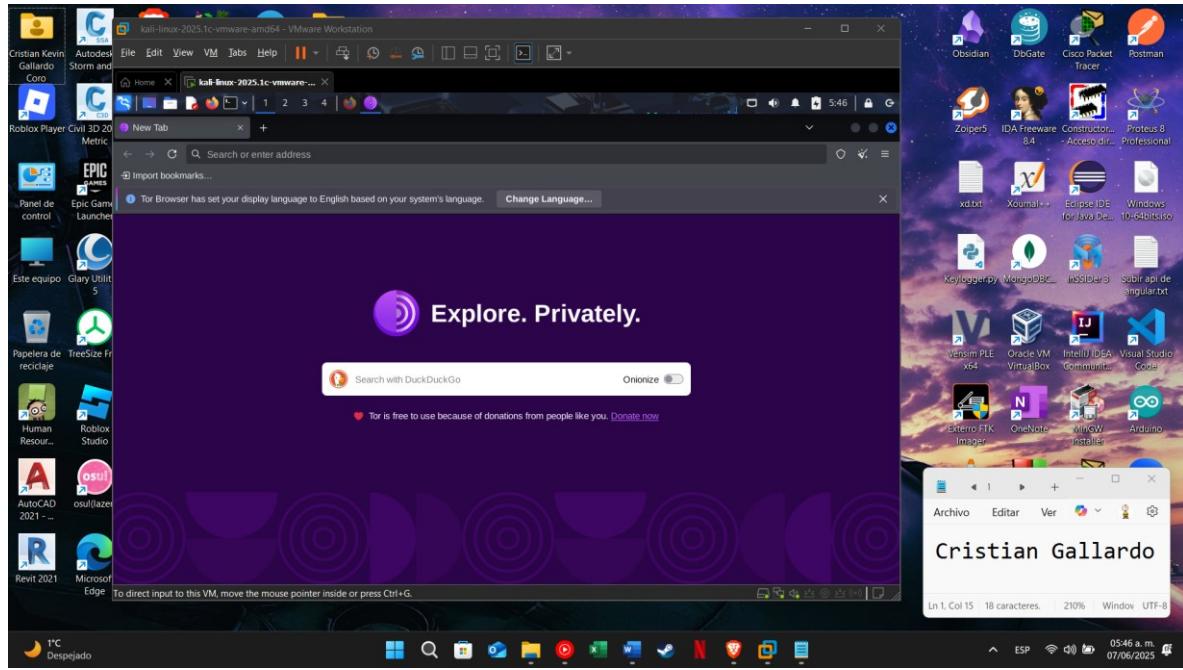


Practica Nro 3

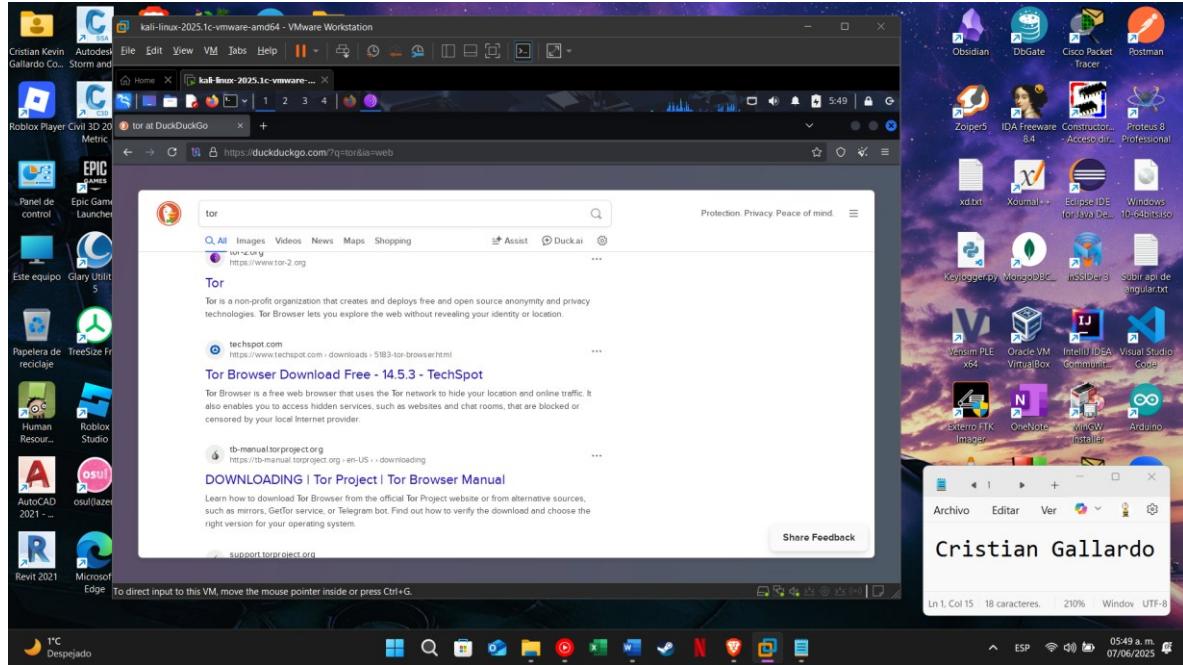
Univ. Cristian Kevin Gallardo Coro

PARTE 1

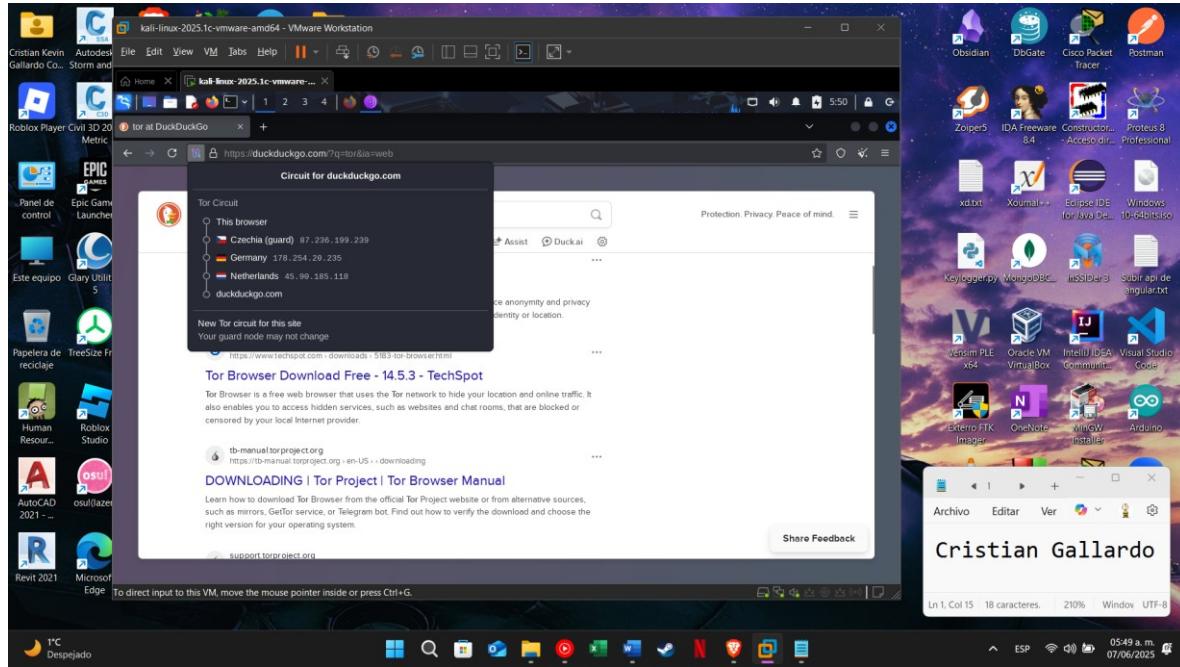
- Instalamos tor en Kali Linux



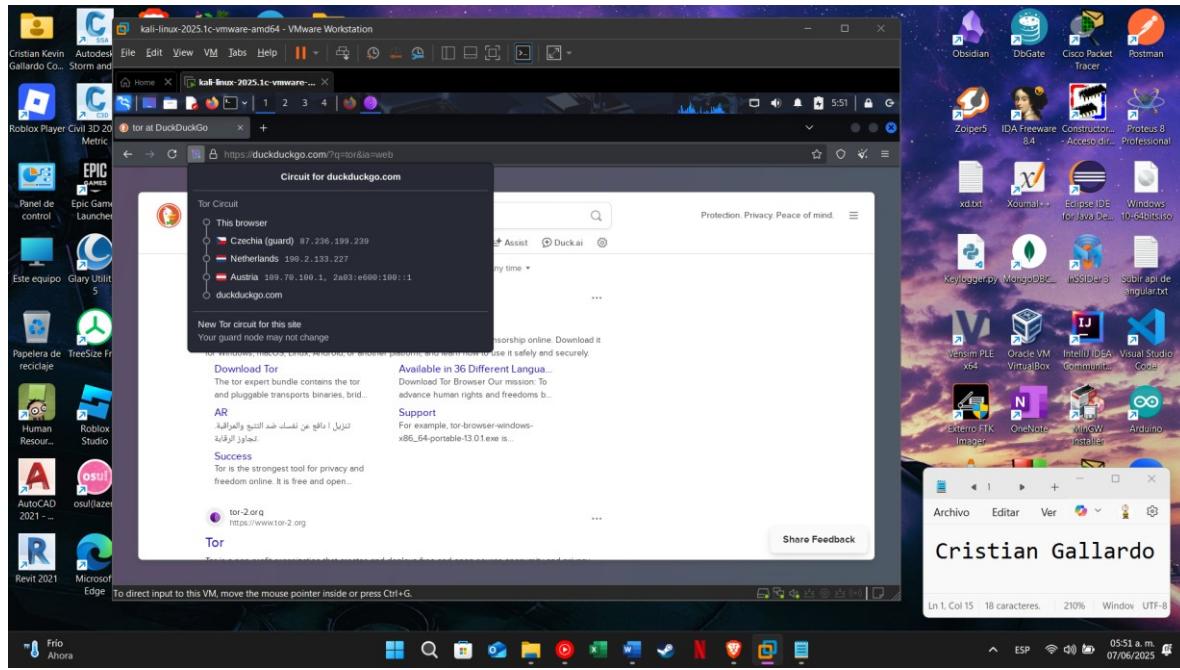
- Buscamos una página cualquiera



- Vemos las IPs por las cuales pasamos



- Presionamos en new tor circuit for this site, y vemos como se cambian los países

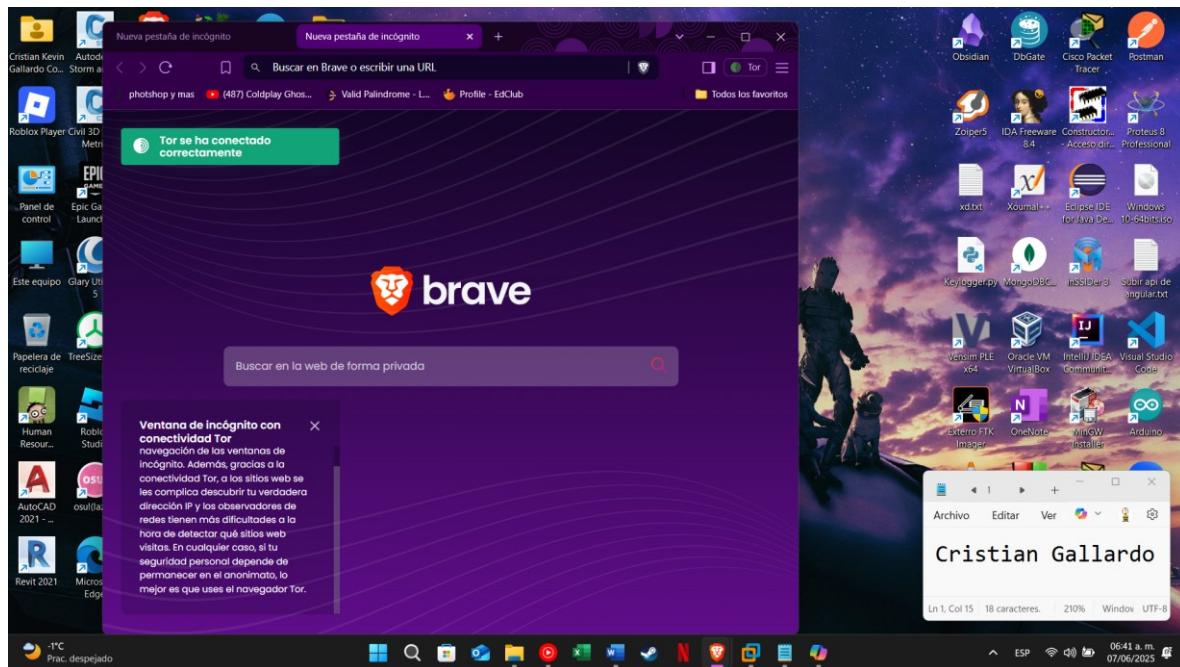
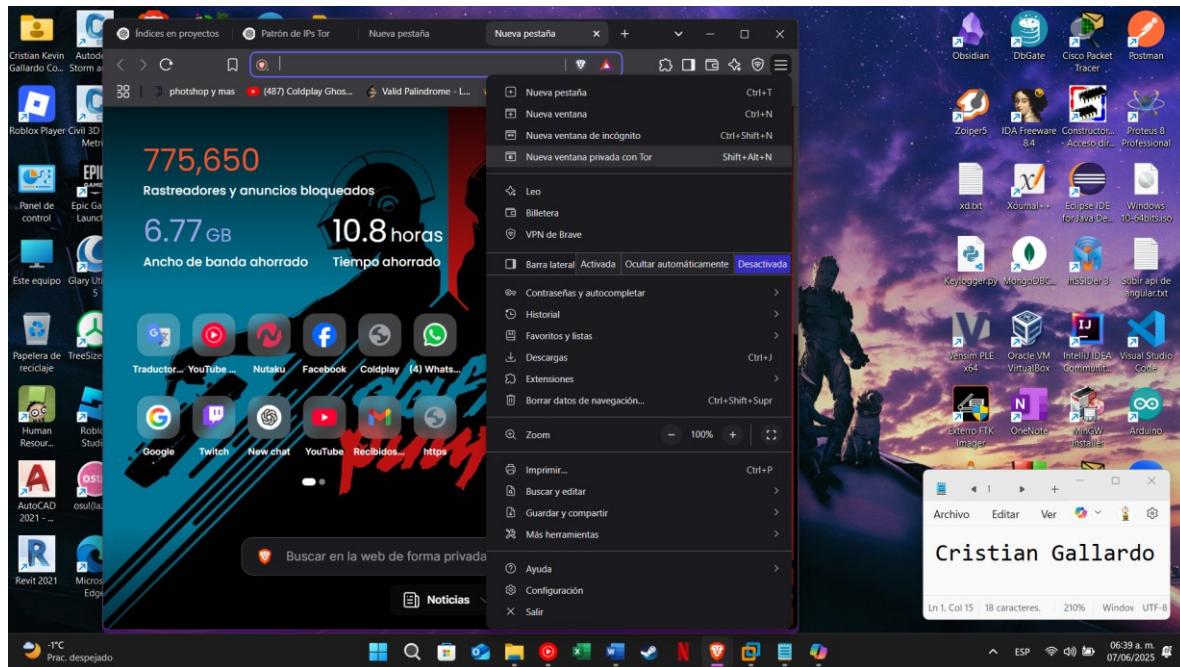


