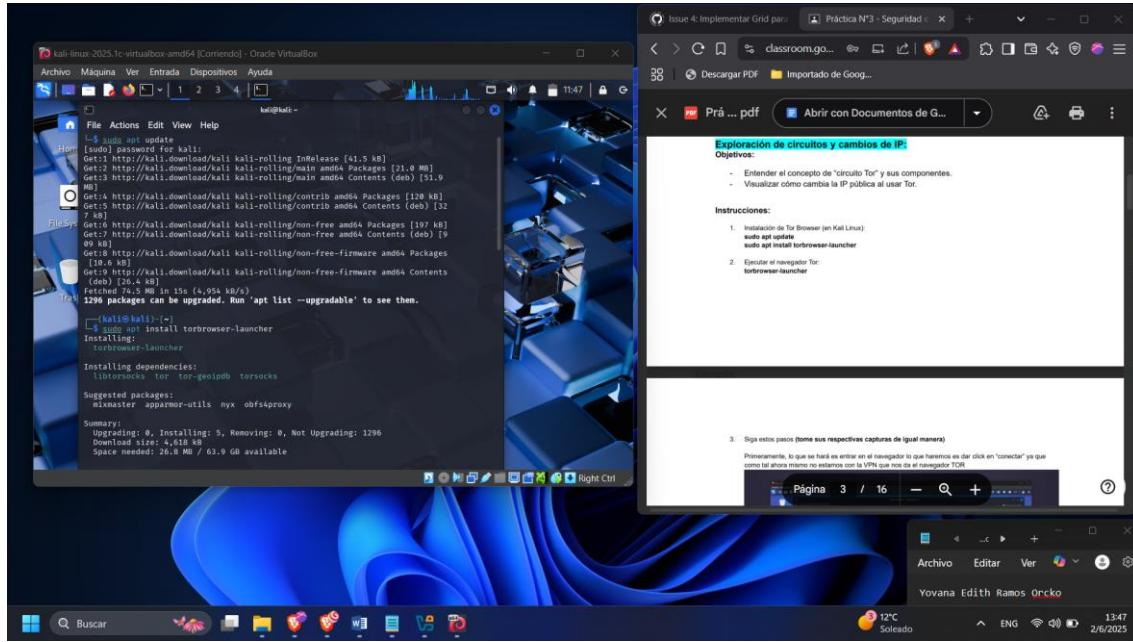


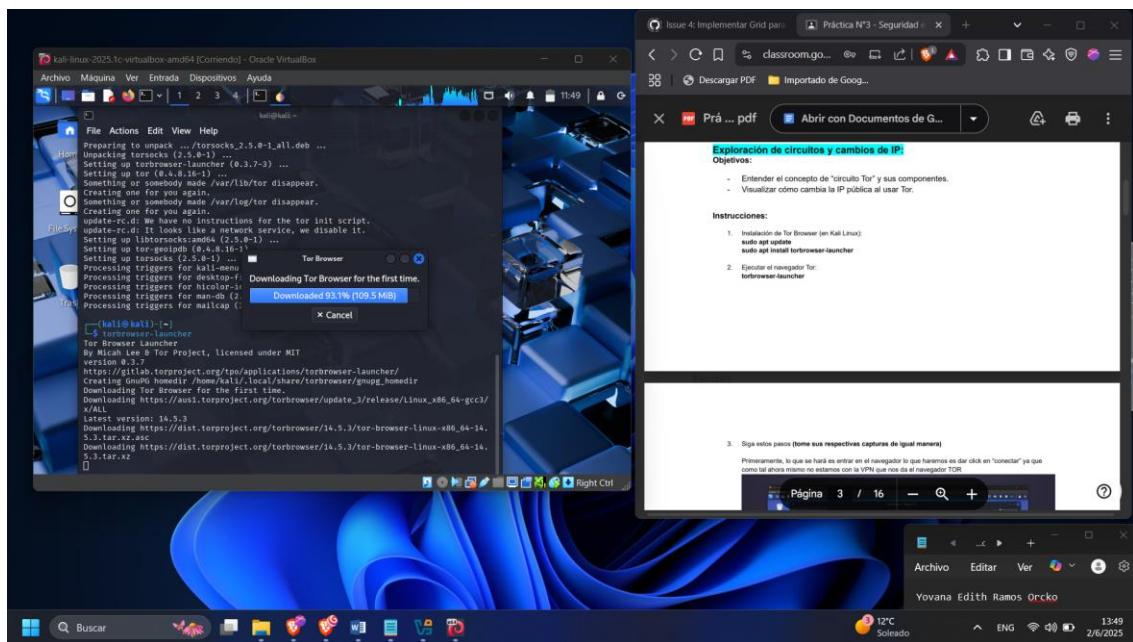
UNIVERSIDAD AUTONOMA "TOMAS FRIAS"			
CARRERA DE INGENIERIA DE SISTEMAS			
Materia:	Seguridad de Sistemas (SIS-737)		
Docente:	M.Sc. Ing. Javier Alexander Duran Miranda		N Practica
Auxiliar:	Univ. Aldrin Roger Perez Miranda		
Fecha de Publicación	27/05/2025		3
Fecha de Entrega	10/06/2025		
Grupo:	1	Sede	Potosi

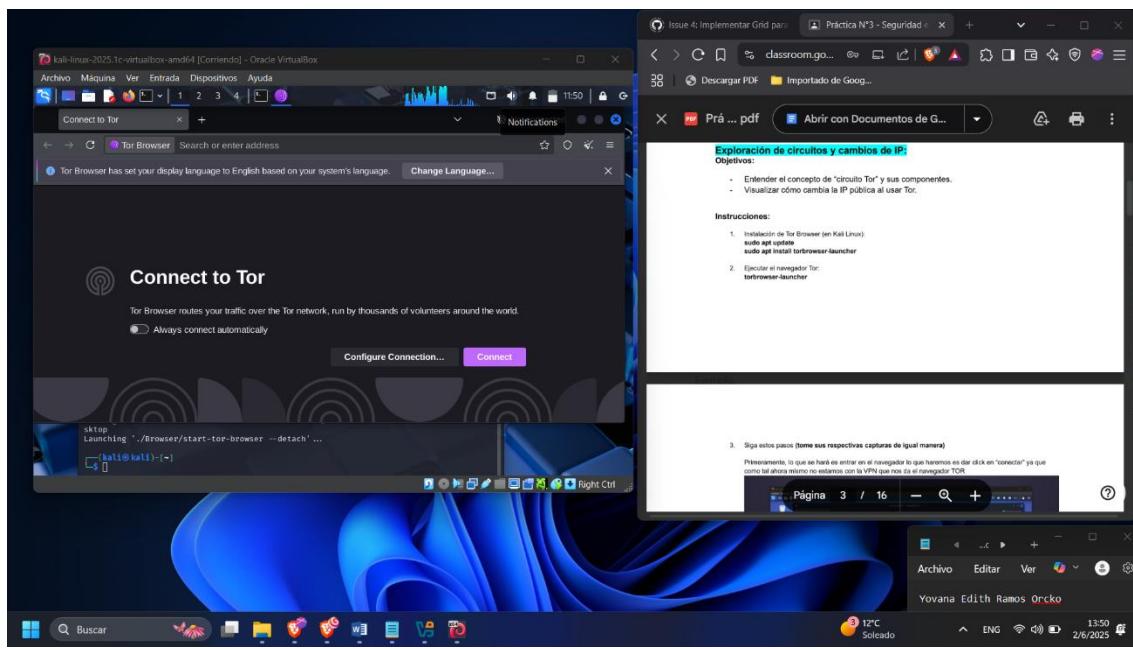
Parte 1:

1. Instalación de Tor Browser

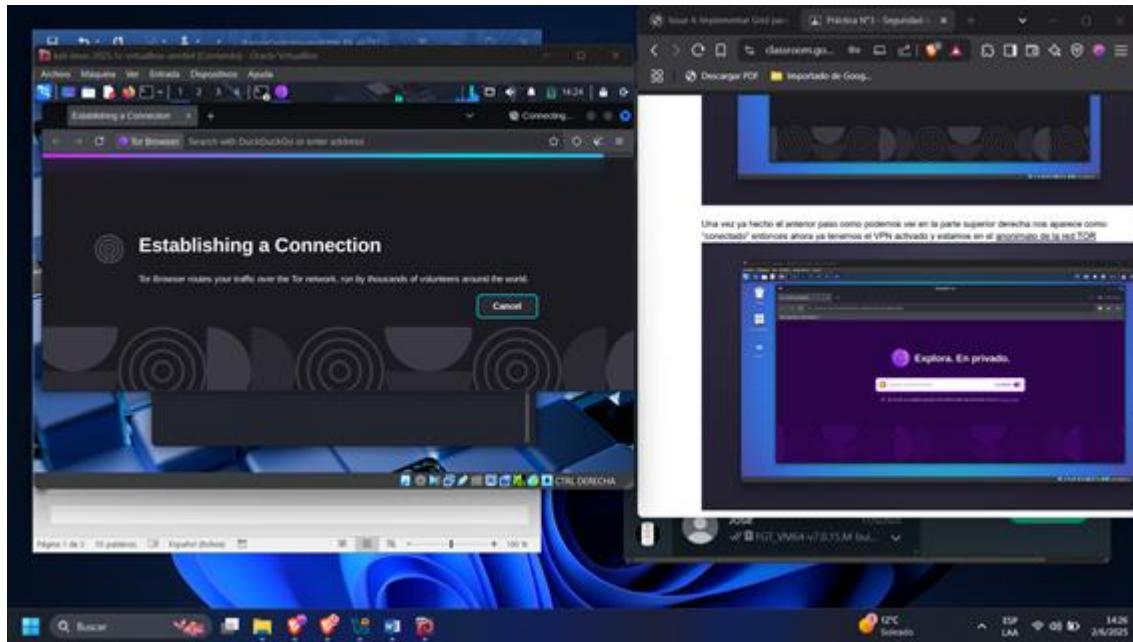


2. Ejecutar navegador

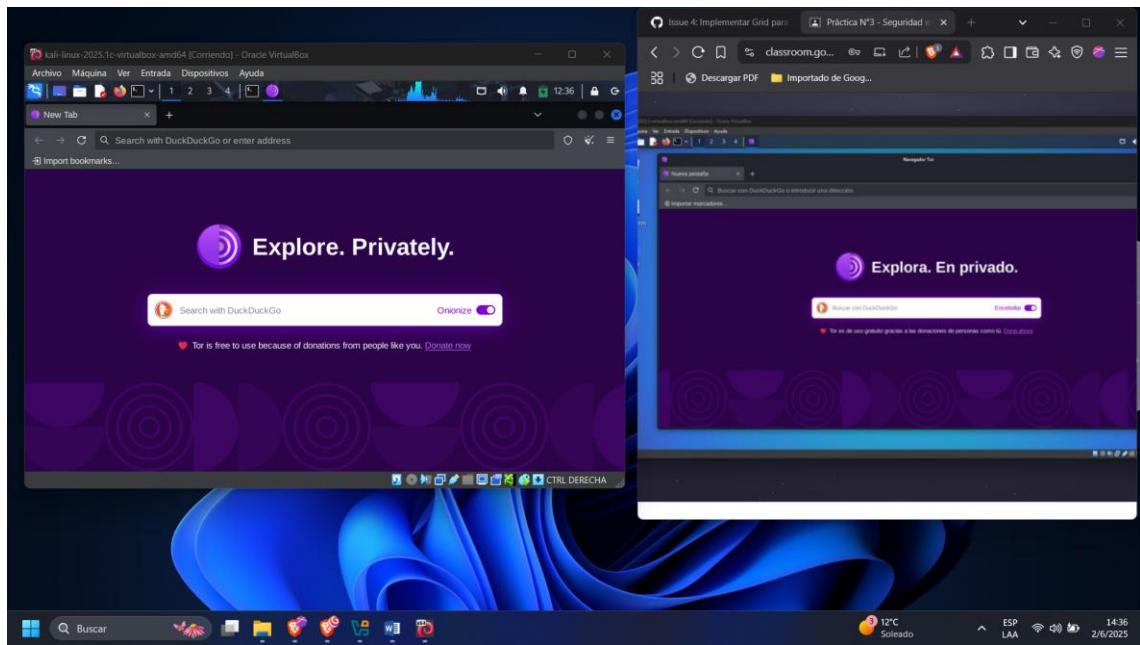
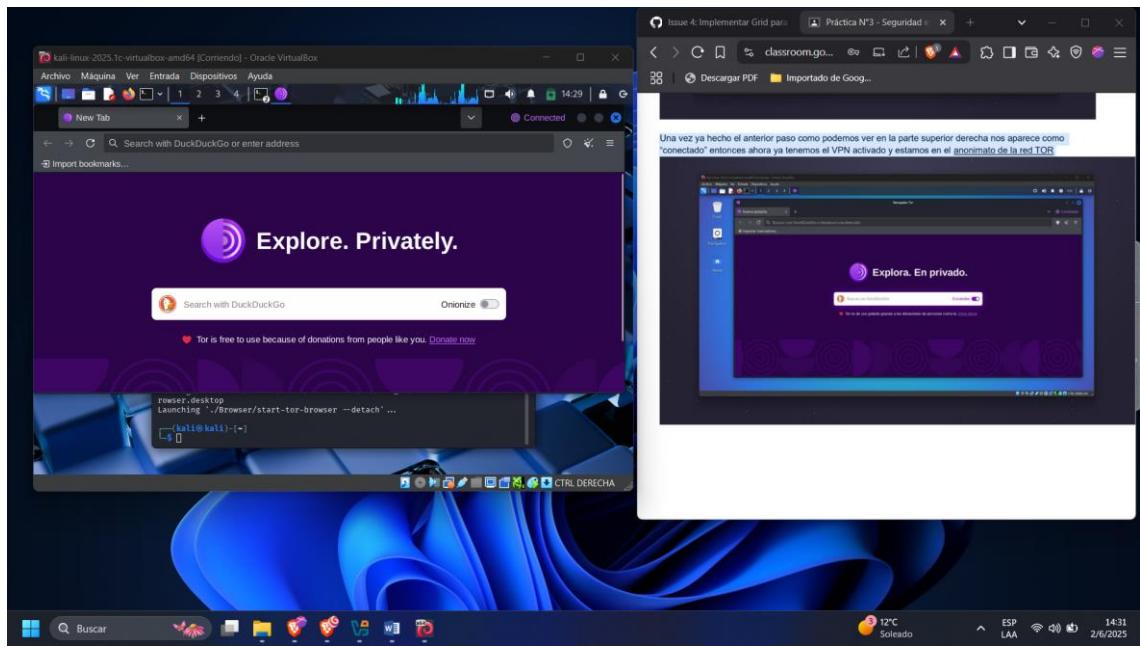




