



# JUPITER

# LABS

## Informe de ejecutivo de Red Team

KeepCoding

Profesor: Pablo Ambite

Realizado por: Mónica Durán Alfonso

Email: [monicadual1915@gmail.com](mailto:monicadual1915@gmail.com)

Linkedin: Mónica Durán

Noviembre 2024

# TABLA DE CONTENIDOS

1.Introducción

2.Investigación de los activos

2.1.Nombres y empresas incluidas en la matriz

2.2.Sistemas Autónomos (AS)

2.3.Rangos de Red.

2.4.Dominios y subdominios

3.Planificación del ataque

4.Laboratorio

4.1 Active Directory.

4.2Comand & Control.

5.Resumen final

# 1.Introducción

**KAYAK** es un agregador de tarifas y metabuscador de viajes en línea. El sitio web de KAYAK y sus aplicaciones móviles permiten a sus usuarios comparar y reservar vuelos, hoteles, coches de alquiler y paquetes de vacaciones en cientos de proveedores a la vez.

Desde el 2013 es parte de Booking Holding, líder mundial en la industria de viajes online.



Imagen.1 Empresas adheridas a Booking Holdings Inc.

www.kayak.com

including localised versions:  
e.g. [www.kayak.de](http://www.kayak.de),  
[www.kayak.fr](http://www.kayak.fr) and  
[www.kayak.co.uk](http://www.kayak.co.uk), etc. Please  
check  
<https://www.kayak.com/global>  
for full list of domains that  
belong to us.

| Domain | In scope | Critical | Eligible | Jan 24, 2023 | 182 (39%) |
|--------|----------|----------|----------|--------------|-----------|
|--------|----------|----------|----------|--------------|-----------|

Imagen.2 Dominio principal de la cía.

Para la realización de la práctica se ha escogido el dominio principal del Scope de HackerOne, ya que es el dominio principal de la compañía y permite un reconocimiento amplio ([www.kayak.com](http://www.kayak.com)).

## 2. Información de los activos

### 2.1. Nombres y empresas incluidas en la matriz

En este caso vamos a realizar una recopilación de información del objetivo utilizando técnicas pasivas ya que así no dejamos evidencias de que estamos vigilando su sistema.

Para ello, accedemos a la página oficial de Kayak para ver que empresas tiene asociadas a dicho dominio, encontramos:

#### Subsidiarias de Kayak

Kayak gestiona varias marcas internacionales, incluyendo:

- **SWOODOO**
- **Checkfelix**
- **Momondo**
- **Cheapflights**
- **Mundi**
- **HotelsCombined**

Estas marcas forman parte del grupo Kayak y ofrecen servicios similares de comparación de precios y búsqueda de viajes.

Del mismo modo, en HackerOne, obtenemos los demás dominios de la empresa objetivo.

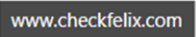






|   |        |          |          |          |                    |
|---|--------|----------|----------|----------|--------------------|
| <a href="#">www.checkfelix.com</a><br>   | Domain | In scope | Critical | Eligible | 24,<br>2023        |
| <a href="#">www.hotelscombined.com</a><br>including local versions: e.g.<br><a href="#">www.hotelscombined.com.au</a> ,<br><a href="#">www.hotelscombined.co.kr</a> ,<br>etc. Please check<br><a href="https://www.kayak.com/global">https://www.kayak.com/global</a><br>for full list of domains that<br>belong to us. | Domain | In scope | Critical | Eligible | Jan<br>24,<br>2023 |

Imagen.3 Dominios dentro de la empresa objetivo.

|   |        |          |  |  |                    |
|---|--------|----------|--|--|--------------------|
| <b>www.momondo.com</b><br>including localised versions:<br>e.g. <a href="http://www.momondo.dk">www.momondo.dk</a> ,<br><a href="http://www.momondo.se">www.momondo.se</a> , etc. | Domain | In scope |  Critical |  Eligible | Jan<br>24,<br>2023 |
| <b>www.mundi.com.br</b>   | Domain | In scope |  Critical |  Eligible | Jan<br>24,<br>2023 |
| <b>www.swoodoo.com</b>  | Domain | In scope |  Critical |  Eligible | Jan<br>24,<br>2023 |

*Imagen.4 Dominios dentro de la empresa objetivo.*

Al saber que nuestra empresa objetivo gestiona otras empresas podemos conseguir:

- 1.Tener una mayor amplitud de la superficie de ataque.
- 2.Mayor número de dominios, subdominios, rangos de IP, etc...lo que nos proporciona una visión más completa de la infraestructura de la empresa.
- 3.Estas empresas pueden tener diferentes niveles de seguridad y protección.
- 4.Mayor rango frente a ataques de ingeniería social para poder llegar a la empresa matriz.
- 5.Vectores de ataques diferentes ya que cada empresa puede disponer de proveedores de servicios diferentes.
- 6.Si estas empresas están localizadas en otras zonas geográficas pueden tener regulaciones de leyes de privacidad diferentes entre sí.
- 7.Al conocer la estructura completa de la empresa podemos realizar simulaciones de ataque más realistas y completas.

## \*CRUNCHBASE

Es una plataforma que mediante las bases de datos comerciales nos proporcionan información detallada sobre empresas y sus relaciones comerciales.

Procedemos a realizar una búsqueda en su web de nuestra empresa objetivo y nos reporta información de gran utilidad como las adquisiciones que ha realizado, perfiles de los empleados más relevantes como el CEO, Presidente, Director General...

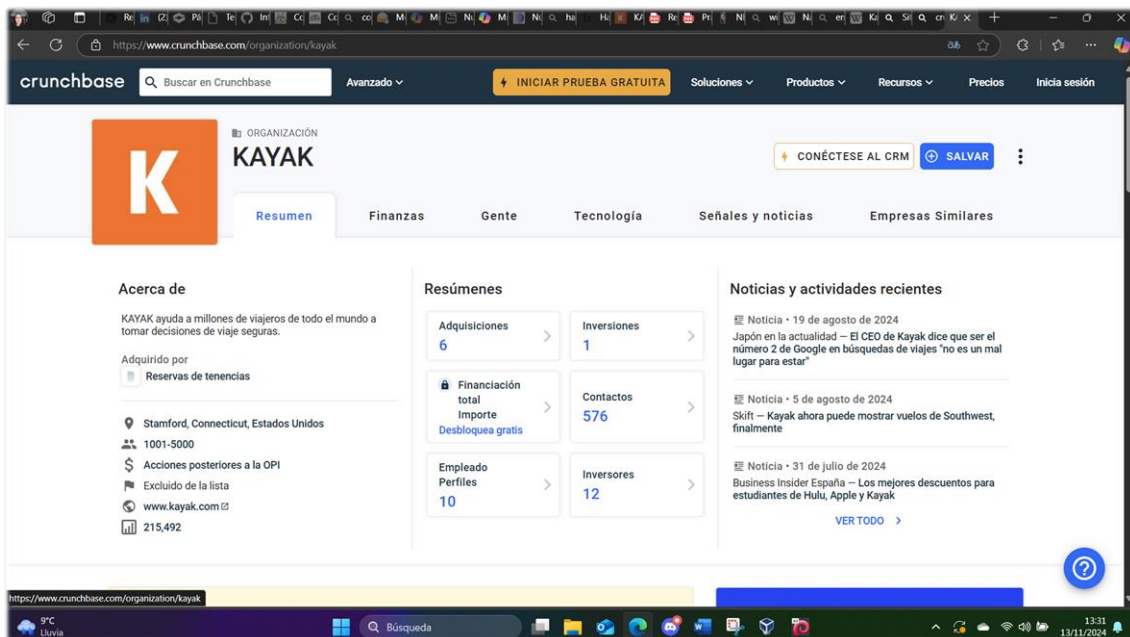


Imagen.5 Información de la empresa obtenida a través de la plataforma Crunchbase.

Adquisiciones

Número de Adquisiciones

6

KAYAK ha adquirido 6 Organizaciones. Su adquisición más reciente fue **HotelesCombinado** en 9 de julio de 2018.

 ¿Qué tipos de adquisiciones realiza esta organización con mayor frecuencia?