EVALUACION 1

1. Aparecen ciertos países más seguido, debido a su mayor permisividad en el anonimato y también porque estos VPNs tiene sus servidores alojados en estos países
2. Aparte de que se repitan ciertos países, no parece haber un patrón que estos sigan en específico, algo para mencionar podría ser que primero pasa por una IP de bajo valor como

40.X.X.X o 80.X.X.X y generalmente son seguidos por IPs de alto valor como 193.X.X.X o 185.X.X.X

3. El navegador Brave tiene una función, la cual le permite su conexión de manera incógnita mediante su modo tor, el cual bien no tiene todas las opciones que brinda Tor, como la de cambiar de IPs, puede servir como alternativa a este



PARTE 2

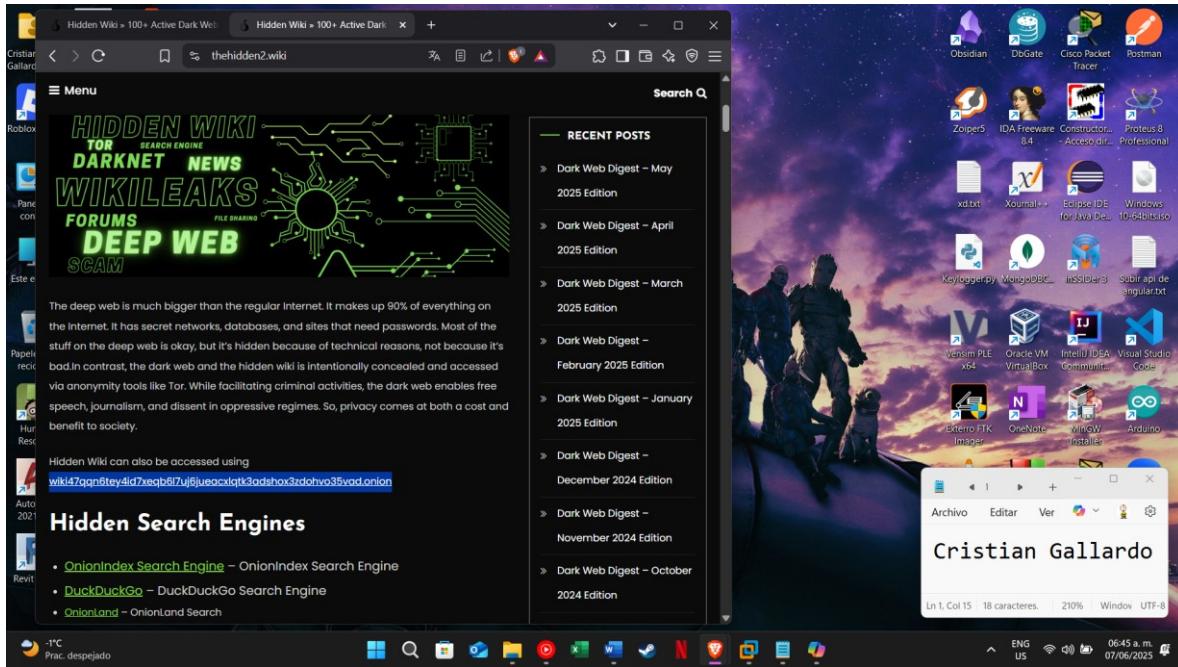
- Ingresamos a Nuestro navegador de preferencia



- Buscamos el enlace mencionado por la practica

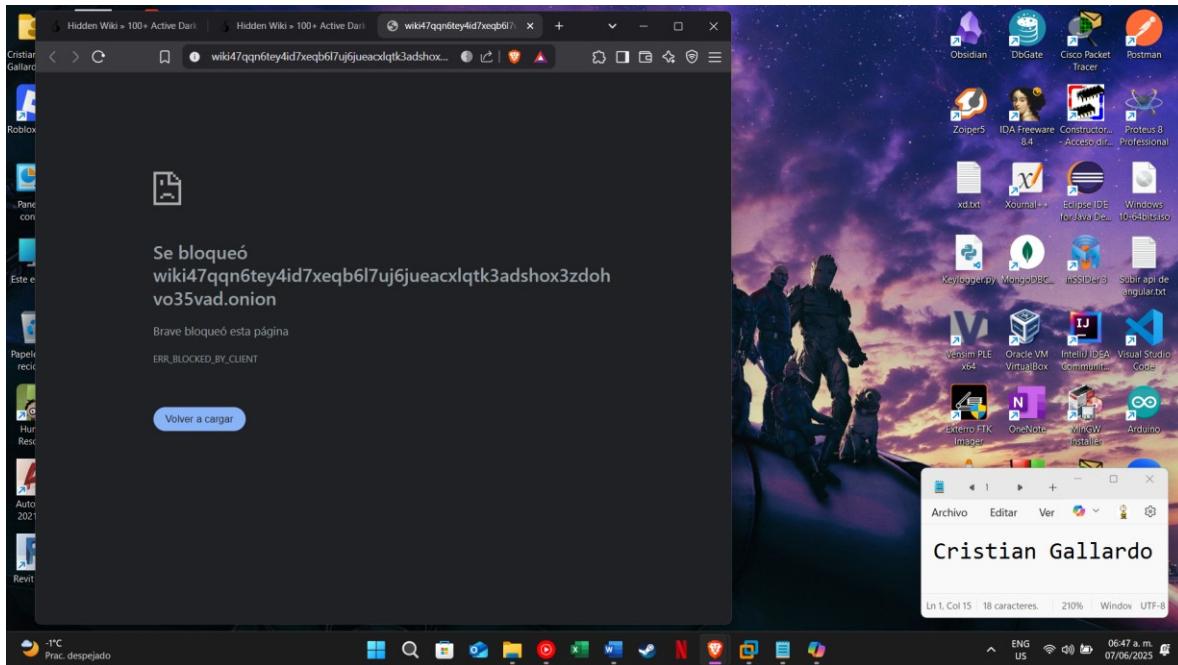


- Buscamos en la pagina el enlace hacia la verdadera pagina .onion

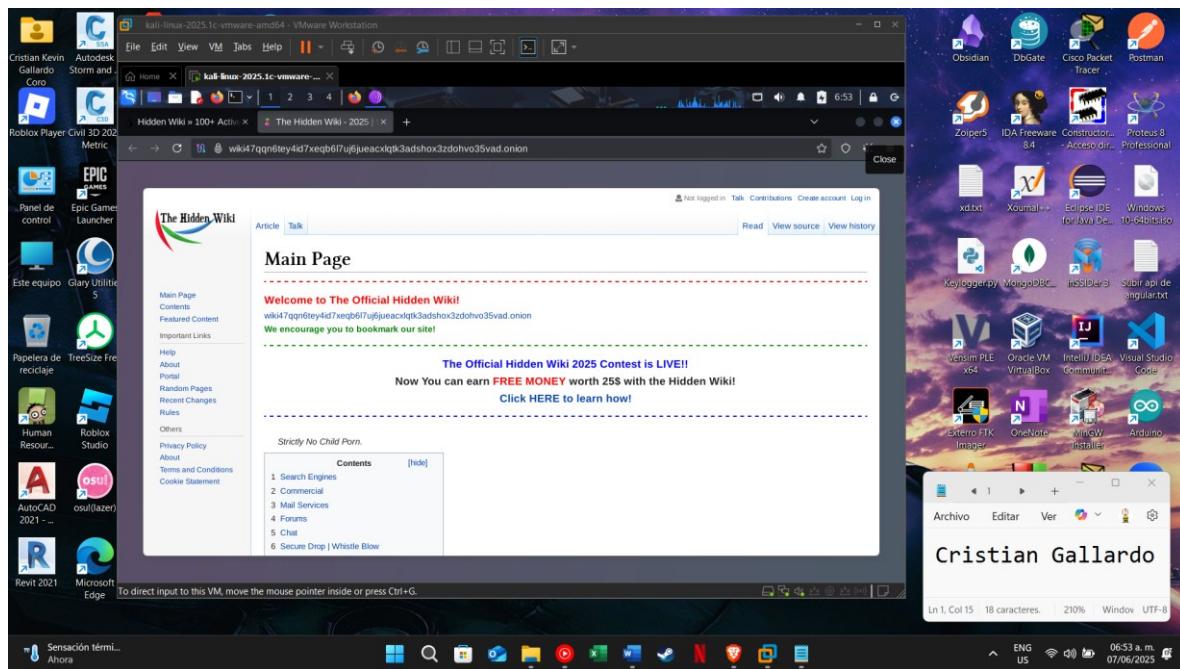
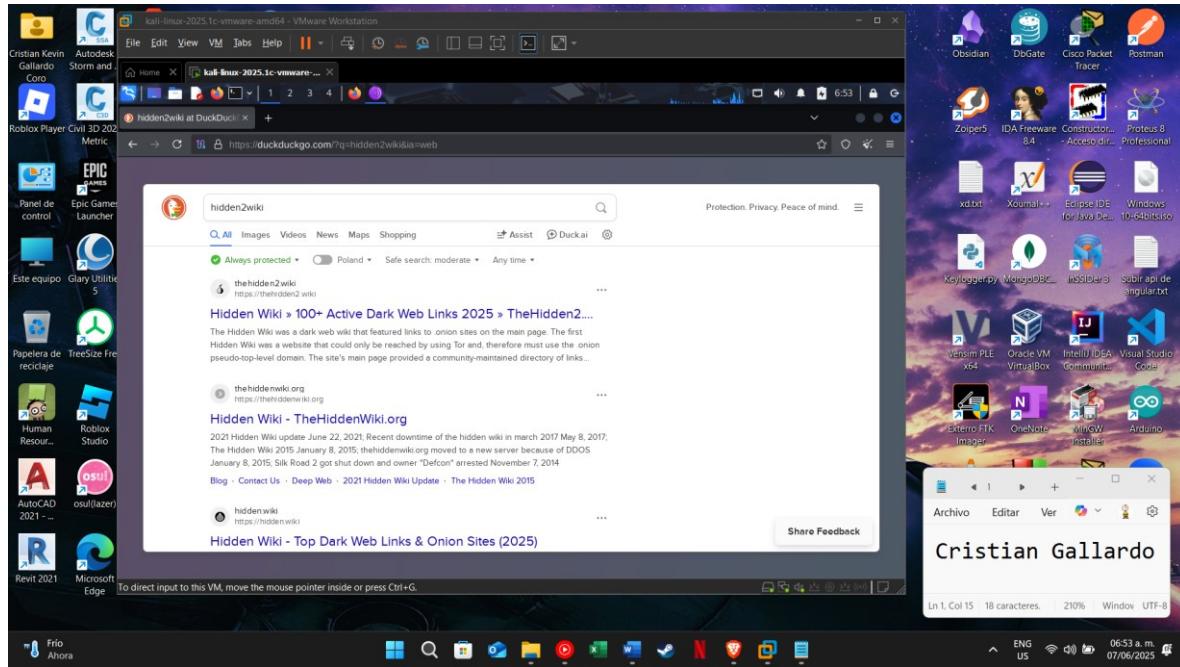


EVALUACION 2

1. El navegador bloquea el acceso a un enlace .onion en mi caso lo hizo porque el navegador detecto el enlace como peligroso y bloqueo cualquier acceso a este



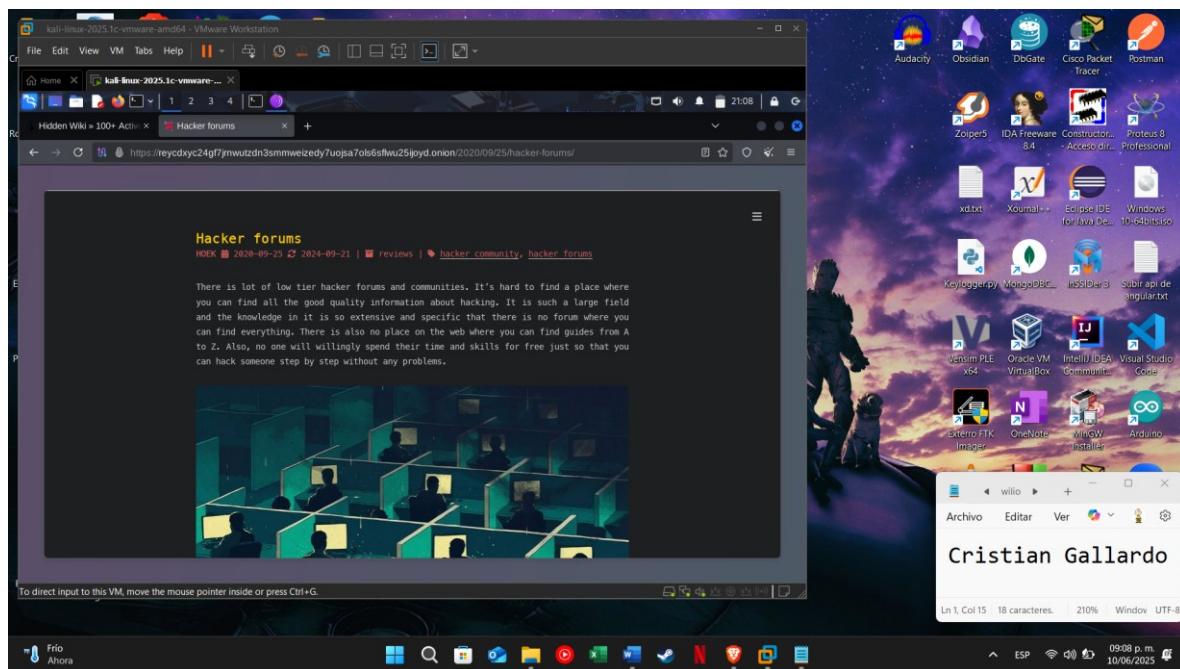
2. Usando el navegador Tor esta vez si se pudo acceder a la pagina web con un tiempo de espera un poco mas tardado de lo normal, unos 5 segundos de espera



