

Práctica de laboratorio - Búsqueda de información a partir de certificados SSL

Objetivos

- Ver información de certificados en hosts
- Acceder a la información detallada del certificado
- Usar herramientas de escaneo de SSL en Kali
- Usar las herramientas de Kali para recopilar información del certificado

Trasfondo / Escenario

Los certificados SSL / TLS proporcionan dos amplias funciones. En primer lugar, proporcionan una forma de que las personas que acceden a él puedan validar la propiedad de un sitio web. En segundo lugar, proporcionan un medio por el cual se cifra la comunicación entre un cliente y un servidor para que no pueda ser leída o alterada por partes no autorizadas. También proporcionan la información necesaria para que un navegador cree una conexión segura y cifrada a un sitio web a través del protocolo HTTPS. Los certificados se utilizan detrás de escena cuando los usuarios navegan por Internet. En la mayoría de los casos, los usuarios no saben que están en uso. Los usuarios los detectan si falta un certificado, está desactualizado o está mal configurado.

La información del certificado se puede ver localmente para un sitio web que se muestra actualmente en un navegador haciendo clic en el icono de candado junto a la URL en el navegador. Los certificados también se almacenan localmente para las propias autoridades de certificación. Hay varias formas de verlos. El formato de la información del certificado de clave pública lo especifica el estándar X.509.

Los hackers éticos pueden utilizar la información de los certificados públicos en la fase de reconocimiento de las pruebas de penetración. La información del certificado puede revelar detalles sobre una organización, incluidos nombres de dominio y subdominio, fechas de emisión y vencimiento y claves públicas de certificados. Además, ciertas versiones de software, como OpenSSL, tienen vulnerabilidades ampliamente conocidas que pueden aprovecharse, incluida la vulnerabilidad al error Heartbleed. Además, es posible que algunos certificados utilicen algoritmos de cifrado débiles.

Recursos necesarios

- Kali VM personalizada para el curso de Ethical Hacker
- Acceso a Internet

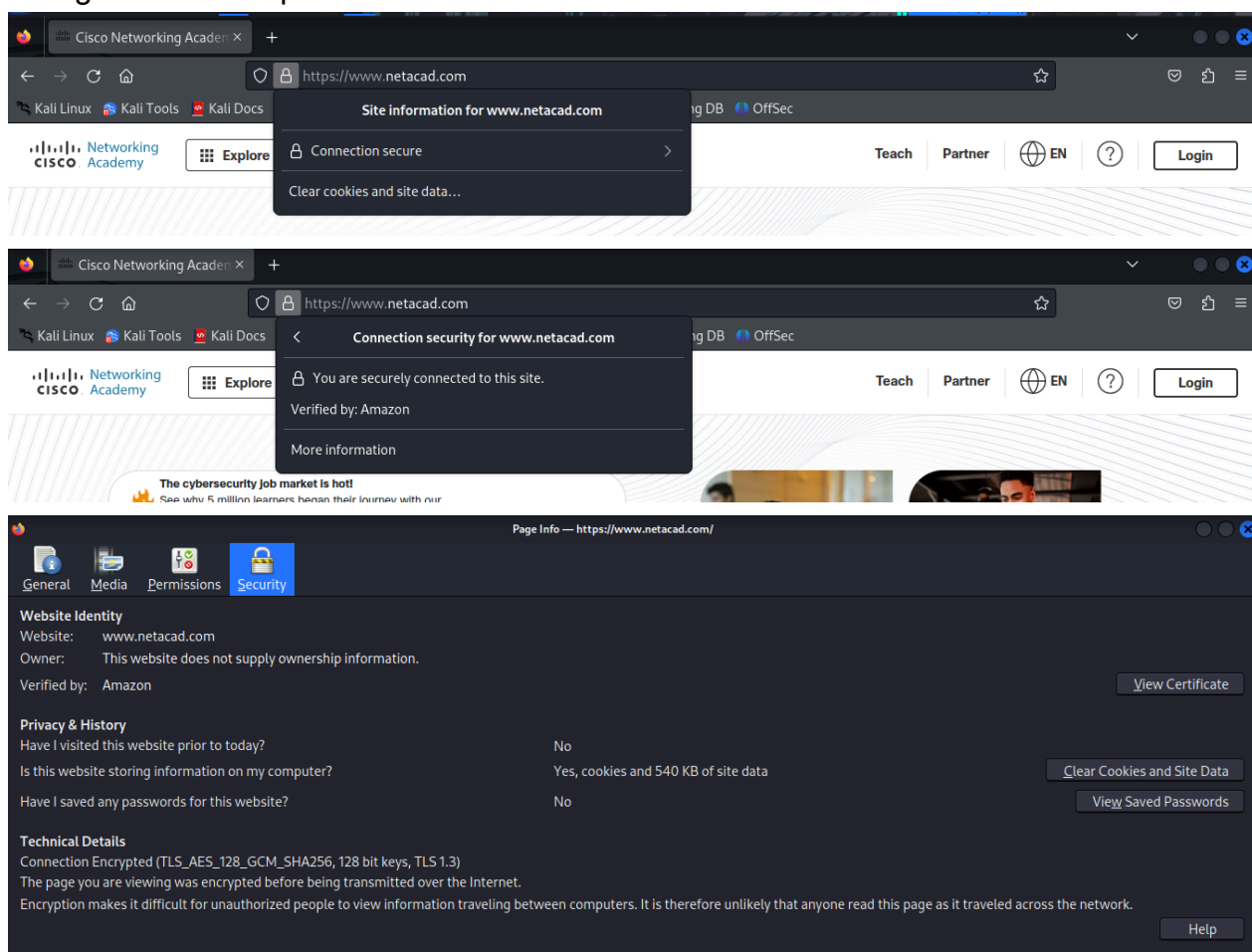
Instrucciones

Parte 1: Ver información del certificado en hosts

Algunos certificados SSL se almacenan localmente en hosts de red. Estos certificados permiten una comunicación segura entre un host y un servidor a través de una cadena de certificados. Un host almacena certificados intermedios y raíz como parte del proceso de autenticación SSL.

