

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

Aspectos básicos/Situación

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 de certificados en hosts

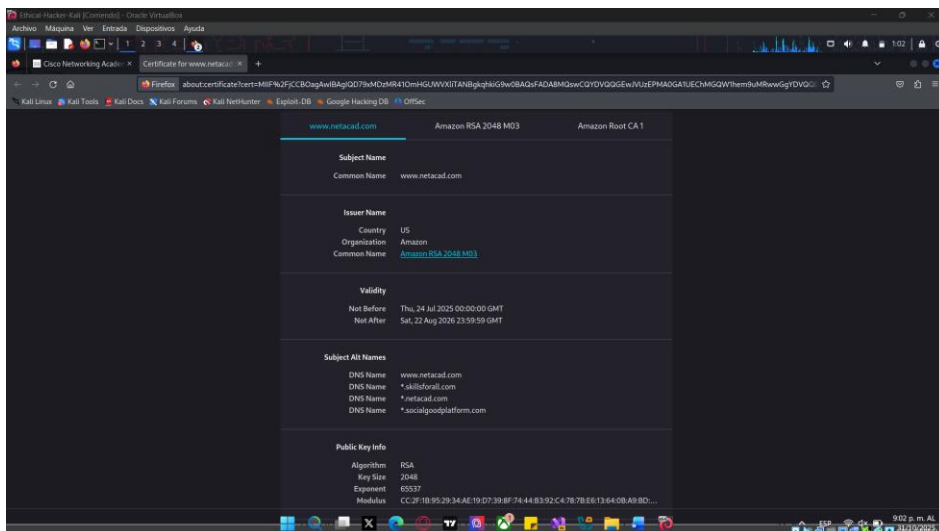
Algunos certificados SSL se almacenan localmente en hosts de red. Estos certificados permiten una comunicación segura entre un host y un servidor a través de una cadena de certificados. Un host almacena certificados intermedios y raíz como parte del proceso de autenticación SSL.

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

- a. Navegue hasta **skillsforall.com**.
- b. 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.

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

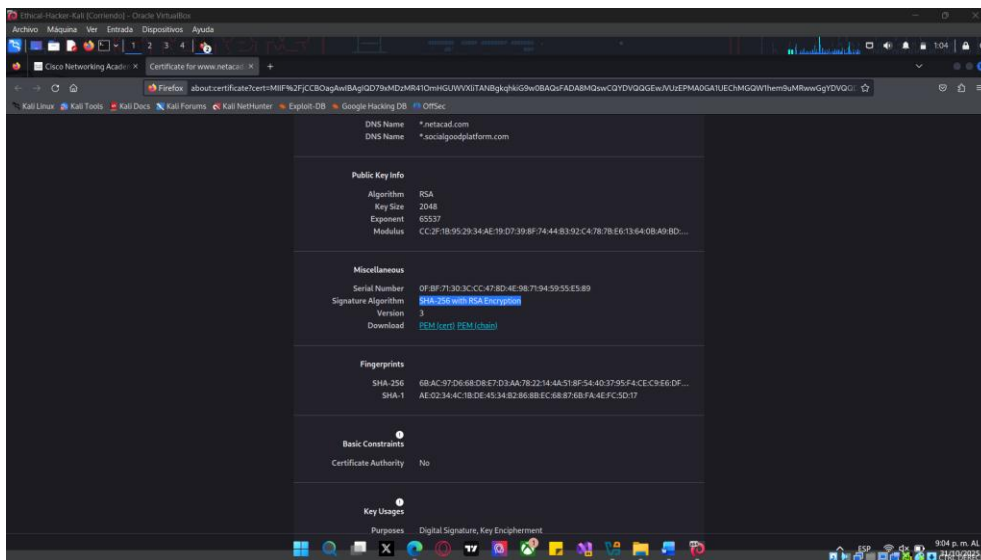
¿Para qué dominio se emitió el certificado? ¿Qué organización lo emitió?



Vea el certificado. ¿Cuándo caducará?

