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.590.

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.

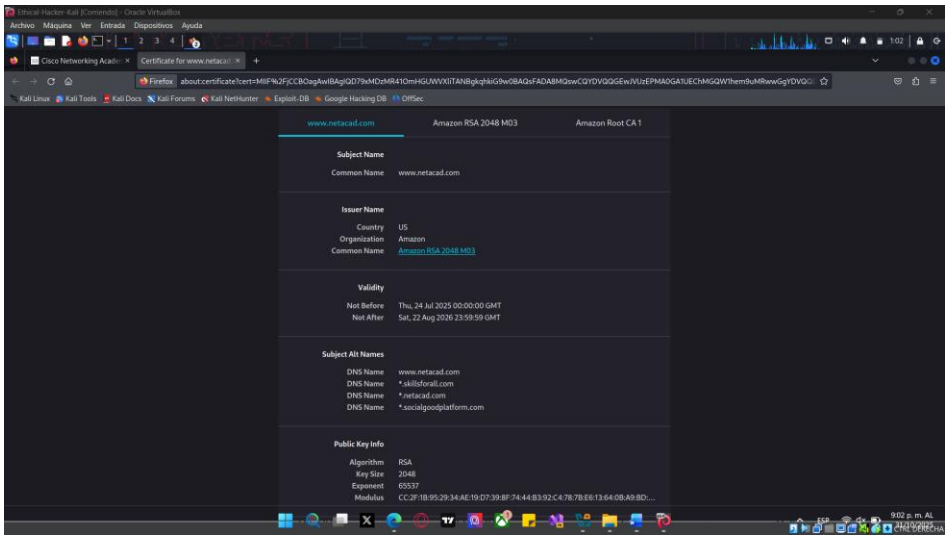
a. Navegue hasta **skillsforall.com**.

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.

c. 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.

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

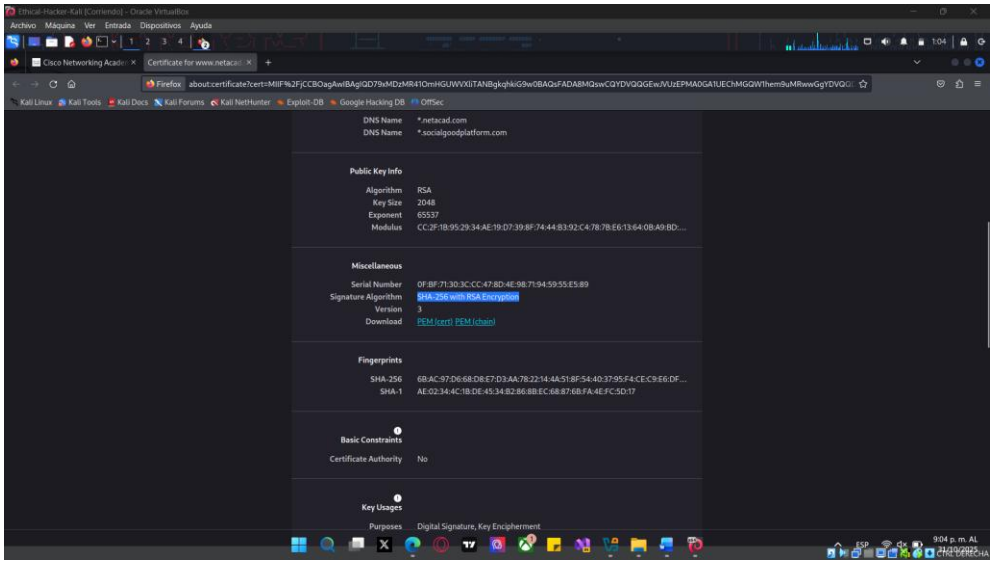
¿Para qué dominio se emitió el certificado? ¿Qué organización lo emitió?



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.

