Estudio y análisis del anonimato en la red: herramientas y técnicas para la maximización del anonimato

Adrián Mantilla Esteban

Grado de Ingeniería Informática

Seguridad Informática

Jorge Miguel Moneo

Andreu Pere Isern Deyà

13/06/2023

Universitat Oberta
de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	***Estudio y análisis del anonimato en la red: herramientas y técnicas para la maximización del anonimato***
Nombre del autor:	*Adrián Mantilla Esteban*
Nombre del consultor/a:	*Jorge Miguel Moneo*
Nombre del PRA:	*Andreu Pere Isern Deyà*
Fecha de entrega (mm/aaaa):	*06/2023*
Titulación o programa:	*Grado de Ingeniería Informática*
Área del Trabajo Final:	*Seguridad informática*
Idioma del trabajo:	*Castellano*
Palabras clave	*Anonimato, redes, seguridad*

Resumen del Trabajo

En este Trabajo Final de Grado se analizan navegadores web y tecnologías de anonimato, como las VPN, los proxies y la red Tor, junto con sus limitaciones y vulnerabilidades. Además, se tratan herramientas como Proxychains, Tails y Qubes OS, y se analizan técnicas de escaneo de puertos para evadir sistemas de detección de intrusos.

Los objetivos principales del trabajo son evaluar el nivel de anonimato y privacidad de estas tecnologías y la efectividad de las técnicas de ocultación de identidad y sigilo en el escaneo de puertos durante un ejercicio de pentesting.

La metodología utilizada incluye la explicación teórica de los diferentes elementos y tres pruebas prácticas:

En la primera prueba, se evaluó la privacidad de los navegadores.

En la segunda prueba, se configuró una página web sobre un servidor Apache2, al que se conectó un cliente utilizando diferentes tecnologías y técnicas de anonimato, con el fin de comprobar su eficacia.

En la tercera prueba, se llevaron a cabo pruebas de escaneos de puertos utilizando técnicas de sigilo y ocultación de identidad para determinar si era posible evadir un sistema de detección de intrusiones y mantener la identidad del atacante oculta.

Los resultados obtenidos demuestran que estas tecnologías permiten obtener un alto nivel de anonimato siempre y cuando se configuren correctamente y se tengan en cuenta las limitaciones y posibles vulnerabilidades. Respecto al escaneo de puertos, destacan el uso de métodos de ocultación de IP y escaneo Idle para evitar ser identificados.

Abstract

In this Final Degree Project, web browsers and anonymity technologies, such as VPNs, proxies and the Tor network, are analyzed along with their limitations and vulnerabilities. In addition, tools like Proxychains, Tails, and Qubes OS are discussed, and port scanning techniques to evade intrusion detection systems are analyzed.

The main objectives of this work are to evaluate the level of anonymity and privacy of these technologies and the effectiveness of identity concealment and stealth techniques in port scanning during a pentesting exercise.

The methodology used includes the theoretical explanation of the different elements and three practical tests:

In the first test, browser privacy was tested.

In the second test, a web page was configured on an Apache2 server, to which a client was connected using different technologies and anonymization techniques, in order to check its effectiveness.

In the third trial, tests of port scans using stealth and identity concealment techniques were conducted to determine if it was possible to evade an intrusion detection system and keep the attacker's identity hidden.

The results obtained show that these technologies allow to obtain a high level of anonymity as long as they are configured correctly and the limitations and possible vulnerabilities are taken into account. Regarding port scanning, they highlight the use of IP concealment methods and Idle scanning to avoid being identified.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1. Contexto y justificación del Trabajo

Actualmente, internet cuenta con aproximadamente 5,16 billones de usuarios, un 64,4% de la población mundial [1]. En un mundo cada vez más digitalizado, la necesidad de proteger la información personal y garantizar la seguridad de las redes se ha vuelto crítica. Los ejercicios de pentesting (prueba de penetración) se han convertido en una práctica habitual en la industria de la ciberseguridad, y las empresas están cada vez más preocupadas por proteger sus sistemas y datos de posibles ataques. Prueba de ello es que, en el año 2020, el 89% de los líderes ejecutivos consideraban la ciberseguridad como una alta prioridad [2].

En este trabajo se analizan y evalúan diversas técnicas y herramientas que pueden ser utilizadas para maximizar el anonimato en la fase de recopilación activa de información de un ejercicio de pentesting. Esta fase resulta de gran importancia, ya que proporciona información valiosa sobre las vulnerabilidades y debilidades de los sistemas informáticos de la empresa. Durante la misma, existe gran riesgo de ser detectado, pues se interactúa directamente con el objetivo. Por ello, resulta de gran importancia utilizar técnicas que reduzcan este riesgo y que permitan poner a prueba las defensas de la compañía y su eficiencia [3].

Este trabajo ofrece soluciones prácticas que evitan llamar la atención del objetivo y comprometer el anonimato durante la recopilación activa de información, lo que puede ser de gran utilidad para profesionales de la ciberseguridad y el pentesting. Además de ayudar a prevenir futuros ataques.

La recopilación de información no solo se realiza en el contexto de los ejercicios de pentesting, sino también por parte de algunos sitios web que rastrean los hábitos de navegación y el comportamiento de los usuarios [4]. Además, actualmente, es común que los usuarios se conecten a internet a través de redes Wi-Fi públicas, como las de hoteles, centros comerciales o aeropuertos sin adoptar medidas de protección, incrementando los riesgos de sufrir vulneraciones en su privacidad y ciberataques, ya que estas redes son generalmente menos seguras y están más expuestas a ser utilizadas por ciberdelincuentes [5]. El uso de técnicas y herramientas como las VPNs (Redes virtuales privadas) o la red Tor (The Onion Router) y sistemas operativos orientados a la seguridad y el anonimato como Tails o QubesOS puede evitar que terceras personas rastreen la actividad en línea del usuario y ayudan a proteger su privacidad frente a la exposición indeseada de datos de carácter personal [6].

Actualmente, garantizar el acceso a internet y proteger la libertad de expresión de todos los ciudadanos es un importante desafío que debemos enfrentar [7]. Desde el

año 2015, casi uno de cada tres países ha ejercido algún tipo de censura con relación a internet [8]. Algunas técnicas de anonimato permiten a los usuarios acceder a contenido que de otra manera estaría restringido en su país o región [9], esto puede incluir páginas web y redes sociales bloqueadas por el gobierno o servicios de transmisión de vídeo o mensajería censurados.

Ante un entorno global cada vez más afectado por la ciberdelincuencia, el control de la información y la censura se hace imperativo fomentar una mayor conciencia y educación acerca del uso de técnicas y herramientas de anonimato. Por ello, este trabajo resulta relevante para la sociedad en general, pues recopila, describe y analiza una selección de herramientas y técnicas de gran utilidad para la defensa de la libertad de expresión, el acceso a la información, la privacidad, y la seguridad de los usuarios y de las empresas.

1.2. Objetivos del trabajo

El presente Trabajo Final de Grado cuenta con dos objetivos generales:

1- Analizar técnicas y herramientas utilizadas para garantizar el anonimato en la red y proteger la privacidad de los usuarios, como las VPN, los proxies, la red Tor o su uso combinado.

2- Seleccionar, analizar y realizar pruebas con técnicas que permitan mantener el anonimato en la fase de recopilación activa de información durante un ejercicio de pentesting. Como los escaneos con sigilo, escaneos con ocultación de identidad o los escaneos a través de un host zombi.

Además, tiene los siguientes objetivos específicos:

1- Estudiar los distintos tipos de cookies, sus efectos en la privacidad de los usuarios y proponer configuraciones que optimicen la privacidad en algunos de los principales navegadores web.
2- Analizar las vulnerabilidades y limitaciones de la red Tor, los proxies y las VPN en la obtención del anonimato e investigar técnicas que permitan reducirlas.
3- Realizar pruebas para evaluar la efectividad de diversas herramientas y técnicas de anonimato en la red.
4- Exponer las ventajas y desventajas de utilizar algunas de estas técnicas y herramientas.

1.3. Estado del arte

Actualmente, existen diversas tecnologías disponibles para garantizar el anonimato en la red, en el año 1999 se publica el protocolo PPNP (Point-to-Point Tunneling Protocol) creado por Gurdeep Singh-Pall de Microsoft [10] que permite implementar redes privadas virtuales. En el año 2002 se implementa la red Tor [11] una red que enrutaba el tráfico a través de múltiples servidores que realizaban el cifrado de estos creando las llamadas “capas de cebolla” y cuyo objetivo era que internet se pudiera utilizar con

la mayor privacidad posible. Posteriormente han ido apareciendo otras redes que protegen el anonimato como I2P (The Invisible Internet Project) o Freenet.

Algunas organizaciones como OWASP (Open Web Application Security Project) ofrecen una gran cantidad de recomendaciones para mejorar la seguridad en internet. Además, existe una extensa bibliografía sobre técnicas y herramientas para conseguir el anonimato. Como, por ejemplo:

- Deep Web: TOR, FreeNET & I2P Privacidad y Anonimato [12]: este libro realiza un análisis de las diferentes técnicas y herramientas que se utilizan para mejorar la privacidad e implementar el anonimato en la red, centrándose especialmente en el funcionamiento de las redes TOR, FreeNet e I2P.

- Ethical guide to cyber anonymity: Concepts, tools,and techniques to be anonymous from criminals,... unethical hackers, and governments [13]:Es una guía que explica la importancia del anonimato en internet y como mantenerse anónimo mediante la configuración y uso de ciertas herramientas.

El anonimato, no solo es importante para navegar por la red, sino que también es empleado en prácticas de seguridad informática como el pentesting, pruebas en las que se simula un ataque cibernético real sobre un objetivo para conocer sus vulnerabilidades y posteriormente, poder fortalecerlas. Diferentes técnicas y herramientas han sido estudiadas en una gran cantidad de bibliografía, entre la que se encuentra:

- Mastering Kali Linux for Advanced Penetration Testing - Fourth Edition [14]: Explica diferentes técnicas avanzadas de pentesting con la distribución Kali Linux, así como técnicas enfocadas a no ser detectados durante la realización de este.

También se han realizado estudios sobre herramientas utilizadas durante la recopilación activa de información en el pentesting, como por ejemplo Nmap, un software de código abierto utilizado para detectar los hosts de una red y el escaneo de puertos: Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool [15].

En conclusión, existe una gran cantidad de bibliografía sobre el anonimato en las redes, que permite una amplia investigación. Este trabajo ofrece una revisión detallada de algunas de las mejores técnicas y herramientas de anonimato disponibles, incluyendo una selección de aquellas que permiten maximizar la privacidad y el anonimato durante la fase de recopilación activa de información en una prueba de pentesting.

1.4. Impacto ético-social, de sostenibilidad y de diversidad

En el año 2021 los bloqueos de redes sociales por parte de los gobiernos afectaron a 250 millones de personas [8]. Durante el año 2020 se documentaron 155 apagones de

internet en 29 países diferentes, afectando especialmente a países en conflicto, procesos electorales y protestas sociales [16]. Tecnologías de anonimato como la red Tor, los proxies o las VPN pueden permitir que los usuarios eviten estos medios de censura. Por ello, el anonimato en la red puede considerarse como una forma de proteger la seguridad, la privacidad y la libertad de expresión de las personas.

Desde el punto de vista de la sostenibilidad, el uso de navegadores web y de herramientas de anonimización como las VPN puede producir un aumento considerable de la huella de carbono y del consumo de energía de los usuarios [17][18], por lo que se deben seleccionar aquellos proveedores que sean más respetuosos con el medio ambiente y promover el uso responsable y sostenible de estas herramientas.

El anonimato en la red fomenta que personas en riesgo de exclusión social, pertenecientes a minorías o que sufren discriminación por motivo de raza, género, edad, condición sexual, religión u otras características índole personal, puedan expresarse libremente sin miedo a represalias o acoso. Sin embargo, el anonimato no solo se utiliza para ejercer derechos y libertades, sino que también es utilizado por criminales para la realización de actividades delictivas y por personas que por la sensación de impunidad amenazan, realizan acciones de acoso, difunden noticias falsas y promueven la discriminación y los discursos de odio [19].

La Organización de las Naciones Unidas ha establecido 17 Objetivos de Desarrollo Sostenible (ODS), entre los que se incluyen lograr una educación de calidad, reducir las desigualdades, fomentar el trabajo decente y el crecimiento económico y lograr una industria, innovación e infraestructura sostenibles [20]. Para alcanzar estos ODS, es esencial que las personas tengan acceso a la información, e internet es una fuente inagotable de conocimiento, que ofrece libros y revistas digitales, estudios científicos, boletines electrónicos, bibliotecas digitales y foros, entre otros recursos.

Cuando los gobiernos limitan el acceso de los usuarios a internet, están restringiendo el acceso igualitario e inclusivo a la formación de las personas y afectando gravemente el derecho a la educación y el acceso a una educación superior de calidad. Además, las tecnologías digitales e internet ofrecen nuevas oportunidades de trabajo y crecimiento económico, impulsan la innovación y el desarrollo de infraestructuras y permiten un mundo más justo y con instituciones más sólidas, ya que facilitan la participación ciudadana, la igualdad de oportunidades y el reparto equitativo de la riqueza.

Ante los puntos expuestos, es necesario considerar el impacto ético-social, de sostenibilidad y de diversidad del trabajo que produce el uso de herramientas y técnicas de anonimato. Por lo que se debe promover su uso responsable, enfocado a defender la consecución de los objetivos de desarrollo sostenible y los derechos y libertades de las personas.

1.5. Descripción de la metodología

La metodología se divide en las siguientes fases:

- Revisión bibliográfica previa:

Se realiza una revisión general bibliográfica sobre el anonimato en la red que permita establecer un marco teórico de referencia.

- Redacción del plan de trabajo y selección bibliográfica:

- Se concreta el tema a tratar y se eligen las palabras clave.
- Se profundiza en la revisión bibliográfica de diversas fuentes, entre las que se encuentran libros y artículos científicos sobre la privacidad y el anonimato en la red y páginas web oficiales de distintas herramientas.

- Instalación y configuración del entorno de trabajo:

Tras la revisión bibliográfica procederemos a montar una máquina virtual VirtualVox con la distribución Kali Linux sobre un sistema operativo host Windows 10, que será el escenario en el que realizaremos pruebas sobre algunas de estas tecnologías como máquina atacante.

Posteriormente, procederemos a montar una máquina virtual Metasploitable 3 ubuntu y una máquina virtual Metasploitable 3 Windows Server 2008 sobre el mismo sistema host que la anterior. Estas serán utilizadas en el apartado “Fase de obtención activa de información” para la realización de pruebas.

- Análisis y síntesis de información:

Se estudian los distintos tipos de cookies y como afectan a nuestra privacidad en la red. Así mismo, se analizan distintos navegadores y su configuración de la privacidad, con el fin de garantizarla.

Se seleccionarán y analizarán las principales tecnologías, técnicas y herramientas utilizadas por los usuarios para conseguir el anonimato y se analizarán las vulnerabilidades de tres de las tecnologías de anonimización más conocidas, los proxies, las VPN y la red Tor, junto con opciones que permitan optimizar la seguridad de estas, como su uso combinado o los Tor Bridges.

Además, se realizará el análisis de diferentes herramientas y técnicas que ayuden a mantener el anonimato y dificulten nuestra detección durante la fase de recopilación activa de información durante un ejercicio de pentesting. Algunas de las técnicas estudiadas serán la ocultación de la identidad o el escaneo con sigilo.

- Realización de pruebas:

Durante las pruebas analizaremos el tráfico de paquetes de red con el programa Wireshark, con el fin de verificar los resultados producidos por las diferentes técnicas y herramientas.

- Redacción de conclusiones:

Se podrán realizar conclusiones sobre los distintos apartados, sobre la consecución de los objetivos y generales del trabajo.

1.6. Planificación del trabajo

Nombre	Fecha de inicio	Fecha de fin
TFG	1/3/23	7/7/23
Documentación previa	1/3/23	8/3/23
Desarrollo del plan de trabajo	9/3/23	13/3/23
Entrega PEC 1	14/3/23	14/3/23
Instalación y configurac...	15/3/23	17/3/23
Análisis de cookies y navegadores web	18/3/23	22/3/23
Análisis de las principa...	23/3/23	1/4/23
Estudio de las posibles ...	2/4/23	6/4/23
Análisis de técnicas y h...	7/4/23	10/4/23
Entrega PEC 2	12/4/23	12/4/23
Técnicas de anonimización...	13/4/23	16/4/23
Técnicas de escaneo con ...	17/4/23	20/4/23
Escaneo de puertos con s...	21/4/23	24/4/23
Crear un scanner mediant...	25/4/23	28/4/23
Otras técnicas de escane...	1/5/23	6/5/23
Entrega PEC 3	9/5/23	9/5/23
Redacción de la memoria	10/5/23	19/5/23
Conclusión	22/5/23	24/5/23
Entrega PEC 4	13/6/23	13/6/23
Desarrollo de la presentación virtual	14/6/23	18/6/23
Entrega de la presentación virtual	20/6/23	20/6/23
Defensa del TFG	26/6/23	7/7/23

Figura 1: Relación de tareas

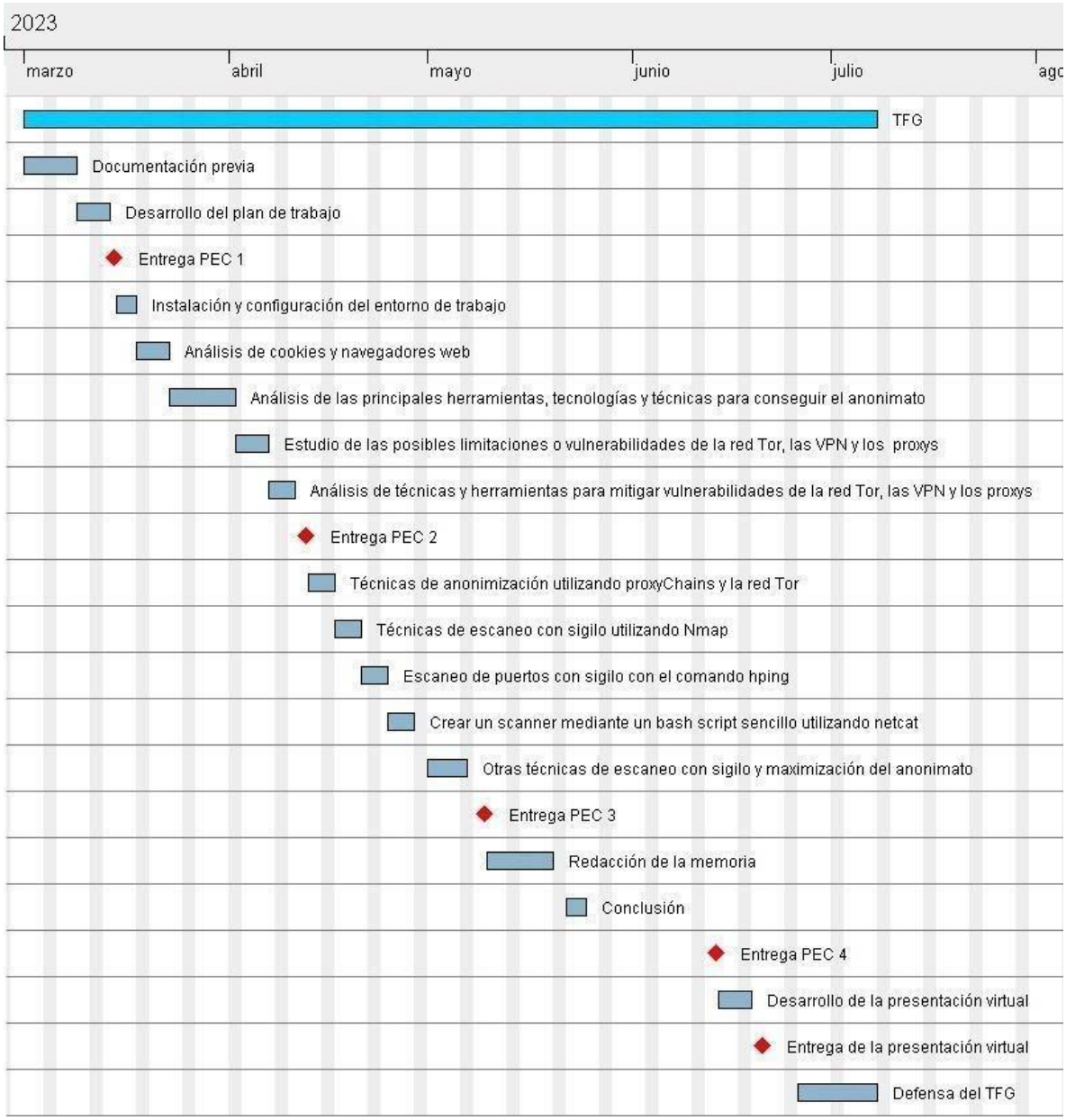

Figura 2: Diagrama de Gantt

1.7. Tareas

- Documentación previa

    - Se obtiene bibliografía sobre el ámbito del trabajo a través de repositorios digitales, buscadores de bibliotecas, Google Scholar y páginas oficiales de herramientas.

- Desarrollo del plan de trabajo

- Se define el tema concreto del trabajo, su alcance, objetivos, palabras clave, problema a resolver, el estado del arte y se realiza la planificación temporal del mismo.

- Instalación y configuración del entorno de trabajo

  - Se realiza la instalación de las máquinas virtuales y se realiza su configuración.

  - Se instala el sniffer Wireshark para comprobar el tráfico de red durante las pruebas.

- Análisis de las cookies, cookies de terceros y cookies persistentes, como afectan a la privacidad del usuario y la configuración de la privacidad en varios navegadores web.

- Análisis de las principales herramientas, tecnologías y técnicas para conseguir el anonimato en la red. (VPN, Proxy, Tor, I2P, Whonix, Tails, QubesOs, etc)

- Análisis de las posibles limitaciones o vulnerabilidades de la red Tor, las VPN y los proxies en la obtención del anonimato. (Nodos de entrada y salida en Tor, VPN que almacenan logs, proxies cuya información puede estar siendo observada…)

- Análisis de técnicas y herramientas para mitigar las vulnerabilidades de la red Tor, las VPN y los proxies.

- Fase de obtención activa de información durante un ejercicio de pentesting:

  - Técnicas de anonimización utilizando proxyChains y la red Tor.

  - Técnicas de escaneo con sigilo utilizando Nmap

  - Escaneo de puertos con sigilo con el comando hping

  - Crear un scanner mediante un bash script sencillo utilizando netcat

  - Examinar otras técnicas de escaneo con sigilo y optimización del anonimato.

- Redacción de la memoria

- Conclusión

- Desarrollo de la presentación virtual

- Defensa del TFG

1.8. Riesgos

1- Planificación incorrecta: Los periodos definidos en la realización de tareas podrían no ajustarse al tiempo real necesario para su realización, dando lugar a no poder cumplir con los objetivos temporales fijados.

Para prevenir este riesgo se deben ajustar los plazos a las condiciones reales de tiempo semanal disponible para dedicar a la realización de tareas.

2- Riesgo de contingencia: En caso de que alguna tarea no pueda ser realizada o completada en el plazo objetivo y exista tiempo material para realizarla antes de la entrega final, deberá realizarse en los periodos con menor carga de trabajo.

Pueden surgir eventos imprevistos durante la realización del trabajo que no permitan seguir el plan temporal establecido.

Una medida para contrarrestar este riesgo sería limitar el alcance del trabajo.

3- Fuentes no fiables: Actualmente internet dispone de una cantidad inmensa de información, sin embargo, no toda cumple con los criterios de rigurosidad necesarios para la realización de un trabajo académico.

Para evitar este riesgo, se debe utilizar información proveniente de fuentes oficiales y fiables.

4- Falta de recursos bibliográficos: Es posible que no se encuentren recursos y bibliografía sobre algún tema.

5- Perdida de datos: Al utilizar medios digitales para la realización del trabajo existe la posibilidad de perder información que no haya sido guardada correctamente o sufrir ataques que puedan ponerla en riesgo.