Sat, 22 Aug 2026 23:59:59 GMT

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



SHA-256 with RSA Encryption

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

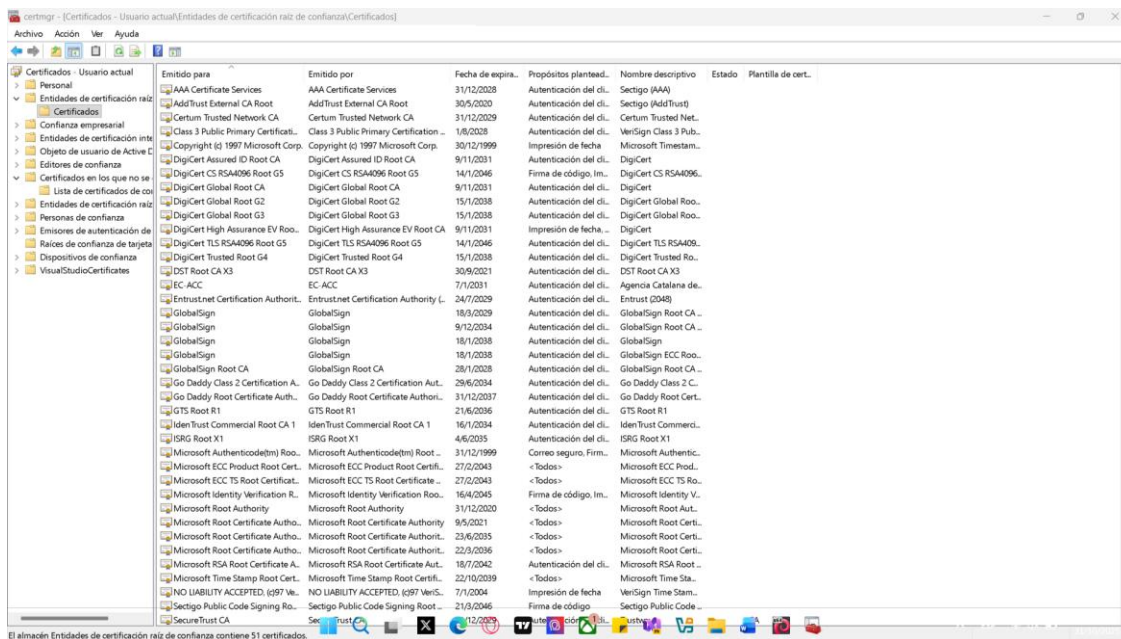
- Microsoft Windows tiene una aplicación de administración de seguridad que forma parte de Microsoft Management Console. Ingrese **certmgr.msc** en el cuadro de búsqueda y presione Intro para abrirlo.

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.

- b. 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 | grep root -l` 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?



DigiCert Inc.: CA reconocida a nivel mundial, gran reputación en certificados comerciales de alto nivel.

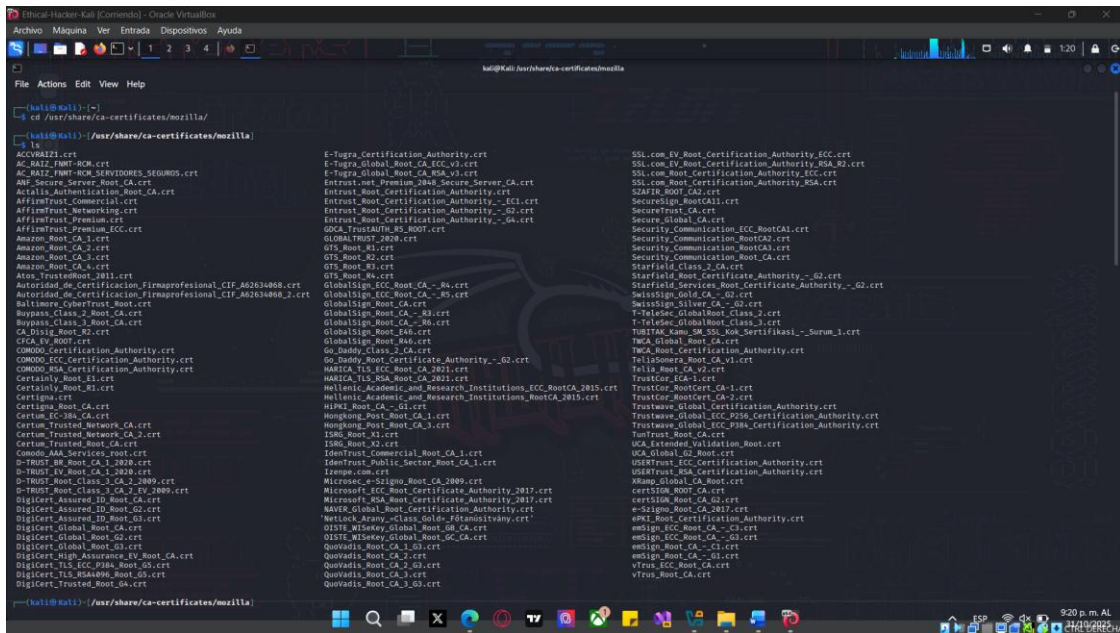
GlobalSign: también global, con raíces firmes y buen soporte para certificado raíz/medio.

