
SSL
Http
Https

Lab - Finding Information from SSL Certificates
SSL certificates are an essential part of online security. They are used to both encrypt data as it transmitted and establish that a website can be trusted as a source or destination for data. It is important to understand the identification and encryption information that is available in SSL certificates.

Objectives

- View Certificate Information on Hosts
- Access Detailed Certificate Information
- Use SSL Analysis Tools in Kali
- Use Kali Tools to Gather Certificate Information

Background / Scenario

SSL/TLS certificates functions.

1. They provide a way that the ownership of a website can be validated by people who are accessing it.
2. They provide a means by which communication between a client and server is encrypted so that it cannot be read or altered by unauthorized parties.

3. They provide the information required for a browser to create a secure, encrypted connection to a website over the HTTPS protocol.

Certificates are used behind the scenes as users browse the internet. In most cases, users are not aware that they are in use. The users become aware of them if a certificate is missing, out of date, or misconfigured.

Certificate information can be viewed locally for a website that is currently displayed in a browser by clicking the padlock icon next to the **URL** in the browser. Certificates are also stored locally for the certificate authorities themselves. There are various ways to view them. The format of public key certificate information is specified by the **X.509 standard.**

Ethical hackers can use public certificate information in the reconnaissance phase of penetration tests. Certificate information can reveal details about an organization including domain and subdomain names, issuance and expiration dates, and certificate public keys. In addition, certain versions of software, such as OpenSSL, have widely known vulnerabilities that can be exploited, including vulnerability to the heartbleed bug. In addition, it is possible that some certificates could use weak encryption algorithms.

Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

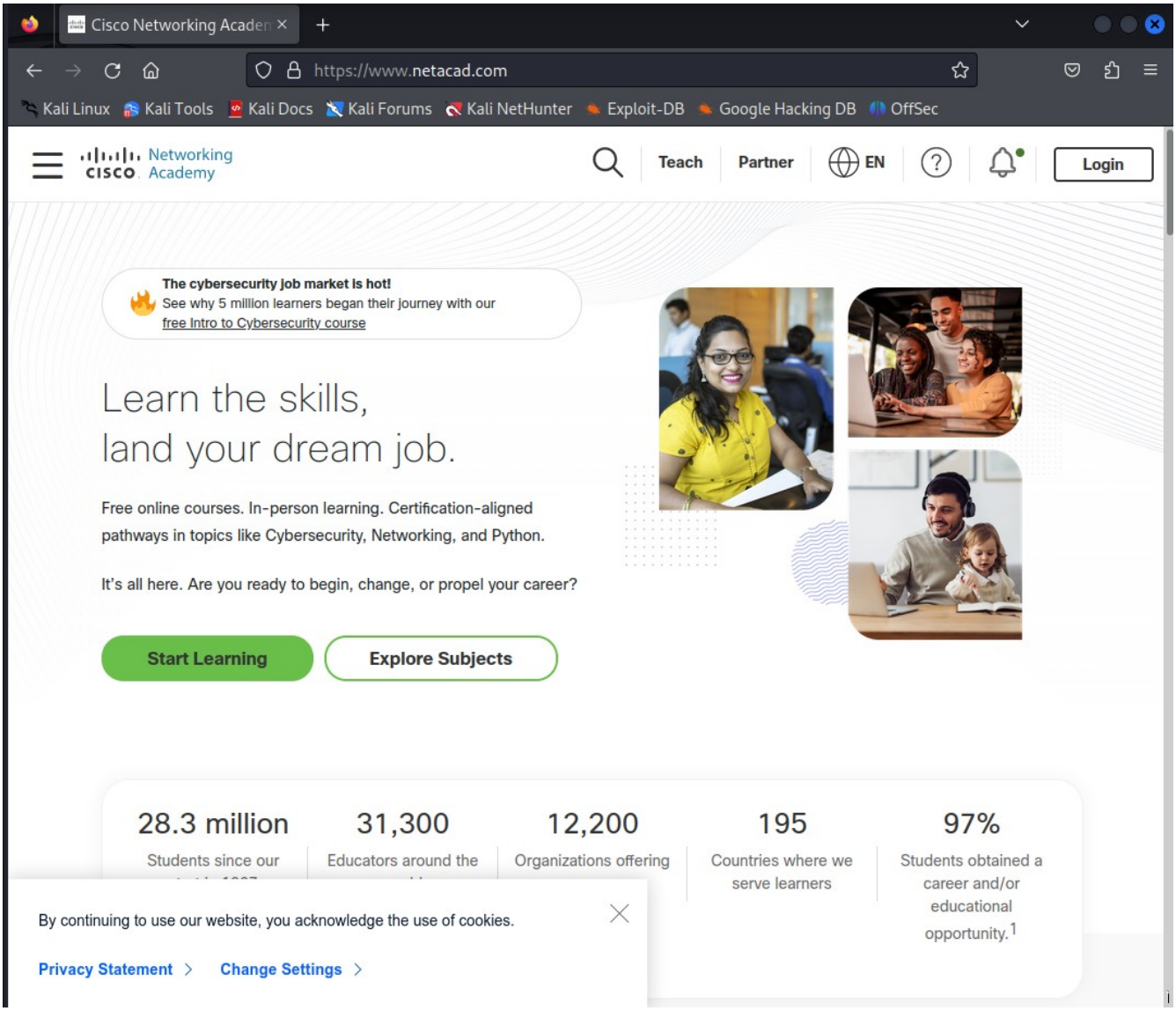
Instructions

Part 1: View Certificate Information on Hosts

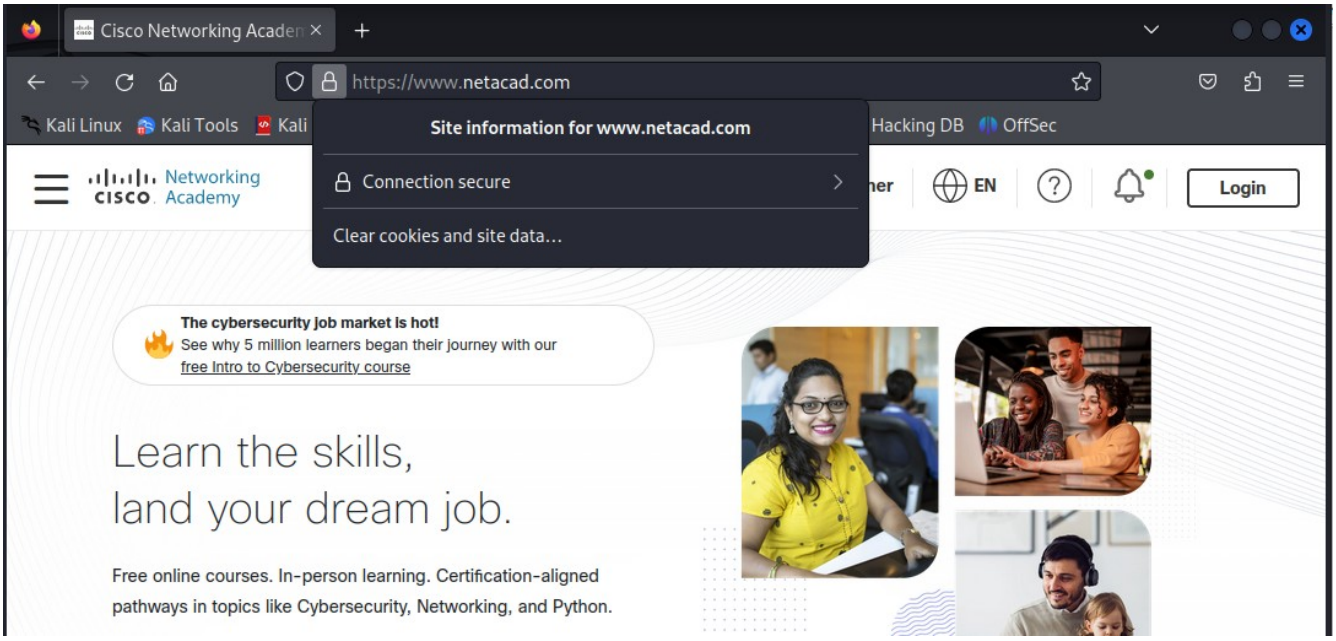
Some SSL certificates are stored locally on network hosts. These certificates allow secure communication between a host and a server through a certificate chain. A host stores intermediate and root certificates as part of the SSL authentication process.

Step 1: View site certificates from a browser.

a. Navigate to netacad.com.