Se realizarán copias de seguridad de forma regular en una memoria usb para asegurar los avances.

1.9. Cambios en la planificación y tareas

Debido a que la extensión final del TFG es superior a la prevista inicialmente, se decide incluir las siguientes tareas como anexos:

- Escaneo de puertos con sigilo con el comando hping
- Crear un scanner mediante un bash script sencillo utilizando netcat

Además, por el mismo motivo, se decide no incluir otras técnicas de escaneo con sigilo y optimización del anonimato fuera de las presentadas para Nmap y hping.

2. Anonimato y privacidad en la web

En internet, la privacidad es la capacidad del usuario para decidir qué información comparte y con quién, mientras que el anonimato, es la capacidad mantener oculta su identidad. Aunque son términos diferentes, se encuentran relacionados, puesto que algunos elementos que recopilan información del usuario pueden llegar a poner en riesgo su anonimato, llegando incluso a construir un perfil único de este.

En este capítulo se abordan dos aspectos cruciales del anonimato y la privacidad en la red: los navegadores web y las cookies, pequeños ficheros que los sitios web almacenan en los dispositivos de los usuarios para ofrecer una mejor experiencia de navegación, pero también para rastrearlos y obtener información sobre sus hábitos de navegación. Además, se incluye una guía de configuración que aborda recomendaciones específicas para una selección de navegadores web. Estas configuraciones ayudarán a optimizar la protección de la información personal y limitar el seguimiento no deseado por parte de terceros.

2.1. ¿Qué son las cookies?

Las cookies son ficheros de texto de pequeño tamaño que contienen información enviada por un sitio web y que son almacenados en el navegador del usuario. El objetivo de estos ficheros es permitir a la página recordar la actividad previa del navegador, ya que el protocolo HTTP se trata de un protocolo sin estado, en el que cada petición-respuesta entre el servidor web y el cliente es independiente y no permite guardar la información generada en la interacción [21].

Cuando un usuario entra por primera vez en una página web que utiliza cookies, esta envía una cookie que será almacenada por el navegador del cliente. Cuando se vuelva a acceder a las páginas web del mismo servidor, con el mismo navegador y con el mismo ordenador, esta cookie será enviada al servidor web y reconocida. Este sistema produce un reconocimiento incompleto del usuario, pues pese a que se requiere que se cumplan los tres requisitos (mismo ordenador, mismo navegador y servidor web) podría tratarse de usuarios diferentes utilizando la misma computadora.

Las cookies permiten ofrecer una mejor experiencia al usuario recordando información de inicios de sesión, formularios, elementos del carrito de compra en las páginas e-commerce, preferencias de búsqueda, etc [21]. Sin embargo, a menudo generan controversia, ya que estas pueden ser almacenadas en el disco duro del usuario sin que sea consciente, y también pueden tener funciones de rastreo, que registran los diferentes sitios web que el usuario ha visitado y sus hábitos de navegación. Las cookies también pueden contener información sensible como contraseñas o números de tarjetas de crédito, que ponen en riesgo la seguridad y privacidad del usuario ante posibles ataques.

2.1.1. Tipos de cookies

Existen diferentes tipos de cookies y no todas afectan de igual forma a la privacidad. Desde mayo del año 2018 con la entrada en vigor del Reglamento General de Protección de Datos (RGPD) [22], las páginas web están obligadas a informar del tipo de cookies que emplean, su finalidad y procedencia. Sin embargo, muchos usuarios simplemente aceptan estas cookies sin pararse a leer sus características.

Las cookies pueden ser clasificadas de las siguientes formas:

Entidad que las gestiona:

- Cookies propias: Son creadas, enviadas y gestionadas por el propio dominio desde el que se presta el servicio al que ha accedido el usuario.

- Cookies de terceros: En este caso, las cookies son enviadas por un dominio diferente al visitado por el usuario, que tiene contenido en la página web consultada, como imágenes o anuncios. Estas cookies no suelen ser necesarias para una correcta navegación y recogen información que posteriormente será utilizada para mostrar anuncios personalizados o realizar estudios de mercado.

Tiempo de permanencia activa:

- Cookies de sesión: Estas cookies se mantienen activas durante la sesión del usuario en el sitio web y recopilan información necesaria únicamente para esta sesión. Una vez que la sesión termina, son eliminadas de forma automática.

- Cookies persistentes: Pueden permanecer almacenadas y activas durante un periodo definido por el creador de la cookie, este periodo puede ser de incluso años y se especifica en la cabecera de respuesta HTTP Set-cookie con el atributo “Expires” para indicar una fecha concreta o Max-Age si se quiere indicar un valor temporal [21].

Según la agencia española de protección de datos (AEPD) [23] podemos distinguir los siguientes tipos de cookies en función de su Finalidad:

- Cookies técnicas: Estas cookies son necesarias para el correcto funcionamiento de la página web, plataforma o aplicación y para el uso de sus servicios. Entre sus funciones podemos encontrar: identificar la sesión, controlar el tráfico y la comunicación de datos, acceder a zonas de acceso restringido o utilizar elementos de seguridad. No es obligatorio que notifiquen al usuario su instalación en el equipo siempre y cuando su finalidad sea la de permitir un servicio que este ha solicitado.

- **Cookies de personalización:** Permiten personalizar la experiencia del usuario, ya sirven para recordar características y opciones generales de navegación por la página web. Como, por ejemplo, el idioma, tipo de navegador que ha realizado el acceso o la cantidad de resultados a mostrar tras realizar una búsqueda. Si es el usuario quien selecciona estas características, no existirá obligación de notificar su instalación.

- **Cookies de análisis:** Almacenan información sobre el comportamiento del usuario en la página web con fines analíticos que permitan realizar mejoras sobre la misma.

Por ejemplo, cuantas veces visita la página, cuanto tiempo permanece en ella o a qué hora la ha visitado.

- **Cookies de publicidad comportamental:** Recopilan información sobre los hábitos, comportamientos y preferencias del usuario con el fin de crear un perfil de interés y ofrecer publicidad personalizada. Por ejemplo, pueden realizar un análisis de las páginas visitadas por el usuario, búsquedas, etc. Estos perfiles de interés pueden ser posteriormente vendidos o compartidos con anunciantes publicitarios.

De entre las anteriores, las cookies de terceros son las que presentan un mayor riesgo para la privacidad, ya que pueden traquear al usuario a través de diferentes sitios web. Además, pueden almacenar diferentes tipos de información privada del usuario, como, por ejemplo: dirección de correo electrónico, edad, sexo, tiempo de permanencia en páginas web, documentos identificativos, patrones de comportamiento, preferencias de compra… Estas cookies se almacenan tanto en el disco duro del usuario como en el servidor del anunciante y permiten crear un perfil de usuario con la intención de ofrecer publicidad personaliza.

2.1.2. ¿Cómo funcionan las cookies de terceros?

Supongamos una página web llamada "web.com". Esta página contiene un banner de publicidad de otro sitio llamado "webrastreo.com". Cuando el usuario accede a la página web.com, se produce una conexión a webrastreo.com y se envían cookies de terceros con un identificador único, las cuales son almacenadas en el navegador del usuario. Cuando el usuario visita otra página, por ejemplo, "otraweb.com", que también contiene un banner de publicidad de webrastreo.com, se produce una comunicación entre las cookies de terceros almacenadas en el navegador del usuario y el servidor de webrastreo.com. De esta forma y mediante el valor del identificador único, webrastreo.com puede saber que el usuario ha visitado tanto web.com como otraweb.com. Este mismo proceso se repetirá cada vez que el usuario visite una página que contenga un banner de publicidad de webrastreo.com, permitiéndole realizar el seguimiento del usuario.

2.1.3. Cookies persistentes

Supercookies

A diferencia de las cookies, las supercookies no son enviadas por un sitio web y almacenadas en el navegador web. Sino que son insertadas por el proveedor de servicios de Internet (ISP) a nivel de red como encabezados de identificador único (UIDH), lo que hace imposible su eliminación por parte del usuario [24].

Cookies Flash

Son ficheros con extensión .sol enviados por sitios web que utilizan el software Adobe Flash. Pueden recopilar la misma información que las cookies HTTP y son capaces de almacenar gran cantidad de información, pudiendo llegar a ocupar hasta 100kb. Ofrecen gran persistencia, ya que no tienen fecha de expiración por defecto y son

almacenadas en el equipo del usuario en un directorio de datos de la aplicación flash player, con lo cual, si eliminamos las cookies tradicionales del navegador web, las cookies flash no se verán afectadas [25].

Evercookie

Se trata de una API de JavaScript desarrollada por Samy Kamkar para crear cookies extremadamente persistentes [26]. Estas se alojan en múltiples partes del navegador web del cliente y que son capaces de reestablecerse tras su borrado, algo que dificulta en gran medida que puedan ser eliminadas de forma definitiva. Si estas cookies son eliminadas de algunos de los espacios del navegador, mientras alguna permanezca intacta, el sitio web que ha implementado Evercookie detectará que han intentado eliminarlas y volverán a reestablecerse. Únicamente podrán ser eliminadas si se consiguen eliminar de todos los espacios en los que se encuentran almacenadas.

2.2. Navegadores web

Un navegador web, es una aplicación de software que permite visitar sitios web. Cuando un usuario introduce en su navegador la dirección de una página web, se realiza una solicitud al servidor web que la contiene. Estos servidores, transmiten los ficheros de la página al navegador web mediante el Protocolo de Transferencia de Hipertexto (HTTP) o el Protocolo de Transferencia de Hipertexto Seguro (HTTPS) y son transformados por un software llamado motor de renderizado a texto e imágenes, de forma que el contenido sea fácilmente interpretable por el usuario [27].

Existen una gran cantidad de navegadores web, sin embargo, no todos ofrecen las mismas características de seguridad, privacidad y anonimato. En esta sección, se presenta una guía de configuración para optimizar la seguridad y privacidad de una selección de tres navegadores web, Firefox, Brave y Tor Browser, que se destacan por ofrecer características sólidas de seguridad y privacidad para sus usuarios y por contar con una comunidad de desarrollo activa y comprometida. La configuración será realizada de forma que permita una navegación funcional, es decir, cuando configuramos el navegador con opciones de seguridad muy restrictivas pueden aparecer errores en las páginas que no permitan una navegación satisfactoria para el usuario. Por tanto, en la configuración ofrecida, se valora la optimización de la seguridad manteniendo la funcionalidad de la navegación.

Además de esta guía, se realiza una comparativa de los tres navegadores (Firefox Versión 112.0.2 (64-bit), Brave Versión 1.50.121 Chromium: 112.0.5615.138 (Build oficial) (64 bits) y Tor Browser versión 12.0.4 (based on Mozilla Firefox 102.9.0esr) (64-bit)), en la que se comparan diferentes funciones de seguridad, privacidad y anonimato. También se realiza una comparativa de puntuaciones obtenidas en varias páginas web que ofrecen test para comprobar características de privacidad y anonimato de los navegadores.

2.2.1. Mozilla Firefox

Se trata de un navegador gratuito y de código abierto presentado en el año 2004 como Firefox 1.0 [28]. Actualmente implementa un gran número de opciones de seguridad y es utilizado por millones de personas en todo el mundo, tanto en ordenador como en dispositivos móviles.

2.2.1.1. Guía de configuración de Mozilla Firefox

Para comenzar pulsaremos en el botón (≡), situado en la esquina superior derecha del navegador y seleccionaremos “Ajustes”. En el menú general iremos a la sección “Actualizaciones de Firefox” y activaremos las actualizaciones automáticas, ya que es importante que el navegador se encuentre actualizado para evitar errores y mantener la seguridad.

En Firefox, JavaScript se encuentra activado por defecto. Esto crea vulnerabilidades que pueden ser aprovechadas por un atacante. Para desactivarlo, debemos escribir “about:config” en la barra de búsqueda y a continuación buscar el parámetro “javascript.enabled”. Una vez encontrado, cambiaremos su valor de “true” a “false”.

Firefox, ofrece un menú de privacidad y seguridad en el que se pueden elegir diferentes configuraciones para evitar que los rastreadores en línea recopilen nuestra información.

Para acceder a este menú, dentro de ajustes, pulsaremos en la opción “Privacidad&Seguridad.

<u>Protección contra el rastreo mejorada</u>

Por defecto, el navegador viene configurado con la opción estándar, que bloquea los siguientes elementos:

- Rastreadores sociales: Son rastreadores que las redes sociales colocan en sitios web externos a ellas para recopilar datos de navegación del usuario, con el objetivo de ofrecer anuncios personalizados.

- **Cookies de sitios cruzados en todas las ventanas:** Son las llamadas cookies de terceros, que permiten a un sitio web diferente al visitado por el usuario realizar un seguimiento de su navegación.

- **Rastreadores de contenido:** Son rastreadores cuyo código se encuentra incluido dentro de vídeos, botones, anuncios y otros tipos de contenido de una página web.

- **Criptomineros:** Se tratan de scripts que son implantados en el ordenador del usuario, sin consentimiento, por piratas informáticos, con el fin de obtener recursos y potencia informática para realizar el minado de criptomonedas. Lo que reduce el rendimiento del equipo e incrementa el consumo energético del mismo.

- **Fingerprinters:** Recopilan información del equipo del usuario, como elementos de hardware instalados, configuraciones del navegador, extensiones y aplicaciones

instaladas o resolución de pantalla, para crear un perfil único de usuario y rastrear su navegación.

Se debe tener en cuenta que en este modo los rastreadores de contenido únicamente son bloqueados cuando se realiza la navegación utilizando una ventana privada y que si queremos bloquearlos utilizando la ventana estándar deberemos cambiar la configuración de privacidad del navegador.

Firefox utiliza un sistema llamado “Enhanced Tracking Protection blocks” que bloquea una lista de rastreadores conocidos ofrecida por la compañía Disconnect [29]. Dentro de este sistema se encuentra “Total Cookie Protection”, que se encuentra activo por defecto en la ventana estándar y que mantiene cookie jar diferentes para cada página web que visita el usuario [30]. De esta forma, limita las cookies de terceros al sitio web que las envía e impide que puedan seguir al usuario cuando visita otros sitios.

La configuración “estricto” cuenta con las mismas protecciones que la configuración estándar, pero en este caso, los rastreadores de contenido son bloqueados no solo utilizando ventanas privadas sino también ventanas por defecto.

Por último, la configuración “Personalizado”, permite definir de forma personalizada aquellos scripts y rastreadores que deseamos que sean o no bloqueados.

Seleccionaremos la opción “personalizado” y “bloquear todas las cookies entre sitios”.

Otra función interesante de Firefox es que permite indicar a los sitios web que no deseamos que rastreen nuestra navegación. Sin embargo, en este caso, los sitios deciden en última instancia y de forma voluntaria si respetan nuestra voluntad. Seleccionaremos la opción “siempre” para que siempre realice esta solicitud.

Cookies y datos del sitio

Las páginas web no solo pueden almacenar cookies en nuestro navegador, sino que también pueden almacenar datos y ficheros en nuestro disco duro. Mozilla ofrece la opción de eliminar las cookies y los datos de sitios web visitados cada vez que cerremos el navegador. Seleccionaremos esta opción.

Usuarios y contraseñas

En esta sección únicamente dejaremos marcadas las casillas “Sugerir generar contraseñas seguras”. Esta opción permite que Firefox genere una contraseña segura. En caso de que decidamos guardar las contraseñas en el navegador, seleccionaremos “Usar una contraseña maestra”. Esta contraseña será requerida cada vez que el navegador necesite utilizar alguna de las contraseñas que tenemos almacenadas.

Historial

Elegiremos no recordar el historial de navegación. Para ello seleccionamos en la pestaña desplegable “No recordar el historial”. Hay que tener en cuenta que el historial almacenado antes de activar esta opción continuará en nuestro disco duro, por lo tanto, debemos de realizar la limpieza del historial para eliminarlo. Para ello pulsaremos en el botón “Limpiar historial”, marcaremos todas las casillas, tanto del apartado “Historial” como “Datos” y pulsaremos el botón “Aceptar”.

Permisos

Entraremos en la configuración de ubicación, cámara, micrófono y notificaciones. Eliminaremos todos los sitios web que nos aparezcan en el listado de accesos y marcaremos que se bloqueen las nuevas solicitudes de acceso.

Dejaremos activado el bloqueo de ventanas emergentes y solicitaremos que se nos avise cuando los sitios web intenten instalar complementos.

En la sección “Recopilación y uso de datos de Firefox” desactivaremos todas las casillas. Aunque Firefox cuenta con una política de privacidad bien definida y un compromiso de transparencia con el usuario no permitiremos que el navegador recabe datos para obtener un mayor grado de privacidad.

Protección contra contenido engañoso y software peligroso

Las herramientas de protección de Firefox comprueban las listas de páginas web denunciadas por Pishing. Cuando el usuario intenta acceder a una de estas páginas, se muestra un aviso. Si el usuario descarga un archivo de aplicación Firefox comprueba si el sitio aparece en el listado de sitios conocidos por contener malware y en caso afirmativo, lo bloqueará de forma automática. En caso de que la página no aparezca en los listados, Firefox realiza una consulta sobre este software a Google Safe Browsing para verificar su seguridad [31]. Igualmente, cuando el navegador detecte una descarga potencialmente peligrosa, por contener un fichero infectado, podremos seleccionar que lo bloquee de forma automática.

Para obtener estas protecciones marcaremos todas las casillas de este apartado.

Certificados

Los certificados son emitidos por entidades certificadoras, para que sean válidos, deben pertenecer a una entidad certificadora de confianza y no deben estar revocados ni expirados. Para comprobar su estado, Firefox puede consultar los servidores que utilizan el protocolo OCSP (Online Certificate Status Protocol) que permite verificar un certificado en su entidad certificadora.

Esta casilla deberá de estar activa ya que permite verificar la autenticidad del sitio web y mejorar la seguridad de navegación.

Modo solo-HTTPS

El protocolo HTTPS es un protocolo de aplicación basado en el protocolo HTTP que permite establecer comunicaciones cifradas extremo a extremo. Esto quiere decir que el tráfico web permanece encriptado desde el navegador web del cliente hasta el servidor de la página que esté visitando. Este protocolo es especialmente utilizado en aquellas páginas que requieren introducir información sensible como datos de cuentas bancarias, tarjetas de crédito o credenciales y se representa en la barra de direcciones del navegador con el símbolo de un candado y al inicio de la dirección de un sitio web como https://.

El protocolo HTTPS utiliza el sistema de cifrado SSL/TLS (Secure Socket Layer/ Transport Layer Security) que requiere de un certificado SSL válido expedido por una autoridad de certificación (CAs) y una clave privada para iniciar la negociación de la seguridad del canal de comunicación entre el cliente y el servidor.

Los pasos del protocolo SSL con intercambio de claves RSA son los siguientes [32]:

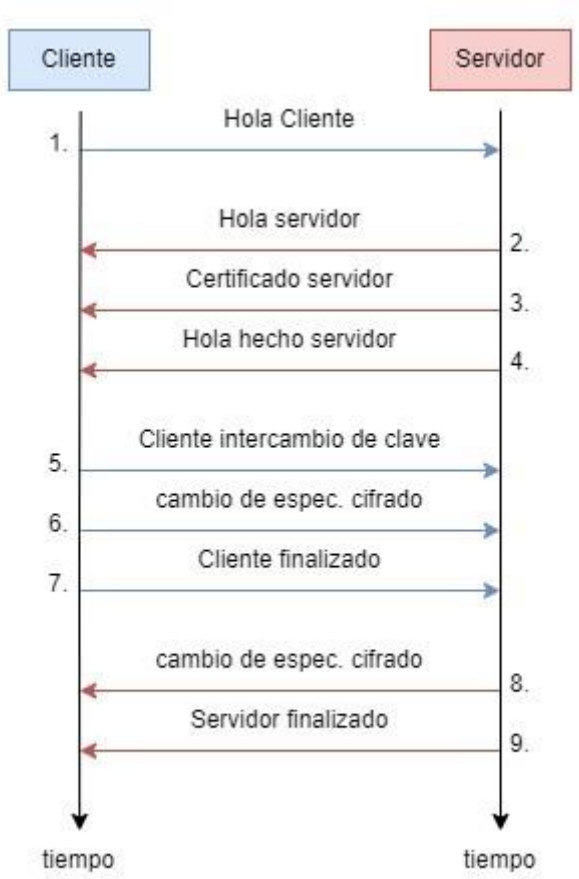

Figura 3: protocolo SSL con intercambio de claves RSA

1. El cliente saluda al servidor, indica la versión SSL con la que quiere comunicarse y envía un listado con las versiones de cifrado soportadas.

2. El servidor saluda al cliente e indica la versión de cifrado SSL elegida.

3. El servidor envía al cliente su certificado SSL (del que se obtiene la su clave pública).

4. El servidor indica que ha terminado los mensajes asociados al mensaje hola.

5. El cliente verifica el certificado SSL del servidor y envía el secreto_pre_master (valor obtenido del intercambio de claves) cifrado con la clave pública del servidor. Este lo descifra con su clave privada y tanto servidor como cliente convierten el secreto_pre_master en secreto_master. Cliente y servidor generan las claves de sesión.

6. El cliente envía un mensaje con el cambio de las especificaciones de cifrado.

7. El cliente indica que ha finalizado para verificar que el intercambio de clave y la autenticación han sido un éxito.

8. El servidor envía un mensaje con el cambio de las especificaciones de cifrado.

9. El servidor indica que ha finalizado la negociación, confirmando que el intercambio de la clave y la autenticación han sido un éxito. Tanto servidor como cliente pueden realizar la comunicación segura mediante datos cifrados.

El modo solo HTTPS fuerza a todas las páginas a las que accedemos con Firefox y que soportan HTTPS utilicen este protocolo para la navegación. En caso de que la página no soporte el modo HTTPS, obtendremos un aviso de sitio no seguro y se mostrará un desplegable que permite reconfigurar el modo solo-HTTPS, de forma que podamos desactivarlo para que en caso deseado podamos acceder al sitio.

Para obtener esta protección pulsaremos sobre el botón de opción “Activar el modo solo-HTTPS en todas las ventanas”.

2.2.2. Brave

Brave es un navegador web basado en el código abierto de Chromium. Fue desarrollado por Brave Software en 2016 y destaca por implementar diversas herramientas para proteger la privacidad y la seguridad del usuario tanto en PC (Windows, macOS y Linux) como en dispositivos móviles (Android e iOS). Utiliza un sistema de protección de la privacidad basado en tres capas [33]:

- **Escudos Brave:** Es la primera capa, que integra protecciones de bloqueo de rastreadores, cookies de terceros, huella digital, etc.

- **Protecciones avanzadas:** Protecciones frente al rastreo de redirecciones, bloqueo de RRSS, ventanas privadas para navegación a través de Tor, limitación de la vida de las cookies de JavaScript a 7 días, etc.

- **Políticas y prácticas:** Brave no recopila datos del usuario, como por ejemplo el historial de navegación y se compromete a cumplir el Reglamento general de protección de datos de la Unión Europea (RGPD) y la Ley de privacidad del consumidor de California (CCPA).

2.2.2.1 Guía de configuración de Brave

Escudos Brave

Para realizar la configuración de las opciones de privacidad debemos acceder al botón situado en la esquina derecha del navegador, pulsar en “configuración” y posteriormente seleccionar “Escudos Brave”.

En esta sección encontramos las siguientes opciones:

- Bloqueo de rastreadores y anuncios: Permite bloquear los anuncios que nos muestran algunos sitios web y también los rastreadores que recopilan datos sobre nuestro comportamiento en la navegación.

Seleccionaremos la opción “Agresivo” para ser lo menos permisivos posible con estos.

- Bloquear scripts: Un Script es un fragmento de código que se encuentra insertado en una página HTML. Los Scripts pueden ser escritos con diferentes lenguajes de programación como VBScript o JavaScript, aunque este último es el más utilizado actualmente. Al cargar una página, los scripts son ejecutados por el navegador del usuario y pueden mostrar anuncios, pop-ups o contener código malicioso como vectores de ataque Cross-Site Scripting (XSS).

