DNS Brute-Force

DNS Brute-Force es una técnica utilizada para identificar posibles subdominios mediante el envío de múltiples solicitudes DNS con distintos nombres predefinidos.

Como primer paso, se empleará la herramienta **resolvalid** para obtener una lista actualizada de servidores DNS. Los resultados se almacenarán en el archivo resolvers.txt para su posterior uso.

A continuación, se muestra una captura de pantalla durante la ejecución de la herramienta **shuffledns**, utilizando la lista de resolvers obtenida previamente. Su función es verificar qué subdominios existen realmente resolviendo sus registros DNS. Los resultados generados se guardarán en el archivo shuffledns.txt para su posterior análisis.

Google Analytics

Google Analytics es una herramienta ampliamente utilizada por organizaciones para monitorizar el tráfico web y generar estadísticas sobre el comportamiento de los visitantes.

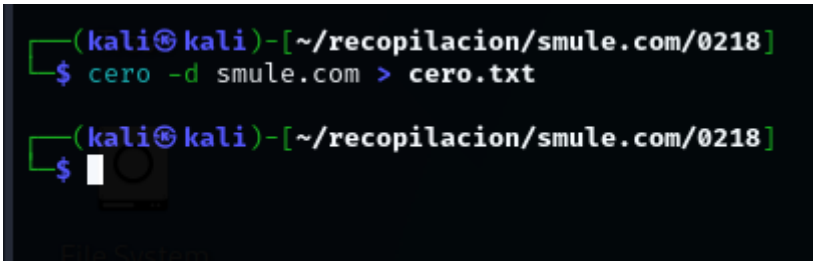
Es posible extraer el identificador de Google Analytics de una página web y utilizarlo para consultar diversas bases de datos con el fin de identificar otros dominios y subdominios asociados al mismo identificador.

A continuación, se muestra una captura de pantalla durante la ejecución de la herramienta **analyticsrelationships** utilizada para este propósito. Como se puede observar, la herramienta no devuelve resultados, lo que indica que el sitio web examinado no utiliza Google Analytics.

TLS Probing

TLS Probing es el proceso de análisis de la configuración y seguridad de un servicio que utiliza el protocolo Transport Layer Security (TLS), en algunas ocasiones, los certificados SSL/TLS pueden incluir dominios y subdominios asociados a una organización. Esta información puede ser útil para identificar activos adicionales dentro de una infraestructura.

