

Reconocimiento de una Organización

Módulo - Recopilación de
Información

Alejandro Delgado Martínez
53344428-E

INTRODUCCIÓN

El presente informe tiene como objetivo realizar un reconocimiento exhaustivo de una organización elegida, que en este caso será Epic Games, con la intención de extraer toda la información sensible que pueda ser relevante para entender su estado actual de seguridad y proponer medidas de mejora.

Durante este ejercicio, se aplicarán diversas técnicas y herramientas exploradas a lo largo del módulo, incluyendo Footprinting, Fingerprinting y técnicas OSINT (Open Source Intelligence). Esto nos permitirá una comprensión profunda de la estructura y la operación de la organización, así como la identificación de cualquier información crítica que pueda estar expuesta o ser susceptible a explotación.

En el desarrollo del informe, se detallarán los procedimientos y los hallazgos obtenidos a través de estas técnicas, incluyendo la recopilación de datos sobre los dominios y subdominios relacionados, el análisis de vulnerabilidades y la información adicional recopilada mediante técnicas OSINT como correos electrónicos y empleados relevantes.

1. SELECCIÓN DE OBJETIVO

El objetivo designado para este proyecto es la reconocida empresa Epic Games, sobre la cual vamos a realizar un análisis detenido dentro del siguiente alcance:

***.epicgames.com**



***.epicgames.com**

Note: This asset may contain endpoints not hosted by Epic Games (third party endpoints). These third party endpoints are not eligible for bounty. Please take note of the infrastructure you are assessing, if the endpoint is not hosted on AWS and/or the ASN is not associated with Epic Games then it is most likely not hosted by Epic Games.

If you are unsure whether or not an asset is considered third party please submit a preliminary finding for confirmation.

Other

In scope

Critical

Eligible

24/01/2023

Una vez hemos realizado esto, vamos a crear los directorios adecuados:

```
(kali@kali)-[~/Desktop]
$ cd Práctica

(kali@kali)-[~/Desktop/Práctica]
$ mkdir epicgames
```

2. FOOTPRINTING

Iniciando con la etapa de Footprinting, que es fundamental para recopilar información crucial mediante técnicas de fuerza bruta, lo primero que hicimos fue descargar una lista que contiene subdominios comúnmente utilizados por las empresas, desde la siguiente URL:

```
https://github.com/danielmiessler/SecLists/blob/master/Discovery/DNS/subdomains-top1million-110000.txt
```

Guardamos el archivo descargado como subdomains.txt.

Posteriormente, nos dedicamos a la creación de una lista de DNS válidos, una tarea que requerirá repetirse aproximadamente cada 30 días para mantener la actualización de los datos. Para realizar esta tarea, empleamos el siguiente comando:

```
dnsvalidator -tL  
https://raw.githubusercontent.com/blechschmidt/massdns/master/lists/resolvers.txt  
-t -threads 500 -o $HOME/Desktop/practica/lists/resolvers.txt
```

A través de este comando, estamos realizando las siguientes operaciones:

1. Utilizamos la herramienta dnsvalidator para verificar la operatividad de los servidores DNS enlistados.
2. Descargamos un listado de servidores DNS desde el enlace proporcionado.
3. Facilitamos el proceso de verificación mediante la ejecución de 500 hilos simultáneos, lo que acelera notablemente la tarea.
4. Generamos y almacenamos un nuevo archivo de texto denominado resolvers.txt dentro de una carpeta específica, que contiene los servidores DNS válidos y operativos. Este archivo será de suma importancia ya que será utilizado posteriormente para lanzar nuestras consultas DNS sobre el alcance definido, en este caso, el dominio *.epicgames.com.

Esta estructurada metodología nos permite establecer un entorno preparado y organizado, crucial para la ejecución de las siguientes fases de nuestro proyecto de recolección y análisis de información.

2.1 SHUFFLEDNS

Con la preparación previa concluida, nos enfocaremos en emplear la herramienta ShuffleDNS para descubrir subdominios asociados al alcance especificado de *.epicgames.com.

ShuffleDNS se destaca por su capacidad de trabajar junto con resolvers masivos y listas de subdominios precompiladas para identificar subdominios válidos de manera eficaz y eficiente.

Iniciaremos el proceso utilizando ShuffleDNS, proporcionándole el archivo de resolvers.txt y subdomains.txt que preparamos anteriormente. La ejecución de esta herramienta nos permitirá explorar y descubrir subdominios asociados al dominio principal de Epic Games.

Al concluir la ejecución de ShuffleDNS, se generará un archivo de texto (shuffledns_subdominios.txt) que recopilará todos los subdominios descubiertos durante el proceso.

2.2 GOOGLE ANALYTICS

El siguiente paso en nuestra investigación consiste en utilizar una herramienta que explore Google Analytics, lo que puede facilitar la extracción de dominios y subdominios asociados desde diversas bases de datos que también empleen este servicio.



```
(kali㉿kali)-[~/Desktop/practica/epicgames]
$ analyticsrelationships --url https://www.epicgames.com

UA-ID
DOMAINS

> Get related domains / subdomains by looking at Google Analytics IDs
> Python version
> By @JosueEncinar

[+] Analyzing url: https://www.epicgames.com
[-] Tagmanager URL not found
```

Al intentar ejecutar la herramienta, nos encontramos con que no logra encontrar el recurso deseado. Ante esta situación, procedemos a revisar si el servicio de Google Analytics está operativo o si se encuentra en una interrupción temporal.

Tras verificar y confirmar que el servicio está funcionando correctamente, podemos decir que el alcance definido, *.epicgames.com, no está utilizando Google Analytics.

Con esta información en mano, decidimos avanzar hacia el siguiente punto de nuestra investigación. Esta etapa nos ha proporcionado una pieza valiosa de información respecto a la no-utilización de Google Analytics por parte de Epic Games en el dominio especificado, lo que podría indicar una preferencia por otras plataformas de análisis de tráfico web o una gestión de analytics in-house.

2.3 TLS PROBING

El análisis de los certificados SSL/TLS puede ser una fuente rica en información, ya que en ocasiones contienen dominios y/o subdominios que pertenecen a la organización analizada. Para esta tarea, decidimos utilizar la herramienta **cero**, que se diseñó específicamente para explorar y extraer información de los certificados SSL/TLS.

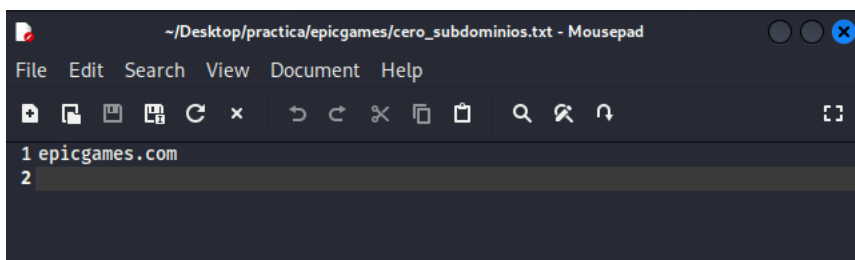
El comando ejecutado fue el siguiente:

```
cero -d epicgames.com > cero_subdominios.txt
```

En este comando, **-d** especifica el dominio que queremos analizar, y la salida se redirige a un archivo de texto llamado **cero_subdominios.txt** para una revisión posterior.

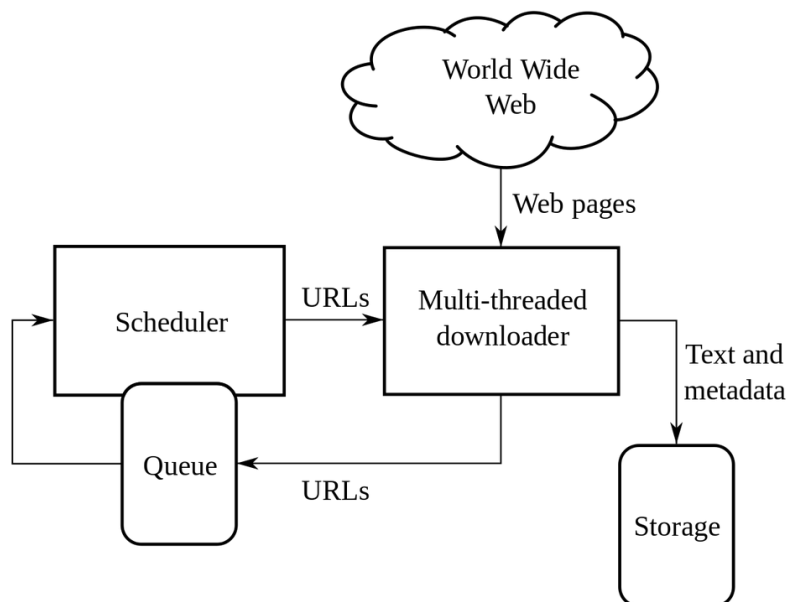
Sin embargo, al revisar los resultados proporcionados por la herramienta, encontramos que no fueron tan fructíferos como esperábamos. La herramienta solo ha logrado identificar y proporcionar el dominio principal **epicgames.com**, sin revelar ningún subdominio adicional que pudiera estar asociado con la organización.

Este resultado, aunque no es el ideal, es un indicativo que nos ayuda a entender que el certificado SSL/TLS utilizado por Epic Games en este caso no tiene listados otros subdominios.



2.4 WEB SCRAPING

El Web Scraping es una técnica valiosa que implica la extracción recursiva de información desde una página web. Esta técnica puede ser de gran utilidad para descubrir subdominios asociados a la organización en estudio.



El proceso de Web Scraping se desglosará en tres etapas esenciales:

1. Obtener los archivos de código fuente y código JavaScript de manera recursiva para extraer los subdominios (scraping).
2. Limpiar el output para conservar únicamente los subdominios.
3. Verificar la validez de los subdominios descubiertos.

