PORTADA

NOMBRE: BRAYN SAHAGUN

PROFESOR: JIMENEZ SANCHEZ ISMAEL

ESCUELA: UPQROO

CARRERA: INGENIERÍA EN SOFTWARE

MATERIA: SISTEMAS OPERATIVOS

GRUPO: 27BV **CUATRIMESTRE:** 7mo

¿Qué es hardening?

En informática, el hardening o endurecimiento es el proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuanto más funciones desempeña; en principio un sistema con una única función es más seguro que uno con muchos propósitos.

Aplicando CIS Benchmark a mi sistema operativo Linux

Requisitos

- **VirtualBox 7.0**
- **Kali Linux**
- **Firefox**

¿Por qué hacer hardening en Firefox?

1. Protección contra amenazas en línea:

Malware y spyware: Al fortalecer la seguridad de Firefox, se reducen las posibilidades de que malware o spyware puedan comprometer tu sistema a través de vulnerabilidades en el navegador.

2. Privacidad y protección de datos:

Rastreo en línea: El hardening puede incluir medidas para reducir el rastreo en línea y proteger tu privacidad. Esto puede incluir la configuración de opciones de privacidad avanzadas y el uso de extensiones de navegador que bloquean rastreadores.

3. Control de scripts y complementos:

Scripts maliciosos: Configurar el navegador para bloquear scripts maliciosos y desactivar complementos innecesarios puede reducir la exposición a amenazas en línea.

4. Configuraciones de seguridad avanzadas:

Configuraciones de cifrado: Asegurarse de que las conexiones estén cifradas correctamente al utilizar HTTPS siempre que sea posible.

Configuraciones de red: Configurar preferencias de red seguras puede ayudar a prevenir ataques como ataques de intermediarios (Man-in-the-Middle).

Cambiar las preferencias de Firefox

1. En “ajustes” o ingresando en el navegador “about preferences”.

2. **Eliminación de "Recommended by Pocket":** Se retira la funcionalidad "Recommended by Pocket" para mejorar la privacidad y reducir la exposición a contenido no solicitado.

3. **Cambio del motor de búsqueda a "DuckDuckGo":** Se establece DuckDuckGo como el motor de búsqueda predeterminado para mejorar la privacidad del usuario, ya que este motor de búsqueda no rastrea la información del usuario.

4. **Activación de la protección de seguimiento:** Se habilita la protección de seguimiento para bloquear la recopilación no deseada de datos por parte de sitios web y anunciantes.

5. **Desactivación del guardado de contraseñas:** Se deshabilita la función de guardado automático de contraseñas para aumentar la seguridad y evitar posibles riesgos de seguridad.

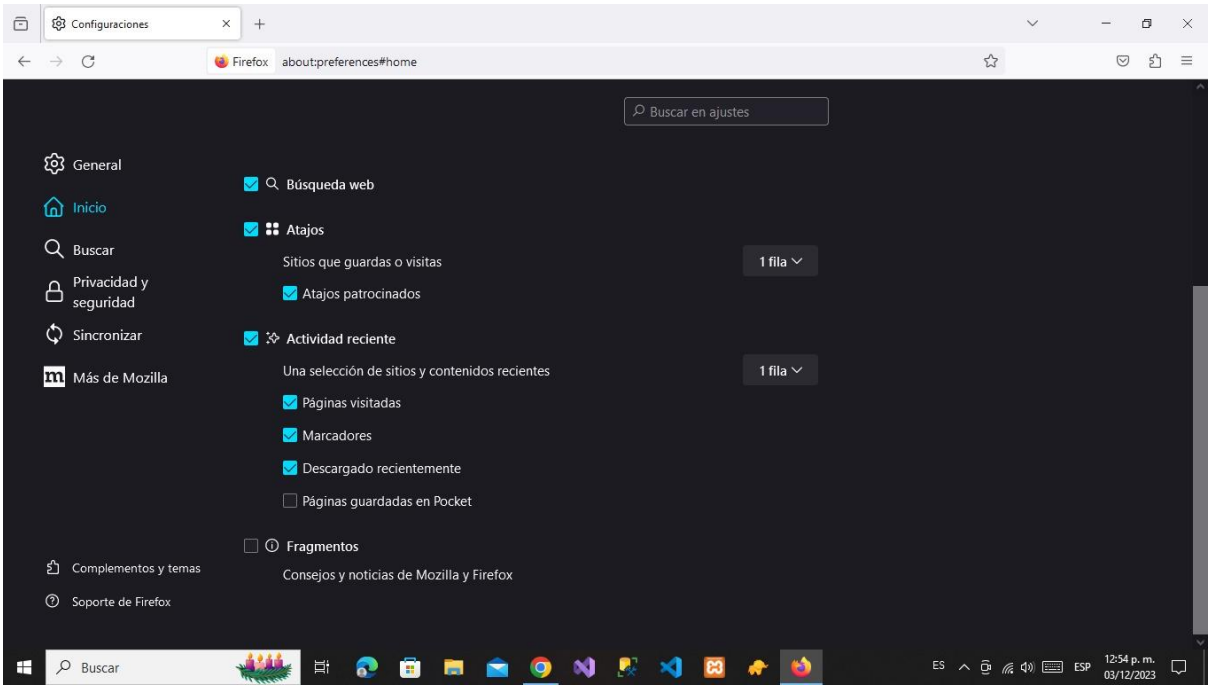
6. **Bloqueo del acceso a la ubicación:** Se impide que los sitios web accedan a la ubicación del usuario, lo que contribuye a preservar la privacidad geográfica.

