Laboratório - Armazenamento de Autoridade de Certificação .

Objetivos

Parte 1: Certificados Confiáveis pelo Seu Navegador

Parte 2: Verificando o Man-In-Middle

Histórico/Cenário

Conforme a web evoluiu, também cresceu a necessidade de segurança. HTTPS (onde o 'S' significa segurança) junto com o conceito de Autoridade de Certificação foi introduzido pela Netscape em 1994 e ainda é usado hoje. Neste laboratório, você irá:

- Liste todos os certificados confiáveis por seu navegador (preenchidos em seu computador)
- Use hashes para detectar se sua conexão com a Internet está sendo interceptada (concluída na máquina virtual CyberOps Workstation)

Recursos necessários

- Máquina Virtual CyberOps Workstation
- Acesso à Internet

Instruções

Parte 1: Certificados confiáveis pelo seu navegador

HTTPS depende de uma entidade de terceiros para validação. Conhecida como Autoridade de Certificação (CA), essa entidade de terceira parte verifica se um nome de domínio realmente pertence à organização que reivindica sua propriedade. Se a verificação for marcada, a CA cria um certificado assinado digitalmente contendo informações sobre a organização, incluindo sua chave pública.

Todo o sistema é baseado no fato de que os navegadores da web e os sistemas operacionais são fornecidos com uma lista de CAs em que confiam. Todos os certificados assinados por qualquer uma das CAs na lista serão vistos pelo navegador como legítimos e automaticamente confiáveis. Para tornar o sistema mais seguro e escalável, as CAs frequentemente distribuem a tarefa de criar e assinar certificados entre muitas CAs filhas. O CA pai é conhecido como CA raiz. Se um navegador confiar em uma CA raiz, ele também confiará em todas as CAs filhas.

Nota: Embora os armazenamentos de certificados sejam semelhantes entre os navegadores, este laboratório se concentra em **Chrome 81** e **Firefox 75**. O menu e os gráficos podem ser diferentes para outras versões do navegador da web.

Siga as etapas para exibir a loja da CA em seu navegador:

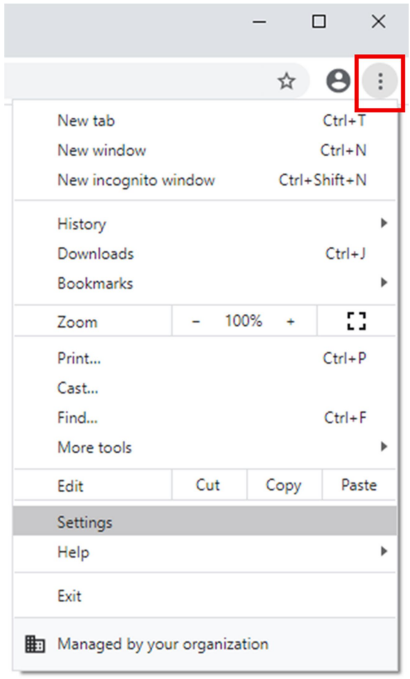
Etapa 1: Exibir os certificados raiz no Chrome.

Você pode executar esta etapa em sua máquina local ou usar o FireFox na CyberOps Workstation VM. Se você usa o Firefox, prossiga para a Etapa 2. Se você usa um navegador diferente do Chrome ou Firefox, pesquise na Internet as etapas para exibir seus certificados raiz.

Nota: O menu e os gráficos podem ser diferentes para outras versões do navegador Chrome.

a. Abra o navegador Chrome em seu PC.