Para llevar a cabo este proceso, nos apoyaremos en dos herramientas especializadas:

- **KATANA:** encargada de la tarea de scraping.
- **UNFURL:** diseñada para extraer el dominio de una URL.

2.4.1 KATANA

Para utilizar Katana, ejecutaremos el siguiente comando que almacenará los resultados en un archivo de texto:

```
echo epicgames.com | katana -silent -jc -o katana_subdominios.txt -kf robotstxt, sitemapxml
```

Una vez ejecutado este comando, obtendremos una lista de subdominios, algunos de los cuales podrían no ser relevantes para nuestro análisis, lo que nos lleva a la necesidad de limpiar y filtrar los datos recopilados.

2.4.2 UNFURL

Para la limpieza de los datos, utilizaremos la herramienta UNFURL, que nos permitirá extraer y conservar únicamente los dominios únicos que están dentro del alcance definido. Ejecutaremos el siguiente comando para limpiar los datos y almacenar los resultados en un nuevo archivo:

```
cat katana_subdominios.txt | unfurl -unique domains > katana_subdominiosOK.txt
```

Con este proceso, ahora tendremos dos archivos: uno conteniendo todos los dominios y otro con los dominios filtrados y limpios.

```
(kali@kali)-[~/Desktop/practica/epicgames]
$ ls
cero_subdominios.txt  katana_subdominiosOK.txt  katana_subdominios.txt  shuffledns_subdominios.txt
```

Dado que el archivo filtrado (katana_subdominiosOK.txt) es el que nos interesa para las fases subsiguientes de nuestro análisis, procederemos a eliminar el archivo original que contiene todos los dominios mediante el siguiente comando:

```
rm -f katana_subdominios.txt
```

De esta manera, conservamos el archivo katana_subdominiosOK.txt que contiene la lista de subdominios filtrados y relevantes para nuestro análisis, lo que nos sitúa en una posición favorable para continuar con las etapas siguientes de nuestra evaluación sobre la infraestructura digital de Epic Games.

```
(kali@kali)-[~/Desktop/practica/epicgames]
$ ls
cero_subdominios.txt  katana_subdominiosOK.txt  shuffledns_subdominios.txt
```

2.4.3 CTFR

CTFR es una herramienta de reconocimiento de subdominios que aprovecha la información contenida en los certificados SSL/TLS, particularmente en sitios web que utilizan el protocolo HTTPS. Esta herramienta puede ser crucial en el ámbito de la ciberseguridad, especialmente durante las pruebas de penetración (pentesting) para descubrir subdominios que podrían ser potenciales vectores de ataque.

El comando para trabajar con el CTFR es el siguiente:

```
ctfr -d epicgames.com > ctfr_subdominios.txt
```

Este comando le indica a CTFR que realice un escaneo de subdominios en epicgames.com y que almacene los resultados en ctfr_subdominios.txt.

Posteriormente, para limpiar y filtrar la lista de subdominios obtenidos, utilizaremos el siguiente comando:

```
cat ctfr_subdominios.txt | grep -oE '\*\.\(S+\)' | sed 's/\*\.\(.*\)\/1/g' | unfurl --unique domains > ctfr_subdominiosOK.txt
```

Este comando utiliza grep para extraer líneas que contienen patrones de subdominio, sed para procesar y formatear estos patrones, y unfurl para extraer y listar dominios únicos, almacenando los resultados limpios en ctfr_subdominiosOK.txt.

Finalmente, para eliminar el archivo original y conservar solo el archivo limpio, se utiliza el siguiente comando:

```
rm -f ctfr_subdominios.txt
```

2.5 BÚSQUEDAS PASIVAS

En esta etapa, emplearemos la herramienta GAU (GetAllUrls) que es esencial para recopilar URLs conocidas asociadas a un dominio específico. Esta herramienta es altamente valiosa en el ámbito de la ciberseguridad y el análisis forense web, ya que permite recopilar un gran volumen de URLs que pueden ser exploradas posteriormente para identificar posibles vectores de ataque o información sensible.

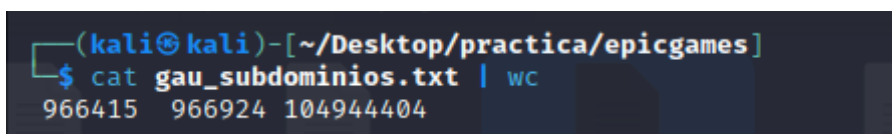
El comando a utilizar para ejecutar GAU es el siguiente:

```
gau -threads 5 epicgames.com -o gau_subdominios.txt
```

Este comando instruye a GAU para recopilar URLs del dominio **epicgames.com**, utilizando 5 hilos de ejecución, y almacenar los resultados en el archivo **gau_subdominios.txt**.

Dado que GAU puede generar un archivo con un gran número de entradas, es prudente revisar el tamaño del archivo resultante con el siguiente comando:

```
cat gau_subdominios.txt | wc
```



```
(kali㉿kali)-[~/Desktop/practica/epicgames]  
$ cat gau_subdominios.txt | wc  
966415 966924 104944404
```

Este comando devolverá el número total de líneas en el archivo, que corresponde al número de URLs recopiladas.

Para filtrar y conservar solo los subdominios que son relevantes para nuestro análisis, ejecutaremos el siguiente comando que limpiará el archivo original:


```
cat gau_subdominios.txt | unfurl --unique domains > gau_subdominiosOK.txt
```

```
(kali㉿kali)-[~/Desktop/practica/epicgames]
$ cat gau_subdominiosOK.txt | wc
 214    214   8376
```

Este comando utiliza **unfurl** para extraer y listar solo los dominios únicos del archivo original, almacenando los resultados limpios en **gau_subdominiosOK.txt**.

Finalmente, para eliminar el archivo original y conservar solo el archivo limpio y filtrado, ejecutaremos el siguiente comando:

```
rm -f gau_subdominios.txt
```

2.6 UNIR LOS SUBDOMINIOS

Después de haber empleado una variedad de herramientas y técnicas para recopilar subdominios, el paso siguiente es consolidar todos estos subdominios en un archivo único.

Este archivo único facilitará la revisión y el análisis posterior, además de permitir una rápida identificación de subdominios duplicados o irrelevantes para el alcance de nuestro análisis.

Si visualizamos, actualmente tenemos estos ficheros:

```
(kali㉿kali)-[~/Desktop/practica/epicgames]
$ ls -lht
total 32K
-rw-r--r-- 1 kali kali 8.2K Oct 14 10:45 gau_subdominiosOK.txt
-rw-r--r-- 1 kali kali 6.9K Oct 14 10:21 ctfr_subdominiosOK.txt
-rw-r--r-- 1 kali kali  32 Oct 14 07:07 katana_subdominiosOK.txt
-rw-r--r-- 1 kali kali  14 Oct 14 06:55 cero_subdominios.txt
-rw-r--r-- 1 kali kali  891 Oct 13 14:12 shuffledns_subdominios.txt
```

Para unificar todos estos subdominios en un archivo único y eliminar los duplicados, emplearemos el siguiente comando:

```
cat *_subdominios*.txt | unfurl --unique domains > subdominiosOK.txt
```

Este comando concatena todos los archivos que contienen la palabra "subdominios" en su nombre, extrae los dominios únicos de esos archivos y los almacena en un nuevo archivo llamado **subdominiosOK.txt**.

A continuación, para asegurar que todos los subdominios listados estén dentro del alcance definido (**epicgames.com**), y para homogeneizar los subdominios a minúsculas, aplicaremos el siguiente comando:

```
cat subdominiosOK.txt | grep -E '\.epicgames\.com$' | tr '[:upper:]' '[:lower:]' | unfurl --unique domains > subdominiosOK_scope.txt
```

Este comando filtra los subdominios para incluir solo aquellos que terminan en **.epicgames.com**, convierte cualquier letra mayúscula a minúscula, y extrae los dominios únicos una vez más, almacenando el resultado en **subdominiosOK_scope.txt**.

Con estos pasos, habremos creado un archivo único y limpio que contiene todos los subdominios relevantes y únicos asociados a **epicgames.com**. Este archivo consolidado será de gran utilidad para las siguientes fases de nuestro análisis, permitiendo una visión clara y organizada de los subdominios que forman parte de la infraestructura digital de Epic Games.

Ahora estamos mejor posicionados para proceder con un análisis más detallado de estos subdominios, explorando posibles vulnerabilidades y recolectando información adicional que pueda ser crucial para cumplir los objetivos de nuestro proyecto.

```
(kali㉿kali)-[~/Desktop/practica/epicgames]
$ cat subdominiosOK_scope.txt | wc
  449    449   15825
```

2.7 COMPROBAR LOS DOMINIOS

Tras la exhaustiva búsqueda y consolidación de subdominios, el paso lógico siguiente es verificar la validez de estos dominios para asegurar que están activos y accesibles. Para esta tarea, utilizaremos la herramienta **httpx** que es eficaz para verificar el estado de los dominios.

El comando proporcionado es el siguiente:

```
cat subdominiosOK_scope.txt | httpx -silent -mc 200,401,403 -o subdominiosvivos.txt
```

Este comando toma la lista de subdominios del archivo **subdominiosOK_scope.txt**, verifica cada subdominio con **httpx** en modo silencioso (**-silent**), acepta códigos de estado HTTP 200, 401 y 403 como válidos (**-mc 200,401,403**), y almacena los subdominios válidos en un archivo llamado **subdominiosvivos.txt**.