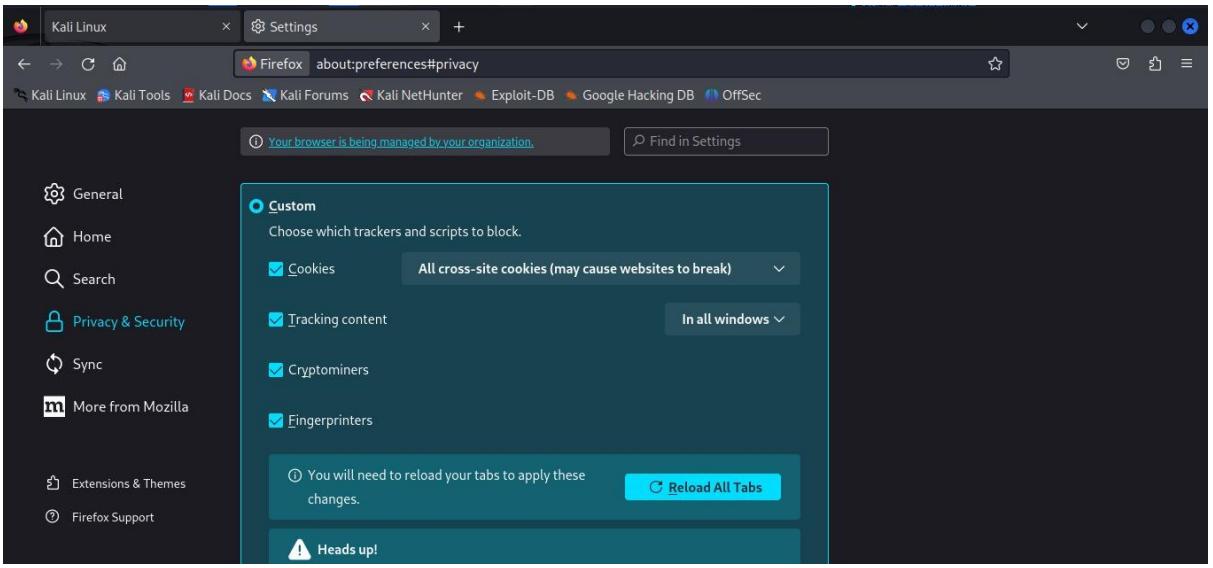
7. **Bloqueo de notificaciones:** Se bloquea la recepción de notificaciones no solicitadas de sitios web, mejorando la experiencia de navegación y reduciendo posibles molestias.

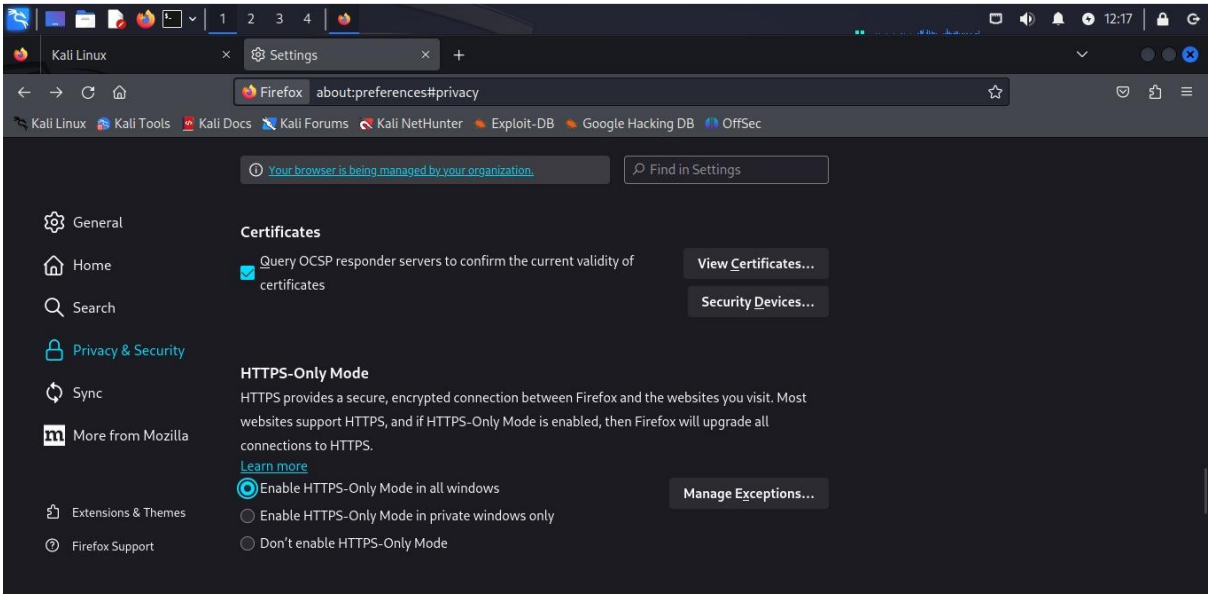
8. **Bloqueo de reproducción automática:** Se evita la reproducción automática de contenido multimedia, proporcionando al usuario un mayor control sobre su experiencia en línea.