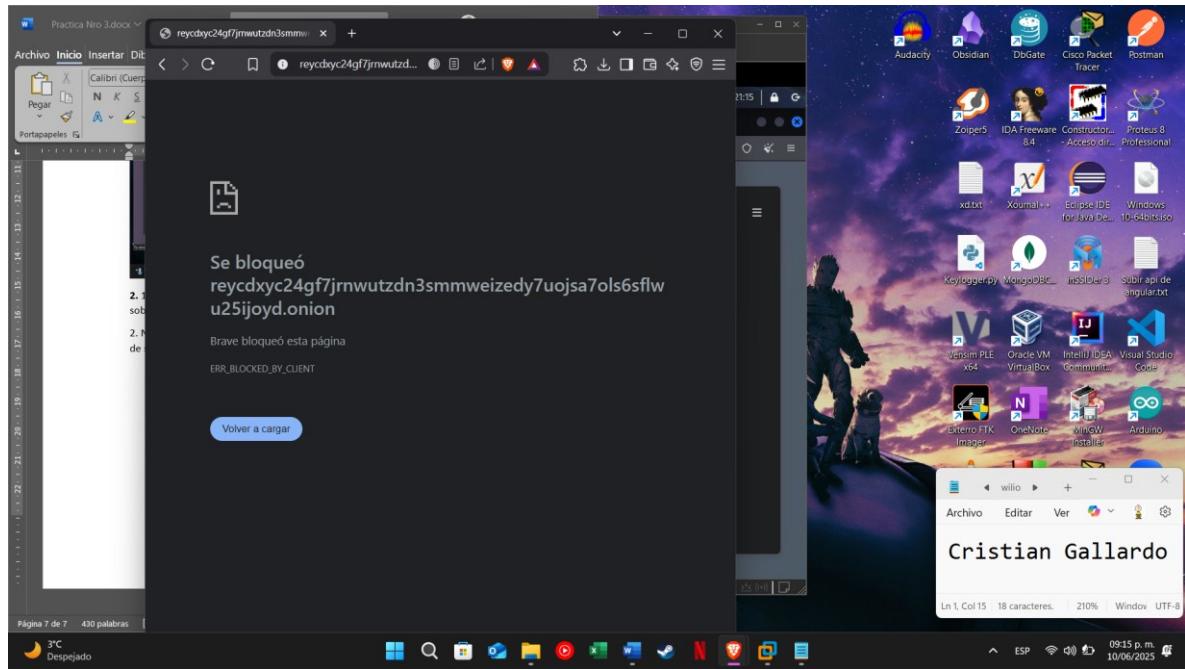
3. 1. En el caso del navegador convencional, este bloquea la conexión, mientras que el navegador Tor permite la conexión de manera normal al sitio
2. No, no accede bloquea el acceso a un enlace .onion en mi caso lo hizo porque el navegador detectó el enlace como peligroso y bloquó cualquier acceso a este
3. En sencillas palabras cumple la función de puerta para poder acceder a estos sitios, ya que nos permite conectar a la red Tor, la cual si puede acceder a sitios con la extensión onion, y es importante su uso, ya que además nos brinda una capa más de protección mediante el uso de VPNs

PARTE 3

- Accedemos al link brindado por el auxiliar

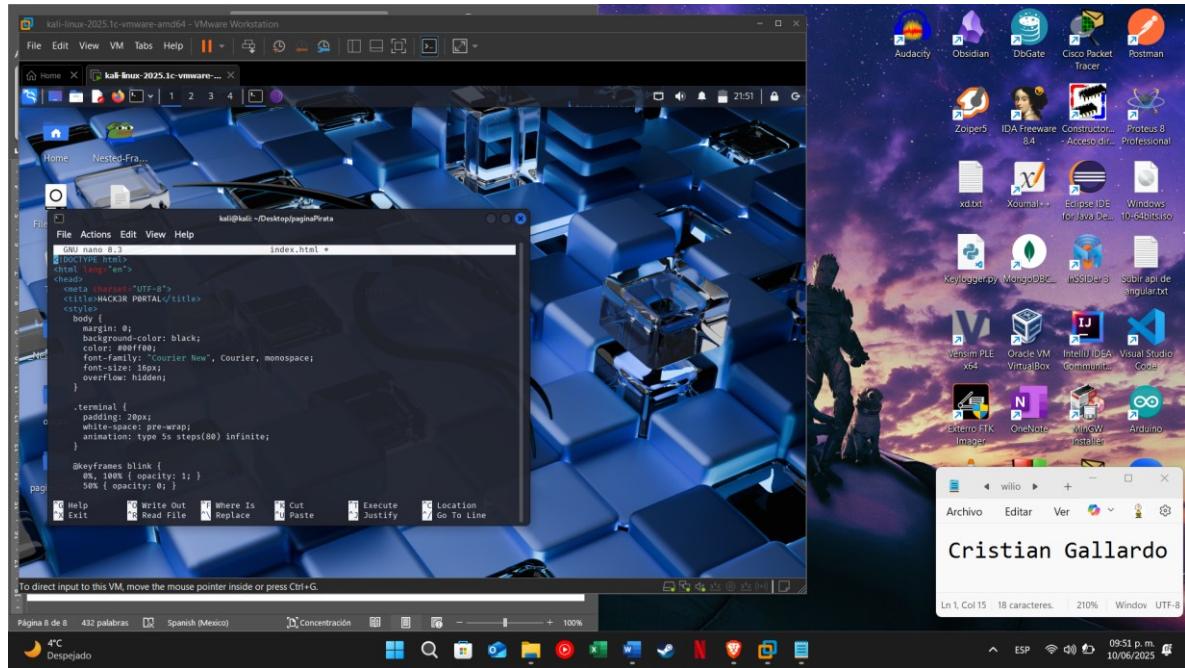


2. 1. El autor habla de lo difícil que es encontrar un lugar donde se guarde información de calidad sobre hacking y que en ese sitio encontraremos algo de esa información
2. No, no puede acceder, ya que es un enlace onion y como se dijo antes mayormente por motivos de seguridad no se pueden ingresar a enlaces con estas extensiones

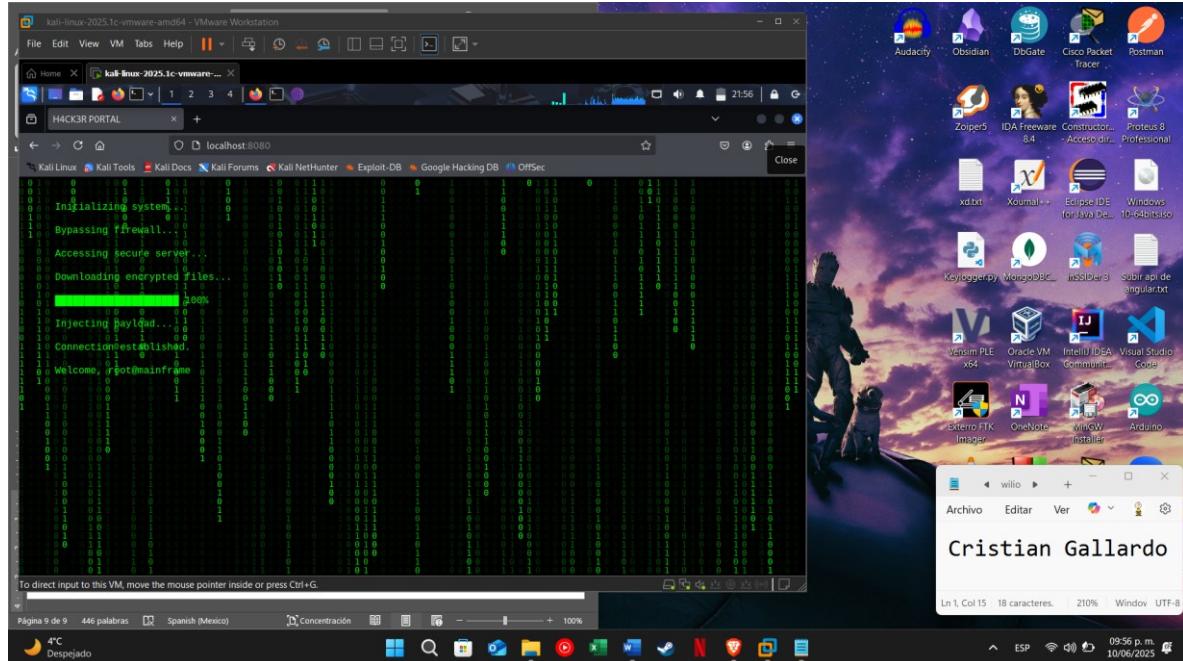
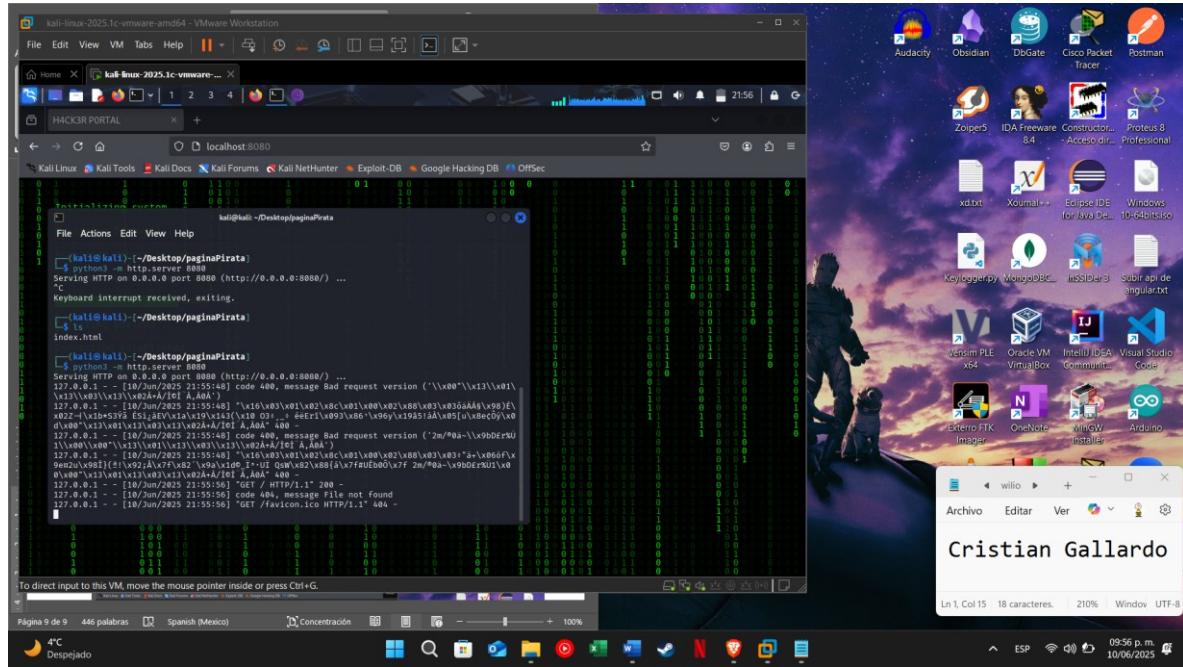


PARTE 4

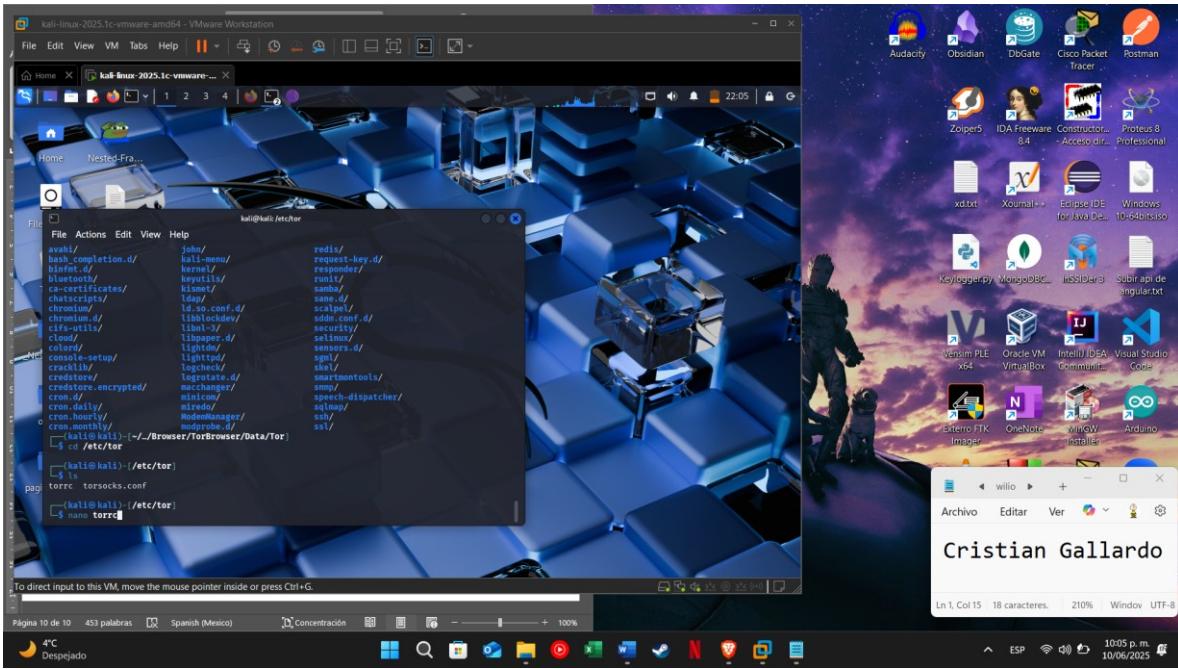
- Primeramente creamos una pagina estilo dark web



