckGo y busca 3 dominios que puedan ser interesantes y estén relacionados con el módulo de Hacking ético.

Esta es mi IP Geolocalizada con Google Chrome.



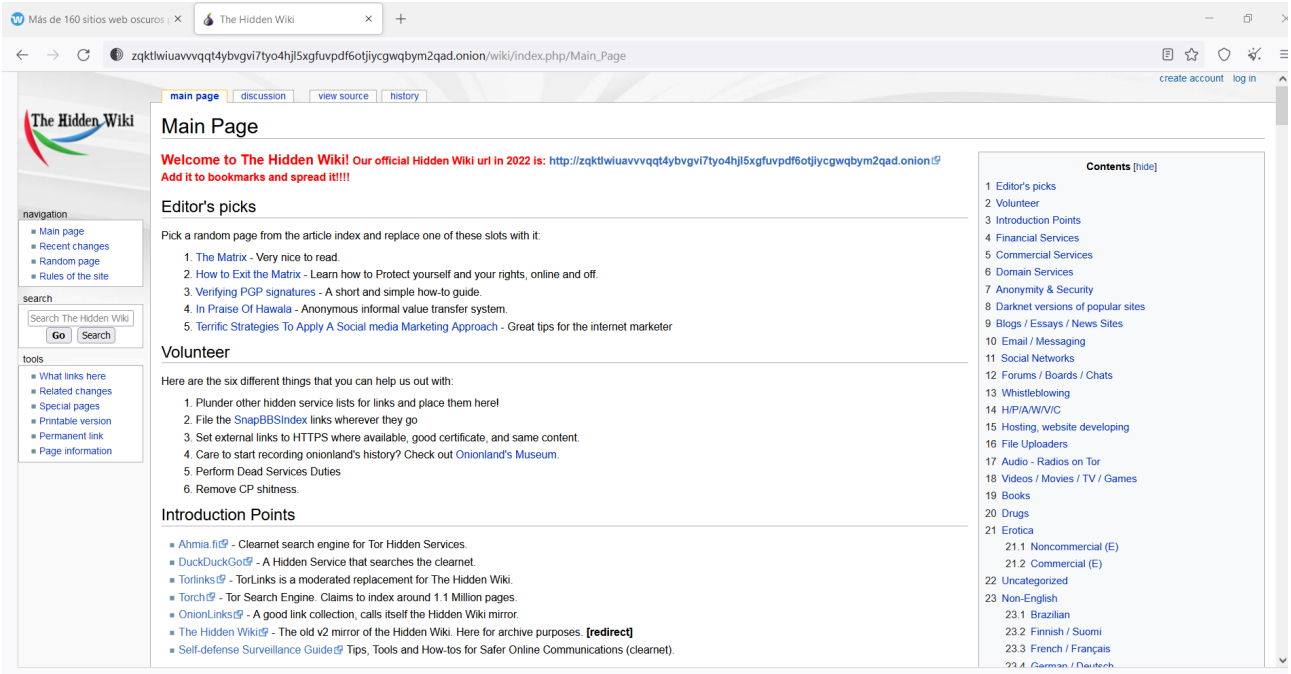
En cambio con Tor esta es mi IP



Como podemos ver tenemos mucha más información sobre nosotros si no usamos Tor.

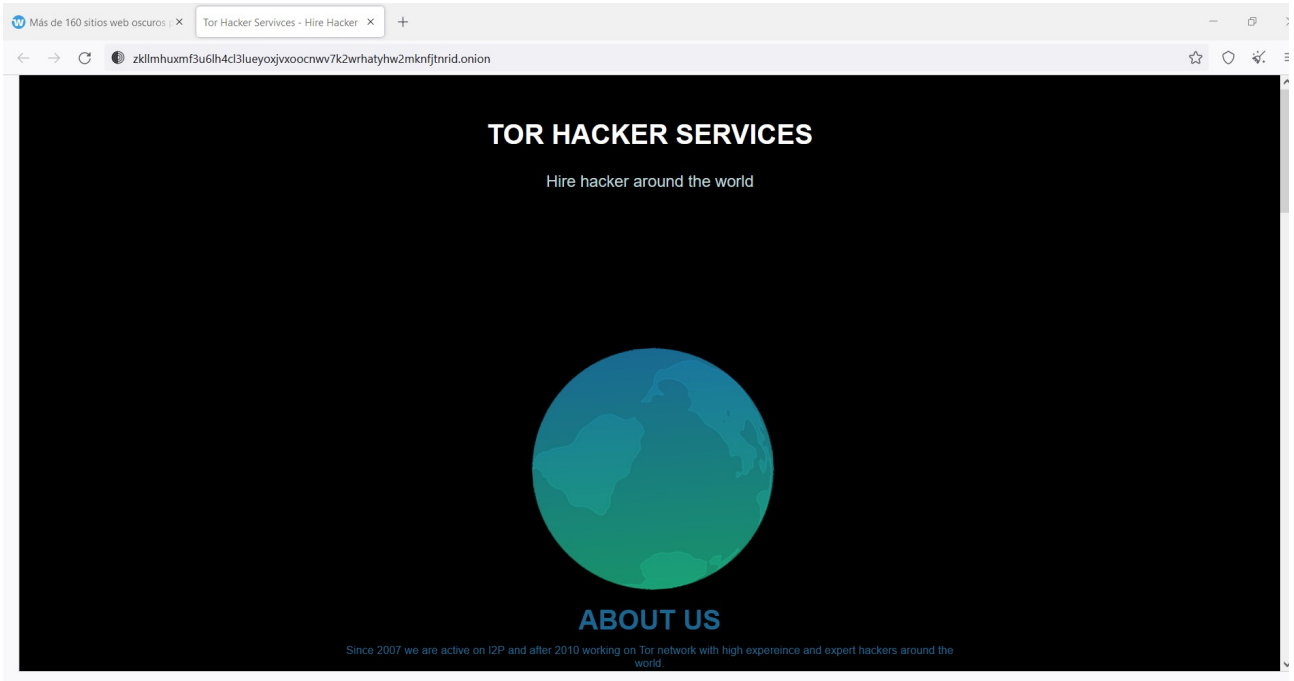
En una página "normal" de internet podemos encontrar páginas .onion que solo podremos entrar con Tor, yo he usado un artículo de un blog con una lista de estos enlaces. Dentro de esta he elegido estas páginas:

The Hidden Wiki, que es una página con mucha información para aquella gente que está empezando en la Dark Web.