9. **Deshabilitación de telemetría e informe de errores:** Se apaga la recopilación de datos de telemetría y la generación de informes de errores, preservando la privacidad del usuario y reduciendo el intercambio de información con el proveedor del navegador.

10. **Habilitación del modo HTTPS:** Se activa el modo de habilitación HTTPS para mejorar la seguridad de las conexiones y garantizar que la comunicación con los sitios web sea cifrada y segura.

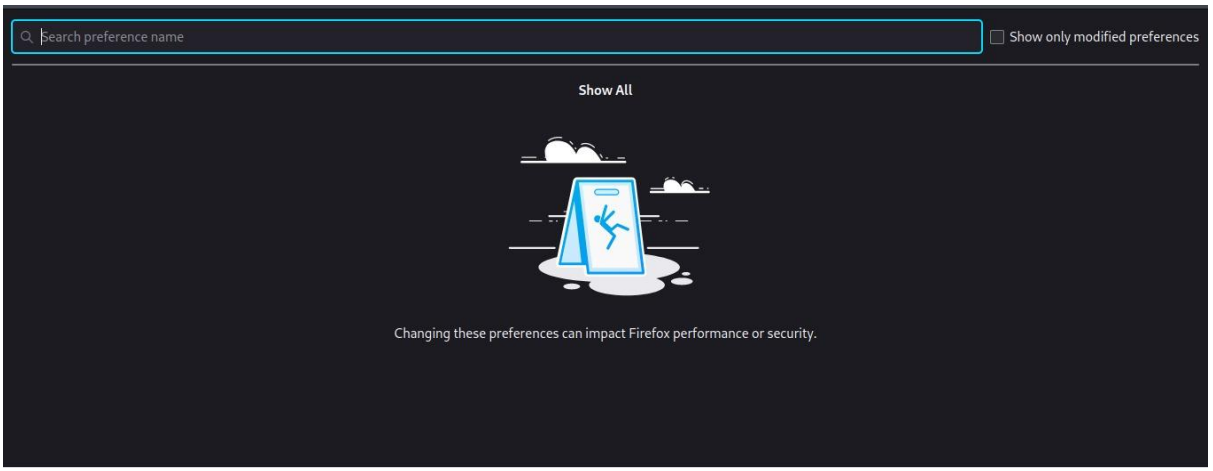

Configuraciones
Firefox about:preferences#home
Buscar en ajustes
General
Inicio
Buscar
Privacidad y seguridad
Sincronizar
Más de Mozilla
Búsqueda web
Atajos
Sitios que guardas o visitas
1 fila
Atajos patrocinados
Actividad reciente
Una selección de sitios y contenidos recientes
1 fila
Páginas visitadas
Marcadores
Descargado recientemente
Páginas guardadas en Pocket
Fragmentos
Consejos y noticias de Mozilla y Firefox
Complementos y temas
Soporte de Firefox
Buscar
ES
ESP
12:54 p. m.
03/12/2023


Kali Linux
Settings
Firefox about:preferences#privacy
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Your browser is being managed by your organization.
Find in Settings
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Extensions & Themes
Firefox Support
Custom
Choose which trackers and scripts to block.
Cookies
All cross-site cookies (may cause websites to break)
Tracking content
In all windows
Cryptominers
Fingerprinters
You will need to reload your tabs to apply these changes.
Reload All Tabs
Heads up!



Sumergirse en la configuración avanzada

1. Ingresar en el navegador “about:config”.



Configuraciones recomendadas para todos. [L1]

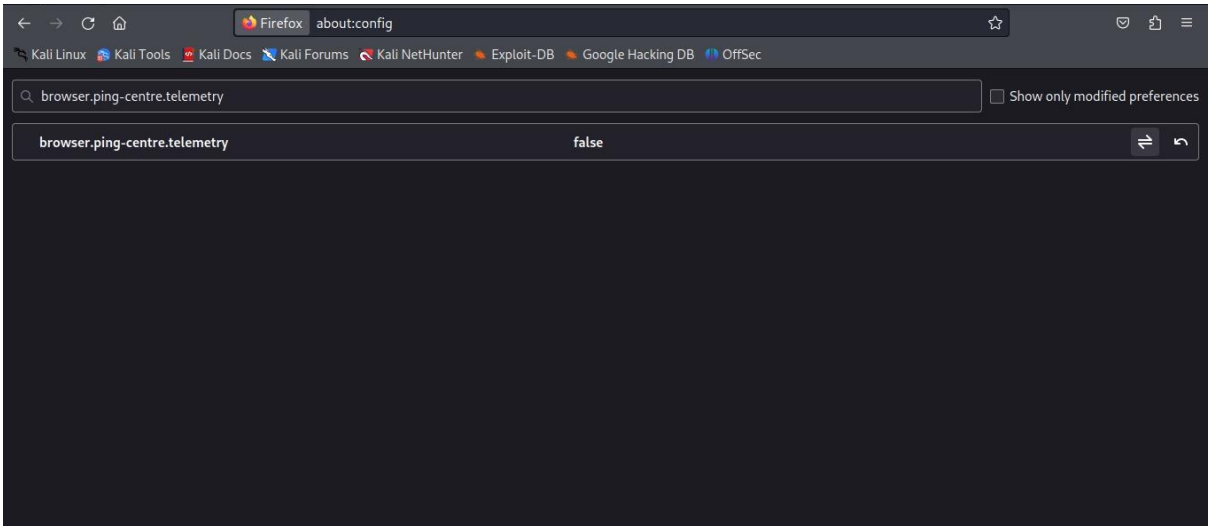
Desactivar telemetría [L1]
Cambiar browser.newtabpage.activity-stream.feeds.telemetry a false
Cambiar browser.ping-centre.telemetry a false
Cambiar browser.tabs.crashReporting.sendReport a false
Cambiar devtools.onboarding.telemetry.logged a false
Cambiar toolkit.telemetry.enabled a false
Eliminar la URL para toolkit.telemetry.server y dejarla vacía
Cambiar toolkit.telemetry.unified a false