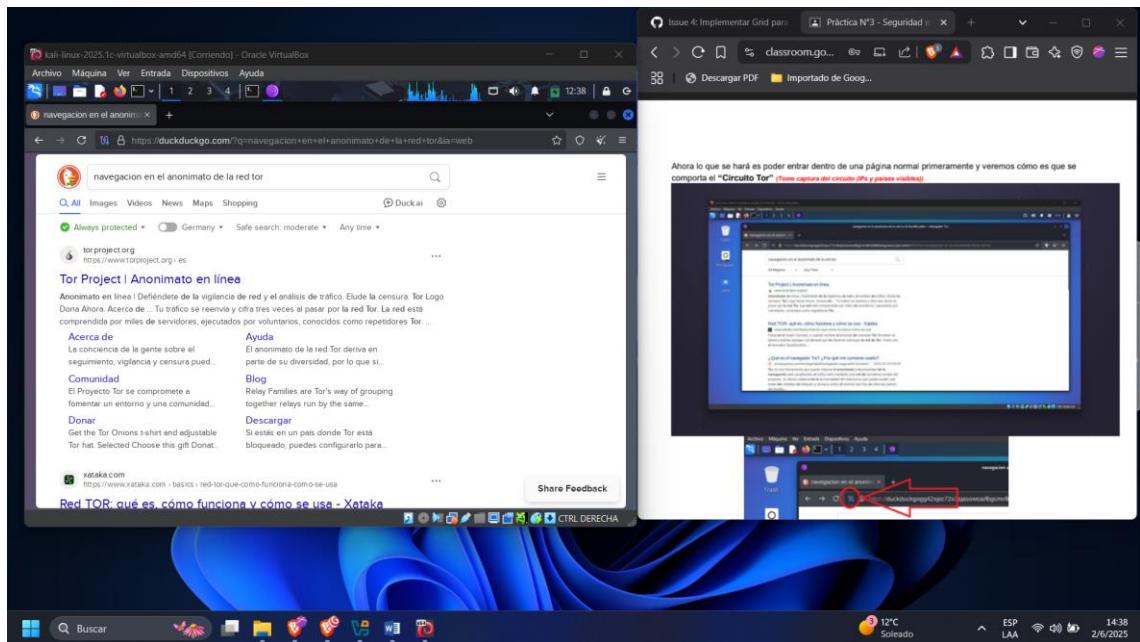
3. Seguir pasos



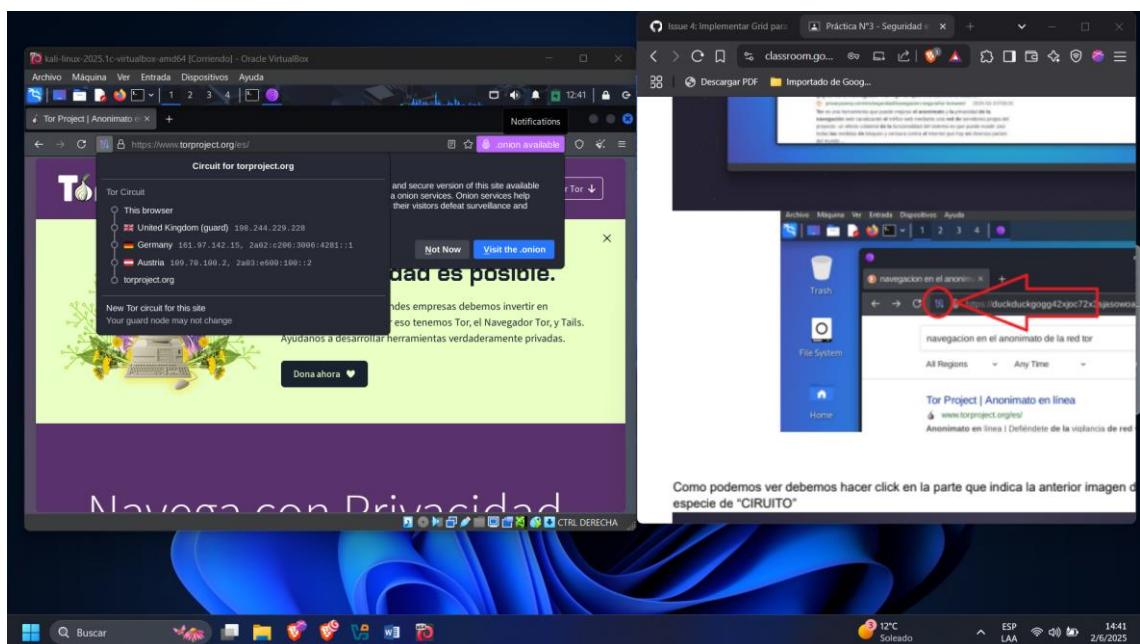
Anonimato tor



Como se comporta el circuito Tor

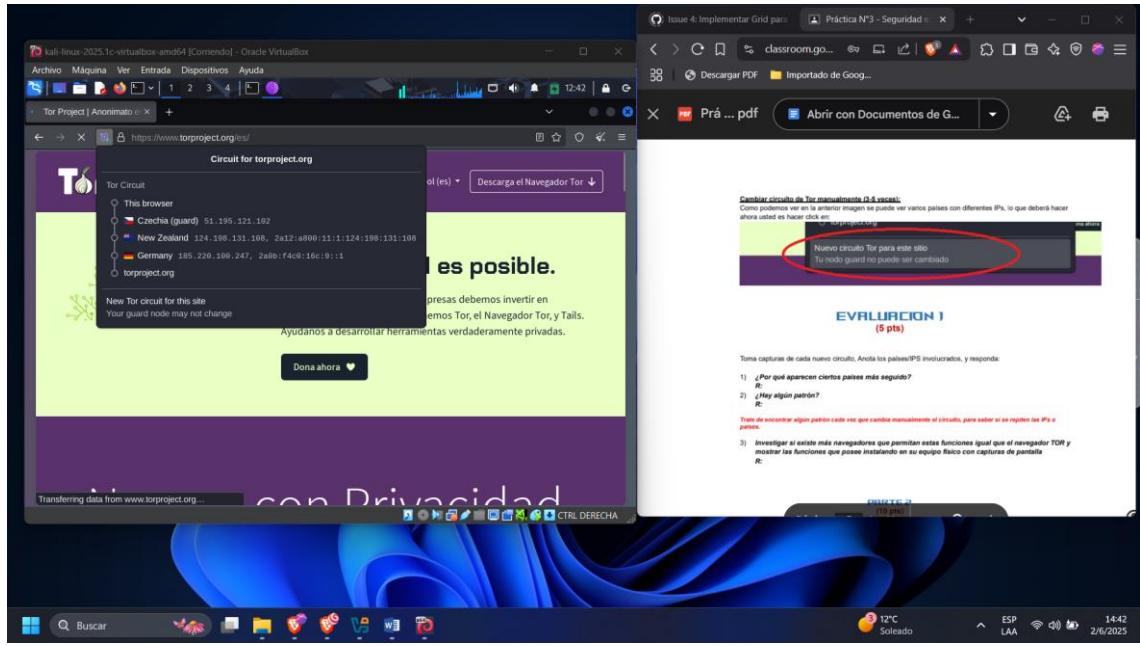


Click CIRCUITO

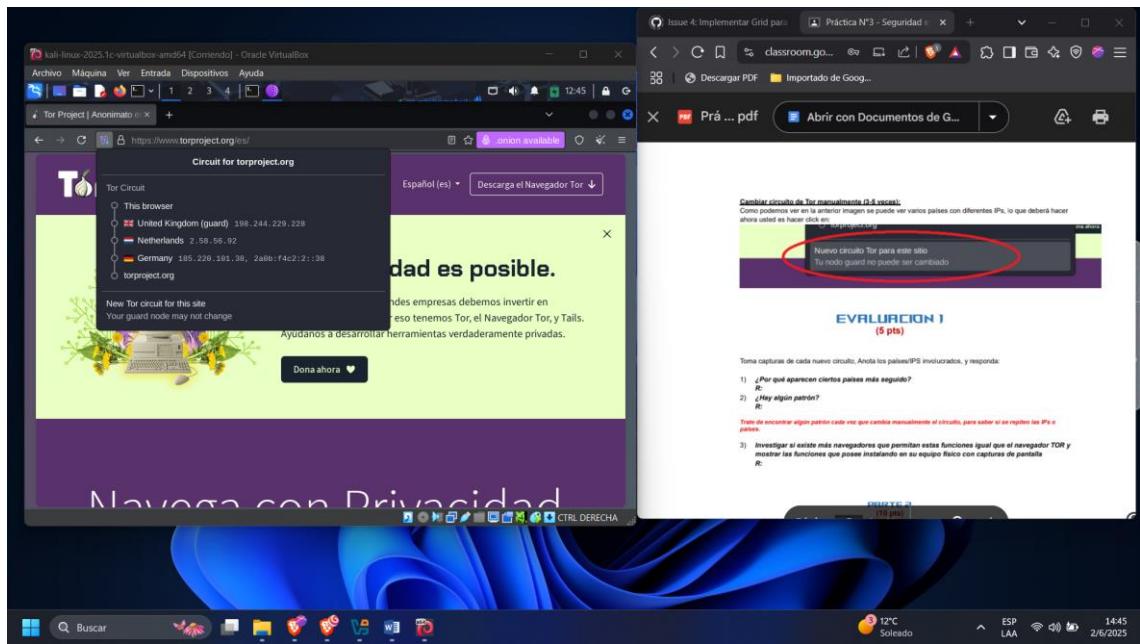


Cambiar circuito manualmente

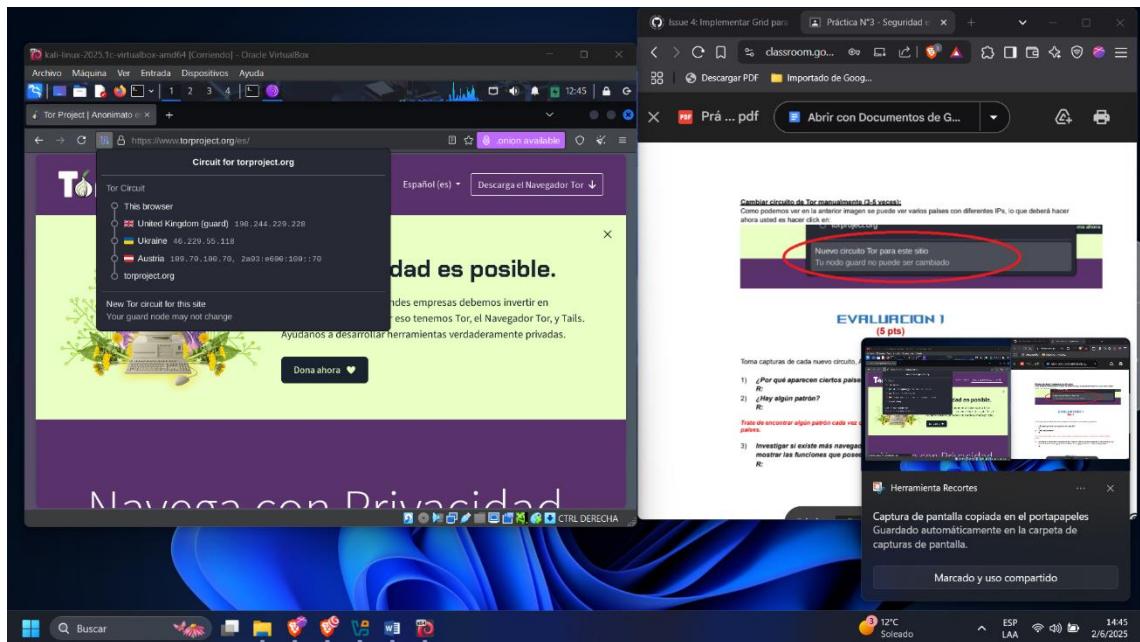
1-



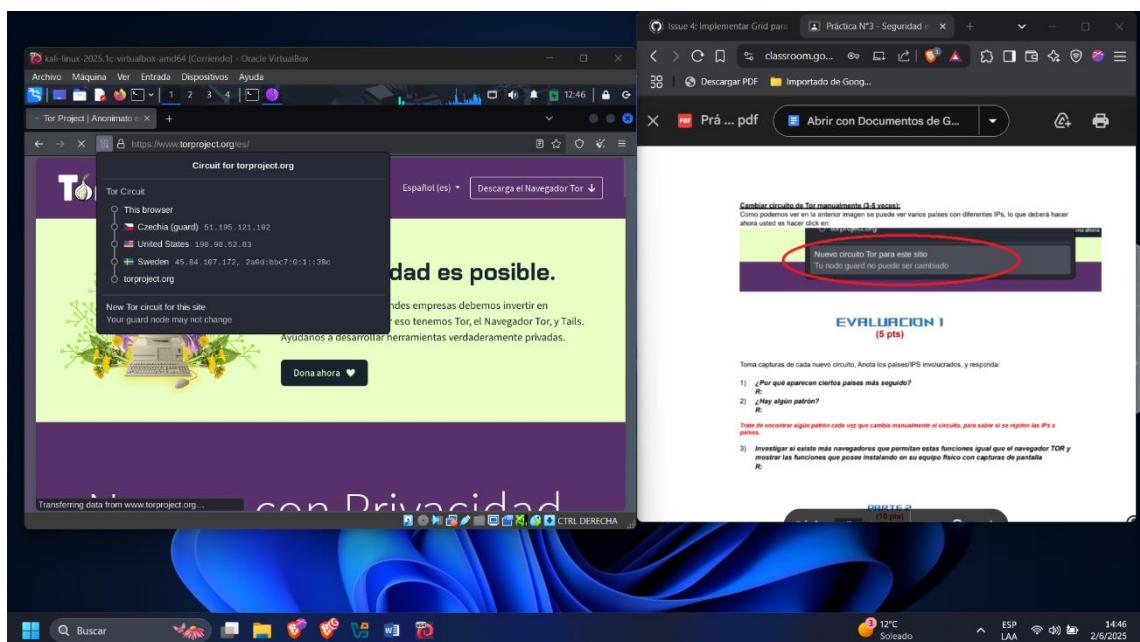
2-



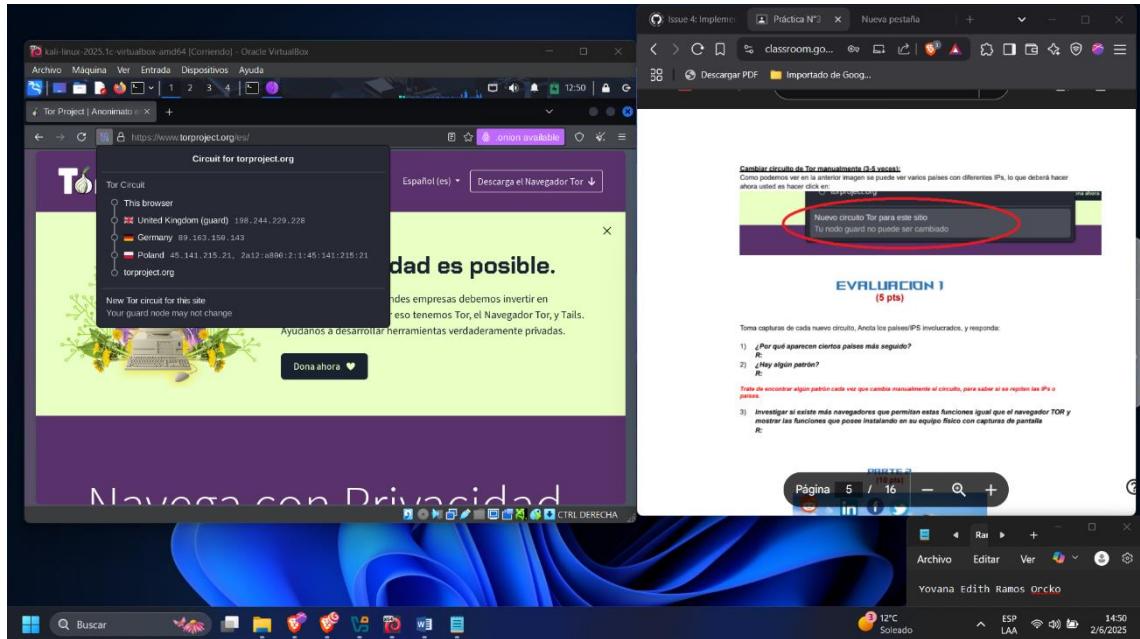
3-



4-



5-



EVALUACION

1) ¿Por qué aparecen ciertos países más seguido?

Porque algunos países tienen más nodos disponibles en la red tor (Estados Unidos, Alemania...), por eso suelen aparecer más.

2) ¿Hay algún patrón?

Es que suele haber veces que se repiten ciertos países como salida (exit nodes), principalmente en regiones con más infraestructura de red y libertad de acceso.

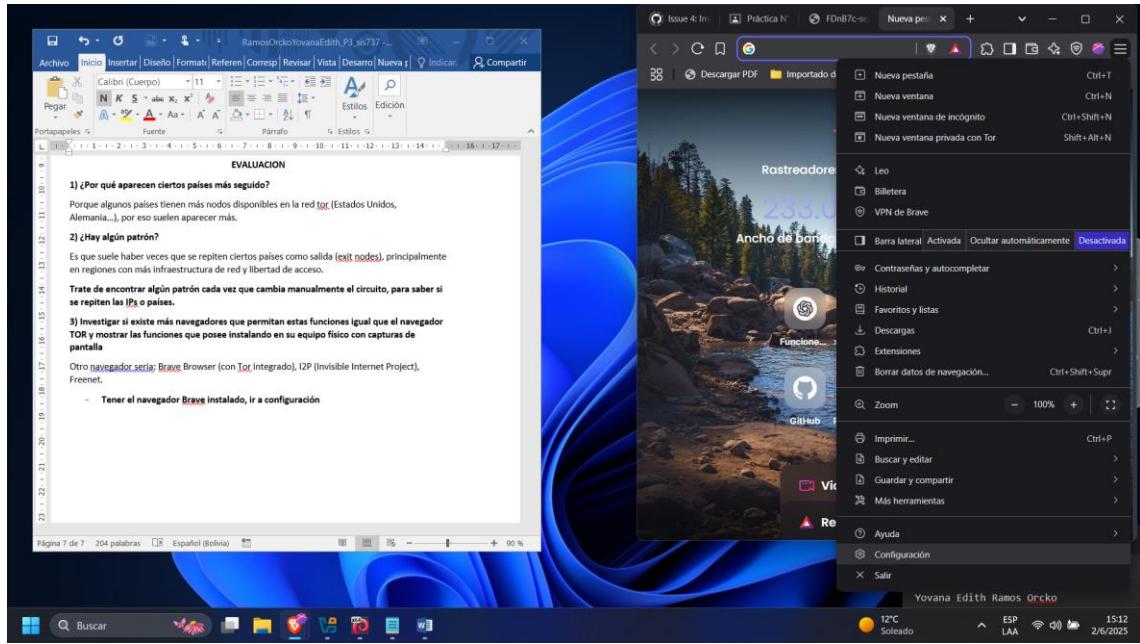
Trate de encontrar algún patrón cada vez que cambia manualmente el circuito, para saber si se repiten las IPs o países.