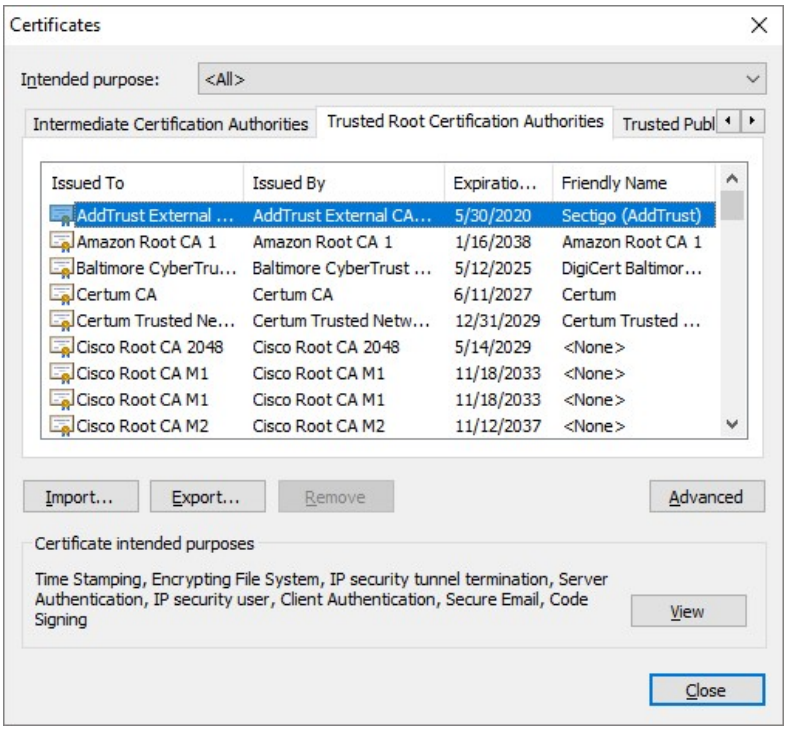
b. Clique no ícone de três pontos na extremidade direita da barra de endereço para exibir as opções do Chrome. Clique em **Configurações**.



c. Role para baixo até **Privacy and security** e clique em **More**.

d. Role para baixo e selecione **Manage certificates**.

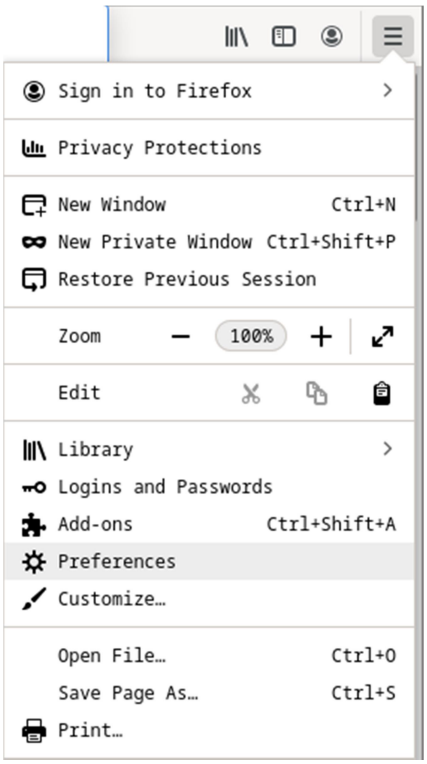
e. Na janela Certificado, selecione a guia **Trusted Root Certification Authorities** para mostrar todos os certificados e autoridades de certificação confiáveis para o Chrome.



Etapa 2: Exibir os certificados no armazenamento da CA no Firefox.

Nota: O menu e os gráficos podem ser diferentes para outras versões do navegador Firefox e entre diferentes sistemas operacionais. **O Firefox 75** na CyberOps Workstation VM é mostrado nesta etapa.