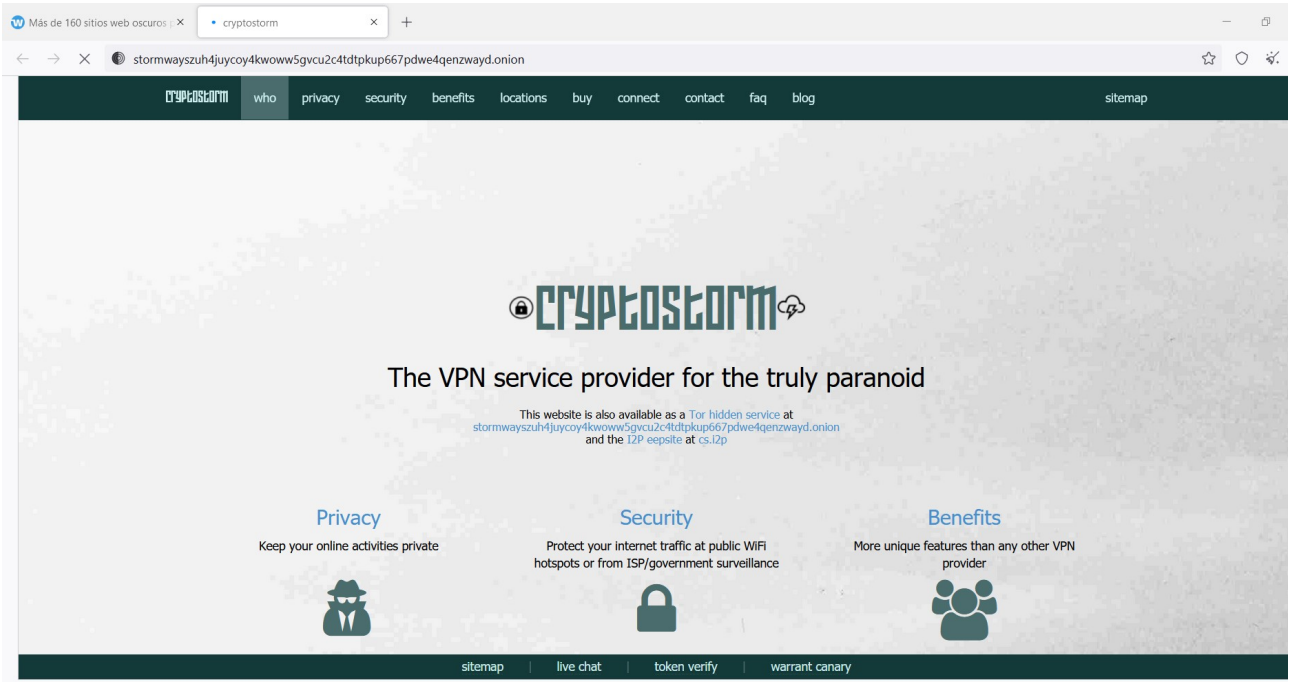


Top Hacker Services:

En esta página se pueden comprar con bitcoins diferentes servicios de hacking y espionaje.



Cryptostorm: Es una página que mejora la privacidad mediante el uso de VPN



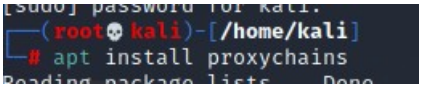
b) Uso de tor y proxychain desde la terminal. Explica cómo utilizar comandos desde la terminal para que utilicen la red Tor. Para ello deberás instalar y configurar tor y proxychains.

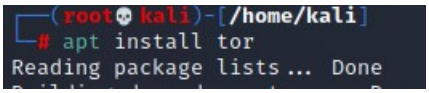
Existe la posibilidad de instalar Tor en linux y controlarlo desde la terminal.

Tor en esta terminal se inicia iniciando el procesostart-tor-browser, también podemos usar el buscador duck duck go cloandolo desde su repositorio de github git clone https://github.com/jarun/ddgr.git

Ahora nos vamos a nuestra máquina kali a comprobarlo:

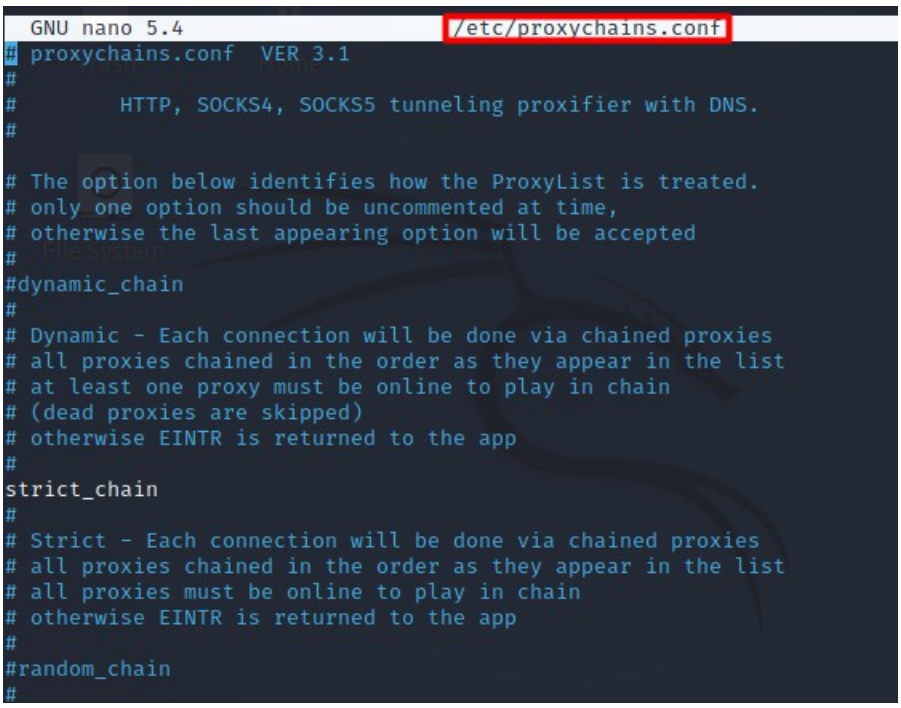
Primero de todo instalamos las proxychains y tor con apt:





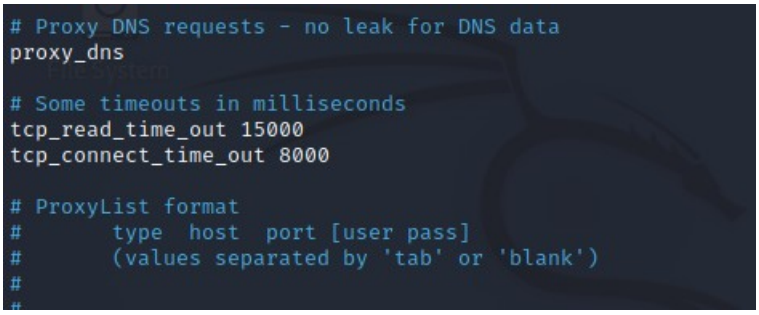
La herramienta proxychains nos permite tunelear nuestro tráfico a través de proxys http.

El fichero de configuración lo podemos encontrar en: /etc/proxychains.conf

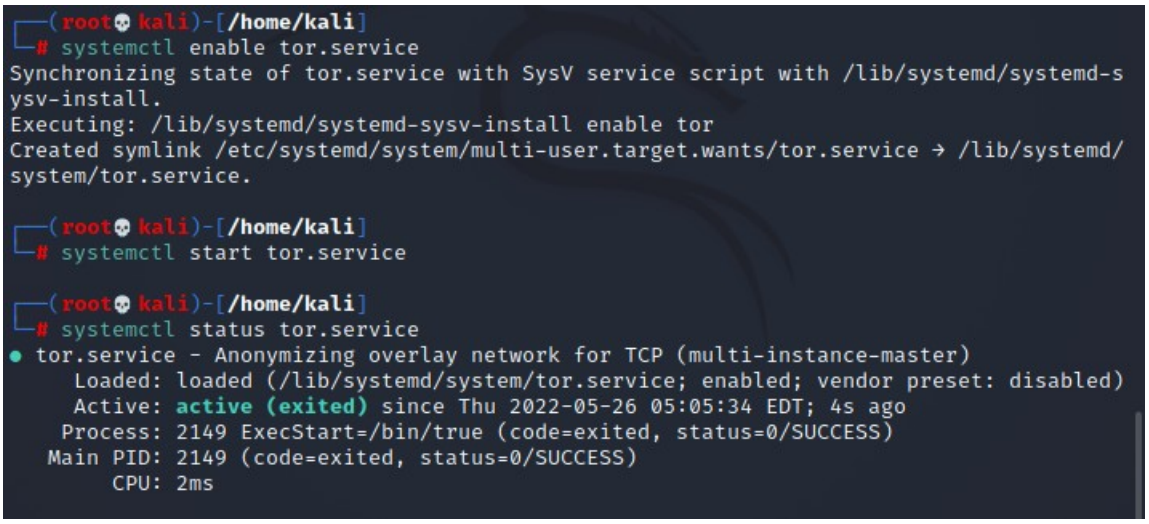


Aquí podemos elegir como queremos los canales, es decir si elige los proxys aleatoriamente o no.

También tenemos otras opciones, como el tiempo de conexión y lectura o el proxy dns:



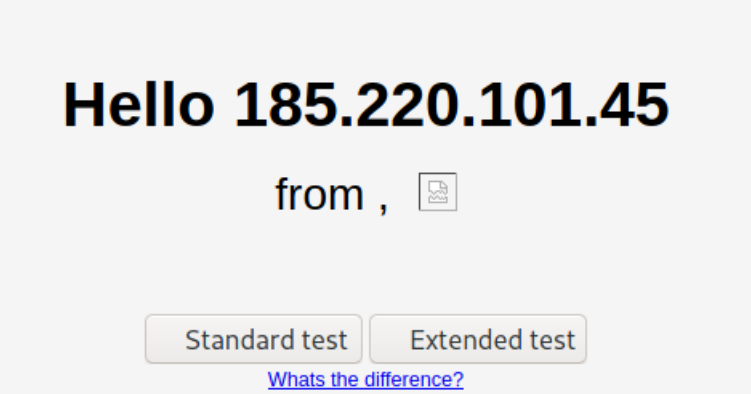
Una vez visto esto vamos a habilitar e iniciar el servicio Tor, lo hacemos con enable y start, luego comprobamos que está iniciado con status:



Ya estamos listos para usar las proxychains, ahora elegimos la página que nos conectamos, probamos con dnsleaktest, ya que nos dirá la localización y comprobaremos si está funcionando:

```
┌──(kali㉿kali)-[~]
└─$ proxychains firefox dnsleaktest.com
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  dnsleaktest.com:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  content-signature-2.cdn.mozilla.net:443 [proxychains] DLL init: proxychains-ng 4.14
  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  firefox.settings.services.mozilla.com:443 [proxychains] DLL init: proxychains-ng 4.14
  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  firefox.settings.services.mozilla.com:443 [proxychains] DLL init: proxychains-ng 4.14
  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  dnsleaktest.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  safebrowsing.googleapis.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  push.services.mozilla.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  r3.o.lencr.org:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ocsp.pki.goog:80  ...  OK
```

Se nos abre Firefox y carga la página, obviamente tardando más de lo habitual:



Ahora comprobamos con el test la localización y que funciona:

Vemos que la IP y el hostname son de Tor y que no es capaz de darnos una localización, por lo tanto ya estamos navegando con Tor:

Test complete

Query round	Progress...	Servers found
1	.....	1

IP	Hostname	ISP	Country
185.220.101.32	tor-exit-32.for-privacy.net.	Cia Triad Security LLC	

c) Uso de tor + VPN. Explica las diferencias entre el uso de proxys, vpsn, tor y proxychains y valora las ventajas y desventajas de cada uno y qué problemáticas podemos encontrar, ¿son 100% seguras y anónimas? A continuación añade el uso de una VPN como ProtonVPN junto a tor y proxychain.

Un servidor proxy es un intermediario entre el navegador e Internet. El navegador se conecta al proxy, que conecta el navegador a Internet. Entonces tu identidad en internet es el proxy y tu dirección IP está oculta.

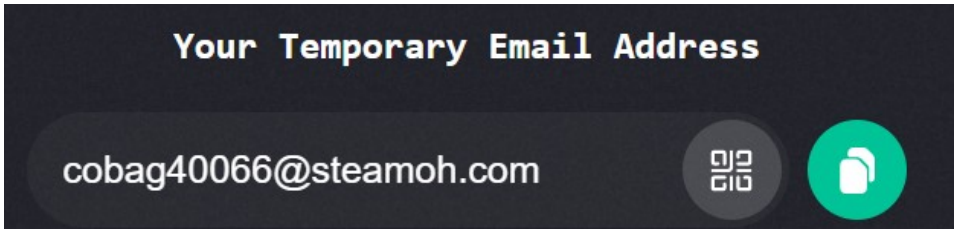
Una VPN es un servidor remoto que conecta al usuario a Internet, cifra todo el tráfico que accede tu dispositivo a través suya y además cubre el 100% del tráfico de internet.

Tor en cambio como ya sabemos es un protocolo que anonimiza el tráfico de Internet bajo numerosas capas de cifrado.

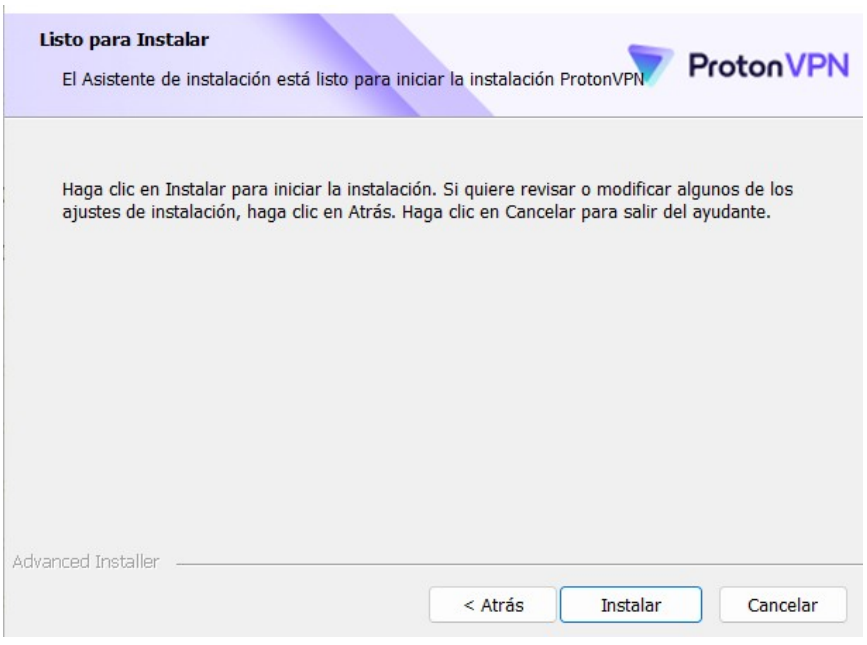
Los "problemas" al utilizar Tor y proxychain es que no te cifran todo lo que sale de tu dispositivo a diferencia de una VPN , por ejemplo con Tor serás anónimo al buscar en Tor Browser pero no si usas otro programa que se conecte a Internet. Además una VPN suele ser más rápida que el protocolo Tor y más segura. Eso sí para que sea totalmente privada tu búsqueda por navegador lo mejor es usar Tor. Tenemos que tener en cuenta que siempre podremos combinar los diferentes servicios.

Ahora vamos a añadir en la práctica la VPN en Windows:

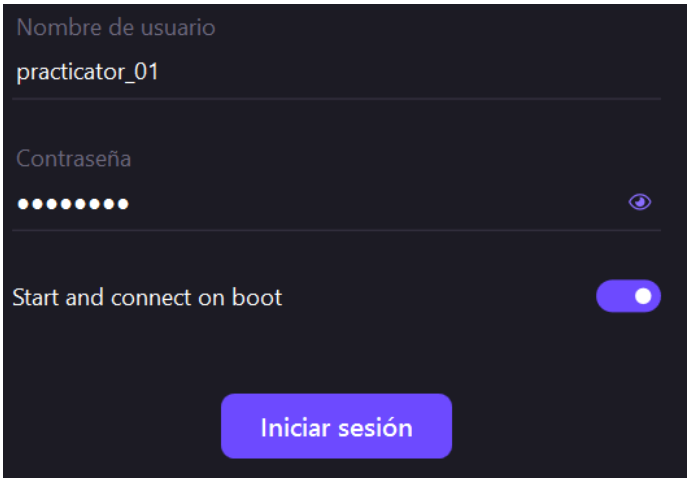
Nos vamos a la página web,primero creamos una cuenta, es recomendable crearla con un email temporal, por ejemplo en la página temp-mail.org