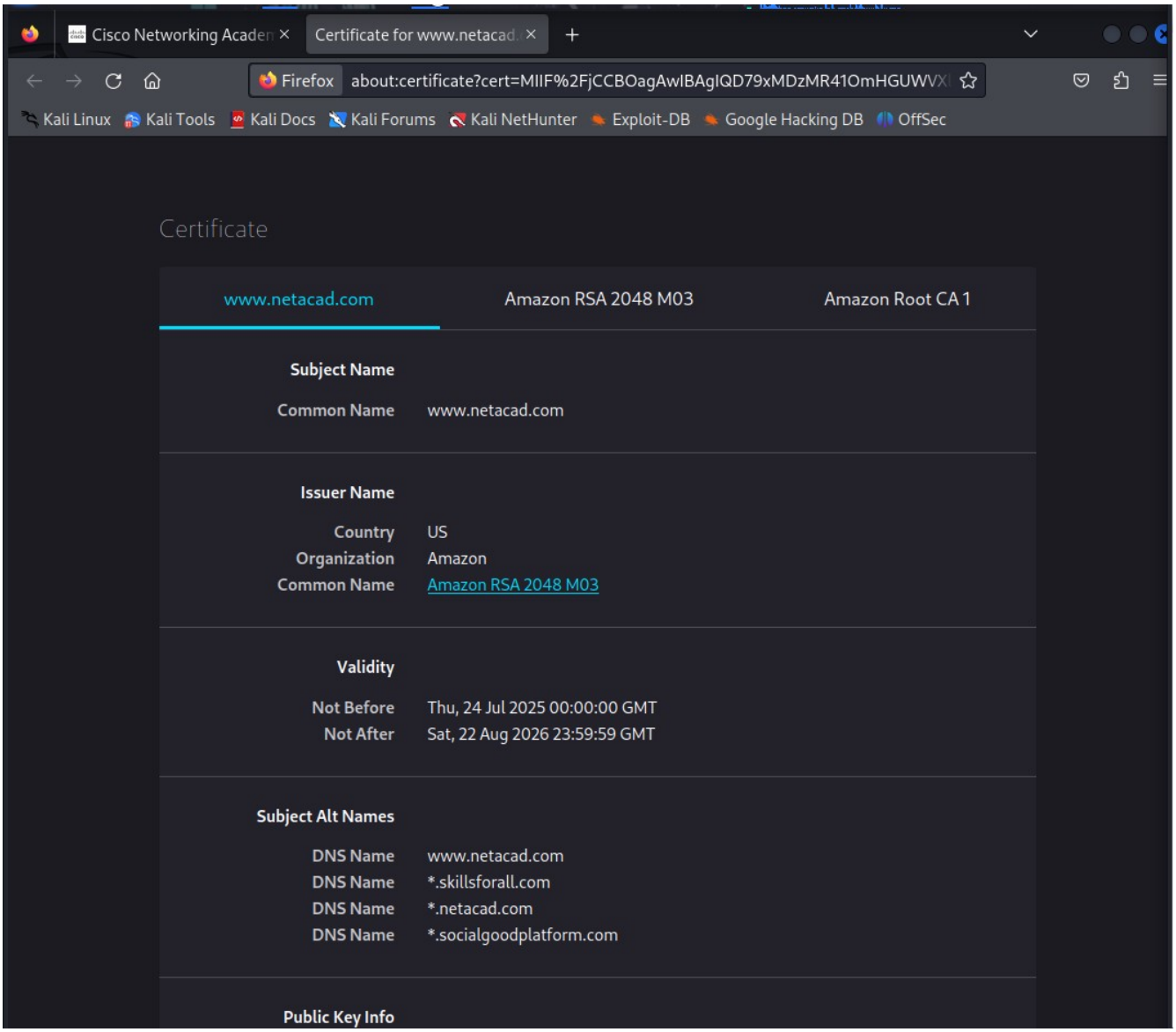


b. In most browsers, a padlock icon appears next to the URL of the site that is currently displayed. Click the padlock icon and explore the settings available.



c. Most browsers have a certificate manager that permits viewing details of certificates for websites or root certificates for certificate authorities. View certificate information while

browsing, using the padlock, or by opening certificate information from the browser security settings.



d. Look at the details for the Cisco Skills for All certificate and answer the following questions.

What domain was the certificate issued to? What organization issued it?

Answer Area

socialgoodplatform.com by Amazon

Show Answer

View the certificate. When will it expire?

Answer Area

Sat, 22 Aug 2026

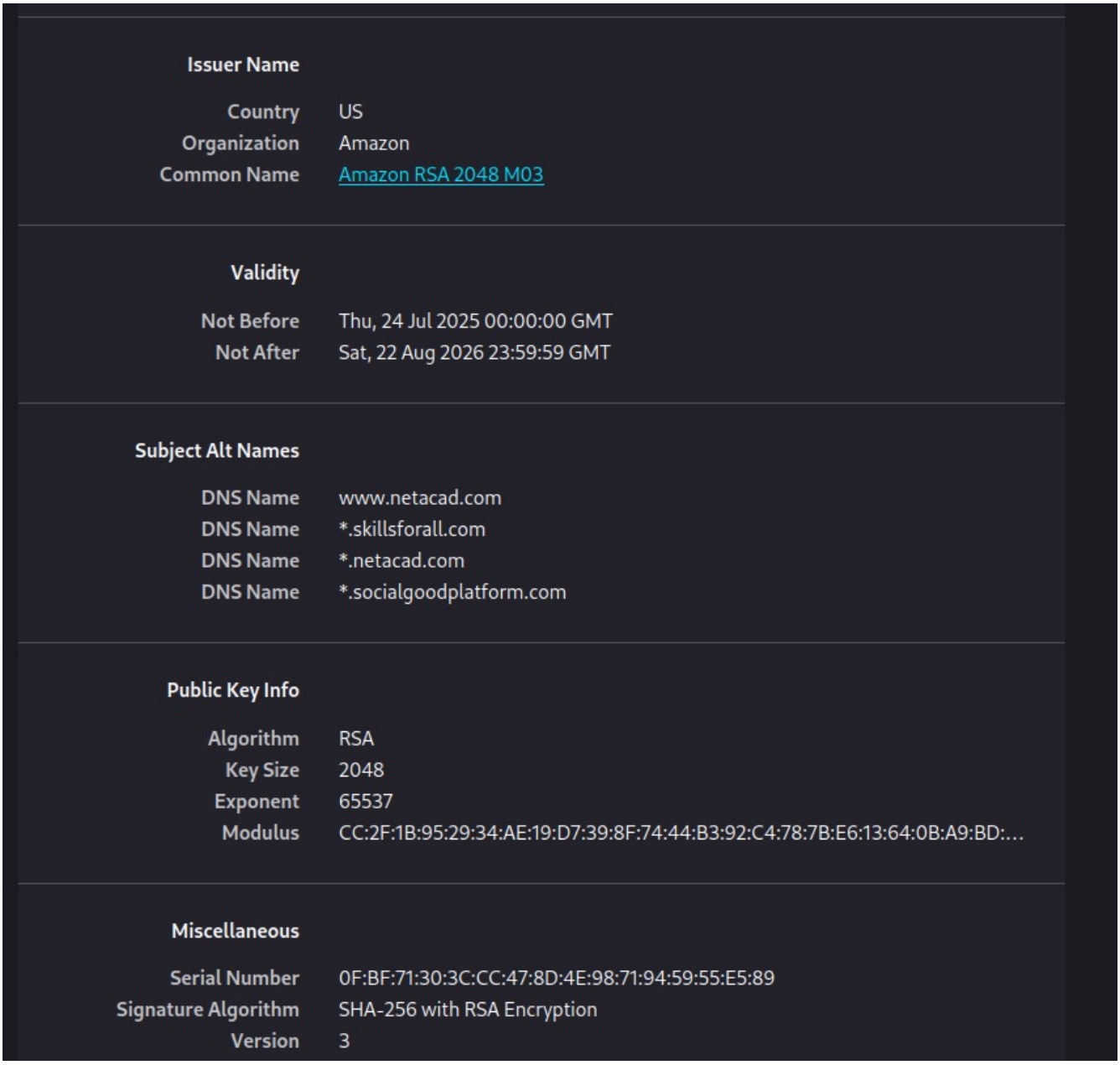
Show Answer

What is the certificate signature encryption algorithm?