Para evitar riesgos de seguridad, seleccionaremos que el bloqueo se encuentre activado.

- Bloquear huellas digitales: Algunos sitios web utilizan técnicas de seguimiento para almacenar información del navegador web y del dispositivo del usuario, como por ejemplo el sistema operativo que utiliza, la resolución de pantalla, aplicaciones instaladas, extensiones del navegador, fecha, hora y otras configuraciones. La combinación de esta información forma la huella digital, que es capaz de identificar a un usuario entre la multitud de usuarios de internet.

Dejaremos esta opción en el modo estricto.

- Bloquear cookies: Seleccionaremos la opción “Solo de terceros” para que no se permita este tipo de cookies.

- Filtrado de contenido: Permite realizar un filtrado de rastreadores, anuncios molestos y otros contenidos indeseados incluidos en diferentes listas. Deberemos activar aquellas listas que pertenezcan al país en el que nos encontramos.

Bloqueo de redes sociales

Pulsaremos ahora en el menú principal de configuración del navegador “Bloqueo de RRSS”. Brave permite bloquear botones de identificación de acceso a redes sociales a través de Google y Facebook de forma que evitamos que se almacenen en nuestro dispositivo cookies de terceros como Google Sign-In.

Los mensajes incrustados son una función que permite insertar contenido de las redes sociales en otros sitios web. Brave permite bloquear los mensajes incrustados de Facebook, Twitter y LinkedIn.

Desactivaremos todas las opciones que nos aparecen en esta sección para evitar que estos sitios puedan insertar cookies en el navegador web y que recopilen datos del usuario.

Privacidad y seguridad

Iremos ahora al apartado “Privacidad y seguridad” del menú principal de configuración

- Borrar datos de navegación: Permite eliminar cookies, archivos, imágenes, contraseñas y otros datos de navegación que pueden quedar almacenados en el

buscador. Hay que tener en cuenta que estos datos contienen información que puede revelar detalles sobre la actividad del usuario e información confidencial como nombres de usuario y contraseñas, por lo que eliminarlos ayuda a proteger la privacidad del usuario y reducir el riesgo de seguimiento en línea.

En esta ventana, seleccionaremos la opción “Al salir” y marcaremos todas las casillas, de esta forma, cada vez que cerremos Brave se eliminarán todos los datos de navegación que haya guardado.

- Cookies y otros datos de sitios: Si queremos el máximo grado de protección seleccionaremos bloquear todas. Sin embargo, esta opción puede hacer que las funciones de algunos sitios web fallen. En este caso seleccionaremos “bloquear cookies de terceros”, de esta forma evitaremos ser rastreados, pero permitiremos aquellas cookies que mejoren nuestra experiencia de usuario.

- Borrar cookies y datos de sitios al cerrar todas las ventanas: Activaremos esta opción para que las cookies se eliminen de forma automática cuando cerramos todas las ventanas del navegador.

- No hacer seguimiento: Activaremos esta opción, ya que, aunque algunos sitios web pueden no cumplir nuestra solicitud, puede evitar que ciertos sitios almacenen nuestros datos o rastreen nuestra navegación.

Seguridad

- Navegación segura: Permite lanzar una advertencia cuando se accede a cualquiera de los sitios web guardados como peligrosos en un listado de Brave. Además, esta advertencia aparecerá también si se realizan descargas de ficheros conocidos como maliciosos o se intentan instalar extensiones del navegador no auditadas por Brave.

Dejaremos activada la opción estándar, que nos avisará de estos peligros en caso de que sucedan.

- Configuración avanzada: Activaremos “Usar siempre conexiones seguras”. Esta opción solicita acceder a las páginas a través del protocolo HTTPS. Se trata de un protocolo de aplicación que encripta los datos que se transfieren entre el navegador web y el sitio web al que accedemos. Sin embargo, debemos de tener en cuenta que un sitio que utiliza el protocolo HTTPS no tiene por qué ser cien por cien seguro, en un estudio realizado por PhisLabs en el año 2017 [34] se indica que un cuarto de los ataques de phishing se realiza a través de páginas que utilizan HTTPS. Pese a que para utilizar este protocolo las páginas deben obtener un certificado SSL, este solo garantiza su identidad y que la transferencia de datos entre esta y el navegador web irán cifrados, pero no asegura que el sitio no sea vulnerable [34].

- Usar DNS seguro: El sistema de nombres de dominio (DNS) traduce las direcciones web textuales fáciles de recordar para las personas, a direcciones IP. Cuando consultamos un dominio, se comprueba si tenemos almacenada la dirección IP de este

en el caché DNS, en caso de no encontrarlo, el navegador envía la dirección que introducimos a un servidor DNS primario, que generalmente pertenece al proveedor de servicios de internet y este a su vez realizará consultas a otros servidores DNS para obtener la dirección IP. Cuando finalmente este servidor DNS reciba la ip del sitio consultado la indicará al navegador, de forma que este sepa en qué dirección debe buscar la información.

El problema de este sistema es que nuestro proveedor de servicios o un tercero que se encuentre en medio de la comunicación puede saber qué sitios web estamos consultando y aprovecharlo para mostrarnos publicidad o sustituir la dirección de respuesta DNS, redirigiéndonos a una página web diferente de la consultada [35].

Algunos proveedores ofrecen conexiones DNS seguras, que utilizan diferentes protocolos de cifrado para que los datos no sean interpretables por agentes maliciosos, como por ejemplo DNS mediante DNS mediante HTTPS (DoH), DNS mediante TLS (DoT) y DNSCrypt. En caso de que nuestro proveedor de servicios no ofrezca esta opción Brave nos permite seleccionar un servidor DNS público de compañías como Cloudflare, Google, CleanBrowsing u OpenDNS.
Por lo tanto, para asegurarnos de que utilizamos siempre un proveedor de DNS seguro seleccionaremos la opción “Con” y elegiremos una de estas cuatro compañías.

Configuración del sitio y de los escudos

Accedemos ahora al apartado de “Configuración del sitio y de los escudos” dentro del menú “Privacidad y seguridad”.

- Permisos: Accederemos a las configuraciones de ubicación, cámara, micrófono y notificaciones y seleccionaremos que no se permita a los sitios el acceso a estos.

- **Contenido:** Configuraremos que elementos de las páginas web estarán permitidos en nuestra navegación. En los apartados JavaScript e Imágenes seleccionaremos que los sitios no puedan utilizar JavaScript y si puedan mostrar imágenes, puesto que estas son elementos que pueden resultar necesarios para el correcto funcionamiento y visualización de las páginas web y solo sería recomendable desactivarlas en entornos que precisen de alta seguridad.

- Ventanas emergentes y redirecciones: Las ventanas emergentes son ventanas que se abren por encima del sitio web que estamos visitando y generalmente son utilizadas para presentar anuncios. La redirección de un dominio es la capacidad de redirigir a una dirección web diferente de la que ha visitado inicialmente, estas se realizan generalmente utilizando htaccess, PHP, etiquetas meta HTML o JavaScript y podrían llevarnos a páginas con código malicioso o que no queramos visitar. Para evitar estos problemas, seleccionaremos la opción “No permitir que los sitios envíen ventanas emergentes ni utilicen redirecciones”.

- Ventanas Tor: Una de las funciones más llamativas de Brave es que nos permite navegar con un alto nivel de anonimato mediante una integración de Tor. Para activar

la opción de conectarnos a través de la red Tor deberemos de activar la opción “ventana privada con Tor”. Tras realizar este paso podremos iniciar la navegación con el mismo presionando Alt + Mayús + N o pulsando sobre el botón (≡) que se encuentra en la esquina superior derecha del navegador y seleccionando “Nueva ventana privada con Tor”.

Redirigir automáticamente a los sitios .onion: En caso de que una página web cuente con versión .onion, Brave abrirá este dominio en una ventana privada con Tor. Podemos activar esta opción, pues, aunque si deseamos tener el mayor nivel de anonimato deberíamos navegar siempre con Tor, puede mejorar la seguridad cuando utilicemos la ventana normal.

- Utilizar puentes: Los puentes Tor, son servidores de la red Tor que no se encuentran listados públicamente y que ayudan a los usuarios a evadir la censura en algunos países y a conectarse a esta red cuando las direcciones IP de los nodos públicos se encuentran bloqueadas en su región.
En este caso, no será necesario que utilicemos estos puentes salvo que nos encontremos en zonas en las que el acceso a la red Tor se encuentre censurada, por ejemplo, a nivel del proveedor de servicios de internet. En cuyo caso una forma rápida de configurarlos es seleccionando “Solicitar un puente a torproject.org” pulsar en “solicitar un nuevo puente” y por último hacer clic en “Aplicar cambios”.

Buscador

Ahora pulsaremos en la opción buscador del menú principal de configuración. En esta sección podemos elegir el buscador por defecto que se utilizará en la barra de navegación, tanto en las ventanas normales como en las privadas. Las opciones que ofrecen un mayor nivel de privacidad son el buscador Brave, DuckDuckGo, Qwart y StartPage [36].

2.2.3. Tor Browser

El navegador Tor es un software gratuito y de código abierto que fue desarrollado en el año 2008 a partir de Firefox [37], con el objetivo de que las personas tengan derecho a navegar por la red de forma privada y sin censura. Por defecto, no guarda ningún historial de navegación y las cookies solo serán válidas durante una única sesión o hasta que solicitemos una nueva identidad al navegador [38]. Se encuentra disponible para Windows, Linux y macOS, así como para Android y su principal característica es que permite acceder a internet y a servicios ocultos a través de la red Tor.

Al utilizar esta red, los usuarios no solo evitan poder ser rastreados por parte de cookies de terceros, sino que obtienen una conexión anónima que impide que los sitios web visitados puedan rastrear su ubicación e identidad. Asimismo, las actividades en línea del usuario se mantienen ocultas para los proveedores de

servicios de Internet, ya que toda la información que viaja a través de Tor se encuentra cifrada. La red Tor será explicada en detalle más adelante.

2.2.3.1. Guía de configuración de Tor Browser

Comenzaremos desactivando JavaScript. Para ello, escribiremos “about:config” en la barra de búsqueda y a continuación buscar el parámetro “javascript.enabled”. Una vez encontrado, cambiaremos su valor de “true” a “false”.

Para configurar las características de este navegador debemos pulsar sobre el botón (≡) que se encuentra en la esquina superior derecha del navegador y seleccionar la opción “Ajustes”. Comenzaremos por el apartado “General” y buscaremos “Actualizaciones de Navegador Tor”, debemos dejar marcada la casilla “instalar actualizaciones de forma automática”.

Privacidad y seguridad

- Servicios Onion: Permite que se dé prioridad a los sitios con extensión. onion, que son aquellos a los cuales solo se puede acceder desde la red Tor. Seleccionaremos “Preguntar siempre”.

- Cookies y datos del sitio: Por defecto, el Navegador Tor elimina todas las cookies y datos del sitio de forma automática cuando lo cerramos.

Usuarios y contraseñas

No es recomendable introducir credenciales de identificación en ningún servicio mientras se utiliza Tor. No obstante, podemos activar las casillas correspondientes a:

- Sugerir y generar contraseñas seguras: Nos ayuda a crear contraseñas seguras y fuertes.

- Mostrar alertas sobre contraseñas para sitios web comprometidos: El navegador Tor, a través de Firefox Lockwise nos mostrará una alerta en caso de que uno de nuestros inicios de sesión guardados pueda encontrarse comprometido. Para ello se comprueba si posteriormente a que guardásemos la contraseña el sitio web en el que utilizamos la sufrió algún ataque en el que se hayan filtrado datos.

- Usar una contraseña maestra: Permite utilizar una contraseña maestra para acceder a los nombres de usuario y contraseñas que hemos guardado en el navegador.

Historial

Dejaremos la opción por defecto, “usar una configuración predeterminada para el historial “, “modo permanente de navegación privada”.

Permisos

Entraremos en la configuración de ubicación, cámara, micrófono y notificaciones. Eliminaremos todos los sitios web que nos aparezcan en el listado de accesos y marcaremos que se bloqueen las nuevas solicitudes de acceso.

Activaremos las opciones “Bloquear ventanas emergentes” y “Advertirle cuando los sitios web intenten instalar complementos” ya que las ventanas emergentes no son solicitadas por el usuario y pueden ser potencialmente peligrosas. También evitaremos que se instalen complementos o extensiones maliciosos que puedan comprometer nuestra privacidad.

Seguridad

Elegiremos el modo “Más seguro”, ya que este ofrece un balance proporcionado entre seguridad y funcionalidad frente a las opciones “Estándar” y “El más seguro de todos”. En este modo, JavaScript estará desactivado siempre y cuando el sitio web al que accedemos no utilice HTTPS.

Protección contra contenido engañoso y software peligroso

Activaremos todas las casillas: “Bloquear contenido peligroso y engañoso”, “Bloquear descargas peligrosas” y “Advertirle sobre software no deseado y poco usual”. Ya que Mediante esta configuración pretendemos protegernos del “phising” y “malware”.

Certificados

Activaremos “Consultar a los servidores respondedores OCSP para confirmar la validez actual de los certificados”, puesto que nos permite confirmar que los certificados se encuentran en vigor y que no ha sido revocados.

Modo solo-HTTPS

Seleccionaremos “Activar el modo solo-HTTPS en todas las ventanas “. En caso de que los sitios web que visitemos admitan HTTPS, se realizará la conexión entre el navegador y servidor web con este protocolo.

Finalmente, Para comenzar la navegación deberemos acceder al menú conexión, dentro de la sección “Ajustes” indicada anteriormente y pulsar sobre conectar.

2.3. Comparativa de los navegadores presentados

Como hemos visto, cada navegador dispone de sus propias características para la protección de la privacidad, seguridad y anonimato del usuario. En la siguiente tabla, se realiza una comparativa de cada una de ellas.

Se debe tener en cuenta que la comparativa se realiza sin instalar extensiones, únicamente con la instalación del navegador y configuración por defecto. El equipo empleado en las comparativas es el mismo para todos los navegadores, con el mismo sistema operativo (Windows 10 Pro) y se utiliza la misma configuración de este.

Tabla 1: Comparativa de características de los navegadores

	Mozilla Firefox	Brave	Tor Browser
Navegación privada	✓	✓	✓
Rastreadores sociales	✓	✓	✓
Rastreadores de contenido	✓	✓	✓
Cookies de terceros	✓	✓	✓
Bloqueador de anuncios	✗	✓	✗
Bloquear descargas peligrosas	✓	✓	✓
Criptomineros	✓	✓	✓
Fingerprinters	✓	✓	✓
Protección pishing	✓	✓	✓
Alerta de filtración de datos	✓	✗	✓
Contraseña maestra	✓	✗	✓
Generar contraseñas seguras	✓	✗	✓
Sugerir a los sitios no rastrear	✓	✓	✗
Modo solo-HTTPS	✓	✓	✓
Navegación red Tor	✗	✓	✓

Coveryourtracks.eff.org es un proyecto de Electronic Frontier Foundation que comprueba la efectividad de los navegadores contra el rastreo y fingerprinting [39].

Resultados de la configuración por defecto:

Tabla 2: Comparativa Coveryourtracks configuración por defecto

	Mozilla Firefox	**Brave**	**Tor Browser**
Bloqueo de anuncios de rastreo	Protección parcial	Protección parcial	Si
Bloqueo de rastreadores invisibles	Protección parcial	Protección parcial	Si
Protección de huella digital	Su navegador tiene una huella digital única	Su navegador tiene una huella digital aleatoria	Su navegador tiene una huella digital no única
Nivel de protección contra el rastreo web	Alguna protección frente a rastreo web	Alguna protección frente a rastreo web	Fuerte protección frente a rastreo web
Bits de identificación	16.85	17.85	10.61

Resultados tras la configuración:

Tabla 3: Comparativa Coveryourtracks configuración propuesta

	Mozilla Firefox	**Brave**	**Tor Browser**
Bloqueo de anuncios de rastreo	Sí	Sí	Si
Bloqueo de rastreadores invisibles	Sí	Sí	Si
Protección de huella digital	No	SÍ	Su navegador tiene una huella digital no única
Nivel de protección contra el rastreo web	Fuerte protección frente a rastreo web	Fuerte protección frente a rastreo web	Fuerte protección frente a rastreo web
Bits de identificación	14.53	11.2	12.18

Como podemos ver en la configuración por defecto, el navegador Tor Browser ha obtenido la mejor puntuación en el nivel de protección contra los rastreadores y el menor valor en bits de identificación. Esto es debido a que Tor aísla de forma independiente cada sitio web y muestra la misma información de huella digital para todos los usuarios [40]. También cabe destacar que el navegador Brave ha ofrecido protección frente a la huella digital al generar una huella aleatoria.

Tras realizar la configuración propuesta en la guía podemos ver una mejora en la seguridad de todos los parámetros evaluados en los navegadores salvo los bits de identificación de Tor Browser que han pasado de 10.61 a 12.18. Esto puede ser debido a que cuando realizamos modificaciones en la configuración de Tor Browser nos estamos diferenciando de la mayoría de los usuarios de este navegador, y seremos más vulnerables a técnicas de fingerprinting. Por lo tanto, no es conveniente realizar grandes cambios en la configuración de este.

Adblock-tester.com realiza diversas pruebas para comprobar la eficacia del navegador para bloquear nuncios [41]. Para realizar esta prueba es necesario mantener activado JavaScript en todos los navegadores.

Resultados de la configuración por defecto:

Tabla 4: Comparativa adblock-tester configuración por defecto

	Puntuación
Mozilla Firefox	58/100
Brave	78/100
Tor Browser	58/100

Resultados tras la configuración:

Tabla 5: Comparativa adblock-tester configuración propuesta

	Puntuación
Mozilla Firefox	76/100
Brave	96/100
Tor Browser	65/100

El navegador Brave ha obtenido las mejores puntuaciones tanto con la configuración por defecto como con la configuración propuesta. Se puede ver el incremento en las puntuaciones de todos los navegadores tras el cambio de configuración.

Conclusiones

Todos los navegadores ofrecen un nivel de protección de la privacidad aceptable, ofreciendo los navegadores TOR y Brave los mejores resultados en nivel de protección de rastreo web y Firefox y Brave en bloqueo de anuncios según los parámetros evaluados.

En cuanto al grado de anonimato ofrecido por estos navegadores, Brave y TOR browser ofrecen navegación anónima a través de la red Tor, mientras que Firefox carece de esta función.

3. Tecnologías, herramientas y técnicas de anonimato

Cada día, millones de personas exponen sus datos en internet sin ser conscientes del riesgo que supone para su privacidad y anonimato. Estos datos pueden ser observados por los proveedores de servicios de internet o por terceros malintencionados. Las tecnologías, herramientas y técnicas de anonimato permiten al usuario ocultar su identidad, proteger su privacidad y acceder a contenidos que pueden encontrarse censurados.

En este apartado, se realiza una selección de tecnologías, técnicas y herramientas para obtener el anonimato en línea. Se analizan algunas de las vulnerabilidades de tres de las principales herramientas: las VPN, los proxies y la red Tor. Además, se expondrán técnicas que ayuden a mitigar estas vulnerabilidades.

3.1. VPNs

Una VPN (Red Virtual Privada) es una tecnología que permite a los usuarios conectarse a una red privada a través de una red pública, como por ejemplo Internet, utilizando un protocolo denominado protocolo de tunelización (Tunneling protocol).

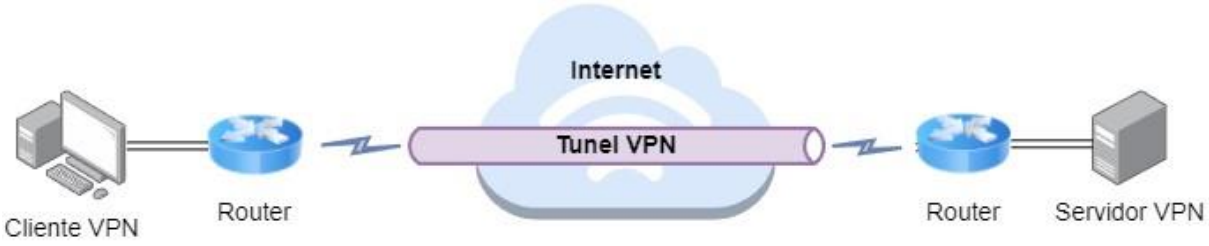

Figura 4: Protocolo de tunelización

Para establecer una red virtual privada, es necesario que el servidor VPN autentique al cliente VPN y ambos realicen un intercambio de claves de cifrado y descifrado. A continuación, se establece un túnel de cifrado seguro por donde circularán los datos de red, divididos en paquetes. Antes de que el cliente envíe un paquete, este se encapsula en un paquete externo, se cifra y se le añade una nueva cabecera que contiene la dirección IP del servidor VPN, para que a través del túnel puedan llegar al destino correspondiente.

Cuando el servidor VPN recibe el paquete, lo descifra, lo desencapsula y lo envía a la dirección del servidor de destino. En este proceso, se oculta la dirección IP del usuario, por lo que el servidor de destino verá como dirección de origen de los datos la dirección IP del servidor VPN.

Cuando el servidor de destino envía un paquete al servidor VPN, este lo encapsula, lo cifra y envía al usuario a través del túnel seguro que han establecido. Finalmente, el cliente VPN, descifra y desencapsula el paquete recibido, obteniendo el contenido original.

Actualmente, pueden utilizarse diferentes protocolos de comunicación en las VPN, como, por ejemplo, PPTP, IPSec, L2TP/IPsec u OpenVPN, que suelen ser elegidos en función del tipo de red VPN implementada [42].

Los tipos de red VPN más utilizados son:

- VPN personal: Es Utilizada por la mayor parte de los usuarios de internet, en la cual el usuario se conecta directamente a los servidores del proveedor VPN para realizar la navegación.

- VPN punto a punto: Suelen ser utilizadas por grandes empresas y permiten realizar conexiones seguras de forma directa entre dos redes privadas.

- VPN de acceso remoto: Generalmente son utilizadas por empresas y permiten que un usuario se pueda conectar a una red privada desde cualquier ubicación remota con acceso a internet.

Como hemos visto, una de las principales ventajas de una VPN es que permite a los usuarios acceder a recursos de una red privada de manera segura y remota, de la misma forma que lo haría si estuviera físicamente en ella. Además, la VPN puede utilizarse para garantizar el anonimato del usuario y para acceder a contenido restringido en su zona geográfica, ya que oculta su dirección IP y solo muestra la del servidor VPN que puede estar ubicado en cualquier otra parte del mundo.

Como contrapartida, el proveedor VPN puede conocer la información de los datos que le estamos enviando y almacenar logs con la actividad del usuario, por lo que nunca debemos de pensar que el anonimato proporcionado es absoluto.

3.2. Proxies

Los servidores proxy son servidores que actúan como intermediarios en la conexión entre un usuario y otro servidor en internet.

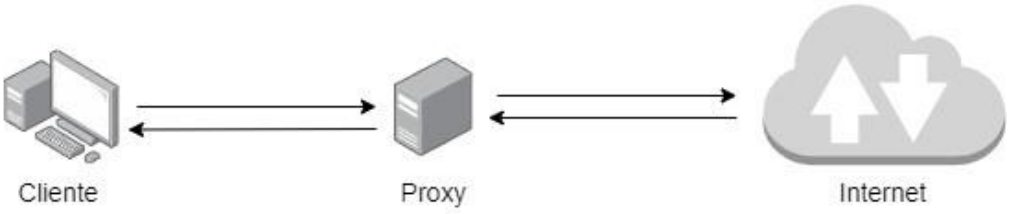

Figura 5: Conexión a internet a través de un servidor proxy

Estos, pueden ser locales, es decir, instalados mediante software y ejecutados en la propia máquina del usuario, o externos, situados como servidores en cualquier parte del mundo.