 MOSTRAR

| Nombre de la adquirida   | Fecha anunciada     | Precio                  | Nombre de la  |
|--|---------------------|-------------------------|---|
|  HotelesCombinado | 9 de julio de 2018  | —                       |  HotelsCombinado por KAYAK         |
|  Mundi            | 3 de agosto de 2017 | —                       |  Mundi es adquirida por KAYAK      |
|  Vuelos baratos   | Jul 24, 2017        | —                       |  Vuelos baratos por KAYAK          |
|  checkfelix       | Abr 6, 2011         | —                       |  checkfelix es adquirida por KAYAK |
|  Swoodoo        | 6 de mayo de 2010   | —                       |  Swoodoo es adquirida por KAYAK  |
|  Esquivar       | Dic 20, 2007        | 200 millones de dólares |  SideStep es adquirida por KAYAK |

Imagen.6 Adquisiciones de la empresa objetivo.

KAYAK tiene 10 Perfiles actuales de los empleados, incluidos los siguientes: CEO y cofundador Steve Hafner.

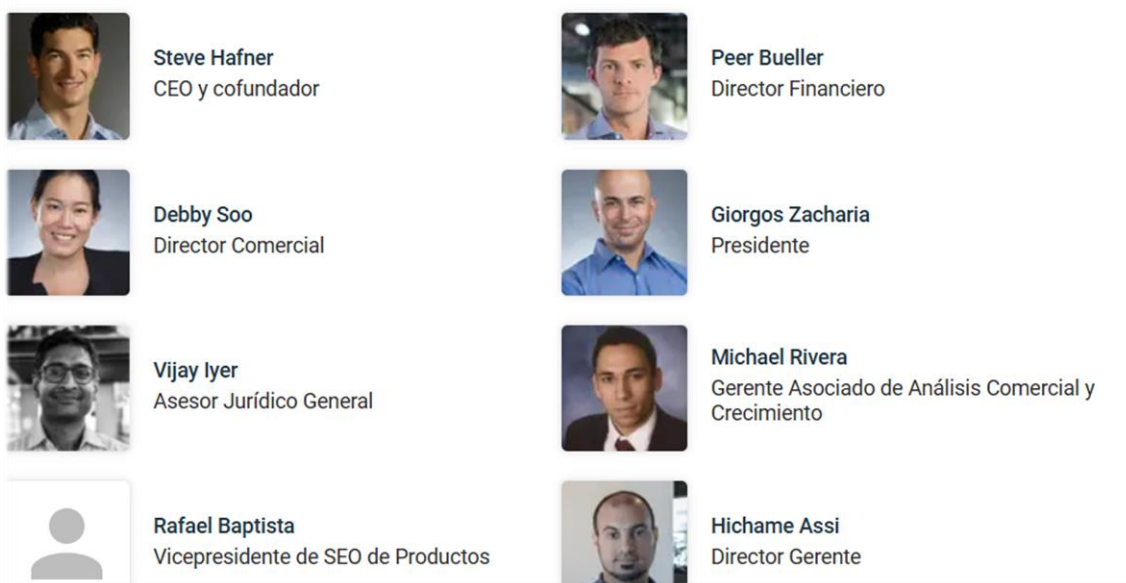


Imagen.7 Perfiles destacados de la empresa objetivo.

## 2.2. SISTEMAS AUTÓNOMOS (AS)

Un Sistema Autónomo (AS) es una colección de redes IP y routers bajo el control de una sola entidad, que presenta una política de enrutamiento común. Los sistemas autónomos son fundamentales para la arquitectura de Internet y se identifican por un número de Sistema Autónomo (ASN).

### \*HURRICANE ELECTRIC

Esta herramienta muestra inicialmente los sistemas autónomos registrados a nombre de la organización objetivo y, posteriormente, los rangos de red que componen dichos rangos.

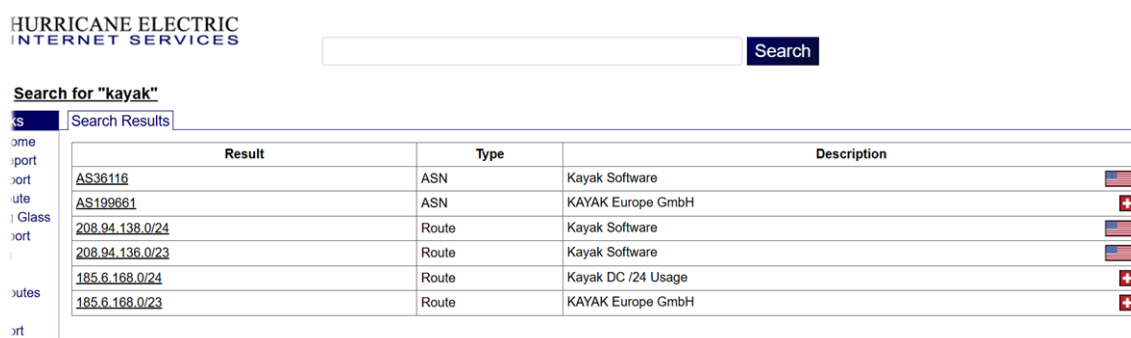


Imagen.8 Sistemas autónomos registrados a nombre de la empresa objetivo.



## \*AMASS

Es una herramienta que es especialmente útil en el ámbito de la seguridad cibernética para mapear la superficie de ataque de una página web.

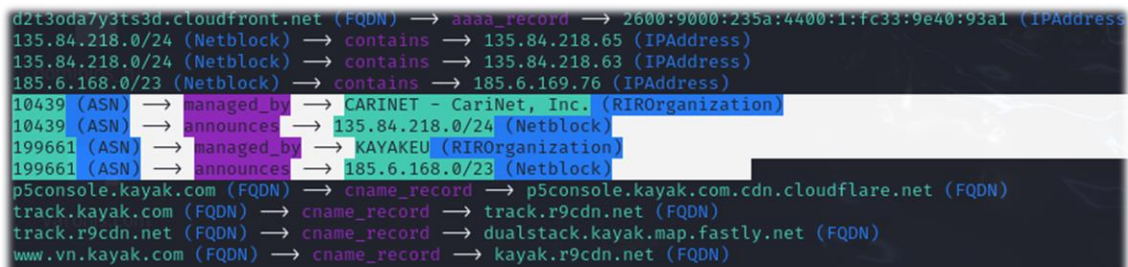
Su instalación en una VM es muy sencilla, solamente hay que descargarse la herramienta con el comando:

```
go install -v github.com/owasp-amass/amass/v4/...@master
```

y luego:

```
amass enum -d kayak.com
```

Esta herramienta nos genera también registros ASN



```
d2t36da/y3ts3d.cloudfront.net (FQDN) → aaaa_record → 2600:9000:235a:4400:1:fc33:9e40:93a1 (IPAddress)
135.84.218.0/24 (Netblock) → contains → 135.84.218.65 (IPAddress)
135.84.218.0/24 (Netblock) → contains → 135.84.218.63 (IPAddress)
185.6.168.0/23 (Netblock) → contains → 185.6.169.76 (IPAddress)
10439 (ASN) → managed_by → CARINET - CariNet, Inc. (RIROrganization)
10439 (ASN) → announces → 135.84.218.0/24 (Netblock)
199661 (ASN) → managed_by → KAYAKEU (RIROrganization)
199661 (ASN) → announces → 185.6.168.0/23 (Netblock)
p5console.kayak.com (FQDN) → cname_record → p5console.kayak.com.cdn.cloudflare.net (FQDN)
track.kayak.com (FQDN) → cname_record → track.r9cdn.net (FQDN)
track.r9cdn.net (FQDN) → cname_record → dualstack.kayak.map.fastly.net (FQDN)
www.vn.kayak.com (FQDN) → cname_record → kayak.r9cdn.net (FQDN)
```

Imagen.9 Otros registros de AS obtenidos de la herramienta WHOIS.