Answer Area

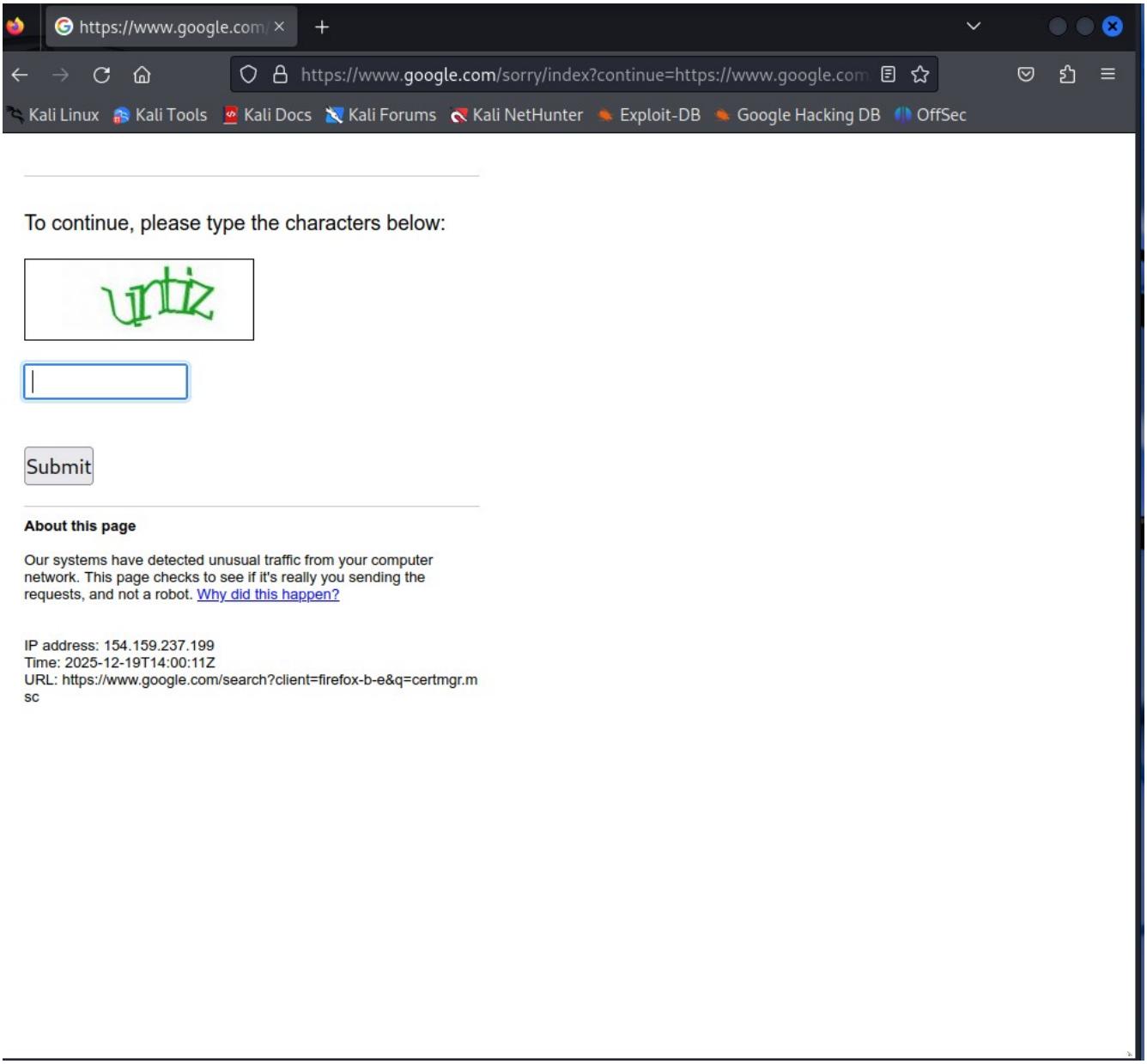
SHA-256 with RSA Encryption

Show Answer

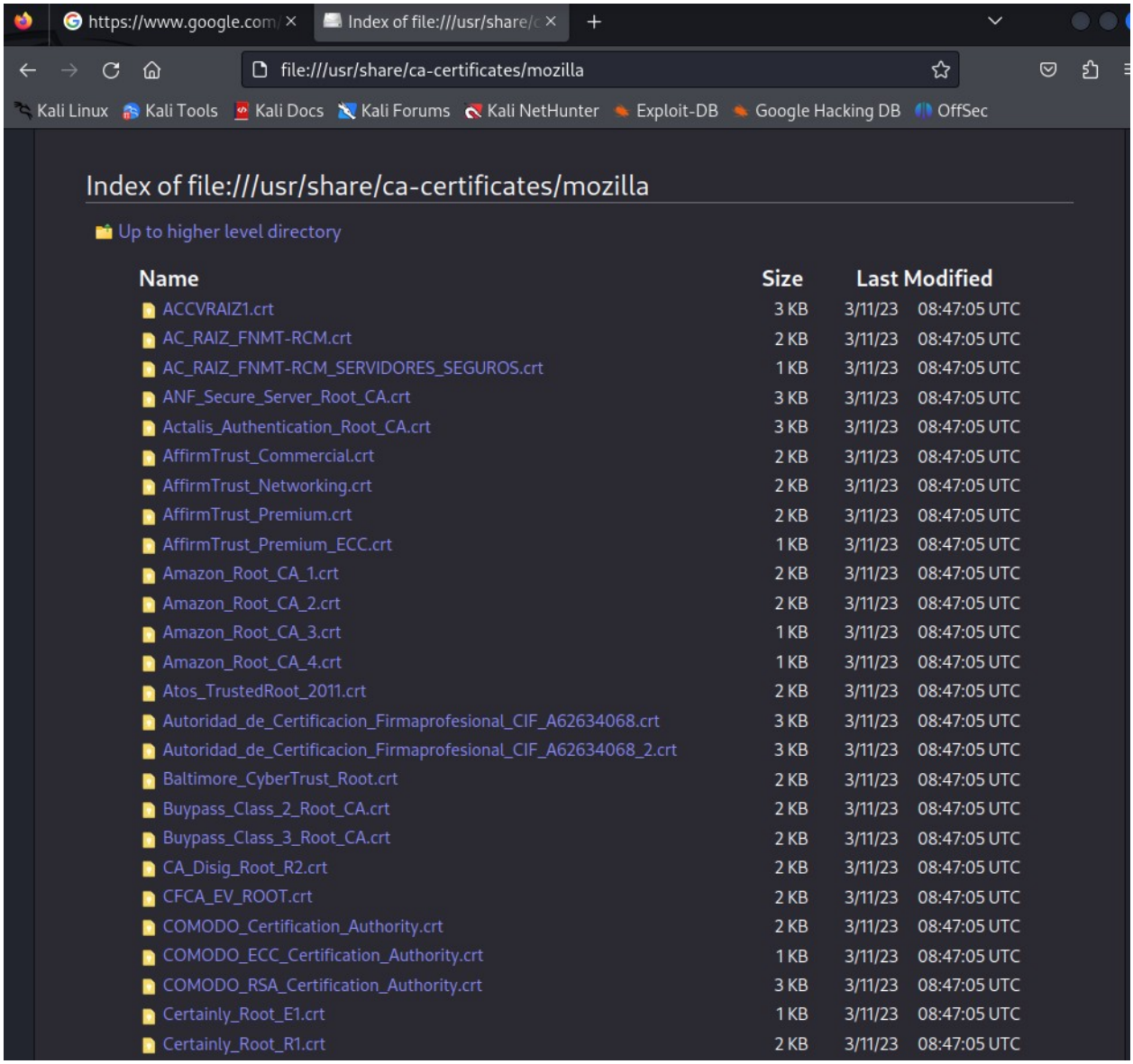


Step 2: View stored certificates in the operating system.

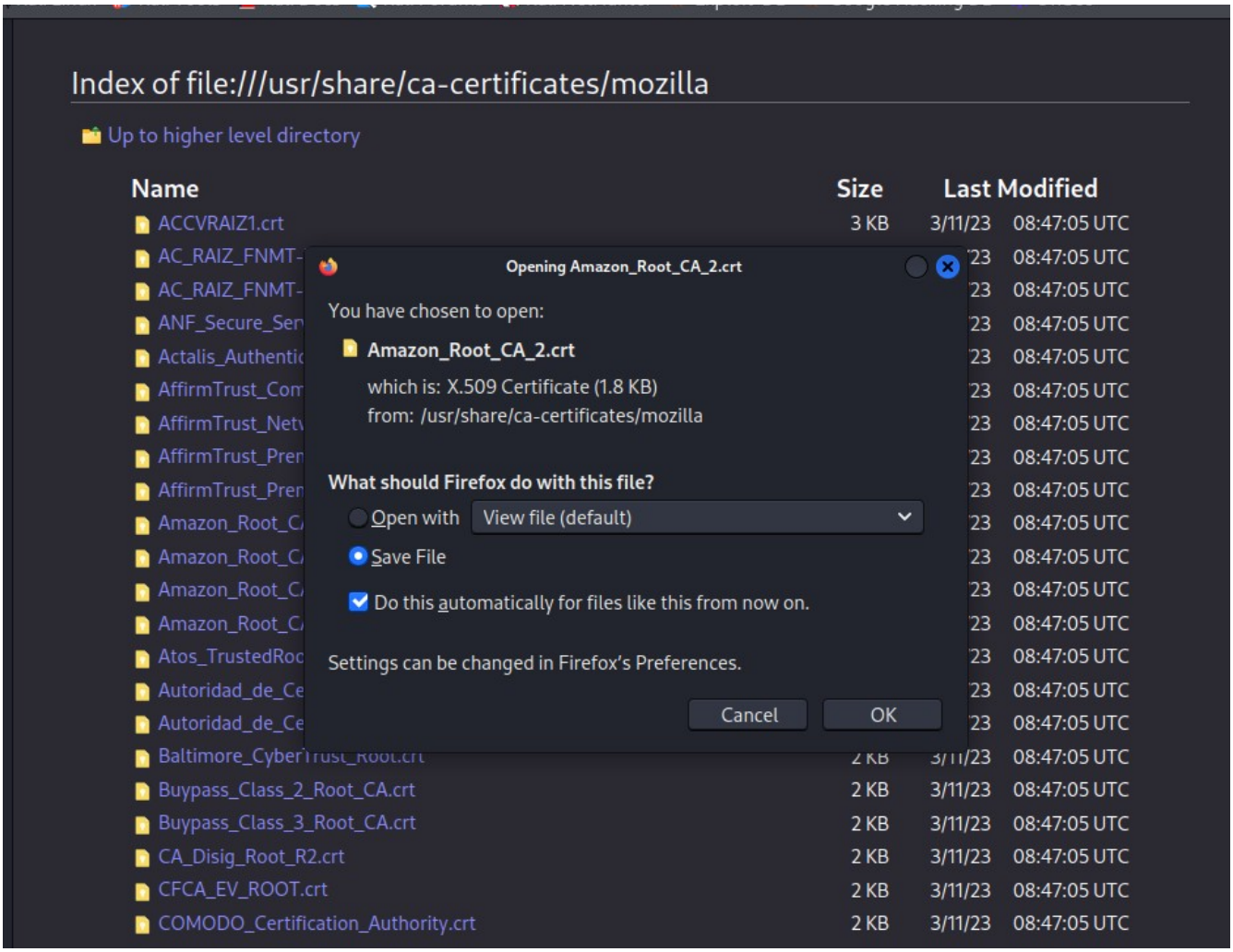
a. Microsoft Windows has a security management application that is part of the Microsoft Management Console. Enter **certmgr.msc** in the search box and press Enter to open it.