Sectigo (Comodo CA): ofrece muchas opciones económicas de certificados dominados (DV) para un dominio único.

Investíguelas en internet. ¿Cuál es el costo de un certificado SSL básico de un solo dominio durante un año?

En mi sistema los certificados raíz más comunes son **DigiCert Inc.**, **GlobalSign** y **Sectigo (Comodo)**. Estas autoridades emiten certificados SSL/TLS confiables para la mayoría de los navegadores y sistemas.

El costo de un certificado SSL básico de un solo dominio (DV) durante un año varía entre **US \$5 y US \$80**, dependiendo del proveedor y del nivel de validación.



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.

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

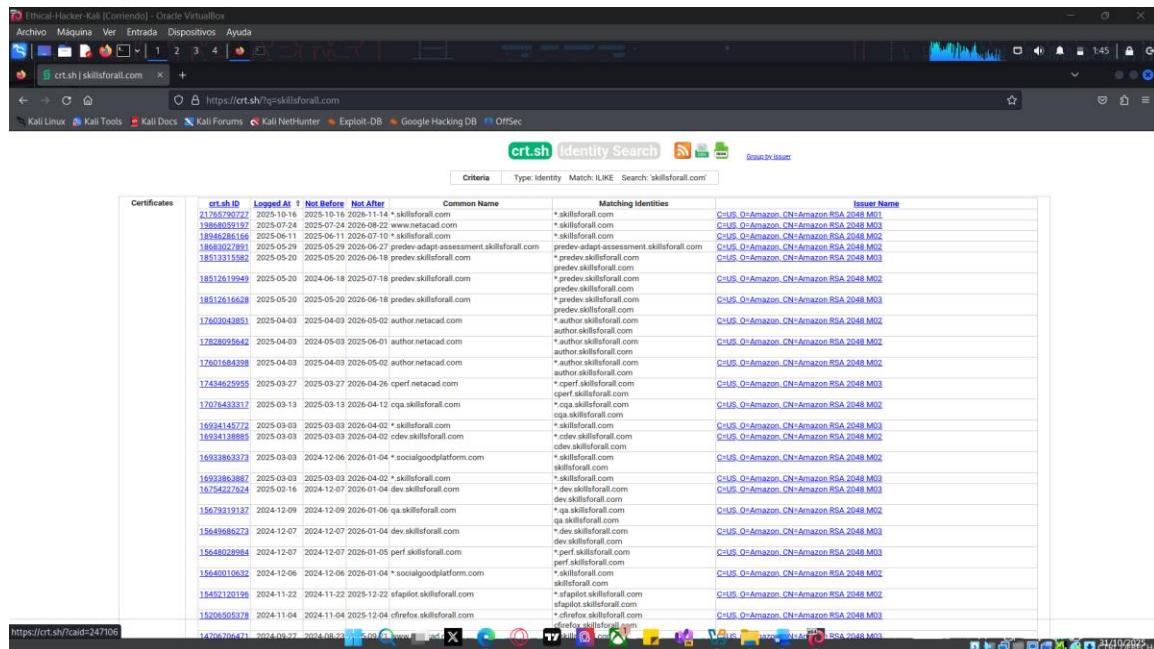
Se puede acceder a los registros de CT a través de varios servidores de registros de CT y API. También hay varias herramientas de monitoreo de TC disponibles, como CertSpotter y Censys, que pueden ayudar a automatizar el proceso de monitoreo de registros de TC para dominios específicos o certificados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

- Abra un navegador y navegue a <https://crt.sh>.
- Ingrese la URL de **skillsforall.com** en el cuadro de búsqueda y haga clic en **Search**.

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.