Paso 1: Vea los certificados del sitio desde un navegador.

1. Navegue hasta skillsforall.com.
2. En la mayoría de los navegadores, aparece un icono de candado junto a la URL del sitio que se muestra actualmente. Haga clic en el icono del candado y explore las configuraciones disponibles.



3. La mayoría de los navegadores tienen un administrador de certificados que permite ver los detalles de los certificados para sitios web o los certificados raíz para las autoridades de certificación. Vea la información del certificado mientras navega, usa el candado o abre la información del certificado desde la configuración de seguridad del navegador.

Certificate		
www.netacad.com	Amazon RSA 2048 M03	Amazon Root CA 1
Subject Name		
Common Name	www.netacad.com	
Issuer Name		
Country	US	
Organization	Amazon	
Common Name	Amazon RSA 2048 M03	
Validity		
Not Before	Fri, 23 Aug 2024 00:00:00 GMT	

(Información detallada sobre el certificado en cuestión)

4. Mire los detalles del certificado Cisco skillsforall y responda las siguientes preguntas.

- ¿Para qué dominio se emitió el certificado? ¿Qué organización lo emitió?

Fue emitido para el dominio **socialgoodplatform.com** y la organización que lo emitió fue IdenTrust.

Subject Alt Names	
DNS Name	www.netacad.com
DNS Name	*.skillsforall.com
DNS Name	*.netacad.com
DNS Name	*.socialgoodplatform.com

- Vea el certificado. ¿Cuándo caducará?

A la fecha de la realización de este laboratorio:

Validity	
Not Before	Fri, 23 Aug 2024 00:00:00 GMT
Not After	Sun, 21 Sep 2025 23:59:59 GMT

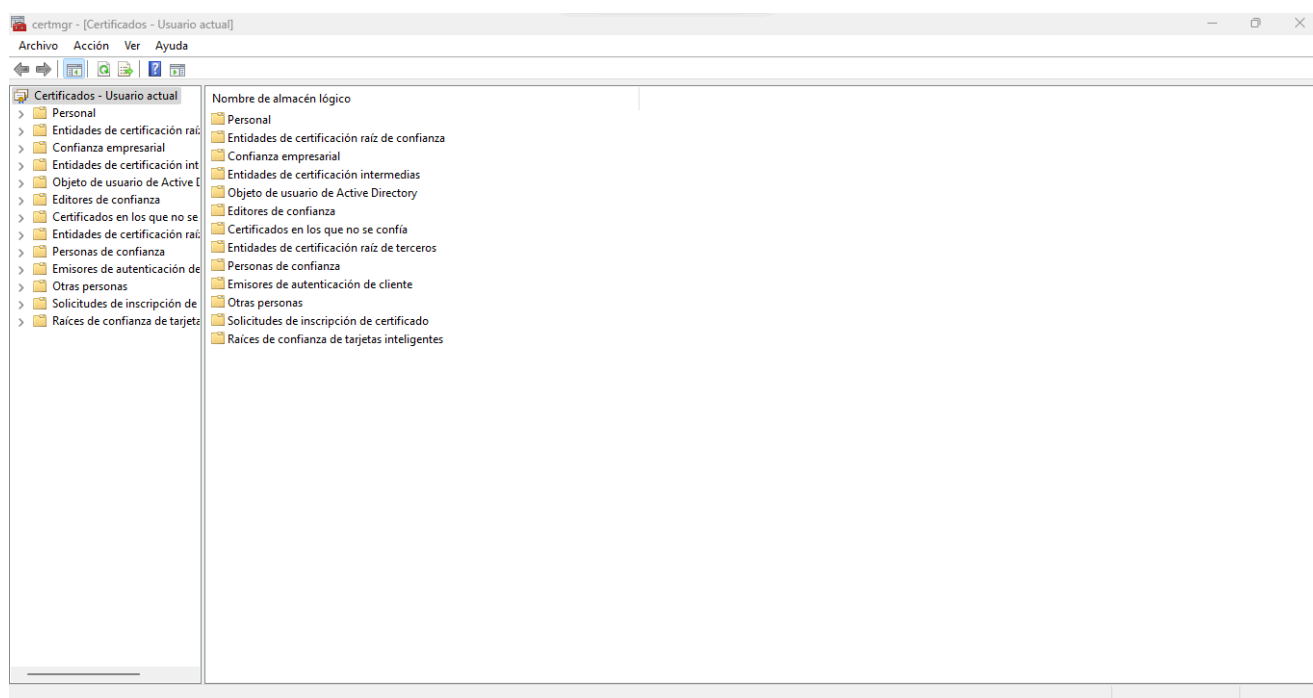
- ¿Cuál es el algoritmo de cifrado de firmas de certificados?

A la fecha de la realización de este laboratorio:

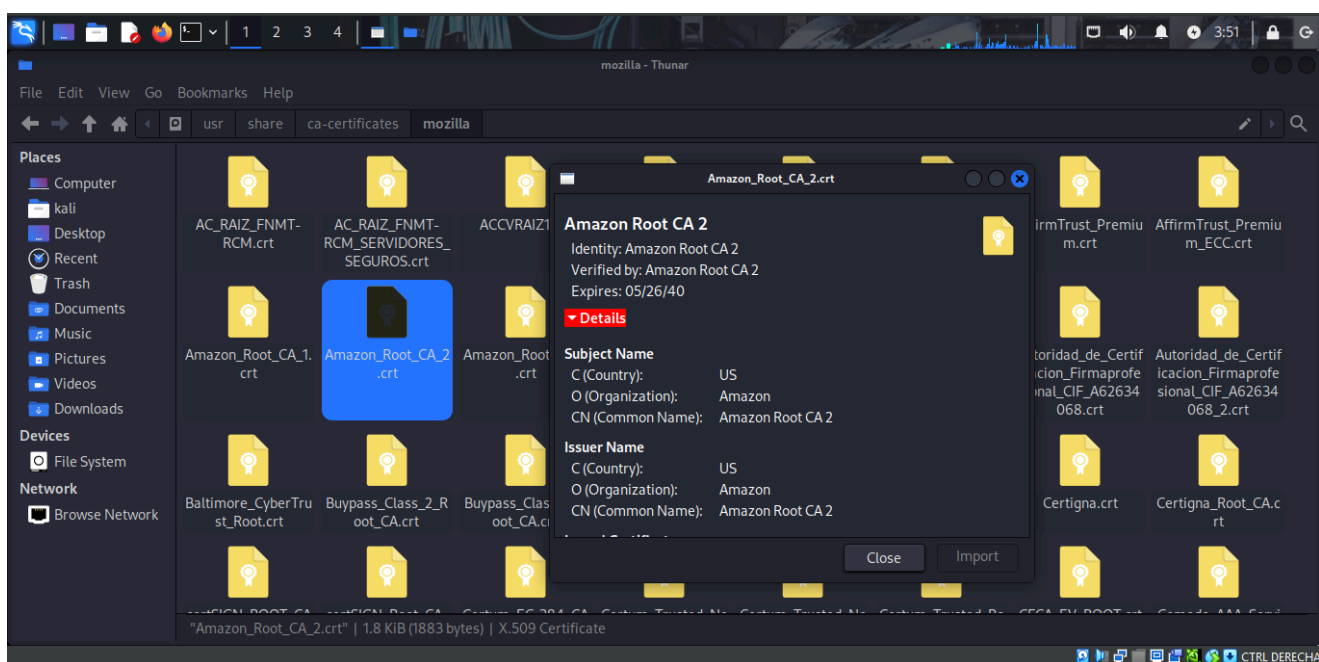
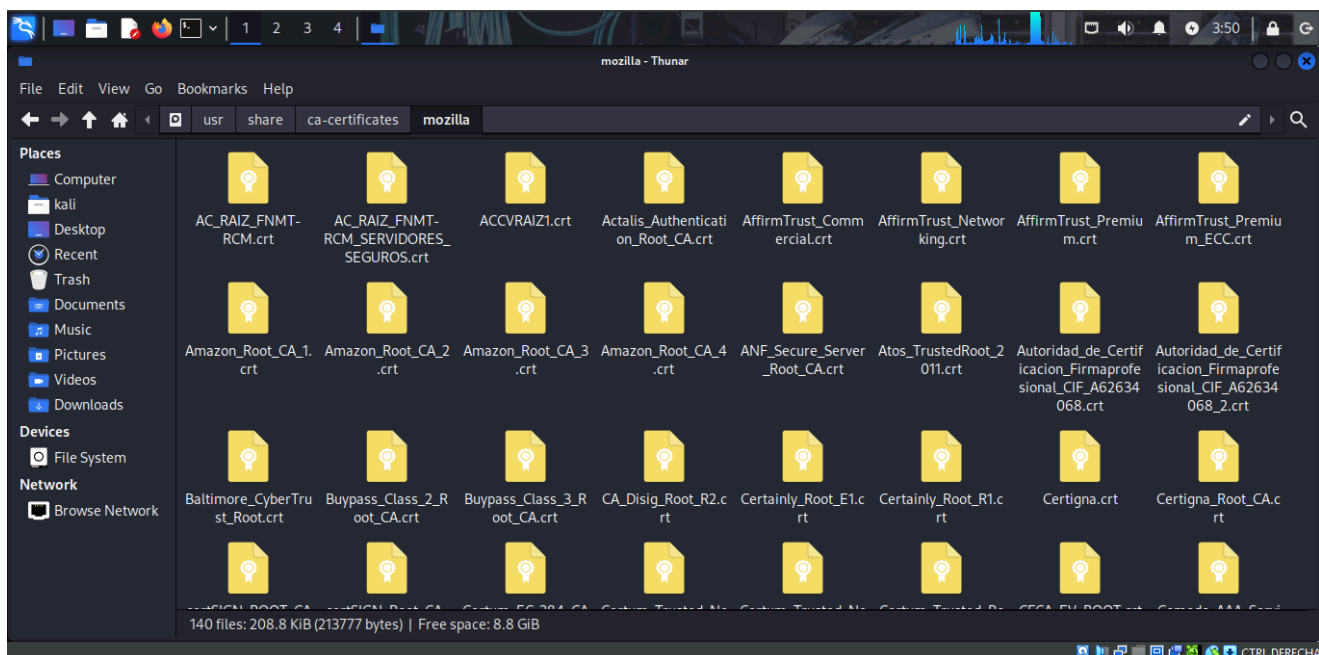
Miscellaneous	
Serial Number	07:7C:02:C1:83:A7:9C:95:F0:21:23:3C:57:09:9A:19
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Paso 2: Vea los certificados almacenados en el sistema operativo.