## \*ROBOTS.TXT

Es un mecanismo para que buscadores como Google o Bing no indexen ciertas páginas, se procede a poner Site: kayak.com -www en la barra de búsqueda y nos devuelve estos resultados de subdominios:

[KAYAK Affiliate Support & FAQ's](https://help.affiliates.kayak.com)

<https://help.affiliates.kayak.com>

KAYAK

<https://p4.kayak.com/flight-routes/Seattle-Tacoma-Intl-SEA/China-C...>

KAYAK

<https://p5.kayak.com/flight-routes/Florida-USFL/Hawaii-USHI>

## \*WHOIS

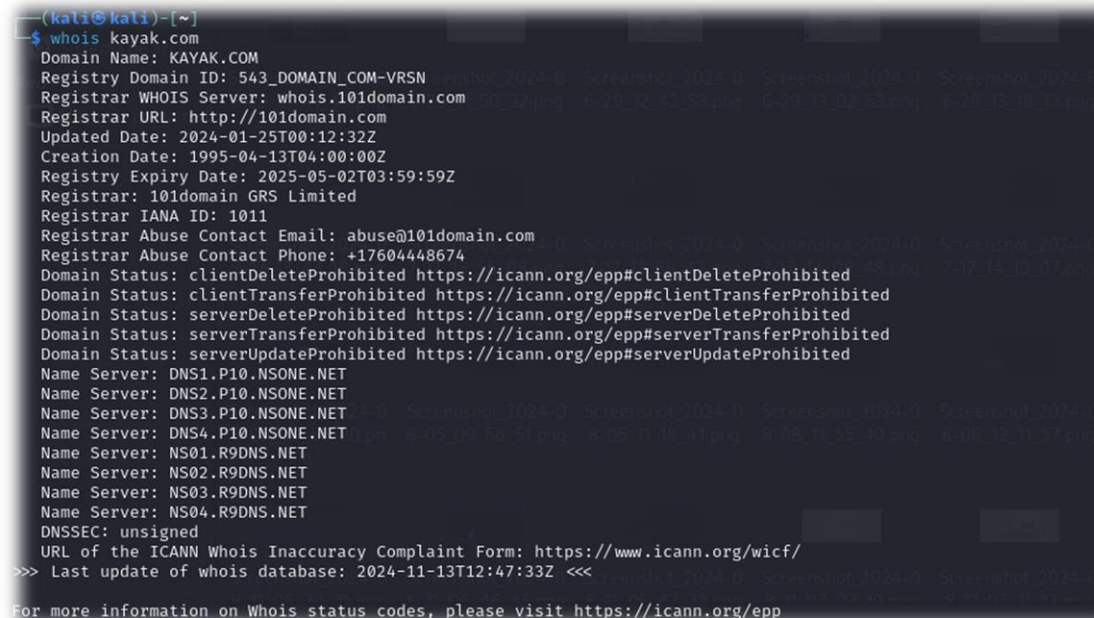
La herramienta whois es una utilidad de línea de comandos que te permite obtener información sobre la propiedad de un dominio, como detalles de registro, fechas de expiración y más.

Para poder hacer uso de ella indico como proceder a su descarga en una VM Debian/Kali o similar desde una terminal y su posterior uso:

```
sudo apt update & upgrade
```

```
sudo apt install whois
```

```
whois kayak.com
```



```
(kali@kali)-[~]
$ whois kayak.com
Domain Name: KAYAK.COM
Registry Domain ID: 543_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.101domain.com
Registrar URL: http://101domain.com
Updated Date: 2024-01-25T00:12:32Z
Creation Date: 1995-04-13T04:00:00Z
Registry Expiry Date: 2025-05-02T03:59:59Z
Registrar: 101domain GRS Limited
Registrar IANA ID: 1011
Registrar Abuse Contact Email: abuse@101domain.com
Registrar Abuse Contact Phone: +17604448674
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: DNS1.P10.NSONE.NET
Name Server: DNS2.P10.NSONE.NET
Name Server: DNS3.P10.NSONE.NET
Name Server: DNS4.P10.NSONE.NET
Name Server: NS01.R9DNS.NET
Name Server: NS02.R9DNS.NET
Name Server: NS03.R9DNS.NET
Name Server: NS04.R9DNS.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-11-13T12:47:33Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

*Imagen.10 Información obtenida a través de la herramienta WHOIS.*

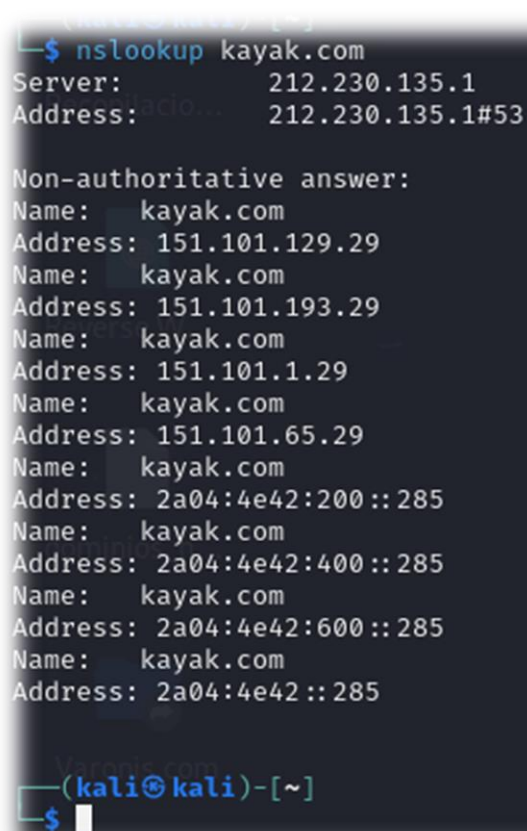
Con este comando obtenemos la siguiente información de nuestro dominio objetivo:

- + **Registrar:** La empresa que gestionó el registro del dominio.
- + **Registrante:** La persona u organización que registró el dominio.
- + **Fechas:** Fechas de creación y expiración del dominio.
- + **Servidores DNS:** Servidores de nombres asociados al dominio.
- + **Contacto técnico y administrativo:** Información de contacto.

## \*NSLOOKUP

Esta herramienta nos permite identificar registros DNS y servidores asociados, su uso es muy sencillo después de proceder a su instalación en la VM Debian procedemos a lanzar el comando.

Nslookup kayak.com



```
(kali㉿kali)-[~]  
└─$ nslookup kayak.com  
Server:      212.230.135.1  
Address:     212.230.135.1#53  
  
Non-authoritative answer:  
Name:   kayak.com  
Address: 151.101.129.29  
Name:   kayak.com  
Address: 151.101.193.29  
Name:   kayak.com  
Address: 151.101.1.29  
Name:   kayak.com  
Address: 151.101.65.29  
Name:   kayak.com  
Address: 2a04:4e42:200::285  
Name:   kayak.com  
Address: 2a04:4e42:400::285  
Name:   kayak.com  
Address: 2a04:4e42:600::285  
Name:   kayak.com  
Address: 2a04:4e42::285  
  
(kali㉿kali)-[~]  
└─$
```

Imagen.11 DNS obtenido a través de la herramienta NSLOOKUP.

## \*AMASS

Nos genera una recopilación de información detallada sobre los registros DNS y los subdominios de kayak.com. que procedemos a remarcar para su posterior investigación.