3) Investigar si existe más navegadores que permitan estas funciones igual que el navegador TOR y mostrar las funciones que posee instalando en su equipo físico con capturas de pantalla

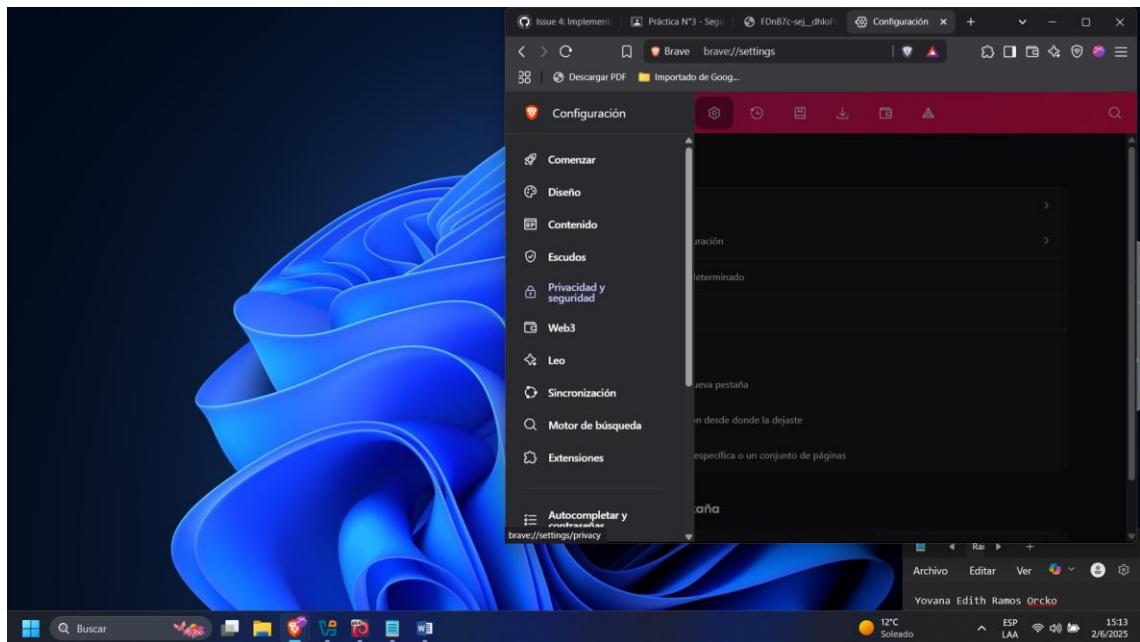
Sí, existen otros navegadores que ofrecen funciones similares al navegador Tor, permitiendo navegación anónima o privada. Se presenta:

El navegador: Brave Browser: Permite navegación privada con Tor integrada, además de bloqueo de rastreadores y anuncios por defecto como también la mejora del rendimiento y privacidad.

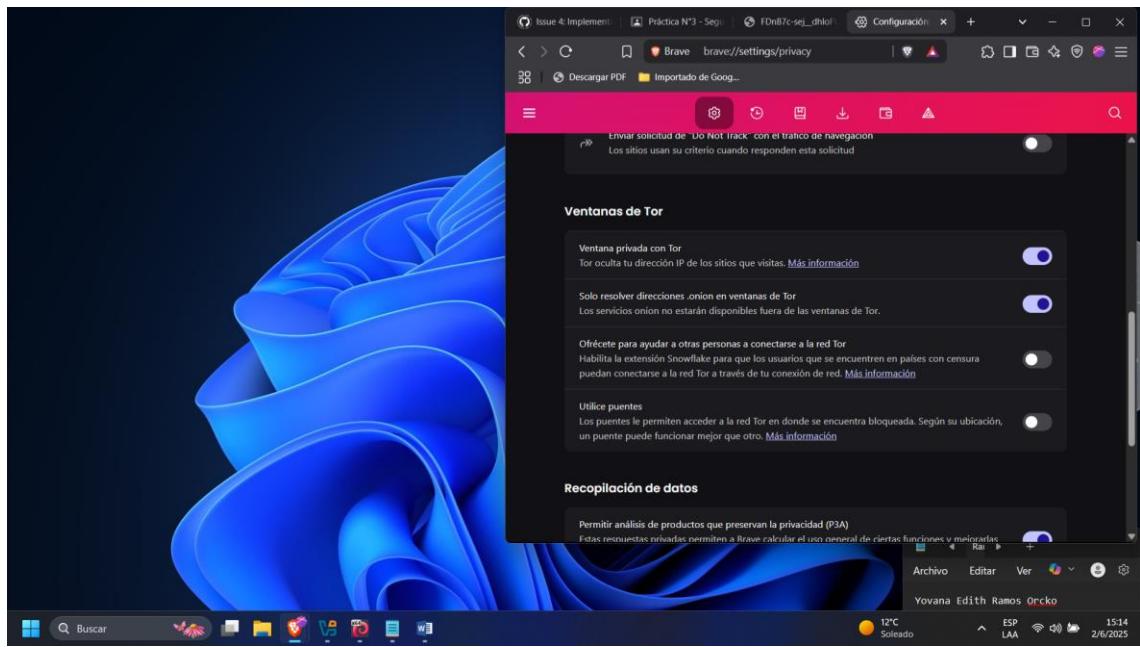
- Tener el navegador Brave instalado, ir a configuración



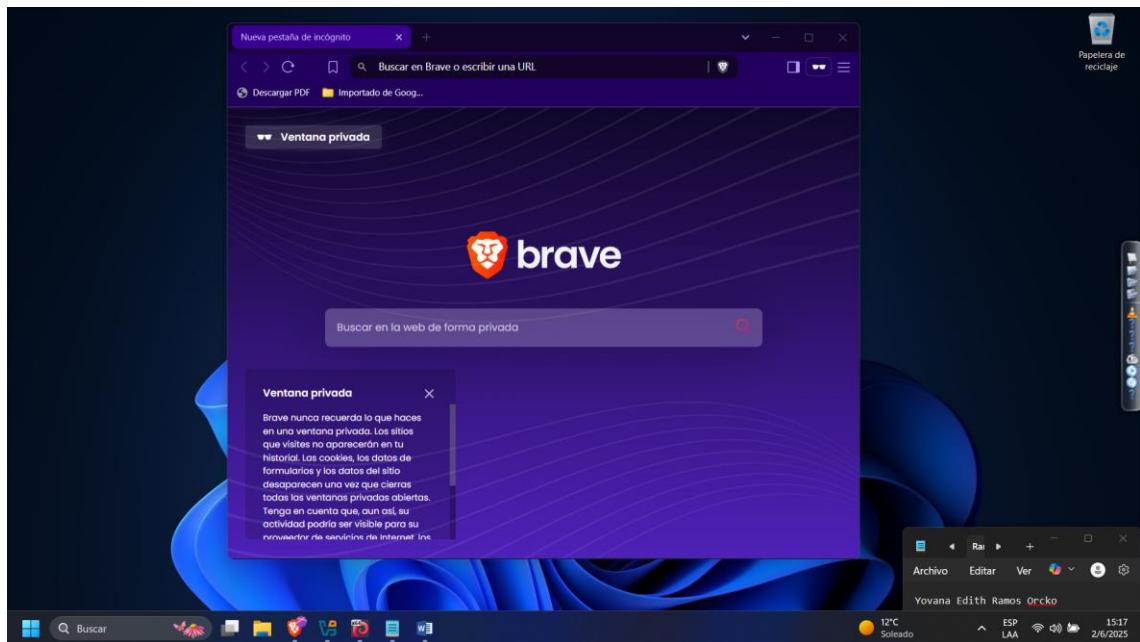
Dirigirse a privacidad y seguridad



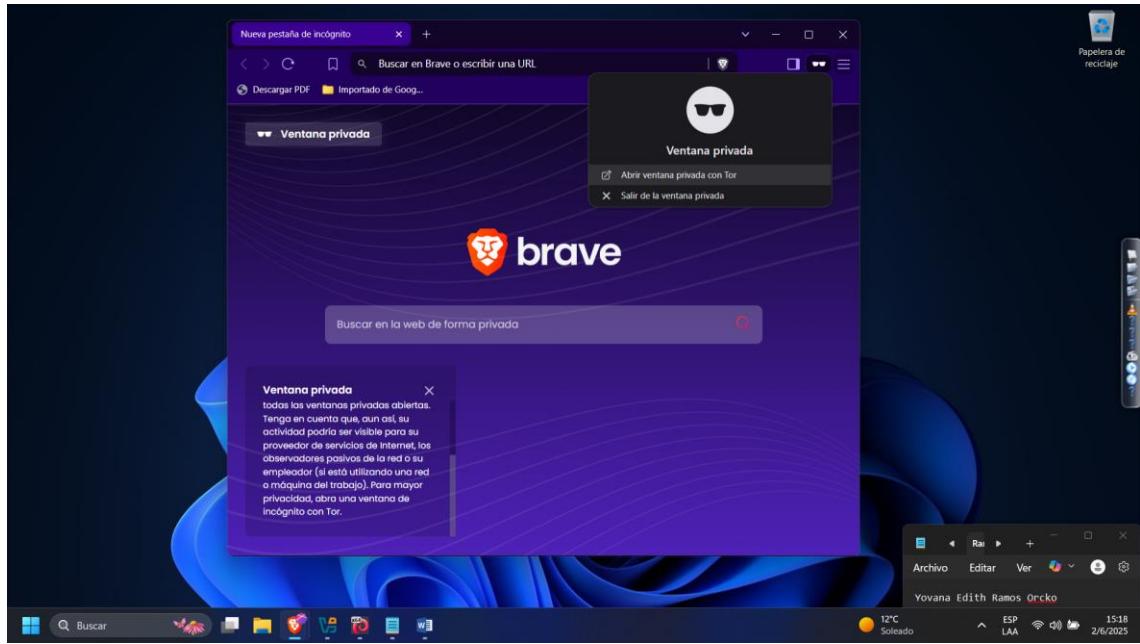
Activar tor, ventana privada



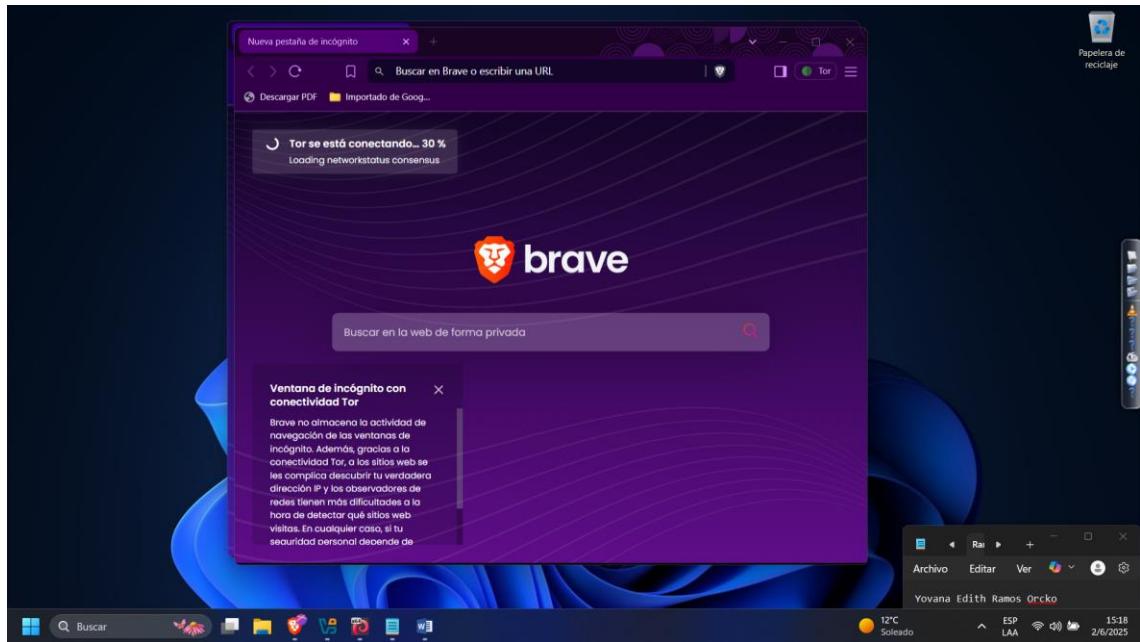
Presiona Ctrl + Shift + N para abrir una ventana privada.