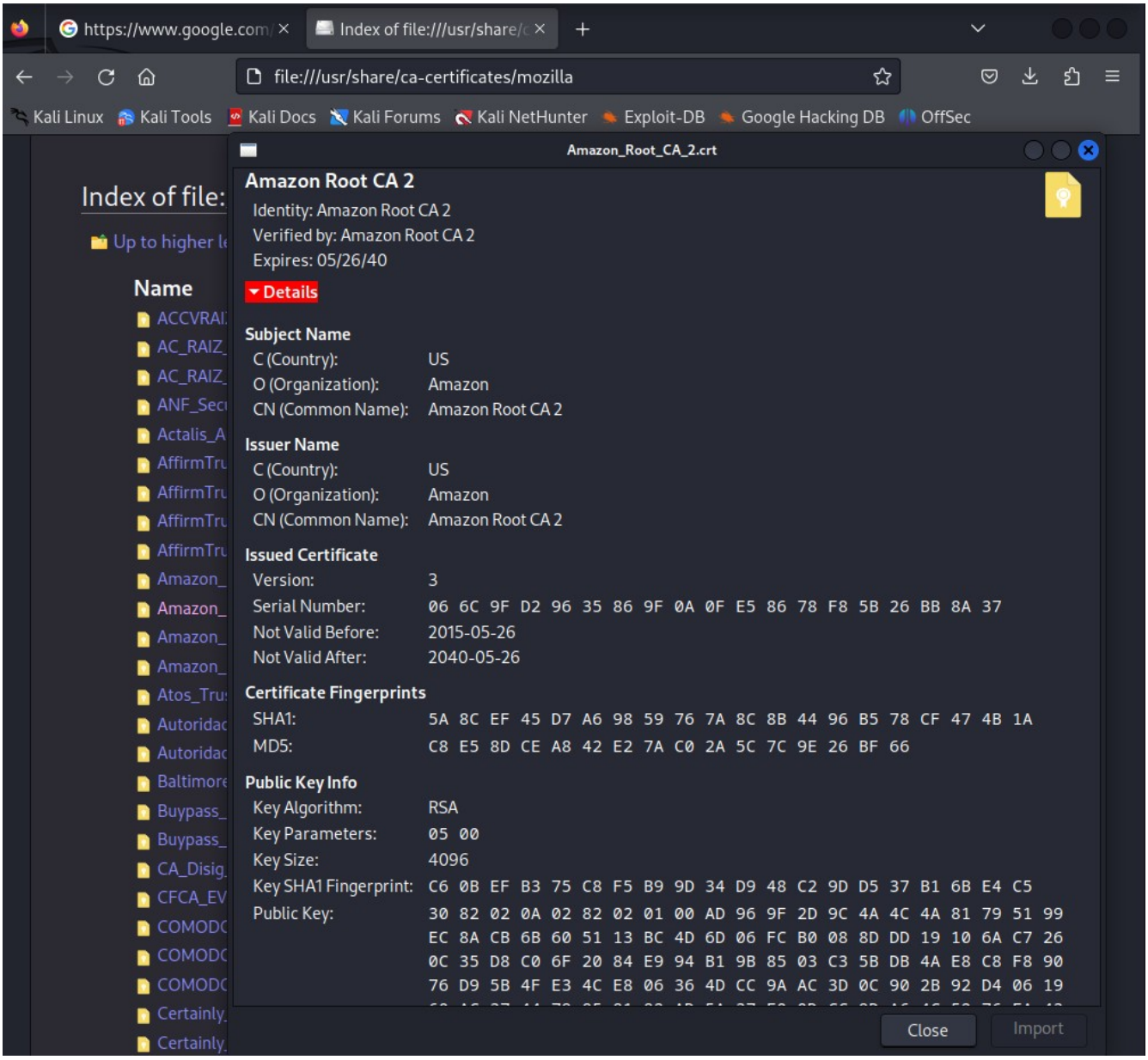
In Kali, you can find the stored certificates in the /usr/share/ca-certificates/mozilla folder.



Right-click a certificate and select **Open With "ViewFile"** to access the information for a certificate.



b. Access information about trusted root and intermediate certificates in Windows by selecting the appropriate certificate folders in the management app.



In Kali, access the certificates folder and use **ls -l | grep root** to list root certificate files, or search for the word **root** in the file manager window.

```
File  Actions  Edit  View  Help

┌──(kali㉿Kali)-[~]
└─$ cd /usr/share/ca-certificates/mozilla/

┌──(kali㉿Kali)-[/usr/share/ca-certificates/mozilla]
└─$ ls -l | grep root
-rw-r--r-- 1 root root 2772 Mar 11  2023 ACCVRAIZ1.crt
-rw-r--r-- 1 root root 1972 Mar 11  2023 AC_RAIZ_FNMT-RCM.crt
-rw-r--r-- 1 root root  904 Mar 11  2023 AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.
crt
-rw-r--r-- 1 root root 2118 Mar 11  2023 ANF_Secure_Server_Root_CA.crt
-rw-r--r-- 1 root root 2049 Mar 11  2023 Actalis_Authentication_Root_CA.crt
-rw-r--r-- 1 root root 1204 Mar 11  2023 AffirmTrust_Commercial.crt
-rw-r--r-- 1 root root 1204 Mar 11  2023 AffirmTrust_Networking.crt
-rw-r--r-- 1 root root 1891 Mar 11  2023 AffirmTrust_Premium.crt
-rw-r--r-- 1 root root  753 Mar 11  2023 AffirmTrust_Premium_ECC.crt
-rw-r--r-- 1 root root 1188 Mar 11  2023 Amazon_Root_CA_1.crt
-rw-r--r-- 1 root root 1883 Mar 11  2023 Amazon_Root_CA_2.crt
-rw-r--r-- 1 root root  656 Mar 11  2023 Amazon_Root_CA_3.crt
-rw-r--r-- 1 root root  737 Mar 11  2023 Amazon_Root_CA_4.crt
-rw-r--r-- 1 root root 1261 Mar 11  2023 Atos_TrustedRoot_2011.crt
-rw-r--r-- 1 root root 2167 Mar 11  2023 Autoridad_de_Certificacion_Firmaprof
esional_CIF_A62634068.crt
-rw-r--r-- 1 root root 2167 Mar 11  2023 Autoridad_de_Certificacion_Firmaprof
esional_CIF_A62634068_2.crt
-rw-r--r-- 1 root root 1261 Mar 11  2023 Baltimore_CyberTrust_Root.crt
-rw-r--r-- 1 root root 1915 Mar 11  2023 Buypass_Class_2_Root_CA.crt
-rw-r--r-- 1 root root 1915 Mar 11  2023 Buypass_Class_3_Root_CA.crt
-rw-r--r-- 1 root root 1935 Mar 11  2023 CA_Disig_Root_R2.crt
-rw-r--r-- 1 root root 1984 Mar 11  2023 CFCA_EV_ROOT.crt
-rw-r--r-- 1 root root 1489 Mar 11  2023 COMODO_Certification_Authority.crt
-rw-r--r-- 1 root root  940 Mar 11  2023 COMODO_ECC_Certification_Authority.c
rt
-rw-r--r-- 1 root root 2086 Mar 11  2023 COMODO_RSA_Certification_Authority.c
rt
-rw-r--r-- 1 root root  741 Mar 11  2023 Certainly_Root_E1.crt
-rw-r--r-- 1 root root 1891 Mar 11  2023 Certainly_Root_R1.crt
-rw-r--r-- 1 root root 1330 Mar 11  2023 Certigna.crt
-rw-r--r-- 1 root root 2264 Mar 11  2023 Certigna_Root_CA.crt
-rw-r--r-- 1 root root  891 Mar 11  2023 Certum_EC-384_CA.crt
-rw-r--r-- 1 root root 1354 Mar 11  2023 Certum_Trusted_Network_CA.crt
-rw-r--r-- 1 root root 2078 Mar 11  2023 Certum_Trusted_Network_CA_2.crt
-rw-r--r-- 1 root root 2053 Mar 11  2023 Certum_Trusted_Root_CA.crt
-rw-r--r-- 1 root root 1517 Mar 11  2023 Comodo_AAA_Services_root.crt
-rw-r--r-- 1 root root 1050 Mar 11  2023 D-TRUST_BR_Root_CA_1_2020.crt
-rw-r--r-- 1 root root 1050 Mar 11  2023 D-TRUST_EV_Root_CA_1_2020.crt
-rw-r--r-- 1 root root 1517 Mar 11  2023 D-TRUST_Root_Class_3_CA_2_2009.crt
-rw-r--r-- 1 root root 1537 Mar 11  2023 D-TRUST_Root_Class_3_CA_2_EV_2009.cr
t
-rw-r--r-- 1 root root 1350 Mar 11  2023 DigiCert_Assured_ID_Root_CA.crt
-rw-r--r-- 1 root root 1306 Mar 11  2023 DigiCert_Assured_ID_Root_G2.crt
-rw-r--r-- 1 root root  851 Mar 11  2023 DigiCert_Assured_ID_Root_G3.crt
-rw-r--r-- 1 root root 1338 Mar 11  2023 DigiCert_Global_Root_CA.crt
```