```
(kali@kali)-[~]
$ amass enum -d kayak.com -max-dns-queries 50
kayak.com (FQDN) → ns_record → ns01.r9dns.net (FQDN)
kayak.com (FQDN) → ns_record → ns02.r9dns.net (FQDN)
kayak.com (FQDN) → ns_record → ns03.r9dns.net (FQDN)
kayak.com (FQDN) → ns_record → ns04.r9dns.net (FQDN)
kayak.com (FQDN) → ns_record → dns1.p10.nsone.net (FQDN)
kayak.com (FQDN) → ns_record → dns2.p10.nsone.net (FQDN)
kayak.com (FQDN) → ns_record → dns3.p10.nsone.net (FQDN)
kayak.com (FQDN) → ns_record → dns4.p10.nsone.net (FQDN)
kayak.com (FQDN) → mx_record → mailstream-west.mxrecord.io (FQDN)
kayak.com (FQDN) → mx_record → mailstream-east.mxrecord.io (FQDN)
kayak.com (FQDN) → mx_record → mailstream-central.mxrecord.mx (FQDN)
cs.kayak.com (FQDN) → cname_record → kayak.r9cdn.net (FQDN)
blog.kayak.com (FQDN) → cname_record → kayak.com (FQDN)
mail.kayak.com (FQDN) → cname_record → ghs.google.com (FQDN)
ghs.google.com (FQDN) → a_record → 142.250.184.19 (IPAddress)
ghs.google.com (FQDN) → aaaa_record → 2a00:1450:4003:808::2013 (IPAddress)
manage.kayak.com (FQDN) → cname_record → brands.r9cdn.net (FQDN)
brands.r9cdn.net (FQDN) → cname_record → dualstack.kayak.map.fastly.net (FQDN)
message.kayak.com (FQDN) → cname_record → kayak.mail.e.sparkpost.com (FQDN)
www.za.kayak.com (FQDN) → cname_record → kayak.r9cdn.net (FQDN)
www.tw.kayak.com (FQDN) → cname_record → kayak.r9cdn.net (FQDN)
cashbackil.kayak.com (FQDN) → cname_record → 000004-whitelabel.property.datahc.com (FQDN)
000004-whitelabel.property.datahc.com (FQDN) → cname_record → hc-slotmatching.r9cdn.net (FQDN)
business=booking.kayak.com (FQDN) → cname_record → affiliates.r9cdn.net (FQDN)
www.il.kayak.com (FQDN) → cname_record → kayak.r9cdn.net (FQDN)
x.kayak.com (FQDN) → cname_record → x4.kayak.com (FQDN)
kiwi.kayak.com (FQDN) → cname_record → www.kiwi.com (FQDN)
www.kiwi.com (FQDN) → a_record → 104.17.91.189 (IPAddress)
www.kiwi.com (FQDN) → a_record → 104.17.92.189 (IPAddress)
kibana-geo-som.kayak.com (FQDN) → cname_record → kibana-geo-som.kayak.com.cdn.cloudflare.net (FQDN)
de.kayak.com (FQDN) → cname_record → kayak.r9cdn.net (FQDN)
www.nz.kayak.com (FQDN) → cname_record → kayak.r9cdn.net (FQDN)
p5console.kayak.com (FQDN) → cname_record → p5console.kayak.com.cdn.cloudflare.net (FQDN)
kibana-provider-som.kayak.com (FQDN) → cname_record → kibana-provider-som.kayak.com.cdn.cloudflare.net (FQDN)
booking.kayak.com (FQDN) → cname_record → brands.r9cdn.net (FQDN)
cz.kayak.com (FQDN) → cname_record → kayak.r9cdn.net (FQDN)
kibana-destiny-som.kayak.com (FQDN) → cname_record → kibana-destiny-som.kayak.com.cdn.cloudflare.net (FQDN)
kibana-geo-zrh.kayak.com (FQDN) → cname_record → kibana-geo-zrh.kayak.com.cdn.cloudflare.net (FQDN)
kibana-docker-som.kayak.com (FQDN) → cname_record → kibana-docker-som.kayak.com.cdn.cloudflare.net (FQDN)
api.travel.kayak.com (FQDN) → cname_record → api.travel.kayak.com.edgekey.net (FQDN)
backpackers.kayak.com (FQDN) → cname_record → affiliates.r9cdn.net (FQDN)
espanol.kayak.com (FQDN) → cname_record → kayak.r9cdn.net (FQDN)
agoda.kayak.com (FQDN) → cname_record → brands.r9cdn.net (FQDN)
optimise.kayak.com (FQDN) → cname_record → 000004-whitelabel.property.datahc.com (FQDN)
nomad.kayak.com (FQDN) → cname_record → brands.r9cdn.net (FQDN)
www.be.kayak.com (FQDN) → cname_record → kayak.r9cdn.net (FQDN)
www.ng.kayak.com (FQDN) → cname_record → kayak.r9cdn.net (FQDN)
```

Imagen.12 Registros DNS obtenido a través de la herramienta AMASS.

## \*WAPPALYZER

Es una extensión del navegador y una herramienta muy útil para entender mejor la infraestructura tecnológica de los sitios web.

Al utilizarla contra nuestra empresa objetivo podemos sacar información muy valiosa sobre las tecnologías con las que trabajan:

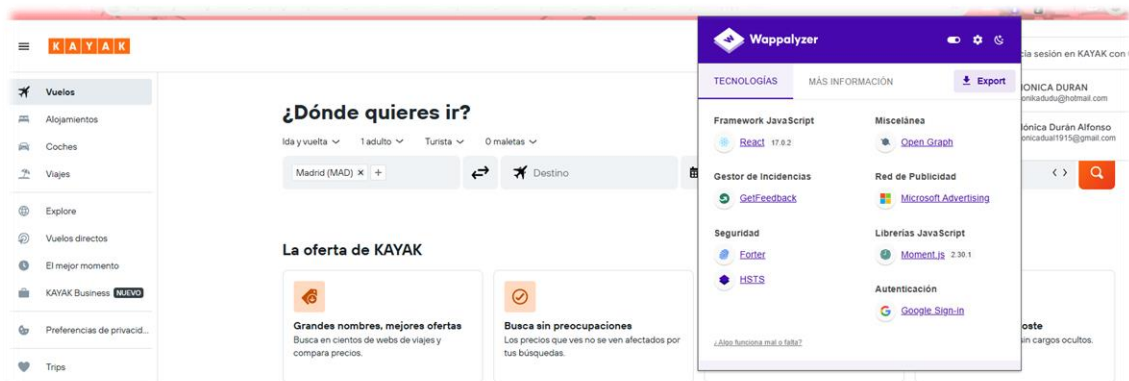


Imagen 13. Tecnologías utilizadas por KAYAK.COM y obtenidas a través de WAPPALYZER.

### React:

XSS (Cross-Site Scripting): Si no se valida y escapa correctamente la entrada del usuario, puede permitir la ejecución de scripts maliciosos.

Inyecciones: Vulnerabilidades como SQL Injection pueden ocurrir si se manipulan las consultas de manera incorrecta.

### GetFeedback:

Exposición de datos sensibles: Si no se implementan correctamente las medidas de seguridad, los datos recopilados pueden ser accesibles por atacantes.

Autenticación débil: Si la autenticación no se maneja adecuadamente, puede ser vulnerable a ataques de fuerza bruta o phishing.

### Forter:

Configuraciones incorrectas: Si no se configuran correctamente las políticas de seguridad, pueden existir brechas que los atacantes puedan explotar.

Actualizaciones de seguridad: Es crucial mantener el software y las soluciones de seguridad actualizadas para protegerse contra nuevas amenazas.

**HSTS (HTTP Strict Transport Security):**

Configuración incorrecta: Si no se implementa correctamente, puede permitir ataques de downgrade que redirijan a conexiones no seguras.