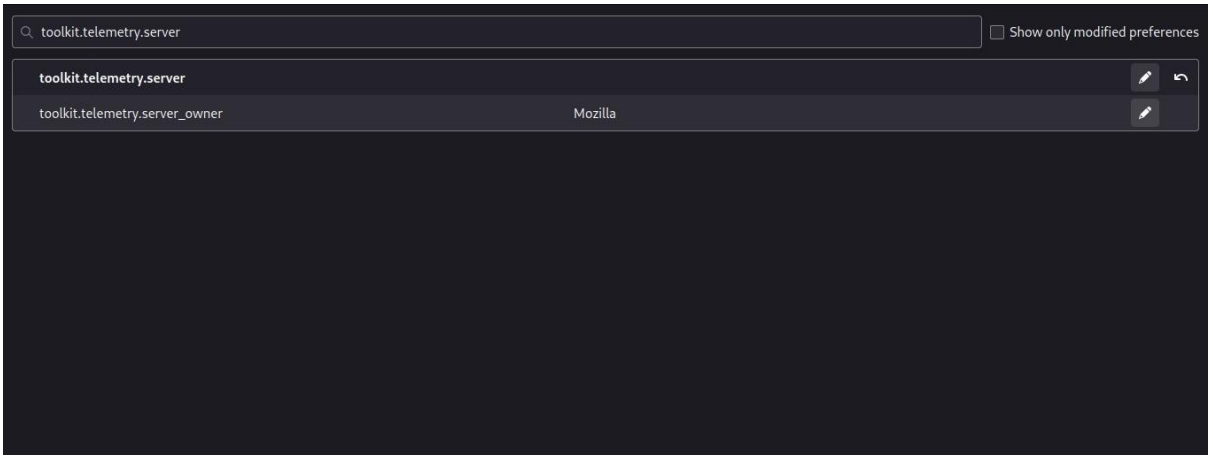
Desactivar Pocket [L1]
Cambiar browser.newtabpage.activity-stream.feeds.discoverystreamfeed a false
Cambiar browser.newtabpage.activity-stream.feeds.section.topstories a false
Cambiar browser.newtabpage.activity-stream.section.highlights.includePocket a false
Cambiar browser.newtabpage.activity-stream.showSponsored a false
Cambiar extensions.pocket.enabled a false

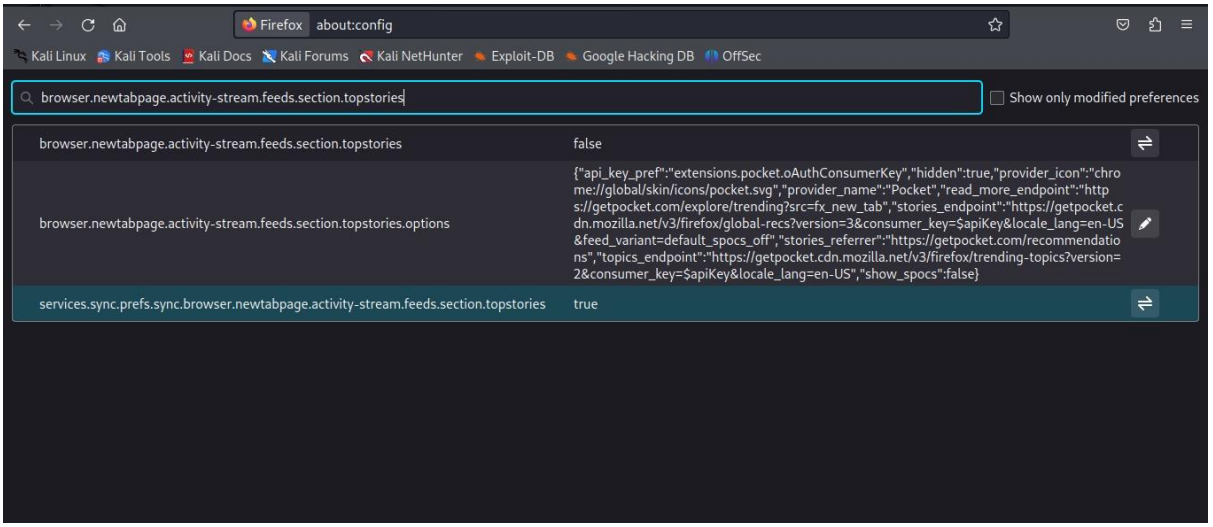
Desactivar el prefetching [L1]
Cambiar network.dns.disablePrefetch a true
Cambiar network.prefetch-next a false

Desactivar JavaScript en PDF [L1]
Cambiar pdfjs.enableScripting a false.