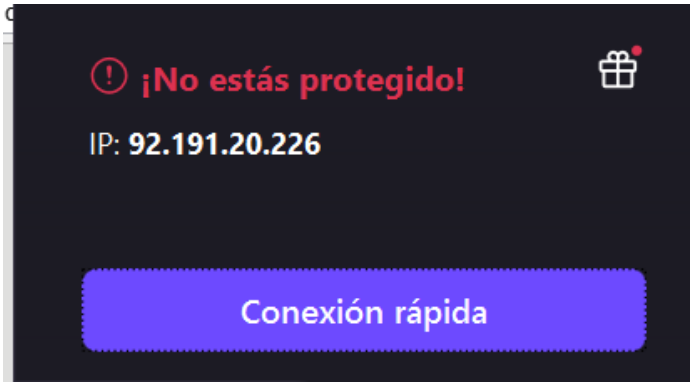
Ahora que tenemos la cuenta podemos instalar:

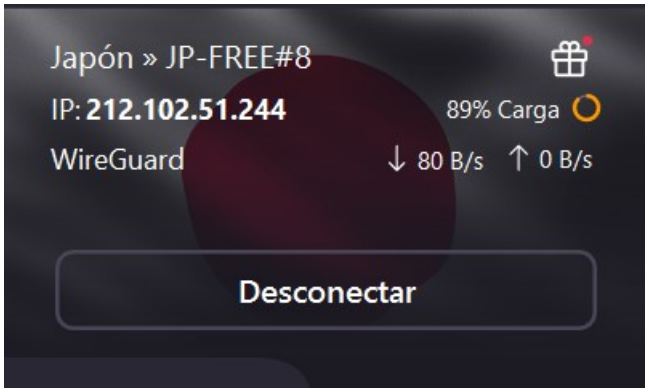


Añadimos el usuario y contraseña que creamos antes:

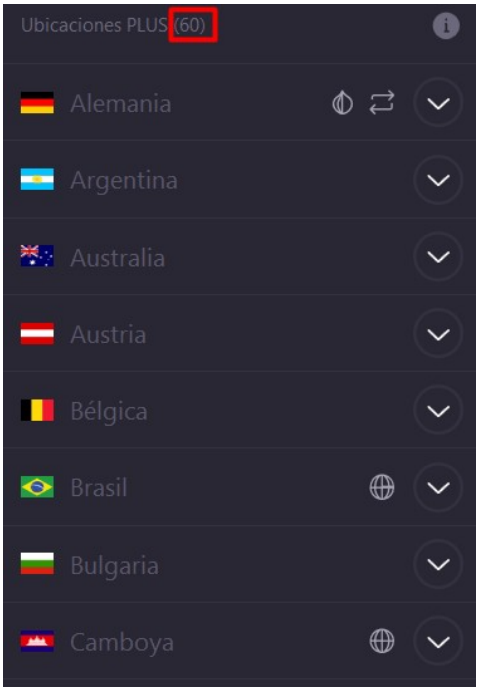


Le damos a conexión rápida y se nos conectará a uno de los servidores gratuitos, en mi aso japón:





Podemos ver que en la versión de pago a múltiples servidores en distintos países, hasta 60:



Sumando este apartado de la VPN con lo que hemos realizado en la máquina virtual de kali con proxychain, podemos conseguir una seguridad todavía más avanzada. Ya que si por alguna razón fallara alguno de los sistemas, tendríamos la otra capa.

d) Debilidades y vulnerabilidades de Tor. Investiga alguna de las vulnerabilidades o debilidades descritas en la Wikipedia sobre el servicio Tor. Localiza un paper o publicación original y compártela en el foro escribiendo una pequeña reseña explicando en qué consiste.

Si nos vamos a la Wikipedia encontramos diferentes vulnerabilidades, como el Bloqueo de Consenso, Ataque de Análisis de Tráfico, la escucha a escondidas o el Ataque Bad Apple "Manzana Podrida"o el bug de Heartbleed.

Como apunte tenemos el bloqueo de nodos de salida por parte de algunas compañías que hacen, que por ejemplo usando Tor no se pueda editar la Wikipedia.

Bad Apple:

Este ataque se remonta a 2011 y fue realizado por investigadores franceses, documentando que se podía explotar el diseño de Tor y relevar las direcciones IP de los usuarios de BitTorrent, que es un servicio de intercambio de archivos en línea.

En las referencias de la Wikipedia encontramos el paper original: https://www.usenix.org/legacy/events/leet11/tech/full_papers/LeBlond.pdf

Bug de Heartbleed:

Vemos que Tor fue vulnerable a la vulnerabilidad heartbleed de OpenSSL.

En concreto esto ocurrió en el año 2014, cuando en más de un 20% de los nodos de salida de Tor se podía ver texto en plano, incluyendo credenciales. Una vez se supo esto el equipo de Tor lo arregló lo antes posible, pero es un ejemplo de que nada es 100% seguro.

https://threatpost.com/tor-begins-blacklisting-exit-nodes-vulnerable-to-heartbleed/105519/

Ataque de confirmación de tráfico:

En este ataque, que se produjo en 2014, se calculaba el tiempo y el volumen de tráfico que pasaba entre los extremos de repetidores (nodos). Con esto era capaz de ver si pertenecían al mismo usuario, y con esto desanonimizarlo, ya que en el primer nodo tenemos la IP y en el último la página que accede. Consiguieron mandar la señal para acceder a los nodos en las cabeceras del protocolo Tor.