The names of the root certificate files refer to the certificate authority that granted them. What are three of the most common certificate authorities on your computer? Research them on the internet. What is the cost of a single domain basic SSL certificate for one year?

Answer Area

DigiCert $150 to $250+
GlobalSign $249 USD
Go_Daddy $100-$200

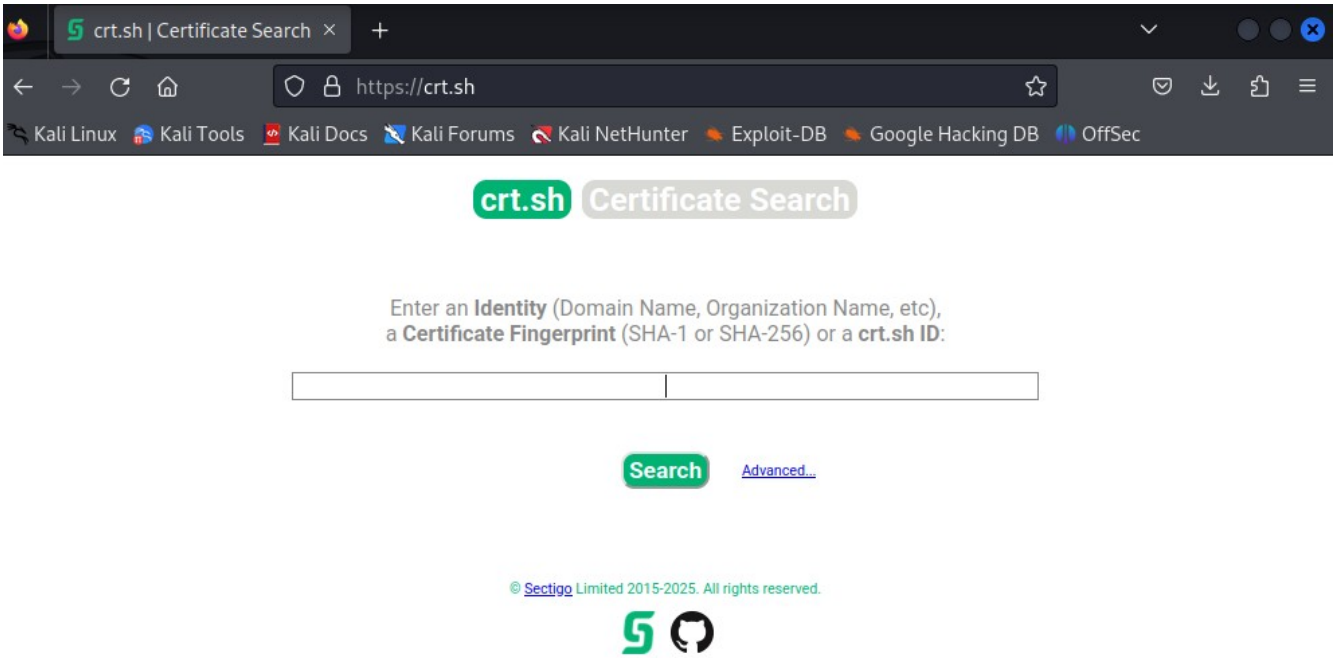
Part 2: Access Detailed Certificate Information Online

Certificate Transparency (CT) is an open framework for monitoring and auditing the issuance of SSL/TLS certificates. CT requires that all publicly trusted certificate authorities (CAs) log all issued certificates in publicly available, tamper-evident, and auditable logs. These logs can be monitored to detect any fraudulent or malicious issuance of SSL/TLS certificates, including certificates issued for domains that the attacker does not control.

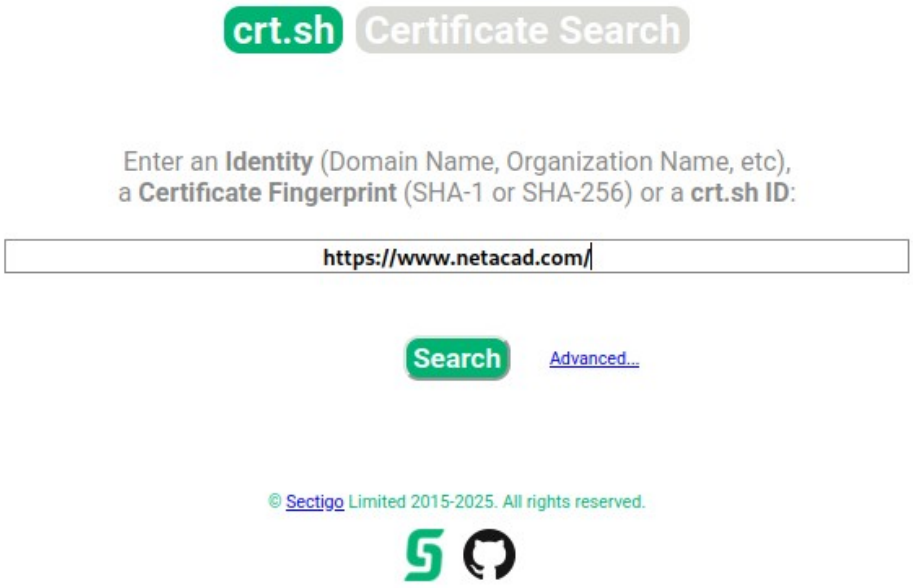
In OSINT, CT logs can be used to gather information about SSL/TLS certificates used by an organization or a specific domain. By analyzing CT logs, analysts can identify certificate issuances and their associated domains, as well as any anomalies or irregularities in certificate issuance. CT logs can also be used to monitor for any unauthorized SSL/TLS certificate issuance, which could indicate a potential security breach.

CT logs can be accessed through various CT log servers and APIs. There are also several CT monitoring tools available, such as CertSpotter and Censys, which can help automate the process of monitoring CT logs for specific domains or SSL/TLS certificates.