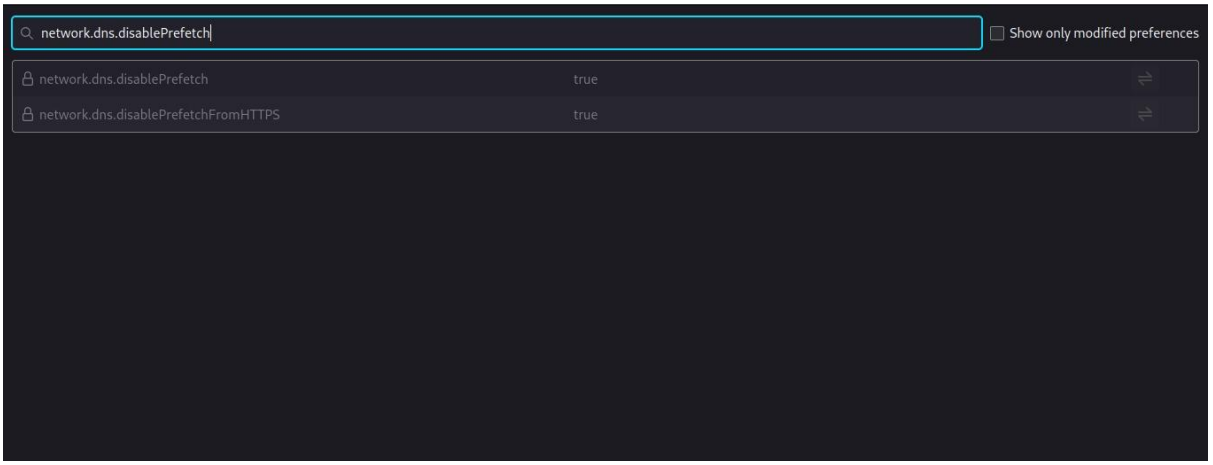
Fortalecer preferencias de SSL [L1]
Cambiar security.ssl3.rsa_des_ede3_sha a false
Cambiar security.ssl.require_safe_negotiation a true






Firefox about:config
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
browser.newtabpage.activity-stream.feeds.section.topstories
Show only modified preferences
browser.newtabpage.activity-stream.feeds.section.topstories false
browser.newtabpage.activity-stream.feeds.section.topstories.options {"api_key_pref":"extensions.pocket.oAuthConsumerKey","hidden":true,"provider_icon":"chrome://global/skin/icons/pocket.svg","provider_name":"Pocket","read_more_endpoint":"https://getpocket.com/explore/trending?src=fx_new_tab","stories_endpoint":"https://getpocket.cdn.mozilla.net/v3/firefox/global-recs?version=3&consumer_key=$apiKey&locale_lang=en-US&feed_variant=default_spocs_off","stories_referrer":"https://getpocket.com/recommendations","topics_endpoint":"https://getpocket.cdn.mozilla.net/v3/firefox/trending-topics?version=2&consumer_key=$apiKey&locale_lang=en-US","show_spocs":false}
services.sync.prefs.sync.browser.newtabpage.activity-stream.feeds.section.topstories true


browser.newtabpage.activity-stream.showSponsored
Show only modified preferences
browser.newtabpage.activity-stream.showSponsored false
browser.newtabpage.activity-stream.showSponsoredTopSites false
services.sync.prefs.sync.browser.newtabpage.activity-stream.showSponsored true
services.sync.prefs.sync.browser.newtabpage.activity-stream.showSponsoredTopSites true


network.dns.disablePrefetch
Show only modified preferences
network.dns.disablePrefetch true
network.dns.disablePrefetchFromHTTPS true


Firefox about:config
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
network.prefetch-next
Show only modified preferences
network.prefetch-next false

Resumen del L1

Desactivar telemetría:

- Deshabilita la telemetría en la página de nueva pestaña, relacionada con pings del navegador y envío de informes de fallos.
- Impide la telemetría asociada al proceso de incorporación de herramientas de desarrollo.
- Desactiva la telemetría en el toolkit del navegador y unifica las configuraciones, eliminando la URL del servidor de telemetría.

Desactivar Pocket:

- Evita la alimentación de Discoverystream, las historias principales y la inclusión de Pocket en la página de nueva pestaña.
- Oculta contenido patrocinado y desactiva la extensión Pocket para la gestión de contenido.

Desactivar prefetching:

- Deshabilita la precarga de DNS y detiene la precarga de la siguiente página web.