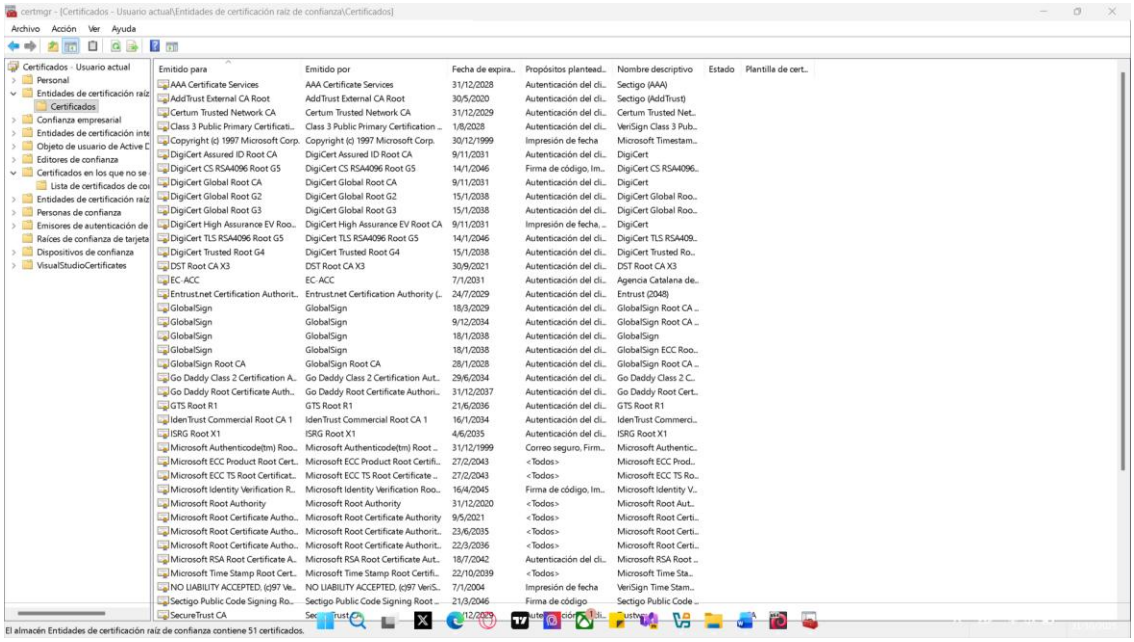
a. Microsoft Windows tiene una aplicación de administración de seguridad que forma parte de Microsoft Management Console. Ingrese **certmgr.msc** en el cuadro de búsqueda y presione Intro para abrirlo.

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?



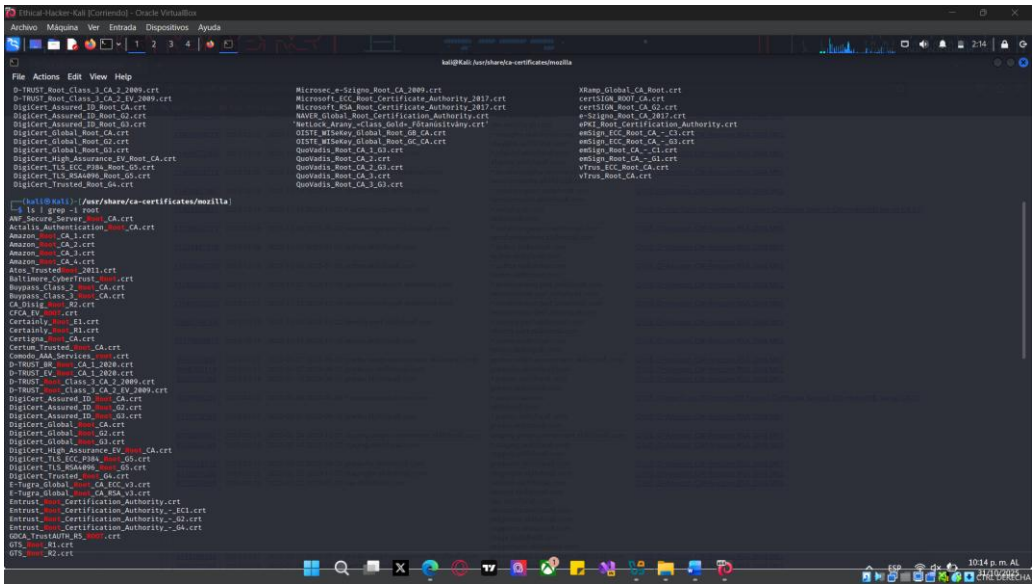
DigiCert Inc.: CA reconocida a nivel mundial, gran reputación en certificados comerciales de alto nivel.