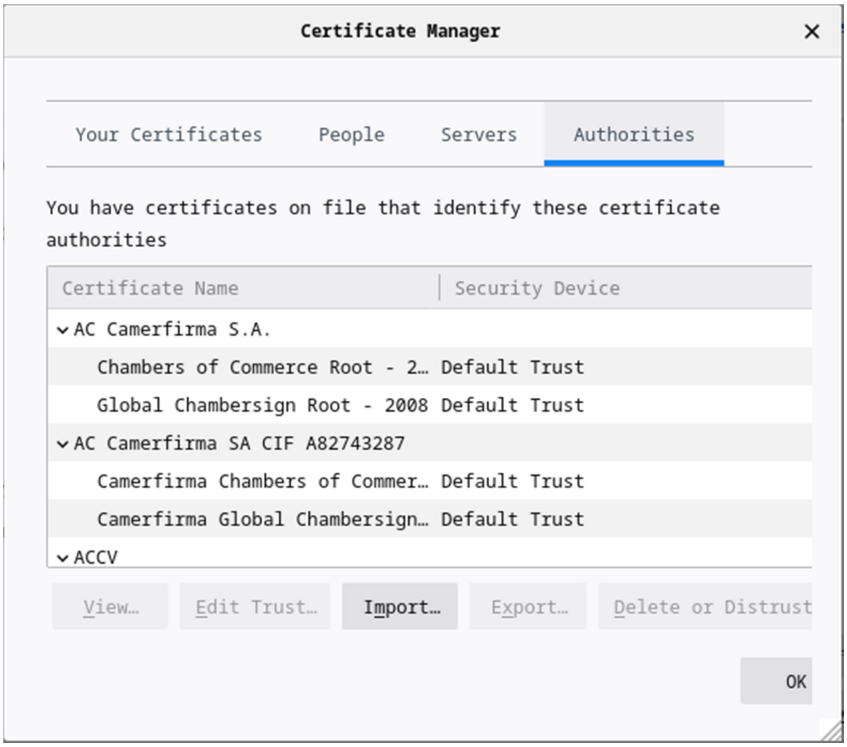
a. Abra o Firefox e clique no ícone Menu. O ícone **Menu** está localizado na extremidade direita da janela do Firefox, próximo à barra de endereço. Clique em **Preferences**.



b. Clique em **Privacy & Security** no painel esquerdo.

c. Role para baixo até a seção Segurança e clique em **View Certificates**.

d. É aberta uma janela que mostra os certificados e autoridades de certificação confiáveis para o Firefox.



Parte 2: Verificando o Man-In-Middle

Esta parte é concluída usando o CyberOps Workstation VM.

Um uso comum de hashes é verificar a integridade dos dados, mas eles também podem ser usados para detectar ataques man-in-the-middle HTTPS.

Para proteger os dados do usuário, cada vez mais sites estão migrando para o tráfego criptografado. Conhecidos como HTTPS, os sites usam protocolos como TLS / SSL para criptografar o tráfego do usuário de ponta a ponta. Depois que o tráfego é criptografado corretamente, é muito difícil para qualquer outra parte, exceto o usuário e o site em questão, ver o conteúdo da mensagem criptografada. Isso é bom para os usuários, mas cria um problema para as organizações que desejam analisar esse tráfego. As empresas e organizações geralmente optam por espiar o tráfego gerado por funcionários para fins de monitoramento. Eles precisavam ser capazes de examinar o tráfego criptografado por TLS / SSL. Isso é feito usando um proxy HTTPS.

Os navegadores da web confiam na identidade de um site visitado se o certificado apresentado por esse site for assinado por uma das CAs instaladas no armazenamento de certificados do navegador. Para poder espiar o tráfego criptografado por TLS / SSL de seus usuários, uma empresa ou organização simplesmente adiciona outra CA à lista de CA instalada do navegador do usuário.

Considere o seguinte cenário: A empresa X contrata um novo funcionário e fornece a ele um novo laptop da empresa. Antes de entregar o laptop, o departamento de TI da empresa instala todos os softwares necessários para o trabalho. Entre o software e os pacotes instalados, o departamento de TI também inclui uma CA extra na lista de CAs confiáveis. Essa CA extra aponta para um computador controlado pela empresa conhecido como proxy HTTPS. Como a empresa controla os padrões de tráfego, o proxy HTTPS pode ser colocado no meio de qualquer conexão. Funciona assim:

1. O usuário tenta estabelecer uma conexão segura com o site HTTPS H, hospedado na Internet. H pode ser qualquer site HTTPS: um banco, loja online, servidor de e-mail, etc.