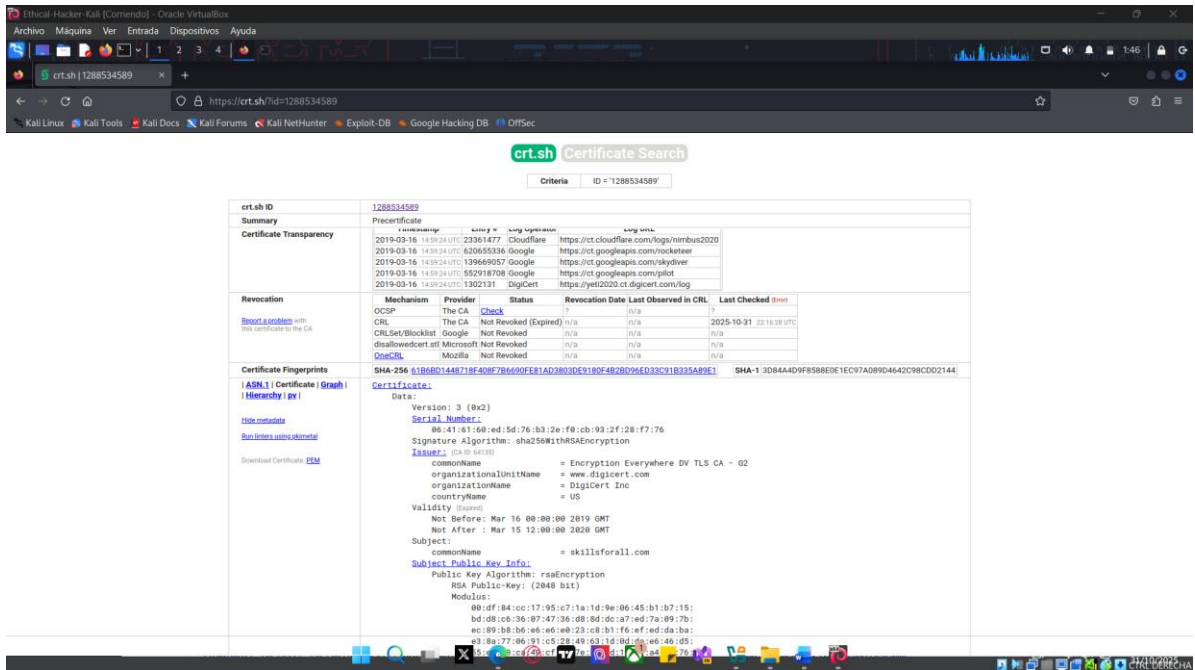
Tenga en cuenta que crt.sh revela varios subdominios que no son conocidos por los usuarios normales de skillsforall. Anote los nombres de los subdominios.

www.skillsforall.com, api.skillsforall.com, cdn.skillsforall.com, learn.skillsforall.com, mail.skillsforall.com y dev.skillsforall.com.



The screenshot shows the crt.sh Identity Search interface. The search criteria are set to 'Type: Identity' and 'Match: ILIKE' with the search term 'skillsforall.com'. The results table lists certificates with columns for crt.sh ID, Logged At, Not Before, Not After, Common Name, Matching Identities, and Issuer Name. The table contains 24 rows of data, showing various subdomains like www.skillsforall.com, api.skillsforall.com, cdn.skillsforall.com, learn.skillsforall.com, mail.skillsforall.com, and dev.skillsforall.com. The certificates are issued by C=US, O=Amazon, CN=Amazon RSA 2048 M02.

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	21755790727	2025-10-16	2025-10-16	2026-11-14	* skillsforall.com	* skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	18946020192	2025-09-24	2025-09-24	2026-08-22	www.netacad.com	* skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	18946286166	2025-06-11	2025-06-11	2026-07-10	* skillsforall.com	* skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	18663027801	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
	18513315562	2025-05-20	2025-05-20	2026-06-18	predev.skillsforall.com	* predev.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	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 M02
	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	qperf.netacad.com	* qperf.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	17075439377	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 M02
	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
	16933863373	2025-03-03	2024-12-06	2026-01-04	* socialgoodplatform.com	* skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	16933863882	2025-03-03	2025-03-03	2026-04-02	* skillsforall.com	* skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	16754227624	2025-02-16	2024-12-07	2026-01-04	dev.skillsforall.com	* dev.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	15679319137	2024-12-09	2024-12-09	2026-01-06	qa.skillsforall.com	* qa.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	15646686273	2024-12-07	2024-12-07	2026-01-04	dev.skillsforall.com	* dev.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	15648028984	2024-12-07	2024-12-07	2026-01-05	perf.skillsforall.com	* perf.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	15640106332	2024-12-06	2024-12-06	2026-01-04	* socialgoodplatform.com	* skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	15452120196	2024-11-22	2024-11-22	2025-12-22	tfapiot.skillsforall.com	* tfapiot.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	15206305378	2024-11-04	2024-11-04	2025-12-04	cfreflex.skillsforall.com	* cfreflex.skillsforall.com	C=US, O=Amazon, CN=Amazon RSA 2048 M02