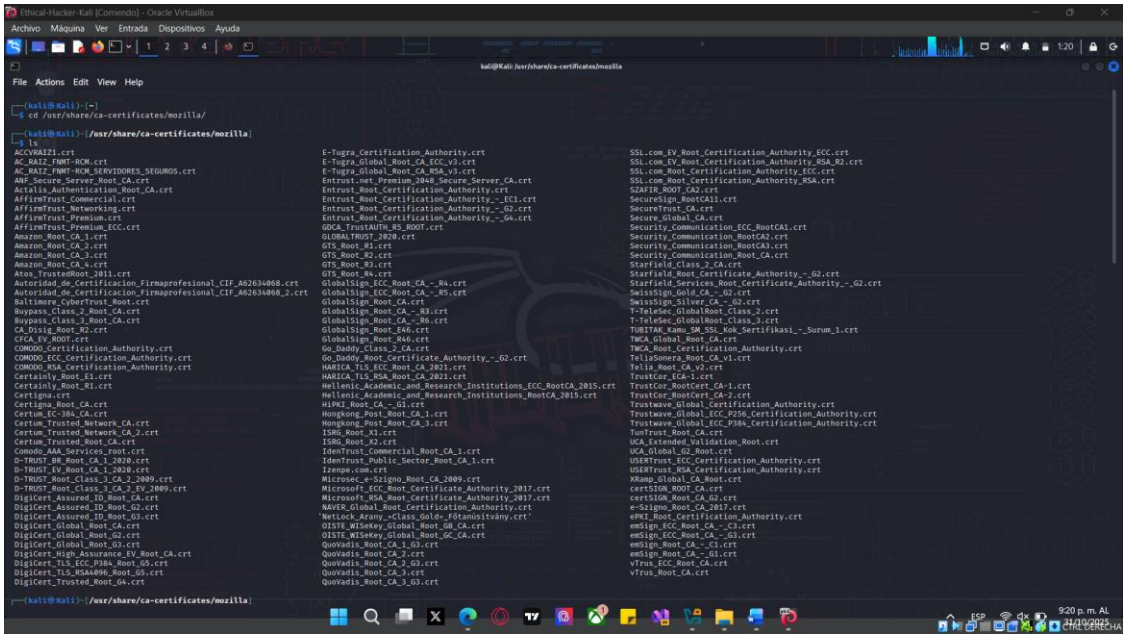
GlobalSign: también global, con raíces firmes y buen soporte para certificado raíz/medio.

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.





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.