**Microsoft Advertising:**

Phishing: Los anuncios maliciosos pueden redirigir a sitios fraudulentos que intentan robar información personal.

Malware: Los anuncios pueden ser utilizados para distribuir software malicioso.

**Moment.js:**

Inyecciones de dependencias: Si se cargan versiones no verificadas o comprometidas de la librería, pueden existir vulnerabilidades.

Falla en la validación de entrada: Si no se valida correctamente la entrada de datos, puede ser vulnerable a ataques XSS.

**Google Sign-in:**

Phishing: Los atacantes pueden intentar engañar a los usuarios para que ingresen sus credenciales en sitios fraudulentos.

Autenticación débil: Si no se implementa correctamente, puede ser vulnerable a ataques de fuerza bruta o phishing.

## \*SHODAN

Es una herramienta valiosa para administradores de sistemas, investigadores de seguridad y auditores que necesitan obtener información detallada sobre dispositivos y servicios conectados a Internet.

En este caso, al visualizar los resultados se observa que nos reporta:

### Información General

- **Hostnames:** www.kayak.com
- **Dominios:** kayak.com
- **País:** Estados Unidos
- **Ciudad:** San José
- **Organización:** Fastly, Inc.
- **ISP:** Fastly, Inc.
- **ASN:** AS54113

### Puertos Abiertos

- **Puertos:** 80/tcp, 443/tcp
- **Errores:** Error de Fastly: dominio desconocido 151.101.41.29

El dominio 151.101.41.29 está devolviendo un error 500, lo que indica un problema con la resolución o configuración del dominio. Esto podría deberse a una mala configuración en el servicio de caché proporcionado por Fastly.

- **HTTP/1.1 500 Domain Not Found**
- Esto indica problemas con la resolución o configuración del dominio en los servidores de caché de Fastly.

### Certificado SSL

- **Emisor:** Let's Encrypt, CN=R10
- **Periodo de Validez:**
  - **Not Before:** 6 de noviembre de 2024
  - **Not After:** 4 de febrero de 2025
- **Sujeto:** CN=www.kayak.com
- **Algoritmo de Clave Pública:** RSA (2048 bit)



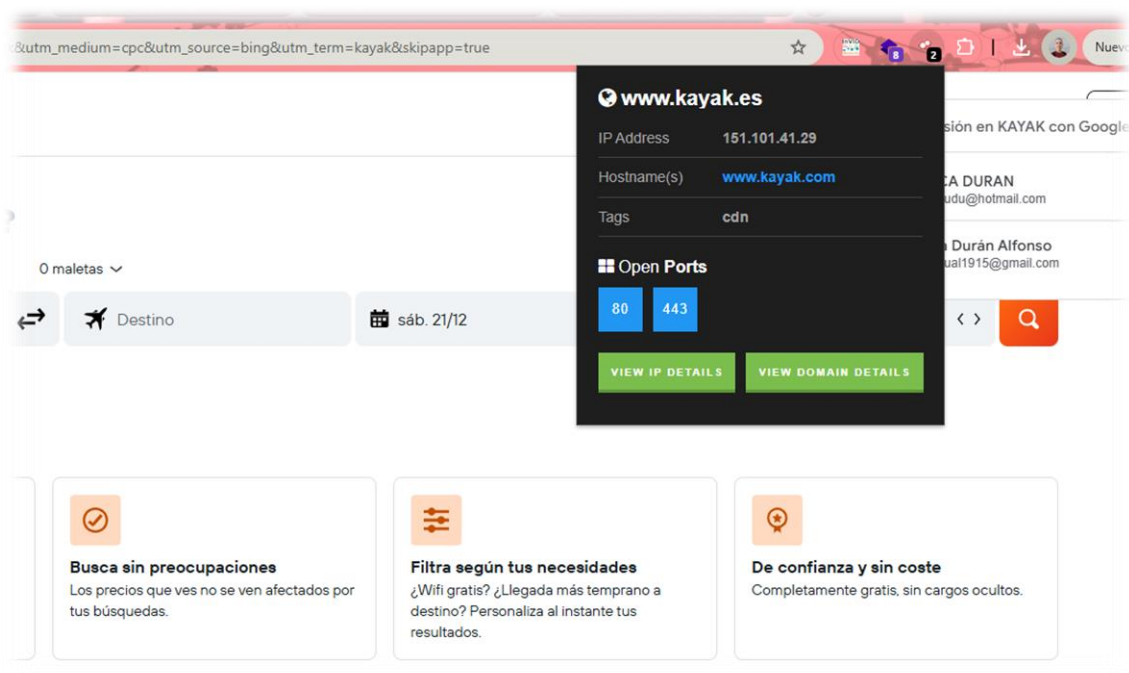


Imagen.14 Información de puertos abiertos de KAYAK.COM obtenida a través de la plataforma SHODAN.

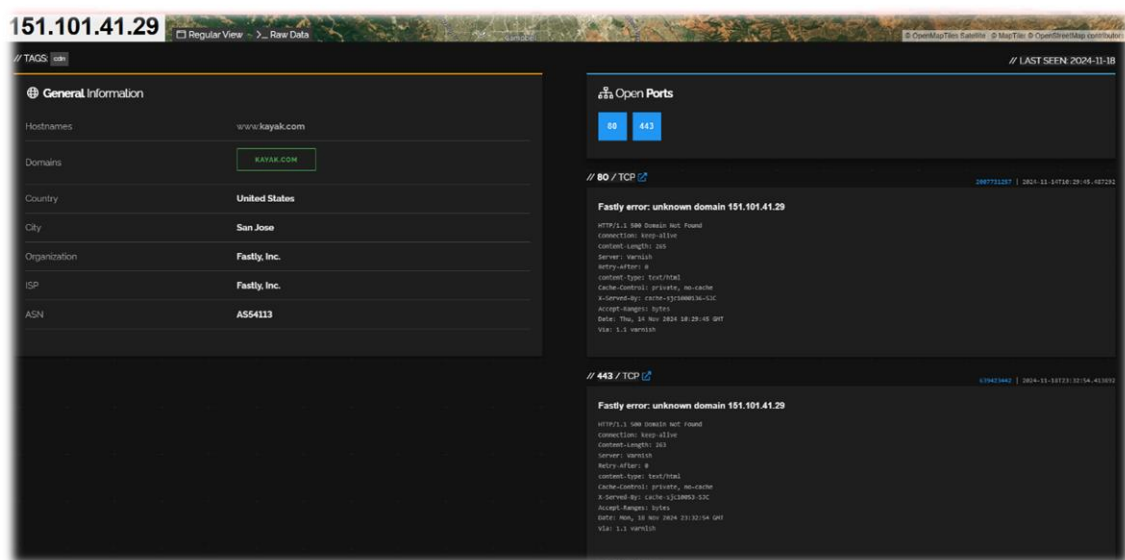


Imagen.15 Información de certificados SSL de KAYAK.COM



### 3. Planificación del ataque

Este ejercicio es puramente académico y no implica ningún intento real de intrusión, a continuación, se van a detallar los posibles pasos a seguir para conseguir entrada a través de un AC.

#### 1. Recopilación de Información Inicial

- Objetivo: Identificar los sistemas y servicios utilizados por KAYAK, especialmente aquellos relacionados con Active Directory.
- Para ellos se ha hecho uso de las diferentes herramientas de recopilación de información del objetivo que hemos detallado anteriormente.

#### 2. Enumeración de Servicios de Active Directory

- Objetivo: **Identificar servidores y servicios específicos de Active Directory que estén accesibles.**
- Herramientas:
  - Nmap: **Para escanear puertos comunes de Active Directory (80,443,389, 636, 3268, 3269).**

#### 3. Recolección de Información sobre el Active Directory

- Objetivo: Obtener información detallada del Active Directory, como nombres de dominio, controladores de dominio y otras configuraciones.
- Herramientas:
  - LDAP Enumeration: Utilizar herramientas para enumerar entradas LDAP si los puertos LDAP están abiertos.
  - BloodHound: Para visualizar la topología del Active Directory (teóricamente, no invasivamente).

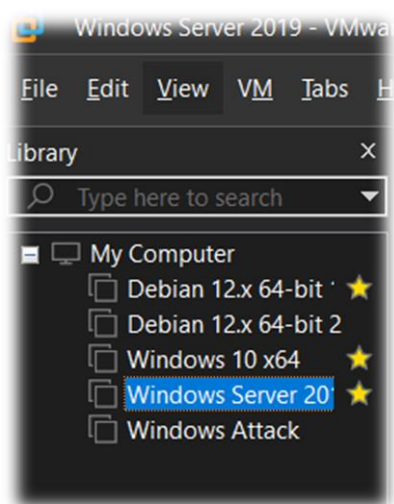
#### 4. Teorización del Vector de Entrada mediante Phishing

- Objetivo: Diseñar un escenario de phishing para obtener credenciales de acceso al Active Directory.
- Pasos:
  - Recopilación de Información sobre Empleados: Utilizar LinkedIn, redes sociales y otros recursos públicos para identificar empleados de KAYAK.
  - Diseño del Correo de Phishing: Crear un correo electrónico convincente que simule una comunicación legítima de la empresa, como una actualización de seguridad o un documento importante.

- Envío del Correo de Phishing: Teorizar el envío del correo a múltiples empleados para aumentar la probabilidad de que alguien caiga en el engaño.
- Captura de Credenciales: Suponer que un empleado ingresa sus credenciales en un sitio falso o formulario de phishing.

## 4.Laboratorio

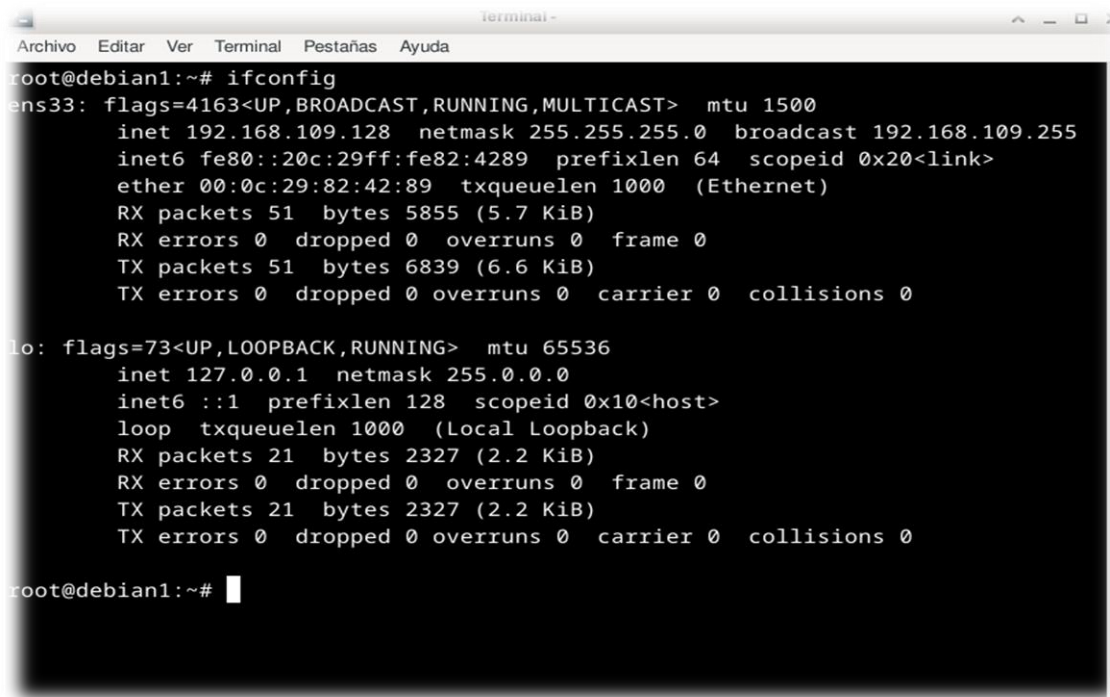
Procedemos a montar el laboratorio que en nuestro caso contara con los siguientes elementos:



*Imagen.16 Máquinas del laboratorio.*

- Máquina Linux (C&C) IP **192.168.109.128**
- Máquina Windows 10 (victima) IP **192.168.109.5**
- Máquina Windows Server 2019 (AD) IP **192.168.109.7**

Tanto en la VM Windows 10 como en la VM Win Server procedemos a cambiar las IPs dinámicas por IPs fijas en RED>PROPIEDADES>IP fija.

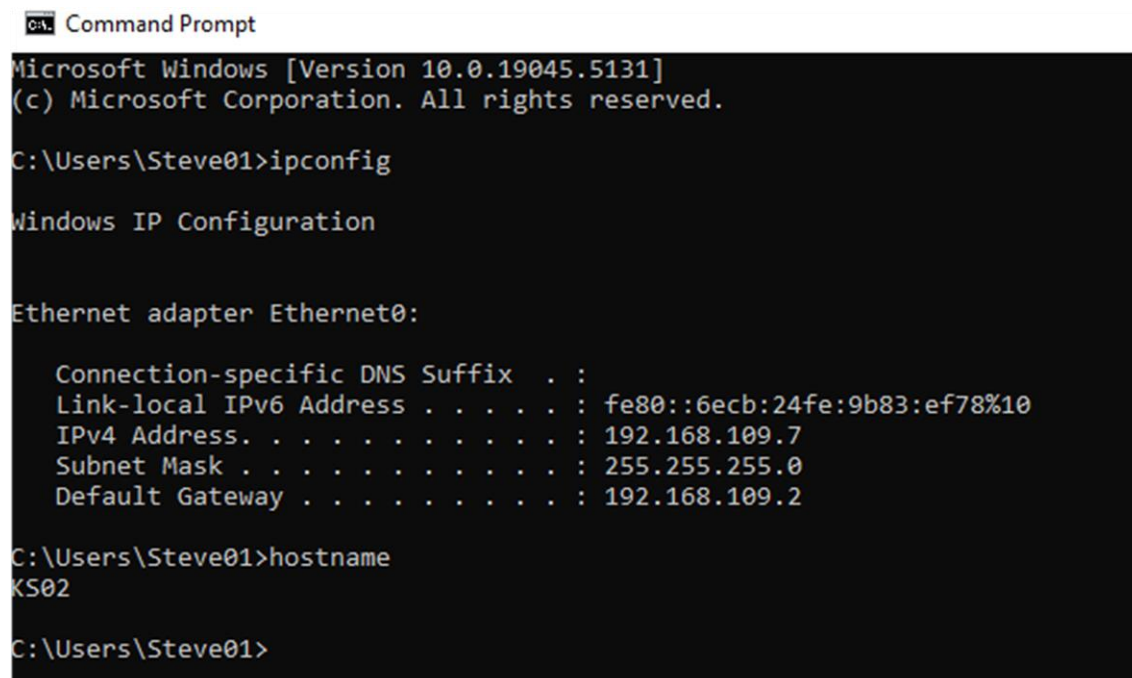
A terminal window titled 'terminal' with a menu bar (Archivo, Editar, Ver, Terminal, Pestañas, Ayuda). The prompt is 'root@debian1:~#'. The command 'ifconfig' has been executed, showing details for 'ens33' and 'lo'.