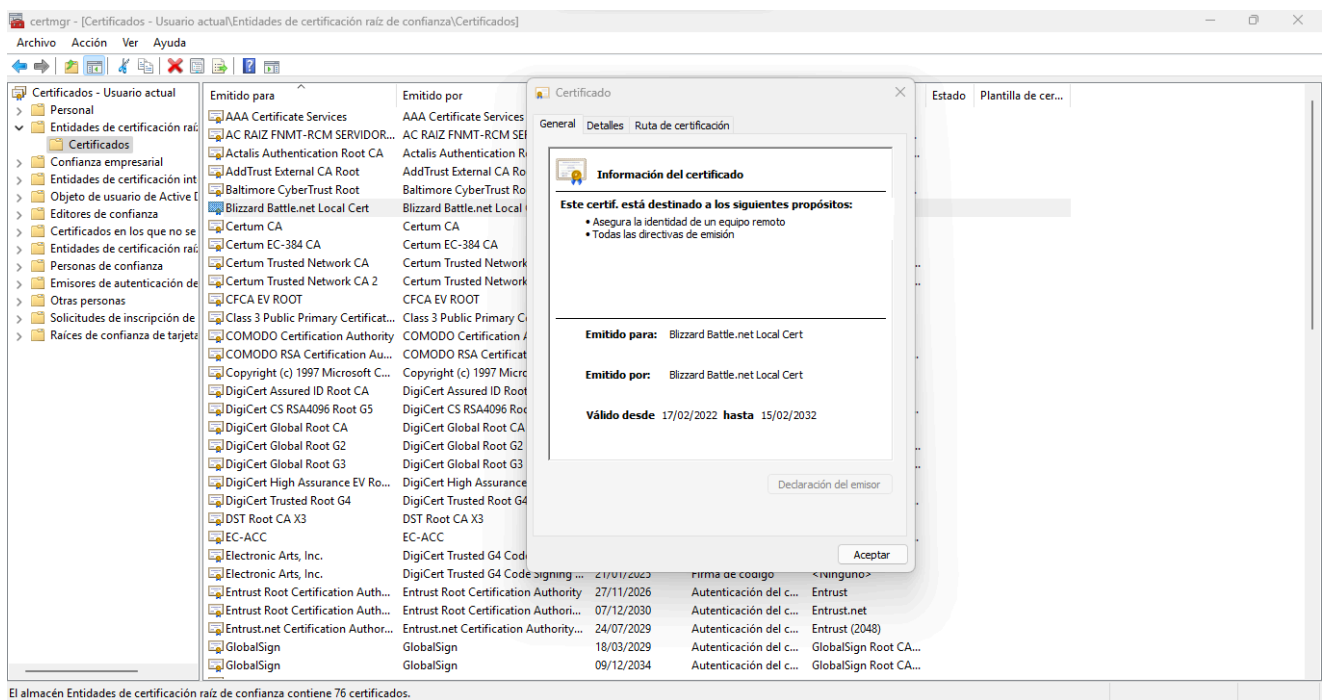
1. Microsoft Windows tiene una aplicación de administración de seguridad que forma parte de Microsoft Management Console. Ingrese **certmgr.msc** en el cuadro de búsqueda y presione Intro para abrirlo.



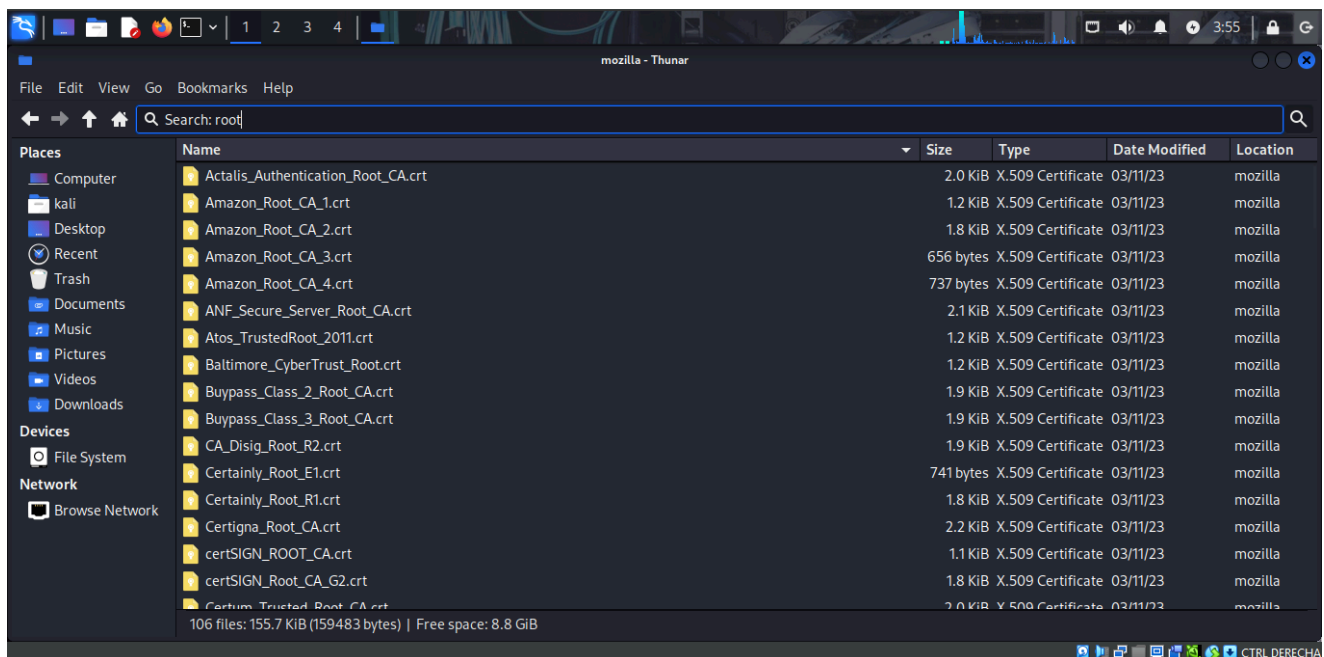
En Kali, puede encontrar los certificados almacenados en la carpeta `/usr/share/ca-certificates/mozilla`. Haga clic con el botón derecho en un certificado y seleccione **Open With “ViewFile”** para acceder a la información de un certificado.



2. Acceda a la información sobre certificados raíz e intermedios de confianza en Windows seleccionando las carpetas de certificados correspondientes en la aplicación de administración.



En Kali, acceda a la carpeta de certificados y use **ls -l | grep root** para enumerar los archivos de certificados raíz, o busque la palabra **root** en la ventana del administrador de archivos.



Los nombres de los archivos de certificado raíz hacen referencia a la autoridad de certificación que los otorgó.

¿Cuáles son las tres autoridades de certificación más comunes en su equipo? Investíguelas en internet.

- **Microsoft:** (Microsoft Authenticode, Microsoft ECC, Microsoft Root Authority, Microsoft RSA Root, Microsoft Time Stamp Root). Esto es esperable, ya que mi SO es Windows y Microsoft tiene sus propias CAs para emitir certificados para sus servicios y software.