Desactivar JavaScript en PDF:

- Impide la ejecución de scripts en documentos PDF.

Fortalecer preferencias de SSL:

- Desactiva el cifrado RSA_DES_EDE3_SHA en SSL y exige una negociación segura en SSL.

Estas acciones buscan mejorar la privacidad, reducir la recopilación de datos no deseados y fortalecer la seguridad en la experiencia de navegación en Firefox.

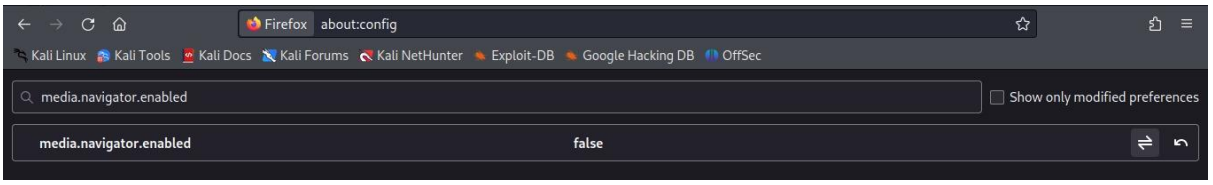
Configuraciones que pueden causar inconvenientes menores. [L2]

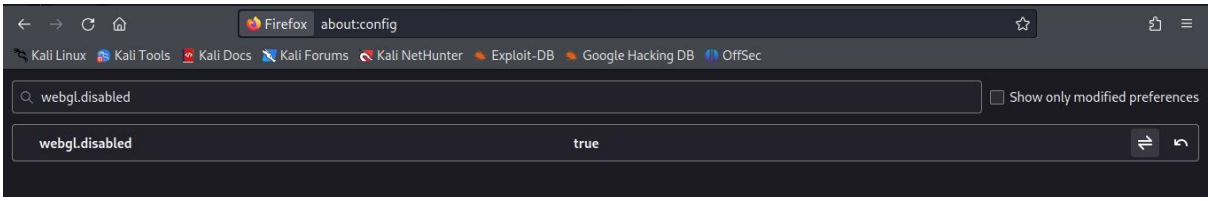
Desactivar soporte de geolocalización [L2]
Cambiar geo.enabled a false.

Desactivar soporte de notificaciones [L2]
Cambiar dom.webnotifications.enabled a false.

Desactivar WebRTC [L2]
Cambiar media.peerconnection.enabled a false
Cambiar media.navigator.enabled a false

Desactivar WebGL [L2]
Cambiar webgl.disabled a true.





Resumen del L2

Desactivar soporte de geolocalización:

- Impide que los sitios web accedan a la información de ubicación del usuario, mejorando la privacidad al prevenir la revelación no deseada de datos de geolocalización.

Desactivar soporte de notificaciones:

- Deshabilita las notificaciones web, reduciendo distracciones y preservando la privacidad al limitar la interacción con notificaciones no deseadas de los sitios web.

Desactivar WebRTC (Comunicaciones en tiempo real en la web):

- Evita la posibilidad de compartir información de audio y video sin consentimiento y mejorando la privacidad en comunicaciones en tiempo real.

Desactivar WebGL (Gráficos 3D en el navegador):

- Mejora la seguridad al prevenir posibles vulnerabilidades relacionadas con gráficos 3D en el navegador.

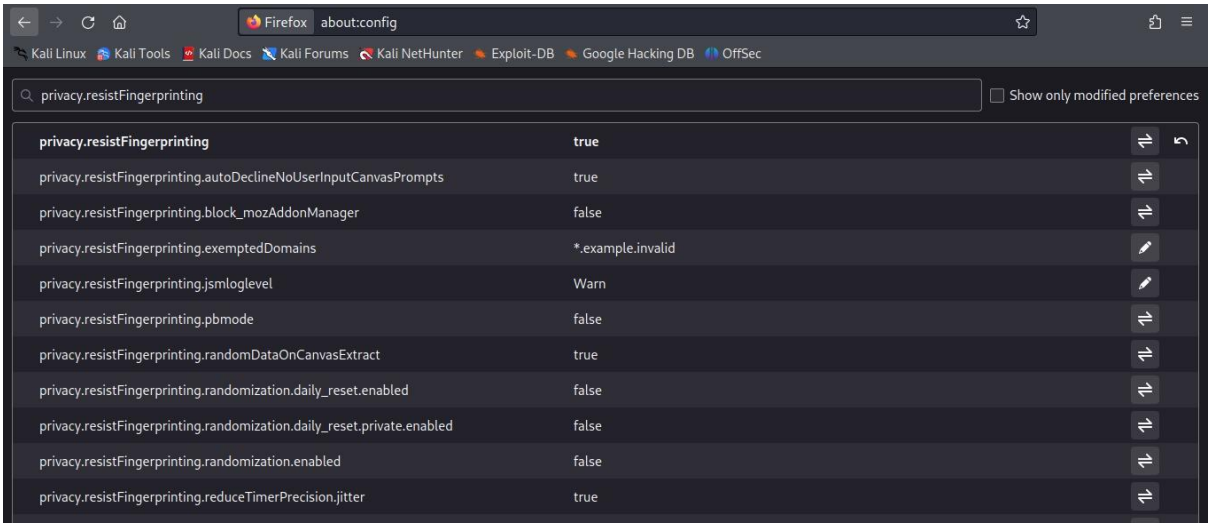
Estas configuraciones ofrecen mayor control sobre la privacidad y seguridad al desactivar funciones específicas en Firefox que podrían exponer datos del usuario o presentar posibles riesgos de seguridad.