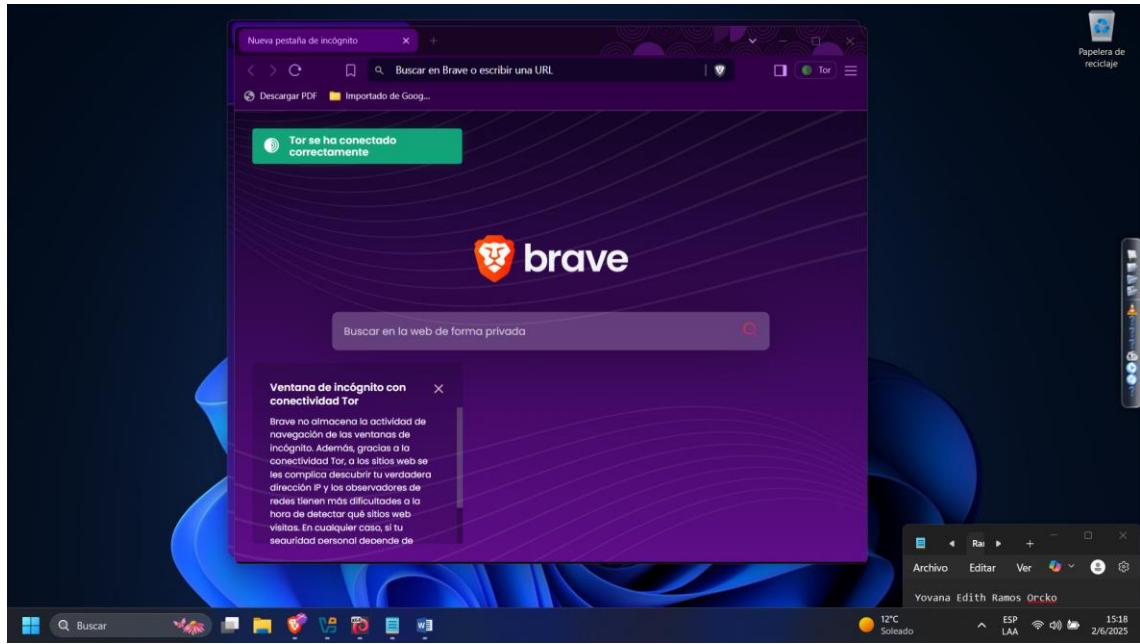
Click abrir ventana privada con tor



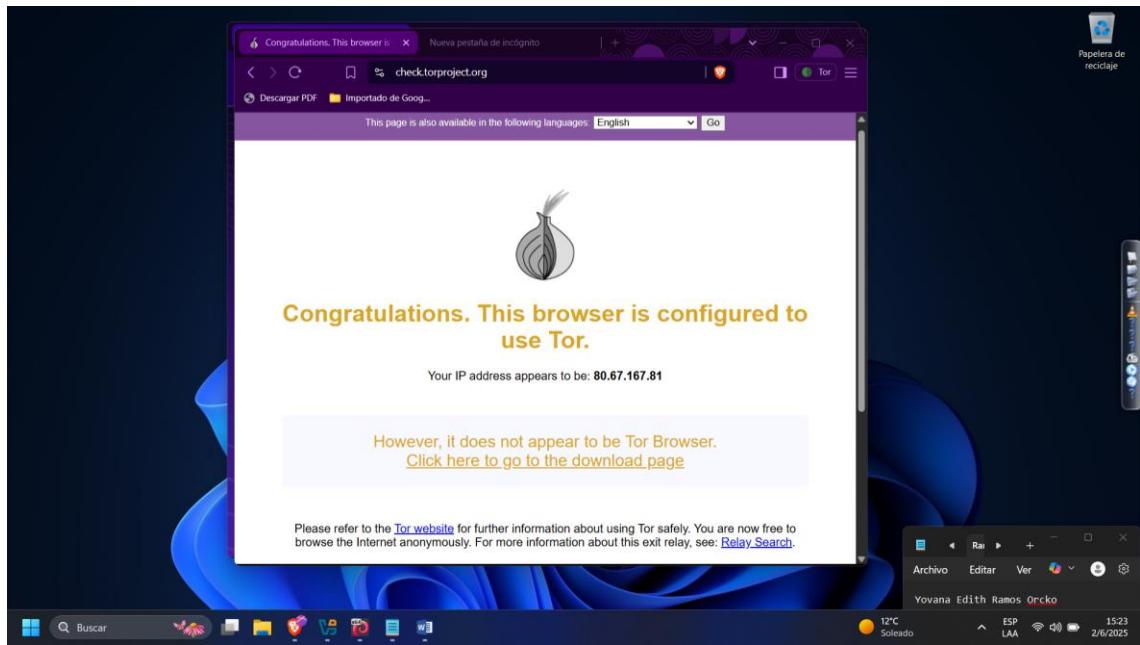
Cargando

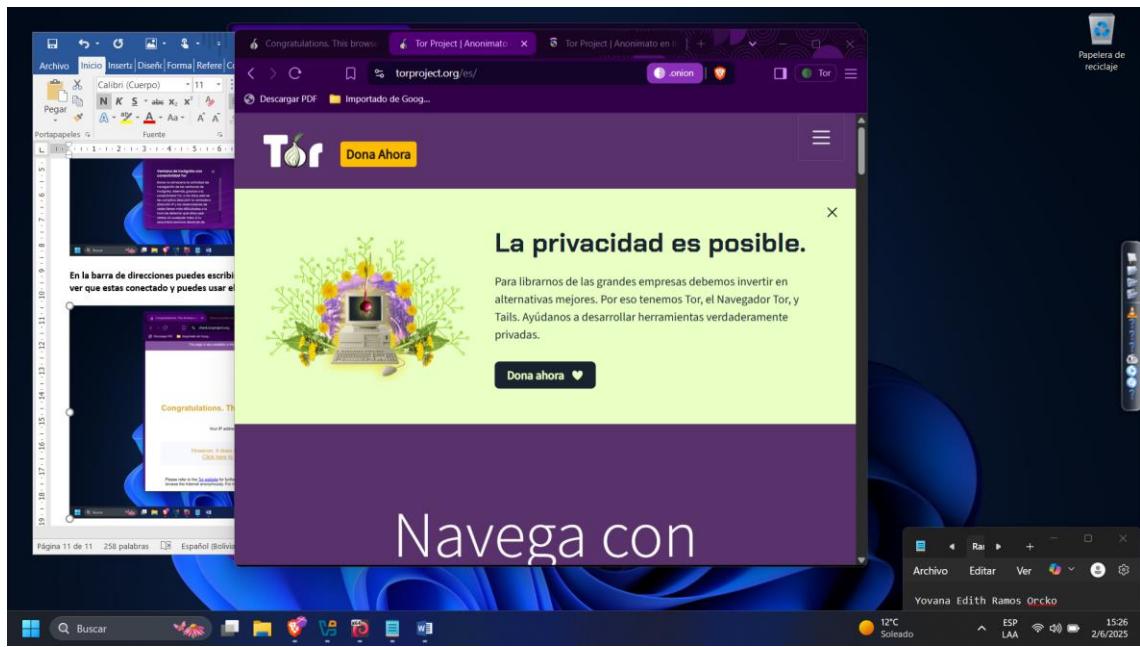


Tor se ha conectado



En la barra de direcciones puedes escribir: check.torproject.org, para observar que se puede ver que estas conectado y puedes usar el navegador tor



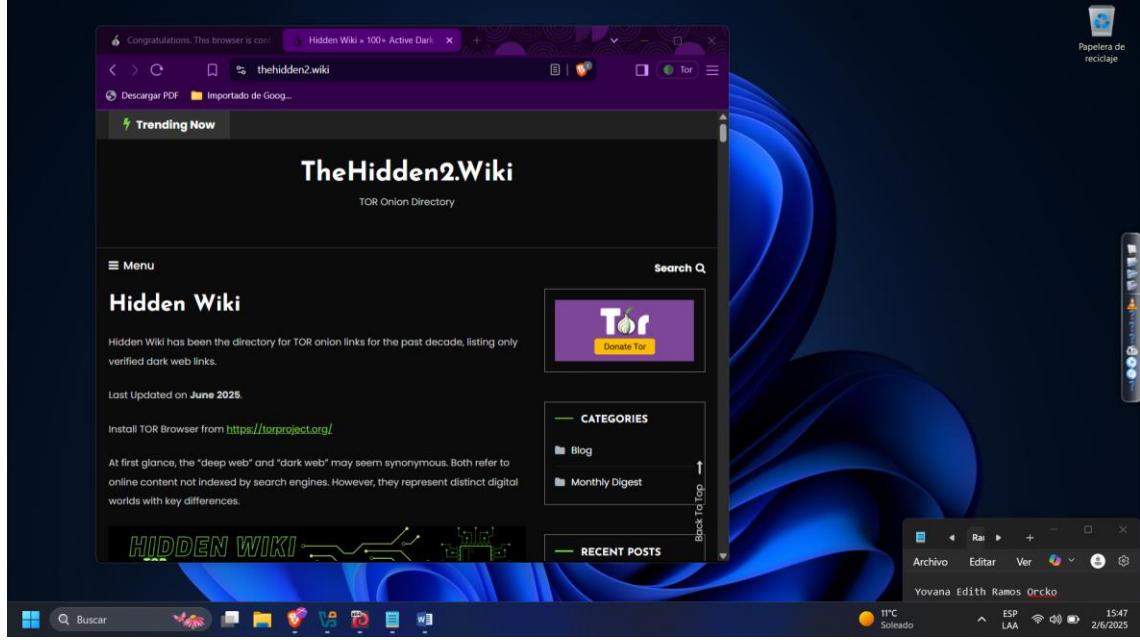


PARTE 2

Comparación entre navegadores

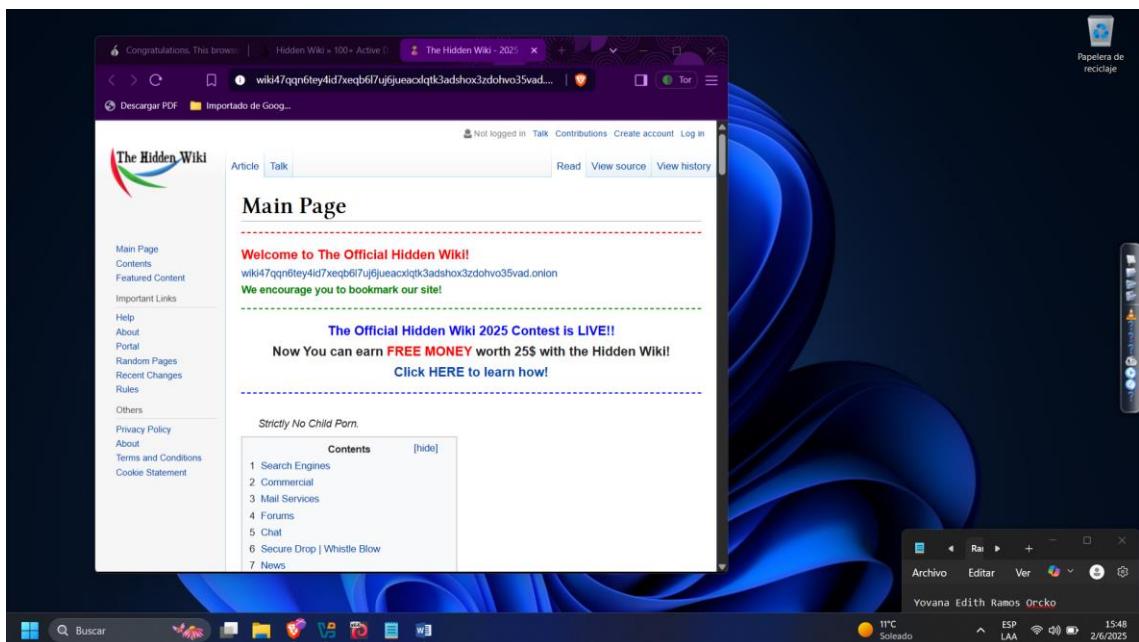
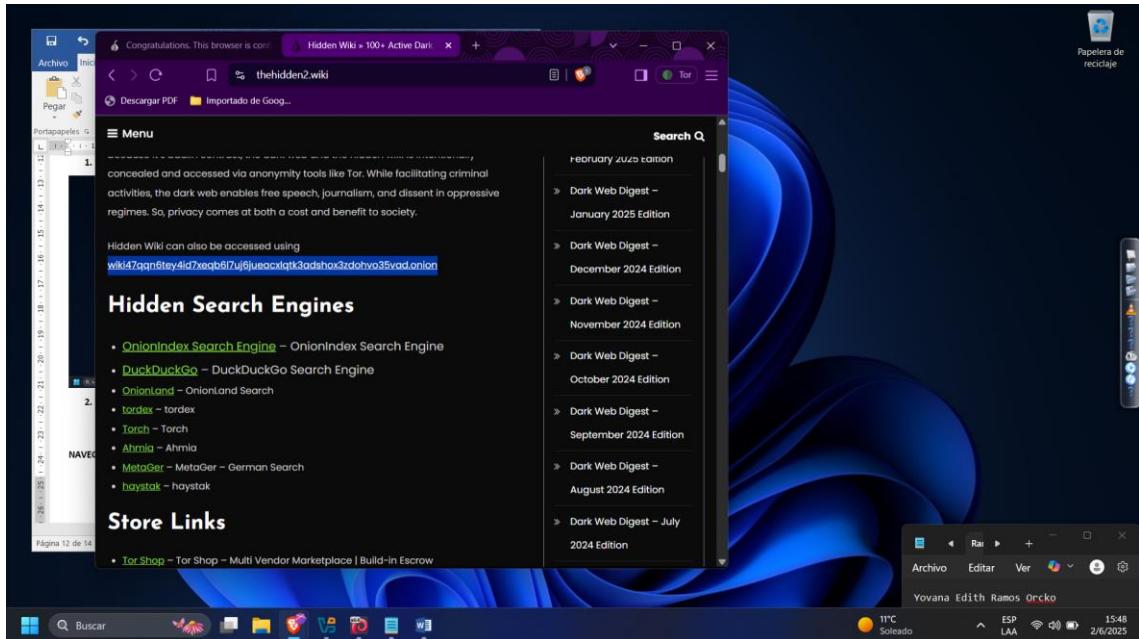
NAVEGADOR INTEGRADO CON TOR

1. Acceder a <https://thehidden2.wiki/>



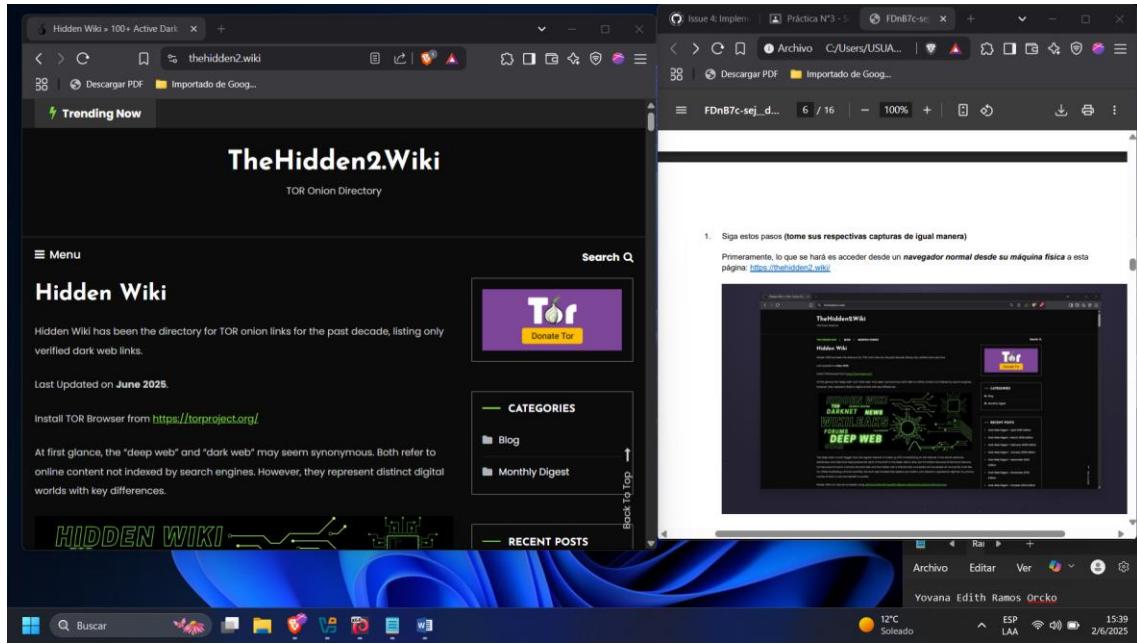
2. Enlace .onion original:

<http://wiki47qqn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion/>



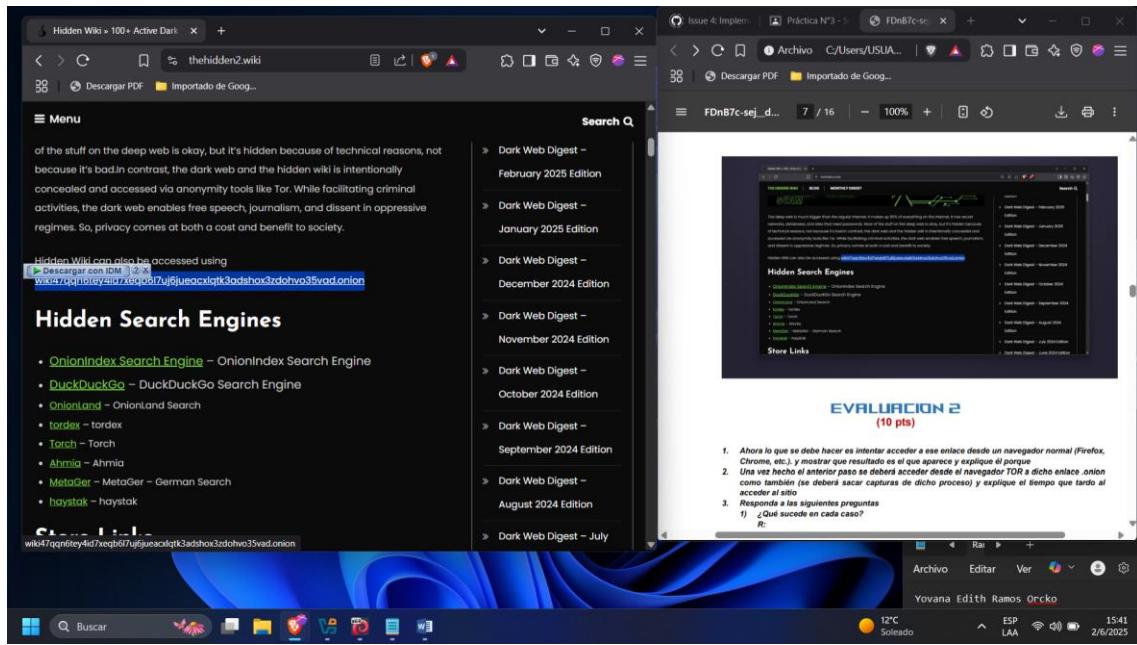
NAVEGADOR NORMAL

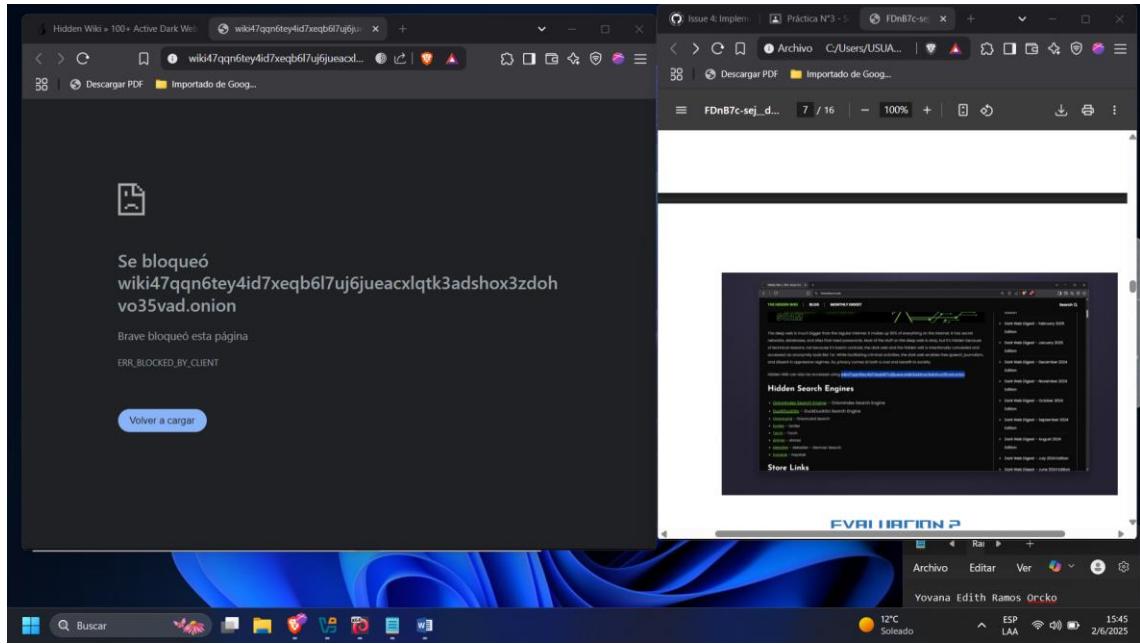
1. Acceder a <https://thehidden2.wiki/>



2. Enlace .onion original:

<http://wiki47qgn6tey4id7xeqb6l7uj6ueacxlqtk3adshox3zdohvo35vad.onion>



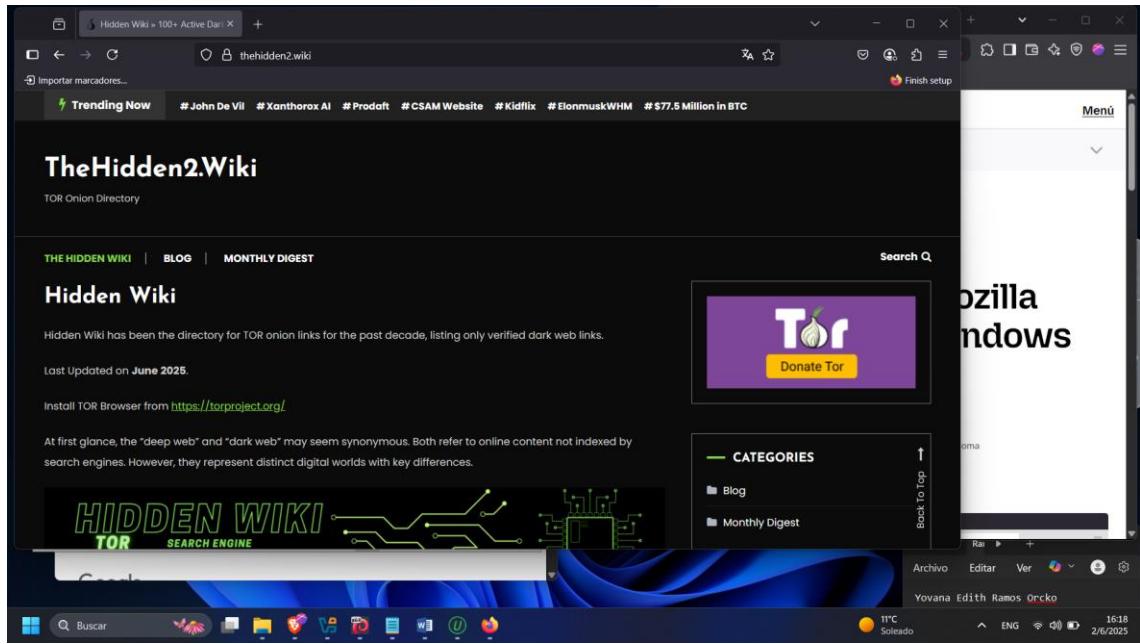


EVALUACION 2

1. Ahora lo que se debe hacer es intentar acceder a ese enlace desde un navegador normal (Firefox, Chrome, etc.). y mostrar que resultado es el que aparece y explique él porque

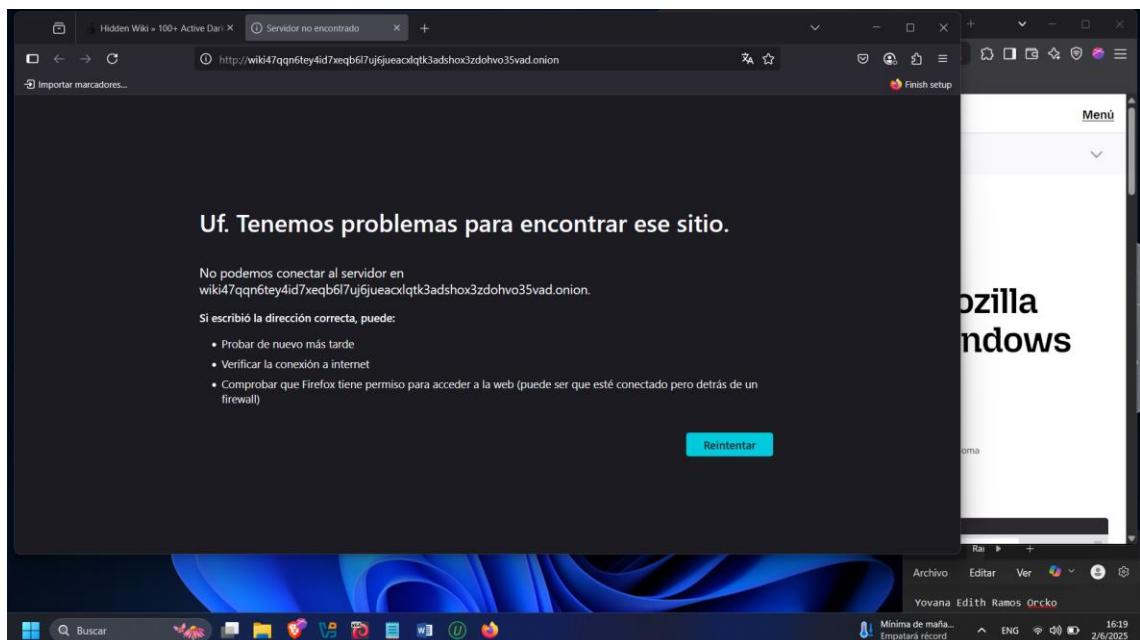
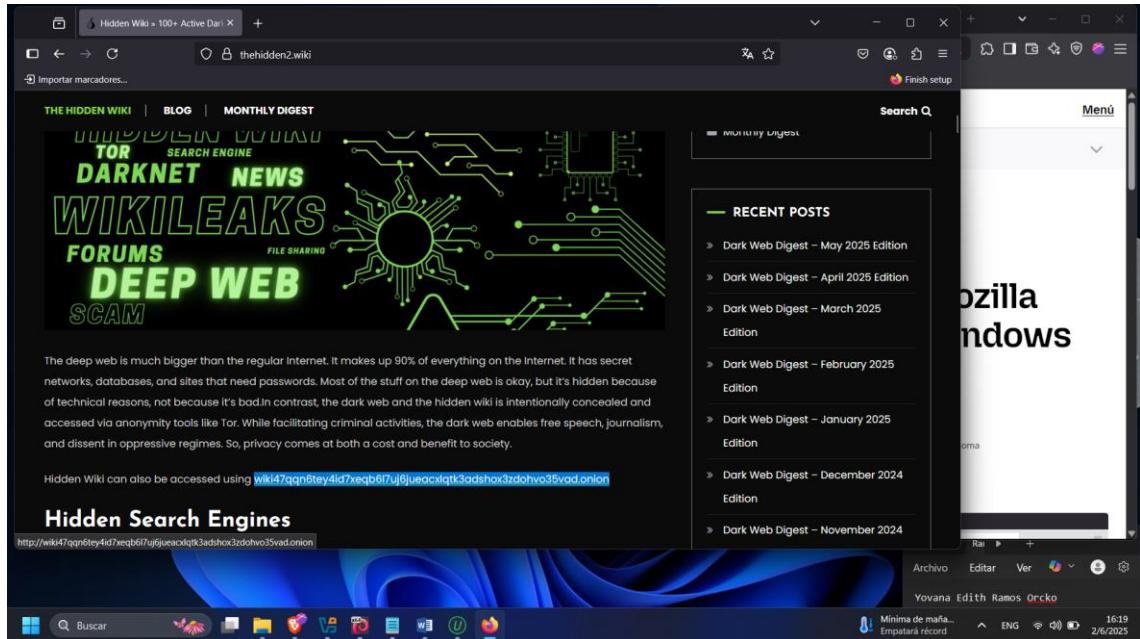
NAVEGADOR NORMAL FIREFOX

1. Acceder a <https://thehidden2.wiki/>



2. Enlace .onion original:

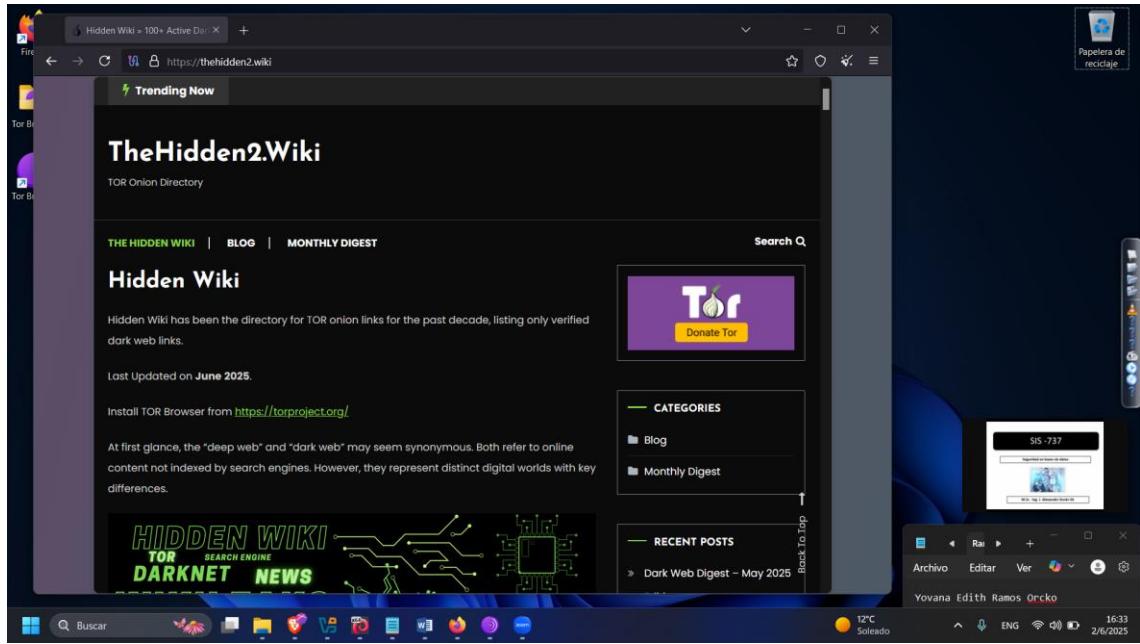
<http://wiki47qnn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion/>



2. Una vez hecho el anterior paso se deberá acceder desde el navegador TOR a dicho enlace .onion como también (se deberá sacar capturas de dicho proceso) y explique el tiempo que tardó al acceder al sitio

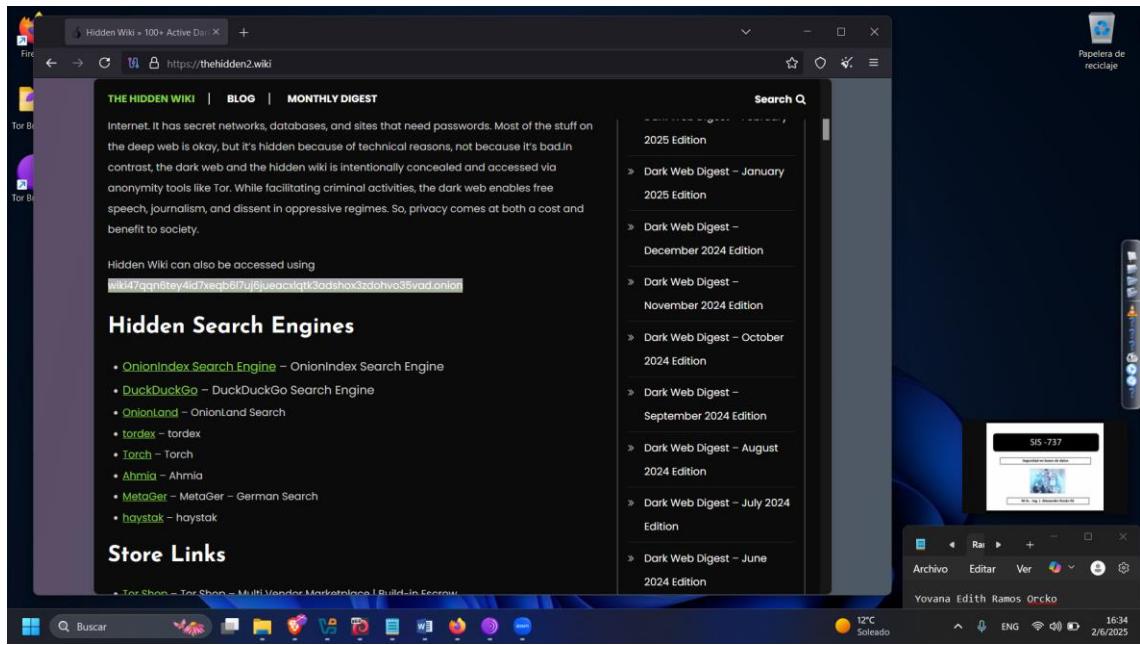
NAVEGADOR TOR

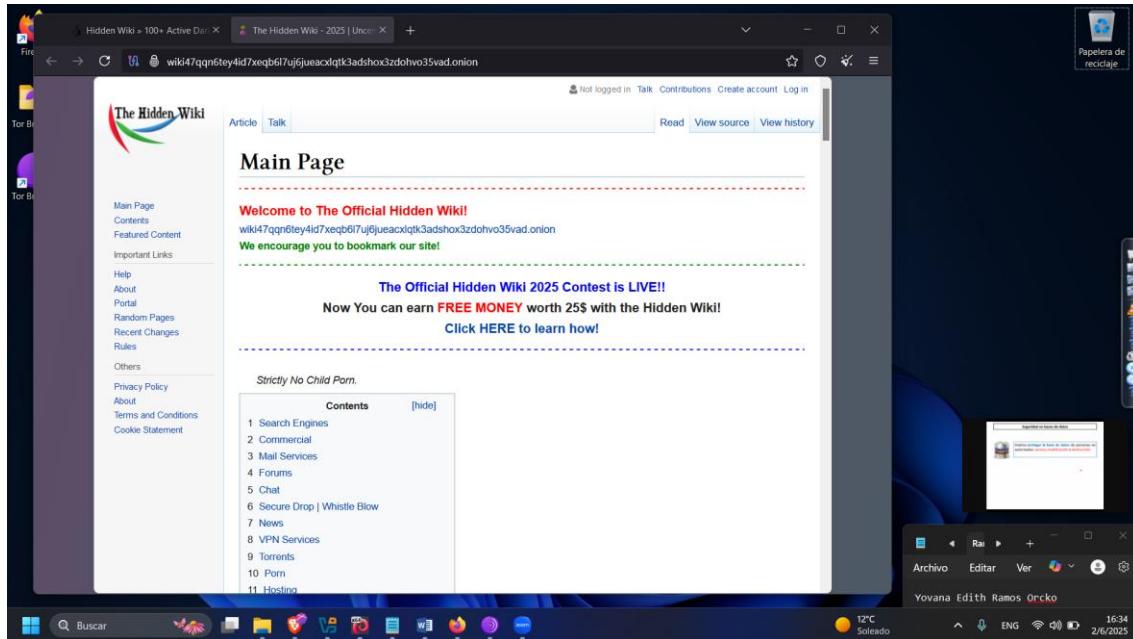
1. Acceder a <https://thehidden2.wiki/>



2. Enlace .onion original:

<http://wiki47qgn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion/>





Tarda menos de 10 segundos en cargar el enlace original.

3. Responda a las siguientes preguntas

1) ¿Qué sucede en cada caso?

El navegador Firefox normal no puede acceder al enlace de .onion original, por lo que solo muestra que no se puede acceder a esta página, además porque no existe esa dirección en la red de internet pública.

En el navegador Tor, la misma dirección carga correctamente, aunque toma más tiempo en cargar que en la web tradicional.

2) ¿El navegador normal si accede / no accede? Explique qué es lo que sucede y justifique la respuesta

El navegador normal no accede. Las direcciones .onion están en la red Tor (deep web), ya que requieren una conexión especial que enrute el tráfico a través de la red Tor, lo cual un navegador normal no hace.

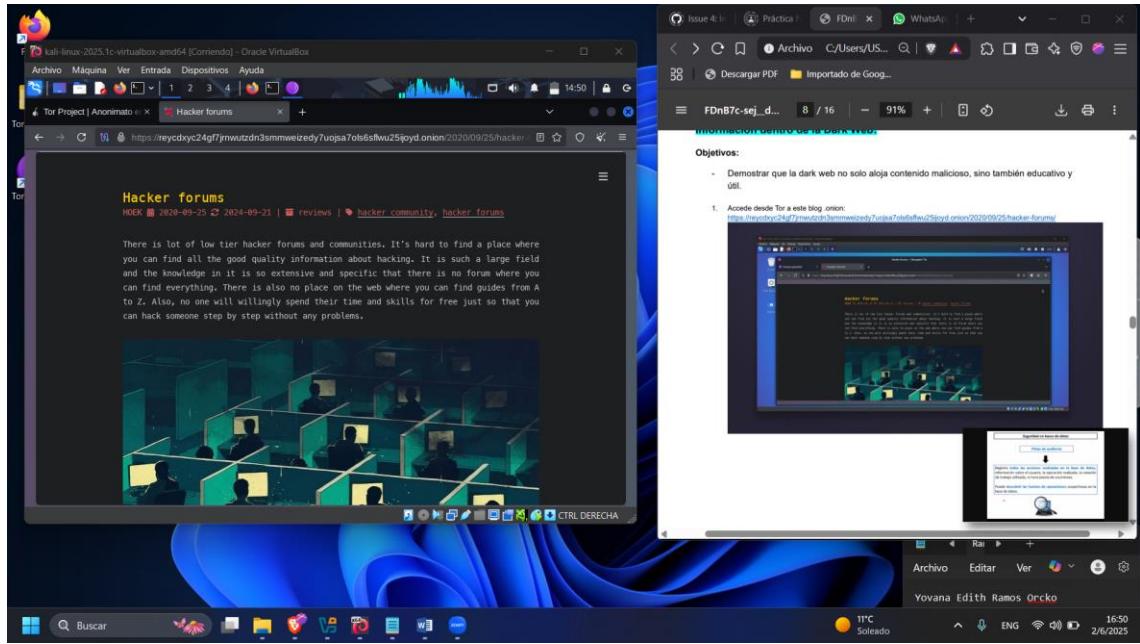
3) ¿Qué rol tiene la red Tor en este proceso? Explique por qué es importante usar el navegador TOR

La red Tor actúa como una red de anonimato. Su uso es esencial para proteger la identidad del usuario, acceder a sitios censurados o anónimos y evitar rastreo.