```
root@debian1:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.109.128  netmask 255.255.255.0  broadcast 192.168.109.255
    inet6 fe80::20c:29ff:fe82:4289  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:82:42:89  txqueuelen 1000  (Ethernet)
    RX packets 51  bytes 5855 (5.7 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 51  bytes 6839 (6.6 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 21  bytes 2327 (2.2 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 21  bytes 2327 (2.2 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@debian1:~#
```

Imagen.17 IP VM Debian C&C.

A Windows Command Prompt window titled 'C:\> Command Prompt'. It shows the output of 'ipconfig' and 'hostname' commands.

```
C:\> Command Prompt

Microsoft Windows [Version 10.0.19045.5131]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Steve01>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6ecb:24fe:9b83:ef78%10
    IPv4 Address. . . . . : 192.168.109.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.109.2

C:\Users\Steve01>hostname
KS02

C:\Users\Steve01>
```

Imagen.18 IP y HOSTNAME de VM Víctima Windows 10.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.6532]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::369a:6d23:b37a:2609%6
    IPv4 Address. . . . . : 192.168.109.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.109.2

C:\Users\Administrator>hostname
KS01

C:\Users\Administrator>
```

Imagen.19 IP y HOSTNAME de VM Windows Server.

## 4.1Active Directory

Este es el active directory creado en la máquina Windows Server siguiendo estos pasos para su instalación:

1º Settings>system>about>change name>KS01>install

2º Add Roles>DNS Server>Active Directory Domain Services

3ºPromocionamos el servidor a domain controller

\*Creamos un nuevo directorio (icono de flag)

4º Tools>Active directory users and computers >creamos usuarios/grupos

y procedemos a representar la red de nuestra empresa objetivo:

Servidor principal: **KAYAK.local**

Usuarios creados: **Steve Hafner (CEO)**

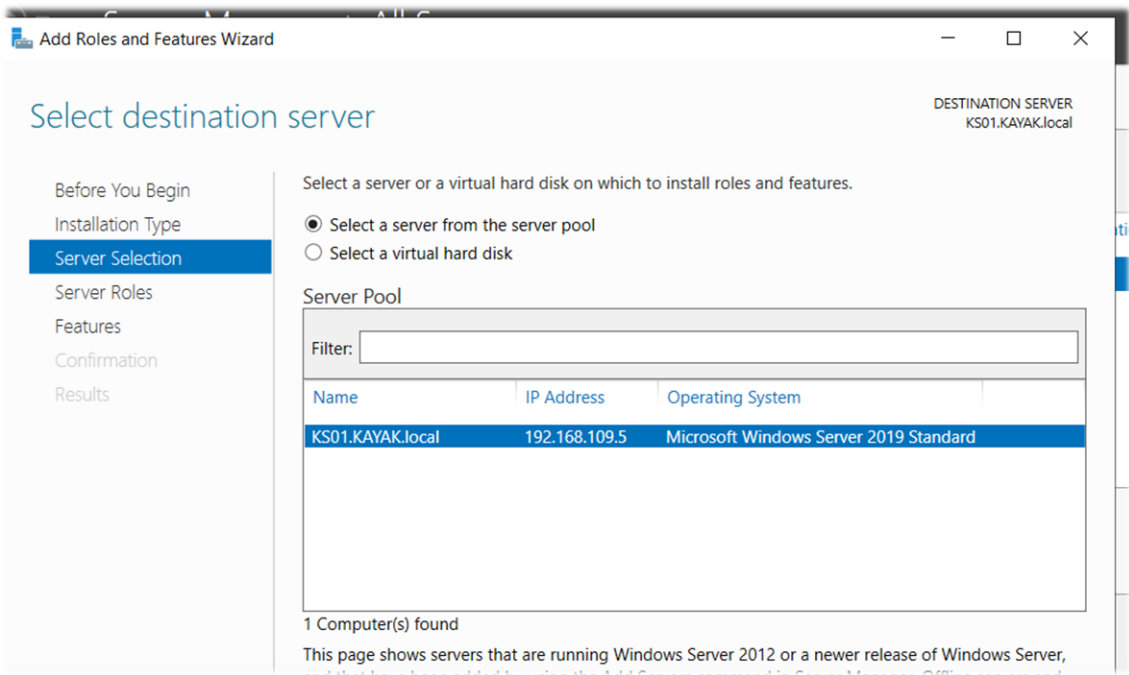


Imagen.20 Servidor creado en VM Windows Server de empresa KAYAK.