2. Como a empresa controla os padrões de tráfego, ela faz com que todo o tráfego do usuário atravesse o proxy HTTPS. O proxy HTTPS então *personifica* o site H e apresenta um certificado autoassinado para provar que é H. O proxy HTTPS basicamente diz “Olá, sou o site HTTPS H. Aqui está meu certificado. Foi assinado por ... eu mesmo. ”
3. Como o certificado apresentado é assinado por um dos CAs incluídos no armazenamento de CA do laptop (lembre-se, ele foi adicionado por TI), o navegador da web acredita erroneamente que está realmente se comunicando com H. Observe que, se o CA extra não tivesse sido adicionado a o armazenamento da CA, o laptop não confiaria no certificado e perceberia imediatamente que outra pessoa estava tentando *se passar* por H.
4. O laptop confia na conexão e estabelece um canal seguro com o proxy HTTPS, acreditando erroneamente que está se comunicando com segurança com H.
5. O proxy HTTPS agora estabelece uma segunda conexão segura com H, o site que o usuário estava tentando acessar desde o início.
6. O proxy HTTPS é agora o ponto final de duas conexões seguras separadas; um estabelecido com o usuário e outro estabelecido com H. Como o HTTPS é o ponto final de ambas as conexões, ele agora pode descriptografar o tráfego de ambas as conexões.
7. O proxy HTTPS agora pode receber tráfego de usuário criptografado por TLS/SSL destinado a H, descriptografá-lo, inspecioná-lo, criptografá-lo novamente usando TLS/SSL e enviá-lo para H. Quando H responde, o proxy HTTPS reverte o processo antes de encaminhar o tráfego para o usuário.

Observe que o processo é mais transparente para o usuário, que vê a conexão como criptografada por TLS/SSL (marcas verdes no navegador). Embora a conexão seja segura (criptografada por TLS / SSL), ela foi estabelecida com um site espúrio.

Mesmo que sua presença seja mais transparente para o usuário, os proxies TLS podem ser facilmente detectados com a ajuda de hashes. Considerando o exemplo acima, como o proxy HTTPS não tem acesso às chaves privadas do site H, o certificado que ele apresenta ao usuário é diferente do certificado apresentado por H. Incluído em cada certificado está um valor conhecido como *impressão digital*. Essencialmente, um hash calculado e assinado pelo emissor do certificado, a impressão digital atua como um resumo exclusivo de todo o conteúdo do certificado. Se uma letra do certificado for modificada, a impressão digital produzirá um valor completamente diferente quando calculada. Por causa dessa propriedade, as impressões digitais são usadas para comparar certificados rapidamente. Voltando ao exemplo acima, o usuário pode solicitar o certificado de H e comparar a impressão digital incluída nele com a fornecida quando a conexão com o site H foi estabelecida. Se as impressões digitais corresponderem, a conexão foi realmente estabelecida com H. Se as impressões digitais não corresponderem, a conexão foi estabelecida com algum outro ponto de extremidade.

Siga as etapas abaixo para avaliar se há um proxy HTTPS em sua conexão.

Etapa 1: Coletando a impressão digital correta e não modificada do certificado.

A primeira etapa é coletar algumas impressões digitais do site. Isso é importante porque eles serão usados para comparação posteriormente. A tabela abaixo contém algumas impressões digitais de certificado de site de sites populares.

Observação: as impressões digitais SHA-1 mostradas na Tabela 1 podem não ser mais válidas, pois as organizações renovam regularmente seus certificados. Uma impressão digital também é chamada de impressão digital em máquinas com Windows.