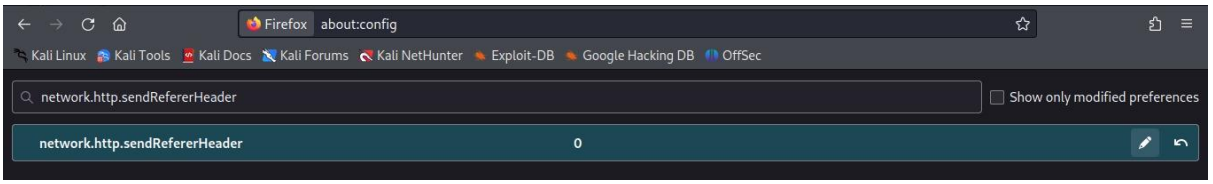
Configuraciones para usuarios avanzados. [L3]

Resistir la huella digital del navegador [L3]
Cambiar privacy.resistFingerprinting a true.

Desactivar encabezados de referencia [L3]
Cambiar network.http.sendRefererHeader a 0.

Cambiar comportamientos de cookies [L3]
Cambiar privacy.firstparty.isolate a true.





Resumen del L3

Resistir la huella digital del navegador [L3]:

- Permite que el navegador sea más resistente al seguimiento mediante la manipulación de la información que un sitio web puede recopilar sobre el usuario. Esto ayuda a preservar la privacidad al reducir la identificación única del navegador.

Desactivar encabezados de referencia [L3]:

- Impide que el navegador envíe información sobre la página de origen al acceder a un enlace. Esto ayuda a evitar el rastreo del usuario a través de referencias y mejora la privacidad al limitar la información compartida con sitios web externos.

Cambiar comportamientos de cookies [L3]:

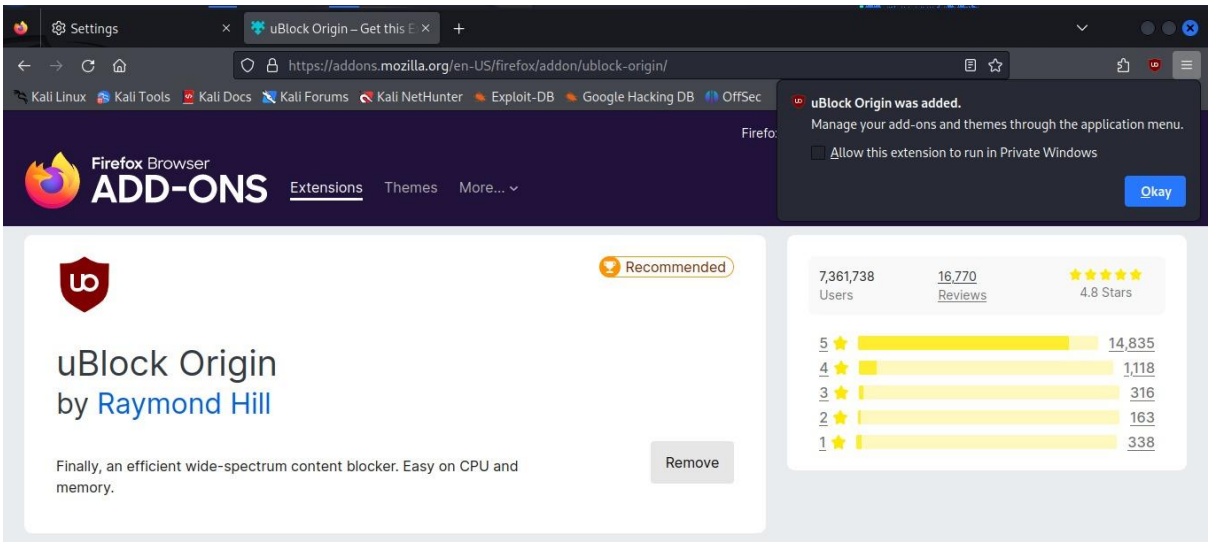
- Aísla las cookies de primeros partidos, lo que significa que las cookies de un sitio web no se compartirán con otros sitios. Esto mejora la privacidad al limitar la interconexión de datos entre diferentes dominios.