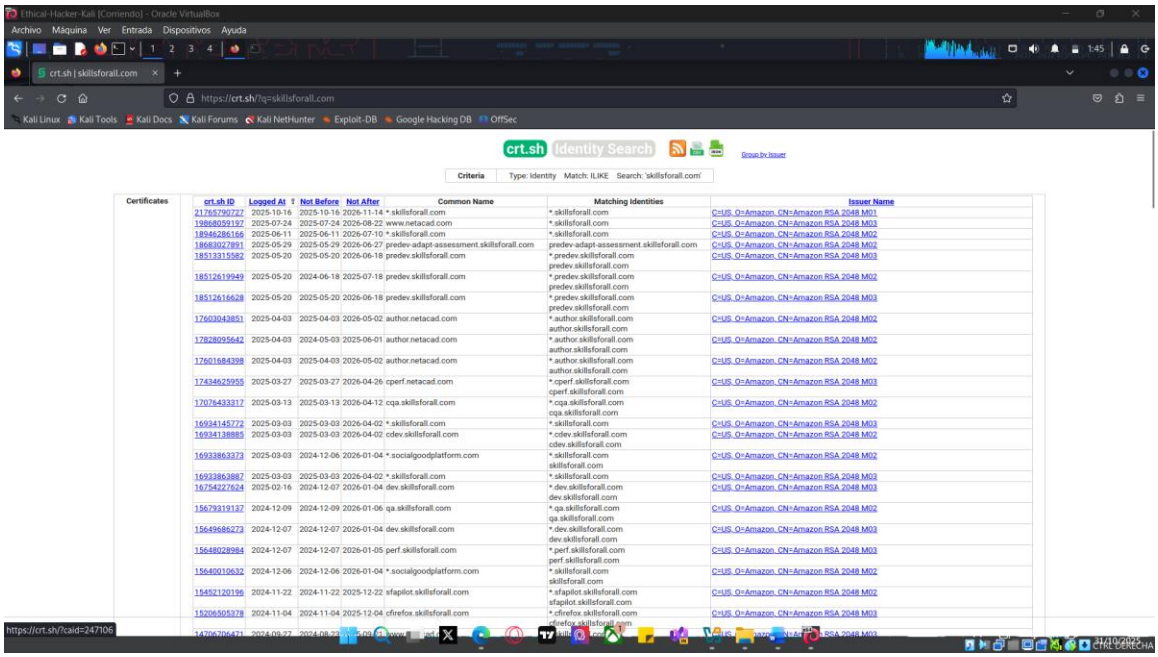
a. Abra un navegador y navegue a https://crt.sh.

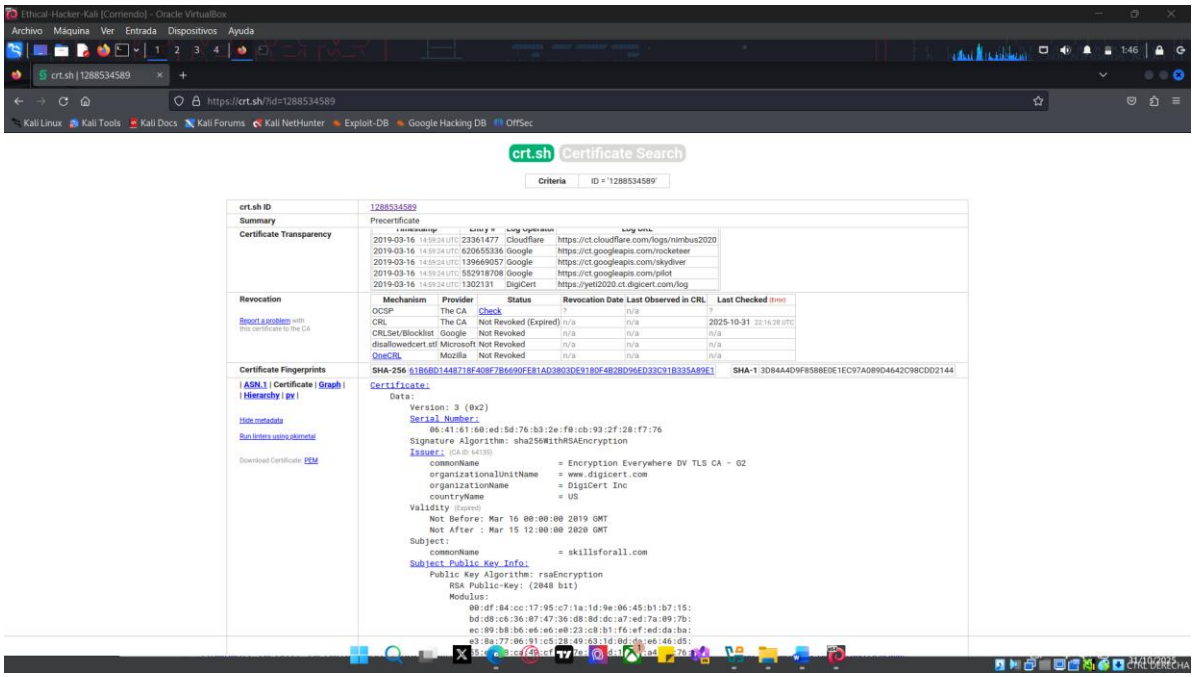
b. Ingrese la URL de **skillsforall.com** en el cuadro de búsqueda y haga clic en **Search**.