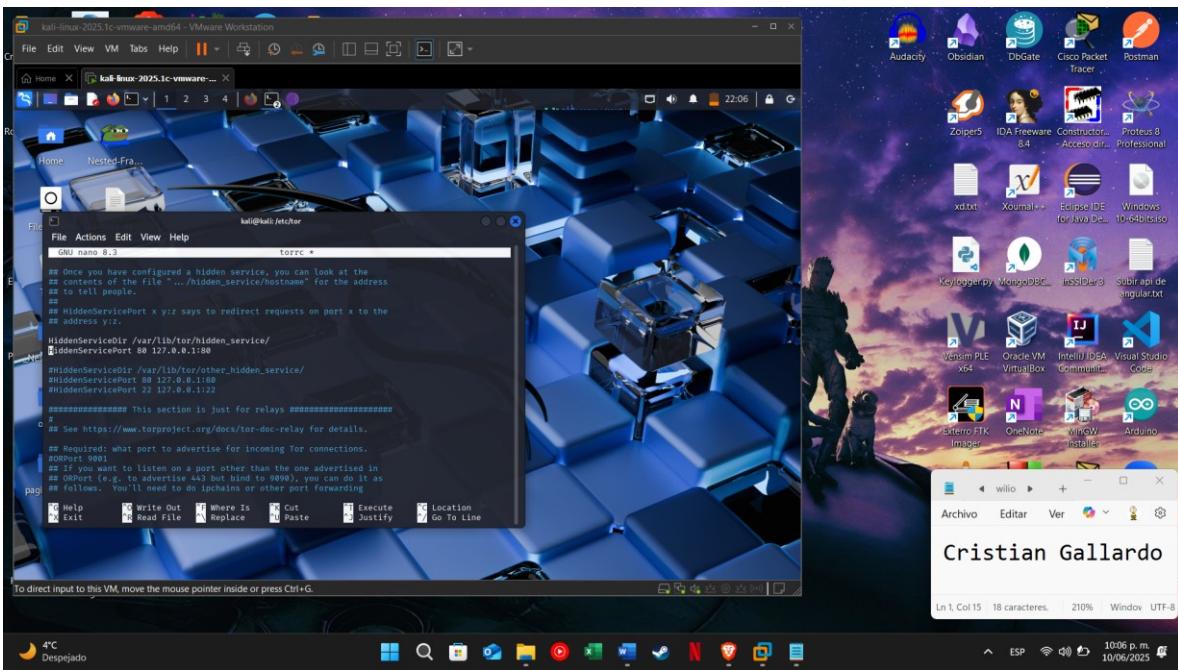
- Levantamos la página en el puerto 8080



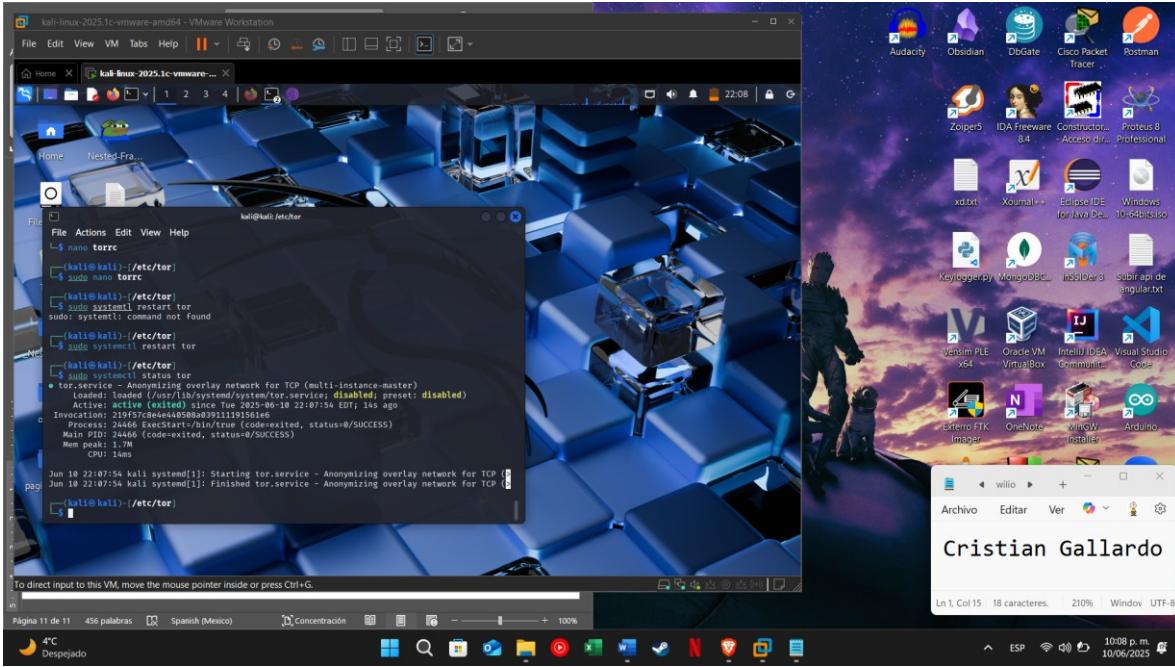
- Vamos al archivo de configuración de TOR



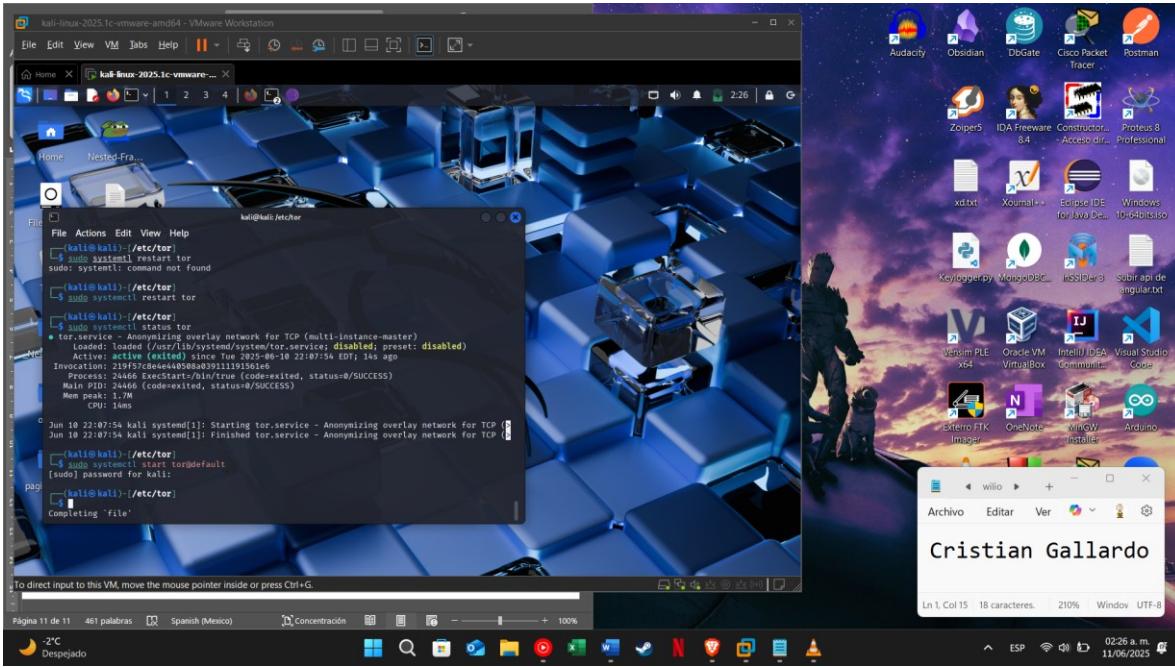
- Descomentamos las líneas



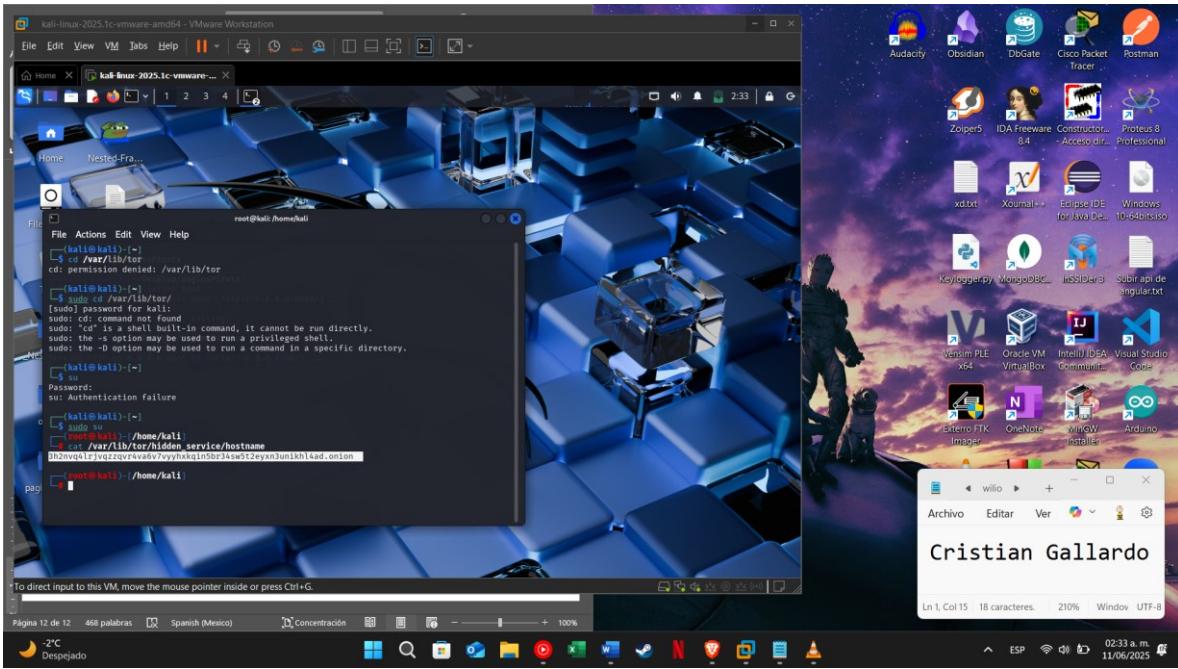
- Reiniciamos el servicio de TOR



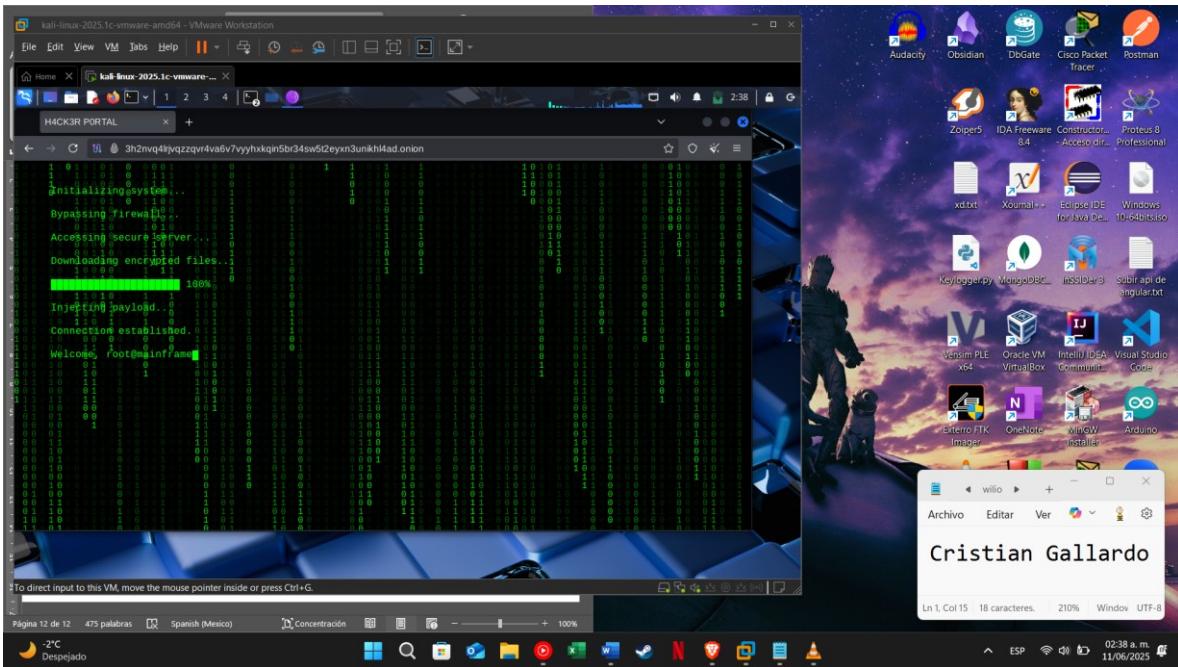
- Publicamos nuestra página en la red privada