Aquí tenemos el reporte en el blog de tor:

https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack/

Ejercicio 3: Securizando el entorno de trabajo.

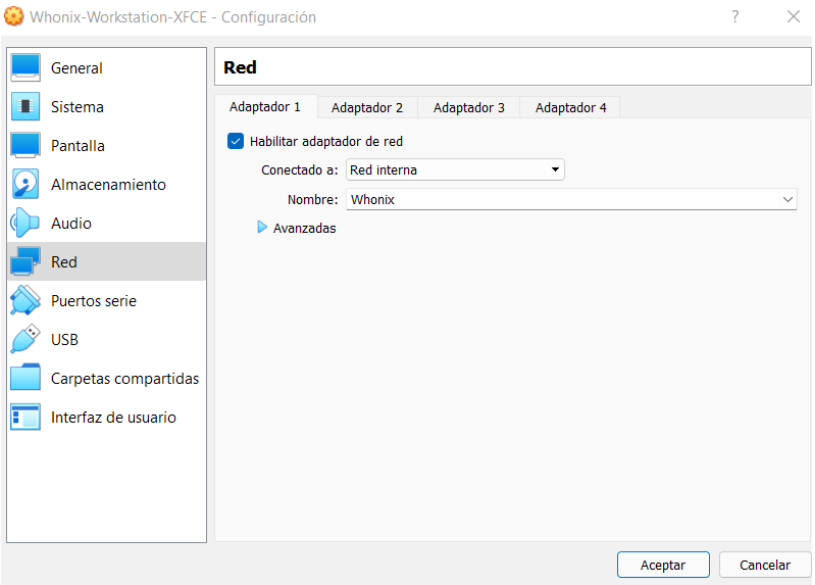
Descripción:

A menudo usamos diferentes dispositivos para conectarnos a Internet, equipos portátiles, sobremesa, tablets, teléfonos móviles. Para desempeñar nuestro trabajo con garantías es importante independizar los dispositivos de trabajo de los personales siempre que sea posible. En cualquier caso, el dispositivo que usemos para realizar nuestro trabajo deberá tener las herramientas y configuración apropiada para poder hacerlo de manera anónima y segura.

En este ejercicio deberás configurar tu ordenador personal y tu dispositivo móvil con las herramientas que creas convenientes para desempeñar tu trabajo de forma anónima y segura. Para ello, se recomienda consultar las páginas de los proyectos Prism-Break y Privacy Tools vistas en la unidad.

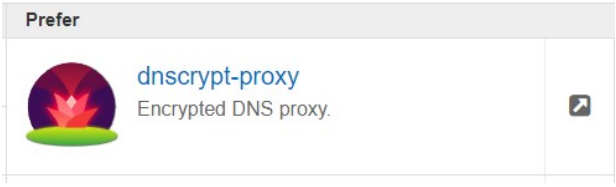
a) Configuración de seguridad del ordenador personal. Prepara una máquina virtual con una distribución Tails o Whonix y valora su utilidad, así como la configuración de otras herramientas que sean necesarias.

En nuestro caso hemos instalado una máquina Whonix para probarla, lo primero que observamos es que se divide en dos al instalarse, gateway y workstation. Son ambas parecidas y basadas en linux. Al iniciarla vemos que podemos poner en las opciones de inicio el uso del protocolo tor y de proxy. Para poder navegar por internet tendremos que usar la máquina workstation, la otra solo sirve de puerta de enlace y la red en la máquina workstation será interna para comunicarse con la otra máquina.

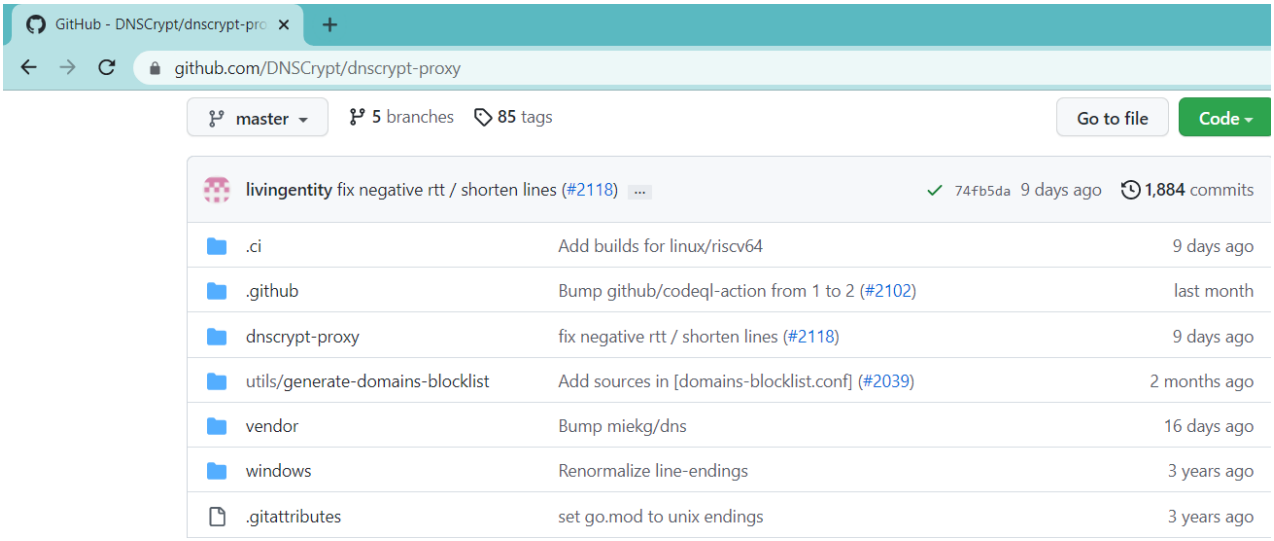


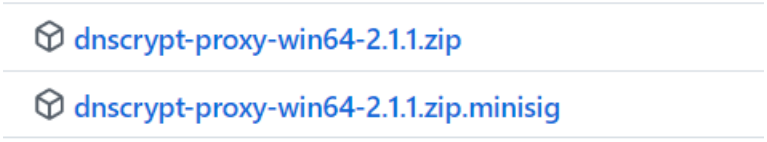
Observamos como el navegador que tenemos en la máquina workstation es el tor browser y cómo una vez configurado todo tenemos conexión a internet.