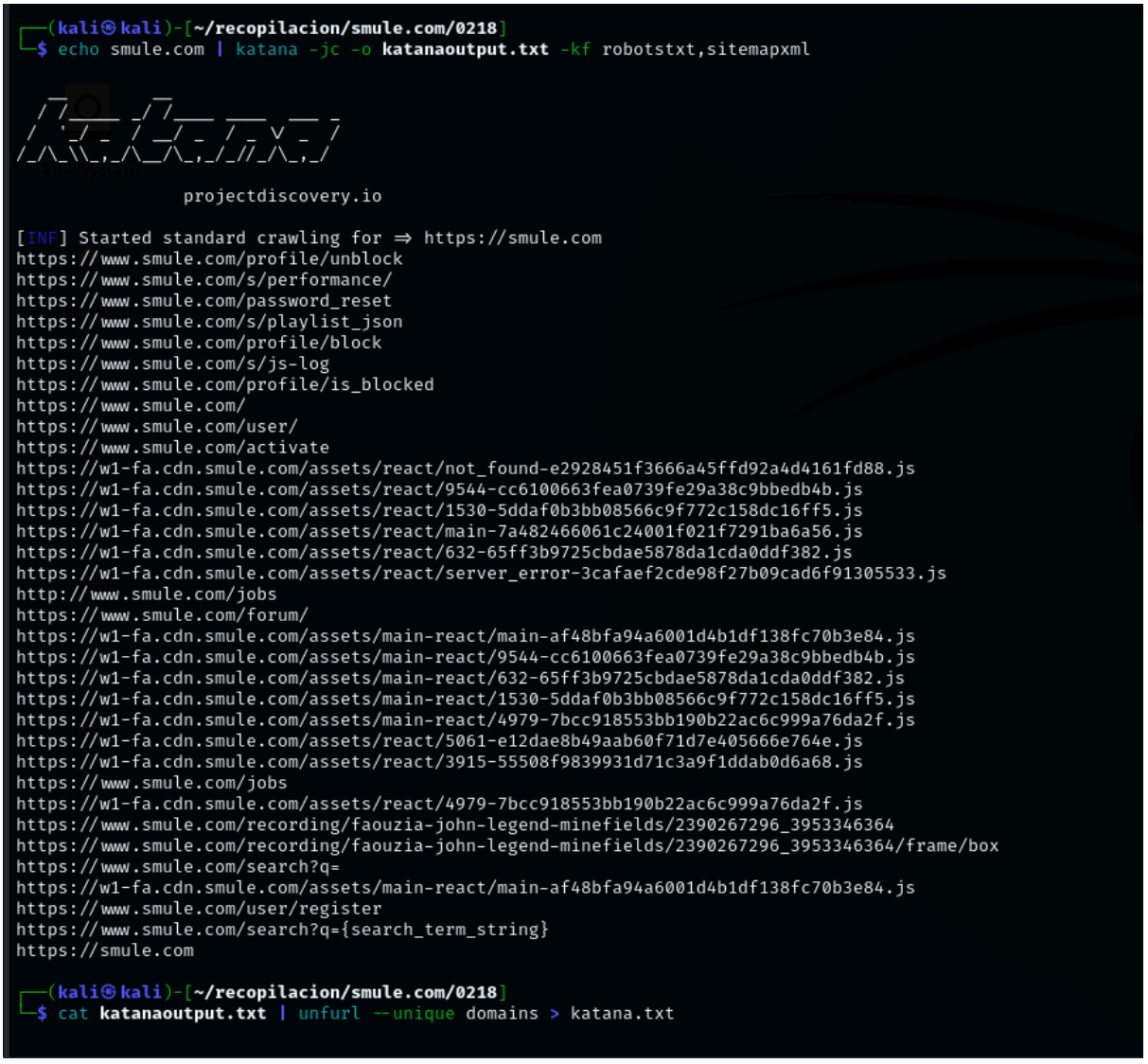
Para llevar a cabo este análisis, se ha utilizado la herramienta **Cero**, que permite extraer y examinar los certificados SSL/TLS en busca de dominios relacionados con la organización. En este caso la herramienta solo ha devuelto el dominio principal, con lo cual esta técnica no ha sido efectiva.



Web Scrapping

Web Scraping es el proceso de extracción automatizada de información de sitios web. Su objetivo es recopilar datos estructurados a partir del contenido de una página web, en este caso, para identificar subdominios.

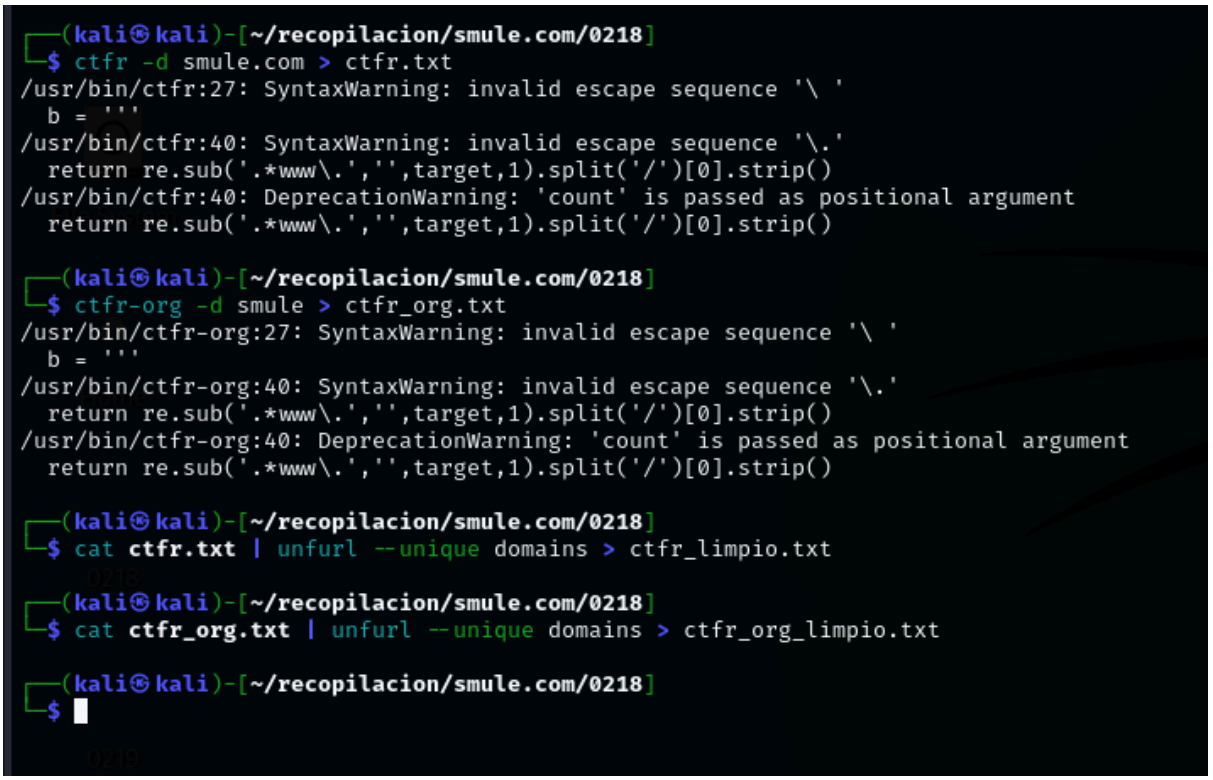
Para este propósito, se ha utilizado la herramienta **Katana**. Los resultados obtenidos se almacenan en el archivo katanaoutput.txt. Posteriormente, mediante el comando **unfurl**, se depuran los datos y se guardan en el archivo katana.txt, donde se puede comprobar que solamente se ha encontrado un subdominio diferente al principal, w1-fa.cdn.smule.com