- Vemos el enlace que se nos dio

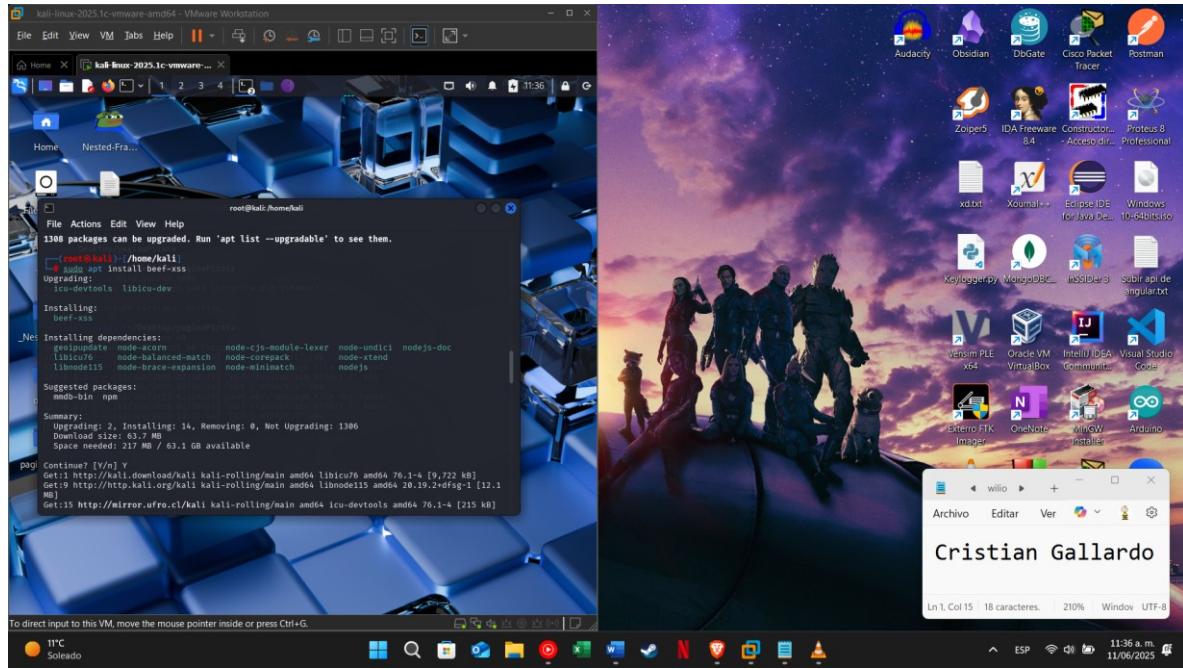


- Podemos verificar que efectivamente podemos acceder a la pagina web mediante el enlace proporcionado

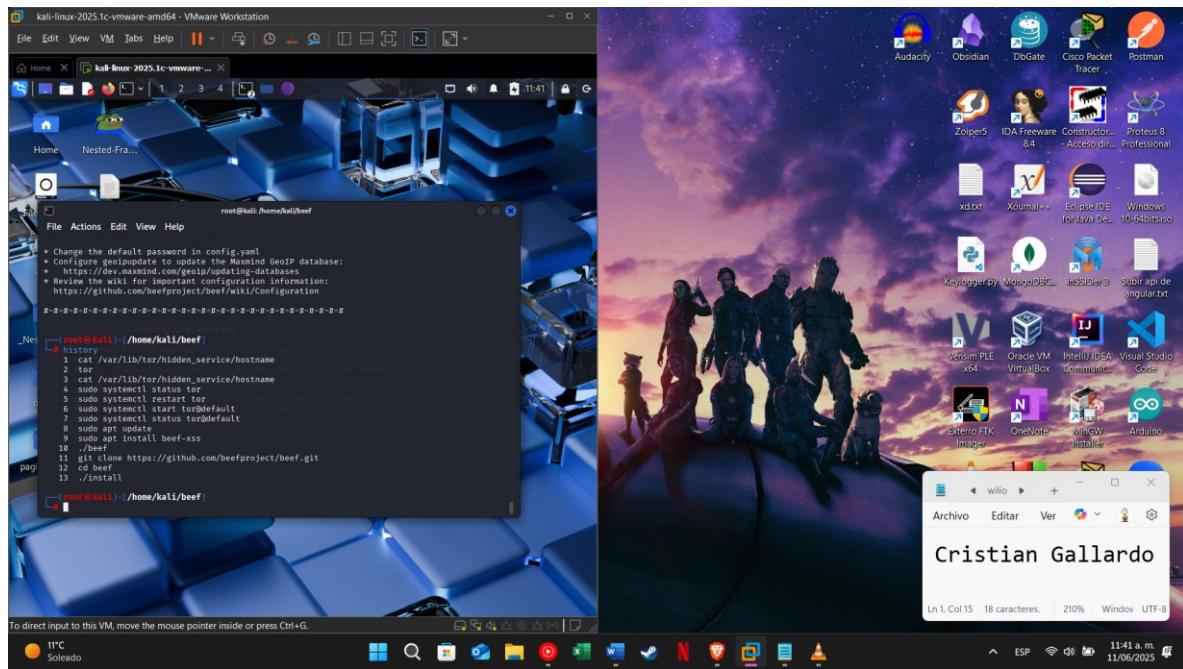


EVALUACION 3

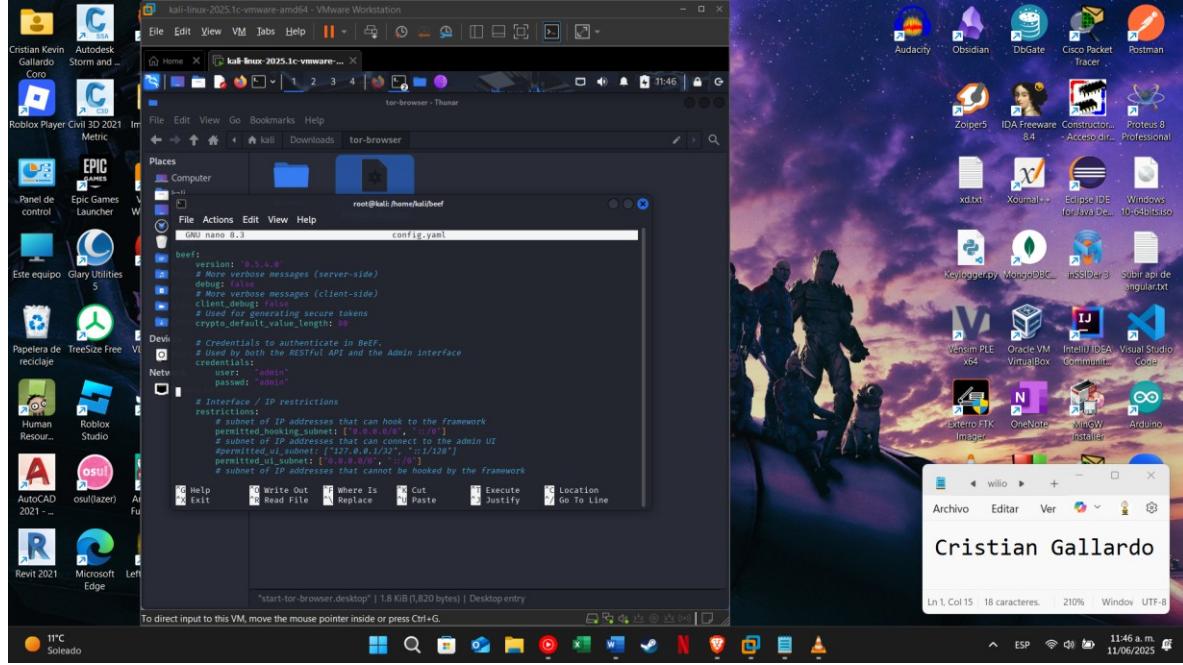
- Primeramente, realizamos de instalación de Beef en nuestro servidor Kali



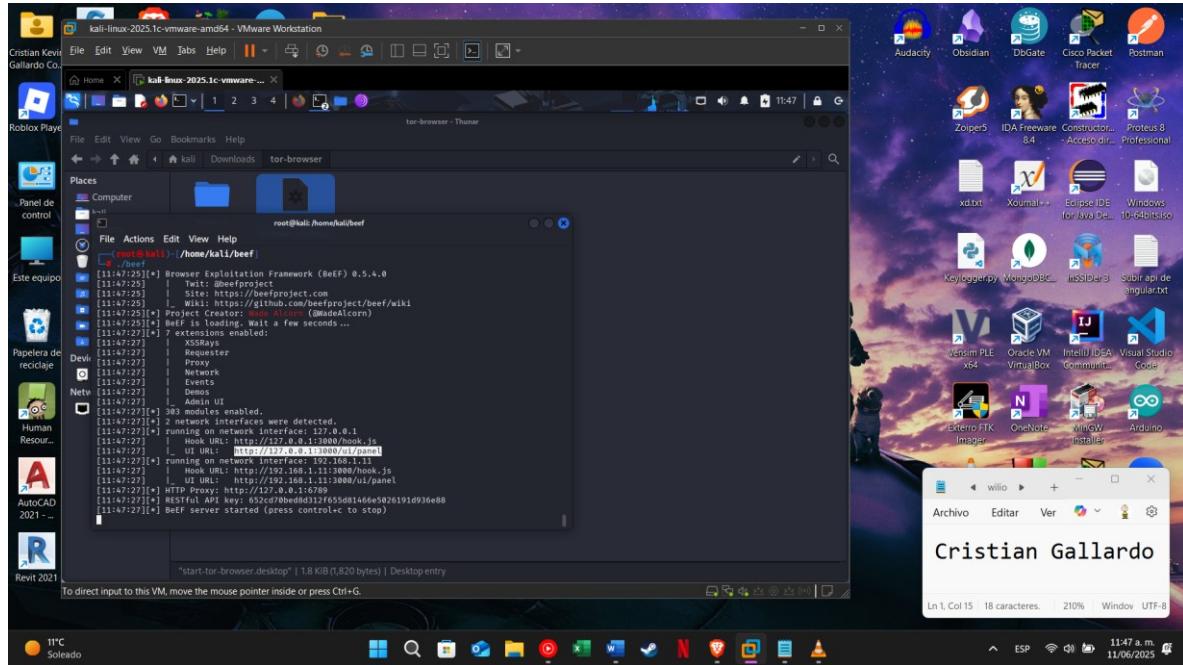
- Clonamos el repositorio de Beef, accedemos y lo instalamos

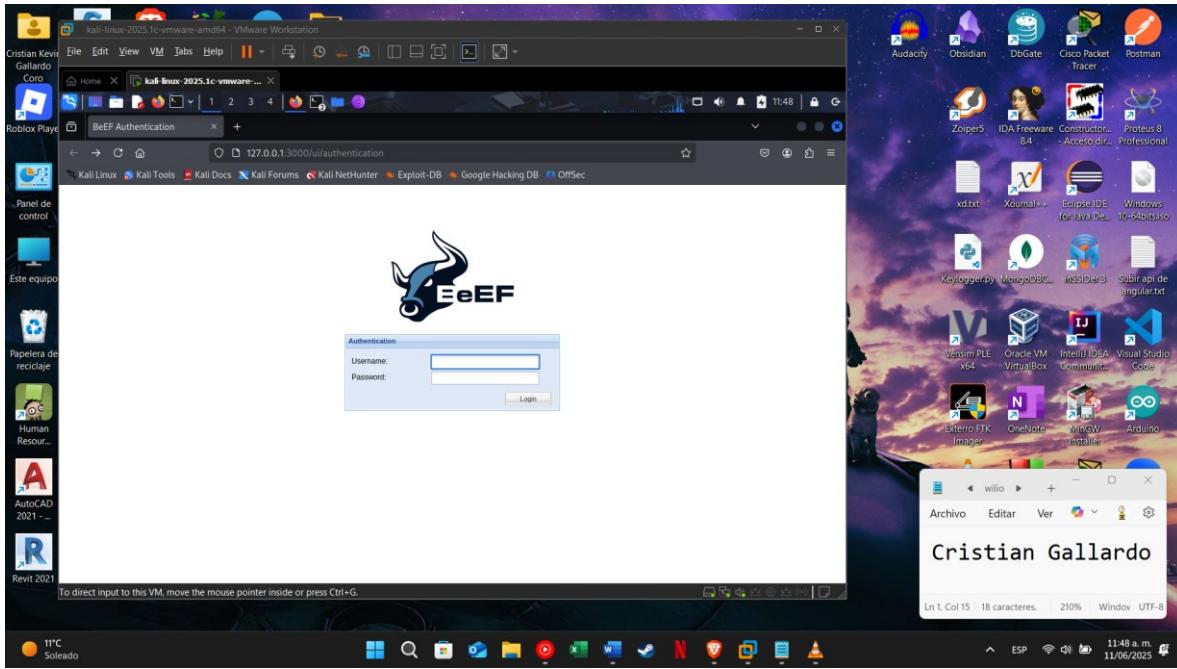


- Editamos el archivo config.yaml y cambiamos las credenciales de ingreso, user y pswd, en mi caso por admin admin

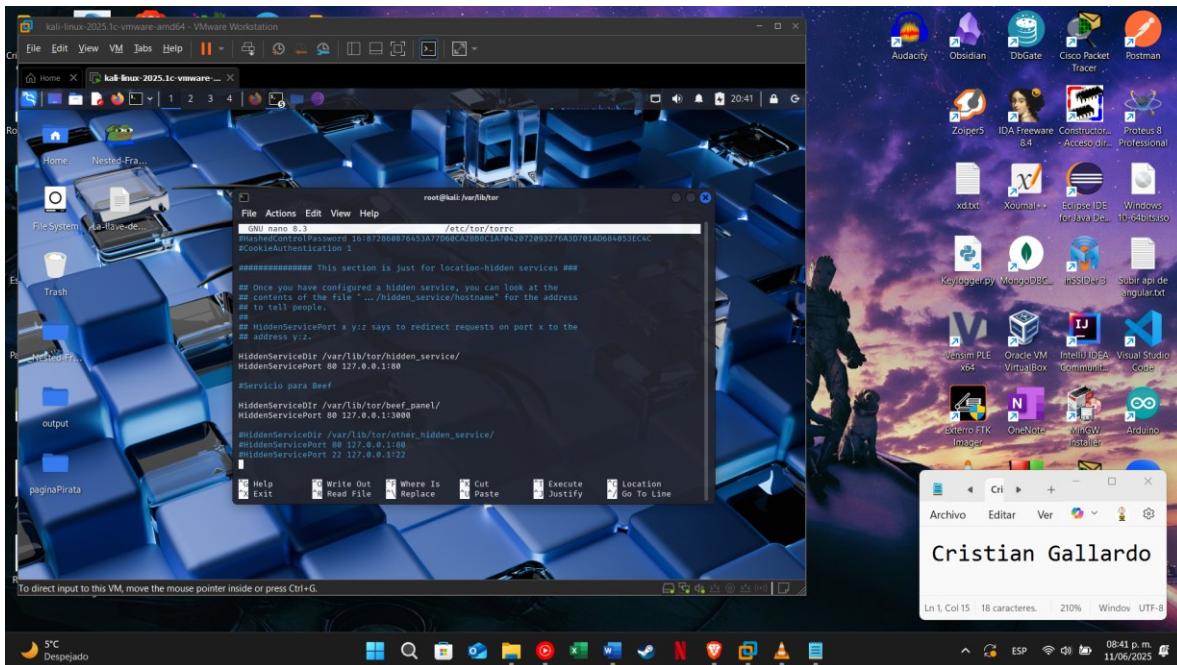


- Iniciamos el servicio y este nos dará un link, el cual nos llevará a la interfaz gráfica de BeEF, donde se nos pedirá las credenciales de sesión