PARTE 3

1. Accede desde Tor a este blog .onion:

<https://reycdxyc24gf7jrnwutzdn3smmweizedy7uojsa7ols6sflwu25ijoyd.onion/2020/09/25/hacker-forums/>



2. Responda a las siguientes preguntas

1) ¿Qué es lo que dice el autor de este blog?

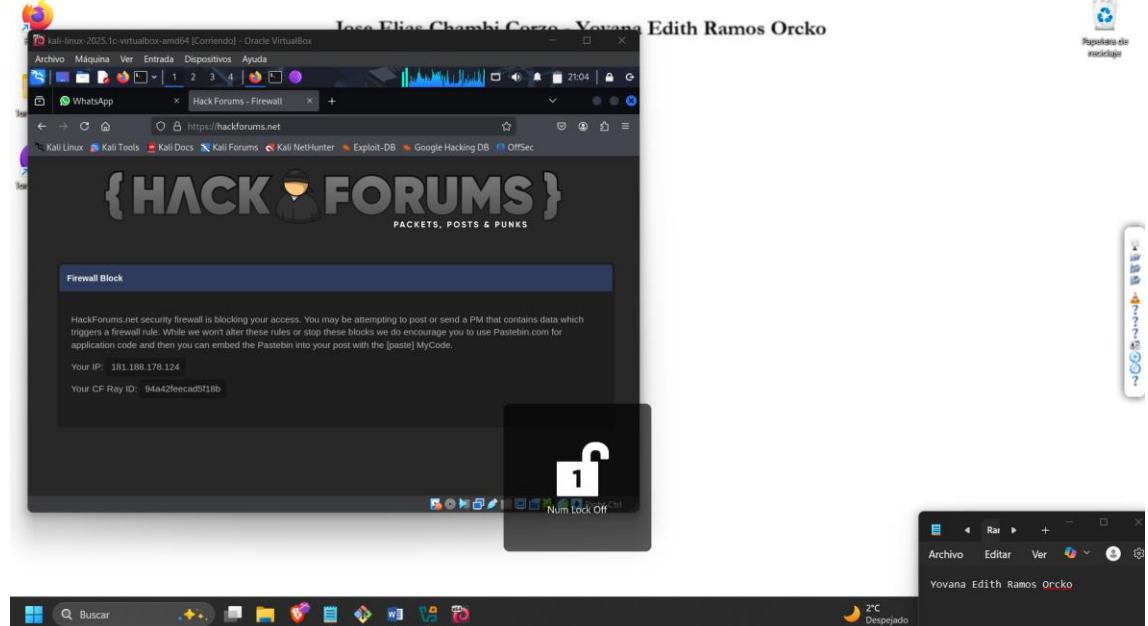
Indica que los foros de hacking no ofrecen guías completas ni soluciones mágicas.

Aprender hacking requiere conocimiento en redes, programación y mucha práctica., por lo que recomienda no confiar en todo lo que se ve y usar los foros como apoyo para aprender, no como fuente principal.

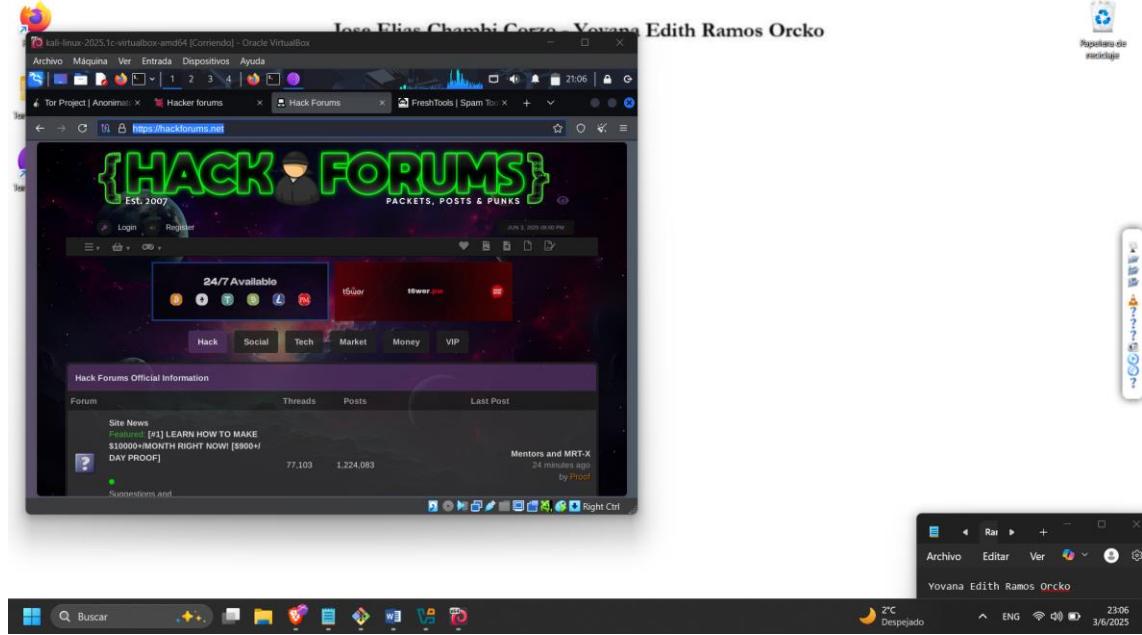
2) Pruebe abriendo el enlace .onion en un navegador normal, ¿El un navegador normal si accede / no accede? Explique qué es lo que sucede y justifique la respuesta

No accede a enlaces .onion un navegador normal porque pertenecen a la red Tor, que requiere un navegador especial. Ademas se observa de que estos dominios no están en el DNS público y solo funcionan dentro de la red Tor.

Accediendo por navegador normal a <https://hackforums.net>



Accediendo por la red tor a <https://hackforums.net>



3) ¿Qué rol tiene la red Tor en este proceso? Explique por qué es importante usar el navegador TOR en estos sitios web o blogs (según lo que navego dentro de los enlaces que tiene el blog)?

El rol de la red Tor en este proceso es que permite acceder a sitios .onion de forma anónima y segura. Además de que es importante usar el navegador Tor para proteger la identidad del usuario y poder entrar a este tipo de sitios, como los foros mencionados en el blog.

4) ¿Qué enlaces de los que habla el autor de este blog le pareció más interesante? Saque capturas del sitio que encontró interesante y explique porque

Me parecio mas interesante el enlace Hack Forums (<https://hackforums.net/>) ya que tiene muchos temas técnicos, debates sobre ciberseguridad y recursos educativos.

2. Responde a los siguientes preguntas:

- 1) ¿Qué es lo que dice el autor de este blog?

Indicar que los foros de hacking no ofrecen guías completas ni soluciones mágicas. Aprender hacking requiere conocimiento en redes, programación y mucha práctica, por lo que recomienda no confiar en todo lo que se ve y usar los foros como apoyo para aprender.

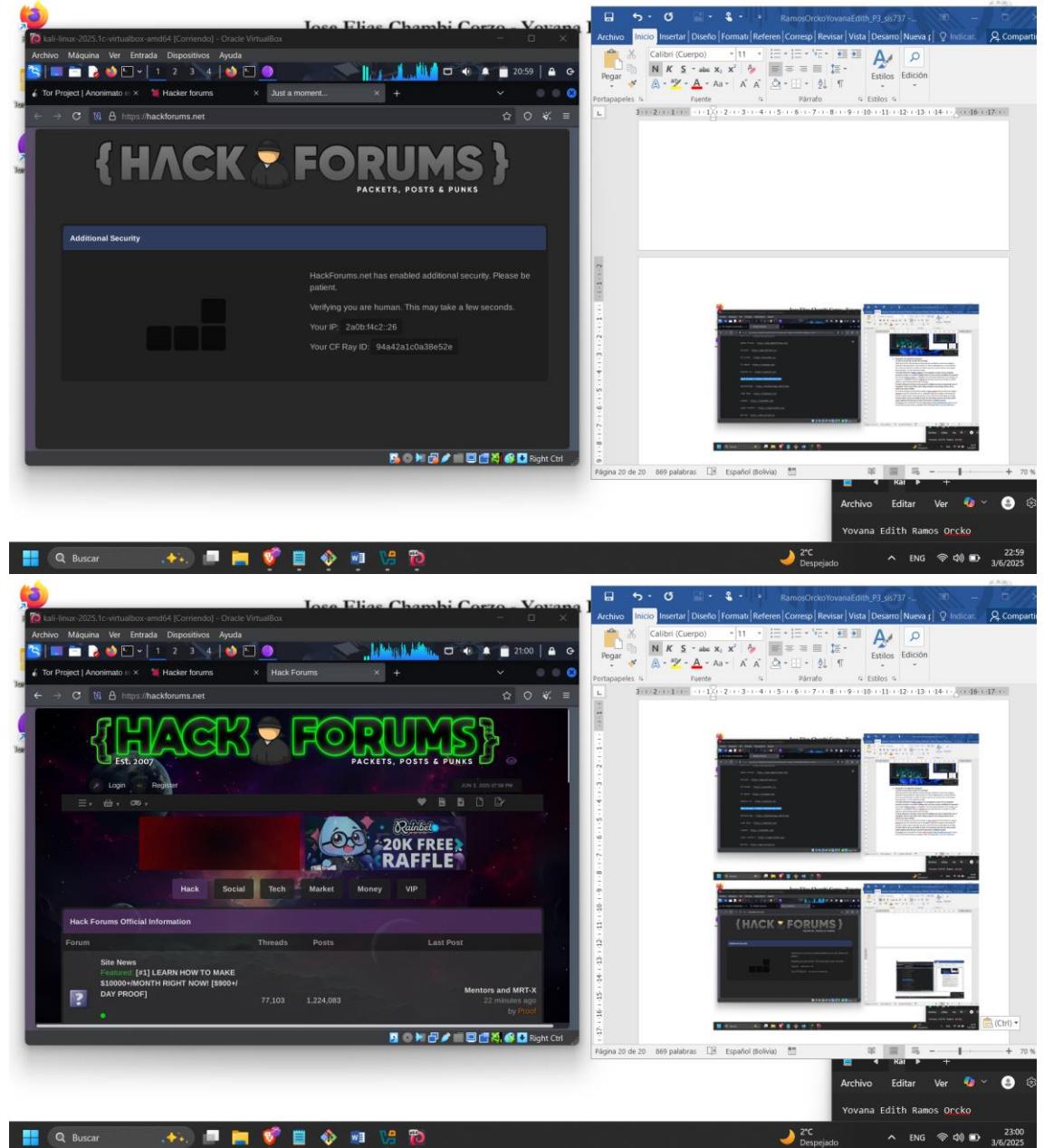
- 2) Prueba abriendo el enlace adjunto en un navegador normal, (en un navegador normal si accede / no accede). Explícate qué es lo que sucede y justifícalo la respuesta No accede a <https://reycodex24g7jmrwutzd3smmeizedy7uojsa7ols6sfwu25jyod.onion> porque pertenece a la red Tor, que responde a <https://www.reyez.net> y que estos dominios no están en el DNS público y solo funcionan dentro de la red Tor.

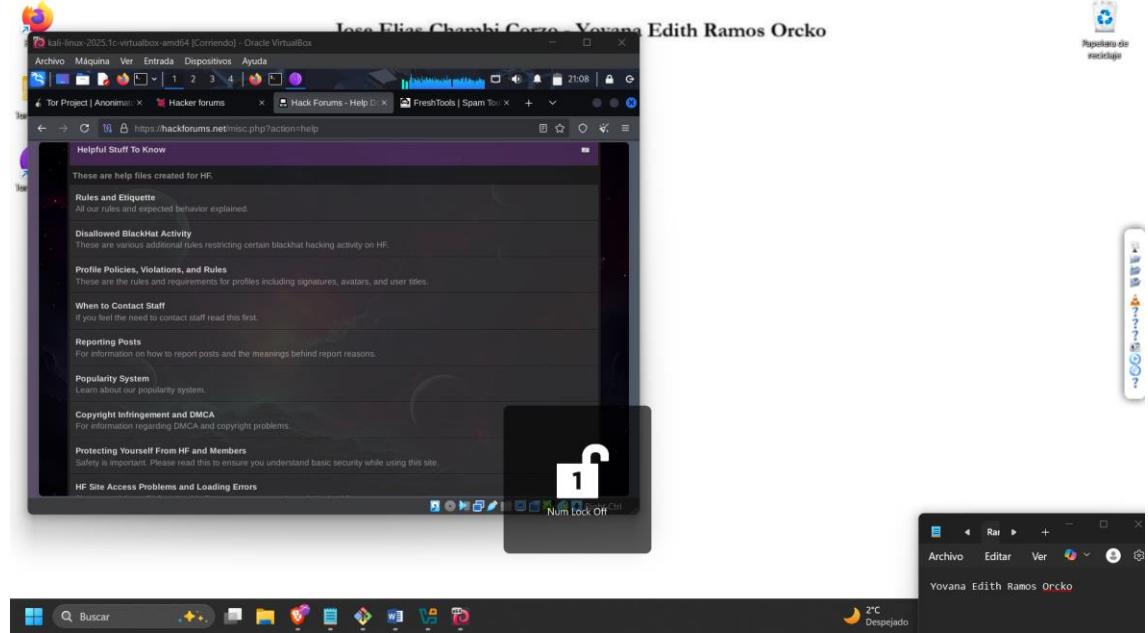
- 3) ¿Qué rol tiene la red Tor en este proceso? Explícate por qué es importante usar el navegador TOR en estos sitios web o blogs. Elegí los que consideras más interesantes los enlaces que tiene el blog?

El rol de la red Tor es que permite acceder a sitios de foros anónimos y segura. Además de que es importante usar el navegador Tor para proteger la identidad del usuario y poder entrar a este tipo de sitios, como los foros mencionados en el blog.

- 4) ¿Cuáles enlaces de los que habla el autor de este blog le pareció más interesante? Selecciona cuales del sitio te parecieron más interesante y explícalo porque

Más interesante me parecio el enlace <https://hackforums.net/> ya que tiene muchos temas tecnicos, debates sobre ciberseguridad y recursos educativos.