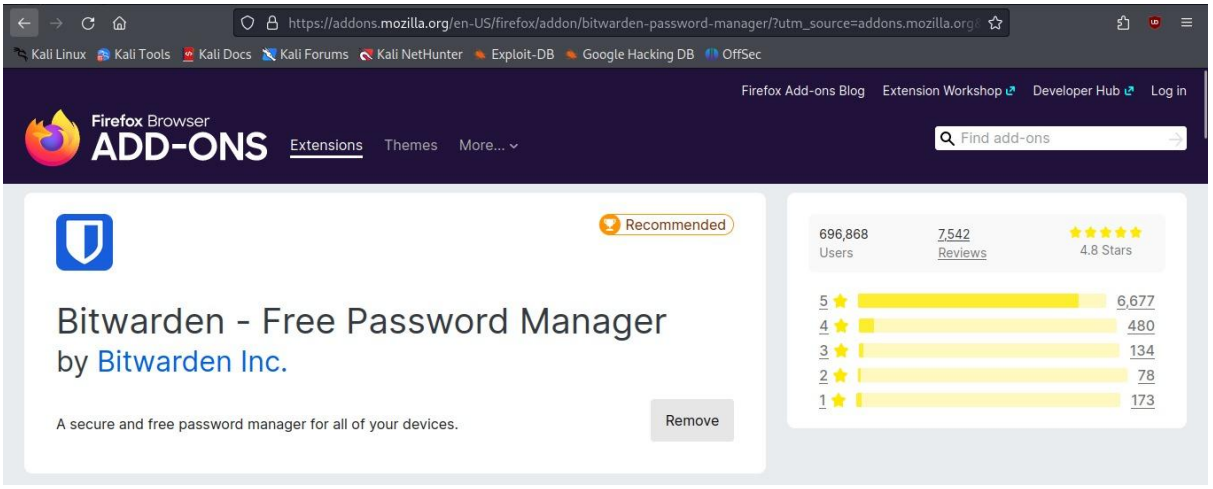
Estas configuraciones refuerzan la privacidad en Firefox al dificultar el seguimiento del usuario mediante la resistencia a la huella digital del navegador, al desactivar el envío de información de referencia y al aislar las cookies de primeros partidos, reduciendo así la interconexión de datos entre sitios web y mejorando la privacidad del usuario.

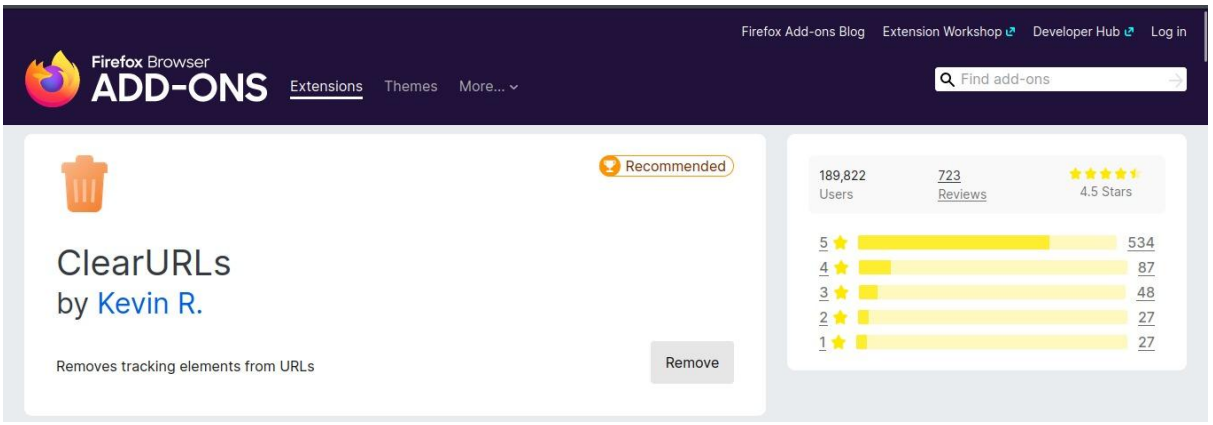
Instalar algunos Add-Ons

Ingresa en el navegador:

https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/
https://addons.mozilla.org/en-US/firefox/addon/bitwarden-password-manager/
https://addons.mozilla.org/en-US/firefox/addon/clearurls/







uBlock Origin:

- Propósito: Bloquear anuncios intrusivos, rastreadores, scripts maliciosos y otros elementos no deseados en las páginas web.
- Ventajas:
    - Mejora la velocidad de carga de las páginas al evitar la descarga de elementos innecesarios.
    - Aumenta la privacidad al bloquear rastreadores y scripts no deseados.
    - Reduce la distracción al eliminar anuncios molestos.

Bitwarden Password Manager:

- Propósito: Generar contraseñas seguras, rellenar automáticamente formularios y sincronizar datos entre varios dispositivos.
- Ventajas:
    - Facilita el proceso de inicio de sesión al autocompletar información de inicio de sesión.
    - Sincroniza de forma segura datos entre dispositivos para un acceso conveniente.

ClearURLs:

- Propósito: Ayudar a proteger la privacidad al evitar que sitios web y servicios de seguimiento recopilen información sobre las actividades de navegación.
- Ventajas:
    - Mejora la privacidad al eliminar parámetros de seguimiento presentes en las URL.
    - Evita redirecciones no deseadas y acorta las URL para una experiencia de navegación más limpia.
    - Reduce la exposición a servicios de seguimiento y publicidad basada en comportamiento.

Estas extensiones ofrecen mejoras significativas en términos de privacidad, seguridad y experiencia de navegación al bloquear contenido no deseado, gestionar contraseñas de forma segura y limpiar las URL de elementos de seguimiento.