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.





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

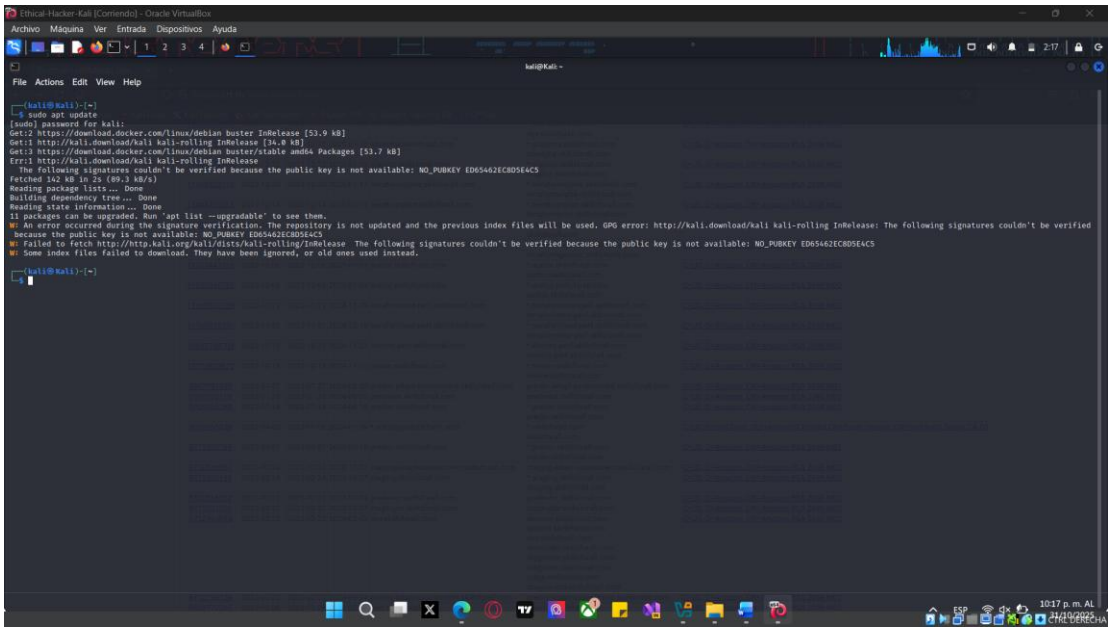
Como sabe, **sslscan** es una herramienta de reconocimiento de Kali que recopilará información sobre los certificados SSL asociados con los dominios. Es una utilidad de línea de comandos. Usaremos **sslscan** para recopilar información sobre certificados y usaremos otra utilidad, llamada **aha**, para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

Paso 1: Instalar aha.

