

## 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.

```
(kali@kali)-[~]
$ cd recopilacion

(kali@kali)-[~/recopilacion]
$ cd lists

(kali@kali)-[~/recopilacion/lists]
$ resolvalid -o resolvers.txt
No DNS server source file or URL provided. Using default public DNS list.
Checking 474 of 62790 DNS servers. Results: 138 valid - 336 non-valid DNS servers. 0.75% completed.
```

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.

```
(kali@kali)-[~/recopilacion/smule.com/0218]
$ shuffledns -mode bruteforce -d smule.com -w /home/kali/recopilacion/lists/domains.txt -r /home/kali/recopilacion/lists/resolvers.txt -silent > shuffledns.txt

(kali@kali)-[~/recopilacion/smule.com/0218]
$
```

## 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.

```
(kali@kali)-[~/recopilacion/smule.com/0218]
$ analyticsrelationships --url https://www.smule.com > analytics.txt
/usr/bin/analyticsrelationships:34: SyntaxWarning: invalid escape sequence '\d'
  pattern = "UA-\d+-\d+"
/usr/bin/analyticsrelationships:47: SyntaxWarning: invalid escape sequence '\.'
  pattern = "(www\.(googletagmanager\.(com/ns\.(html\?id=[A-Z0-9\-\_]+))"
/usr/bin/analyticsrelationships:49: SyntaxWarning: invalid escape sequence '\d'
  pattern3 = "UA-\d+-\d+"
/usr/bin/analyticsrelationships:78: SyntaxWarning: invalid escape sequence '\-'
  pattern = "/relationships/[a-z0-9\-\_\.]+\.[a-z]+"

UA-ID
DOMAINS

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

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

(kali@kali)-[~/recopilacion/smule.com/0218]
$
```

## 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.

```
(kali@kali)-[~/recopilacion/smule.com/0218]
$ cero -d smule.com > cero.txt

(kali@kali)-[~/recopilacion/smule.com/0218]
$
```

## Web Scrapping

Web Scrapping 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`

```
(kali@kali)-[~/recopilacion/smule.com/0218]
$ echo smule.com | katana -jc -o katanaoutput.txt -kf robotstxt,sitemapxml

projectdiscovery.io

[INF] Started standard crawling for => https://smule.com
https://www.smule.com/profile/unblock
https://www.smule.com/s/performance/
https://www.smule.com/password_reset
https://www.smule.com/s/playlist_json
https://www.smule.com/profile/block
https://www.smule.com/s/js-log
https://www.smule.com/profile/is_blocked
https://www.smule.com/
https://www.smule.com/user/
https://www.smule.com/activate
https://w1-fa.cdn.smule.com/assets/react/not_found-e2928451f3666a45ffd92a4d4161fd88.js
https://w1-fa.cdn.smule.com/assets/react/9544-cc6100663fea0739fe29a38c9bbdb4b.js
https://w1-fa.cdn.smule.com/assets/react/1530-5ddaf0b3bb08566c9f772c158dc16ff5.js
https://w1-fa.cdn.smule.com/assets/react/main-7a482466061c24001f021f7291ba6a56.js
https://w1-fa.cdn.smule.com/assets/react/632-65ff3b9725cbdae5878da1cda0ddf382.js
https://w1-fa.cdn.smule.com/assets/react/server_error-3cafaef2cde98f27b09cad6f91305533.js
http://www.smule.com/jobs
https://www.smule.com/forum/
https://w1-fa.cdn.smule.com/assets/main-react/main-af48bfa94a6001d4b1df138fc70b3e84.js
https://w1-fa.cdn.smule.com/assets/main-react/9544-cc6100663fea0739fe29a38c9bbdb4b.js
https://w1-fa.cdn.smule.com/assets/main-react/632-65ff3b9725cbdae5878da1cda0ddf382.js
https://w1-fa.cdn.smule.com/assets/main-react/1530-5ddaf0b3bb08566c9f772c158dc16ff5.js
https://w1-fa.cdn.smule.com/assets/main-react/4979-7bcc918553bb190b22ac6c999a76da2f.js
https://w1-fa.cdn.smule.com/assets/react/5061-e12dae8b49aab60f71d7e405666e764e.js
https://w1-fa.cdn.smule.com/assets/react/3915-55508f9839931d71c3a9f1ddab0d6a68.js
https://www.smule.com/jobs
https://w1-fa.cdn.smule.com/assets/react/4979-7bcc918553bb190b22ac6c999a76da2f.js
https://www.smule.com/recording/faouzia-john-legend-minefields/2390267296_3953346364
https://www.smule.com/recording/faouzia-john-legend-minefields/2390267296_3953346364/frame/box
https://www.smule.com/search?q=
https://w1-fa.cdn.smule.com/assets/main-react/main-af48bfa94a6001d4b1df138fc70b3e84.js
https://www.smule.com/user/register
https://www.smule.com/search?q={search_term_string}
https://smule.com

(kali@kali)-[~/recopilacion/smule.com/0218]
$ cat katanaoutput.txt | unfurl --unique domains > katana.txt
```

## 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.

```
(kali㉿kali)-[~/recopilacion/smule.com/0218]
$ ctfr -d smule.com > ctfr.txt
/usr/bin/ctfr:27: SyntaxWarning: invalid escape sequence '\ '
  b = ''
/usr/bin/ctfr:40: SyntaxWarning: invalid escape sequence '\.'
  return re.sub('.*www\.', '', target, 1).split('/')[0].strip()
/usr/bin/ctfr:40: DeprecationWarning: 'count' is passed as positional argument
  return re.sub('.*www\.', '', target, 1).split('/')[0].strip()

(kali㉿kali)-[~/recopilacion/smule.com/0218]
$ ctfr-org -d smule > ctfr_org.txt
/usr/bin/ctfr-org:27: SyntaxWarning: invalid escape sequence '\ '
  b = ''
/usr/bin/ctfr-org:40: SyntaxWarning: invalid escape sequence '\.'
  return re.sub('.*www\.', '', target, 1).split('/')[0].strip()
/usr/bin/ctfr-org:40: DeprecationWarning: 'count' is passed as positional argument
  return re.sub('.*www\.', '', target, 1).split('/')[0].strip()

(kali㉿kali)-[~/recopilacion/smule.com/0218]
$ cat ctfr.txt | unfurl --unique domains > ctfr_limpio.txt

(kali㉿kali)-[~/recopilacion/smule.com/0218]
$ cat ctfr_org.txt | unfurl --unique domains > ctfr_org_limpio.txt

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

## 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**.