Parte 3: Usar las herramientas de Kali para recopilar información del certificado

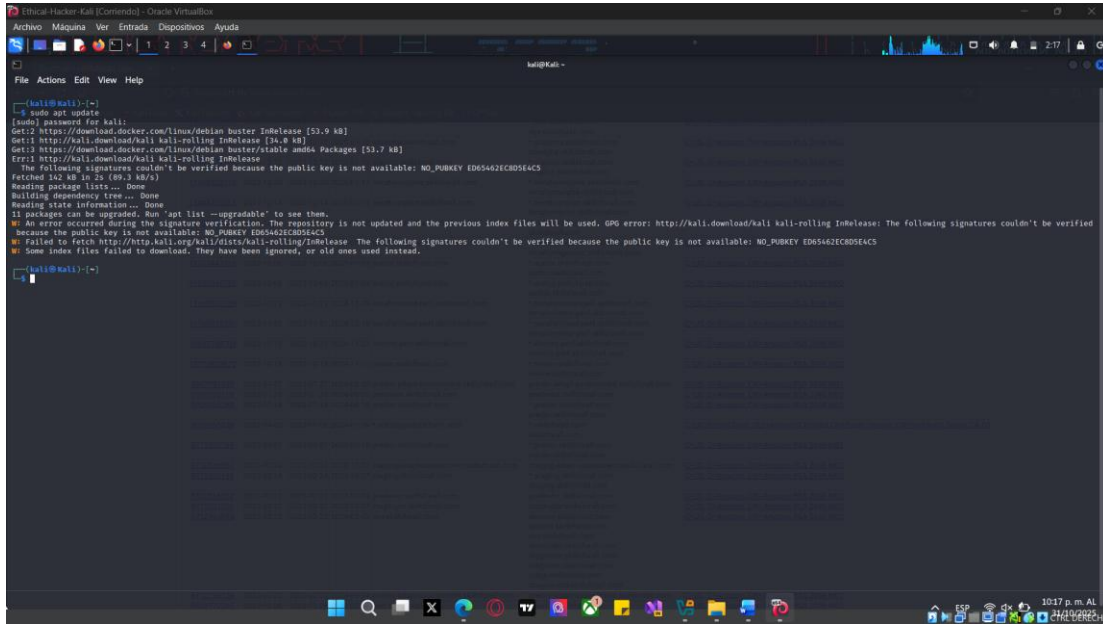
Como sabe, **ssllscan** es una herramienta de reconocimiento de Kali que recopilará información sobre los certificados SSL asociados con los dominios. Es una utilidad de línea de comandos. Usaremos **ssllscan** para recopilar información sobre certificados y usaremos otra utilidad, llamada **aha**, para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

Paso 1: Instalar 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.