Tabela 1 - Sites populares e suas impressões digitais de certificado SHA-1

Local	Domínios Cobertos por Certificado	Impressão Digital do Certificado SHA-1 (a partir de maio 2020)
www.cisco.com	www.cisco.com	E2:BD:0B:58:C6:B4:FF:91:D6:23:AB:44:0D:8F:64:76:29:4E:30:0B
www.facebook.com	*.facebook.com	BB:E7:A0:97:C7:92:B2:2D:00:38:12:69:E4:64:E9:04:96:4B:C7:41
www.wikipedia.org	*.wikipedia.org	A8:F9:F7:79:BE:DB:3E:EB:59:F0:1D:A6:34:08:A1:64:5D:28:48:44
twitter.com	twitter.com	73:33:BB:96:1D:DB:9C:0C:4F:E5:1C:FF:68:26:CF:5E:3F:50:AB:96
www.linkedin.com	www.linkedin.com	04:BC:C5:09:DD:AE:99:40:7E:99:A5:65:32:68:EC:5D:2D:D7:5A:19

Quais são as impressões digitais? Por que eles são importantes?

Quem calcula as impressões digitais? Como encontrá-los?

Etapa 2: Reúna a impressão digital do certificado em uso pela CyberOps Workstation VM.

Agora que temos as impressões digitais reais, é hora de obter as impressões digitais de um host local e comparar os valores. Se as impressões digitais não corresponderem, o certificado em uso NÃO pertence ao site HTTPS sendo verificado, o que significa que há um proxy HTTPS entre o computador host e o site HTTPS sendo verificado. A correspondência de impressões digitais significa que nenhum proxy HTTPS está instalado.

a. Use os três comandos canalizados abaixo para buscar a impressão digital para Cisco.com. A linha abaixo usa OpenSSL para se conectar a cisco.com na porta 443 (HTTPS), solicitar o certificado e armazená-lo em um arquivo de texto chamado **cisco.pem**. A saída também é mostrada para contexto.

```
[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
verificar retorno: 1
depth=1 C = US, O = HydrantID (Avalanche Cloud Corporation), CN = HydrantID SSL ICA G2
verificar retorno: 1
depth=0 C = US, ST = CA, L = San Jose, O = "Cisco Systems, Inc.", CN = www.cisco.com
verificar retorno: 1
CONCLUÍDO
```

b. Opcionalmente, use o comando **cat** para listar o conteúdo do certificado obtido e armazenado no arquivo de texto **cisco.pem**:

```
[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-----
[analista @secOps ~] $
```

c. Agora que o certificado está salvo no arquivo de texto **cisco.pem**, use o comando abaixo para extrair e exibir sua impressão digital:

```
[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
[analista @secOps ~] $
```

Nota: O valor da sua impressão digital pode ser diferente por dois motivos. Primeiro, você pode estar usando um sistema operacional diferente do CyberOps Workstation VM. Em segundo lugar, os certificados são atualizados regularmente, alterando o valor da impressão digital.

Qual algoritmo hash foi usado pelo OpenSSL para calcular a impressão digital?

Por que esse algoritmo específico foi escolhido? Isso importa?

Etapa 3: Compare as impressões digitais

Use a Tabela 1 para comparar a impressão digital do certificado adquirida diretamente do site Cisco HTTPS com aquela adquirida de sua rede. Lembre-se de que as impressões digitais podem mudar com o tempo.

As impressões digitais são iguais?

O que isso significa?

Este método é 100% infalível?

Parte 3: Desafios (opcional)

a. Verifique as impressões digitais dos sites mostrados na Tabela 1, mas usando a GUI do seu navegador da web.

   Dicas: Encontre uma maneira de exibir a impressão digital por meio da GUI do navegador. Lembre-se: o Google é útil neste exercício, e o Windows costuma se referir à impressão digital como **Thumbprint**.

b. Use o OpenSSL (Parte 2, Etapas 1 a 3) para verificar todas as impressões digitais listadas na Tabela 1

Perguntas para reflexão

O que seria necessário para o proxy HTTPS funcionar?