- **GlobalSign:** (GlobalSign, GlobalSign Code Signing Root CA, GlobalSign Root CA). Es una CA muy grande y conocida a nivel mundial.
- **DigiCert:** (DigiCert Assured ID Root CA, DigiCert Global Root CA, DigiCert High Assurance EV Root CA, DigiCert Trusted Root CA). DigiCert es una de las CAs líderes y compró a otras como Symantec/VeriSign, por lo que es común ver sus certificados.
- **¿Cuál es el costo de un certificado SSL básico de un solo dominio durante un año?**

Un certificado SSL básico de un solo dominio por un año (Validación de Dominio - DV) puede salir desde **7 a 10 dólares**. Si se va por uno de Validación de Organización (OV), que es para empresas, van desde los **37 dólares**.

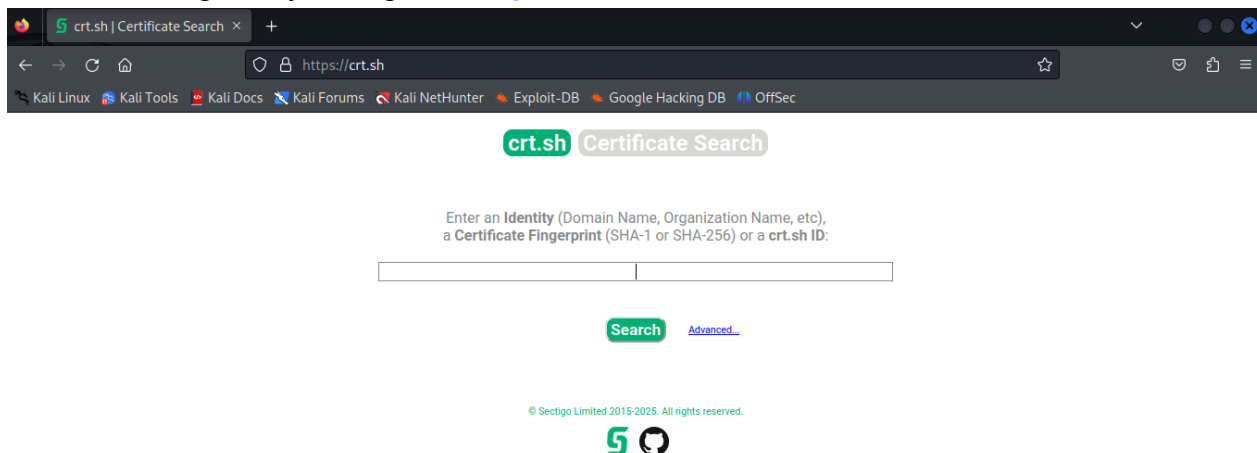
Parte 2: Acceda a información detallada del certificado en línea

La transparencia de certificados (CT) es un marco abierto para monitorear y auditar la emisión de certificados SSL / TLS. CT requiere que todas las autoridades de certificación (CA) de confianza pública registren todos los certificados emitidos en registros auditables, a prueba de manipulaciones y disponibles públicamente. Estos registros se pueden monitorear para detectar cualquier emisión fraudulenta o maliciosa de certificados SSL / TLS, incluidos los certificados emitidos para dominios que el atacante no controla.

En OSINT, los registros de CT se pueden utilizar para recopilar información sobre los certificados SSL / TLS utilizados por una organización o un dominio específico. Al analizar los registros de TC, los analistas pueden identificar las emisiones de certificados y sus dominios asociados, así como cualquier anomalía o irregularidad en la emisión de certificados. Los registros de TC también se pueden usar para monitorear cualquier emisión no autorizada de certificados SSL / TLS, lo que podría indicar una posible violación de la seguridad.

Se puede acceder a los registros de CT a través de varios servidores de registros de CT y API. También hay varias herramientas de monitoreo de TC disponibles, como CertSpotter y Censys, que pueden ayudar a automatizar el proceso de monitoreo de registros de TC para dominios específicos o certificados SSL / TLS.

1. Abra un navegador y navegue a <https://crt.sh>.



2. Ingrese la URL de skillsforall en el cuadro de búsqueda y haga clic en **Search**.

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	18946286166	2025-06-11	2025-06-11	2026-07-10	*.skillsforall.com	*.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	18683027891	2025-05-29	2025-05-29	2026-06-27	predev-adapt-assessment.skillsforall.com	predev-adapt-assessment.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	18513315582	2025-05-20	2025-05-20	2026-06-18	predev.skillsforall.com	*.predev.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M03
	18512619949	2025-05-20	2024-06-18	2025-07-18	predev.skillsforall.com	*.predev.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	18512616628	2025-05-20	2025-05-20	2026-06-18	predev.skillsforall.com	*.predev.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M03
	17603043851	2025-04-03	2025-04-03	2026-05-02	author.netacad.com	*.author.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	17828095642	2025-04-03	2024-05-03	2025-06-01	author.netacad.com	*.author.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	17601684398	2025-04-03	2025-04-03	2026-05-02	author.netacad.com	*.author.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	17434625955	2025-03-27	2025-03-27	2026-04-26	cperf.netacad.com	*.cperf.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M03
	17076433317	2025-03-13	2025-03-13	2026-04-12	cqa.skillsforall.com	*.cqa.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	16934145772	2025-03-03	2025-03-03	2026-04-02	*.skillsforall.com	*.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M03
	16934138885	2025-03-03	2025-03-03	2026-04-02	cdev.skillsforall.com	*.cdev.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02

3. La tabla resultante enumera información completa de los certificados emitidos a skillsforall.com y subdominios relacionados. La lista se remonta a 2019. crt.sh proporciona ID para los certificados, pero estos ID son relevantes solo para crt.sh. Hacer clic en una ID lo lleva a los detalles del certificado disponibles.