Además de locales y externos, los proxies se pueden clasificar en diferentes tipos; algunos de ellos son los siguientes:

Proxies en función de la dirección del tráfico

- Servidor proxy o proxy de reenvío:

Es el tipo de proxy estándar, su funcionamiento es el siguiente:

Cuando un usuario utiliza un proxy y envía una consulta dirigida a un servidor, esta no se transmite directamente al servidor de destino, sino que se envía primero al servidor proxy. El servidor proxy recibe la consulta, la verifica, y después la reenvía al servidor de destino utilizando su propia dirección IP. De esta manera, la dirección IP del usuario permanece oculta.

Del mismo modo, cuando el servidor de destino envía una respuesta, lo hace a la dirección IP del servidor proxy, que reenvía la respuesta a la dirección del usuario. Así, el usuario puede acceder al contenido del servidor de destino sin exponer su propia dirección IP.

- Proxy inverso:

Su función, es inversa a la del proxy de reenvío. El proxy inverso se sitúa delante de uno o varios servidores web en una red privada e intercepta todas las consultas que los clientes le realizan antes de reenviarlas al servidor correspondiente [43]. De esta forma, asegura que todas las comunicaciones que establezca el servidor web pasen primero a través de él. Los proxies inversos ocultan la dirección IP del servidor, y controlan y restringen el acceso de los usuarios al mismo. Esto permite evitar ataques dirigidos al servidor web y administrar la carga de tráfico, ya que el proxy inverso puede redistribuirla en caso de existir más servidores para evitar sobrecargas.

Los proxies inversos también permiten almacenar datos del servidor web en caché, esto permite reducir el número de consultas al servidor web y reducir el tiempo de espera para el cliente. Por ejemplo, cuando un usuario consulta una página web, el servidor responde enviando esta página al proxy inverso, esa página puede ser almacenada en el servidor proxy, de forma que, si otro cliente la solicita, no será necesario volver a transmitir la consulta hasta el servidor web, sino que será el propio proxy el que enviará la página almacenada.

Otra de las funciones que se pueden configurar en un proxy inverso, es el encriptado y desencriptado de las comunicaciones SSL o TLS. El proxy inverso, puede encriptar las respuestas que envía al usuario y desencriptar las solicitudes que transfiere al servidor web para reducir su carga de trabajo.

Proxies en función de nivel de anonimato

- Proxy transparentes:

Este tipo de proxy no oculta la información de identificación del usuario. Cuando este realiza una consulta a un servidor web a través de un proxy transparente, el servidor puede ver que la consulta proviene de la dirección IP del usuario en la cabecera HTTP XForwarded-For. Además, también puede ver qué estamos utilizando un proxy en la cabecera HTTP Via [44]. Generalmente se utilizan por organizaciones e instituciones como filtro para restringir el contenido de los sitios web.

- Proxy anónimo:

Los proxies anónimos no proporcionan la dirección IP del usuario a los servidores de destino, ya que no la envían en la cabecera X-Forwarded-For. Sin embargo, no ocultan que se está utilizando un proxy para realizar la conexión, por lo que en ocasiones esta puede ser bloqueada por el servidor.

- Proxies de gran anonimato o proxies de élite:

Al igual que los proxies anónimos, no proporcionan la dirección IP del usuario en la cabecera X-Forwarded-For. sin embargo, estos, también ocultan su propio uso ya que no envían la cabecera Via y modifican cada cierto tiempo su dirección IP, por lo que los servidores de destino no pueden reconocer que la conexión ha sido establecida a través un proxy [45].

Proxies por tipo de uso

- Proxy Web:

Son proxies a los que se accede a través de una página web que realiza la función de interfaz. A través de ellos únicamente se puede transferir contenido web, es decir solo utilizan los protocolos HTTP y HTTPS y nos permiten navegar por internet ocultando nuestra dirección IP.

- Proxy NAT:

Un proxy NAT (Network Address Translation) Sirve para enmascarar las direcciones IP privadas de una red LAN traduciéndolas a una única dirección IP pública que será la que se exponga a una red no segura como internet. Este proxy también puede restringir las conexiones provenientes del exterior a la red privada y redirigirlas a un servidor encargado de tramitar las peticiones. [46]

Esta tecnología, generalmente, es utilizada para sortear restricciones en el acceso a contenido web que imponen ciertos países o para evitar restricciones establecidas a nuestra propia dirección IP. Sin embargo, Al igual que otras tecnologías de anonimización, los proxies también son utilizados por algunas personas para realizar ataques ocultando su identidad.

3.3. La red Tor

A mediados de los años 90 David Goldschlag, Mike Reed y Paul Syverson, del US Naval Research Lab (NRL) en busca de un protocolo que permitiese crear conexiones privadas y anónimas para navegar por internet comienzan las primeras investigaciones sobre el enrutamiento de cebolla [11].

La red Tor se implementa en el año 2002. Sin embargo, su acceso era complejo, por lo que sus usuarios eran mayoritariamente personas con conocimientos técnicos sobre informática. En el año 2006 se funda la organización sin ánimo de lucro Tor Project, Inc, encargada de mantener el desarrollo de Tor y en 2008, se desarrolla el navegador Tor, que simplifica el acceso a esta red y consigue que el número de usuarios se multiplique [11]. De igual forma, también comienzan a multiplicarse el número de páginas ocultas en lo que se denomina la “Dark Web”, páginas que muchas veces aprovechan el anonimato que proporciona la red Tor para albergar contenido ilegal, siendo la más conocida “Silk Road”, un sitio web dedicado a la compraventa de droga que permaneció activo desde el año 2011 al 2013.

Sin embargo, la red Tor no solo se utiliza por aquellos que desean acceder a la Dark Web, sino también por periodistas, activistas y personas en general que se preocupan por mantener su anonimato. En la actualidad, se estima que la red cuenta con más de 6000 nodos [47] y más de 2.000.000 de usuarios, sin contar aquellos que utilizan puentes para evitar la censura que existe en sus países [48].

3.3.1. Estructura y funcionamiento de la red Tor

La red Tor es una red distribuida compuesta por miles de nodos (también llamados repetidores) unidos por túneles virtuales y administrados por voluntarios. Cuando nos conectamos a esta red, se establece una conexión entre nuestro dispositivo y al menos tres de estos repetidores, que son elegidos de forma aleatoria, formando un circuito. Es importante destacar que cada circuito se forma con nodos únicos, es decir, sin repeticiones.

Los repetidores pueden ser de cuatro tipos:

- **Repetidores de guarda:** Son los nodos de entrada a la red Tor, son seleccionados de forma aleatoria y conocen la dirección IP pública del usuario. Debido a esto, son un punto crítico dentro de la red. Para evitar ataques de desanonimización, al contrario que el resto de los nodos no cambia al realizarse un cambio de circuito durante una sesión, sino que se mantiene durante un periodo de dos o tres meses.

- **Repetidores intermedios:** Estos nodos se encuentran entre el repetidor de guarda y el repetidor de salida y desconocen la dirección IP del usuario, ya que solo conocen las direcciones IP del nodo predecesor y descendiente. Además, no conocen el contenido de los paquetes, ya que se encuentran cifrados.

- **Repetidores de salida:** Se trata del nodo final del circuito que envía directamente los datos recibidos y descifrados al servidor de destino. La dirección IP de este nodo de salida será vista por los servidores externos a la red Tor como la dirección de origen de los datos. Este nodo es otro punto crítico dentro de la red Tor, ya que conoce la información de los datos enviados por el usuario.

- **Puente:** Los nodos de Tor tienen direcciones IP públicas, lo que permite que algunos gobiernos o proveedores de servicios de Internet bloqueen estas direcciones para evitar que las personas accedan a sitios censurados. Para ayudar a estas personas a conectarse a la red Tor, algunas direcciones de nodos no se publican, lo que dificulta que los gobiernos opresivos las incluyan en las listas de bloqueo [49]. Estos nodos no publicados se llaman "puentes" y también son útiles para aquellos usuarios que no desean que su proveedor de servicios de Internet sepa que están utilizando esta red. Sin embargo, algunos gobiernos han encontrado la forma de bloquear estos puentes, por ejemplo, a finales del año 2011, el gran firewall de china (CFG) comenzó a bloquear puentes que no se encontraban publicados [50]. Para que los usuarios se puedan conectar a Tor en estos países resulta necesario añadir una capa adicional de ofuscación mediante transportes conectables. Actualmente, pueden utilizarse tres transportes conectables diferentes: obfs4, snowflake, or meek-azure, que ofrecen al usuario protección frente a la inspección profunda de paquetes (DPI).

Una vez seleccionado el circuito, para poder enviar los paquetes desde el usuario al servidor de destino se debe aplicar el protocolo de enrutamiento de cebolla, que recibe su nombre porque durante el mismo se añaden o retiran varias capas de cifrado.

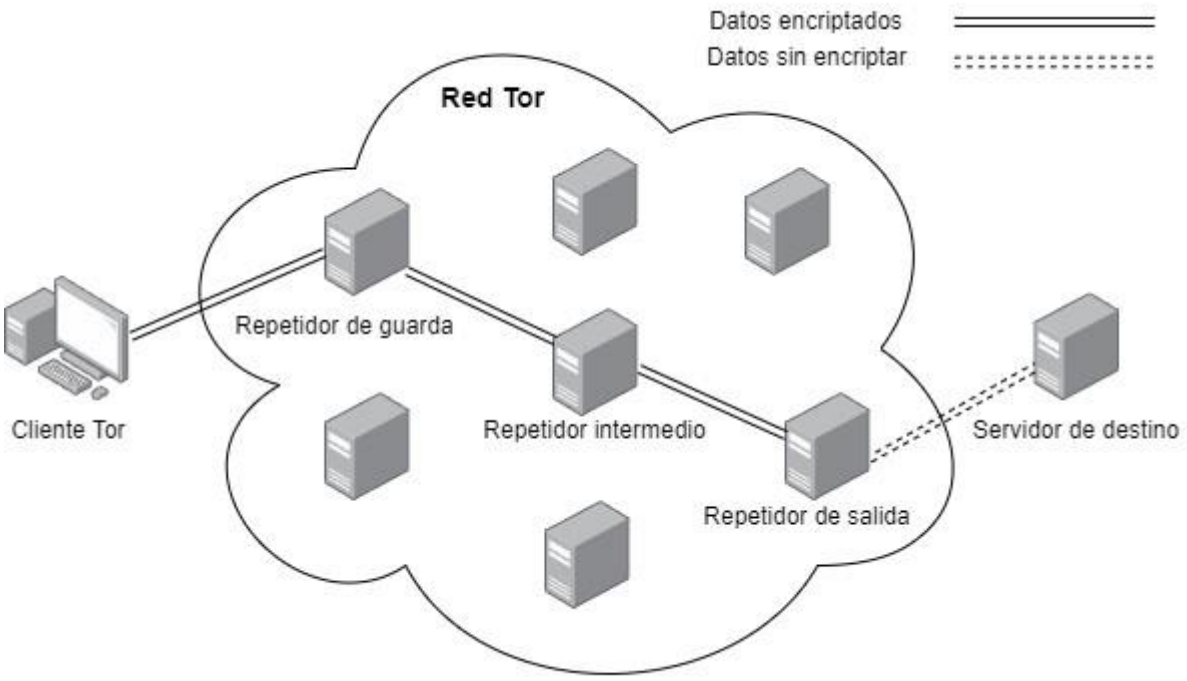

Figura 6: Red Tor

El proceso sigue la secuencia que se describe a continuación:

El cliente Tor, consulta el directorio de servicios de Tor para obtener una lista de repetidores, que serán seleccionados para formar parte del circuito mediante el algoritmo de selección de repetidores de Tor [51]. El cliente construye el circuito y negocia una clave simétrica con cada uno de los nodos [52], utilizando el protocolo Diffie-Hellman. El cliente, dividirá los paquetes de red que se van a enviar a través de la red Tor en pequeños paquetes de 512 bytes (llamados celdas) y realizará el primer cifrado del paquete de red con la clave del repetidor de salida. Posteriormente, este paquete es encapsulado añadiendo una nueva cabecera con la dirección IP de este repetidor. Este proceso se repite, ahora cifrando el paquete encapsulado que hemos obtenido anteriormente con la clave del repetidor intermedio y encapsulándolo con una nueva cabecera que contiene la dirección IP de este repetidor. El mismo proceso se llevará a cabo finalmente utilizando la clave y dirección IP del repetidor de guarda. Al terminar el proceso se habrán añadido al paquete tantas capas de cifrado y encapsulado como nodos tiene el circuito.

El paquete es enviado al nodo de guarda, que lo recibe, desencapsula y descifra la primera capa de cifrado con su clave privada. Este nodo envía el paquete al nodo con la dirección IP que aparece en la cabecera del paquete, que corresponderá al nodo intermedio. Cuando este nodo recibe el paquete, lo desencapsula y descifra la segunda capa con su clave privada y envía el paquete a la dirección IP de su cabecera, que corresponde a la dirección del nodo de salida. Cuando el nodo de salida recibe el paquete, al igual que en los casos anteriores, desencapsula y descifra el paquete, con la diferencia de que todas las capas de cifrado ya han sido descifradas, por lo que este nodo puede ver el contenido original del paquete con la dirección del servidor de destino. El repetidor de salida envía el paquete al servidor de destino, quien verá la dirección IP de este nodo como la IP de origen del paquete.

Cuando el servidor de destino envía el paquete de respuesta al usuario, se realiza el proceso inverso. El repetidor de salida recibe el paquete, lo cifra con su clave, lo encapsula añadiendo en su cabecera la dirección IP del repetidor intermedio y lo envía a esta dirección. El repetidor intermedio recibirá el paquete, lo cifrará con su clave, lo encapsulará añadiendo en la cabecera la dirección IP del repetidor de guarda y se lo enviará. Igualmente, el repetidor de guarda recibirá el paquete, lo cifrará con su clave pública, lo encapsulará añadiendo en su cabecera la dirección IP pública del usuario y lo enviará. Cuando el usuario reciba el paquete, desencapsulará y descifrará cada una de las capas con las claves públicas de los repetidores, obteniendo el paquete original de respuesta.

Durante todo el proceso se mantiene la privacidad y anonimato del usuario, ya que, aunque el nodo de salida y el servidor de destino conocen el contenido del paquete, desconocen la dirección IP pública del usuario y así mismo, aunque el nodo de guarda conoce la dirección del usuario, no conoce el contenido del paquete, por lo que ningún nodo obtiene la información completa sobre quién es el usuario y para qué está usando red Tor.

3.4. ProxyChains

Es un software Opensource para sistemas GNU/Linux que fuerza a las conexiones TCP de cualquier aplicación a salir a través de un proxy, como por ejemplo TOR, o cualquier proxy Socks4, Socks5 o HTTP(S) [53]. PorxyChains permite encadenar diferentes servidores proxy, de forma que las peticiones y respuestas entre el usuario y el servidor de destino deban de pasar por cada uno de ellos. Al distribuir la conexión en varios saltos resulta más complicado conocer la dirección IP de origen de la conexión, por lo que aumenta el nivel de anonimato.

Cuando utilizamos una VPN, nuestro tráfico viaja encriptado entre el cliente VPN y el servidor VPN, sin embargo, nuestro proveedor VPN conoce nuestra dirección IP pública. Si utilizamos proxychains para que nuestra conexión pase primero a través de un proxy, el servidor VPN verá como origen de la conexión la dirección de nuestro proxy, ocultando nuestra identidad.

Esta herramienta también nos permite aumentar nuestra seguridad al utilizar la red Tor. Como explicamos anteriormente, cuando nos conectamos a la red Tor, el repetidor de guarda conoce nuestra dirección IP pública, lo que provoca un punto crítico de conexión que podría ser aprovechado por terceros para realizar ataques de desanonimización. Si, primeramente, nuestra conexión pasa a través de un proxy, evitamos que nuestra IP sea revelada al nodo de entrada de la red Tor, de esta forma, aunque el atacante controle también el nodo de salida y mediante un sniffer analice los datos, no podrá saber la dirección IP real del usuario que los genera.

Este software también es utilizado por algunas personas para fines poco éticos, como, por ejemplo, realizar ataques informáticos u otros delitos. Los servidores proxy que se incluyen en la lista de encadenamiento, pueden encontrarse en diferentes países. Cuando se inicia una investigación judicial, es necesario obtener permisos de la jurisdicción en la que se encuentran cada uno de los proxies y seguir la cadena hasta llegar al origen. Esto dificulta enormemente la labor de los investigadores que pueden encontrarse con países que por motivos políticos no prestan la colaboración necesaria.

Como se ha expuesto, el encadenamiento de proxies ofrece una gran ventaja, ya que permite mejorar el anonimato utilizando diferentes tecnologías. Sin embargo, se debe de tener en cuenta que la velocidad de conexión disminuye con cada encadenamiento.

Configuración de ProxyChains

Ejecutamos el fichero de configuración de ProxyChains “proxychains4.conf”, que, por defecto, se encuentra en la carpeta /etc/ del directorio raíz en Ubuntu.

Para que una función de ProxyChains se encuentre activa deberá de estar descomentada, es decir, no deberá de comenzar con el carácter “#”, en cuyo caso deberemos de eliminarlo.

Al final del fichero, encontramos el apartado [Proxylist], donde deberemos de introducir la lista de datos de los proxies que vamos a utilizar con el siguiente formato: Tipo de proxy, dirección IP, puerto, usuario (opcional), contraseña (opcional).

Por ejemplo:

socks5 192.98.40.03 1080 usuario contraseña

HTTP 192.20.32.01 8080

Para redirigir el tráfico de red a través de una aplicación que se encuentra conectada a la red local como por ejemplo Tor, deberemos de introducir como dirección IP (127.0.0.1) y el puerto de salida del servicio, que en caso correspondería al 9050. Cabe destacar que antes de redirigir el tráfico a través de TOR, se deberá de haber instalado y activado el servicio.

Posteriormente, tan solo se tendrá que escribir en la terminal “proxychains4” antes de la aplicación cuyo tráfico se desea redireccionar a través de Proxychains. Por ejemplo, “proxychains Firefox”.

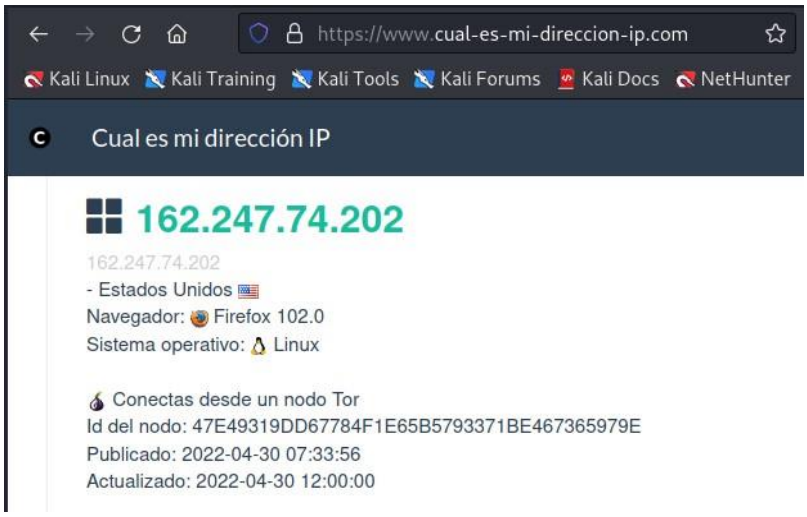

Figura 7: Sitio web cual-es-mi-dirección-ip.com

Los tipos de proxy soportados son HTTP, HTTPS, socks4 o socks5 y pueden utilizarse en la lista de proxies de forma combinada. Sin embargo, se debe de tener en cuenta que si se elige HTTP o HTTPS solo se podrán redirigir a través de ese proxy paquetes de red que utilicen estos protocolos.

ProxyChains tiene cuatro modos de tratar las cadenas:

- Cadena dinámica: Conecta los proxies en el mismo orden que el listado, en caso de que alguno no responda, se salta al siguiente.

- Cadena estricta: Funciona de igual forma que la cadena dinámica, pero en caso de que algún proxy no responda, se cancela la cadena.

- Cadena de turnos: Conecta el número de proxies indicado en el comando “chain_len” en el mismo orden que el listado. Al menos un proxy deberá de estar funcionando para formar la cadena, que tendrá como primer proxy el último de la anterior cadena invocada.

- Cadena aleatoria: Establece conexiones eligiendo proxies de la lista de forma aleatoria. El número de proxies será el indicado en el comando “chain_len”.

ProxyChains también cuenta con otras funcionalidades:

- modo tranquilo: Si se activa este modo, no se muestra la actividad de proxyChains en la consola.

- solicitud Proxy DNS: Ofrece tres modos de realizar las consultas DNS sin que se produzcan fugas.

- Tiempos de espera: indican el tiempo máximo de espera para recibir contestación del proxy y el tiempo de espera máximo para establecer conexión con el mismo antes de descartarlos.

- Exclusión de conexiones: Permite excluir las direcciones con los puertos indicados en diferentes opciones.

Para redirigir el tráfico de una aplicación a través de ProxyChains será tan sencillo como escribir en la consola de comandos “proxychains4” antes del nombre de la aplicación que se quiera ejecutar y los argumentos necesarios de esta.

Por ejemplo:

proxychains4 firefox

proxychains4 nmap –sn –v 192.168.20.5/24

4. Vulnerabilidades y limitaciones

Según el Instituto Nacional de Ciberseguridad (INCIBE) “una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma” [54]. Por otra parte, una limitación en informática es la incapacidad de un sistema para realizar una función.

A continuación, se explican algunas de las principales vulnerabilidades y limitaciones de los Proxy, las VPN y la red Tor.

4.1. Vulnerabilidades y limitaciones de las VPNs

Proveedor no confiable

Como hemos visto las VPN crean un túnel seguro para transmitir los datos entre el cliente VPN y el servidor VPN, cualquier persona que este escuchando la comunicación intermedia solo podrá observar que los datos viajan cifrados. Sin embargo, cuando el servidor VPN recibe, descifra y desencapsula los paquetes, tiene

acceso al contenido original y además conoce la dirección IP pública del usuario. Por este motivo es de gran importancia realizar una selección exhaustiva del servicio VPN que vamos a utilizar, intentando evitar VPNs gratuitas y eligiendo únicamente aquellas que sean confiables.

Proveedores que almacenan logs

Algunos proveedores de VPN almacenan información del historial de los usuarios. Es decir, mantienen un registro (log) de la actividad del usuario, generalmente, para comprobar que este cumple con las condiciones de uso del servicio. Uno de los motivos por los que muchos usuarios utilizan VPNs es para ocultar información de navegación a sus proveedores de servicios de internet, en caso de que el proveedor de VPN almacene registros, únicamente estamos cambiando la entidad que los almacena.

Los proveedores de VPN-no log, no almacenan datos personales ni registros de actividad del usuario, esto permite obtener un mayor nivel de anonimato y privacidad que con los proveedores anteriores.

Por lo tanto, al elegir un servicio VPN es importante leer cuidadosamente sus condiciones de uso y políticas de privacidad para comprobar que no almacenan logs. De esta forma, se garantiza que nuestro proveedor aporta un nivel óptimo de seguridad y anonimato.

Cortes de conexión

En caso de que la conexión VPN del usuario se interrumpa, es posible que no se dé cuenta, y los datos que envía a partir de ese momento pasen a ser enviados directamente y sin cifrado al servidor de destino. Por este motivo, el servicio de VPN debe ofrecer la función Kill switch, que garantiza el corte de la conexión a internet, preservando el anonimato de nuestra dirección IP y la seguridad de nuestros datos en estos casos.

Filtración de DNS

En las conexiones VPN, todo el tráfico generado por el usuario debe ser enviado a través del túnel cifrado hasta el servidor VPN. Cuando utilizamos una VPN y realizamos una solicitud mediante el envió de un paquete DNS para obtener la dirección IP de un servidor, este debe ser enviado a través del túnel de cifrado hasta los servidores DNS del proveedor de la VPN. sin embargo, por diferentes motivos, como, por ejemplo, realizar una mala configuración del servicio VPN o utilizar un proveedor que no dispone de servidores DNS, pueden producirse fugas. Cuando esto sucede, el usuario envía los paquetes directamente a un servidor DNS del proveedor de servicios de internet, por lo que el mismo podrá saber qué servicios o páginas estamos visitando y además nuestra conexión será vulnerable a ataques “hombre en el medio” (MITM).