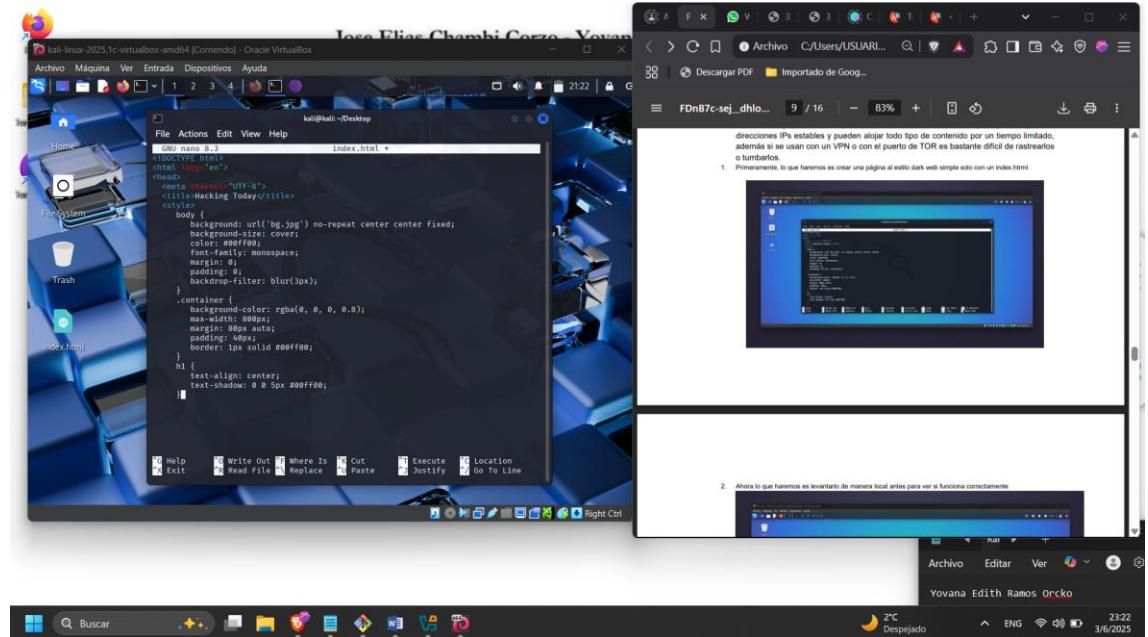




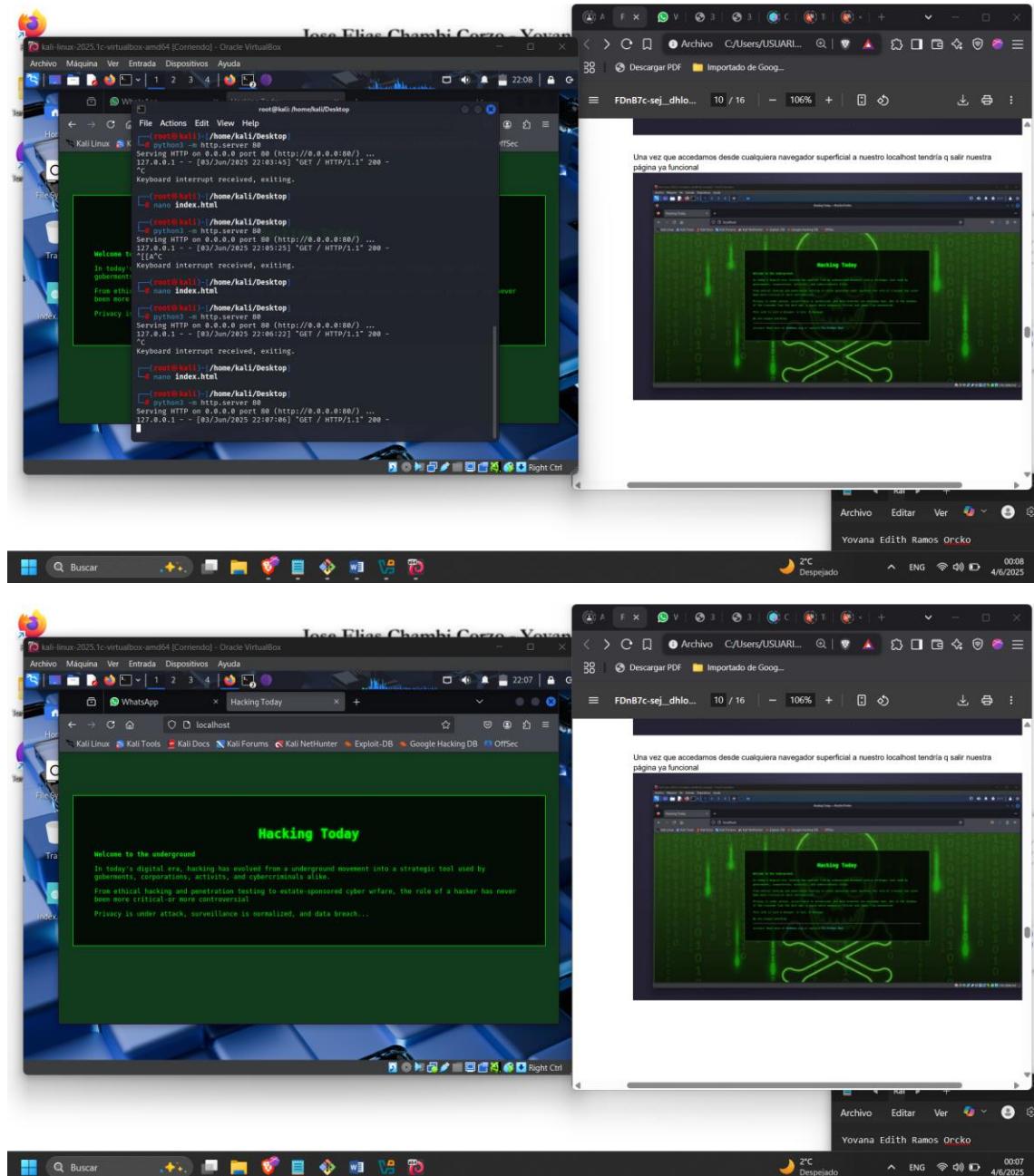
PARTE 4

Creacion de servidores onion

1. Crear página dark web



2. Levantarla de manera local



Ir a archivo de configuración que tiene TOR

```

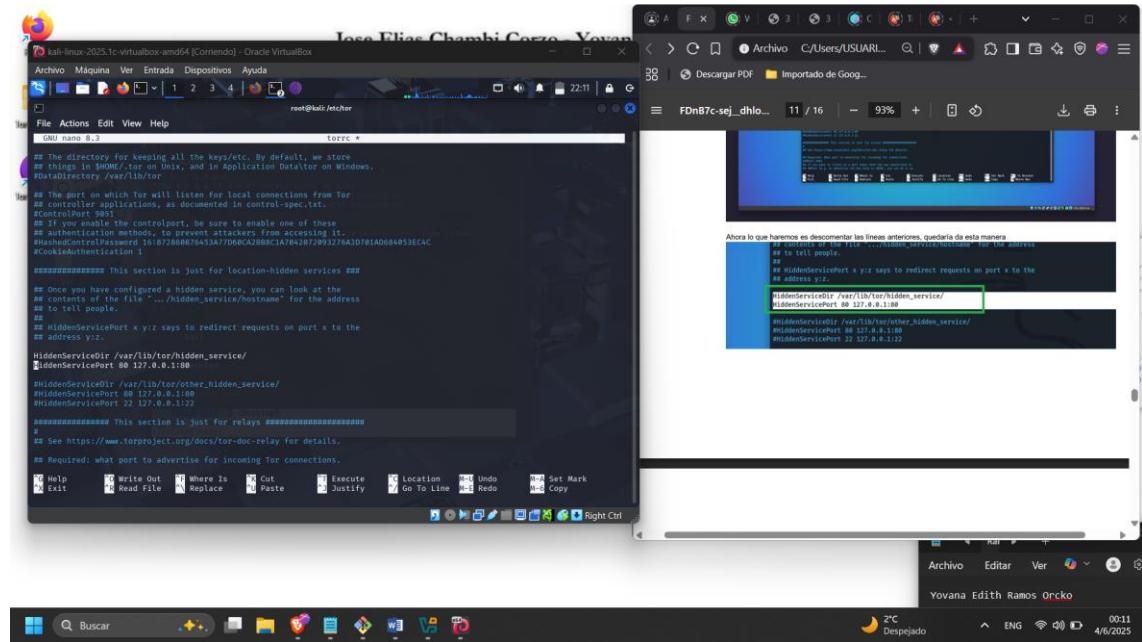
root@kali:~# nano torrc
# The directory for keeping all the keys/etc. By default, we store
# things in $HOME/.tor on Unix, and in Application Data on Windows.
#HiddenServiceDir /var/lib/tor/hidden_service
#HiddenServicePort 80 127.0.0.1:80
#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22
# This section is just for location-hidden services #
# Once you have configured a hidden service, you can look at the
# contents of the file ".../hidden_service/hostname" for the address
# to tell people.
# If you enable the controlport, be sure to enable one of these
# methods to prevent attackers from accessing it.
#HashedControlPassword 161872868676453A77D0BCA298C1A7A842872B93272A63D781AD684053EC4C
#CookieAuthentication 1

# This section is just for relays #
# See https://www.torproject.org/docs/tor-doc-relay for details.
# Required: what port to advertise for incoming Tor connections.

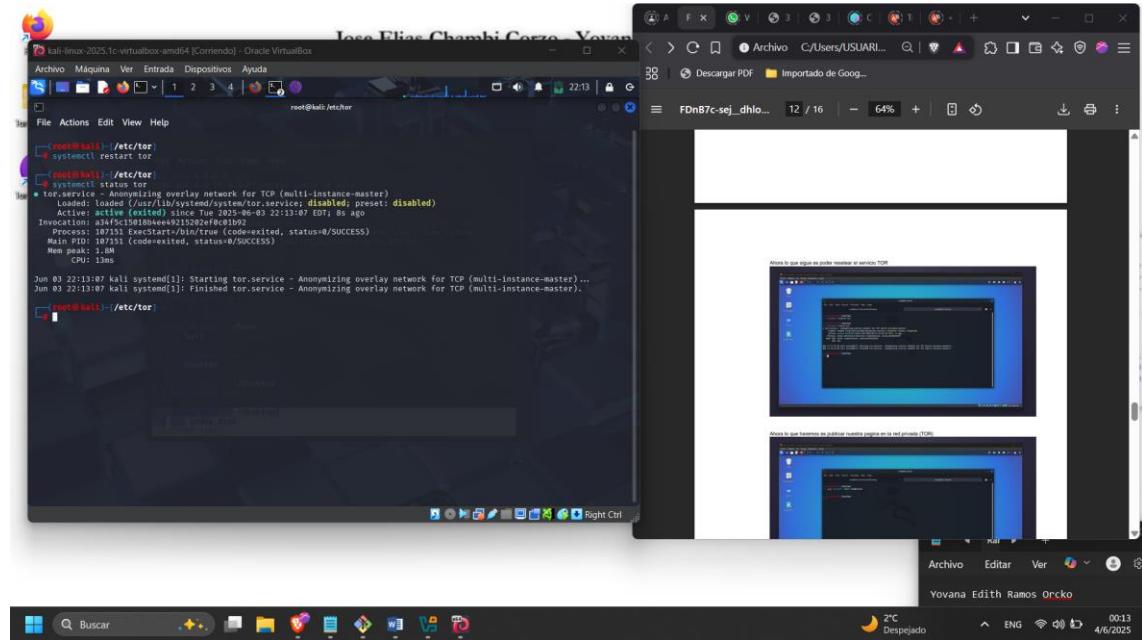
# Help           # Write Out   # Where Is   # Cut        # Execute      # Location    # Undo       # Set Mark
# Exit          # Read File  # Replace   # Paste      # Go To Line  # Redo       # Copy

```

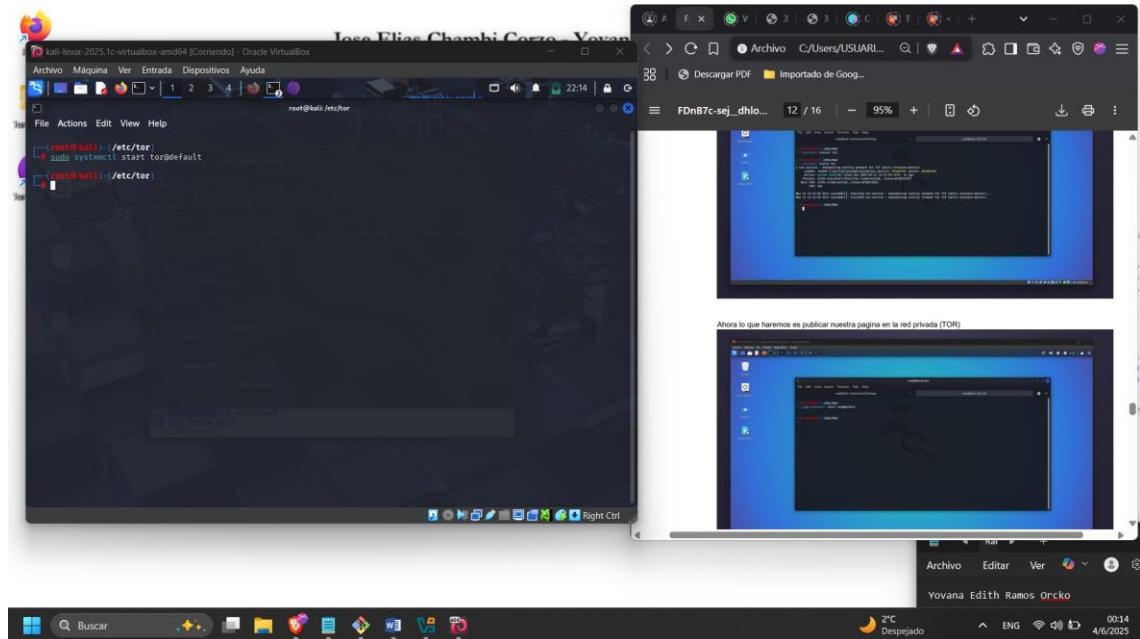
Descomentar las líneas



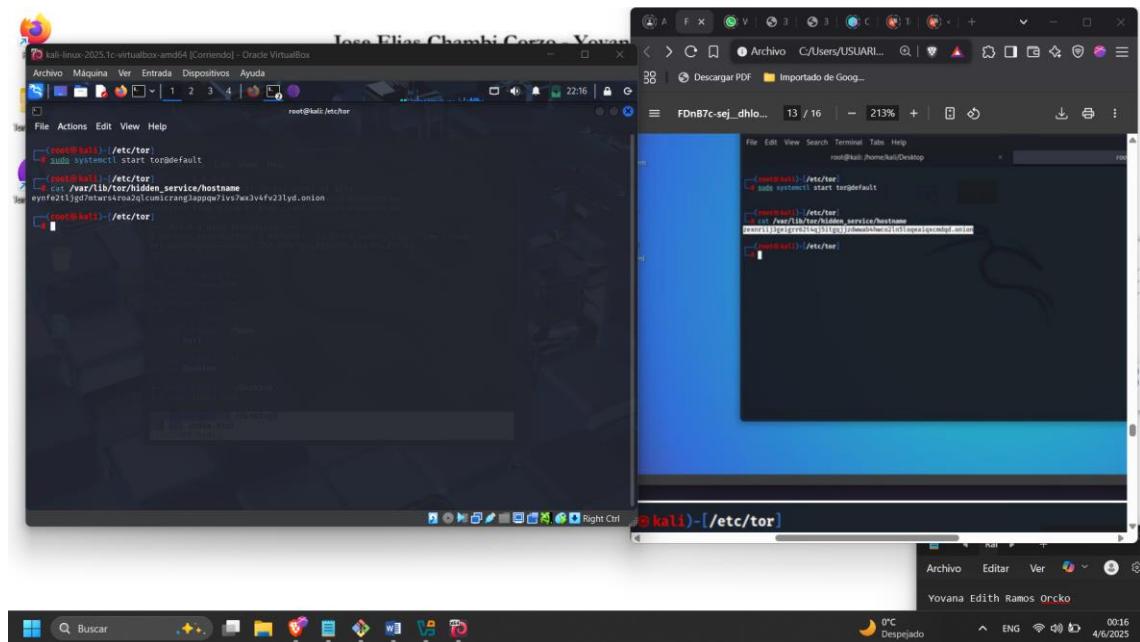
Resetear TOR



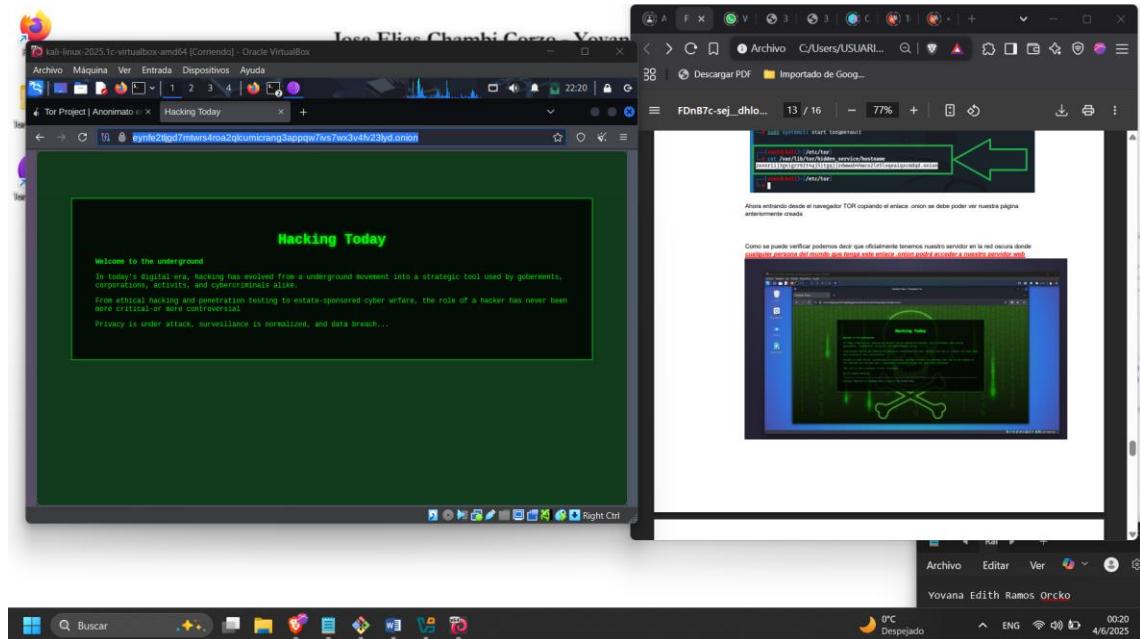
Publicar la página en la red TOR



Observar en que sitio se encuentra en el enlace .onion la pagina



Entrar al navegador TOR copiando el enlace .onion



EVALUACION 3

Recursos:

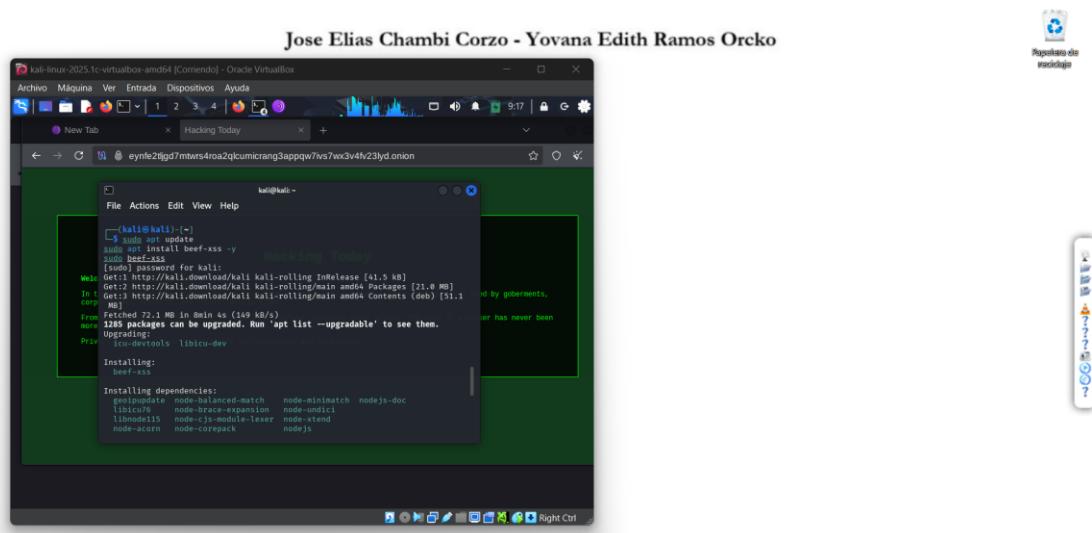
Servidor -> KaliLinux 2025.1 modo NAT

Cliente -> KaliLinux 2022.4 modo Bridged

Misma red de entorno

Simular a un atacante que analiza una víctima mediante Tor.

- Instalar y configurar Beef en el servidor



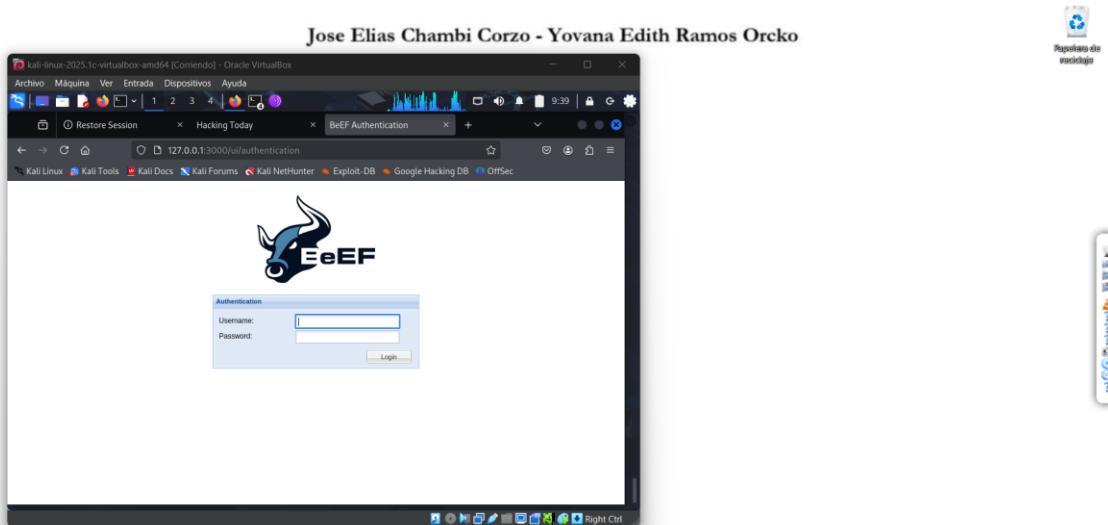
Te pedirá un password, debes anotarla y luego se observa que el servicio Beef está iniciando normalmente

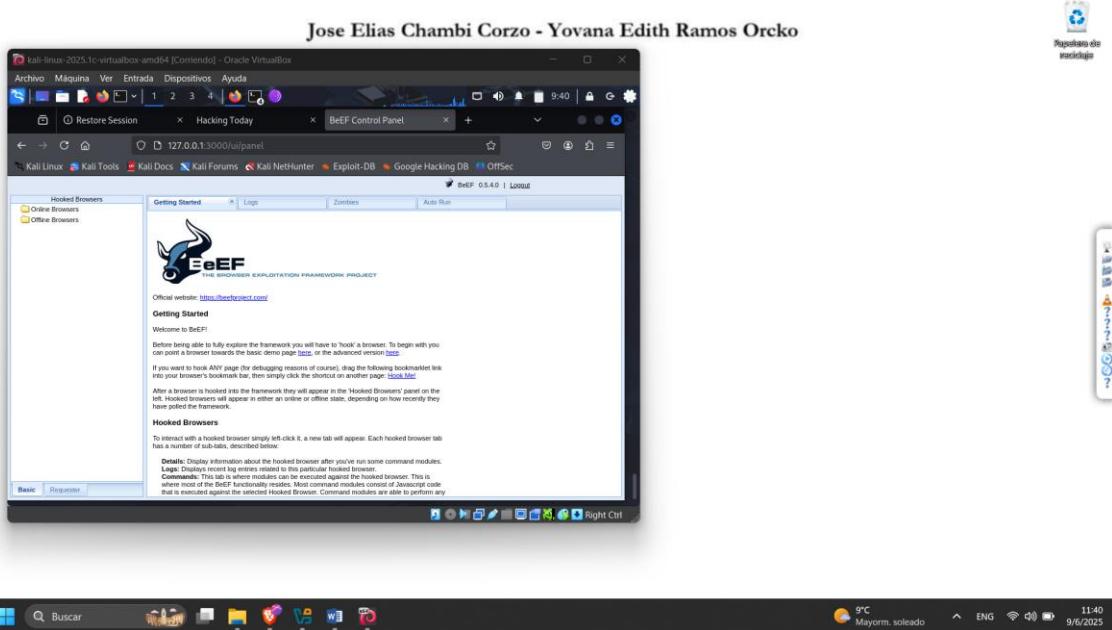


Ahora debes abrir el link en el navegador

```
[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5 ... 4 ... 3 ... 2 ...
1 ...
```

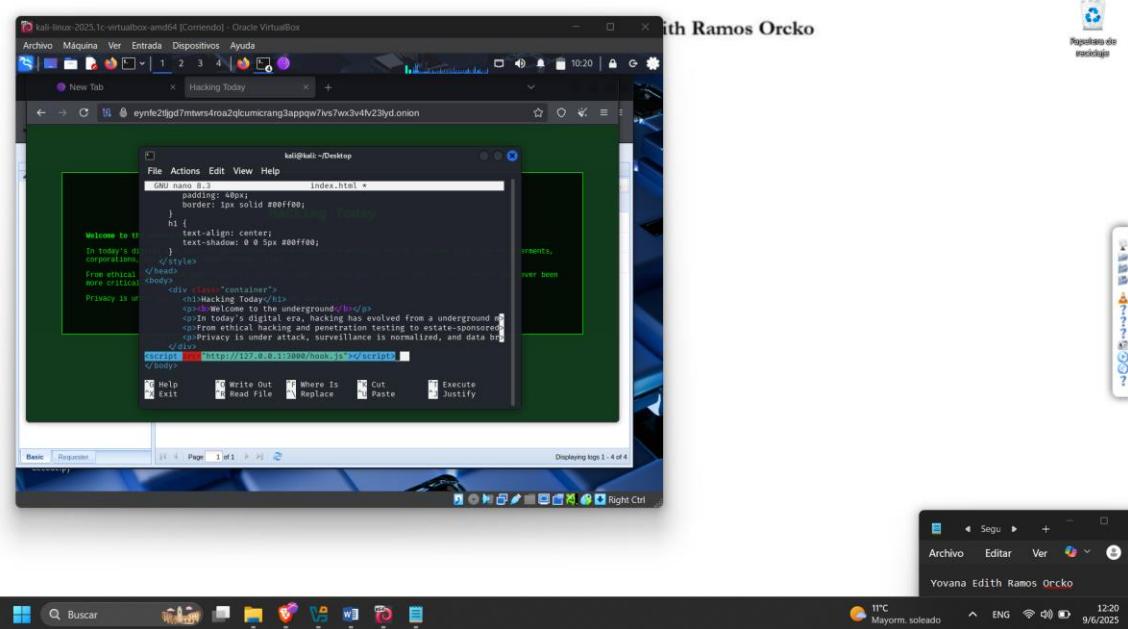
Navegador del servidor user: beef password:(la contraseña que puso cuando se le pidió)



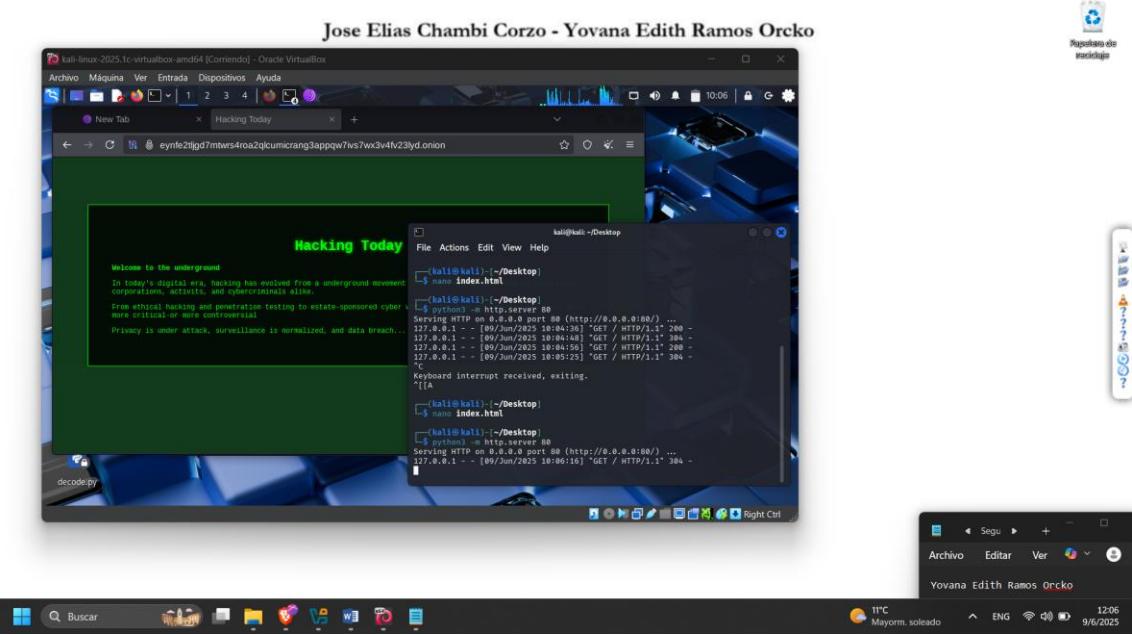


El **hook** de BeEF es un pequeño script que **conecta el navegador de la víctima al servidor BeEF**, permitiendo que puedas controlar y lanzar ataques desde la interfaz web de BeEF

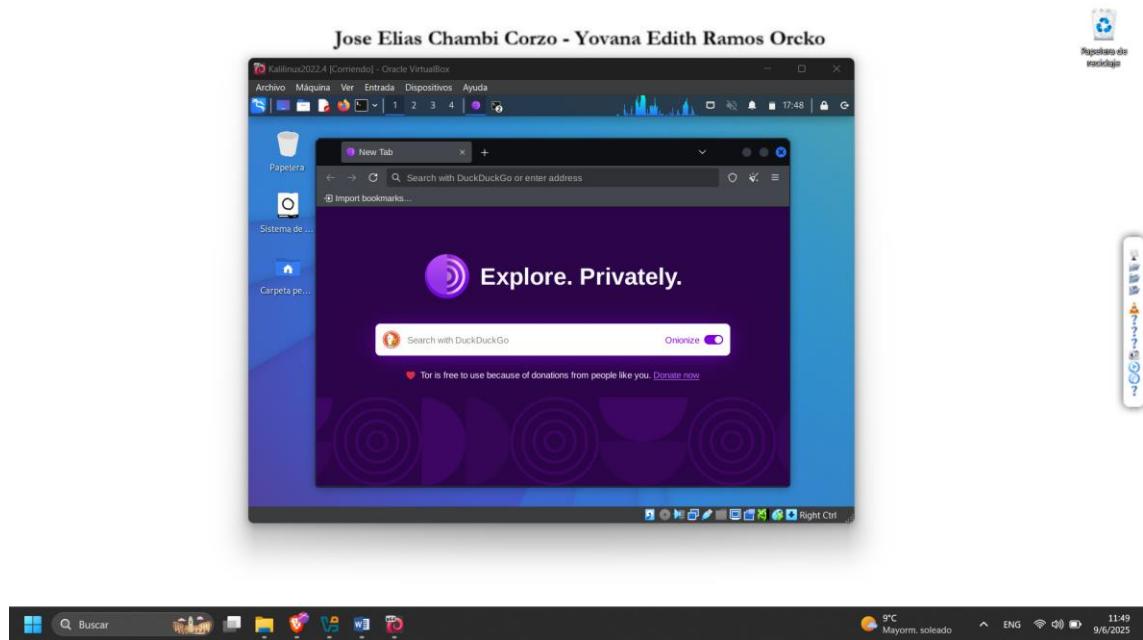
Modificar el archivo **index.html** y agregar el script del hook



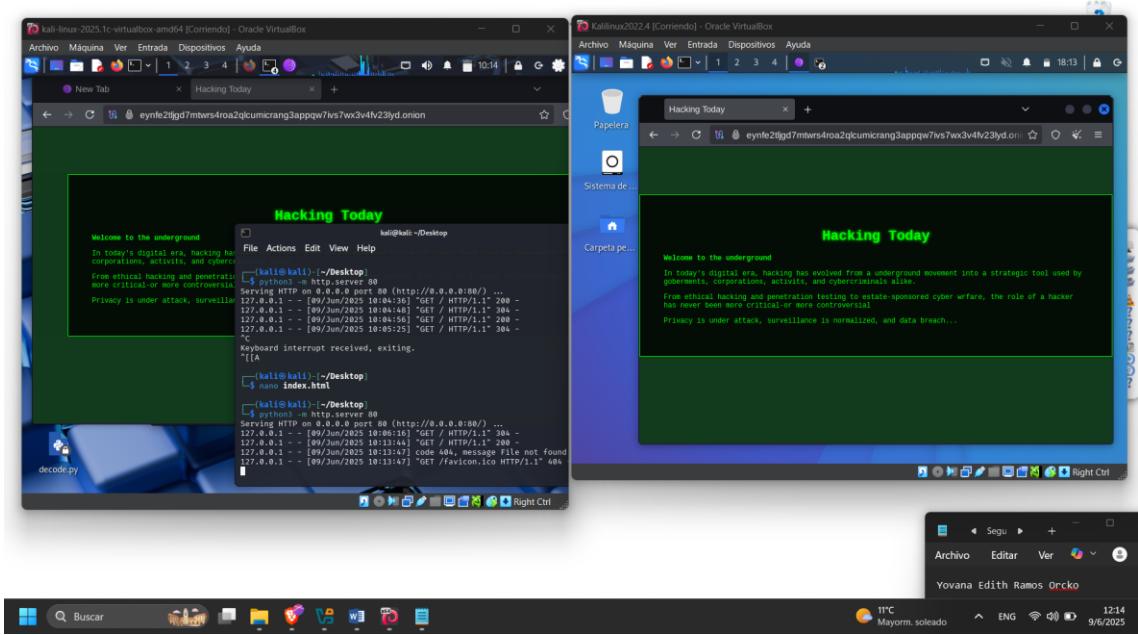
Verificar que el servidor web sigue levantado



Cliente Kalilinux conectado a Tor (como ya se tiene los pasos que se debe tener para obtener el navegador Tor, simplemente se mostrara que la maquina cliente está conectado al navegador Tor)



Una vez dentro ingresar a la dirección. onion que proporciona el servidor



Ahora el script será <script src="hook.js"></script> en index.html es y al volver a cargar la pagina .onion se obtiene esto del cliente, se llena la información para probar lo siguiente