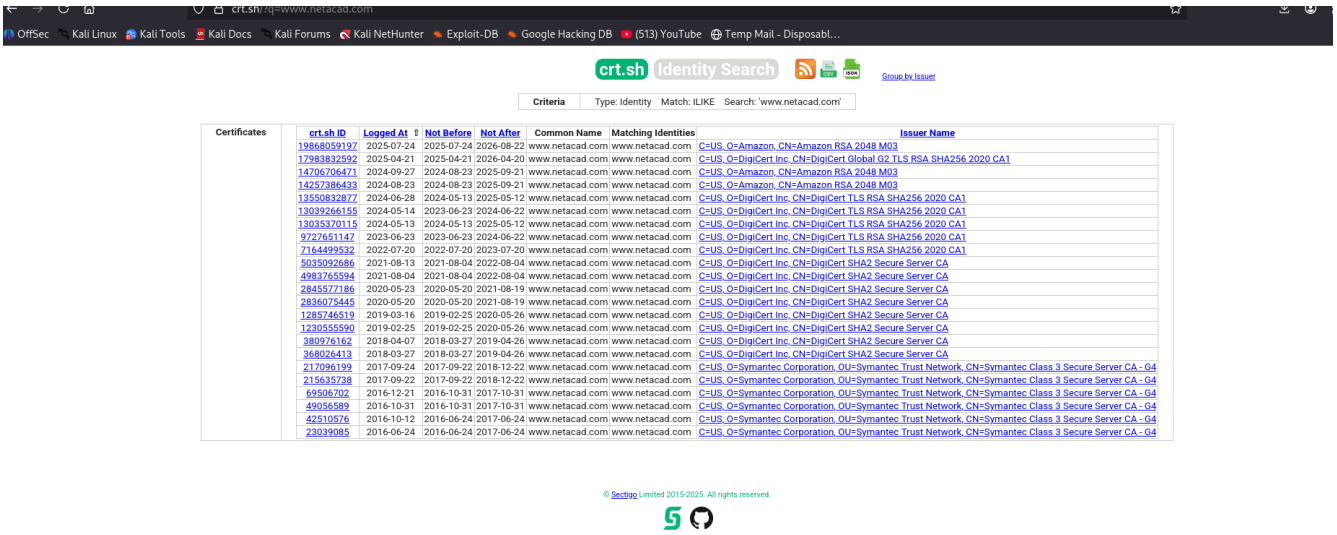
a. Open a browser and navigate to **https://crt.sh**



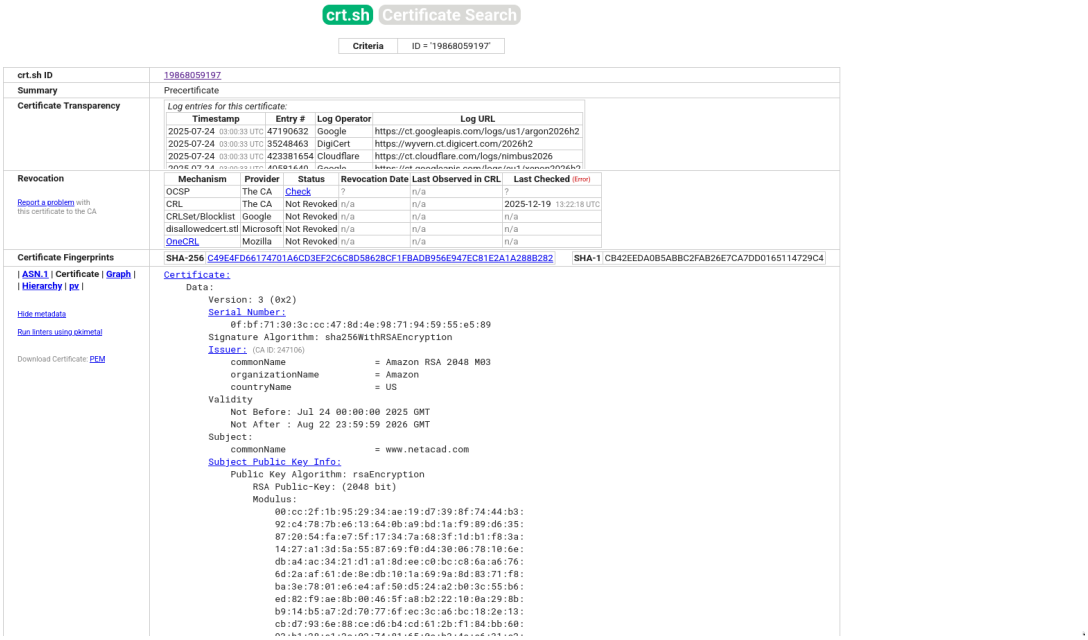
b. Enter the Skills for All URL in the search box and click **Search**.



c. The resulting table lists comprehensive information for certificates issued to netacad.com and related subdomains. The list goes back to 2016. crt.sh



d. provides IDs for the certificates but these IDs are relevant to crt.sh only. Clicking an ID takes you to the available certificate details



crt.sh Certificate Search

Criteria | ID = '19868059197'

crt.sh ID	19868059197
Summary	Precertificate

Certificate Transparency

Log entries for this certificate:

Timestamp	Entry #	Log Operator	Log URL
2025-07-24 03:00:33 UTC	47190632	Google	https://ct.googleapis.com/logs/us1/argon2026h2
2025-07-24 03:00:33 UTC	35248463	DigiCert	https://wyvern.ct.digicert.com/2026h2
2025-07-24 03:00:33 UTC	423381654	Cloudflare	https://ct.cloudflare.com/logs/nimbus2026
2025-07-24 03:00:33 UTC	40681440	Google	https://ct.googleapis.com/logs/eu1/xenon2026h2

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Not Revoked	n/a	n/a	2025-12-19 13:22:18 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