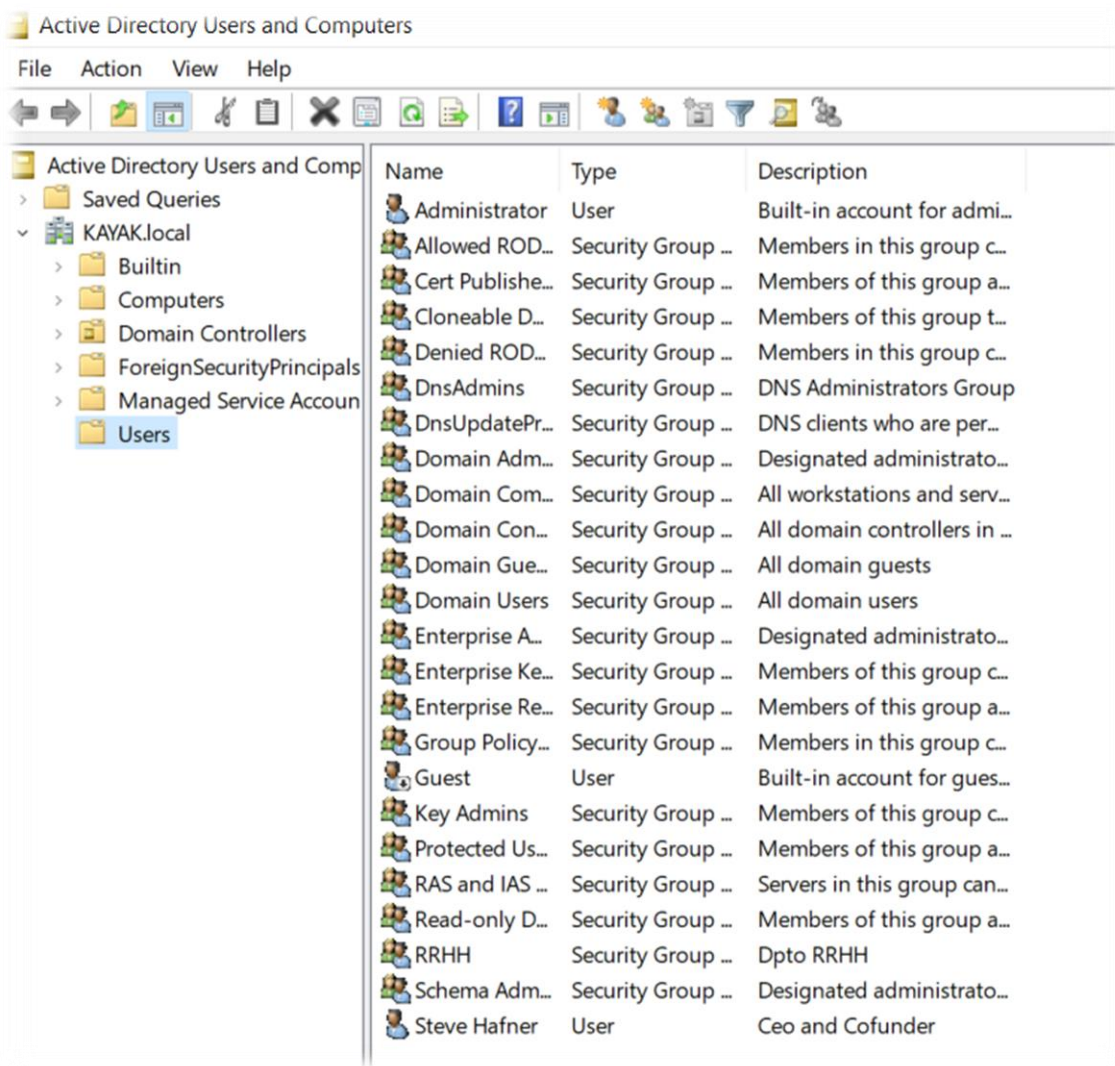


Imagen.21 Usuario creado en VM Windows Server de la empresa KAYAK.

## 4.2. Comand & Control

Mientras tanto en nuestra VM Debian vamos a configurar el **Havoc**, en la terminal ejecutamos el comando:

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

```
Cd Havoc/
```

```
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 libsqlite3-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
```

```
cd teamserver/
```

```
go mod download golang.org/x/sys
```

```
go versión (1.23.3)
```

```
go mod download github.com/ugorji/go
```

```
make ts-build(compilar)
```

```
make client-build
```