Certificate Transparency Logs

Los Certificate Transparency Logs son bases de datos públicas y verificables que almacenan certificados SSL/TLS emitidos por autoridades certificadoras. Su objetivo es

detectar certificados maliciosos o emitidos sin autorización. A continuación, se muestra una captura de pantalla durante la ejecución de la herramienta **ctfr**, mediante la cual es posible utilizar estos logs para buscar subdominios asociados a un certificado. Así mismo se ha modificado la herramienta, para que haga una segunda búsqueda mediante el nombre de la organización a la que pertenece el dominio principal. Posteriormente se procede a depurar los archivos obtenidos con el comando **unfurl**, y se comprueba que la técnica ha sido efectiva, ya que ha devuelto nuevos subdominios al analizar el dominio principal.



Archivos web y caché

Wayback Machine es un servicio de archivo web creado por Internet Archive que permite acceder a versiones antiguas de sitios web. Captura y almacena copias de páginas a lo largo del tiempo, permitiendo a los usuarios ver cómo lucían en el pasado. Es útil para recuperar contenido eliminado, analizar cambios históricos y verificar información. Su base de datos contiene miles de millones de páginas archivadas desde 1996. Mediante la herramienta **gau** se van a analizar todas las URL indexadas del dominio smule.com en Wayback Machine. Una vez más se depurarán los resultados con el comando **unfurl**.

```
┌──(kali㉿kali)-[~/recopilacion/smule.com/0218]
└─$ gau --threads 5 smule.com --o gauoutput.txt
WARN[0000] error reading config: Config file /home/kali/.gau.toml not found, using default config

┌──(kali㉿kali)-[~/recopilacion/smule.com/0218]
└─$ cat gauoutput.txt | unfurl --unique domains > gau.txt

┌──(kali㉿kali)-[~/recopilacion/smule.com/0218]
└─$ 
```

```
┌──(kali㉿kali)-[~/recopilacion/smule.com/0218]
└─$ cat analytics.txt cero.txt katana.txt shuffledns.txt gau.txt ctfr_org_limpio.txt ctfr_limpio.txt > subdominios.txt

┌──(kali㉿kali)-[~/recopilacion/smule.com/0218]
└─$ 
```

```
┌──(kali㉿kali)-[~/recopilacion/smule.com/0218]
└─$ cat subdominios.txt | alterx | dnsx > alterx.txt
   ___   ____          ____  __
  / _ | / / /____ ____/ __ \/ /
 / __ |/ / __/ -_) __/>  <
/_/ |_/_/\__/\__/_/  /_/|_|

                projectdiscovery.io

         __         __  __
     ___/ /___  ___ \ \/ /
    / _  / _ \(_-<  >  <
   (_,_/_//_/___/_/\_\

                projectdiscovery.io

[INF] Current alterx version v0.0.4 (outdated)
[INF] Generated 70638 permutations in 0.0823s
```