Lab - Finding Information from 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 provide two broad functions. First, they provide a way that the ownership of a website can be validated by people who are accessing it. Second, 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. They also provide the information required for a browser to create a secure, encrypted connection to a web site 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 The users become aware of them if a certificate is missing, out of date, or misconfigured.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 skillsforall.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

```
<!----><!---->
```

View the certificate. When will it expire?

Answer Area

```
<!----><!---->
```

What is the certificate signature encryption algorithm?

Answer Area

```
<!----><!---->
```

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.

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

```
<!----><!---->
```

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 skillsforall.com and related subdomains. The list goes back to 2019. crt.sh provides IDs for the certificates but these IDs are relevant to crt.sh only. Clicking an ID takes you to the available certificate details.

Note that crt.sh reveals several subdomains that are not known to normal Skills for All users. Note the names of the subdomains. Who do you think these subdomains are intended to be used by? Explain.

Answer Area

```
<!----><!---->
```

What other domain is associated with the Skills for All domain according to the crt.sh information?

Answer Area

```
<!----><!---->
```

Search crt.sh on the domain that is affiliated with skillsforall.com. What general observation can you make about the domains revealed from this search? What does this imply about the network?

Answer Area

```
<!----><!---->
```

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
Answer Area <!----><!---->	Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	Answer Area <!----><!---->	Answer Area <!----><!---->

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.

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

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

b. 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 skillsforall.com target.

```
┌──(kali㉿Kali)-[~]
└─$ sslscan skillsforall.com
```

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.

b. 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.

```
┌──(kali㉿Kali)-[~]
└─$ sslscan skillsforall.com | aha > sfa_cert.html
```

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.

c. 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.

Reflection Question

Compare the output of the tools used in this lab. Which tool seems to give the most useful information?

Answer Area

```
<!----><!---->
```