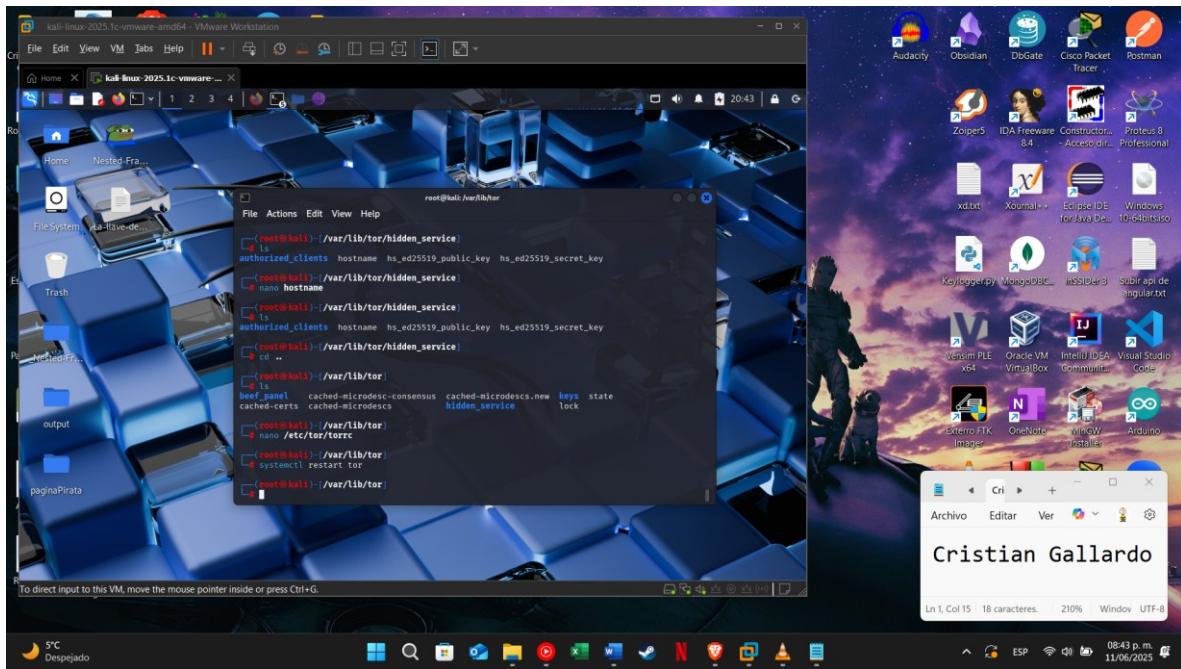




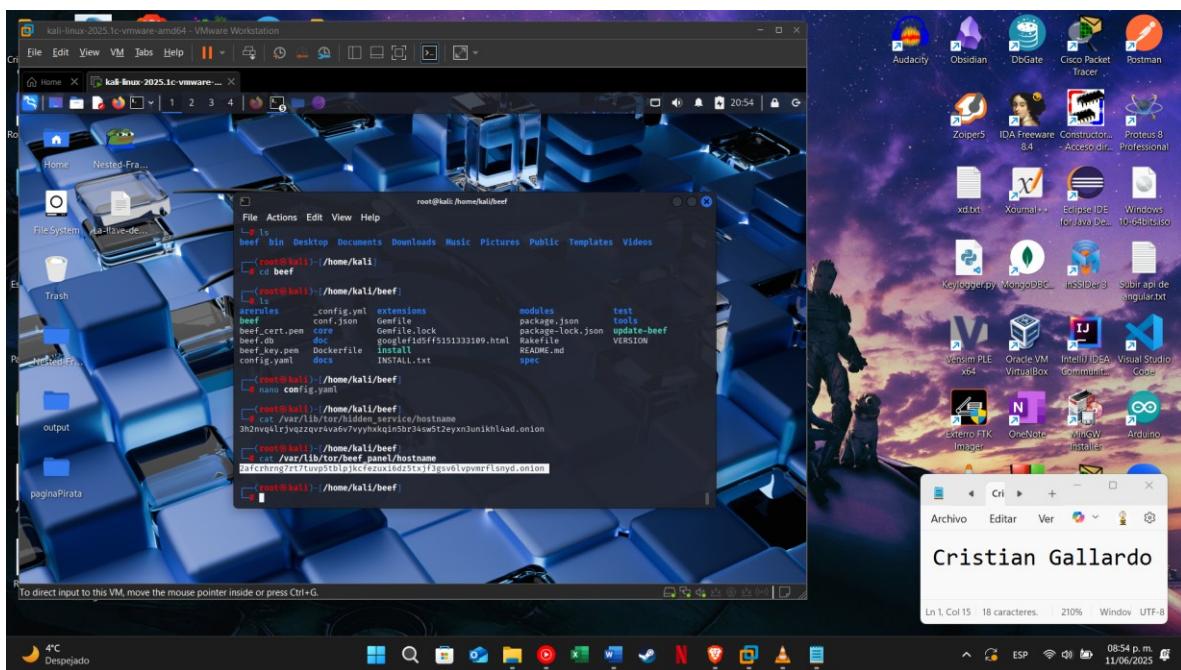
- Ahora crearemos en el archivo config.yaml una pagina aparte para que beef se encuentre en línea, donde se escuchará en el puerto 3000



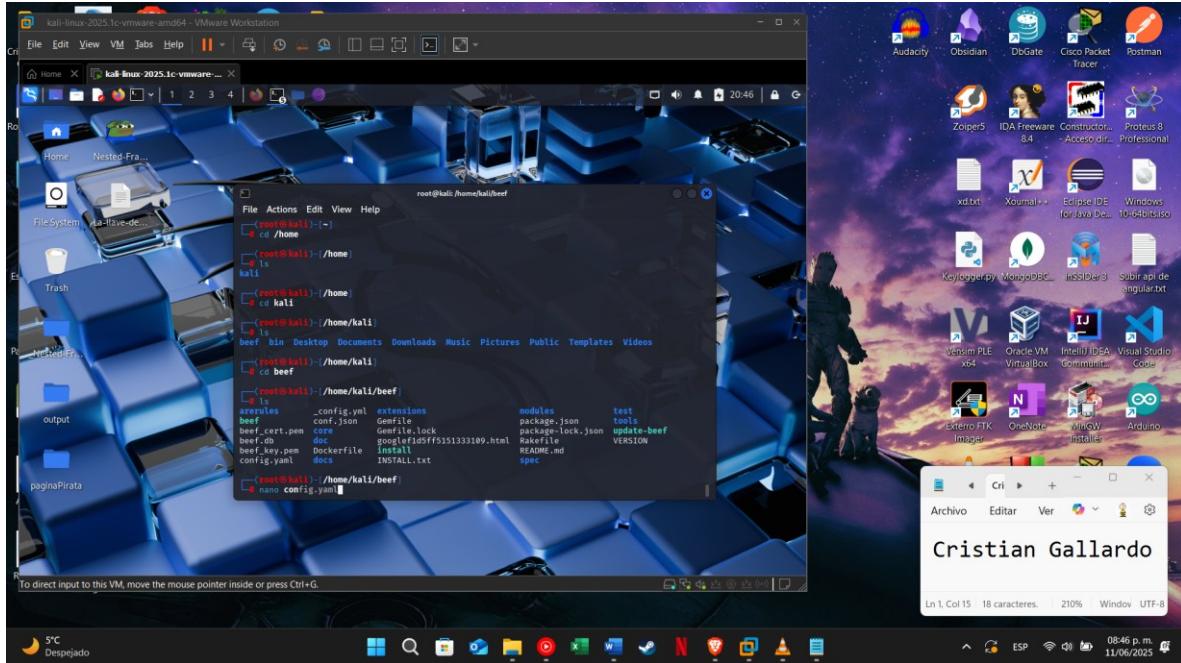
- Seguidamente reiniciamos el servicio de TOR



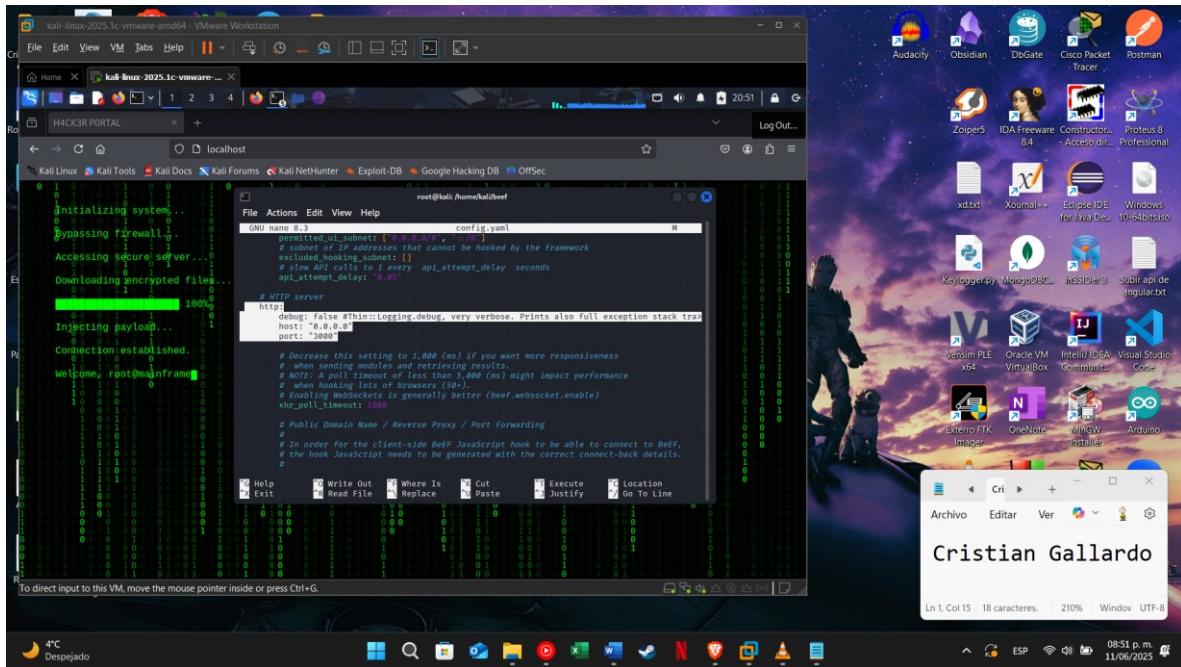
- Verificamos que se nos haya dado una dirección url con la cual conectaremos al index



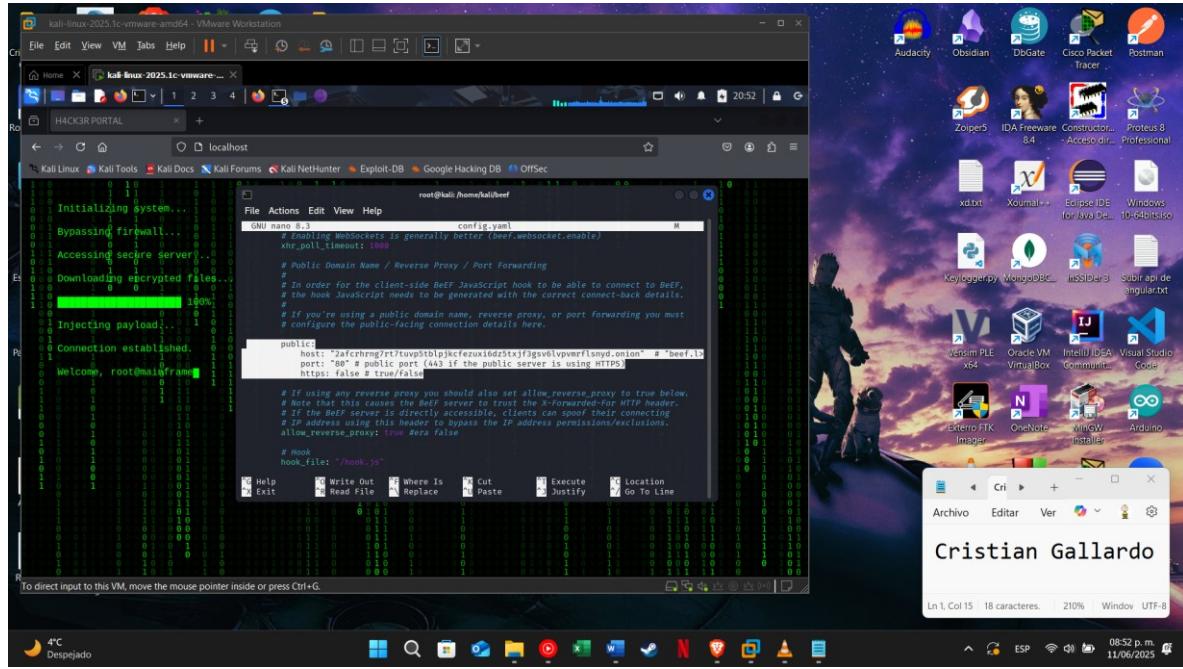
- Nos dirigiremos al directorio donde clonamos beef y cambiaremos los archivos de configuración