En otras herramientas, vamos a probar dnscrypt, para tener el DNS encriptado en vez de usar los públicos de Google en nuestro ordenador personal Windows:



Para ello nos vamos a Github y nos descargamos el código, en el Readme tenemos el link a la última versión de Windows:





Ahora lo Instalamos con el fichero correspondiente y lo iniciamos:

```
[2022-05-27 13:54:49] [NOTICE] Installed as a service. Use `-service start` to start
[2022-05-27 13:54:50] [NOTICE] Service started

Thank you for using DNSCrypt-Proxy!
Press [Enter] to exit . . .
```

Con esta herramienta también podemos bloquear nombres o IP mediante algunos ficheros de configuración:

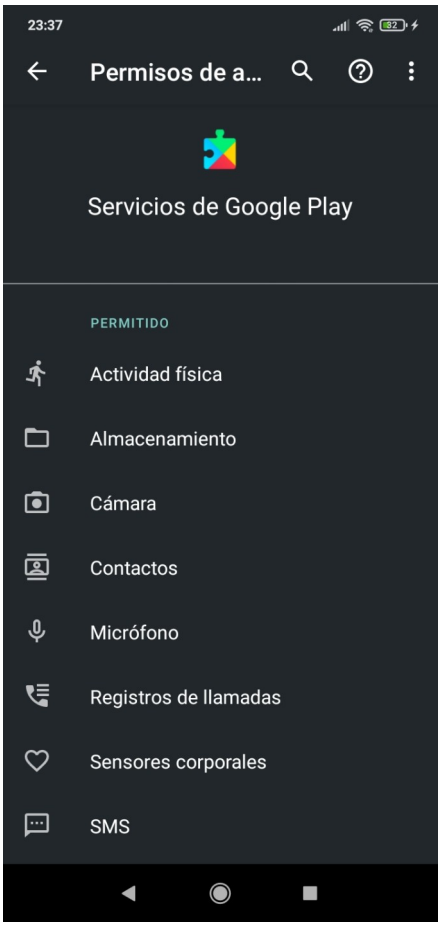
```
############################
#        Blocklist         #
############################

## Rules for name-based query blocking, one per line
##
## Example of valid patterns:
##
## ads.*          | matches anything with an "ads." prefix
## *.example.com  | matches example.com and all names within that zone such as www.example.
## example.com    | identical to the above
## =example.com   | block example.com but not *.example.com
## *sex*          | matches any name containing that substring
## ads[0-9]*      | matches "ads" followed by one or more digits
## ads*.example*  | *, ? and [] can be used anywhere, but prefixes/suffixes are faster

ad.*
ads.*
banner.*
banners.*
creatives.*
oas.*
oascentral.*        # inline comments are allowed after a pound sign
stats.*
```

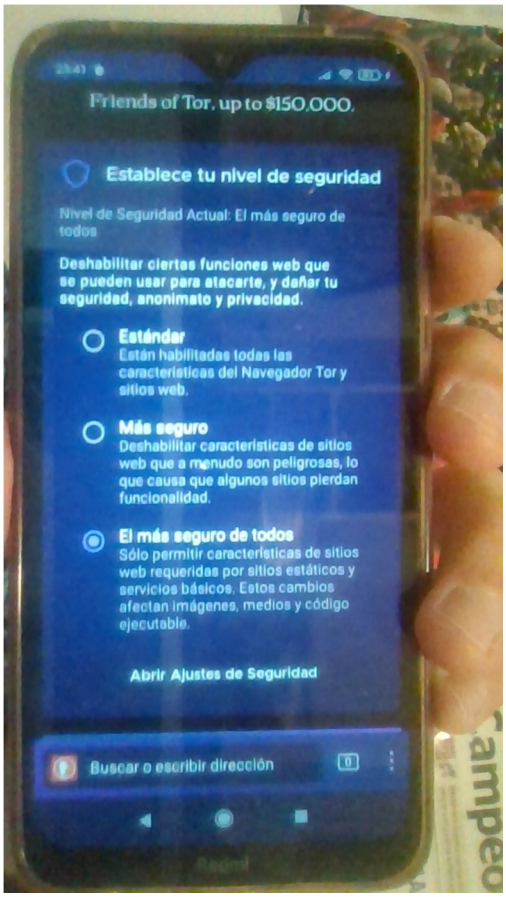
b) Configuración de seguridad del dispositivo móvil.

En mi caso mi dispositivo móvil es un Android, en Android se recomienda reemplazar las aplicaciones proporcionadas por Google por Replicant, o compilar Android desde la fuente.

También vigilar los permisos de las aplicaciones sobre todo de las de google en el caso que no se hayan reemplazado estas y hay que tener mucho cuidado con las puertas traseras de Google Play.

En esta captura observamos la cantidad de permisos que tienen los Servicios de Google Play.





Se recomienda encriptar el móvil y hacer copias de seguridad sin tener en cuenta a Google.

Además es mejor si retiramos el micrófono del teléfono.

Para navegar anonimamente configuraremos el cortafuegos y el script de de soporte de Tor, esto lo vemos en la segunda captura con tor browser, que tiene varios niveles de seguridad, la más segura solo se permiten ejecutar algunas características de los sitios web. La captura está hecha a mano ya que no se permiten hacer capturas en Tor Browser por seguridad.