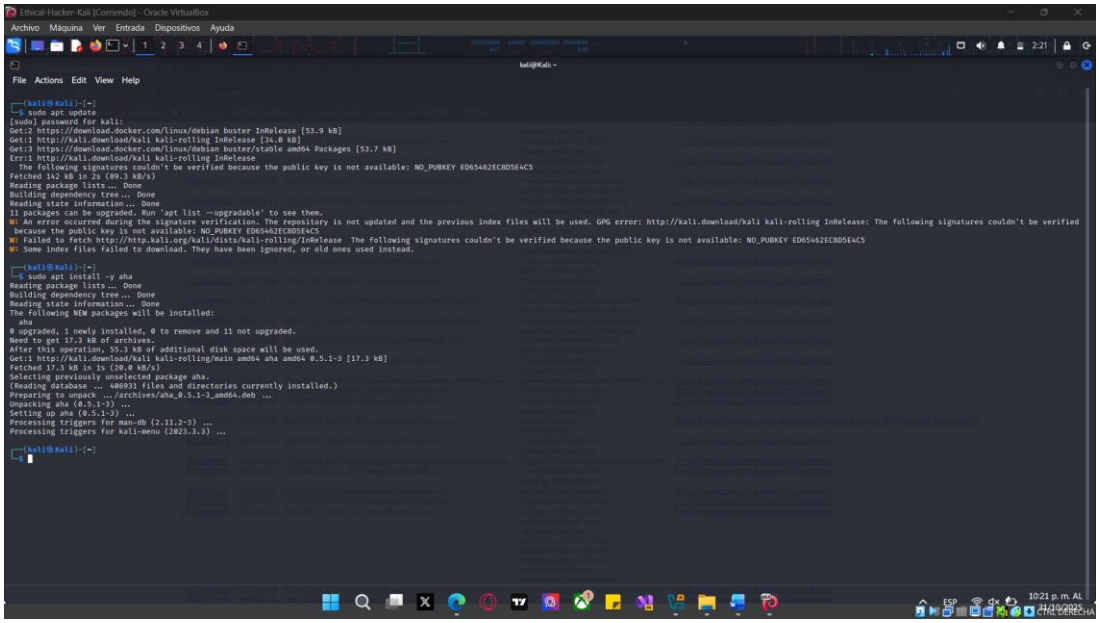
La aplicación **aha** crea un archivo HTML estándar que captura la salida de los comandos del terminal en archivos HTML estándar. Aha captura cualquier código de color y formato básico de la salida del comando. También tiene opciones de línea de comandos que le permiten especificar su propio formato,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

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

```
┌──(kali㉿Kali)-[~]
└─$ sudo apt update
```



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.



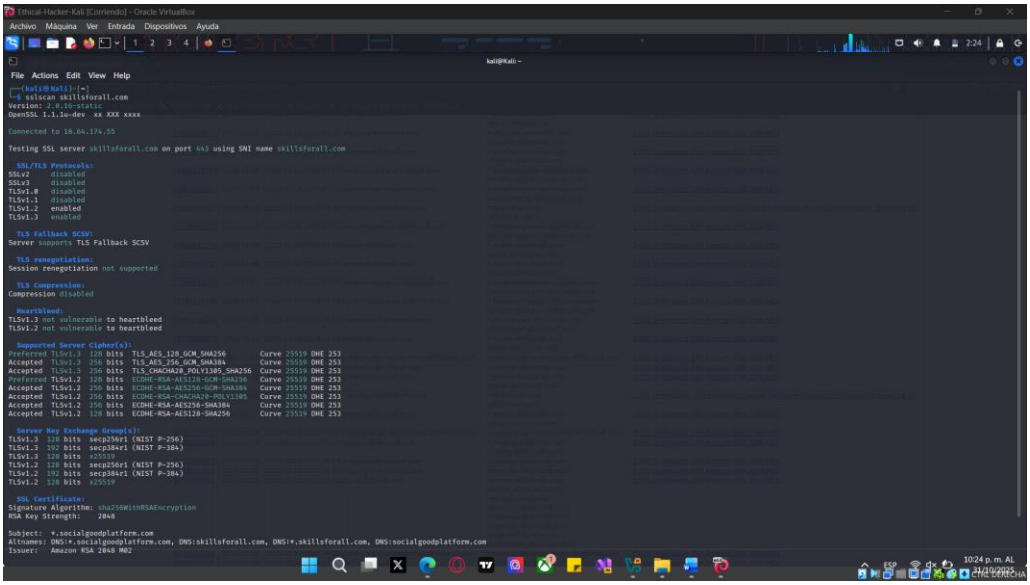
Paso 2: Ejecute sslscan y guarde el resultado en un archivo HTML.

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:

- 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.



b. Si bien sslscan 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 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.

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.