**Lab - Certificate Authority Stores**

## Certificates Trusted by Your Browser

### Display the Root Certificates in Firefox.

A screenshot of a computer

Description automatically generated

## Checking for Man-In-Middle

### Gathering the correct and unmodified certificate fingerprint.

What are the fingerprints? Why are they important?

A certificate fingerprint is a hash calculated against the certificate. It is important because it allows for a quick way to verify if any information inside the certificate has been tampered with.

Who calculates fingerprints? How to find them?

The certificate fingerprint is usually calculated by the CA that signs the certificate. After it has been computed, the CA includes it in the certificate itself. The fingerprint can be easily displayed when viewing the certificate.

### Gather the certificate fingerprint in use by the CyberOps Workstation VM.

* + - 1. Use the three piped commands below to fetch the fingerprint for Cisco.com. The line below uses OpenSSL to connect to cisco.com on port 443 (HTTPS), request the certificate and store it on a text file named **cisco.pem**. The output is also shown for context.

[analyst@secOps ~]$ **echo -n | openssl s\_client -connect cisco.com:443 | sed   
-ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > ./cisco.pem**

depth=2 C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 2

verify return:1

depth=1 C = US, O = HydrantID (Avalanche Cloud Corporation), CN = HydrantID SSL ICA G2

verify return:1

depth=0 C = US, ST = CA, L = San Jose, O = "Cisco Systems, Inc.", CN = www.cisco.com

verify return:1

DONE

A screenshot of a computer

Description automatically generated

* + - 1. Optionally, use the **cat** command to list the contents of the fetched certificate and stored in the **cisco.pem** text file:

[analyst@secOps ~]$ **cat cisco.pem**

-----BEGIN CERTIFICATE-----

MIIG1zCCBL+gAwIBAgIUKBO9xTQoMemc9zFHNkdMW+SgFO4wDQYJKoZIhvcNAQEL

BQAwXjELMAkGA1UEBhMCVVMxMDAuBgNVBAoTJ0h5ZHJhbnRJRCAoQXZhbGFuY2hl

IENsb3VkIENvcnBvcmF0aW9uKTEdMBsGA1UEAxMUSHlkcmFudElEIFNTTCBJQ0Eg

RzIwHhcNMTcxMjA3MjIxODU1WhcNMTkxMjA3MjIyODAwWjBjMQswCQYDVQQGEwJV

UzELMAkGA1UECAwCQ0ExETAPBgNVBAcMCFNhbiBKb3NlMRwwGgYDVQQKDBNDaXNj

byBTeXN0ZW1zLCBJbmMuMRYwFAYDVQQDDA13d3cuY2lzY28uY29tMIIBIjANBgkq

yvo6dWpJdSircYy8HG0nz4+936+2waIVf1BBQXZUjNVuws74Z/eLIpl2c6tANmE0

q1i7fiWgItjDQ8rfjeX0oto6rvp8AXPjPY6X7PT1ulfhkLYnxqXHPETRwr8l5COO

MDEh95cRxATXNAlWAwLcBT7lDmrGron6rW6hDtuUPPG/rjZeZbNww5p/nT3EXX2L

Rh+m0R4j/tuvy/77YRWyp/VZhmSLrvZEYiVjM2MgCXBvqR+aQ9zWJkw+CAm5Z414

Eiv5RLctegYuBUMGTH1al9r5cuzfwEg2mNkxl4I/mtDro2kDAv7bcTm8T1LsZAO/

1bWvudsrTA8jksw+1WGAEd9bHi3ZpJPYedlL

-----END CERTIFICATE-----

[analyst@secOps ~]$

A screenshot of a computer

Description automatically generated

* + - 1. Now that the certificate is saved in the **cisco.pem** text file, use the command below to extract and display its fingerprint:

[analyst@secOps ~]$ **openssl x509 -noout -in cisco.pem -fingerprint -sha1**

SHA1 Fingerprint=64:19:CA:40:E2:1B:3F:92:29:21:A9:CE:60:7D:C9:0C:39:B5:71:3E

[analyst@secOps ~]$

A screenshot of a computer

Description automatically generated

**Note**: Your fingerprint value may be different for two reasons. First, you may be using a different operating system than the CyberOps Workstation VM. Second, certificates are regularly refreshed changing the fingerprint value.

#### Questions:

What hash algorithm was used by OpenSSL to calculate the fingerprint?

SHA-1

Why was that specific algorithm chosen? Does it matter?

The fingerprints acquired and shown in the table are all SHA-1. Any other algorithm used by OpenSSL when computing the fingerprint would yield a different hash and therefore a different fingerprint, invalidating the test.

### Compare the Fingerprints

Do the fingerprints match?

No

What does it mean?

May be cisco have refresh their CA fingerprints.

Is this method 100% foolproof?

No. While non-matching fingerprints communicates SSL/TLS traffic interception, matching fingerprints should be handled with care. A few exceptions to consider are: 1. The CyberOps Workstation VM will likely NOT have any enterprise-owned CA root certificates installed. In that scenario, the VM may not have its traffic intercepted while other machines in local network do. 2. The enterprise could use dynamic rules to intercept only selected sites.

## Challenges (Optional)

* + - 1. Check the fingerprints for the sites shown in Table-1 but using your web browser’s GUI.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* + - 1. Use the OpenSSL (Part 2, Steps 1 through 3) to check all the fingerprints listed in Table-1

# Reflection Question

What would be necessary for the HTTPS proxy to work?

The local machine would have to trust the HTTPS proxy blindly. When companies or organizations want to monitor HTTPS traffic, they often use a technique called SSL/TLS interception, SSL/TLS inspection, or HTTPS proxying. In this scenario, the organization installs the SSL/TLS certificate of the HTTPS proxy into the root certificate store of the local machines. This process is also known as "SSL/TLS certificate pinning" or "SSL/TLS certificate installation."