Ejercicio 4: Generando identidades falsas para ciberinvestigaciones

Descripción:

El último ejercicio consistirá en generar perfiles en redes sociales con identidades falsas que puedas emplear en ciberinvestigaciones. Investiga si hay herramientas que te puedan ayudar a esta labor ya que un buen perfil falso debería tener algún tipo de actividad para que pueda parecer una cuenta real.

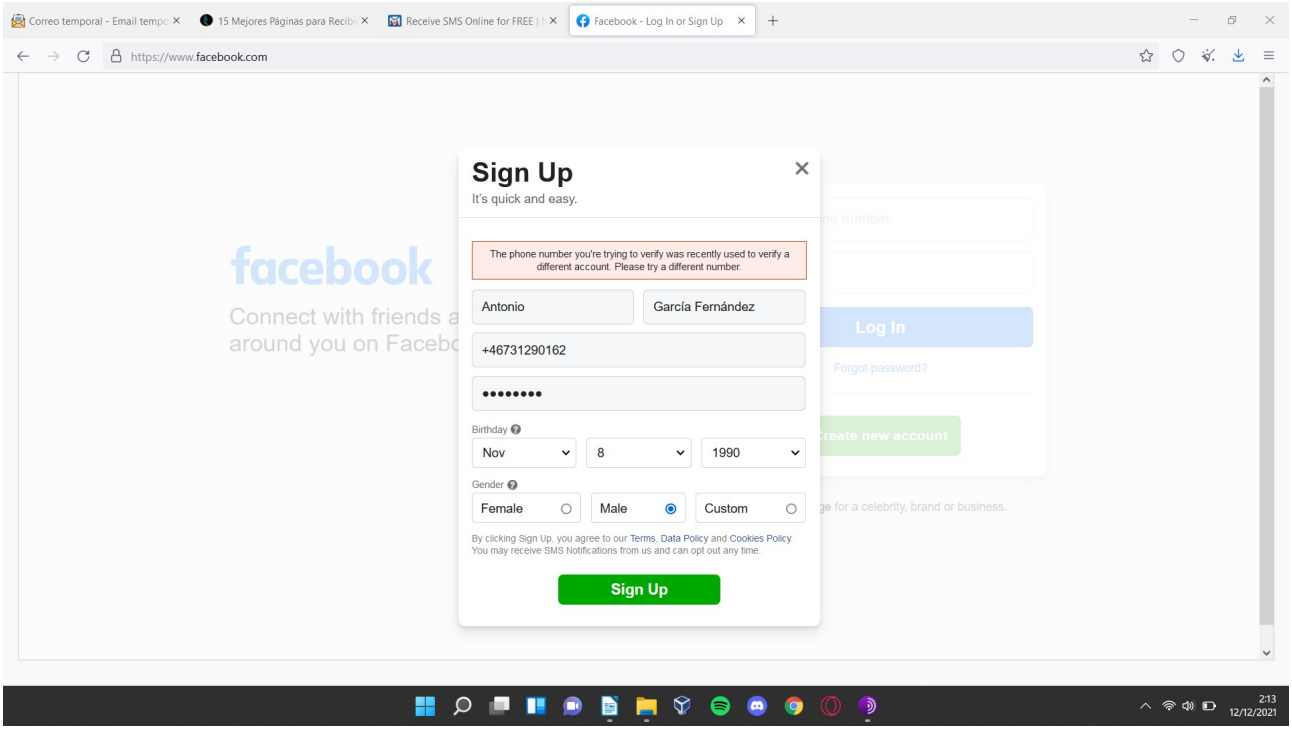
Resolución:

Vamos a intentar crear un perfil falso desde tor y generando una cara con la web https://thispersondoesnotexist.com/ y con un correo electrónico temporal con la web https://correotemporal.org/. Intentaremos hacer un twitter y un facebook.

En twitter, el código de verificación lo podemos ver en la propia web de correo temporal.

Pero luego te pide aunque en un principio no, meter un número de teléfono y hacer la verificación.

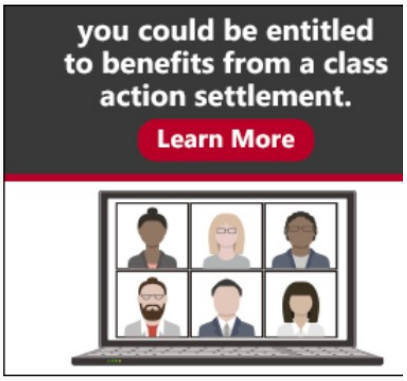
He buscado múltiples páginas de números de teléfono para verificar sin poner el nuestro real. Al hacer esto he descubierto que las redes tienen un mecanismo que no dej usar el mismo número para verificar varias cuentas, la única vez que lo he conseguido al ver el la web se veía con asteriscos el código, asi que ha sido imposible crear la cuenta.



Correo Temporal

Aplicación gratuita que te permite generar un **email temporal anónimo y privado** para recibir mensajes en él sin registro alguno. Así mismo, podrás **enviar mensajes anónimos** desde nuestra aplicación totalmente gratis.

Protege tu **email personal** de SPAM utilizando un **correo temporal** gratuito.



Tu email temporal

hudson14r_v971r@vixej.com

Tu email expira el día: **30/10/2022**, luego, será eliminado y no podrás volver a recuperarlo.

Tus mensajes recibidos

A continuación, mostramos los mensajes recibidos en tu **correo temporal** y el estado de tus mensajes enviados.

Asunto	Remitente	Fecha
443462 is your Twitter verification code	Twitter <verify@twitter.com>	12/12/2021 12:46:12 am
Tiene un nuevo mensaje	CorreoTemporal.org	-