Los subdominios válidos devueltos tienen el siguiente formato:

```
https://accf5076e09d.epic-social-game-overlay-prod-ci.ol.epicgames.com
```

Para limpiar y extraer solo el nombre del dominio, utilizaremos el siguiente comando:

```
cat subdominiosvivos.txt | unfurl -unique domains > subdominios_targets.txt
```

Este comando utiliza **unfurl** para extraer los dominios únicos de las URLs y almacenarlos en un archivo llamado **subdominios_targets.txt**.

Al concluir este proceso, obtendremos un listado optimizado de subdominios activos y válidos que forman parte de la infraestructura digital de Epic Games. Este listado será una valiosa referencia para las futuras etapas de nuestro análisis, proporcionando un punto de partida sólido para explorar cada subdominio en detalle, identificar posibles vulnerabilidades, y recopilar información adicional que pueda ser relevante para los objetivos de nuestro proyecto.

Con un listado limpio y validado, estamos en una posición más fuerte para proceder con análisis más detallados y específicos de la infraestructura digital de Epic Games.

El resultado sería este:

accf5076e09d.epic-social-game-overlay-prod-ci.ol.epicgames.com
0a4b53775655.epic-social-game-overlay-prod-ci.ol.epicgames.com
caldera-service-prod.ecosec.on.epicgames.com
create-epic-kitt-react.fnsocial.on.epicgames.com
cdn-0001.qstv.on.epicgames.com
cdn2.epicgames.com
cdn1.epicgames.com
download.epicgames.com
download2.epicgames.com
download3.epicgames.com
download4.epicgames.com
download-test.epicgames.com
fastly-download.epicgames.com
epic-social-social-modules-prod.ol.epicgames.com
epic-social-game-overlay-prod.ol.epicgames.com
fn-hotconfigs.ogs.live.on.epicgames.com
fortnite-island-screenshots-live-cdn.ol.epicgames.com
launcher.store.epicgames.com
installer.ega.ol.epicgames.com
jira.epicgames.com
media-cdn.epicgames.com
merchantpool1.epicgames.com
modules-cdn.eac-gamedev.on.epicgames.com
modules-cdn.eac-prod.on.epicgames.com
nelly-service-prod-cloudflare.ecosec.on.epicgames.com
platypus-ci.fnsocial.on.epicgames.com
redirect.epicgames.com
safety.epicgames.com

perf.store.on.epicgames.com
static-assets-prod.epicgames.com
store.epicgames.com
status.epicgames.com
talon-service-v4-prod.ak.epicgames.com
talon-service-prod.ak.epicgames.com
talon-website-prod.ak.epicgames.com
unrealstudio.epicgames.com
wex-public-service-live-prod.epic-social-game-overlay-prod-ci.ol.epicgames.com

3. FINGERPRINTING

3.1 NMAP

Con un listado validados de subdominios en mano, ahora estamos en posición de llevar a cabo un escaneo para recolectar información adicional y valiosa de estos. NMAP (Network Mapper) es la herramienta que utilizaremos en esta fase.

NMAP es altamente efectiva para descubrir hosts activos, servicios corriendo, y otras características relevantes de la red.

El comando especificado para esta tarea es el siguiente:

```
nmap -sn -iL subdominios_target.txt > nmap_subdominios.txt
```

En este comando:

- **-sn:** Especifica un escaneo de ping, que ayuda a determinar si los subdominios están activos o no.
- **-iL:** Indica a NMAP que lea la lista de subdominios a escanear desde el archivo **subdominios_target.txt**.
- **> nmap_subdominios.txt:** Redirige la salida de NMAP a un archivo llamado **nmap_subdominios.txt**.

Como resultado, el archivo **nmap_subdominios.txt** contendrá información sobre los subdominios que están activos y han respondido al ping de NMAP. Esto proporciona una visión inicial sobre qué subdominios están operativos y, por lo tanto, merecen una investigación más detallada.

```
(kali@kali)-[~/Desktop/practica/epicgames]
$ ls -lht
total 84K
-rw-r--r-- 1 kali kali 10K Oct 14 11:36 nmap_subdominios.txt
-rw-r--r-- 1 kali kali 1.3K Oct 14 11:27 subdominios_targets.txt
-rw-r--r-- 1 kali kali 1.6K Oct 14 11:22 subdominiosvivos.txt
-rw-r--r-- 1 kali kali 16K Oct 14 11:03 subdominiosOK_scope.txt
-rw-r--r-- 1 kali kali 16K Oct 14 10:57 subdominiosOK.txt
-rw-r--r-- 1 kali kali 8.2K Oct 14 10:45 gau_subdominiosOK.txt
-rw-r--r-- 1 kali kali 6.9K Oct 14 10:21 ctfr_subdominiosOK.txt
-rw-r--r-- 1 kali kali 32 Oct 14 07:07 katana_subdominiosOK.txt
-rw-r--r-- 1 kali kali 14 Oct 14 06:55 cero_subdominios.txt
-rw-r--r-- 1 kali kali 891 Oct 13 14:12 shuffledns_subdominios.txt
```

Ahora procederemos a limpiar el archivo generado por NMAP para extraer solamente las direcciones IP asociadas a los subdominios. La limpieza es esencial para tener un archivo más manejable y enfocado en los datos que necesitamos para los siguientes pasos de nuestro análisis.

El comando para limpiar y extraer las direcciones IP es el siguiente:

```
cat nmap_subdominios.txt | grep -oE '[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+' > nmap_ips.txt
```

Este comando utiliza **grep** para buscar y extraer todas las ocurrencias de patrones que corresponden a direcciones IP del archivo **nmap_subdominios.txt**, y almacena estas direcciones IP en un nuevo archivo llamado **nmap_ips.txt**.

Para eliminar el archivo original y conservar solo el archivo con las direcciones IP, se ejecuta el siguiente comando:

```
rm -rf nmap_subdominios.txt
```

Ahora, con el objetivo de explorar los métodos HTTP admitidos por los subdominios, utilizaremos NMAP nuevamente con un script especial para escanear los métodos HTTP en los puertos 80 y 443, que son los puertos estándar para el tráfico HTTP y HTTPS, respectivamente.

El comando para esta tarea es el siguiente:

```
nmap -p80,443 --script http-methods -iL subdominios_targets.txt > nmap_httpmethods.txt
```

En este comando:

- **-p80,443**: Especifica los puertos a escanear (80 y 443).
- **--script http-methods**: Indica a NMAP que utilice el script **http-methods** para identificar los métodos HTTP admitidos en los subdominios.
- **-iL subdominios_targets.txt**: Indica a NMAP que lea la lista de subdominios a escanear desde el archivo **subdominios_targets.txt**.
- **> nmap_httpmethods.txt**: Redirige la salida de NMAP a un archivo llamado **nmap_httpmethods.txt**.

Como resultado, el archivo **nmap_httpmethods.txt** contendrá información sobre los métodos HTTP admitidos por cada subdominio en los puertos 80 y 443.

Esta información es valiosa para entender las posibles vías de interacción con los servicios web en los subdominios de Epic Games, y puede revelar posibles vectores de ataque o áreas que requieren una mayor protección y revisión.

3.2 MASSCAN

Ahora vamos a utilizar Masscan, que es conocido por escanear puertos a una velocidad muy alta, lo que lo hace extremadamente eficaz para explorar un gran número de puertos en poco tiempo. Sin embargo, a diferencia de NMAP, Masscan requiere direcciones IP en lugar de nombres de dominio.

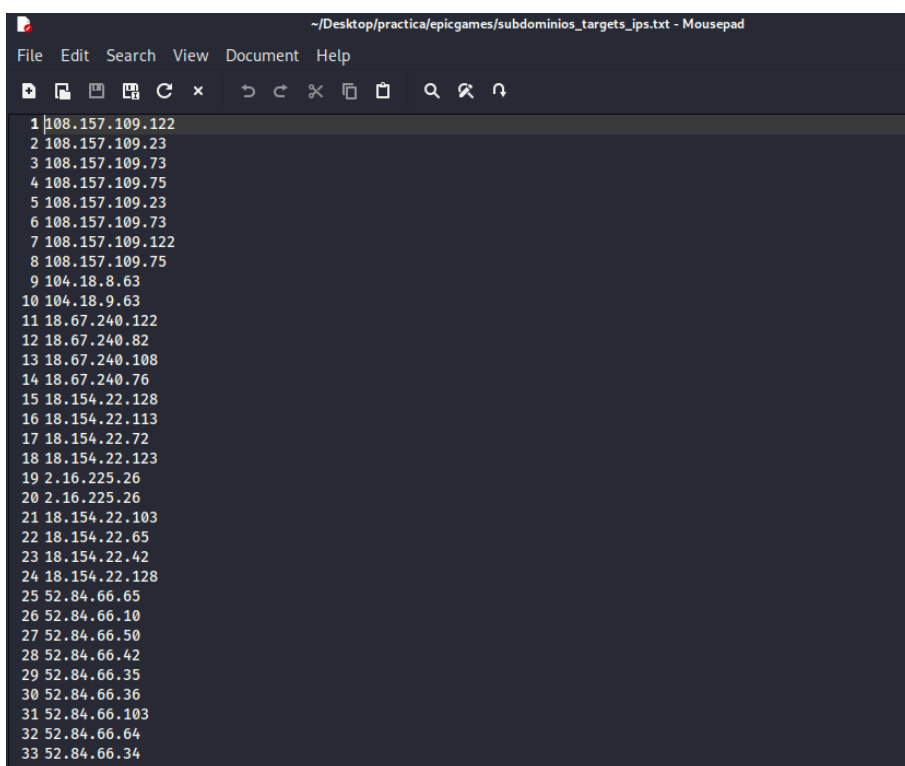
Para convertir los nombres de dominio en nuestro archivo **subdominios_targets.txt** a direcciones IP, utilizaremos el siguiente comando que emplea la herramienta **dig**:

```
for subdominio in $(cat subdominios_targets.txt); do dig +short $subdominio | grep -E '([0-9]{1,3}\.){3}[0-9]{1,3}'; done > subdominios_targets_ips.txt
```

En este comando:

- Se realiza un bucle **for** que lee cada línea (nombre de dominio) del archivo **subdominios_targets.txt**.
- Se utiliza **dig +short \$subdominio** para realizar una consulta DNS y obtener la dirección IP correspondiente a cada nombre de dominio.
- **grep -E '([0-9]{1,3}\.){3}[0-9]{1,3}'** filtra la salida de **dig** para asegurar que sólo se capturen las direcciones IP válidas.
- **> subdominios_targets_ips.txt** redirige la salida a un nuevo archivo llamado **subdominios_targets_ips.txt**.