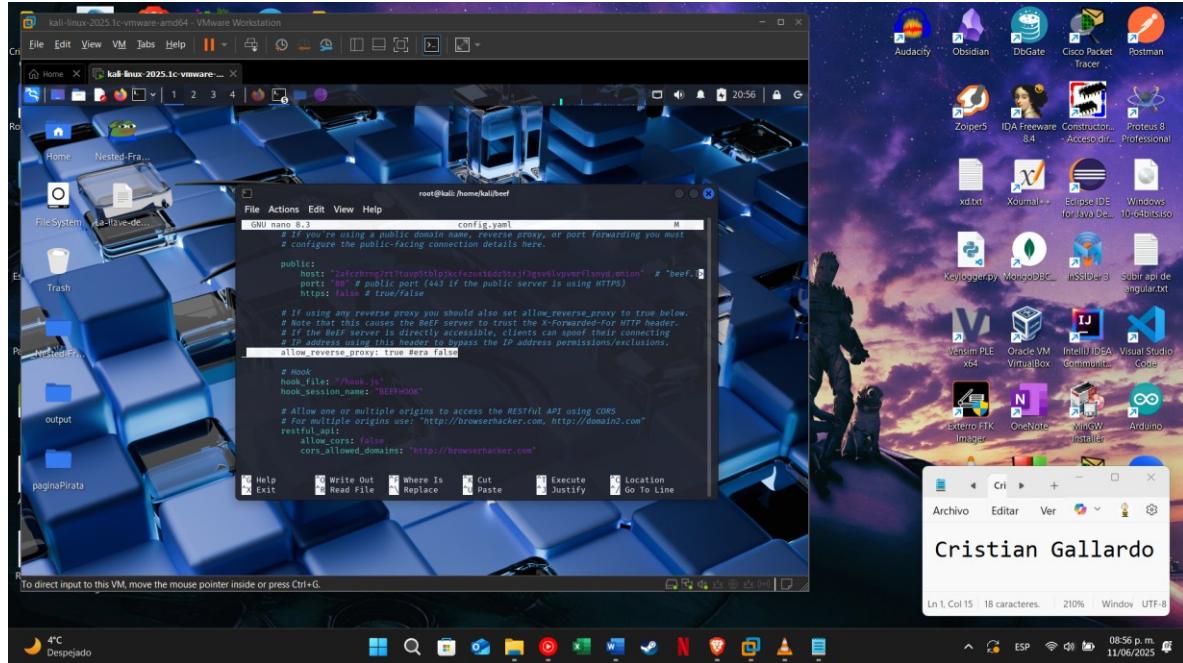
- Cambiaremos el puerto al 3000



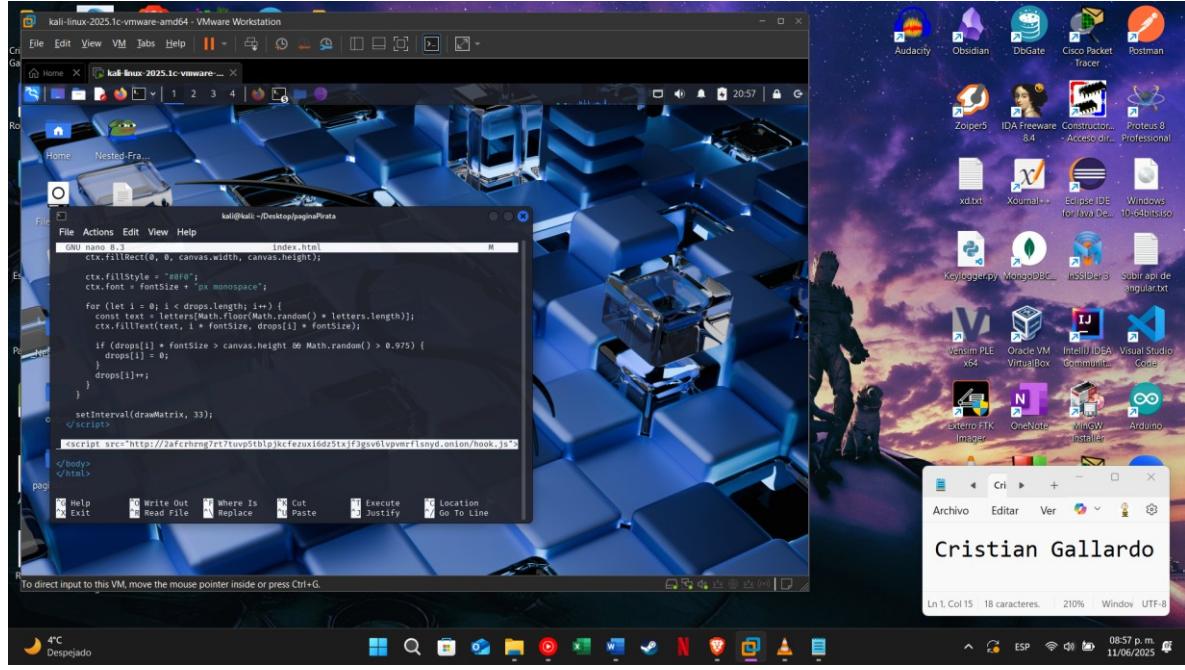
- Descomentaremos esta línea y pondremos la dirección url que nos proporcionó TOR



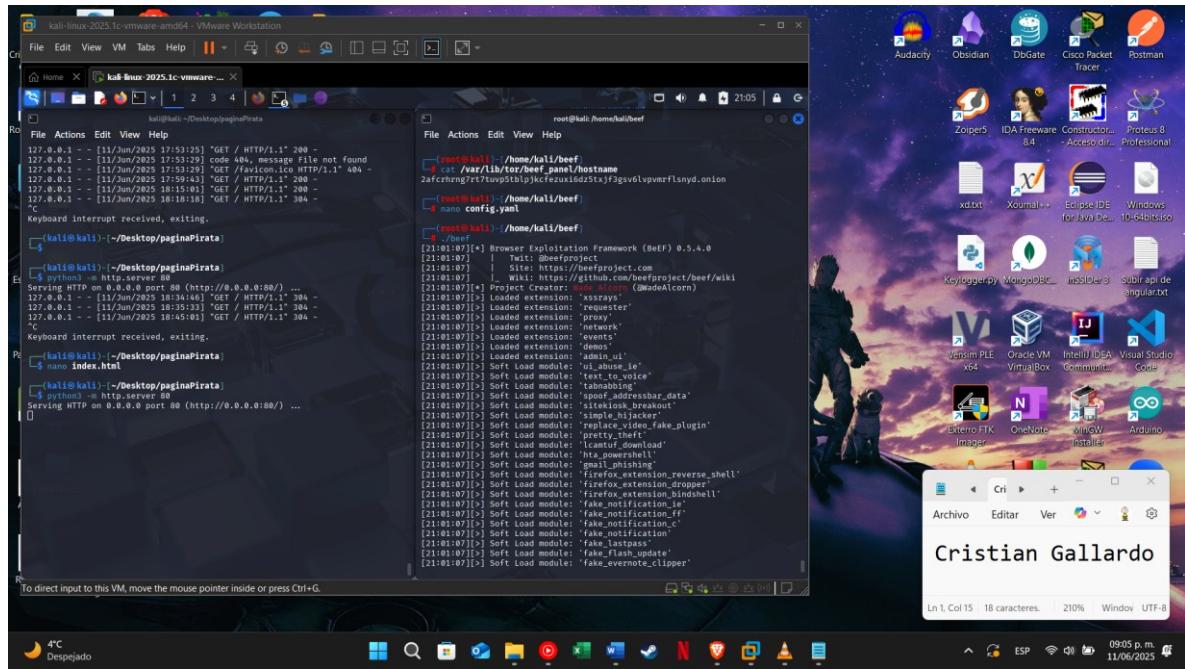
- también habilitaremos el proxy, para una mejor comunicación de paquetes



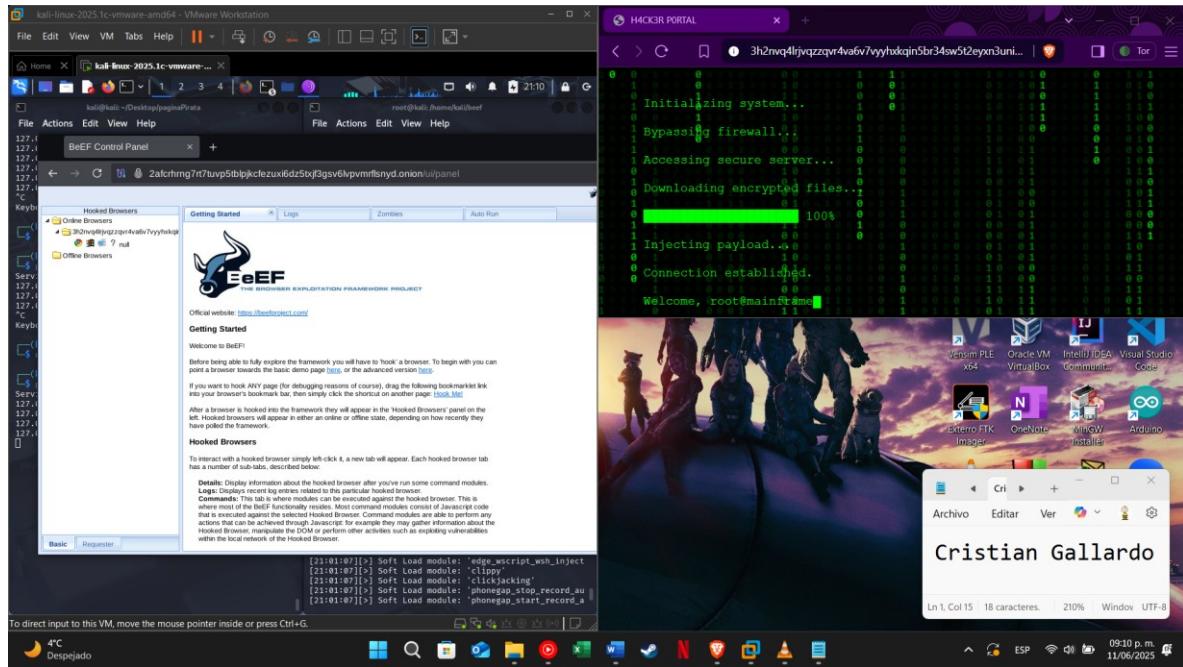
- En nuestro index.html nos iremos a la ultima parte para añadir una sección de script la cual contendrá la url que nos brindó TOR para acceder a beef, la cual se encargará de conectar el index con beef



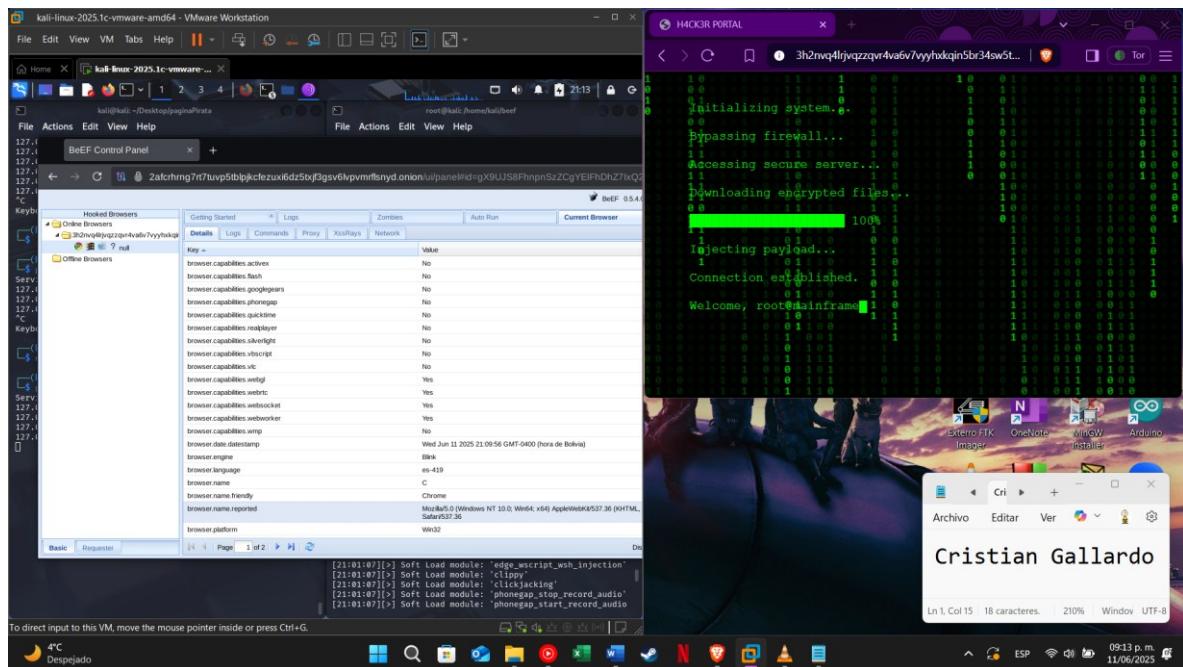
- Levantamos el index con Python y también el servicio de beef



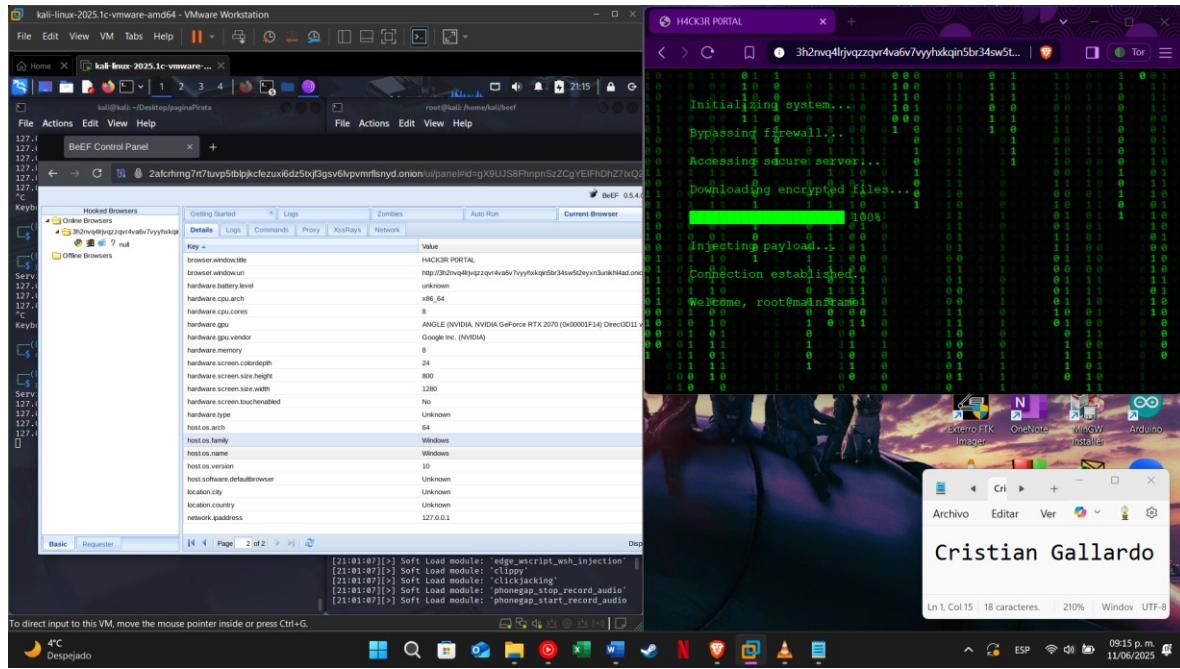
- Accedemos a la url del index.html desde nuestra máquina física y vemos que ya aparecemos dentro de la ui de beef