Fingerprinting o Huella digital

Aunque una VPN oculta la dirección IP del usuario, las técnicas de fingerprinting o huella digital pueden recopilar información variada del dispositivo del usuario, como navegador web utilizado, configuración, extensiones instaladas, sistema operativo,

resolución de pantalla, zona horaria, e incluso los patrones de movimiento que realiza con el ratón en la pantalla, con el fin de identificarlo de forma precisa entre los millones de usuarios de internet y crear un perfil único de usuario [55].

La principal defensa que puede tomar el usuario frente al fingerprinting es que su configuración sea lo más parecida a la configuración por defecto, ya que es la que utilizarán la mayoría de los usuarios. Se debe de evitar instalar extensiones en el navegador, ya que, de esta forma, el equipo del usuario tendrá menos características particulares que le diferencien y la identificación no podrá ser tan precisa.

La navegación a través de una ventana privada o activar las opciones de privacidad que nos suelen ofrecer los navegadores web, como bloquear cookies de terceros o la petición de no seguimiento, no resultan efectivas contra las técnicas de fingerprinting. Sin embargo, la activación de bloqueadores de publicidad como Ghostery y uBlock Origin han demostrado ser eficaces contra el seguimiento de terceras partes [55].

VPN Hijacking

Se trata de un ataque que afecta a algunos sistemas operativos Linux y Unix. En este ataque, la víctima se conecta a un punto de acceso a la red VPN que ha sido previamente controlado por un atacante adyacente. Cuando la víctima establece conexión con su proveedor VPN a través de este punto de acceso, se hace posible descubrir la IP virtual que le ha sido asignada, mediante el envió de paquetes SYN-ACK a su dispositivo.

De forma similar, mediante el envío por parte del atacante de paquetes SYN o SYN-ACK a la IP virtual de la víctima, se puede llegar a determinar si existe una conexión activa con un sitio web concreto.

Una vez que el atacante sabe la dirección IP virtual del usuario y que ha establecido una conexión TCP, mediante el recuento y análisis de los paquetes puede llegar a identificar el número de secuencia (seq) y el número ACK que le permiten inyectar datos en la conexión [56].

4.2. Vulnerabilidades y limitaciones de los proxies

Los servidores proxy cuentan con algunas de las vulnerabilidades y limitaciones explicadas en las VPN, como la identificación por huella digital o la filtración de DNS. Además, otras vulnerabilidades y limitaciones son:

Dirección IP compartida

Algunos servidores proxy pueden compartir la misma dirección IP con varios usuarios [57]. Esto puede provocar que seamos reconocidos en internet como otro de los usuarios del servicio proxy.

Falta de encriptación

Los proxies, interceptan el flujo de datos que circula entre el usuario y el servidor de destino. Este tráfico de datos, generalmente, no va cifrado, y, por tanto, todos los datos que se envíen o reciban serán visibles para el mismo. Por este motivo, se debe tener

especial cuidado en no introducir información sensible como contraseñas o datos bancarios cuando se utiliza un proxy como intermediario [58].

Los proxies pueden no estar configurados para encriptar los datos. Esto los hace vulnerables a la interceptación de la comunicación y el análisis y modificación del tráfico de red por parte de terceros mediante un ataque Hombre en el medio (Man-in-the-middle).

Puertos abiertos

Los proxies suelen tener puertos abiertos que facilitan a los atacantes la explotación de vulnerabilidades. Si un atacante toma el control del servidor proxy, los usuarios que lo utilizan podrían verse expuestos a riesgos como la interceptación de datos, ataques de phishing y la infección con malware, virus y troyanos.

4.3. Vulnerabilidades y limitaciones de la red Tor

Aunque la red Tor nos ofrezca un elevado nivel de anonimato, también tiene vulnerabilidades y limitaciones, por lo que debemos de tener en cuenta que ningún sistema es cien por cien seguro. Algunas de las vulnerabilidades y limitaciones que podemos encontrar son las siguientes:

Ataque de intermediario o máquina en el medio

Los datos que circulan entre el nodo de salida y el servidor de destino no se encuentran cifrados, algunas personas aprovechan esta característica para controlar el nodo de salida y analizar el tráfico de red que sale al servidor de destino para obtener información privada. En este caso el atacante no podrá conocer nuestra dirección IP, pero si podrá ver para qué está utilizando alguien la red Tor.

Supongamos que una persona utiliza la red Tor para mantener su anonimato en la red, pero accede a una red social y visita su perfil, o peor aún, introduce sus credenciales para iniciar sesión. Si alguna persona está interceptando el tráfico de red del nodo de salida, podrá ver qué perfil ha visitado y también las credenciales.

Otra posibilidad es que un atacante pueda controlar el repetidor de guarda y el repetidor de salida. En este caso, este atacante tendría acceso tanto a nuestra dirección IP pública, como a los datos que estamos enviando al servidor de destino.

Ataque de correlación extremo a extremo

Si un atacante consiguiera analizar el tráfico de red entre el usuario y el nodo de guarda y entre el nodo de salida y el servidor de destino, podría relacionar los tiempos de envío de los paquetes. Imaginemos que se analiza el envío de 50 paquetes de red desde una dirección IP y existe una relación temporal directa entre estos 50 paquetes y otros 50 paquetes que son enviados por el nodo de salida, se podría llegar a la

conclusión de quién es el usuario que realiza el envío. Sin embargo, aunque este ataque es posible, no resulta sencillo de realizar, la red Tor cuenta con más de 6000 repetidores en todo el mundo y cada repetidor es utilizado por múltiples usuarios, algo que dificulta en gran medida que el atacante pueda tener acceso a los nodos de entrada y salida de un usuario concreto y poder analizar su tráfico.

Ataque de etiquetado

Para realizar este ataque, es necesario que el nodo de guarda y el nodo de salida estén comprometidos. El atacante intercepta la comunicación en ambos extremos del circuito y modifica el flujo de datos en uno de ellos. Si detecta el cambio realizado en el otro extremo, tendrá la confirmación de quién está enviando los datos al servidor de destino [59].

Visibilidad de Tor

Los proveedores de servicios de internet pueden saber si un cliente está utilizando la red Tor, ya que las direcciones IP de los nodos son públicas [49]. Esto también permite que, por ejemplo, los servidores web, puedan comprobar las direcciones IP en los registros de acceso y ver si se está accediendo a ellos a través de dicha red. De esta forma, algunos proveedores de servicios de internet bloquean el acceso a Tor, y los sitios web pueden bloquear las conexiones provenientes de esta red.

5. Técnicas para mitigar las vulnerabilidades y limitaciones de la red Tor, VPNs y proxies

5.1. Puentes Tor

Para evitar ser bloqueados por algunos proveedores de servicios de internet, Tor Browser permite configurar como nodo de entrada un nodo puente. Ya que las direcciones IP de los nodos puente no se publican, resulta más complicado que el acceso a esta red pueda ser bloqueado [49].

5.2. Tor sobre VPN

Para incrementar el nivel de seguridad, el usuario puede conectarse a un servidor VPN y posteriormente establecer la conexión con los repetidores de la red Tor. Esto permite ocultar la dirección IP del usuario al nodo de guarda e impide a nuestro proveedor de servicios de internet ver contenido de nuestra comunicación y saber que nos estamos conectando a la red Tor. Además, nuestro proveedor de VPN tampoco podrá ver el contenido de la comunicación, ya que esta irá cifrada por Tor.

En algunos casos, los proveedores de servicios de internet bloquean a los clientes el acceso a la red Tor. utilizar una VPN oculta al ISP que nos estamos conectando a esta red, ya que únicamente pueden ver que la conexión se establece con el servidor VPN.

Al utilizar estas dos tecnologías de forma conjunta el tráfico de datos sigue el siguiente proceso:

1. El cliente VPN encripta los datos.
2. Tor encripta los datos con las claves de los nodos del circuito.
3. Los datos doblemente encriptados son enviados al servidor VPN.
4. El servidor VPN desencripta los datos que continúan encriptados por Tor.
5. Los datos son enviados desde el servidor VPN al nodo de entrada en la red Tor.
6. Los datos son enviados a través del circuito establecido por TOR, donde cada nodo de la red descifra una capa de cifrado de los datos.
7. Los datos son enviados sin cifrar desde el nodo de salida al servidor web.

El proceso de los datos de respuesta del servidor web al usuario es el siguiente:

1. El servidor web envía los datos sin encriptar al nodo de salida de la red Tor.
2. Los datos son enviados a través de la red Tor, donde cada nodo, con su clave, encripta los datos con una capa de cifrado.
3. El nodo de entrada envía los datos cifrados por Tor al servidor VPN.
4. El servidor VPN encripta los datos.
5. Los datos doblemente encriptados son enviados al usuario.
6. Tor desencripta los datos con las claves de los nodos del circuito.
7. El cliente VPN desencripta los datos.

Sin embargo, no todo son ventajas, el proveedor de VPN aún sabrá que se está utilizando TOR. Por ello, es importante utilizar servicios VPN que no almacenen logs, y también se debe tener en cuenta que cuando el número de saltos que dan los datos en la red aumentan y se incrementan las capas de cifrado, también se incrementa el tiempo que estos datos tardan en llegar hasta su destino, por lo que se deberá de asumir que la conexión pueda ralentizarse.

5.3. Modo solo HTTPS

Para proteger los datos de un atacante que esté analizando la información entre el nodo de salida y servidor de destino, se puede utilizar el protocolo HTTPS. Como hemos visto anteriormente, tanto el navegador TOR como el navegador Brave cuentan con la opción de forzar la conexión HTTPS siempre que el sitio web que consultamos la tenga disponible. De esta forma, el tráfico que viaja entre el nodo de salida y servidor de destino estará cifrado y los datos no podrán ser interpretados por un atacante intermedio.

Igualmente, este modo tiene ventajas de seguridad a la hora de utilizar un proxy, ya que los datos viajan cifrados, evitando que personas intermedias puedan verlos. Sin embargo, no todos los proxies ni todos los sitios web soportan el protocolo HTTPS, por

lo que se deberá de estar seguro de utilizar un proxy compatible y que el sitio visitado dispone de esta opción.

5.4. Buenas prácticas

En caso de que se pretenda mantener el anonimato, el usuario deberá tener cuidado de no introducir nunca datos que le puedan identificar, como credenciales de inicio de sesión o acceder a su perfil en las redes sociales. Se debe tener en cuenta que, aunque se utilice el protocolo HTTPS y el atacante intermedio no pueda interpretar los datos cifrados, el servidor web de destino si dispondrá de esta información.

6. Comparativa de la red Tor, VPNs y proxies

Se realiza una tabla comparativa de diferentes tecnologías de anonimato analizadas en los apartados 3, 4 y 5:

Tabla 6: Comparativa de la red Tor, VPNs y proxies

	Red Tor	**VPN**	**Proxy HTTP/HTTPS**	**Proxy SOCKS**
Oculta la dirección IP	Sí	Sí	Sí	Sí
Dirección IP	Nodo de la red Tor	Servidor VPN	Servidor Proxy	Servidor Proxy
Encriptación	Encriptación por capas. SSL/TLS para HTTPS	OpenVPN, IPSec, etc. SSL/TLS para HTTPS	Solo proxy HTTPS. SSL/TLS	SSL/TLS para HTTPS
Protocolos	TCP	TCP, UDP …	HTTP/HTTPS	SOCKS4: TCP SOCKS5: TCP/UDP
Registra logs	No	Según el servicio	Según el servicio	Según el servicio
Enrutamiento	A través de múltiples nodos de la red Tor	A través del servidor VPN	A través del servidor proxy	A través del servidor proxy
Limitaciones	Falta de encriptación en el nodo de salida.	El proveedor de VPN tiene acceso a nuestra	Falta de encriptación de los datos en el proxy HTTP,	Falta de encriptación de los datos. El proveedor

	El nodo de entrada conoce nuestra dirección IP.	dirección IP y datos.	El proveedor del proxy tiene acceso a nuestra dirección IP y datos, IP compartida.	del proxy tiene acceso a nuestra dirección IP y datos, IP compartida.
Vulnerabilidades	Ataque de correlación extremo a extremo, hombre en el medio, ataque de etiquetado	VPN jihacking, fingerprinting, filtración de DNS, Puede registrar la actividad del usuario	Hombre en el medio, fingerprinting, Puede registrar la actividad del usuario, puertos abiertos	Hombre en el medio, Puede registrar la actividad del usuario, fingerprinting, puertos abiertos

La red Tor, los proxies y las VPN son tecnologías que permiten ocultar la identidad del usuario, sin embargo, tras los datos expuestos, se puede afirmar que no ofrecen el mismo nivel de anonimato. La encriptación de los datos en la red Tor y el enrutamiento de estos a través de los diferentes nodos, así como la encriptación de los datos de la VPN ofrece una clara ventaja sobre la tecnología proxy. En el caso de que la VPN no almacene logs, el usuario consigue un gran nivel de anonimato, sin tener que limitar el tráfico de red al protocolo TCP como ocurre con la red Tor.

Combinar un servicio VPN junto con la red Tor (Tor sobre VPN), proporciona un mayor nivel de anonimato, ya que oculta que estamos utilizando esta red al proveedor de servicios de internet, la dirección IP del usuario al repetidor de entrada y los datos al servidor VPN.

7. Sistemas operativos anónimos

7.1. Tails

Tails es un sistema operativo portátil, gratuito y de código abierto basado en Dibian/Gnu Linyx que cuenta con un alto nivel de protección para mantener el anonimato y seguridad del usuario y que ha sido recomendado por personalidades como Edwar Snowden o Roger Dingledine [60].

Este sistema operativo cuenta con las siguientes características:

- Puede ejecutarse directamente desde una memoria USB.

- Filtra todo el tráfico de red a través de la red Tor e impide que las aplicaciones puedan conectarse a internet sin utilizarla.

- Es un sistema operativo amnésico, no utiliza el disco duro, se ejecuta desde la memoria del ordenador y cuando se cierra, esta se borra de forma automática, por lo que se elimina toda la actividad realizada por el usuario sin dejar rastros.

- Permite guardar algunos archivos forma persistente dentro de la memoria USB. Estos archivos se cifran de forma automática para securizarlos.

- Contiene varias aplicaciones para trabajar de forma anónima y segura con documentos sensibles, como, por ejemplo, Tor Browser, Thunderbird y OnionShare.

7.2. Whonix

Es un sistema operativo gratuito y de código abierto basado en Debian GNU/Linux que está enfocado en proveer al usuario seguridad, privacidad y anonimato en internet.
Sus características principales son [61]:

- Puede ser ejecutado sobre los sistemas operativos Windows, Linux, MacOs, Qubes y KVM o en una memoria USB.

- Se ejecuta en una máquina virtual y fuerza a todo el tráfico de red a pasar por la red Tor.

- Whonix tiene instalado por defecto el add-on vanguards que mejora la seguridad de la red Tor, ya que incrementa el número mínimo de repetidores de tres a cuatro.

- No colecciona datos personales del usuario.

- Cuenta con una selección de aplicaciones seguras instaladas como KeePassXC, HexChat o Tor Browser.

- Está basado en la distribución Linux kickSecure que ofrece protección ante virus y malware.

7.3. Qubes OS

Qubes OS es un sistema operativo gratuito y de código abierto especialmente diseñado para proteger la seguridad del usuario. Cuenta con un sistema de virtualización basado en Xen, que aísla en compartimentos separados llamados qubes todas las aplicaciones que se ejecutan en el mismo. [62]

Sus principales características son las siguientes:

- Permite utilizar diferentes sistemas operativos, como Windows, Debian y Fedora.
- Implementa el sistema operativo Whonix con acceso a la red Tor.
- Aísla mediante técnicas de virtualización en compartimentos (máquinas virtuales) las aplicaciones ejecutadas sobre el sistema operativo elegido.
- Permite crear contenedores de creación rápida para ejecutar y modificar ficheros no confiables sin afectar al resto de máquinas virtuales. Estos contenedores se autodestruyen al cerrarse.

8. Pruebas de anonimato con servidor Apache2

Para evaluar el anonimato ofrecido por las diferentes tecnologías y técnicas expuestas se crea un servidor web HTTP Apache2 sobre Ubuntu 20.10. Para que el servidor sea accesible desde internet, se utiliza el proveedor de Servicios y host No-IP [63].

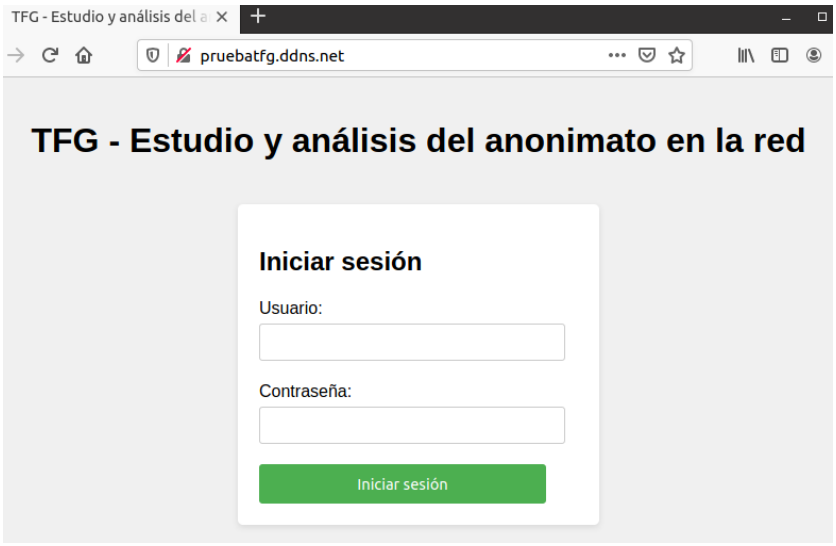

Figura 8: Página web sobre Apache2

El servidor contiene una página web, que tiene la dirección pública “pruebatfg.ddns.net”. Se accederá a esta página utilizando diferentes herramientas de anonimato, con el fin de evaluar mediante el fichero de registro de accesos (access.log) si en algún momento se filtra la dirección IP real del usuario.

Se deben de tener en cuenta las siguientes consideraciones:

- La dirección IP de la máquina de origen es: 192.168.185.228
- La dirección IP pública es: xx.xx.12.169

- Se utilizará el navegador Firefox para realizar las pruebas, salvo cuando la prueba se refiera a Tor Browser.

8.1. Resultados de las pruebas con el servidor Apache2

Conexión sin herramientas de anonimato

xx.xx.12.169 - - [27/May/2023:09:56:33 +0200] "GET / HTTP/1.1" 200 1024 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"

Tor Browser

192.42.116.192 - - [26/May/2023:22:06:07 +0200] "GET / HTTP/1.1" 200 1024 "-" "Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0"

192.42.116.192 - - [26/May/2023:22:06:08 +0200] "GET /favicon.ico HTTP/1.1" 404 496 "http://pruebatfg.ddns.net/" "Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0"

Figura 9: Circuito Tor en Tor Browser

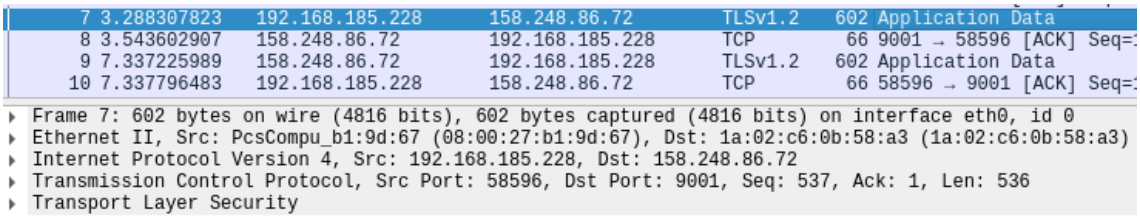

Figura 10: Conexión con el nodo de entrada de la red Tor vista en Wireshark

Red Tor mediante ProxyChains

89.163.143.8 - - [25/May/2023:15:48:57 +0200] "GET / HTTP/1.1" 200 1024 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"

89.163.143.8 - - [25/May/2023:15:48:58 +0200] "GET /favicon.ico HTTP/1.1" 404 496 "http://pruebatfg.ddns.net/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"

```
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  pruebatfg.ddns.net:80
 ...  OK
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  pruebatfg.ddns.net:80
 ...  OK
```

Figura 11: Conexión al servidor web Apache2 con Tor a través de Proxychains

Encadenamiento de proxies socks4 mediante ProxyChains

72.206.181.97 - - [27/May/2023:02:01:22 +0200] "GET / HTTP/1.1" 200 1024 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"

72.206.181.97 - - [27/May/2023:02:01:23 +0200] "GET /favicon.ico HTTP/1.1" 404 496 "http://pruebatfg.ddns.net/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4         127.0.0.1 9050
socks4  94.101.55.201   4153
socks4  184.178.172.14  4145
socks4  72.206.181.97   64943
socks4  85.228.43.192   4153
```

Figura 12: Lista de proxies

```
[proxychains] Dynamic chain  ...  72.206.181.97:64943  ...  pruebatfg.ddns.ne
t:80  ...  OK
```

Figura 13: Conexión proxy con ProxyChains

Proxy de élite

68.204.104.121 - - [27/May/2023:08:56:26 +0200] "GET / HTTP/1.1" 200 987 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"

```
402 29.208829726  192.168.185.228  64.225.4.29      HTTP   524 GET http://pruebatfg.ddns.net/ HTTP/1.1
403 29.353198502  64.225.4.29      192.168.185.228  TCP     66 9865 → 39614 [ACK] Seq=1 Ack=459 Win=64
404 29.857154081  64.225.4.29      192.168.185.228  HTTP   1053 HTTP/1.1 200 OK  (text/html)