crt.sh Certificate Search

Criteria ID = '1288534589'

crt.sh ID	1288534589																																										
Summary	Precertificate																																										
Certificate Transparency	<p>Log entries for this certificate:</p> <table border="1"> <thead> <tr> <th>Timestamp</th> <th>Entry #</th> <th>Log Operator</th> <th>Log URL</th> </tr> </thead> <tbody> <tr> <td>2019-03-16 14:59:24 UTC</td> <td>23361477</td> <td>Cloudflare</td> <td>https://ct.cloudflare.com/logs/nimbus2020</td> </tr> <tr> <td>2019-03-16 14:59:24 UTC</td> <td>620655336</td> <td>Google</td> <td>https://ct.googleapis.com/rocketeer</td> </tr> <tr> <td>2019-03-16 14:59:24 UTC</td> <td>139669057</td> <td>Google</td> <td>https://ct.googleapis.com/skydiver</td> </tr> <tr> <td>2019-03-16 14:59:24 UTC</td> <td>559018708</td> <td>Google</td> <td>https://ct.googleapis.com/pilot</td> </tr> </tbody> </table>							Timestamp	Entry #	Log Operator	Log URL	2019-03-16 14:59:24 UTC	23361477	Cloudflare	https://ct.cloudflare.com/logs/nimbus2020	2019-03-16 14:59:24 UTC	620655336	Google	https://ct.googleapis.com/rocketeer	2019-03-16 14:59:24 UTC	139669057	Google	https://ct.googleapis.com/skydiver	2019-03-16 14:59:24 UTC	559018708	Google	https://ct.googleapis.com/pilot																
Timestamp	Entry #	Log Operator	Log URL																																								
2019-03-16 14:59:24 UTC	23361477	Cloudflare	https://ct.cloudflare.com/logs/nimbus2020																																								
2019-03-16 14:59:24 UTC	620655336	Google	https://ct.googleapis.com/rocketeer																																								
2019-03-16 14:59:24 UTC	139669057	Google	https://ct.googleapis.com/skydiver																																								
2019-03-16 14:59:24 UTC	559018708	Google	https://ct.googleapis.com/pilot																																								
Revocation	<table border="1"> <thead> <tr> <th>Mechanism</th> <th>Provider</th> <th>Status</th> <th>Revocation Date</th> <th>Last Observed in CRL</th> <th>Last Checked (Error)</th> </tr> </thead> <tbody> <tr> <td>OCSP</td> <td>The CA</td> <td>Check</td> <td>?</td> <td>n/a</td> <td>?</td> </tr> <tr> <td>CRL</td> <td>The CA</td> <td>Not Revoked (Expired)</td> <td>n/a</td> <td>n/a</td> <td>2025-07-07 01:33:37 UTC</td> </tr> <tr> <td>CRLSet/Blocklist</td> <td>Google</td> <td>Not Revoked</td> <td>n/a</td> <td>n/a</td> <td>n/a</td> </tr> <tr> <td>disallowedcert.stl</td> <td>Microsoft</td> <td>Not Revoked</td> <td>n/a</td> <td>n/a</td> <td>n/a</td> </tr> <tr> <td>OneCRL</td> <td>Mozilla</td> <td>Not Revoked</td> <td>n/a</td> <td>n/a</td> <td>n/a</td> </tr> </tbody> </table>							Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)	OCSP	The CA	Check	?	n/a	?	CRL	The CA	Not Revoked (Expired)	n/a	n/a	2025-07-07 01:33:37 UTC	CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a	disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a	OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a
Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)																																						
OCSP	The CA	Check	?	n/a	?																																						
CRL	The CA	Not Revoked (Expired)	n/a	n/a	2025-07-07 01:33:37 UTC																																						
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a																																						
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a																																						
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a																																						
Certificate Fingerprints	<p>SHA-256 61B6BD1448718F408F7B6690FE81AD3803DE9180F4B2BD96ED33C91B335A89E1 SHA-1 3D84A4D9F8588E0E1EC97A089D4642C98CDD2144</p> <p>ASN.1 Certificate Graph Hierarchy px Hide metadata Run linters using okmimetal</p> <p>Certificate:</p> <p>Data:</p> <p>Version: 3 (0x2)</p> <p>Serial Number:</p> <p>06:41:61:68:ed:5d:76:b3:2e:f0:cb:93:2f:28:f7:76</p> <p>Signature Algorithm: sha256WithRSAEncryption</p>																																										

Tenga en cuenta que crt.sh revela varios subdominios que no son conocidos por los usuarios normales de skillsforall. Anote los nombres de los subdominios.

- ¿Quién cree que deben utilizar estos subdominios? Explique.

Prestando atención a los nombres que comienzan con 'dev' y 'stage', puedo deducir que estos subdominios están diseñados para desarrolladores que trabajan en el sitio web de skillsforall.

- ¿Qué otro dominio está asociado con el dominio skillsforall según la información de crt.sh?

El otro dominio asociado es **socialgoodplatform.com**

16933863373	2025-03-03	2024-12-06	2026-01-04	*.socialgoodplatform.com	*.skillsforall.com skillsforall.com	C=US,O=Amazon,CN=Amazon RSA 2048 M02
-----------------------------	------------	------------	------------	--	--	--