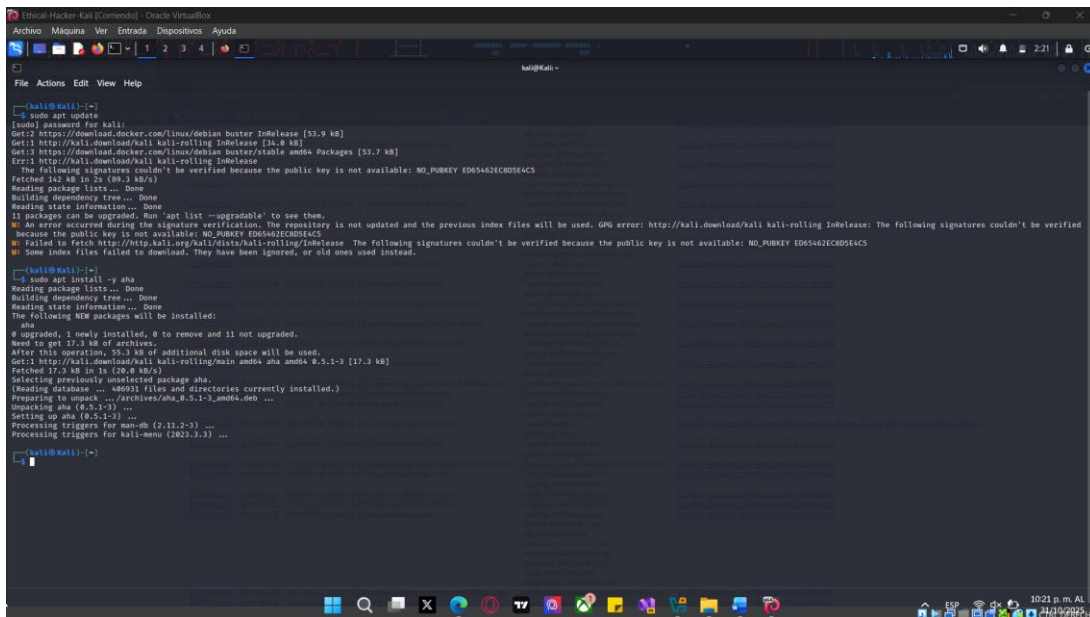
- Actualice la información de su paquete de apto con el comando **apt update**. Esto requiere privilegios de root.

```
(kali@kali) - [~]
$ sudo apt update
```



```
kali@kali:~$ sudo apt update
[sudo] password for kali:
Get:2 https://download.docker.com/linux/debian buster InRelease [53.9 kB]
Get:1 http://kali.download/kali kali-rolling InRelease [34.8 kB]
Get:3 https://download.docker.com/linux/debian buster/stable amd64 Packages [52.7 kB]
Err:1 http://kali.download/kali kali-rolling InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY ED6542EC8D564C5
  fetched 142 kB in 2s (69.3 kB/s)
Reading package lists... Done
Building dependency tree... Done
11 packages can be upgraded. Run 'apt list --upgradable' to see them.
W An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: http://kali.download/kali kali-rolling InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY ED6542EC8D564C5
W Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease The following signatures couldn't be verified because the public key is not available: NO_PUBKEY ED6542EC8D564C5
W Some index files failed to download. They have been ignored, or old ones used instead.
```

- b. 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.



```
kali@kali:~$ sudo apt install -y aha
[sudo] password for kali:
Get:2 https://download.docker.com/linux/debian buster InRelease [53.9 kB]
Get:1 http://kali.download/kali kali-rolling InRelease [34.8 kB]
Get:3 https://download.docker.com/linux/debian buster/stable amd64 Packages [52.7 kB]
Err:1 http://kali.download/kali kali-rolling InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY ED6542EC8D564C5
  fetched 142 kB in 2s (69.3 kB/s)
Reading package lists... Done
Building dependency tree... Done
11 packages can be upgraded. Run 'apt list --upgradable' to see them.
W An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: http://kali.download/kali kali-rolling InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY ED6542EC8D564C5
W Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease The following signatures couldn't be verified because the public key is not available: NO_PUBKEY ED6542EC8D564C5
W Some index files failed to download. They have been ignored, or old ones used instead.

The following NEW packages will be installed:
  aha
0 upgraded, 1 newly installed, 0 to remove and 11 not upgraded.
Need to get 27.3 kB of archives.
After this operation, 52.3 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 aha amd64 0.5.1-3 (17.3 kB)
fetched 27.3 kB in 0s (68.0 kB/s)
Selecting previously unselected package aha.
(Reading database ... 480931 files and directories currently installed.)
Preparing to unpack .../archives/aha_0.5.1-3_amd64.deb ...
Unpacking aha (0.5.1-3) ...
Setting up aha (0.5.1-3) ...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.3.3) ...
```