Al finalizar este proceso, se generará un archivo **subdominios_targets_ips.txt** que contiene las direcciones IP correspondientes a los nombres de dominio en **subdominios_targets.txt**. Este archivo de IPs será la entrada necesaria para ejecutar Masscan en la siguiente fase.



Ahora estamos listos para utilizar Masscan, una herramienta poderosa conocida por su rapidez en el escaneo de puertos en comparación con otras como Nmap. Nuestro objetivo es examinar una amplia gama de puertos para identificar cualquier anomalía o puertos abiertos que podrían ser de interés para una posterior exploración.

Para ejecutar Masscan, necesitamos proporcionarle la lista de IPs que recopilamos anteriormente. Aquí está el comando que utilizaremos, especificando un extenso rango de puertos para el escaneo:

```
sudo masscan -p1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-
```

```
7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-
7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-
8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-
8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-
8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-
9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-
9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-
9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-
10004,10009-10010,10012,10024-10025,10082,10180,10215,10243,10566,10616-
10617,10621,10626,10628-10629,10778,11110-
11111,11967,12000,12174,12265,12345,13456,13722,13782-
13783,14000,14238,14441-14442,15000,15002-15004,15660,15742,16000-
16001,16012,16016,16018,16080,16113,16992-
16993,17877,17988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19
842,20000,20005,20031,20221-
20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-
27353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-
32785,33354,33899,34571-
34573,35500,38292,40193,40911,41511,42510,44176,44442-
44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-
49176,49400,49999-
50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52
869,54045,54328,55055-55056,55555,55600,56737-
56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65
000,65129,65389 -iL subdominios_targets_ips.txt > massscan_subdominios.txt
```

Una vez generado el archivo mediante el escaneo con Masscan, al revisarlo, podemos identificar varios puertos significativos como el 8080, 5060, 2000, 8008, y 8443.

Estos puertos pueden ser indicativos de servicios específicos corriendo en los servidores que están siendo evaluados. Por ejemplo:

- El puerto **8080** es comúnmente usado para servidores web alternativos.
- El puerto **5060** está asociado con el protocolo SIP utilizado en servicios de VoIP.
- El puerto **2000** podría estar asociado con el protocolo Cisco SCCP.
- El puerto **8008** también es utilizado comúnmente para servidores web alternativos.
- El puerto **8443** es a menudo utilizado para servicios web seguros (https).

En la próxima fase de pentesting, estos hallazgos pueden ser de gran utilidad, ya que proporcionan un punto de partida para realizar ataques dirigidos. Por ejemplo, podemos investigar más a fondo estos puertos para descubrir si hay algún servicio mal configurado o alguna vulnerabilidad conocida que pueda ser explotada.

Este tipo de información es crucial para entender mejor la superficie de ataque y planificar las estrategias de pentesting de manera más eficaz.

3.3 HTTPX

Además del análisis efectuado con las herramientas previamente mencionadas, reincorporaremos la utilización de HTTPX, que en etapas anteriores empleamos para filtrar dominios válidos basándonos en sus respuestas.

En esta fase, nuestro objetivo es examinar la respuesta proporcionada por los dominios válidos. Para ello, ejecutaremos el siguiente comando:

```
cat subdominios_targets.txt | httpx -status-code -title -cdn >httpx_subdominios.txt
```

Al revisar el archivo generado, notamos que muchos de los dominios arrojan un error 403, lo que indica una restricción de acceso. Esto podría ser un indicativo de que hemos sido bloqueados, aunque confirmamos que el dominio está activo.

Posteriormente, nos proponemos a explorar directorios interesantes en los subdominios en análisis (como el directorio 'admin'), utilizando el siguiente comando:

```
cat subdominios_targets.txt | httpx -path=admin -status-code
```

```
[INF] Current httpx version v1.3.5 (latest)
https://platypus-ci.fnsocial.on.epicgames.com/admin [403]
https://store.epicgames.com/admin [403]
https://create-epic-kitt-react.fnsocial.on.epicgames.com/admin [403]
https://safety.epicgames.com/admin [403]
https://download2.epicgames.com/admin [403]
https://download.epicgames.com/admin [403]
https://fastly-download.epicgames.com/admin [403]
https://caldera-service-prod.ecosec.on.epicgames.com/admin [404]
https://launcher.store.epicgames.com/admin [403]
https://nelly-service-prod-cloudflare.ecosec.on.epicgames.com/admin [404]
https://installer.ega.ol.epicgames.com/admin [403]
https://merchantpool1.epicgames.com/admin [200]
https://status.epicgames.com/admin [302]
https://talon-website-prod.ak.epicgames.com/admin [404]
https://talon-service-v4-prod.ak.epicgames.com/admin [404]
https://download3.epicgames.com/admin [403]
https://redirect.epicgames.com/admin [200]
https://media-cdn.epicgames.com/admin [403]
https://perf.store.on.epicgames.com/admin [404]
https://download4.epicgames.com/admin [403]
https://talon-service-prod.ak.epicgames.com/admin [404]
https://cdn1.epicgames.com/admin [403]
https://download-test.epicgames.com/admin [403]
https://modules-cdn.eac-prod.on.epicgames.com/admin [403]
https://wex-public-service-live-prod.epic-social-game-overlay-prod-ci.ol.epicgames.com/admin [403]
https://epic-social-game-overlay-prod.ol.epicgames.com/admin [403]
https://epic-social-social-modules-prod.ol.epicgames.com/admin [403]
https://unrealstudio.epicgames.com/admin [403]
https://cdn2.epicgames.com/admin [403]
https://fortnite-island-screenshots-live-cdn.ol.epicgames.com/admin [403]
https://fn-hotconfigs.ogs.live.on.epicgames.com/admin [403]
https://accf5076e09d.epic-social-game-overlay-prod-ci.ol.epicgames.com/admin [403]
https://cdn-0001.qstv.on.epicgames.com/admin [403]
https://0a4b53775655.epic-social-game-overlay-prod-ci.ol.epicgames.com/admin [403]
https://modules-cdn.eac-gamedev.on.epicgames.com/admin [403]
https://static-assets-prod.epicgames.com/admin [403]
https://jira.epicgames.com/admin [403]
```

Observamos que algunos subdominios responden a esta ruta, lo que sugiere que el directorio 'admin' está presente y podría representar un punto de vulnerabilidad. Para conservar estos hallazgos para una revisión futura, ejecutaremos el mismo comando pero redireccionando la salida a un archivo:

```
cat subdominios_targets.txt | httpx -path=admin -status-code >
httpx_admin_subdominios.txt
```

Con este procedimiento, obtendremos un archivo que registra los subdominios que tienen un directorio 'admin' accesible, lo cual podría ser crucial para las fases subsiguientes de nuestra evaluación de seguridad.

3.4 GOWITNESS

En la fase de recopilación de información, es crucial explorar visualmente los sitios web que estamos analizando, ya que algunos podrían contener paneles administrativos o elementos interesantes que podrían ser de relevancia para un posterior análisis de vulnerabilidades.

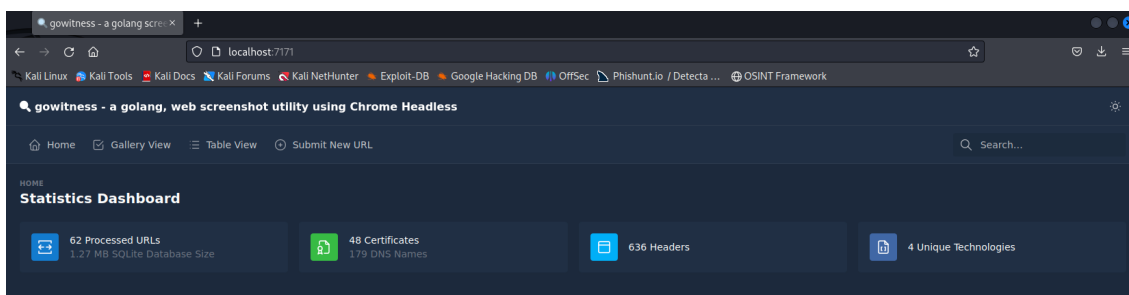
Utilizamos GoWitness para visitar diferentes subdominios, realizar capturas de pantalla, y almacenarlas localmente. Utilizaremos el siguiente comando:

```
gowitness file -f subdominios_targets.txt
```

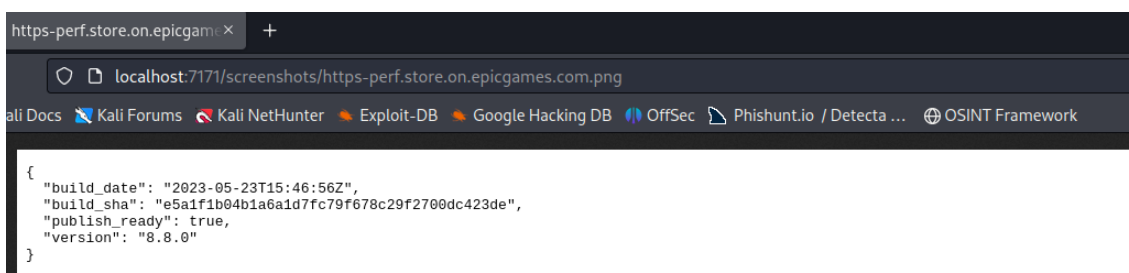
GoWitness crea una carpeta de capturas de pantalla donde almacena las imágenes de los subdominios visitados. Para revisar estas capturas y obtener un informe detallado, ejecutamos:

```
gowitness report serve
```

Este comando inicia un servidor local donde se pueden revisar las capturas junto con un informe. Copiando el enlace al localhost proporcionado, accedemos a una interfaz que presenta las capturas y detalles asociados.