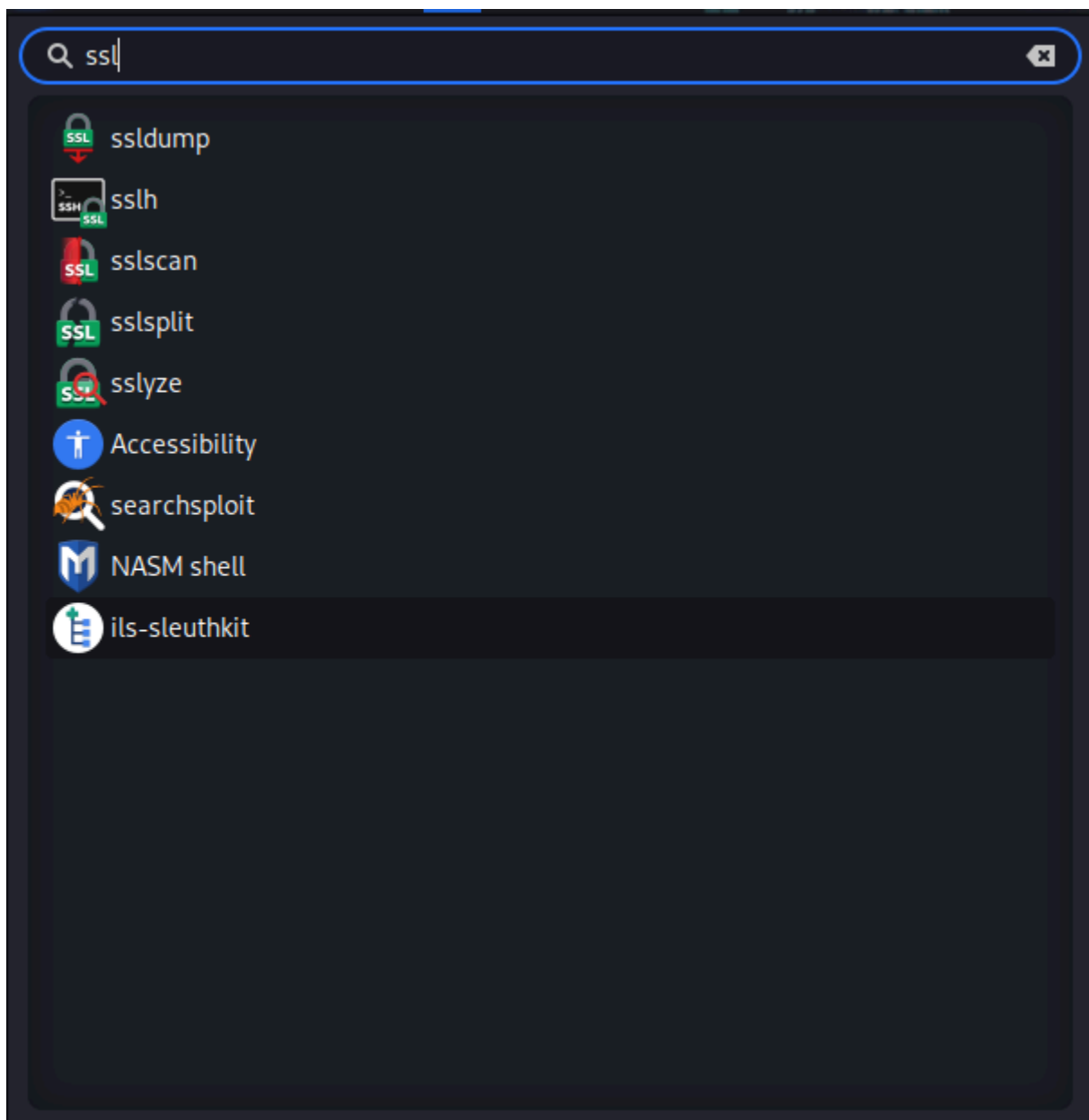
- Busque crt.sh en el dominio afiliado a skillsforall.com. ¿Qué observación general puede hacer sobre los dominios revelados en esta búsqueda? ¿Qué implica esto sobre la red?

Se puede concluir que tiene una gran superficie de ataque **socialgoodplatform.com**.

Parte 3: Usar las herramientas de escaneo de SSL en Kali

Paso 1: Investigar las herramientas de Kali

1. Iniciar la máquina Kali virtual e iniciar sesión
2. Inicie una sesión de terminal.
3. Kali incluye varias herramientas relacionadas con SSL. Haga clic en el icono de programas de Kali y busque el término **ssl**.



4. Utilice la referencia de herramientas de Kali para completar la tabla a continuación para las cinco herramientas de SSL incluidas con su distribución de Kali.

Herramienta	Descripción	Reconocimiento, explotación o utilidad
sslsplit	Consulta los servicios SSL para determinar qué cifrados se admiten.	Reconocimiento
ssldump	Analizador de protocolos de red SSL/TLS que captura y decodifica el tráfico, mostrando detalles de handshakes, suites de cifrado y certificados. Permite ver la comunicación cifrada de forma legible.	Reconocimiento / Análisis de tráfico
sslh	Multiplexor de protocolos que permite aceptar conexiones HTTPS, SSH, OpenVPN, tinc y XMPP en el mismo puerto (comúnmente el 443). Dirige el tráfico al servicio backend adecuado.	Utilidad / Configuración de red

Herramienta	Descripción	Reconocimiento, explotación o utilidad
sslsplit	Herramienta de interceptación SSL/TLS transparente que permite extraer información de comunicaciones cifradas y realizar ataques Man-in-the-Middle (MITM) generando certificados falsificados sobre la marcha.	Explotación / Análisis de tráfico
sslyze	Herramienta de Python para analizar la configuración SSL/TLS de un servidor, identificando posibles malas configuraciones y vulnerabilidades (como Heartbleed, soporte de versiones de TLS, compresión, etc.).	Reconocimiento / Análisis de vulnerabilidades
Herramienta	Descripción	Reconocimiento, explotación o utilidad

Parte 4: Usar las herramientas de Kali para recopilar información del certificado

Como sabe, **sslscan** es una herramienta de reconocimiento de Kali que recopila información sobre los certificados SSL asociados con los dominios. Es una utilidad de línea de comandos. Usaremos **sslscan** para recopilar información sobre certificados y usaremos otra utilidad, llamada **aha**, para enviar los resultados a un archivo HTML.

Paso 1: Instale aha.

La aplicación **aha** crea un archivo HTML estándar que captura la salida de los comandos del terminal en archivos HTML estándar. Aha captura cualquier código de color y formato básico de la salida del comando. También tiene opciones de línea de comandos que le permiten especificar su propio formato, como el color de fondo, las hojas de estilo para aplicar y el ajuste de palabras, entre otras configuraciones.

1. Actualice la información de su paquete de apto con el comando **apt update**. Esto requiere privilegios de root.

```
└─(kali㉿Kali)-[~]
```

```
└─$ sudo apt update
```

2. Instale aha con el comando **sudo apt install -y aha**. La opción -y supone que **sí** son las respuestas a todas las solicitudes y que se puede ejecutar de forma no interactiva. En este caso, está dando permiso para instalar aha.