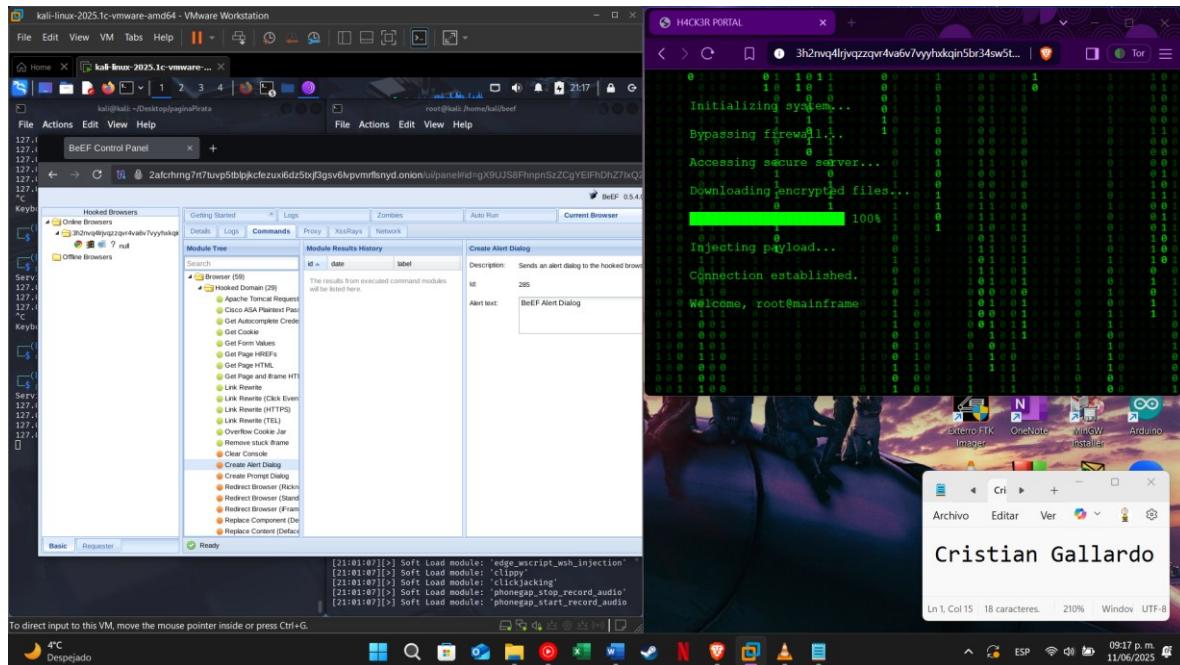
- Seleccionando el dispositivo, podemos ver, por todos los navegadores por el cual navega nuestra VPN



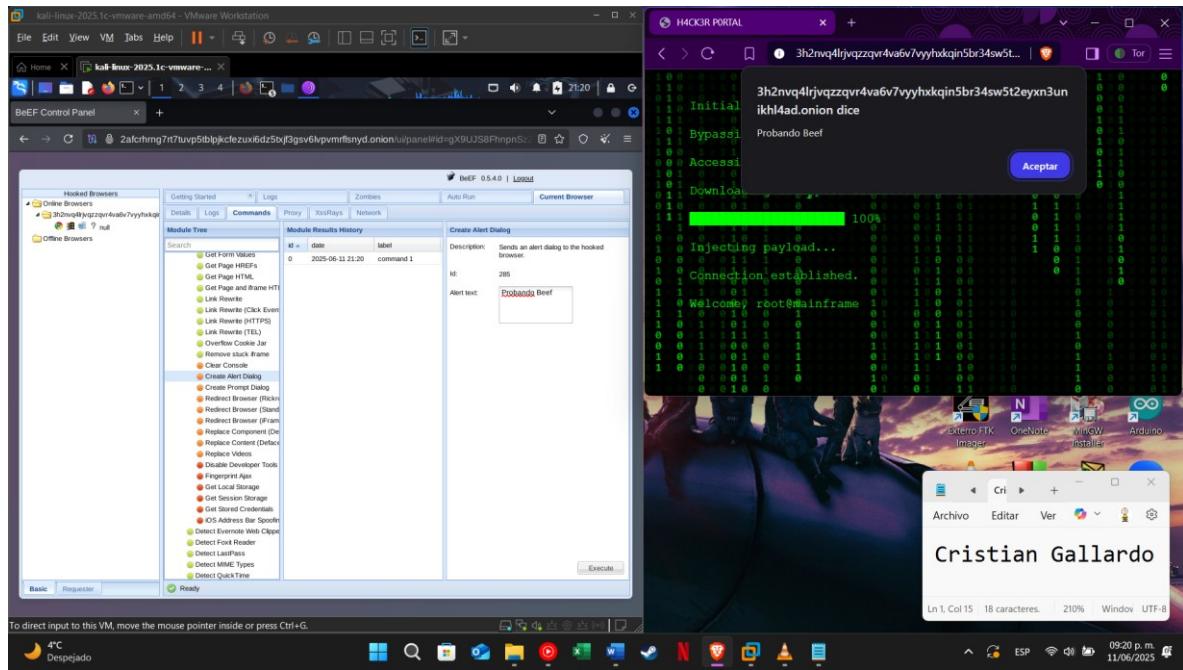
- También podemos ver ciertas características físicas que se pudieron llegar a recopilar de nuestro dispositivo



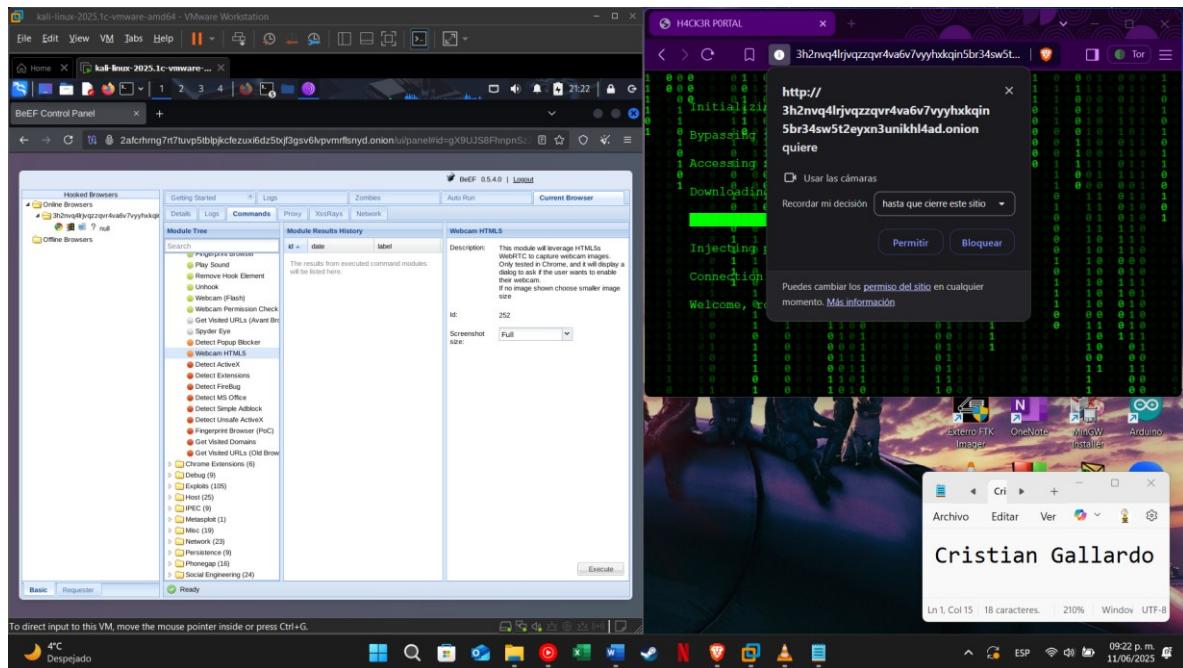
- Dentro de la sección de comands → Browser → Hooked Domain podemos mandar alertas básicas



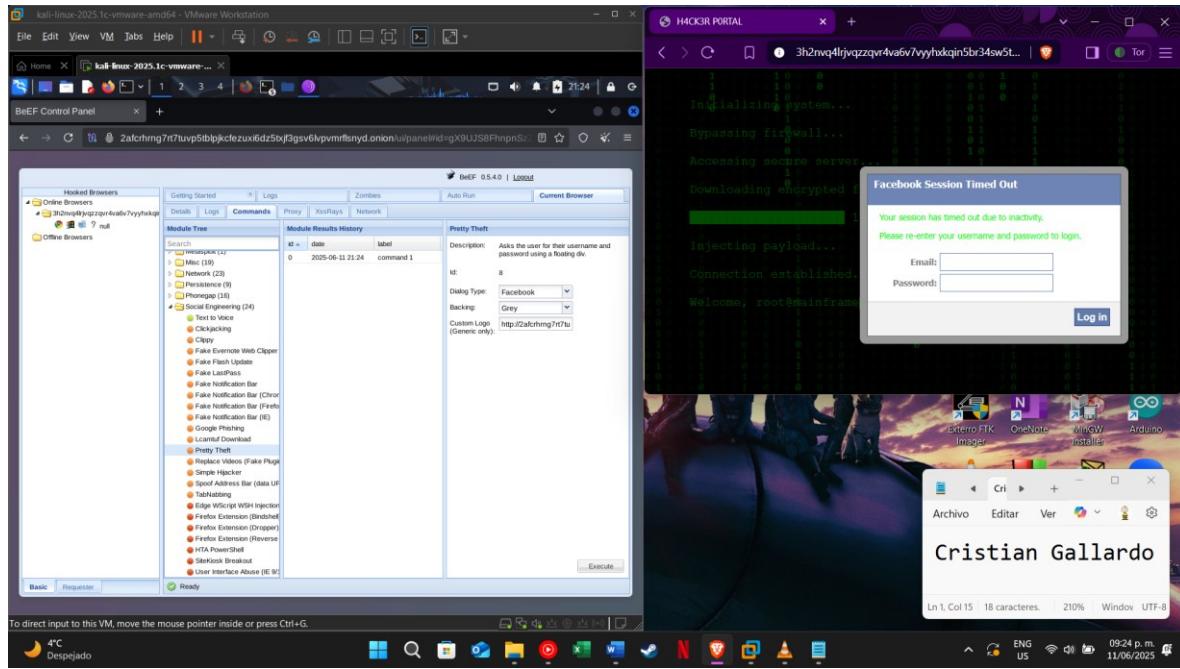
- Como por ejemplo el envío de una alerta personalizada con **Create Alert Dialog**



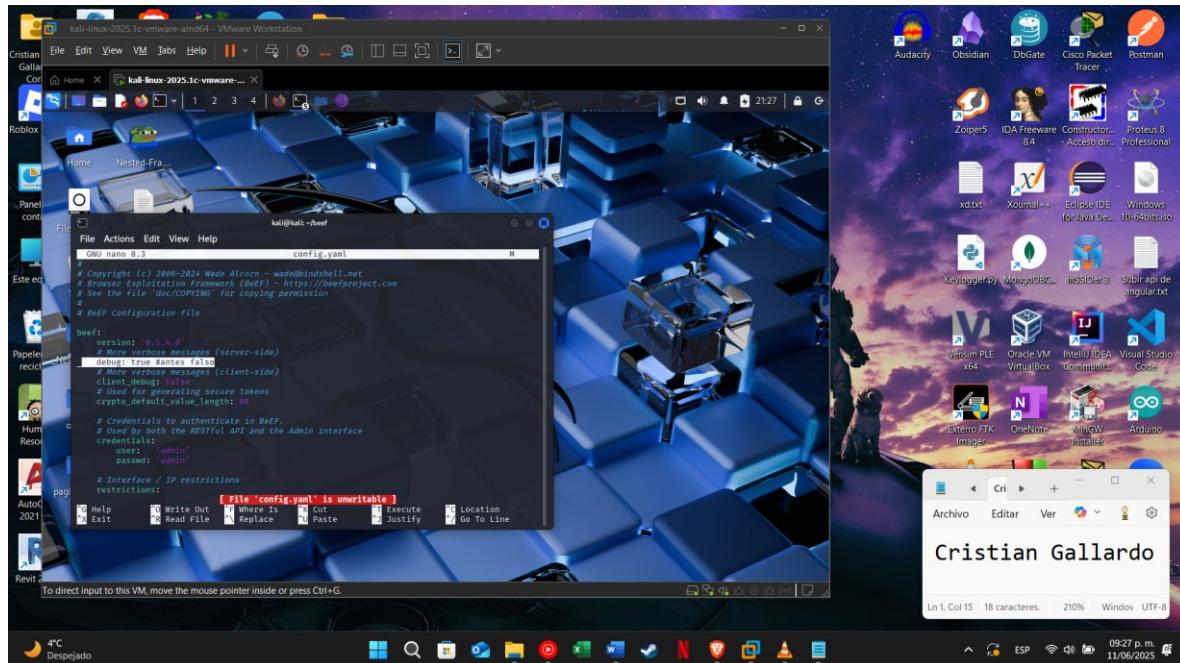
- O también de confirmar acciones para realizar ciertas cosas, como, por ejemplo, la habilitación de la cámara con **Webcam HTML 5**



- Y también para el envío de prompts, donde podemos robar datos simulando un reinicio de cuenta usando Social Engineering → **Pretty Theft**



- Para la simulación básica de un keylogger aprovecharemos uno de los servicios de beef que es el debug, este registra todo lo que se haga dentro de la página, hasta lo que se escribe, cambiaremos de estado a true, y reiniciamos beef



- Reiniciado nuestro servicio volvemos a entrar a la página, y veremos que desde la consola donde ejecutamos beef se guarda todo lo que se haya hecho, incluso lo que se escribió