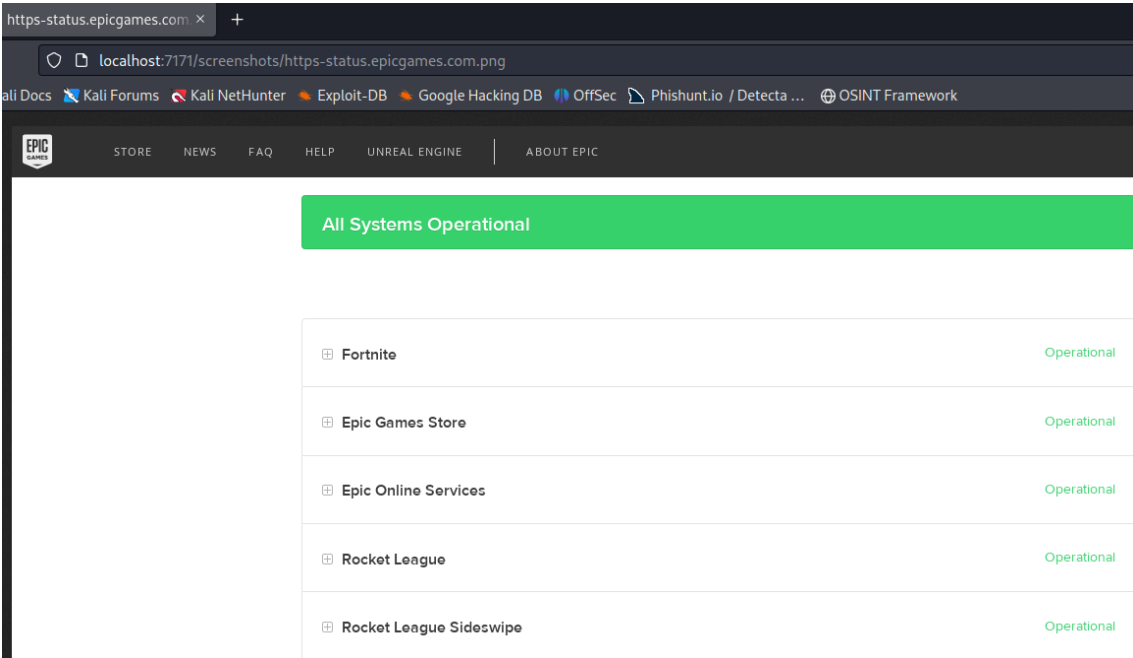
Tras revisar las capturas, identificamos varios puntos de interés para un análisis de vulnerabilidades posterior:



En una captura, encontramos un JSON expuesto que detalla la construcción de una encriptación SHA. Este hallazgo pique nuestra curiosidad y podría ser relevante

explorar por qué esta información se encuentra expuesta durante la fase de reconocimiento.

La exposición de mecanismos de encriptación podría indicar configuraciones inseguras o la posibilidad de explotar debilidades criptográficas.



En otro dominio, las capturas revelan todos los servicios operativos que componen Epic Games, proporcionando una visualización de los servicios activos en ese momento.

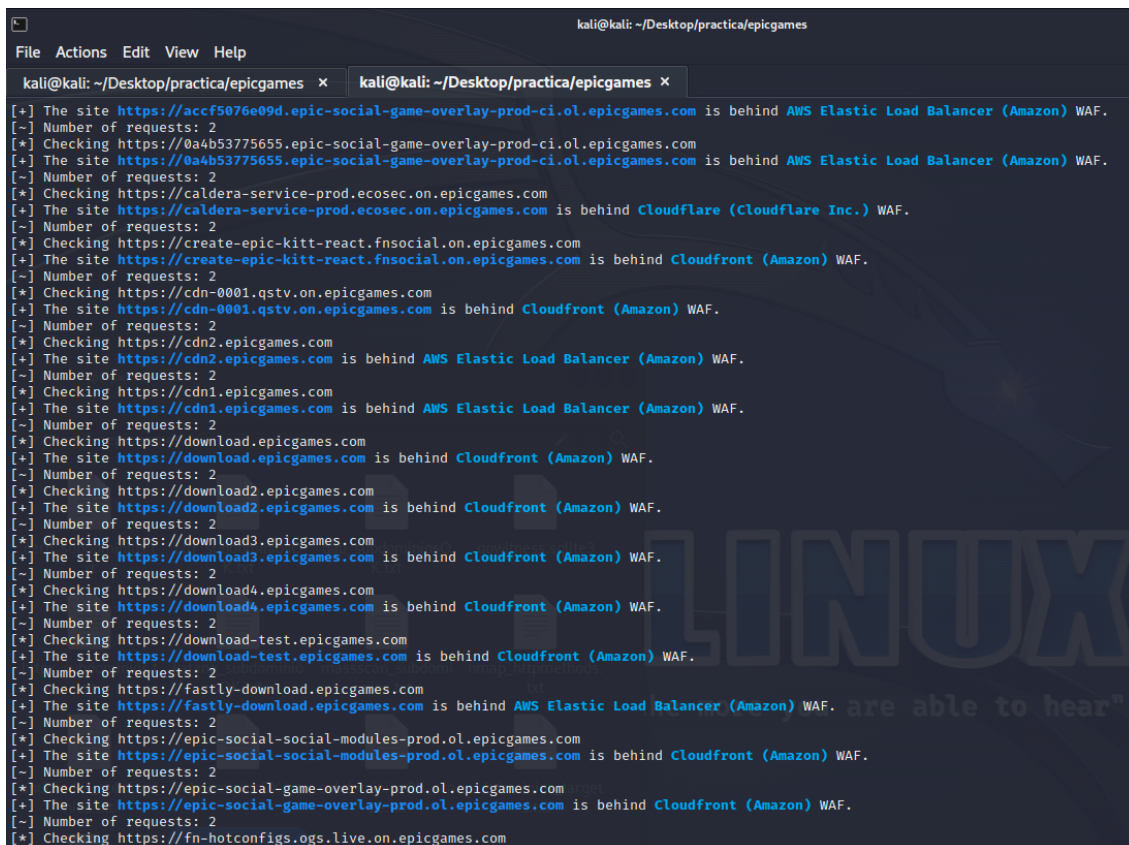
Este dominio podría ser un punto de entrada valioso para entender la infraestructura de la red y los servicios en ejecución, lo que es crucial para planificar etapas posteriores de pruebas de penetración.

3.5 WAFWOOF

Utilizando la herramienta WafWoof, aspiramos a identificar el Web Application Firewall (WAF) que protege los subdominios en los que estamos enfocados. El comando adecuado para ejecutar esta herramienta será proporcionado a continuación:

```
wafw00f -i subdominios_targets.txt -o > wafwoof_subdominios.txt
```

Una visualización rápida del resultado:



```
kali@kali: ~/Desktop/practica/epicgames
File Actions Edit View Help
kali@kali: ~/Desktop/practica/epicgames x kali@kali: ~/Desktop/practica/epicgames x
[+] The site https://accf5076e09d.epic-social-game-overlay-prod-ci.ol.epicgames.com is behind AWS Elastic Load Balancer (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://0a4b53775655.epic-social-game-overlay-prod-ci.ol.epicgames.com
[+] The site https://0a4b53775655.epic-social-game-overlay-prod-ci.ol.epicgames.com is behind AWS Elastic Load Balancer (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://caldera-service-prod.ecosec.on.epicgames.com
[+] The site https://caldera-service-prod.ecosec.on.epicgames.com is behind Cloudflare (Cloudflare Inc.) WAF.
[-] Number of requests: 2
[*] Checking https://create-epic-kitt-react.fnsocial.on.epicgames.com
[+] The site https://create-epic-kitt-react.fnsocial.on.epicgames.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://cdn-0001.qstv.on.epicgames.com
[+] The site https://cdn-0001.qstv.on.epicgames.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://cdn2.epicgames.com
[+] The site https://cdn2.epicgames.com is behind AWS Elastic Load Balancer (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://cdn1.epicgames.com
[+] The site https://cdn1.epicgames.com is behind AWS Elastic Load Balancer (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://download.epicgames.com
[+] The site https://download.epicgames.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://download2.epicgames.com
[+] The site https://download2.epicgames.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://download3.epicgames.com
[+] The site https://download3.epicgames.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://download4.epicgames.com
[+] The site https://download4.epicgames.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://download-test.epicgames.com
[+] The site https://download-test.epicgames.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://fastly-download.epicgames.com
[+] The site https://fastly-download.epicgames.com is behind AWS Elastic Load Balancer (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://epic-social-social-modules-prod.ol.epicgames.com
[+] The site https://epic-social-social-modules-prod.ol.epicgames.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://epic-social-game-overlay-prod.ol.epicgames.com
[+] The site https://epic-social-game-overlay-prod.ol.epicgames.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://fn-hotconfigs.ogs.live.on.epicgames.com
```

En el ejemplo simplificado de los resultados que se presentan, observamos que se utilizan hasta tres diferentes firewalls para salvaguardar sus dominios, a saber:

- AWS Elastic Load Balancer (Amazon)
- Cloudflare (Cloudflare Inc.)
- Cloudfront (Amazon)

Esta distribución de WAFs es peculiar; comúnmente, la protección se canaliza a través de una sola plataforma, no de tres distintas.