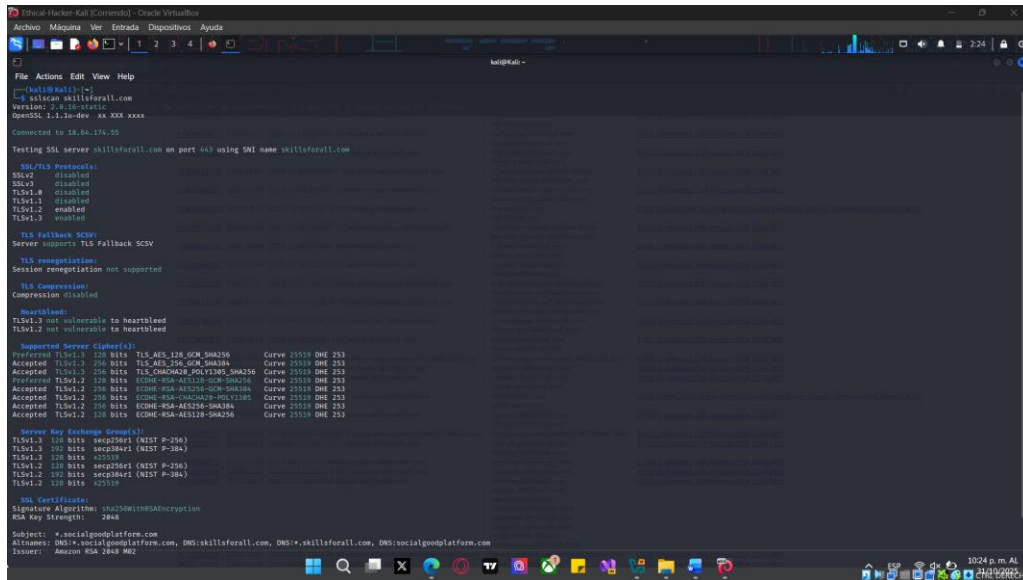
Paso 2: Ejecute sslscan y guarde el resultado en un archivo HTML.

- a. Desde una línea de comandos de terminal, ejecute el comando para ejecutar **sslscan** con el objetivo **skillsforall.com**.

```
(kali@kali) - [~]
└─$ sslscan 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:

- o Texto de fondo rojo: cifrado NULO. No se utilizó cifrado.
- o 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.
- o Amarillo: cifrado débil (menor o igual a 56 bits) o algoritmo de firma débil, como SHA-1.
- o Violeta: cifrado anónimo, como ADH o AECDH.



```
kali@kali:~$ sslls skillsforall.com
version: 1.4.10-stable
OpenSSL 1.1.1a-dev xx XXX xxxx

Connected to 18.64.174.55

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

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

TLS fallback SCV:
Server supports TLS fallback SCV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbeats:
TLSv1.2 not vulnerable to heartbeat
TLSv1.3 not vulnerable to heartbeat

Supported Server Ciphers:
Preferred TLSv1.2 256 Bits TLS_AES_128_GCM_SHA256 Curve 25519 DH256
Accepted TLSv1.1 256 Bits TLS_AES_128_GCM_SHA256 Curve 25519 DH256
Accepted TLSv1.2 256 Bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DH256
Preferred TLSv1.2 128 Bits ECDHE-RSA-AES128-GCM-SHA384 Curve 25519 DH256
Accepted TLSv1.2 256 Bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DH256
Accepted TLSv1.2 256 Bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DH256
Accepted TLSv1.2 256 Bits ECDHE-RSA-AES256-SHA384 Curve 25519 DH256
Accepted TLSv1.2 128 Bits ECDHE-RSA-AES128-SHA256 Curve 25519 DH256

Server Key Exchange Groups:
TLSv1.3 128 Bits secp256r1 (NIST P-256)
TLSv1.3 128 Bits secp384r1 (NIST P-384)
TLSv1.3 128 Bits secp521r1 (NIST P-521)
TLSv1.2 128 Bits secp256r1 (NIST P-256)
TLSv1.2 128 Bits secp384r1 (NIST P-384)
TLSv1.2 128 Bits secp521r1 (NIST P-521)

SSL Certificates:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: *.socialgoodplatform.com
AltNames: DNS:*.socialgoodplatform.com, DNS:skillsforall.com, DNS:socialgoodplatform.com
Issuer: Amazon RSA 2048 M02
```

- b. Si bien `sslls` ofrece opciones para generar resultados en formatos de archivo de texto o XML, `aha` proporciona la legibilidad de HTML y la preservación de la codificación de colores. Para usar `aha`, canalice la salida del comando `sslls` a `aha` y luego redirija la salida de `aha` a un archivo HTML.

```
—(kali@kali) - [~]
```

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

`sslls` 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.

- c. 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.

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

```
Ethical-Hacker-Kali [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
crtsh | skillsforall.com 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 18.64.174.87

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
Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve 25519 DHE 253

Server Key Exchange Group(s):
TLSv1.3 128 bits secp256r1 (NIST P-256)
TLSv1.3 192 bits secp384r1 (NIST P-384)
TLSv1.3 128 bits x25519
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 128 bits x25519

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048
```