Nos abrimos dos terminales y en una ejecutamos dentro de la carpeta opt/Havoc

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

Y en la otra

```
./havoc client
```

Nos abrimos en una terminal e iniciamos el servidor con el puerto 80 a la escucha:



```
root@debian1:~# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

*Imagen.22 Puerto 80 a la escucha en VM Debian.*

Y ya podemos crear nuestro listeners en **Havoc**

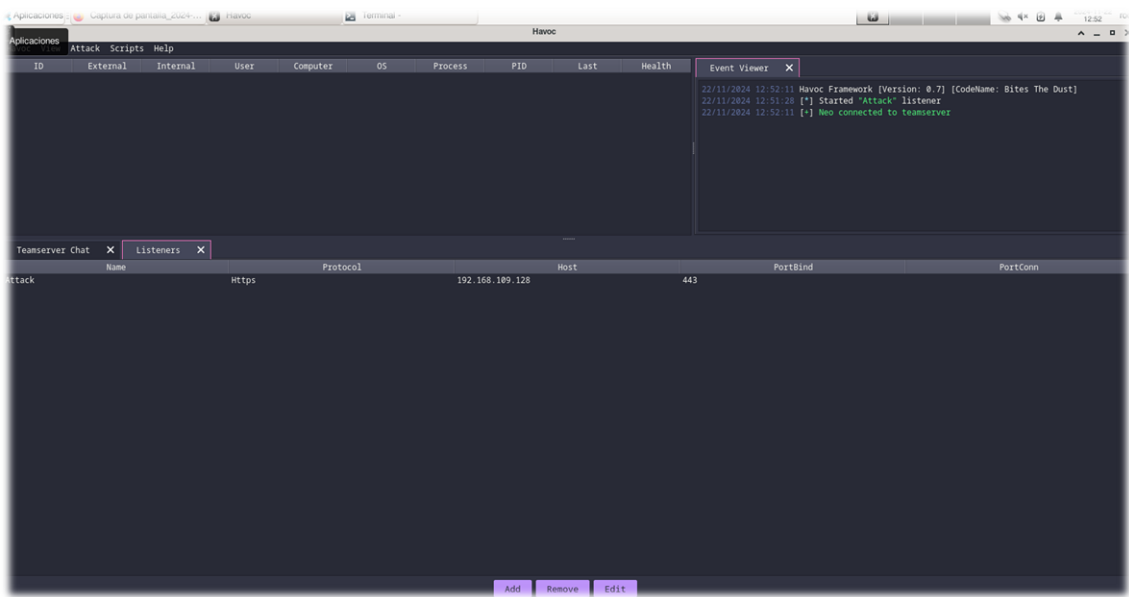


Imagen.23 Creación del listener en Havoc .

Y también nuestro payload

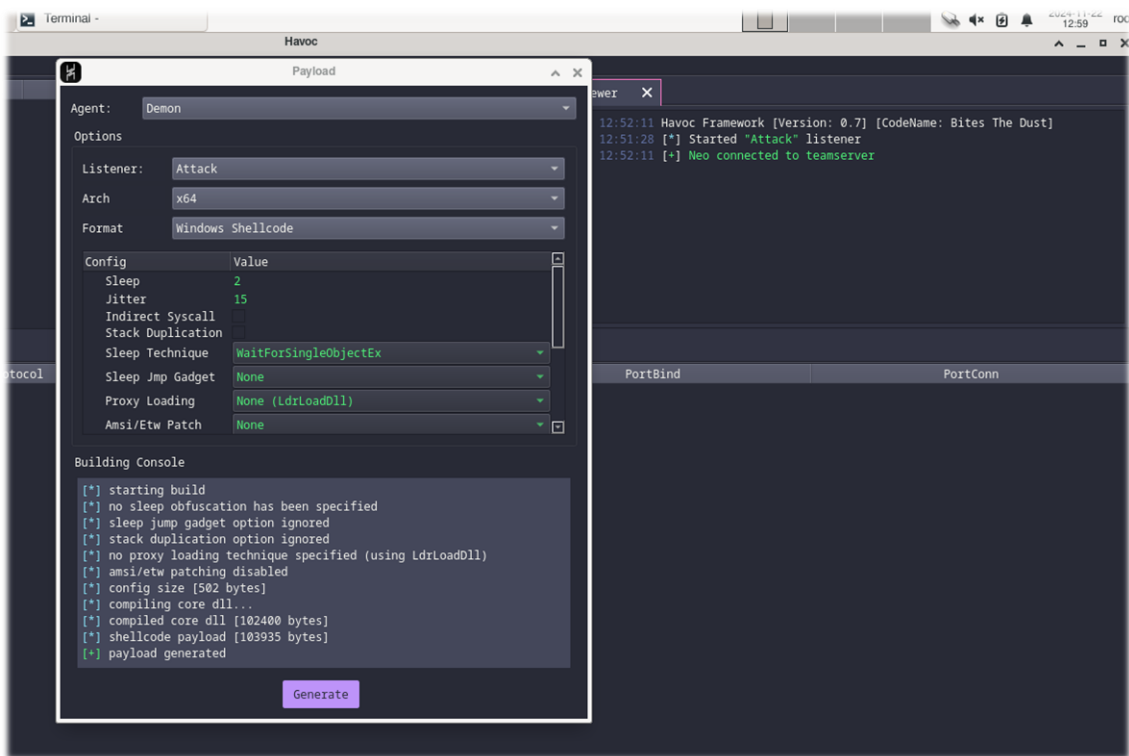


Imagen.24 Creación del payload en Havoc.



Una vez este creado y modificado nuestro código con un editor de código como VisualStudioCode, eliminando strings (Console.WriteLine, if(path == null)) y calcx64 para que no sea detectado por ningún antivirus se procede a guardar.

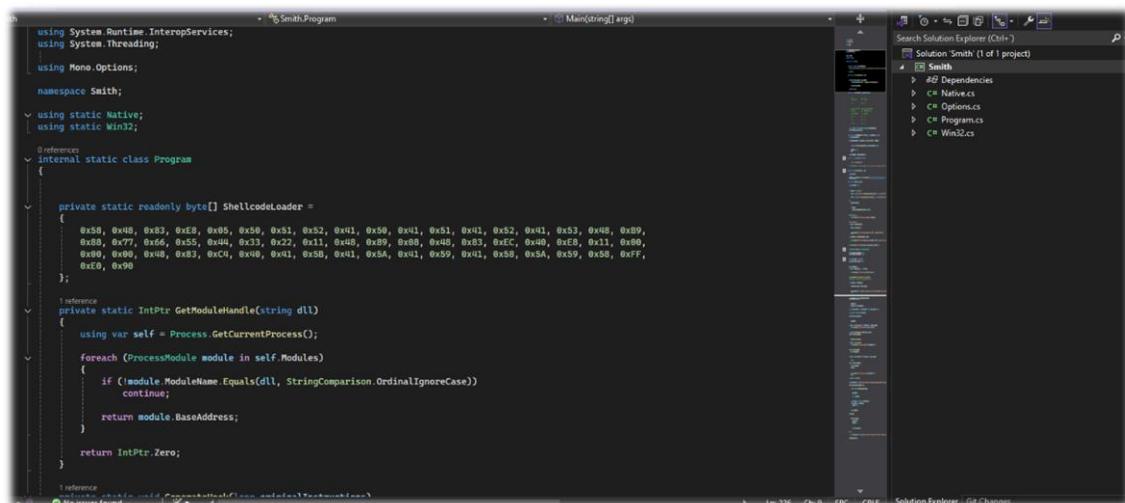


Imagen.25 Código malware modificado en VSC.

Y es aquí cuando nos toca realizar un correo de phishing diseñado para parecer legítimo y convencer a Steve de abrir el archivo adjunto.

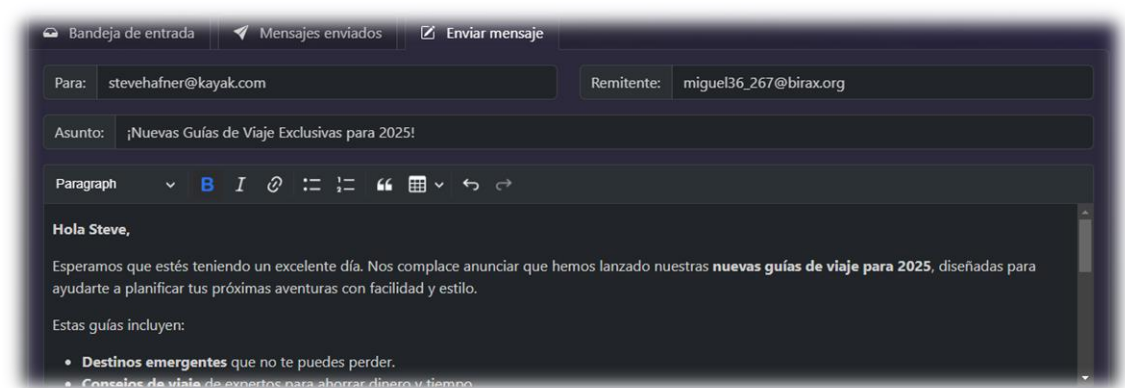


Imagen.26 Email para iniciar el ataque mediante phishing.

Podemos ver en nuestra terminal de **Havoc** que el usuario objetivo ha abierto el archivo malicioso y hemos infectado la máquina objetivo:

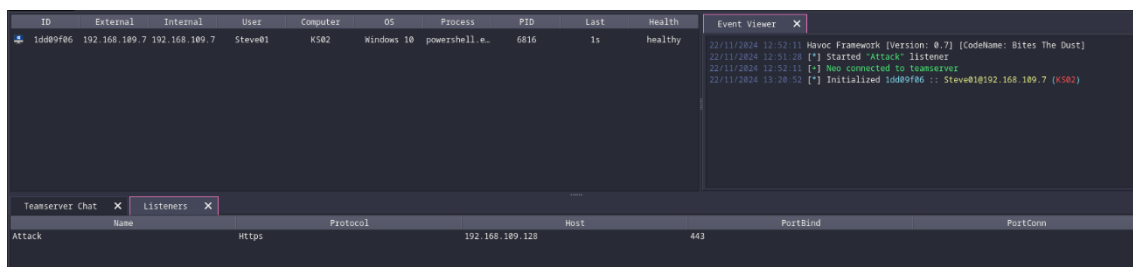


Imagen.27 Reporte en Havoc de que el ataque ha sido ejecutado con éxito.

## 5. Resumen final

En esta práctica, hemos seguido un enfoque estructurado para lograr el ataque y posterior control de la empresa objetivo, **KAYAK.COM**, mediante un ataque de phishing. A continuación, se resumen los pasos seguidos:

### 1. Configuración del Entorno

- **Máquina 1: Servidor con Active Directory (Windows Server):**
  - Instalación y configuración de Active Directory.
  - Promoción del servidor a controlador de dominio.
- **Máquina 2: Comand & Control (Windows):**
  - Unión al dominio configurado en el servidor.
  - Verificación de la conexión y autenticación en el dominio.
- **Máquina 3: Ejecución de Havoc (Debian):**
  - Instalación y configuración de Havoc para la creación y envío de malware.

### 2. Recopilación de Información

- **Herramientas Utilizadas:**
  - **Whois, Nslookup, Shodan y Nmap:** Para obtener información sobre los registros de dominio, servidores y servicios expuestos.

- **LDAP Enumeration y BloodHound:** Para recolectar información detallada del Active Directory en un entorno simulado.

### **3. Diseño del Ataque de Phishing**

- **Recopilación de Información sobre Empleados:**
  - Identificación de empleados de KAYAK mediante LinkedIn y redes sociales.
- **Creación del Correo de Phishing:**
  - Diseño de un correo convincente sobre nuevas guías de viaje, dirigido a Steve, con un archivo adjunto malicioso.
- **Envío del Correo:**
  - Utilización de un cliente de correo en Debian para enviar el phishing.

### **4. Ejecución del Malware**

- **Configuración de Havoc:**
  - Creación del payload malicioso.
- **Envío y Ejecución del Malware:**
  - Envío del correo de phishing y ejecución del malware en la máquina Debian (Comand Control).
  - Monitoreo de la conexión establecida y control del payload desde Debian.