3.6 FFUF

FFUF (Fuzz Faster U Fool) es una herramienta poderosa y eficaz para el descubrimiento de contenido web. Mediante el empleo de listas de palabras especificadas, ffuf efectúa múltiples solicitudes al sitio web, proporcionando un reflejo detallado de las respuestas obtenidas.

Para usar esta herramienta, utilizaremos el siguiente comando:

```
ffuf -w common.txt -t 5 -mc 200 -u https://store.epicgames.com/FUZZ >
ffuf_subdominios.txt
```

El comando inicial que se proporcionó tenía como objetivo analizar una URL específica. Sin embargo, los resultados no fueron los esperados.

Posteriormente, se elaboró un script para automatizar el proceso de análisis en múltiples subdominios. Este script recorre cada subdominio listado en el archivo **subdominios_targets.txt**, y ejecuta ffuf en cada uno de ellos.

El script, una vez otorgados los permisos de ejecución, se ejecuta y los resultados se almacenan en el archivo **ffuf_subdominios.txt**. Esta automatización es crucial para economizar tiempo y esfuerzos en el proceso de análisis.

```
#!/bin/bash

# Leer cada línea del archivo subdominios_targets.txt
while IFS= read -r subdomain
do
    # Ejecutar ffuf en cada subdominio
    ffuf -w common.txt -t 5 -mc 200 -u "http://$subdomain/FUZZ" >>
    ffuf_subdominios.txt
done < subdominios_targets.txt

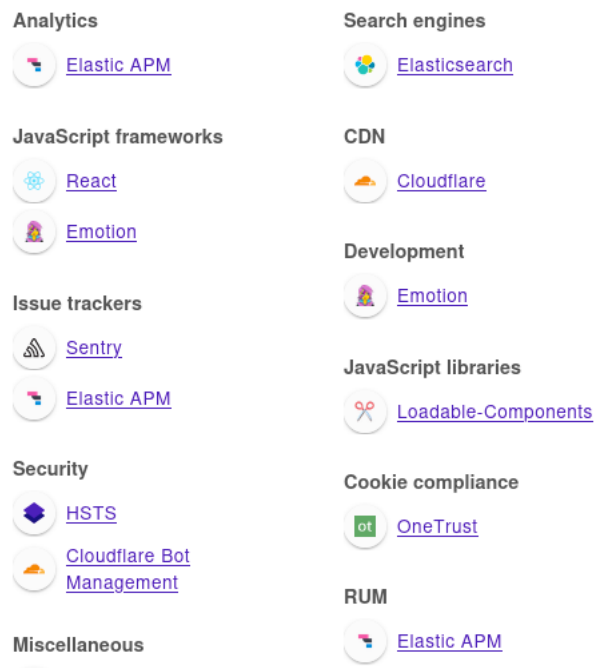
# Dar permisos de ejecución
chmod +x ffuf_script.sh

# Ejecutar el script
./ffuf_script.sh
```

Tras la ejecución del script, se identificaron algunos directorios que podrían ser de interés para un análisis de vulnerabilidades posterior, incluyendo los directorios **Soap**, **Test**, y **.well-known/http-opportunistic**.

3.7 WAPPALYZER

Wappalyzer es una herramienta valiosa que permite identificar las tecnologías utilizadas en los sitios web. En el análisis realizado, se han identificado una serie de tecnologías y herramientas que forman parte de la estructura del sitio web en cuestión.



Aquí se proporciona una desglose más detallado y una posible interpretación de los hallazgos:

1. **Analytics:**
 - **Elastic APM:** Una aplicación de monitoreo de desempeño que proporciona detalles sobre errores, latencias y otros datos relevantes que pueden ayudar a optimizar el desempeño del sitio web.
2. **Search Engines:**
 - **ElasticSearch:** Un motor de búsqueda y analítica basado en RESTful que mejora las capacidades de búsqueda en el sitio web.
3. **Javascript Frameworks:**
 - **React:** Una biblioteca de JavaScript para construir interfaces de usuario, que proporciona una experiencia de usuario fluida y eficiente.
 - **Emotion:** Una librería performante y flexible de styled-components para diseñar aplicaciones.
4. **CDN:**
 - **Cloudflare:** Una red de entrega de contenido que mejora la velocidad de carga y la seguridad del sitio web.

5. **Development:**

- **Emotion:** Como se mencionó anteriormente, es una librería que ayuda a estilizar aplicaciones de manera eficaz.

6. **Issue Trackers:**

- **Sentry:** Una plataforma de monitoreo de errores y seguimiento de problemas que ayuda a identificar y resolver problemas rápidamente.
- **Elastic APM:** También funciona como una herramienta de seguimiento de errores y problemas.

7. **Javascript Libraries:**

- **Loadable Components:** Una biblioteca que permite la carga diferida de componentes en aplicaciones React, lo que puede ayudar a mejorar el desempeño de la página.

8. **Security:**

- **HSTS (HTTP Strict Transport Security):** Un mecanismo web que protege contra ataques man-in-the-middle mediante la forzada del uso de HTTPS.
- **Cloudflare Bot Management:** Una solución que protege el sitio web contra bots maliciosos.

9. **Cookie Compliance:**

- **OneTrust:** Una plataforma que ayuda a gestionar el cumplimiento de normativas sobre cookies y privacidad.

10. **RUM (Real User Monitoring):**

- **Elastic APM:** También proporciona monitoreo en tiempo real de la experiencia del usuario.

La diversidad de tecnologías identificadas refleja una estructura web robusta y moderna. Herramientas como Elastic APM y Cloudflare no sólo mejoran la experiencia del usuario sino que también contribuyen a la seguridad y la eficiencia operativa del sitio web.

Sin embargo, cada tecnología podría tener configuraciones específicas o vulnerabilidades inherentes que podrían ser explotadas si no están adecuadamente configuradas o actualizadas.

Por lo tanto, es esencial tener un conocimiento profundo de estas tecnologías y mantenerlas actualizadas para asegurar una operación segura y eficaz del sitio web.

3.8 WHATWEB

La herramienta WhatWeb es una herramienta de fingerprinting de servidores web que identifica tecnologías web, servidores, plataformas, software, frameworks, plugins, analítica, y más.

Al ejecutar el siguiente comando, WhatWeb escaneará cada dominio listado en el archivo **subdominios_targets.txt**, y generará un archivo de salida llamado **whatweb_subdominios.txt** que contendrá la información recopilada sobre cada dominio.

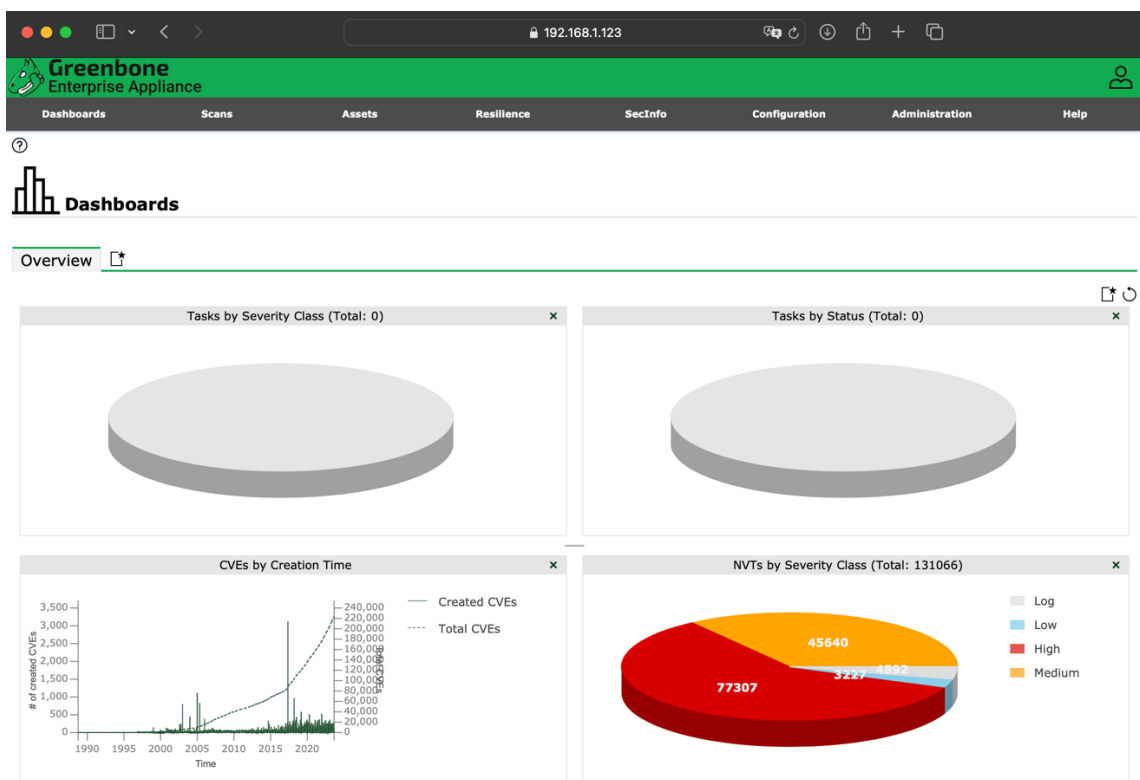
```
whatweb -i subdominios_targets.txt > whatweb_subdominios.txt
```

El resultado de la herramienta se adjuntará como archivo en la entrega de la práctica.