Paso 2: Ejecute sslscan y guarde el resultado en un archivo HTML.

1. Desde la línea de comandos de un terminal, ejecute el comando para ejecutar **ssllscan** con el objetivo **skillsforall.com**.

```
(kali㉿Kali)-[~]
```

```
$ ssllscan skillsforall.com
```

Después de una breve demora, debería ver que los resultados del escaneo comienzan a aparecer en la ventana de terminal. La salida está codificada por colores para facilitar la interpretación de la gravedad de los problemas detectados. El significado de la codificación de colores es el siguiente:

- Texto de fondo rojo: cifrado NULO. No se utilizó cifrado.
- Rojo: cifrado roto (menor o igual a 40 bits), protocolo vulnerable o roto como SSLv2 o SSLv3 o algoritmo de firma de certificados roto como MD5.
- Amarillo: cifrado débil (menor o igual a 56 bits) o algoritmo de firma débil, como SHA-1.
- Violeta: cifrado anónimo, como ADH o AECDH.

```
(kali㉿Kali)-[~]
$ ssllscan skillsforall.com
Version: 2.0.16-static
OpenSSL 1.1.1u-dev  xx XXX xxxx

Connected to 3.160.90.31

Testing SSL server skillsforall.com on port 443 using SNI name skillsforall.com

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    disabled
TLSv1.1    disabled
TLSv1.2    enabled
TLSv1.3    enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
```

2. Si bien ssllscan ofrece opciones para generar resultados en formatos de archivo de texto o XML, ahora proporciona la legibilidad de HTML y la preservación de la codificación de

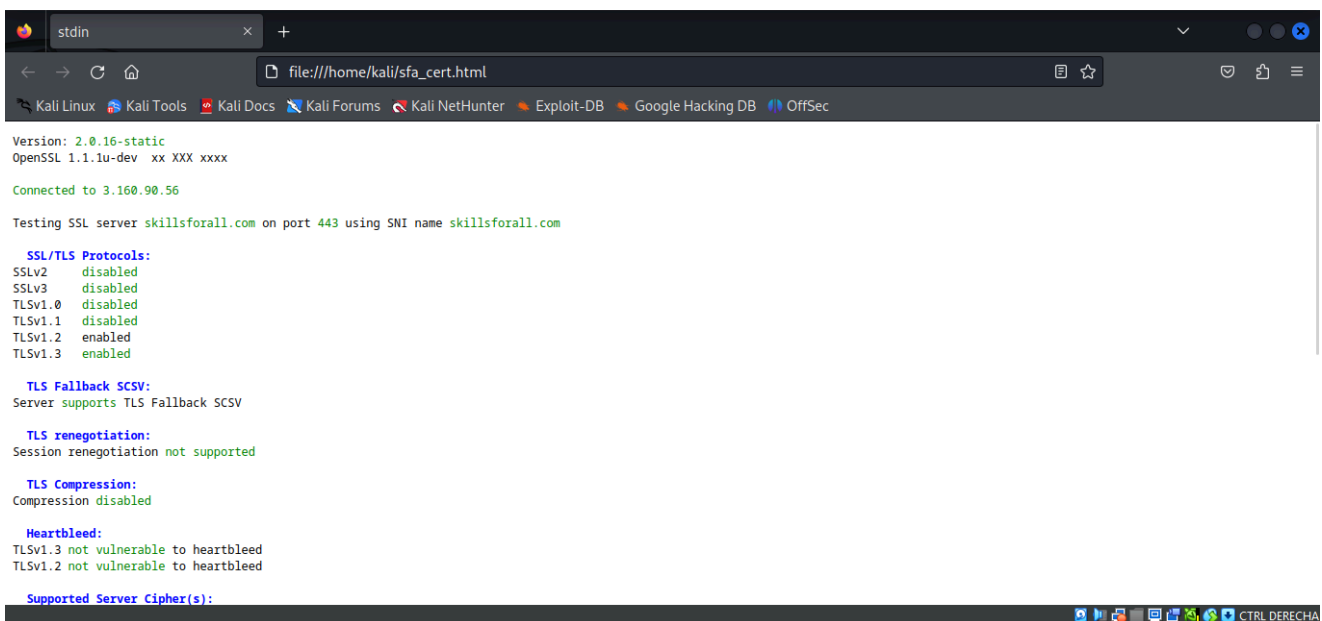
colores. Para usar aha, canalice la salida del comando sslscan a aha y luego redirija la salida de aha a un archivo HTML.

```
—(kali🌀Kali)-[~]
```

```
└─$ sslscan skillsforall.com | aha > sfa_cert.html
```

sslscan guardará el archivo en el directorio de inicio de Kali como lo indica el indicador. Puede agregar una ruta al nombre del archivo o ejecutar el terminal desde un directorio de destino para guardarlo en otro lugar.

3. Busque el archivo HTML y ábralo con Firefox. La salida debe ser similar a la del terminal, excepto que el fondo es blanco. La codificación de colores original debe estar intacta.



```
stdin
file:///home/kali/sfa_cert.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Version: 2.0.16-static
OpenSSL 1.1.1u-dev xx XXX xxxx
Connected to 3.160.90.56
Testing SSL server skillsforall.com on port 443 using SNI name skillsforall.com

SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 disabled
TLSv1.1 disabled
TLSv1.2 enabled
TLSv1.3 enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):
```

Pregunta de reflexión

Compare el resultado de las herramientas utilizadas en esta práctica de laboratorio.

¿Qué herramienta parece brindar la información más útil?

Además de `Crt.sh`, que también busca subdominios que podrían pasar de ser percibidos por las otras tools, `sslyze` va directo al grano porque te da un diagnóstico de seguridad del servidor SSL/TLS y para un informe de auditoría o para saber por dónde empezar a buscar debilidades, esa información es oro puro.