SHA-256 C49E4FD66174701A6CD3EF2C6C8D5862BCF1FBADB956E947EC81E2A1A288B282 SHA-1 CB42EEDA0B5ABBC2FAB26E7CA7DD0165114729C4

| ASN.1 | Certificate | Graph | Hierarchy | pv |

Hide metadata

Run linters using pkimetal

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0f:bf:71:30:3c:cc:47:8d:4e:98:71:94:59:55:e5:89
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 247106)
            commonName               = Amazon RSA 2048 M03
            organizationName         = Amazon
            countryName              = US
        Validity
            Not Before: Jul 24 00:00:00 2025 GMT
            Not After : Aug 22 23:59:59 2026 GMT
        Subject:
            commonName               = www.netacad.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cc:2f:1b:95:29:34:ae:19:d7:39:8f:74:44:b3:
                    92:c4:78:7b:e6:13:64:0b:a9:bd:1a:f9:89:d6:35:
                    87:20:54:fa:e7:5f:17:34:7a:68:3f:1d:b1:f8:3a:
                    14:27:a1:3d:5a:55:87:69:f0:d4:30:06:78:10:6e:
                    db:a4:ac:34:21:d1:a1:8d:ee:c0:bc:c8:6a:a6:76:
                    6d:2a:af:61:de:8e:db:10:1a:69:9a:8d:83:71:f8:
                    ba:3e:78:01:e6:e4:af:50:d5:24:a2:b0:3c:55:b6:
                    ed:82:f9:ae:8b:00:46:5f:a8:b2:22:10:0a:29:8b:
                    b9:14:b5:a7:2d:70:77:6f:ec:3c:a6:bc:18:2e:13:
                    cb:d7:93:6e:88:ce:d6:b4:cd:61:2b:f1:84:bb:60:
```

Part 3: Use SSL Analysis Tools in Kali

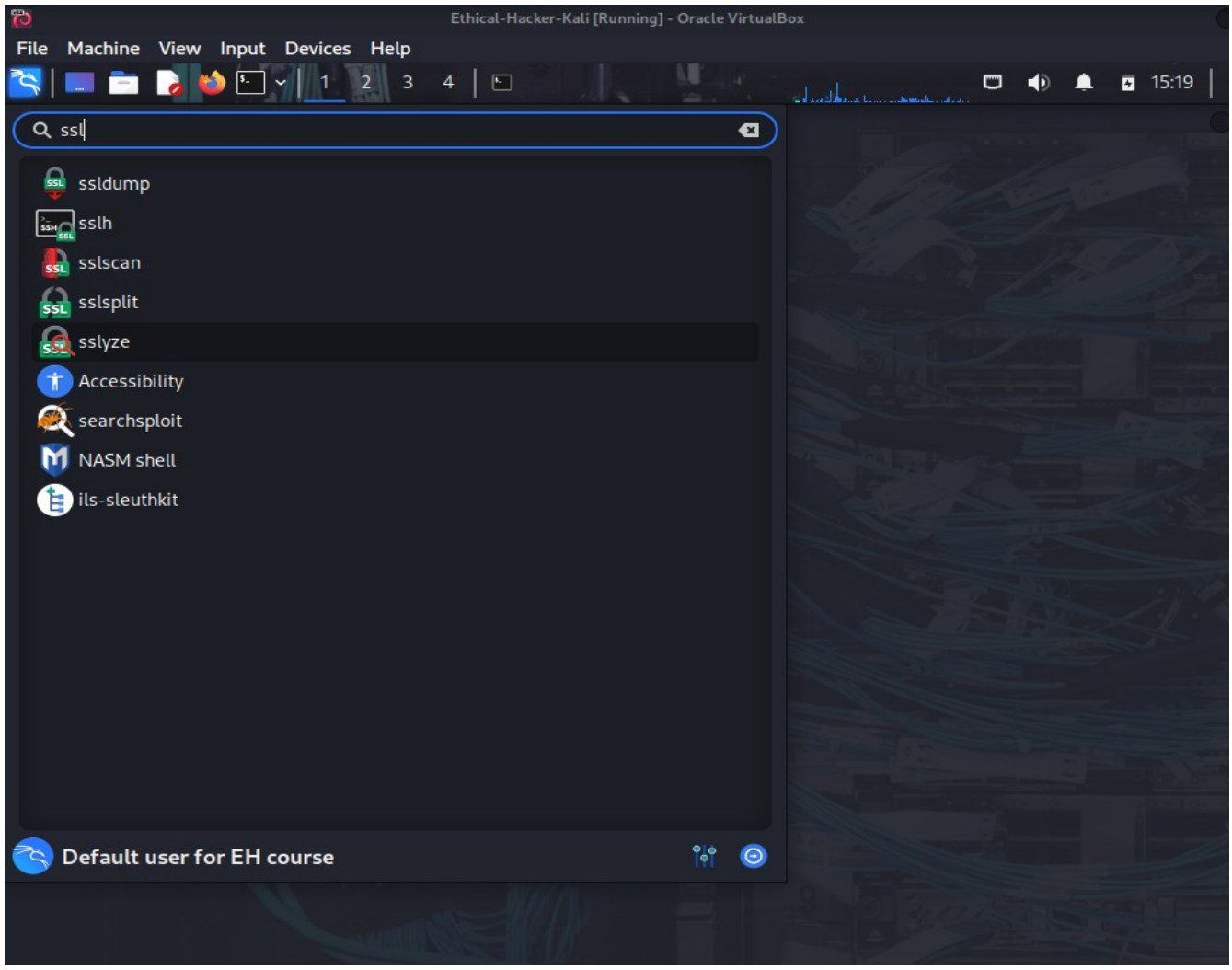
Step 1: Investigate Kali Tools

a. Start the Kali virtual machine and log in.

b. Start a terminal session.

c. Kali comes with several SSL-related tools. Click the Kali programs icon and search on the term **ssl**.

d. Use the Kali tools reference to complete the table below for the five SSL tools included with your Kali distribution.



Tool	Description	Recon, Exploitation, or Utility
sslscan	Queries SSL services to determine what cyphers are supported	Reconnaissance
ssldump	Analyze and decode SSL traffic	Exploitation
sslh	Running multiple services on port 443	Utility
sslsplit	Enable MitM attacks on SSL encrypted network connections	Exploitation
sslyze	Analyze the SSL configuration of a server by connecting to it	Reconnaissance

Part 4: Use Kali Tools to Gather Certificate Information

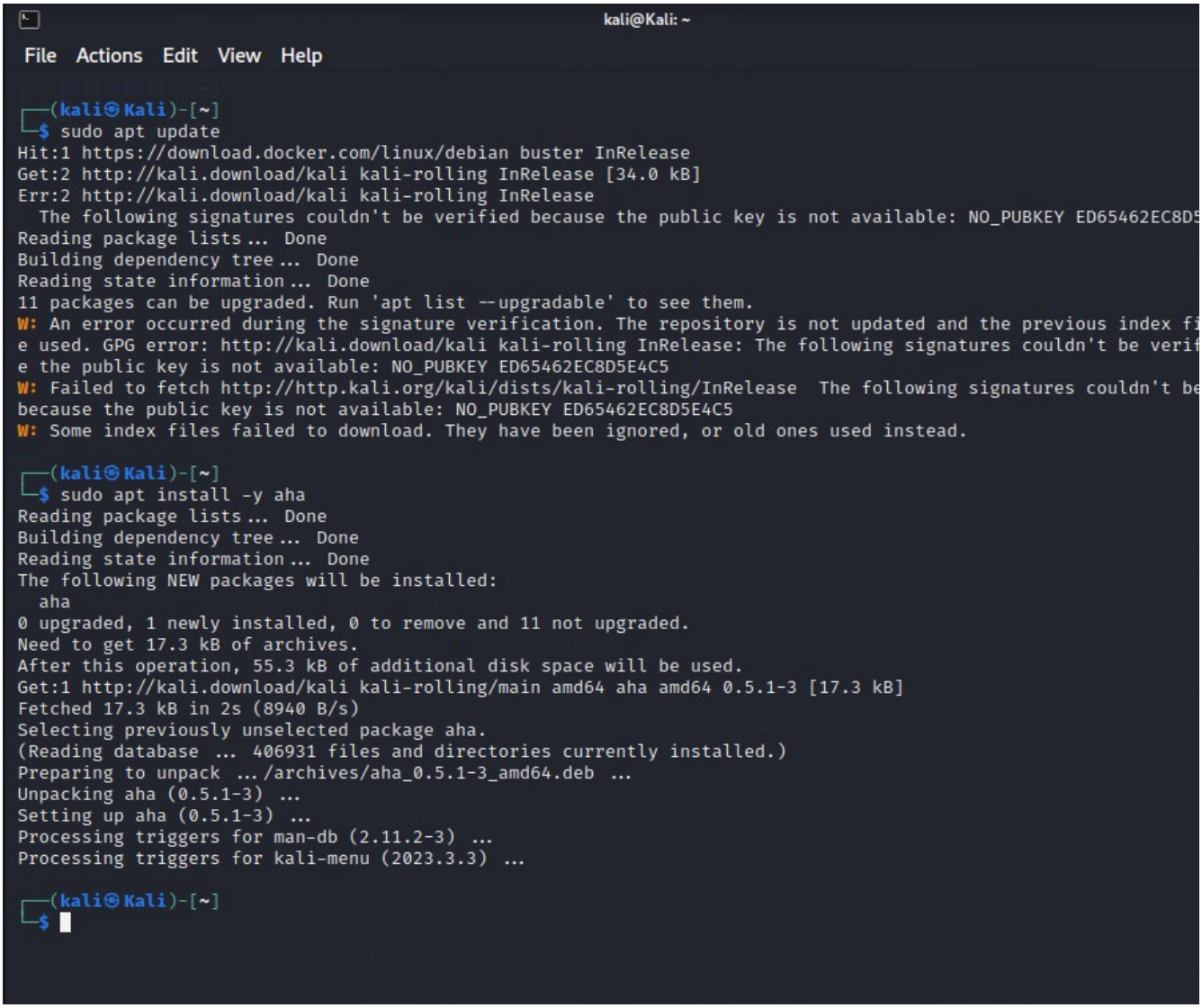
As you know, **sslscan** is a Kali tool reconnaissance that will gather information about SSL certificates that are associated with domains. It is a command line utility. We will use **sslscan** to gather information about certificates and use another utility, called **aha**, to output the results to an HTML file.

Step 1: Install aha.

The application **aha** creates a standard HTML file that captures the output of terminal commands to standard HTML files. Aha captures any color coding and basic formatting of the command output. It also has command line options that allow you to specify your own formatting, such as background color, stylesheets to apply, and word wrap, among other settings.

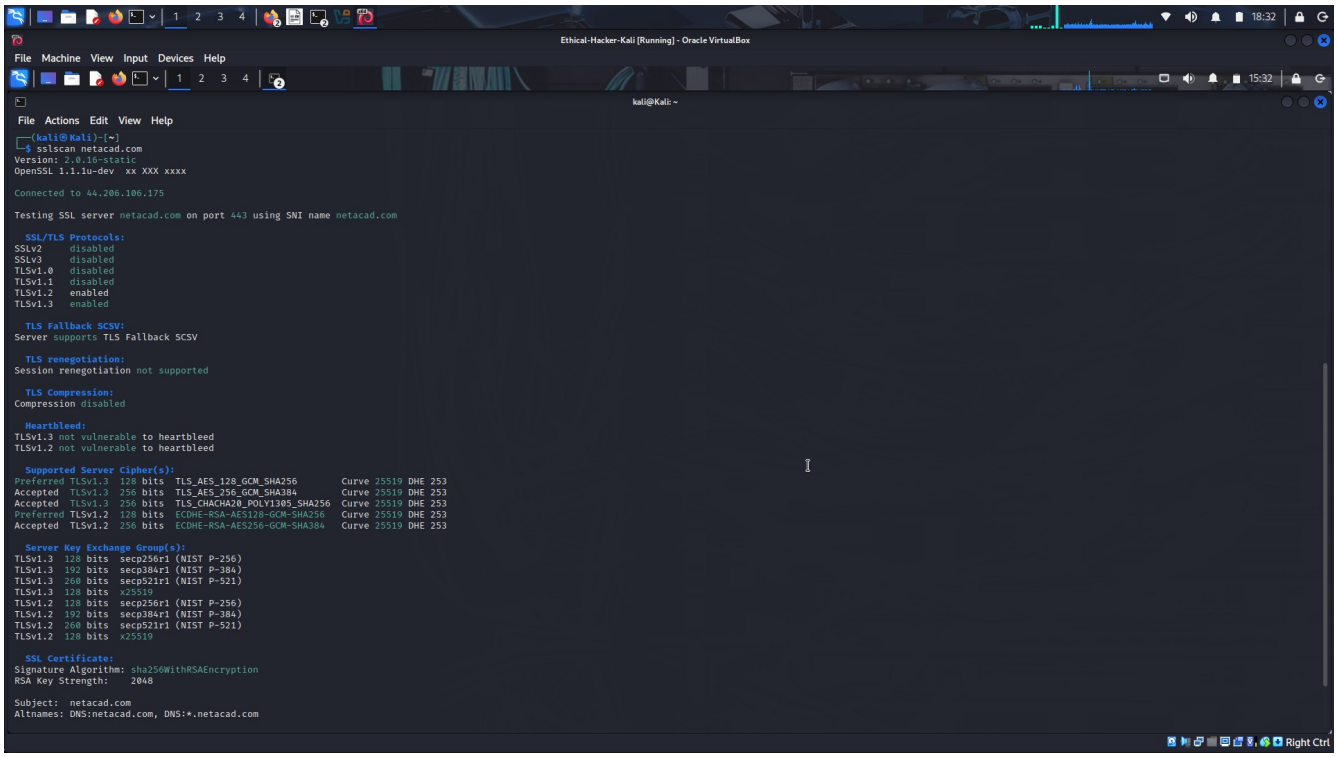