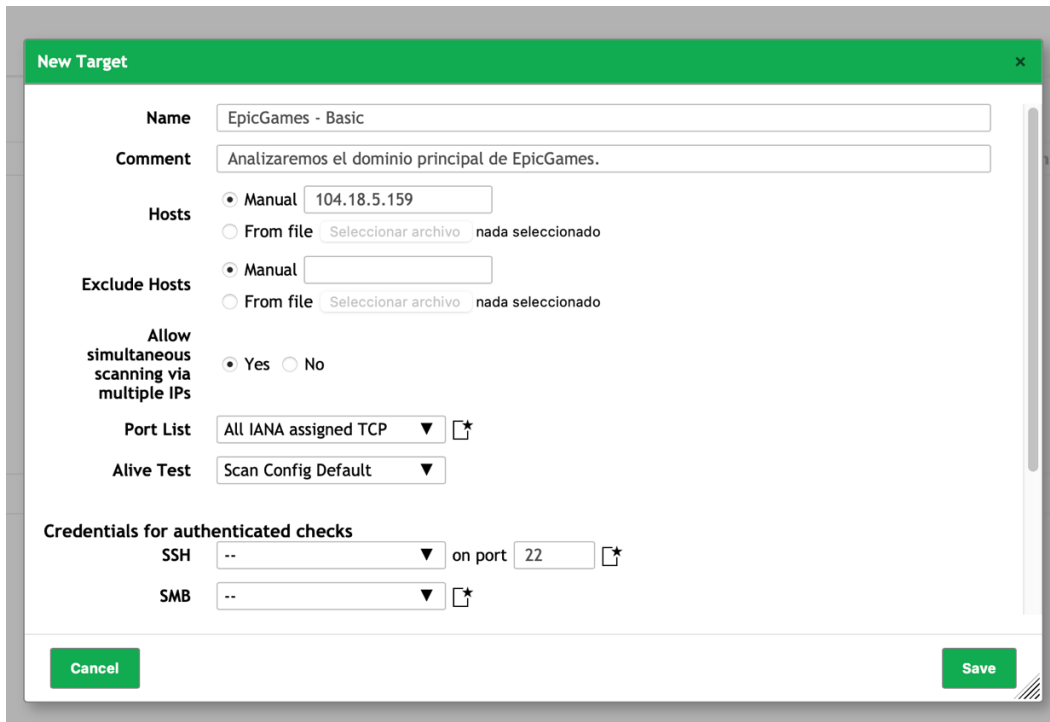
4. ANÁLISIS DE VULNERABILIDADES

4.1 GREENBONE

Procedemos ahora a la fase de análisis de vulnerabilidades, para la cual estableceremos nuestro propio servidor mediante Greenbone. Para ello, descargaremos una máquina virtual, la inicializaremos y, si todo se configura correctamente, deberíamos visualizar la siguiente pantalla:



Posteriormente, definiremos un objetivo, que en este caso será el dominio principal de Epic Games: store.epicgames.com.

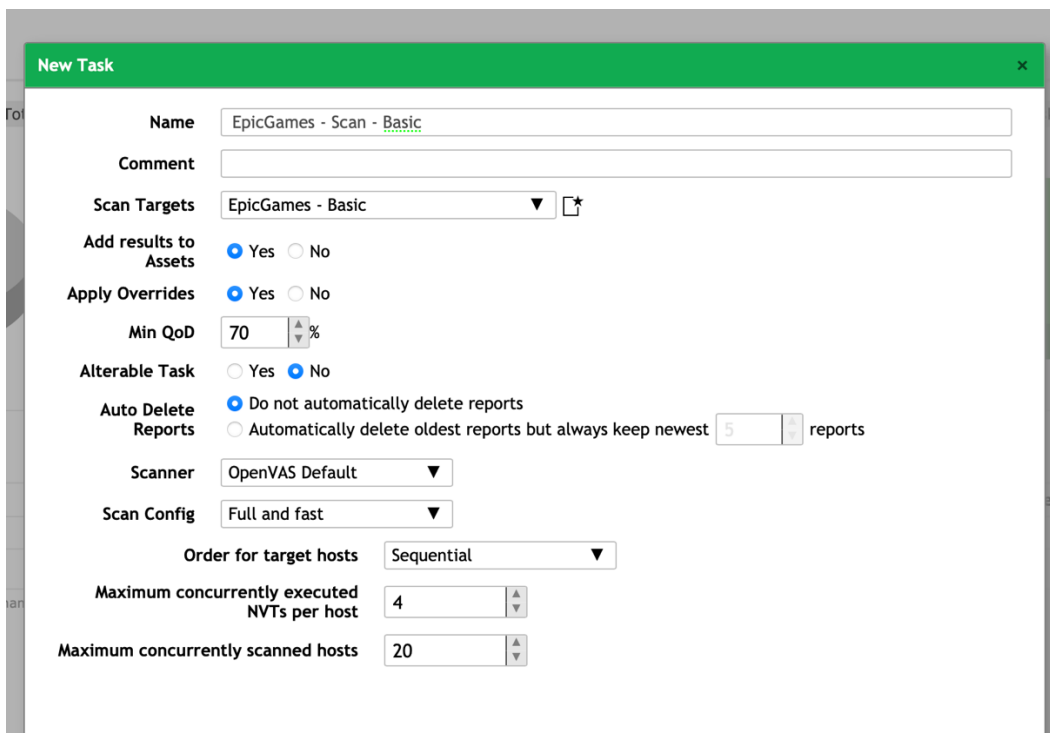


The 'New Target' dialog box is shown with the following configuration:

- Name:** EpicGames - Basic
- Comment:** Analizaremos el dominio principal de EpicGames.
- Hosts:** Manual (104.18.5.159)
- Exclude Hosts:** Manual
- Allow simultaneous scanning via multiple IPs:** Yes
- Port List:** All IANA assigned TCP
- Alive Test:** Scan Config Default
- Credentials for authenticated checks:**
 - SSH: -- on port 22
 - SMB: --

Buttons: Cancel, Save

Una vez establecido el objetivo, procederemos a crear una nueva tarea asociada a este. La configuración de la tarea incluirá la identificación del objetivo previamente definido, lo cual permitirá a Greenbone efectuar un análisis exhaustivo de las vulnerabilidades presentes en el dominio especificado.



The 'New Task' dialog box is shown with the following configuration:

- Name:** EpicGames - Scan - Basic
- Comment:**
- Scan Targets:** EpicGames - Basic
- Add results to Assets:** Yes
- Apply Overrides:** Yes
- Min QoD:** 70 %
- Alterable Task:** No
- Auto Delete Reports:** Do not automatically delete reports
- Scanner:** OpenVAS Default
- Scan Config:** Full and fast
- Order for target hosts:** Sequential
- Maximum concurrently executed NVTs per host:** 4
- Maximum concurrently scanned hosts:** 20

Greenbone Enterprise Appliance

Dashboards
Scans
Assets
Resilience
SecInfo

Report:Sun, Oct 15, 2023 5:52 PM UTC
ID: 4a247ed3-f7e...

Information	Results <small>(2 of 191)</small>	Hosts <small>(2 of 2)</small>	Ports <small>(0 of 13)</small>	Applications <small>(0 of 0)</small>	Operating Systems <small>(1 of 1)</small>	CVEs <small>(0 of 0)</small>	Closed CVEs <small>(0 of 0)</small>	TLS Certificates <small>(0 of 0)</small>	Error Messages <small>(13 of 13)</small>	User Tags <small>(0)</small>
Task Name	EpicGames - Scan - Basic									
Scan Time	Sun, Oct 15, 2023 5:53 PM UTC - Sun, Oct 15, 2023 8:38 PM UTC									
Scan Duration	2:45 h									
Scan Status	Done									
Hosts scanned	2									
Filter	apply_overrides=0 levels=hml min_qod=70									
Timezone	Coordinated Universal Time (UTC)									

Greenbone

Enterprise Appliance

Dashboard

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

🏠

🔍

📄

🔗

🔧

🔒

🔑

Host: 104.18.5.159

ID: 69923ee7-476d-4c4c-924c-506913e1eeaf Created: Sun, Oct 15, 2023 8:37 PM UTC Modified: Sun, Oct 15, 2023 8:38 PM UTC Owner: kai

Information

User Tags

Permissions

Hostname

store.epicgames.com

IP Address

104.18.5.159

Comment

OS

Linux Kernel

192.168.1.123 ▶ 192.168.144.1 ▶ 81.41.225.197 ▶ 81.41.226.30 ▶ 81.46.0.213 ▶ 216.184.113.182 ▶ 81.173.106.39 ▶ 188.114.108.7 ▶ 104.18.5.159

Route

Severity

2.0 (Low)

All Identifiers

Name	Value	Created	Source	Actions
OS	cpe:/o:linux:kernel	Sun, Oct 15, 2023 8:38 PM UTC	Report 4a247ed3-f7e4-49c7-a96f-ae97b8f0ebaa (NVT 1.3.6.1.4.1.25623.1.0.102002)	✕
hostname	store.epicgames.com	Sun, Oct 15, 2023 8:38 PM UTC	Report 4a247ed3-f7e4-49c7-a96f-ae97b8f0ebaa (NVT 1.3.6.1.4.1.25623.1.0.103997)	✕
ip	104.18.5.159	Sun, Oct 15, 2023 8:37 PM UTC	Report 4a247ed3-f7e4-49c7-a96f-ae97b8f0ebaa (Target Host)	✕