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: 1a:02:c6:0b:58:a3 (1a:02:c6:0b:58:a3), Dst: PcsCompu_b1:9d:67 (08:00:27:b1:9d:67)
Internet Protocol Version 4, Src: 64.225.4.29, Dst: 192.168.185.228
Transmission Control Protocol, Src Port: 9865, Dst Port: 56120, Seq: 1, Ack: 1, Len: 0
```

Figura 14: Captura Wireshark de conexión proxy de élite

VPN

149.34.244.163 - - [26/May/2023:23:36:14 +0200] "GET / HTTP/1.1" 200 1024 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"

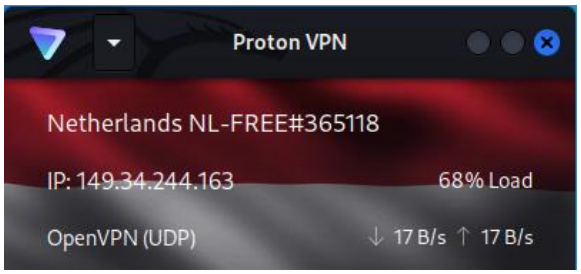

Figura 15: Conexión VPN [64]

129 63.211608451	192.168.185.228	149.34.244.159	OpenVPN	119	MessageType: P_DATA_V2
130 69.152836648	149.34.244.159	192.168.185.228	OpenVPN	119	MessageType: P_DATA_V2
131 69.153297980	192.168.185.228	149.34.244.159	OpenVPN	119	MessageType: P_DATA_V2

Figura 16: Conexión OpenVPN vista con Wireshark

Tor sobre VPN

45.151.167.11 - - [26/May/2023:23:43:12 +0200] "GET / HTTP/1.1" 200 1024 "-" "Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0"

45.151.167.11 - - [26/May/2023:23:43:15 +0200] "GET /favicon.ico HTTP/1.1" 404 496 "http://pruebatfg.ddns.net/" "Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0"

28 3.655671078	192.168.185.228	149.34.244.159	OpenVPN	119	MessageType: P_DATA_V2
29 3.732484542	149.34.244.159	192.168.185.228	OpenVPN	235	MessageType: P_DATA_V2
30 3.775102018	192.168.185.228	149.34.244.159	OpenVPN	119	MessageType: P_DATA_V2
31 8.684344155	149.34.244.159	192.168.185.228	OpenVPN	655	MessageType: P_DATA_V2

Figura 17: Conexión VPN Wireshark

Figura 18: Circuito Tor en Tor Browser

8.2. Conclusiones de los resultados

Como podemos observar, los diferentes métodos y tecnologías han permitido mantener oculta la dirección IP de origen. Además, el proxy de élite ha logrado ocultar también su propia dirección IP, lo cual se refleja en el registro de accesos del servidor web, donde se muestra una dirección diferente a la de este.

El navegador Tor Browser, ha enmascarado la huella digital, algo que no ha sucedido con las tecnologías que han utilizado el navegador Firefox. Este enmascaramiento, sin embargo, delata que el usuario ha utilizado Tor Browser para conectarse, ya que todos los usuarios de este navegador muestran la misma información. También es posible saber que un usuario ha utilizado la red Tor para conectarse a la página, ya que las direcciones IP de los nodos de salida de la red Tor son públicos.

9. Sigilo y anonimato en la fase de recopilación activa de información durante un ejercicio de pentesting

Utilizar herramientas y técnicas de sigilo y anonimato durante un ejercicio de pentesting es importe para simular un ataque lo más real posible. Las redes, pueden tener diferentes elementos de protección para detectar los ataques. Por ello, deben utilizarse técnicas que preserven nuestro anonimato y que impidan que seamos detectados.

Algunos de los sistemas de protección utilizados para detectar intrusiones son [65]:

- Sistema de detección de intrusión de red (NIDS): Recopila los paquetes del tráfico de red y los analiza en busca de patrones sospechosos. Si detecta un ataque, puede tomar medidas protectoras.

- Detección de intrusos basada en host (HIDS): Revisa la actividad del equipo en busca de anomalías. Es capaz de realizar acciones de protección y eliminar intrusiones.

- Sistema de detección de intrusiones (IDS): Es una aplicación que analiza el tráfico de red para detectar intrusiones, y genera alertas en caso de detectarlas. No es capaz de detener una intrusión por sí mismo, por lo que suele asociarse a firewalls.

- Sistema de prevención de intrusiones (IPS): Controla el tráfico de red en tiempo real para detectar el inicio de las intrusiones, y realiza medidas de protección para intentar detenerlas. Es similar al IDS, pero es capaz de realizar labores de protección preventiva.

A continuación, se presentan una serie de técnicas cuyo objetivo es evitar ser detectados por un IDS\IPS durante un ejercicio de pentesting en la fase de recopilación activa de información y mantener nuestro anonimato.

9.1. Nmap

Nmap (Network Mapper) es una herramienta gratuita, de código abierto y disponible para la mayoría de los sistemas operativos, que es utilizada habitualmente en auditorias de seguridad informática y en el reconocimiento de redes. Permite escanear redes de cualquier tamaño en busca hosts, realizar un sondeo de sus puertos y conocer sus servicios, aplicaciones, sistemas operativos, firewalls etc.

Para conocer que servicios y versiones están a la escucha en un puerto, Nmap realiza una solicitud al servicio y comprueba el banner que le devuelve. Es muy común que los servicios muestren información que puede ser utilizada por un atacante para buscar vulnerabilidades, como el nombre, versión e incluso sistema operativo utilizado.

Nmap ofrece distintos protocolos para el escaneo de puertos. Analizaremos aquellos que permiten realizar el sondeo de forma que sea difícil para la máquina objetivo detectarnos o identificarnos.

9.1.1. Escaneo TCP SYN (SYN Scan)

Este protocolo de sondeo de puertos utiliza el protocolo TCP Three way handshake para determinar si un puerto se encuentra en los estados abierto, cerrado o filtrado.

Imaginemos que un cliente quiere establecer conexión con un servidor. El protocolo TCP Three way handshake realiza los siguientes pasos [66]:

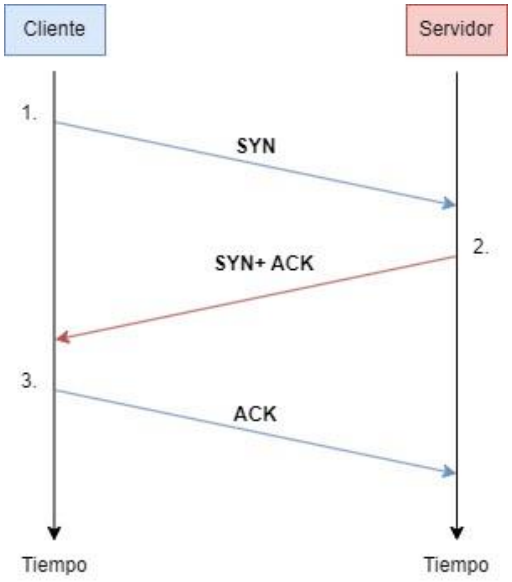

Figura 19: TCP Three way handshake

1. El cliente envía un paquete con la bandera SYN al puerto en que desea establecer conexión con el servidor. El servidor recibe el paquete SYN.

2. Si el servidor acepta realizar la conexión, realiza el envío de un paquete con las banderas SYN y ACK. El cliente recibe el paquete SYN + ACK.

3. El cliente comprueba que se ha establecido conexión enviando un paquete ACK.

El sondeo SYN es el escaneo por defecto en Nmap, para ejecutarlo, necesita que el usuario tenga privilegios, ya que modifica el contenido de los paquetes. Es un tipo de sondeo bastante sigiloso, ya que no llega a completar las conexiones. Es decir, no completa el protocolo Three way handshake, puesto que no es necesario para conocer el estado de los puertos.
El protocolo es el siguiente [67]:

1. El cliente envía un paquete con el flag SYN activo al puerto del servidor.

2. Si el servidor contesta SYN y ACK, será porque el puerto se encuentra abierto a la espera de establecer conexión y si contesta RST (reset) significará que el puerto se encuentra cerrado. Si no se recibe ninguna respuesta del servidor, Nmap volverá a enviar el paquete SYN por segunda vez, y si no hay contestación, confirmará que el puerto se encuentra filtrado. También se considerará filtrado si se reciben un error ICMP de tipo 3 (Destino no alcanzable), códigos 1, 2, 3, 9, 10, o 13.

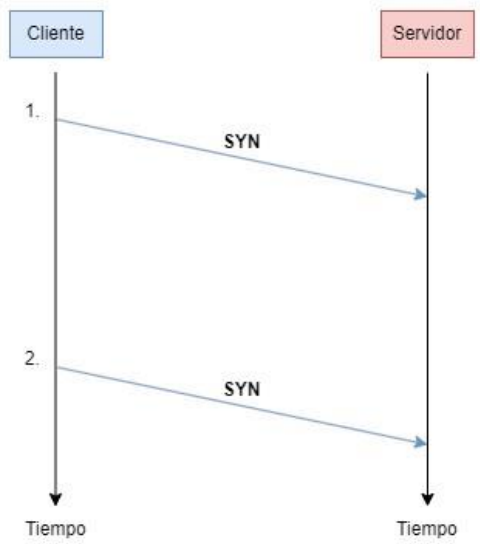

Figura 20: Escaneo SYN con puerto filtrado

3. En caso de que el servidor conteste SYN + ACK, el cliente responderá RST para que el servidor no tenga en cuenta el intento de conexión y si

contesta RST, no será necesario realizar ninguna acción, ya que la conexión ha sido rechazada.

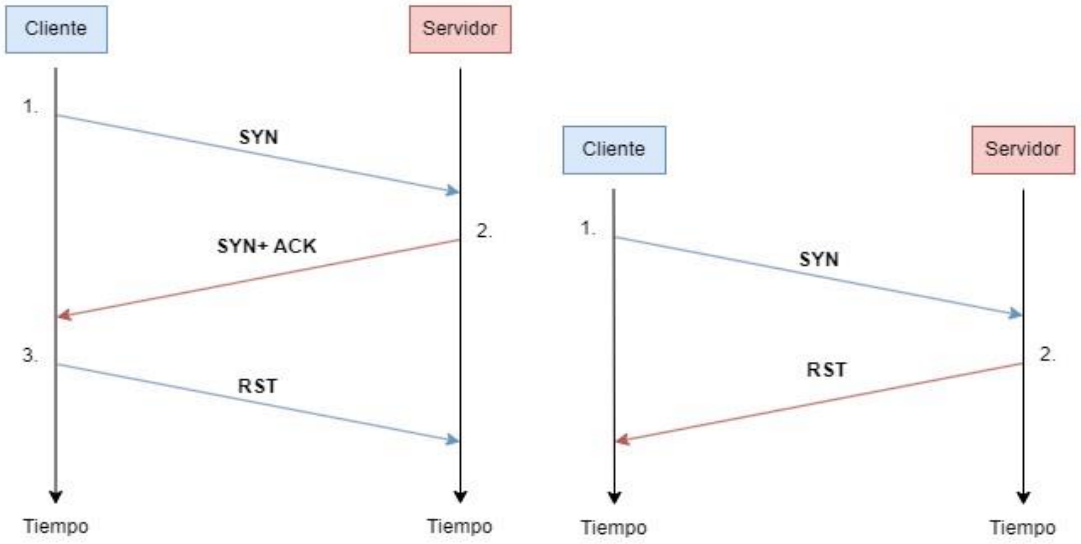

Figura 21: Escaneos SYN con puerto abierto y puerto cerrado

La sintaxis para realizar un escaneo SYN es la siguiente:
sudo nmap -sS <IP_víctima>

nmap: Ejecuta la aplicación Nmap.

-sS: Modo de escaneo SYN Stealth.

9.1.2. Escaneo con señuelos (Decoy Scan)

Nmap, cuenta con la opción -D (Decoy), que modifica la dirección IP de la cabecera de los paquetes enviados de forma que parezca que existen más equipos realizando el escaneo, sin que la víctima pueda diferenciar cual es el origen real de este.

Cuantos más señuelos se utilicen, más difícil será que nos identifiquen. Sin embargo, la protección no es absoluta, ya que, para obtener las respuestas de la víctima, sigue siendo necesario que se envíen paquetes desde la dirección real de origen.

La sintaxis es la siguiente:

nmap -D <IP_señuelo1, IP_señuelo2, IP_señuelo3…> <IP_víctima>

nmap: Ejecuta la aplicación Nmap.
-D: Permite añadir direcciones IP que se utilizarán como señuelos.

sudo nmap -sS -P0 -D <IP_señuelo1, IP_señuelo2, IP_señuelo3…> <IP_víctima>

RND:<Número de señuelos>: genera tantas direcciones IP aleatorias como número de señuelos indicados.

Por ejemplo, el siguiente código generaría 10 direcciones IP aleatorias:

nmap -D RND:10 <IP_víctima>

sudo nmap -sS -P0 -D RND:10 <IP_víctima>

9.1.3. Escaneo inactivo (Idle Scan)

Este tipo de sondeo es el que mejor permite mantener el anonimato del atacante, ya que realiza un sondeo de puertos TCP sin enviar paquetes desde la dirección IP del usuario. Estos se envían desde una dirección IP alternativa, perteneciente a un dispositivo de baja actividad llamado “host zombi”. Por ello, en caso de que se detecte el ataque, la IP de este host será reconocida como la dirección de origen.

El host zombi puede pertenecer a otro usuario y no tener conocimiento de que este está siendo utilizado para realizar el sondeo. Para determinar el estado de los puertos de la víctima, el atacante compara la IPID (Número de Identificación de Fragmento de un paquete IP) de la cabecera de los paquetes recibidos del host zombi. La IPID se incrementa en una unidad con el envío de cada paquete, por ello, es importante que el host zombi sea poco activo, como por ejemplo una impresora, para evitar incrementos de IPID que puedan confundirnos.

El escaneo zombi, también nos permite identificar máquinas de confianza de la máquina objetivo (que por lo general se encontrarán en su mismo segmento de red) y evadir su firewall, ya que puede ser que una máquina nos indique no tiene puertos abiertos, pero desde la dirección IP de un host zombi de confianza si se muestren abiertos [68].

Para entender cómo se realiza un escaneo idle, se deben conocer los siguientes principios:

1- Si una máquina recibe un paquete SYN en caso de aceptar la conexión, responde mediante SYN/ACK.

2- Cuando una máquina recibe un paquete SYN/ACK no solicitado responde con RST.

3- Cuando una máquina recibe un paquete RST no solicitado, lo ignora.

4- Los paquetes IP enviados por una máquina tienen un número de secuencia identificador de fragmento (IPID), este número es incrementado por el sistema operativo cada vez que se envía un paquete.

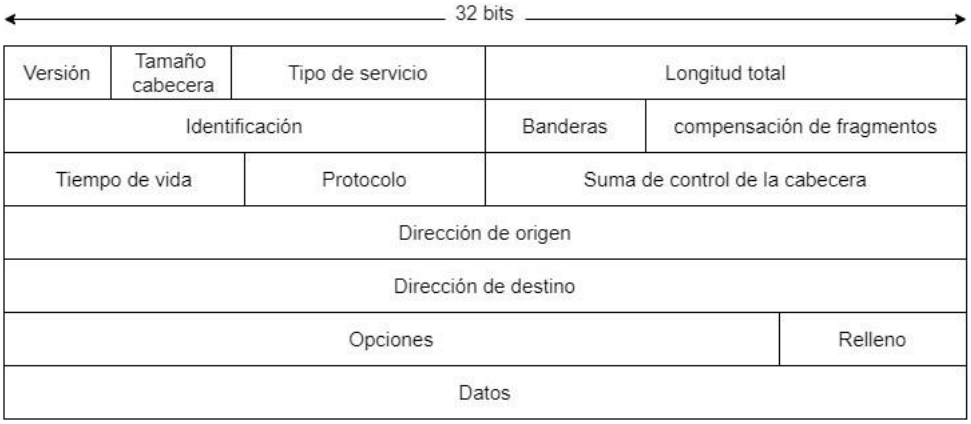

Figura 22: Paquete IP. Basado en [69]

El protocolo de escaneo Idle consta de los siguientes pasos [68]:

En caso de que el puerto de la máquina objetivo se encuentre abierto:

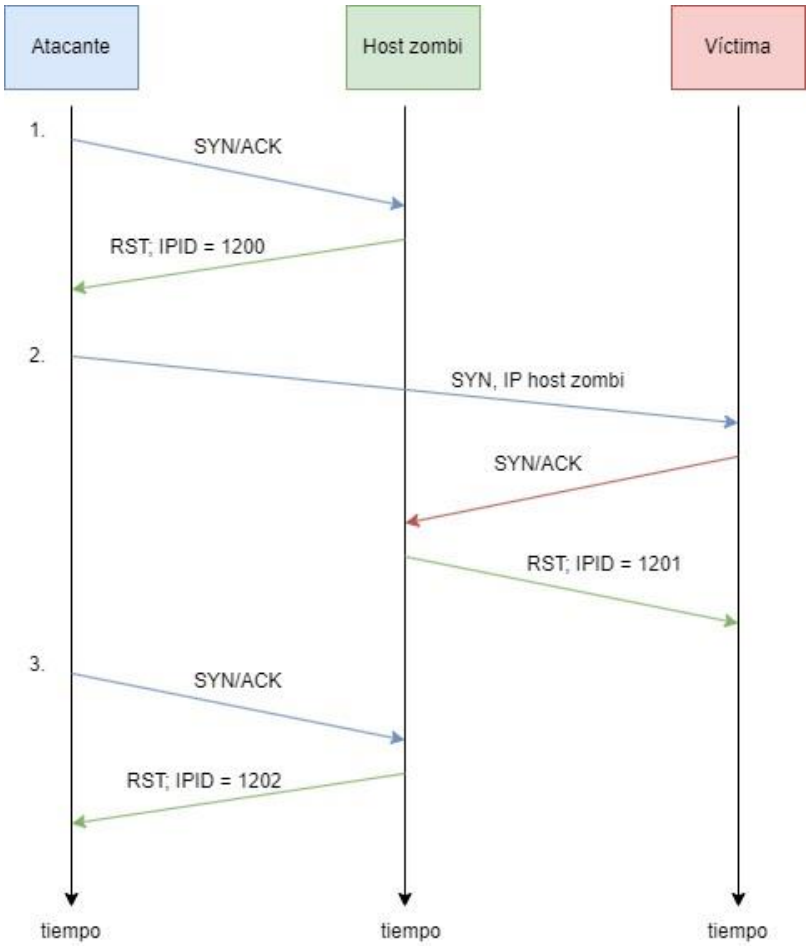

Figura 23: Escaneo Idle con puerto abierto

1. La máquina atacante envía un SYN|ACK al puerto destino del host zombi. El host zombi, responde con RST a la máquina atacante. Su respuesta incluye el identificador de fragmento o IPID.

2. La máquina atacante envía un SYN a la víctima utilizando la dirección IP de la máquina zombi. La máquina objetivo responde SYN/ACK a la máquina zombi. Esta incrementa su IPID en una unidad y responde RST al no haber solicitado inicialmente SYN.

3. La máquina atacante, envía SYN/ACK a la máquina zombi. La máquina zombi incrementa su IPID en una unidad y responde la máquina atacante RST con el número IPID actual.

Comparando el primer IPID recibido, con el segundo, se puede ver que se ha incrementado en dos unidades, una en el paso 2 y otra en el paso 3 Por lo tanto el puerto se encuentra abierto.

En caso de que el puerto de la máquina objetivo se encuentre cerrado:

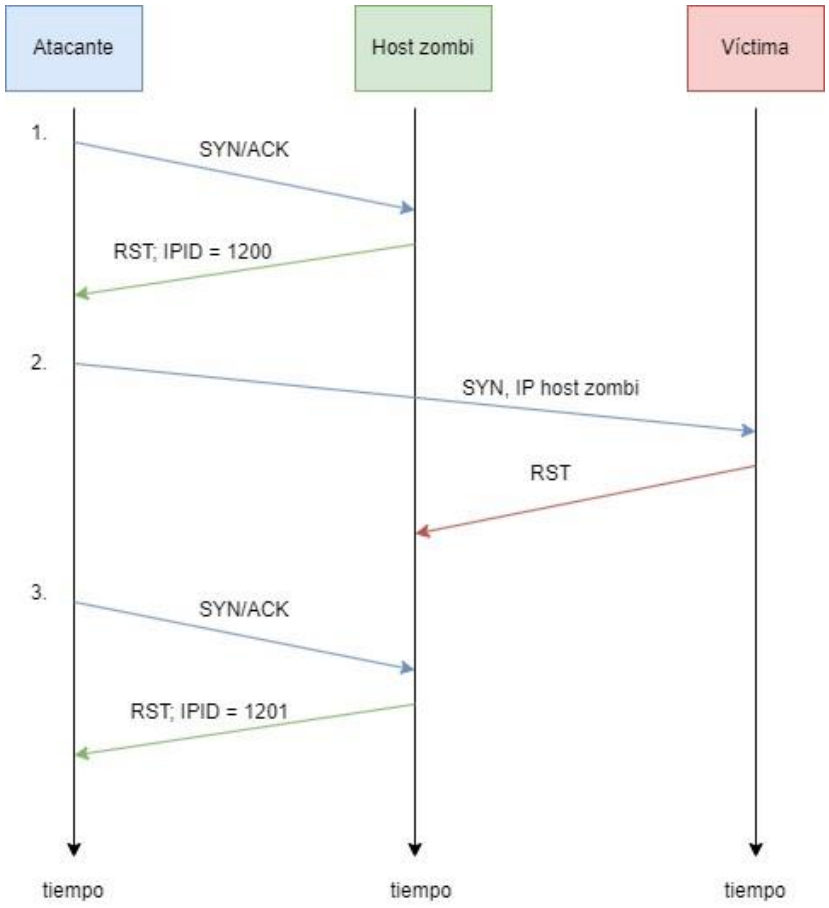

Figura 24: Escaneo Idle con puerto cerrado

1. Se repite el paso 1 indicado anteriormente.

2. La máquina atacante envía un SYN a la víctima utilizando la dirección IP de la máquina zombi. La víctima devuelve RST ya que el puerto se encuentra cerrado. La máquina zombi ignora el mensaje RST.

3. La máquina atacante, envía SYN/ACK a la máquina zombi. La máquina zombi incrementa el IPID y envía RST a la máquina atacante.

Al comparar el IPID inicial y el IPID recibido en el paso 3, la máquina atacante puede ver que este únicamente se ha incrementado en una unidad, correspondiente al paso 3. Por lo tanto, se determina que el puerto está cerrado.

En caso de que el puerto se encuentre filtrado:

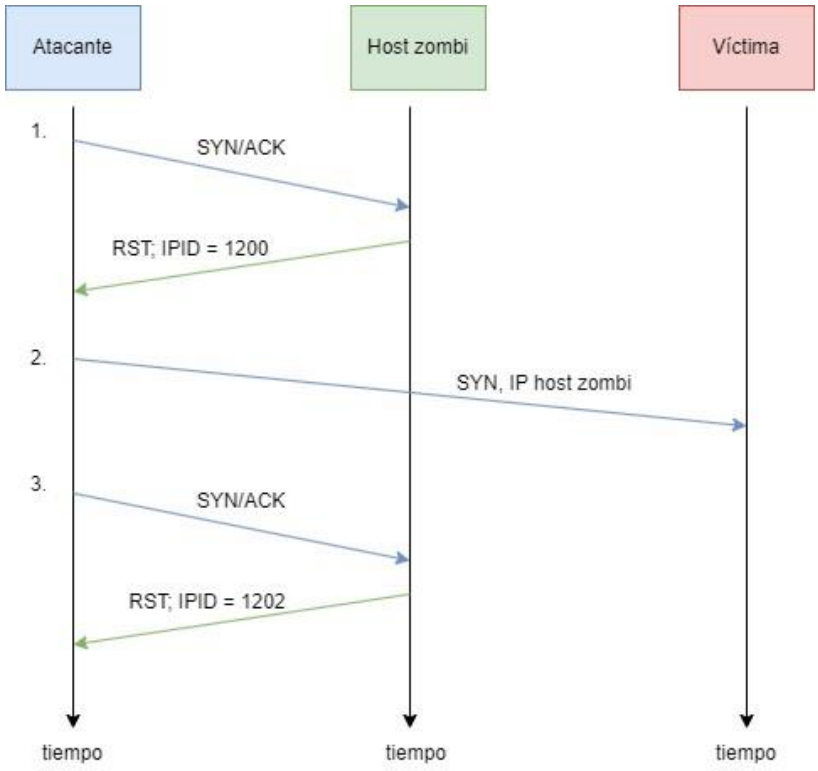

Figura 25: Escaneo inactivo con puerto filtrado

1. Se repite el paso 1 igual que en los casos anteriores.
2. La máquina atacante envía un SYN a la víctima utilizando la dirección IP de la máquina zombi, pero la víctima no envía ninguna respuesta a la máquina zombi.
3. La máquina atacante, envía SYN/ACK a la máquina zombi. La máquina zombi incrementa el IPID y envía RST a la máquina atacante.

Al comparar el IPID inicial y el IPID recibido en el paso 3, la máquina atacante comprueba que solo se ha incrementado en una unidad, por lo que no puede distinguir un puerto filtrado de un puerto cerrado. En este caso, sería conveniente localizar y utilizar un host zombi de confianza de la víctima, en cuyo caso, al repetir el escaneo, se podría evadir el filtrado.

Para realizar el idle scan primeramente necesitamos realizar la búsqueda de host zombis, para ello utilizaremos el script ipidseq proporcionado por Nmap y las siguientes sintaxis de comandos:

nmap -p<puertos> --script ipidseq -IR <Numero de objetivos>

p: Puertos a escanear. Si se desea incluir varios, se separan por comas.

--script: Indica que utilice el script.

Ipidseq: Script incluido por Nmap para localizar host zombi. iR: Objetivos aleatorios.

Los candidatos a host zombi deberán de retornar "|_ipidseq: Incremental!" para ser válidos. Ya que necesitamos que su IPID se incremente tras la transferencia de cada paquete.

Una vez tengamos la dirección del host zombi, realizaremos el sondeo de la máquina objetivo de la siguiente forma:

Escanear objetivo: nmap -sI <Ip zombie> <Ip objetivo>

-sI: Idle Scan. Inicia el escaneo de puertos utilizando la dirección IP del zombi como origen.

9.1.4. Escaneo con falsificación de IP (IP Spoofing)

Nmap permite ocultar nuestra dirección IP al realizar el escaneo de una máquina. Para ello, sustituye en la cabecera de los paquetes la dirección IP de origen por una de nuestra elección. Esta técnica solo funciona si la máquina que estamos escaneando se encuentra en nuestra misma subred, de lo contrario, al haber modificado nuestra dirección IP no recibiremos los paquetes.

La sintaxis para realizar la ocultación de IP es la siguiente:

nmap -e <interfaz de red> -S <dirección IP falsa> <víctima>

9.1.5. Escaneo con falsificación de MAC (MAC Spoofing)

Para ayudarnos a mantener nuestro anonimato y evadir firewalls que pueden haber bloqueado nuestra dirección MAC, podemos ocultarla con la siguiente sintaxis de comandos:

nmap --spoof-mac <dirección MAC falsa> <víctima>

Al realizar la ocultación de la MAC, para recibir los paquetes de respuesta debemos encontrarnos en el mismo segmento de red que la víctima.

9.1.6. Escaneo socks (Socks Scan)

Para ocultar nuestra identidad, podemos redirigir el tráfico de nuestro escáner a través de uno o varios proxies o de la red Tor. Como mencionamos anteriormente, una vez que tenemos el servicio Tor instalado y activo, Proxychains nos permite redirigir el tráfico de red de una aplicación a través de una lista de proxies especificados en su configuración o de nuestra red local mientras el servicio Tor está en ejecución. Esto nos permite redirigir el tráfico de la aplicación a través de la red Tor y mantener nuestra identidad oculta.

Proxychains solo redirige el tráfico TCP, por lo tanto, debemos utilizar técnicas de escaneo que utilicen este mismo protocolo. Para lograrlo, podemos utilizar el comando "-Pn" al ejecutar Nmap para evitar el descubrimiento del host, lo que podría filtrar paquetes ICMP. Además, es importante evitar las filtraciones DNS que puedan revelar nuestra identidad. Para ello, podemos utilizar el comando "-n" o descomentar la opción "proxy_dns" en el archivo de configuración de Proxychains, de modo que redirija las resoluciones DNS a través del proxy.

La sintaxis para realizar el escaneo será la siguiente:

proxychains4 nmap -Pn -n -sT <IP_Víctima>

Nmap también nos permite realizar escaneos de puertos a través de proxies sin necesidad de utilizar aplicaciones externas como proxychains mediante la siguiente sintaxis de comandos:

nmap -Pn -n --proxies <<tipo de proxy><dirección proxy><puerto> <Ip_víctima>

Para comprobar si ocurren filtraciones podemos utilizar el comando tcpdump:

tcpdump -vvv host <IP_Víctima>

9.2. Pruebas en un ejercicio de pentesting

Se realizan una serie de pruebas para comprobar qué técnicas de escaneo permiten mantener el anonimato durante un ejercicio de pentesting en la fase de obtención activa de información, ya sea mediante la ocultación de datos que revelen nuestra identidad o que consigan evitar ser detectadas por los sistemas de detección de intrusiones.

Para la realización de las pruebas se utiliza el mapeador de redes Nmap y las siguientes herramientas:

Snort

Es un sistema de prevención de intrusiones gratuito y de código abierto que utiliza reglas de detección sobre la actividad de la red y genera alertas cuando estas se cumplen [70]. Snort puede ser ejecutado con tres funciones diferentes:

- **Sniffer:** Monitoriza el tráfico de la red.
- **Registro de paquetes:** Recopila los paquetes de red y los registra en un fichero del disco duro para que posteriormente puedan ser analizados.
- **Sistema de prevención de intrusiones/detección de intrusiones:** analiza en tiempo real la actividad de la red en busca de ataques y pruebas definidos en las reglas. En caso de encontrar coincidencias, puede tomar diversas acciones, como mostrar alertas, terminar sesiones, bloquear paquetes o descartarlos.

Snort, por defecto, incluye una serie de reglas creadas por su comunidad, pero también puede utilizar reglas definidas por el propio usuario mediante la siguiente sintaxis:

<acción> <protocolo ip-origen> <puerto-origen> <dirección ip de destino> <puerto de destino> (opciones;).

Para activar Snort en modo IDS se utiliza el siguiente comando:

snort -A console -c /etc/snort/snort. Conf

VirtualBox

Es un software de virtualización de código abierto que permite crear máquinas virtuales. Las máquinas virtuales permiten ejecutar un sistema operativo de forma aislada y segura sobre otro sistema operativo. Con Virtualbox se pueden ejecutar en las máquinas virtuales diferentes versiones de Windows y Linux, así como Solaris, OpenSolaris, OS/2 y OpenBSD [71].

Wireshark

Es un programa gratuito y de código abierto que permite realizar la visualización en tiempo real, captura y análisis detallado de los paquetes de red. Pertenece al grupo de los llamados analizadores de protocolos de red o snifffers y cuenta con numerosos filtros que facilitan la obtención de información.

9.2.1 Topología

Para la realización de las pruebas creamos una red interna y una red externa. En la red interna se encuentran la máquina objetivo (MV Objetivo) y la máquina que contiene el IDS Snort (MV Snort). La máquina Snort además de tener conexión con la red interna, también tiene conexión con la red externa. Esta máquina, analiza, filtra y enruta el tráfico procedente de la red externa hacia la máquina objetivo. En la red

externa, también se encuentran la máquina atacante (MV Atacante) y una máquina zombi (MV Zombi) que nos servirá para realizar las pruebas con escaneo inactivo.

La configuración de red es la siguiente:

Tabla 7: Configuración de red

	MV Objetivo	**MV Atacante**	**MV Snort interna**	**MV Snort externa**
Dirección IP	10.0.5.5	192.168.1.50	10.0.5.4	192.168.1.33
Máscara de red	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Puerta de enlace	10.0.5.4	192.168.1.1	10.0.5.4	192.168.1.1
Interfaz	eth0	eth0	enp0s8	enp0s3

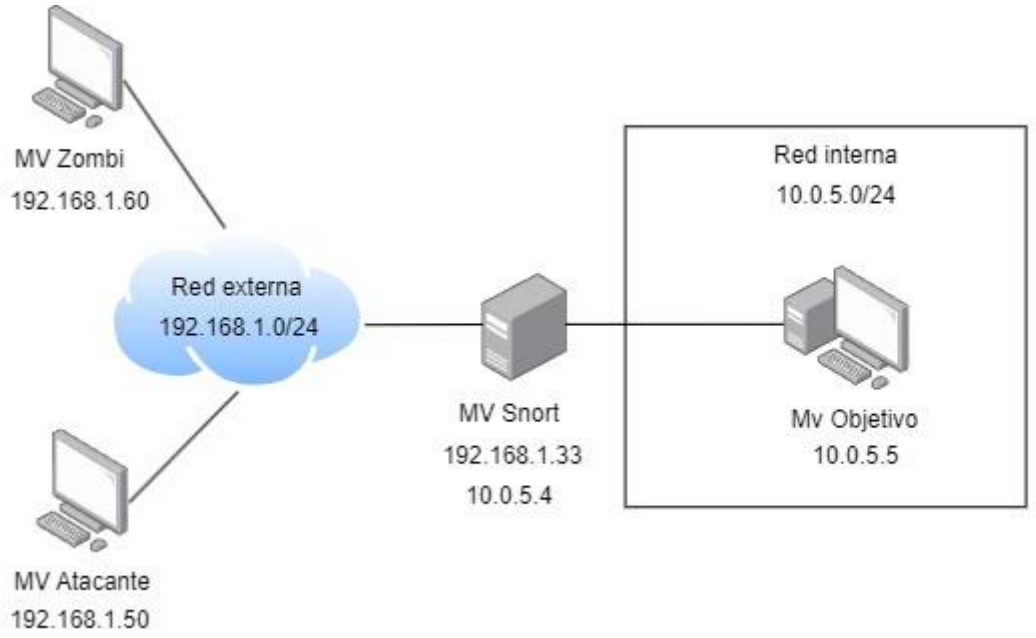

Figura 26: Topología de red

Para enrutar el tráfico de la máquina atacante a la red interna a través de la máquina Snort insertamos el siguiente comando en la consola de la máquina atacante:

ip route add 10.0.5.0/24 via 192.168.1.33 dev eth0

Los sistemas operativos de las máquinas virtuales son los siguientes:

Máquina atacante: Ejecutará la distribución Kali Linux 2021.1.
Máquina objetivo: la máquina objetivo Ubuntu server 14.04 de metaesploitable 3.
Máquina Snort: Ejecuta Ubuntu 20.10.

Máquina zombi: Ejecuta Windows server 2008 de metaesploitable 3.

9.2.2. Configuración de Snort

- Para proteger la red interna, Snort se configura con valor <<HOME_NET>> 10.0.5.0/24. Se considerará atacante cualquier red externa, por lo que se configura <<EXTERNAL_NET>> any.

- Se utilizarán las reglas incluidas en la instalación de Snort versión 2.9.7.0 GRE.

- Se mantiene la configuración por defecto de preprocesadores.

- El resumen de reglas obtenido al ejecutar Snort en modo IDS es el siguiente:

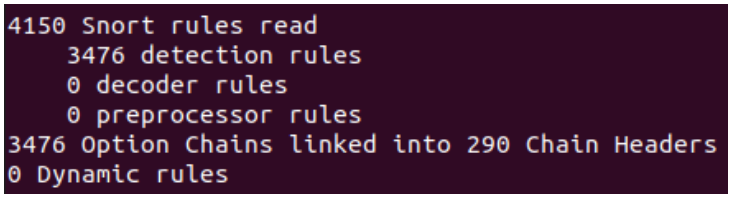

Figura 27: Reglas Snort

9.2.3. Pruebas con diferentes tipos de escaneos

Escaneo TCP SYN

Realizamos un escaneo tipo SYN con el siguiente comando:

sudo nmap -Pn -sS 10.0.5.5

El comando -Pn indica que no se realice el descubrimiento del host.

Snort ha generado dos alertas.

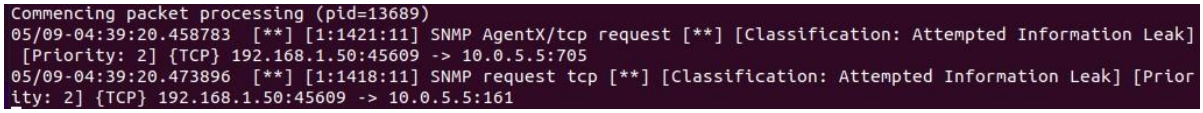

Figura 28: Alertas Snort SYN scan

Escaneo con ocultación de IP

La técnica de ocultación de IP solo permite recibir contestación de la máquina objetivo cuando nos encontramos en su misma red. Para realizar este escaneo se ha modificado el fichero snort.conf, cambiando el valor de “HOME_NET” a “any”, de forma que pueda detectar los escaneos a la red 192.168.1.0/24.

Se ejecuta un escaneo tipo SYN con ocultación de IP, sustituyendo la dirección IP de origen por 192.168.1.220 con el siguiente comando:

Sudo nmap -sS -Pn -e eth0 -S 192.168.1.220 192.168.1.33

El comando -e eth0 indica que la interfaz a utilizar sea eth0.

Snort es capaz de detectar el ataque y muestra dos alertas. La dirección IP de origen es ocultada de forma efectiva:

Figura 29: Alertas Snort ocultación de IP

No se encuentra rastro de la IP real de origen en Wireshark. Solo se identifica la dirección IP falsa:

Figura 30: Captura de Wireshark con ocultación de IP

Ocultación de MAC

Esta técnica nos permite ocultar la dirección MAC del dispositivo empleado para realizar el escaneo. Podemos utilizar direcciones MAC predefinidas para realizar la ocultación, como por ejemplo Apple o cisco:

sudo nmap -Pn -spoof-mac Apple 10.0.5.5

Snort lanza dos alertas:

Figura 31: Alertas Snort con ocultación de MAC

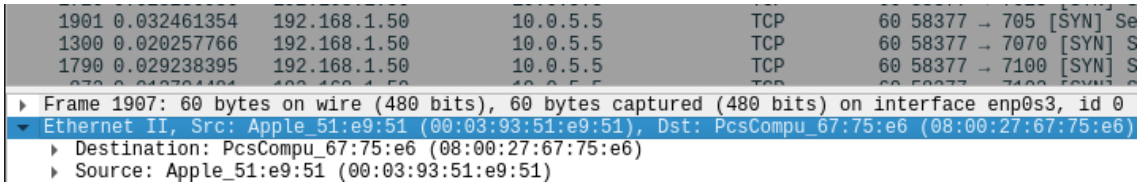

Figura 32: captura de Wireshark con dirección MAC oculta

Escaneo con señuelos

Se realiza un escaneo con señuelos con el comando:

Sudo nmap -sS -Pn -D RND:10 10.0.5.5

El comando RND:10 indica que se utilicen 10 direcciones de señuelos aleatorias.

Se han producido veintidós alertas.

Nuestra dirección IP se oculta entre las direcciones aleatorias, aunque puede seguir siendo detectada.

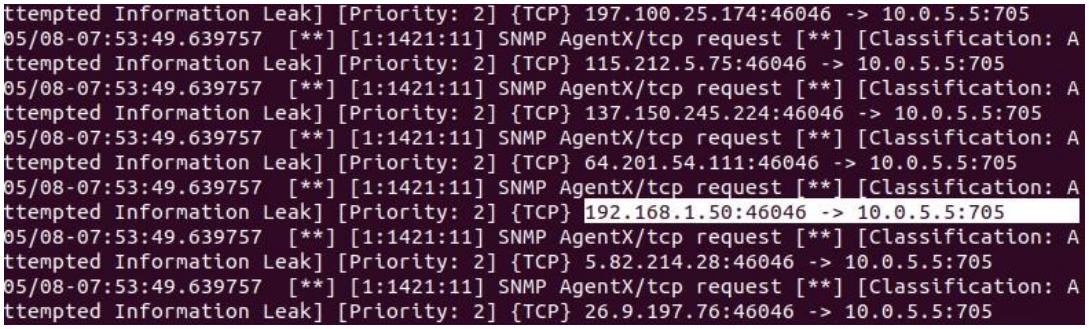

Figura 33: Alertas Snort de escaneo con señuelos

Escaneo inactivo

Se realiza este escaneo a través de la MV zombi con el siguiente comando:

Sudo nmap -sI 192.168.1.60 -Pn 10.0.5.5

Snort lanza cuatro alertas y detecta el origen del escaneo desde la dirección IP del host zombi.

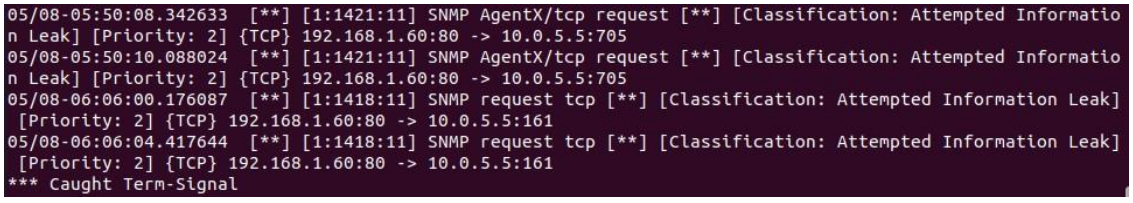

Figura 34: Alertas Snort con escaneo inactivo

Escaneo con reducción de tiempo

Se realiza un escaneo SYN aumentando los tiempos de espera en el envío de paquetes. Estos tiempos pueden ser modificados mediante el comando -T, que abarca de -T0 a -T5, siendo -T0 el modo más lento, -T3 el modo por defecto y -T5 el más rápido.

Para realizar esta prueba, utilizamos los siguientes comandos:

sudo nmap -T2 -Pn -sS 10.0.5.5

Snort ha lanzado 2 alertas:

```
Commencing packet processing (pid=14567)
05/09-05:58:46.443779  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak]
 [Priority: 2] {TCP} 192.168.1.50:52841 -> 10.0.5.5:705
05/09-06:02:24.464540  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Prior
ity: 2] {TCP} 192.168.1.50:52841 -> 10.0.5.5:161
```

Figura 35: Alertas Snort T2

sudo nmap -T5 -Pn -sS 10.0.5.5

Snort ha lanzado 2 alertas:

```
05/27-13:57:52.324379  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Inform
ation Leak] [Priority: 2] {TCP} 192.168.1.50:42896 -> 10.0.5.5:161
05/27-13:57:52.330590  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted
 Information Leak] [Priority: 2] {TCP} 192.168.1.50:42896 -> 10.0.5.5:705
```

Figura 36: Alertas Snort T5

Escaneo con fragmentación de paquetes

Efectuamos un escaneo SYN y utilizamos el comando -f para fragmentar los paquetes IP en paquetes de 8 bits.

sudo nmap -sS -f -Pn 10.0.5.5

Snort ha lanzado 2 alertas:

```
Commencing packet processing (pid=13803)
05/09-04:52:44.571761  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak]
 [Priority: 2] {TCP} 192.168.1.50:48413 -> 10.0.5.5:705
05/09-04:52:44.579699  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Prior
ity: 2] {TCP} 192.168.1.50:48413 -> 10.0.5.5:161
```

Figura 37: Alertas Snort Fragmentación de paquetes

Con wireshark podemos comprobar los paquetes fragmentados:

```
▾ [3 IPv4 Fragments (24 bytes): #4009(8), #4010(8), #4014(8)]
    [Frame: 4009, payload: 0-7 (8 bytes)]
    [Frame: 4010, payload: 8-15 (8 bytes)]
    [Frame: 4014, payload: 16-23 (8 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 24]
    [Reassembled IPv4 data: fdf719a63381ee6b0000000006002040089bc0000020405b4]
```

Figura 38: Wireshark fragmentación de paquetes

Escaneo de los puertos principales

Por defecto, nmap realiza el escaneo de los 1000 puertos más populares. Con el comando --top-ports <número de puertos> podemos especificar el número de puertos más populares que queremos analizar. Esta regla permite reducir la cantidad de paquetes necesarios para escanear un objetivo, al reducir el número de puertos que se están escaneando. Esto dificulta la detección por parte de Snort, ya que se reducen las señales de tráfico que delatan la actividad de escaneo.

En este caso se realiza un escaneo de los 100 puertos más populares según la lista de nmap con el siguiente comando:

Sudo nmap -Pn –top-ports 100 -sS 10.0.5.5

Otra opción para que solo se realice el escaneo de los 100 puertos más populares es el comando -F:

Sudo nmap -Pn -F -sS 10.0.5.5

Snort no ha detectado el escaneo. No se muestran alertas. Ha conseguido detectar la misma cantidad de puertos abiertos que el ataque SYN original, salvo el puerto 6667/tcp open irc.

9.2.4. Comparativa de resultados

Se realiza una tabla comparativa en función de los datos obtenidos con Snort.
Se debe tener en cuenta que se ha utilizado el comando -Pn en todos los tipos de escaneo para evitar la identificación del host.

Tabla 8: Comparativa de resultados con diferentes tipos de escaneos

Tipo de escaneo	Número de alertas	IP detectada	Nivel de ocultación de la IP
TCP SYN	2	Sí	Nulo
SYN con ocultación de IP	2	No	Total
SYN con ocultación de MAC	2	Sí	Nulo
SYN con señuelos	22	Sí	Parcial
Inactivo	4	No	Total
SYN con fragmentos	2	SÍ	Nulo
SYN con tiempo T2	2	Sí	Nulo
SYN con tiempo T5	2	Sí	Nulo
SYN de los 100 puertos principales	0	No	Nulo

Como se puede observar en la tabla, Snort ha sido capaz de detectar todos los escaneos menos el de los 100 puertos principales, ya que este escaneo no ha analizado los puertos que generaban el resto de las alarmas. Además, el escaneo SYN con ocultación de IP, y el escaneo inactivo, han permitido ocultar la dirección IP del atacante de forma total, y el escaneo con señuelos, de forma parcial. Por ello, se recomienda utilizar técnicas de escaneo con señuelos o de ocultación de la IP, así como ocultar la MAC o emplear técnicas de escaneo inactivo para evitar ser identificados.

10. Conclusiones

Resultados

La elección del navegador para conectarse a internet es fundamental para mantener la privacidad. Aunque todos los navegadores analizados ofrecen múltiples opciones para proteger la privacidad y seguridad, los navegadores Brave y Tor han sido las opciones destacadas en las pruebas de rastreo y fingerprinting. Respecto a la navegación anónima, tanto Brave como Tor Browser permiten conectarse a través de la red Tor de forma sencilla ofreciendo un alto grado de anonimato.

En las pruebas realizadas sobre el servidor Apache2, tanto los proxies como la red Tor y la VPNs han conseguido ocultar la dirección IP del usuario. Sin embargo, ocultar la dirección IP por si solo, no es suficiente para garantizar que el usuario no vaya a ser identificado. Por su implementación de red con varios saltos entre nodos, y el cifrado de datos, acceder a los sitios web a través de la red Tor mediante Tor Browser o Tor sobre VPN con el modo solo-HTTPS activado en ambos casos, se muestran como opciones destacadas para obtener una conexión anónima. Si se utilizan sistemas operativos seguros como Whonix o Tails, se reduce aún más el riesgo de poder ser identificado, al evitar posibles filtraciones como la filtración de datos DNS. Sin embargo, ninguna herramienta o técnica puede garantizar al 100% que no sea posible ser identificado, especialmente, si el usuario no mantiene buenas prácticas que puedan revelar su identidad, como utilizar correos electrónicos personales, acceder a perfiles propios de redes sociales, etc. Además, siempre que se utilicen estas herramientas, se debe aceptar que la velocidad de conexión se verá afectada. Por lo tanto, aquellos usuarios que las utilicen en su navegación habitual deberán valorar su conveniencia.

Durante el ejercicio de escaneo de puertos con Nmap, se pudo observar que el riesgo de ser identificado disminuye al reducir el número de puertos escaneados y que la técnica de ocultación MAC esconde esta de forma efectiva. También se pudo observar que las técnicas de ocultación de la dirección IP, el escaneo con señuelos y el escaneo inactivo fueron las que ofrecieron mayores garantías de evitar ser identificados, ya que el sistema de detección de intrusiones Snort demostró ser altamente efectivo en reconocer los ataques.

Objetivos

Se han conseguido alcanzar todos los objetivos planteados al inicio del trabajo. El objetivo general número 1 y los objetivos específicos 2, 3 se han conseguido con los apartados 3, 4, 5, 6, 7 en los que se han analizado diferentes herramientas y técnicas de anonimato, sus vulnerabilidades, limitaciones y técnicas para mitigarlas. El objetivo específico número 4 se ha conseguido en el apartado 8, en el cual se han realizado una serie pruebas para comprobar la efectividad de estas técnicas.

El objetivo general número 2 se ha conseguido en el apartado 9, realizando un análisis de técnicas de sigilo, evasión y anonimato con Nmap, junto con pruebas prácticas para valorar su capacidad de mantener el anonimato del usuario atacante.

El objetivo específico número 1 se ha conseguido en el apartado número 2, en el cual se han analizado los distintos tipos de cookies, las características de privacidad y anonimato de una selección de navegadores y se han ofrecido configuraciones para optimizar la privacidad de estos.

Pese a que se han conseguido todos los objetivos del trabajo, el Trabajo Final de Grado ha requerido emplear una cantidad de tiempo muy superior a la estimada. Además, la planificación inicial de las tareas ha terminado teniendo una extensión mayor a la esperada, por lo que ha sido necesario incluir algunas tareas como anexos.

Conclusiones

Realizar este Trabajo Final de Grado me ha permitido aprender sobre una gran cantidad de herramientas empleadas en ciberseguridad, en especial sobre aquellas empleadas para navegar de forma anónima, máquinas virtuales y escaners. También sobre configuraciones de red y a ser más consciente de la importancia de mantener buenas prácticas que garanticen nuestra privacidad en internet. Además, he descubierto un área profesional que siempre me había llamado la atención, pero sobre la que no había profundizado y de la que me gustaría seguir aprendiendo en el futuro.

Trabajo futuro

Como líneas de investigación futura, sería interesante estudiar en profundidad las diferentes vulnerabilidades de las herramientas de anonimato tratadas, investigar otras redes anónimas como Freenet e I2P y evaluar mediante pruebas el nivel de anonimato ofrecido por los sistemas operativos centrados en ofrecer privacidad y anonimato como Whonix, Tails y Qubes OS. También comprobar la efectividad de las técnicas de escaneo con sigilo y de ocultación de la identidad sobre otros conjuntos de reglas en Snort y sobre otros sistemas IDS, así como ampliar este estudio a otras fases de un ejercicio de pentesting.

11. Bilbliografía

[1] Number of internet and social media users worldwide as of January 2023 [Internet] [fecha de consulta:14/03/2023]. Disponible en: https://www.statista.com/statistics/617136/digitalpopulationworldwide/
1.

[2] Cisco Cybersecurity Report Series 2020 CISO Benchmark Study Securing What's Now and What's Next 20 Cybersecurity Considerations for 2020 [Internet].2020. [fecha de consulta:
14/03/2023]. Disponible en: https://www.cisco.com/c/dam/m/en_hk/ciscolive/2020cisobenchmark-cybersecurity-series.pdf

[3] Security P. Pentesting: una herramienta muy valiosa para tu empresa [Internet]. Panda Security Mediacenter. 2018 [citado 11 de abril de 2023]. Disponible en: https://www.pandasecurity.com/es/mediacenter/seguridad/pentesting-herramientaempresa/

[4] Catalunya UO de. Las webs rastrean a los usuarios incumpliendo la privacidad [Internet]. UOC (Universitat Oberta de Catalunya). [citado 11 de abril de 2023]. Disponible en: https://www.uoc.edu/portal/es/news/actualitat/2023/057-cookies-beacons.html

[5] Guía de ciberataques. Disponible en: https://www.osi.es/sites/default/files/docs/guiaciberataques/osi-guia-ciberataques.pdf

[6] Medidas para minimizar el seguimiento en internet. Agencia Española de Protección de Datos. 2020 [citado 18 de Mayo de 2023]. Disponible en: https://www.aepd.es/sites/default/files/2020-09/nota-tecnica-evitar-seguimiento.pdf

[7] Frank La Rue. Refworld | Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, [Internet]. United Nations; 2013 [citado 18 de mayo de 2023]. Disponible en: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17sessio n/A.HRC.17.27_en.pdf

[8] Gonzalo, Marilín. Casi uno de cada tres países ha censurado redes sociales desde 2015 [Internet]. Newtral. 2022 [citado 11 de abril de 2023]. Disponible en: https://www.newtral.es/censuraenredes-sociales-paises-facebook/20220126/

[9] de Salvador Carrasco, Luis. REDES DE ANONIMIZACIÓN EN INTERNET: CÓMO FUNCIONAN Y CUÁLES SON SUS LÍMITES. Instituto Español de Estudios Estratégicos. 2012; [internet]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO16-2012_RedesAnonimizacionInternet_LdeSalvador.pdf

[10] HAMZEH, K., PALL, G., VERTHEIN, W., TAARUD, J., LITTLE, W. and ZORN, G. Point-topoint tunneling protocol (PPTP). USA: RFC Editor. 1999. DOI 10.17487/rfc2637.

[11] Historia [en línea] [fecha de consulta:14/03/2023]. Disponible en: https://www.torproject.org/es/about/history/

[12] MONTOYA ECHEVERRI, Daniel. Deep web: Tor, freenet & i2p:
Privacidad Y Anonimato. Móstoles, Madrid: Zeroxword Computing S.L, 2016. ISBN 9788460846284.

[13] GUNAWARDANA, Kushantha. Ethical guide to cyber anonymity: Concepts, tools,and techniques to be anonymous from criminals,...
unethical hackers, and governments. Birmingham: Packt publishing limited, 2022. ISBN 9781801810210.

[14] KUMAR VELU, Vijay. Mastering Kali Linux for advanced penetration testing. Become a cybersecurity ethical hacking expert using Metasploit, Nmap, Wireshark, and Burp Suite. Fourth Edition . Birmingham: PACKT Publishing, 2022. ISBN 9781801819770.

[15] SHAH, Mujahid, AHMED, Sheeraz, SAEED, Khalid, JUNAID, Muhammad, KHAN, Hamayun and ATA-UR-REHMAN. Penetration testing active reconnaissance phase – optimized port scanning with Nmap Tool. 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). 2019. DOI 10.1109/icomet.2019.8673520.

[16] Internet shutdown news and report: a year in the fight to #KeepItOn [Internet]. [citado 11 de abril de 2023]. Disponible en: https://www.accessnow.org/keepiton-report-a-year-in-thefight/

[17] Rubio, Isabel. ¿Qué navegador consume menos y cuál asegura mejor mi privacidad? [Internet]. El
País. 2020 [citado 11 de abril de 2023]. Disponible en: https://elpais.com/tecnologia/20200716/que-navegador-consume-menos-y-cual-asegura-mejor-mi-privacidad.html

[18] The hidden environmental costs of VPN gateways | Security Magazine [Internet]. [citado 11 de abril de 2023]. Disponible en: https://www.securitymagazine.com/articles/98381-thehiddenenvironmental-costs-of-vpn-gateways

[19] Internet UE. El 20% de los adolescentes utiliza internet para amenazar a conocidos
[Internet]. [citado 11 de abril de 2023]. Disponible en:
https://www.elmundo.es/elmundo/2013/01/10/espana/1357840097.html

[20] Objetivos de Desarrollo Sostenible | Programa De Las Naciones Unidas Para El Desarrollo [Internet]. UNDP. [citado 10 de mayo de 2023]. Disponible en: https://www.undp.org/es/sustainable-development-goals

[21] HTTP cookies - HTTP | MDN [Internet]. 2022 [citado 11 de abril de 2023]. Disponible en: https://developer.mozilla.org/es/docs/Web/HTTP/Cookies

[22] BOE.es - DOUE-L-2016-80807 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). [Internet]. [citado 11 de abril de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-201680807

[23] Gia sobre el uso de las cookies. [Internet]. 2022. Disponible en: https://www.aepd.es/es/documento/guia-cookies.pdf

[24] Super cookies y cookies zombie [Internet]. Proteccion de datos. 2022 [citado 11 de abril de 2023]. Disponible en: https://www.protecciondatos.org/super-cookies-y-cookies-zombie/

[25] Lott, Joey., Schall, Darron and Peters, Keith. Actionscript 3.0 Cookbook, O'Reilly, 2006, p. 410.

[26] Kamkar, Samy. Evercookie [Internet]. 2023 [citado 12 de abril de 2023]. Disponible en: https://github.com/samyk/evercookie

[27] ¿Qué es un navegador web? [Internet]. Mozilla. [citado 10 de mayo de 2023]. Disponible en: https://www.mozilla.org/es-ES/firefox/browsers/what-is-a-browser/

[28] Historia del proyecto Mozilla [Internet]. Mozilla. [citado 10 de mayo de 2023]. Disponible en: https://www.mozilla.org/es-ES/about/history/

[29] Disconnect [Internet]. [citado 11 de abril de 2023]. Disponible en: https://disconnect.me/trackerprotection

[30] Introducing Total Cookie Protection in Standard Mode | Ayuda de Firefox [Internet]. [citado 9 de junio de 2023]. Disponible en: https://support.mozilla.org/es/kb/introducing-total-cookie-protection-standard-mode?as=u&utm_source=inproduct

[31] Cómo protegerse del «Phishing» y del «Malware» con esta herramienta de Firefox | Ayuda de Firefox [Internet]. [citado 11 de abril de 2023]. Disponible en:

https://support.mozilla.org/es/kb/como-protegerse-del-phishing-y-del-malware-con-estaherramienta-firefox?as=u&utm_source=inproduct

[32] Introducción a SSL con ejemplo de transacción y intercambio de paquetes - Cisco [Internet]. [citado 11 de abril de 2023]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/security-vpn/secure-socket-layer-ssl/116181technote-product-00.html

[33] Funciones de seguridad y protección de la privacidad [Internet]. Brave Browser. [citado 11 de abril de 2023]. Disponible en: https://brave.com/es/privacy-features/

[34] A Quarter of Phishing Attacks are Now Hosted on HTTPS Domains: Why? | PhishLabs [Internet]. [citado 11 de abril de 2023]. Disponible en: https://www.phishlabs.com/blog/quarter-phishing-attacks-hosted-https-domains/

[35] Kaminsky, Stan. Cómo configurar el DNS seguro y el DNS privado [Internet]. 2023 [citado 9 de junio de 2023]. Disponible en: https://www.kaspersky.es/blog/secure-dns-private-dns-benefits/28454/

[36] ¿Hay algún motor de búsqueda que no te rastree? [Internet]. Brave Browser. 2022 [citado 11 de abril de 2023]. Disponible en: https://brave.com/es/learn/no-tracking-search-engine/

[37] ¿Por qué se ha desarrollado el Navegador Tor a partir de Firefox y no de otro navegador? | Tor Project | Ayuda [Internet]. [citado 11 de abril de 2023]. Disponible en: https://support.torproject.org/es/tbb/tbb-4/

[38] ABOUT TOR BROWSER | Tor Project | Tor Browser Manual [Internet]. [citado 11 de abril de 2023]. Disponible en: https://tb-manual.torproject.org/about/

[39] Cover Your Tracks [Internet]. [citado 10 de mayo de 2023]. Disponible en: https://coveryourtracks.eff.org/

[40] The Tor Project | Privacy & Freedom Online [Internet]. [citado 9 de junio de 2023]. Disponible en: https://torproject.org

[41] AdBlock Tester: test your AdBlock extensions [Internet]. [citado 10 de mayo de 2023]. Disponible en: https://adblock-tester.com/

[42] Conoce los tipos de VPN y sus protocolos [Internet]. [citado 10 de junio de 2023]. Disponible en: https://www.kio.tech/blog/data-center/tipos-de-vpn-y-sus-protocolos

[43] En qué consisten los servidores proxy inversos [Internet]. Cloudflare. [citado 11 de abril de 2023]. Disponible en: https://www.cloudflare.com/es-es/learning/cdn/glossary/reverse-proxy/

[44] HTTP headers - HTTP | MDN [Internet]. 2022 [citado 11 de abril de 2023]. Disponible en:
https://developer.mozilla.org/es/docs/Web/HTTP/Headers

[45] ¿Qué es un servidor proxy? | Definición de proxy | Avast [Internet]. [citado 11 de abril de 2023]. Disponible en: https://www.avast.com/es-es/c-what-is-a-proxy-server

[46] Rodríguez, Andrés. ¿Qué es un servidor proxy y cómo funcionan en Internet? [Internet]. Blog. 2020 [citado 11 de abril de 2023]. Disponible en: https://es.godaddy.com/blog/que-esunservidor-proxy-y-como-funcionan-en-internet/

[47] 33.Servers – Tor Metrics [Internet]. [citado 11 de abril de 2023]. Disponible en: https://metrics.torproject.org/networksize.html?start=2014-09-28&end=2023-04-01

[48] Users – Tor Metrics [Internet]. [citado 11 de abril de 2023]. Disponible en: https://metrics.torproject.org/userstats-relay-country.html

[49] Censorship | Tor Project | Support [Internet]. [citado 13 de junio de 2023]. Disponible en: https://support.torproject.org/censorship/

[50] Dunna, Arun. O'Brien, Ciaran and Gill, Phillipa. Analyzing China's Blocking of Unpublished Tor Bridges. University of Massachusetts Amherst. Disponible en: https://www.usenix.org/system/files/conference/foci18/foci18-paperdunna.pdf

[51] torspec - Tor's protocol specifications [Internet]. [citado 11 de abril de 2023]. Disponible en:
https://gitweb.torproject.org/torspec.git?a=blob%20plain;hb=HEAD;f=path-spec.txt

[52] Dingledine, Roger., Mathewson Nick., Syverson Paul. Tor: The Second-Generation Onion Router: [Internet]. Fort Belvoir, VA: Defense Technical Information Center; 2004 ene [citado 12 de abril de 2023]. Disponible en: http://www.dtic.mil/docs/citations/ADA465464

[53] ProxyChains - README (HowTo) TCP and DNS through proxy server. HTTP and SOCKS [Internet]. [citado 11 de abril de 2023]. Disponible en: https://proxychains.sourceforge.net/howto.html

[54] Amenaza Vs Vulnerabilidad Sabes Se Diferencian | Empresas | INCIBE [Internet]. [citado 18 de mayo de 2023]. Disponible en: https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[55] Agencia Española de Protección de Datos. [Internet]. [citado 10 de mayo de 2023]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf

[56] Tolley, William J. oss-sec: [CVE-2019-14899] Inferring and hijacking VPN-tunneled TCP connections. [Internet]. [citado 11 de abril de 2023]. Disponible en: https://seclists.org/osssec/2019/q4/122

[57] Jiménez, Javier. Cómo saltar el proxy y salir directamente a Internet [Internet]. 2023. RedesZone. [citado 13 de junio de 2023]. Disponible en: https://www.redeszone.net/tutoriales/redes-cable/evitar-proxy-internet/

[58] 4 Vulnerabilities Of A Proxy Server | IT Briefcase [Internet]. [citado 10 de junio de 2023]. Disponible en: https://www.itbriefcase.net/4-vulnerabilities-of-a-proxy-server

[59] «One cell is enough to break Tor's anonymity» | Tor Project [Internet]. [citado 11 de abril de 2023]. Disponible en: https://blog.torproject.org/one-cell-enough-break-tors-anonymity/

[60] Tails [Internet]. [citado 12 de abril de 2023]. Disponible en: https://tails.boum.org/index.es.html

[61] Whonix ™ - Overview [Internet]. Whonix. 2023 [citado 10 de junio de 2023]. Disponible en: https://www.whonix.org/wiki/About

[62] Introduction [Internet]. Qubes OS. [citado 12 de abril de 2023]. Disponible en: https://www.qubes-os.org/intro/

[63] DNS Dinámico Gratis - DNS Administrado - Managed Email - Registración de Dominio - No-IP [Internet]. [citado 3 de junio de 2023]. Disponible en: https://www.noip.com/es-MX

[64] Proton VPN: Secure and Free VPN service for protecting your privacy [Internet]. Proton VPN. [citado 2 de junio de 2023]. Disponible en: https://protonvpn.com/

[65] Gómez, Pablo. ¿Qué es un Sistema de Detención de Intrusiones? [Internet]. ICM. 2021 [citado 18 de mayo de 2023]. Disponible en: https://www.icm.es/2021/06/07/ids-intrusiones/

[66] Conrad, Eric., Misenar, Seth., Feldman, Joshua. Chapter 3 - Domain 2: Telecommunications and Network Security. En: Conrad E, Misenar S, Feldman J, editores. CISSP Study Guide (Second Edition) [Internet]. Boston: Syngress; 2012 [citado 10 de junio de 2023]. p. 63-141. Disponible en: https://www.sciencedirect.com/science/article/pii/B9781597499613000030

[67] TCP SYN (Stealth) Scan (-sS) | Nmap Network Scanning [Internet]. [citado 10 de mayo de 2023].
Disponible en: https://nmap.org/book/synscan.html

[68] TCP Idle Scan (-sI) | Nmap Network Scanning [Internet]. [citado 10 de mayo de 2023].
Disponible en: https://nmap.org/book/idlescan.html

[69] Fountain, Thomas. Introduction to Computer Consulting. 1999.

[70] Snort - Network Intrusion Detection & Prevention System [Internet]. [citado 10 de mayo de
2023]. Disponible en: https://www.snort.org/

[71] Oracle VM VirtualBox [Internet]. [citado 10 de mayo de 2023]. Disponible en: https://www.virtualbox.org/

[72] Hping3 [Internet]. [citado 2 de junio de 2023]. Disponible en: https://kali-linux.net/article/hping3/

[73] How to Code Your Own Port Scanner Using BASH Script and netcat Tool in Linux? [Internet]. GeeksforGeeks. 2021 [citado 7 de junio de 2023]. Disponible en: https://www.geeksforgeeks.org/how-to-code-your-own-port-scanner-using-bash-script-and-netcat-tool-in-linux/

[74] Sahu, Ankit. Install snort on Kali [Internet]. DEV Community. 2022 [citado 4 de junio de 2023]. Disponible en: https://dev.to/ankitsahu/install-snort-on-kali-1co8

12. Glosario

- Pentesting: Prueba de penetración.

- Máquina virtual: Ordenador virtual.

- Phishing: Técnica de suplantación de identidad utilizada por ciberdelincuentes.

- Malware: Programa maligno.

-**Cross Site Scripting:** Ataque informático mediante scripts maliciosos.

- **Hombre del medio:** Técnica utilizada para capturar los datos entre una red y un dispositivo.

- Firewall: Sistema de seguridad utilizado para filtrar el tráfico de red.

- MAC: Dirección física de un dispositivo.

- PPTP: Protocolo de tunelización punto a punto.

- IPSec: Protocolo de seguridad de Internet.

- L2TP: Protocolo de tunelización de capa 2.

- RRSS: Redes sociales.

- PHP: Preprocesador de hipertexto.

- NAT: Traducción de direcciones de red.

- API: Interfaz de programación de aplicaciones.

13. Anexos

13.1. Anexo 1: Hping3

Hping3 es una herramienta de Linux que permite analizar y ensamblar paquetes TCP/IP. A diferencia del ping tradicional que solo permite el envío de paquetes ICMP, hping3 también permite el envío de paquetes TCP, UDP y RAW-IP [72].

Escaneo SYN con hping3

Hping también puede ser utilizada como escáner de puertos TCP siguiendo la siguiente sintaxis:

hping3 -S <dirección IP> -p <número de puerto>

Para escanear varios puertos concretos, deberemos separarlos por comas de la siguiente forma:

hping3 -S <dirección IP> -p <puerto1, puerto2, puerto3…>

En caso de querer escanear un rango de puertos indicaremos el puerto inicial y el puerto final separados por una línea media.

hping3 -S <dirección IP> -p <puerto1-puerto10>

Al utilizar los comandos anteriores se produce un escaneo SYN, en el que se envía un paquete TCP SYN desde el cliente a la máquina objetivo, que puede obtener las siguientes respuestas:

Si la respuesta es SYN/ACK, el valor del flag será SA y el puerto escaneado se encontrará abierto. En caso de recibir RST/ACK el valor del flag será RA y el puerto se econtrará cerrado o filtrado.

13.2. Anexo 2: Bash script con Netcat

Netcat es una herramienta de red que puede ser utilizada como escaner de puertos entre otras funciones. Se presenta un script sencillo para llevar a cabo el escaneo de puertos TCP.

Código del script (basado en [73]):

```
#!/bin/bash
ip="$1"
echo "Introduce el puerto inicial: "
read -r start_port
echo "Introduce el puerto final: "
read -r end_port

echo "Se están escaneando los puertos en $ip"

nc -nvvzr "$ip" "$start_port-$end_port" > "ip.txt" 2>&1

echo "puertos abiertos:"
grep -E "open" "ip.txt" | awk '{print $2,$3}'
```

Explicación del código

- ip="$1": Asigna el primer argumento pasado al script a la variable ip.
- read -r start_port: asigna el argumento pasado al script al puerto inicial.
- read -r end_port: asigna el argumento pasado al script al puerto final.

- nc: Ejecuta netcat.
- nvvzr:
- n: Solo Utiliza direcciones IP. Desactiva la resolución de DNS.
- vv: Incrementa el nivel de verbosidad.
- z: Escaneo de puertos en modo de escucha.
- r: Utiliza números de puerto aleatorios

- $ip: Variable que contiene la dirección IP del host objetivo.
- $puerto_inicial-$puerto_final: variables que contienen el puerto inicial y final a analizar.
- > "ip.txt": Envía la salida del comando nc hacia el fichero "ip.txt".
- 2>&1: Permite que los mensajes de error se guarden en el fichero"ip.txt".

- grep -E "open" "$ip.txt": Busca la palabra “open” en el fichero “ip.txt”
- awk '{print $2,$3}': muestra la segunda y tercera columna de las líneas que contienen la palabra "open".

Ejecución del bash script

Para ejecutar el escaner se deben de llevar a cabo los siguientes pasos:

1. copiar el código indicado en un fichero con extensión “sh”. Por ejemplo “escaner.sh”

2. Otorgar permisos al fichero con el comando “sudo chmod +x escaner.sh”

3. Ejecutar el script con el siguiente comando: ./escaner.sh [Dirección IP objetivo]

Posteriormente el programa pedirá los puertos inicial y final que deberemos de introducir para iniciar el escaneo. Al finalizar, muestra aquellos puertos que se encuentran abiertos.

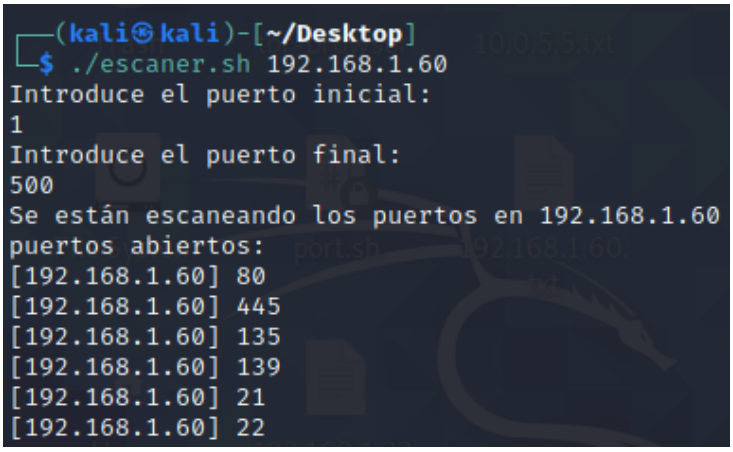

Figura 39: Escaner de puertos netcat

13.3. Anexo 3: Instalación de aplicaciones

Se explica cómo realizar la instalación de algunas de las aplicaciones comentadas en el trabajo en la distribución Linux Ubuntu.

Como procedimiento estándar, antes de realizar cualquiera de estas instalaciones, se deberán actualizar los paquetes del sistema, introduciendo “sudo apt-get update” en la consola de comandos.

Instalación de Proxychains

Para descargar e instalar ProxyChains, escribiremos “apt-get install proxychains4” en la consola de comandos.

Instalación de Tor

Para descargar e instalar Tor, introduciremos “sudo apt-get install tor” en la consola de comandos. Una vez terminada la instalación, necesitaremos iniciar el servicio mediante el comando “sudo service tor start”. Para comprobar que el servicio se encuentra activo, escribiremos, “sudo service tor status”.

Instalación del Script Ipidsec de Nmap

Puede descargar se en la página: https://nmap.org/nsedoc/scripts/ipidseq.html

Una vez descagado, debe introducirse el fichero ipidseq.nse dentro de la carpeta scripts de nmap.

Instalación de Snort 2.9.7.0 GRE

Se realiza la instalación mediante la guía de instalación sugerida para Ubuntu por el usuario Ankit Sahu en dev community [74].

El fichero de configuración, snort.conf se encuentra por defecto en la carpeta: /etc/snort/

Instalación de Apache2

Para realizar la instalación escribiremos “sudo apt-get install apache2”.
Para iniciar el servicio Apache2 se introduce el siguiente comando:
sudo service apache2 start
Para comprobar el estado de Apache2 se introduce el siguiente comando:
sudo service apache2 status

El fichero index.html de la página web se encuentra por defecto en la dirección: /var/www/html.
El fichero de registro de accesos “access.log” se encuentra por defecto en la carpeta /var/Apache2/logs/.