Update your apt package information with the **apt update** command. This requires root privileges.

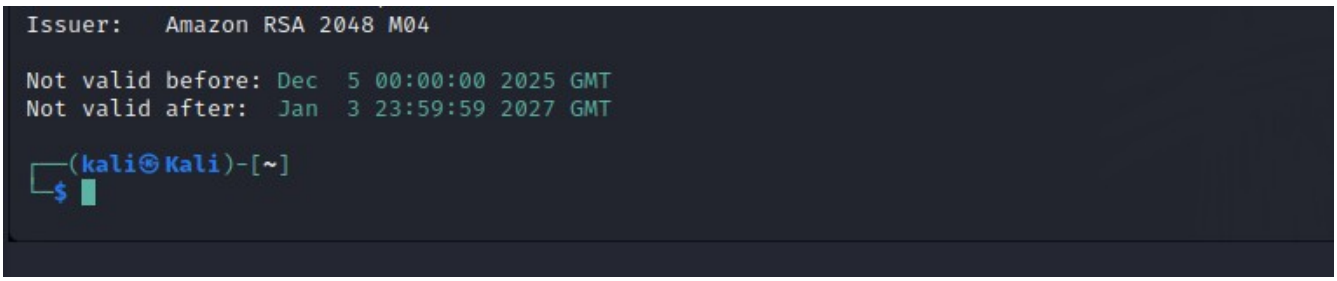
Install aha with the **sudo apt install -y aha** command. The option -y assumes **yes** is the answers to all prompts and can run non-interactively. In this case, you are giving permission to install aha.



Step 2: Run sslscan and save the output to an HTML file.

a. From a terminal command line, execute the command to run **sslscan** with the netacad.com target.





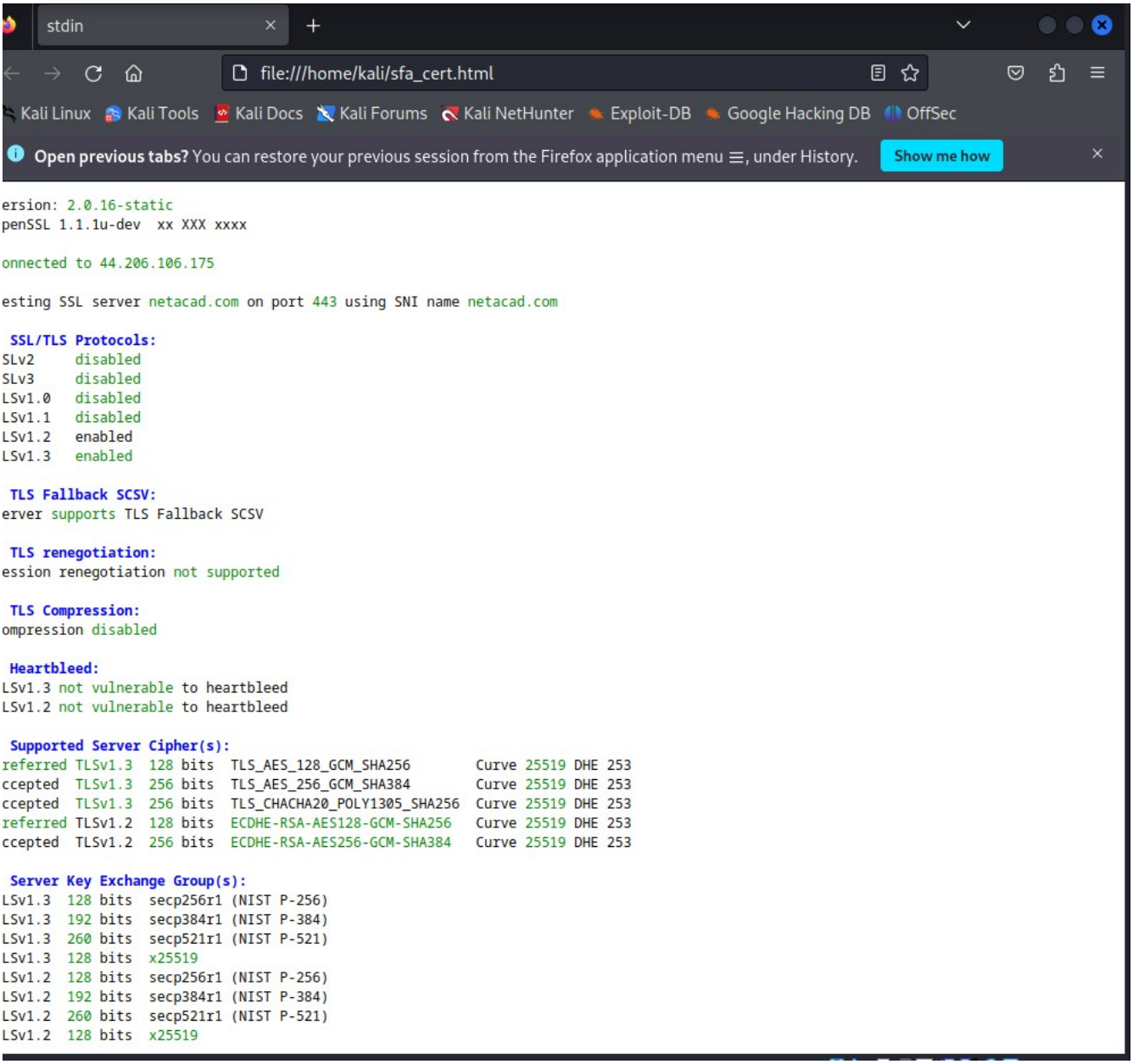
After a brief delay you should see the results of scan begin to appear in the terminal window. The output is color coded to make it easier to interpret the severity of any issues detected. The meaning of the color coding is as follows:

- Red background text – NULL cipher. No encryption was used.
- Red – broken cipher (less than or equal to 40-bit), vulnerable or broken protocol such as SSLv2 or SSLv3 or broken certificate signing algorithm such as MD5.
- Yellow – weak cipher (less than or equal to 56-bit) or weak signing algorithm such as SHA-1.
- Purple – anonymous cipher such as ADH or AECDH.

While sslscan provides options for outputting results in text or XML file formats, the readability of HTML and the preservation of color coding is provided by aha. To use aha, pipe the output of the sslscan command to aha and then redirect the output of aha to a HTML file.

sslscan will save the file in the Kali Home directory as indicated by the prompt. You can add a path to the filename or run the terminal from a destination directory to save it elsewhere.

Locate the HTML file and open it with Firefox. The output should be like that of the terminal except that the background is white. The original color coding should be intact.


stdin
file:///home/kali/sfa_cert.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Open previous tabs? You can restore your previous session from the Firefox application menu ☰, under History.
Show me how
ersion: 2.0.16-static
penSSL 1.1.1u-dev xx XXX xxxx
onnected to 44.206.106.175
esting SSL server netacad.com on port 443 using SNI name netacad.com
SSL/TLS Protocols:
SLv2 disabled
SLv3 disabled
LSv1.0 disabled
LSv1.1 disabled
LSv1.2 enabled
LSv1.3 enabled
TLS Fallback SCSV:
erver supports TLS Fallback SCSV
TLS renegotiation:
ession renegotiation not supported
TLS Compression:
ompression disabled
Heartbleed:
LSv1.3 not vulnerable to heartbleed
LSv1.2 not vulnerable to heartbleed
Supported Server Cipher(s):
referred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
ccepted TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253
ccepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
referred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
ccepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Server Key Exchange Group(s):
LSv1.3 128 bits secp256r1 (NIST P-256)
LSv1.3 192 bits secp384r1 (NIST P-384)
LSv1.3 260 bits secp521r1 (NIST P-521)
LSv1.3 128 bits x25519
LSv1.2 128 bits secp256r1 (NIST P-256)
LSv1.2 192 bits secp384r1 (NIST P-384)
LSv1.2 260 bits secp521r1 (NIST P-521)
LSv1.2 128 bits x25519