Greenbone

Enterprise Appliance

Dashboard

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

🏠

🔍

📄

🔗

🔧

🔒

🔑

Host: 104.18.4.159

ID: 13000f95-e765-4347-a622-62bf17367067 Created: Sun, Oct 15, 2023 8:38 PM UTC Modified: Sun, Oct 15, 2023 8:38 PM UTC Owner: kai

Information

User Tags

Permissions

Hostname

store.epicgames.com

IP Address

104.18.4.159

Comment

OS

Linux Kernel

192.168.1.123 ▶ 192.168.144.1 ▶ 81.41.225.197 ▶ 81.46.0.213 ▶ 216.184.113.248 ▶ 81.173.106.39 ▶ 172.70.56.3 ▶ 104.18.4.159

Route

Severity

2.0 (Low)

All Identifiers

Name	Value	Created	Source	Actions
OS	cpe:/o:linux:kernel	Sun, Oct 15, 2023 8:38 PM UTC	Report 4a247ed3-f7e4-49c7-a96f-ae97b8f0ebaa (NVT 1.3.6.1.4.1.25623.1.0.102002)	✕
hostname	store.epicgames.com	Sun, Oct 15, 2023 8:38 PM UTC	Report 4a247ed3-f7e4-49c7-a96f-ae97b8f0ebaa (NVT 1.3.6.1.4.1.25623.1.0.103997)	✕
ip	104.18.4.159	Sun, Oct 15, 2023 8:38 PM UTC	Report 4a247ed3-f7e4-49c7-a96f-ae97b8f0ebaa (Target Host)	✕

El nivel de severidad 2.6, categorizado como bajo, sugiere que las vulnerabilidades identificadas no representan una amenaza inmediata o crítica para la integridad y seguridad del dominio. Sin embargo, es prudente tomar medidas correctivas para resolver estas vulnerabilidades y mejorar la postura de seguridad del sitio web.

Es recomendable que se realice un análisis adicional con otras herramientas de evaluación de vulnerabilidades o se considere la posibilidad de contratar a un profesional en seguridad de la información para una evaluación más exhaustiva.

4.2 NUCLEI

En esta etapa del análisis, hemos empleado la herramienta Nuclei para examinar el dominio principal de Epic Games en busca de vulnerabilidades potenciales. Nuclei es una herramienta robusta que facilita la identificación de vulnerabilidades en los dominios proporcionados. Para ejecutar el análisis, hemos utilizado el siguiente comando:

```
nuclei -u store.epicgames.com > nuclei_subdominios.txt
```

Se generará un registro detallado del análisis realizado por Nuclei, el cual se conservará en el archivo **nuclei_subdominios.txt**. Este archivo será adjuntado junto con la práctica para una revisión más detenida.

Tras revisar el contenido generado por Nuclei, se concluyó que no hay hallazgos reseñables en esta instancia. Esto sugiere que el dominio principal de Epic Games no presenta vulnerabilidades evidentes o críticas según las definiciones y firmas de vulnerabilidad con las que cuenta la herramienta Nuclei.

```
(kali@kali)-[~/Desktop/practica/epicgames]
$ cat nuclei_subdominios.txt
[dns-saas-service-detection] [dns] [info] store.epicgames.com [store-weighted-cdn.epicgames.com.]
[addeventlistener-detect] [http] [info] https://store.epicgames.com
[google-floc-disabled] [http] [info] https://store.epicgames.com
[httponly-cookie-detect] [http] [info] https://store.epicgames.com
[tech-detect:cloudflare] [http] [info] https://store.epicgames.com
[http-missing-security-headers:strict-transport-security] [http] [info] https://store.epicgames.com
[http-missing-security-headers:content-security-policy] [http] [info] https://store.epicgames.com
[http-missing-security-headers:x-content-type-options] [http] [info] https://store.epicgames.com
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://store.epicgames.com
[http-missing-security-headers:clear-site-data] [http] [info] https://store.epicgames.com
[graphql-field-suggestion] [http] [info] https://store.epicgames.com/graphql
[graphql-get-method] [http] [info] https://store.epicgames.com/graphql?query={__typename}
[graphql-alias-batching] [http] [info] https://store.epicgames.com/graphql
[apollo-server-detect] [http] [info] https://store.epicgames.com/graphql
[waf-detect:cloudflare] [http] [info] https://store.epicgames.com/
[ssl-issuer] [ssl] [info] store.epicgames.com:443 [Cloudflare, Inc.]
[ssl-dns-names] [ssl] [info] store.epicgames.com:443 [sni.cloudflaressl.com,store.epicgames.com]
[tls-version] [ssl] [info] store.epicgames.com:443 [tls12]
[tls-version] [ssl] [info] store.epicgames.com:443 [tls13]
```

Aunque no se identificaron problemas notables en esta pasada, es esencial recordar que ningún análisis de vulnerabilidades es exhaustivo. Las amenazas y las vulnerabilidades evolucionan constantemente, y lo que es seguro hoy puede no serlo mañana.

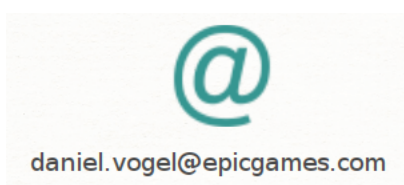
5. OSINT

Al continuar con el proceso de Recolección de Información de Fuentes Abiertas (OSINT, por sus siglas en inglés), hemos empleado la herramienta Maltego. Una vez instalada, Maltego nos permite realizar una exploración profunda basada en el dominio

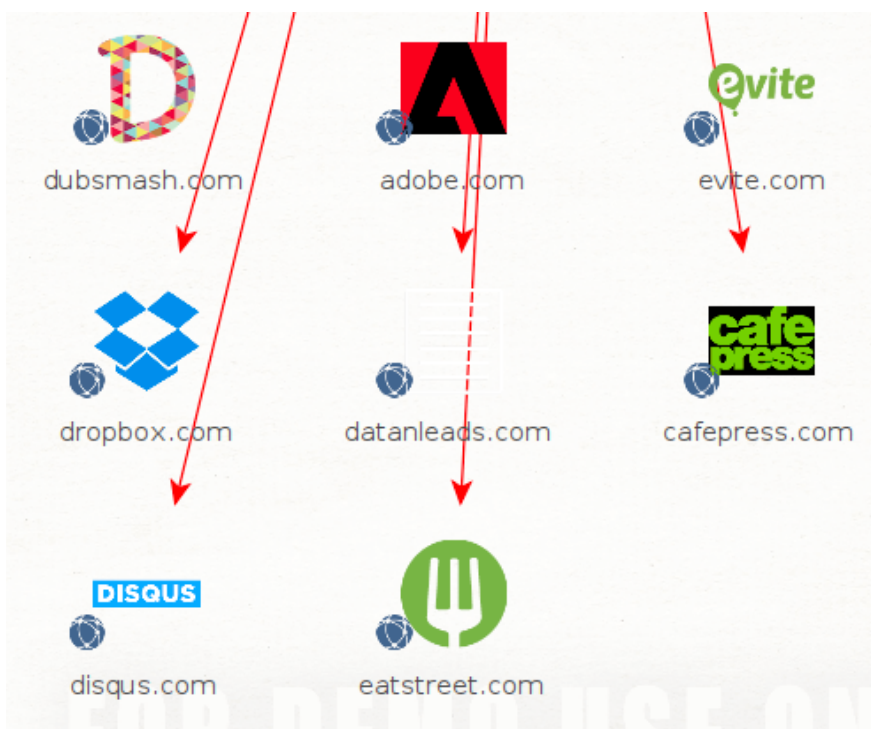
proporcionado, facilitando la recolección de información valiosa tanto de la empresa como de los empleados asociados a ella.

Después de ejecutar el escaneo con Maltego, hemos identificado varios usuarios y correos electrónicos asociados a la empresa Epic Games. Para cada uno de estos elementos, hemos aplicado el transformador "I Have Been Pwned" para investigar si existen registros de estos correos electrónicos en bases de datos de filtraciones pasadas.

Un usuario en particular, identificado como **daniel.vogel@epicgames.com**, ha llamado nuestra atención, ya que aparece en varias filtraciones de datos.



A continuación, se detallan los sitios donde se ha encontrado este correo electrónico, y que en el pasado fueron comprometidos:



Con el propósito de profundizar en la investigación, hemos realizado una búsqueda rápida sobre el usuario en la plataforma X.



Cabe mencionar que el proceso OSINT es una práctica valiosa que puede revelar datos sensibles y potencialmente comprometedores. La información obtenida puede ser utilizada para fortalecer las estrategias de seguridad y para entender mejor el perfil de riesgo de una organización.

En la práctica se adjuntará un archivo con el mapa realizado a la empresa Epic Games.

6. CONCLUSIÓN

A lo largo del desarrollo de este informe, hemos navegado por el fascinante de la Recopilación de Información (OSINT), intentando desentrañando el gigante dominio digital de Epic Games. El ejercicio ha sido tanto educativo como formador, proporcionando una visión detallada de las herramientas y metodologías que pueden ser empleadas para obtener una comprensión profunda de la estructura y seguridad digital de una organización.

Cada herramienta y método utilizado ha contribuido a nuestra comprensión y apreciación del amplio espectro que abarca la Recopilación de Información. Además, los resultados obtenidos han sido esenciales para entender las prácticas actuales de seguridad y cómo estas se interrelacionan en un entorno corporativo real.

Este proyecto ha sido una oportunidad formidable que ha enriquecido nuestro conocimiento y habilidades en el ámbito de la ciberseguridad. Nos ha permitido no solo aprender sobre las herramientas y técnicas de OSINT, sino también comprender la importancia crítica de una robusta postura de seguridad en el mundo digital de hoy.