МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,

СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»

(СПбГУТ)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет инфокоммуникационных сетей и систем

Кафедра защищенных систем связи

Дисциплина Безопасность компьютерных сетей

ЛАБОРАТОРНАЯ РАБОТА №3

Хранилища центров сертификации

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

Студент:

Громов А. А., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Проверил:

Ушаков И. А.

Лабораторная работа. Хранилища центров сертификации

Задачи

Часть 1. Сертификаты, которым доверяет ваш браузер

Часть 2. Выявление атаки через посредника

1. Общие сведения и сценарий

По мере развития Интернета растет необходимость обеспечения безопасности. Протокол HTTPS (где S означает security, то есть «безопасность») наряду с концепцией центров сертификации был предложен компанией Netscape в 1994 г. и по-прежнему используется в настоящее время. В этой лабораторной работе вам предстоит:

* перечислить все сертификаты, которым доверяет ваш браузер (выполняется на вашем компьютере);
* использовать хеши, чтобы выяснить, перехватывается ли ваше интернет-подключение (выполняется на виртуальной машине CyberOps).

1. Необходимые ресурсы

* Виртуальная машина рабочей станции CyberOps
* Доступ к Интернету

1. Сертификаты, которым доверяет ваш браузер

Для проверки HTTPS используют сторонние средства. Стороннее средство, известное как центр сертификации (ЦС), проверяет, что доменное имя действительно принадлежит организации, которая утверждает, что является его владельцем. Если проверка завершается успешно, ЦС создает подписанный сертификат, содержащий сведения об организации, в том числе его общем ключе.

Вся система основывается на том, что веб-обозреватели и операционные системы поставляются со списком доверенных ЦС. Любой сертификат, подписанный каким-нибудь ЦС в списке, будет рассматриваться веб-браузером как законный и автоматически заслуживающий доверия. Для того чтобы сделать систему более безопасной и масштабируемой, ЦС часто распределяют задачу создания и подписывания сертификатов между многими дочерними ЦС. Родительский ЦС называется корневым центром сертификации. Если веб-браузер доверяет корневому центру сертификации, он также доверяет всем его дочерним ЦС.

**Примечание**. Хотя хранилища сертификатов веб-браузеров аналогичны, в данной лабораторной работе рассматриваются **Chrome 56** и **Firefox 59**. Меню и графики могут различаться в зависимости от версии веб-обозревателя.

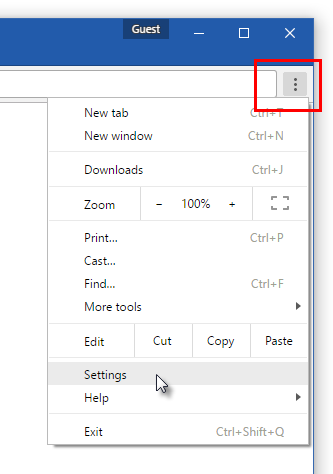
Выполните действия, чтобы открыть хранилище ЦС в браузере.

* 1. Отобразите корневые сертификаты в Chrome.

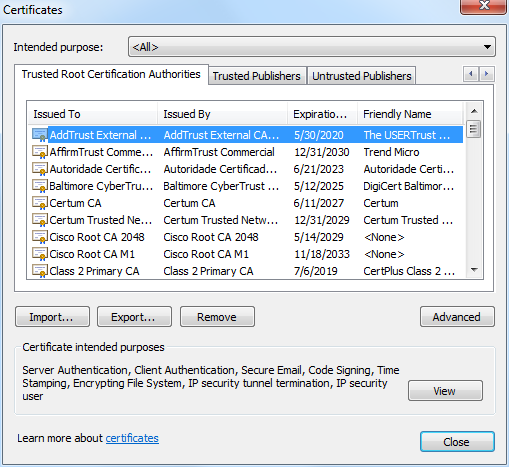
Этот шаг можно выполнить на локальном компьютере или использовать FireFox на виртуальной машине рабочей станции CyberOps. Если вы используете Firefox, перейдите к шагу 2. Если вы используете веб-браузер, отличный от Chrome или Firefox, выполните поиск в Интернете, чтобы найти описание действий, необходимых для отображения своих корневых сертификатов.

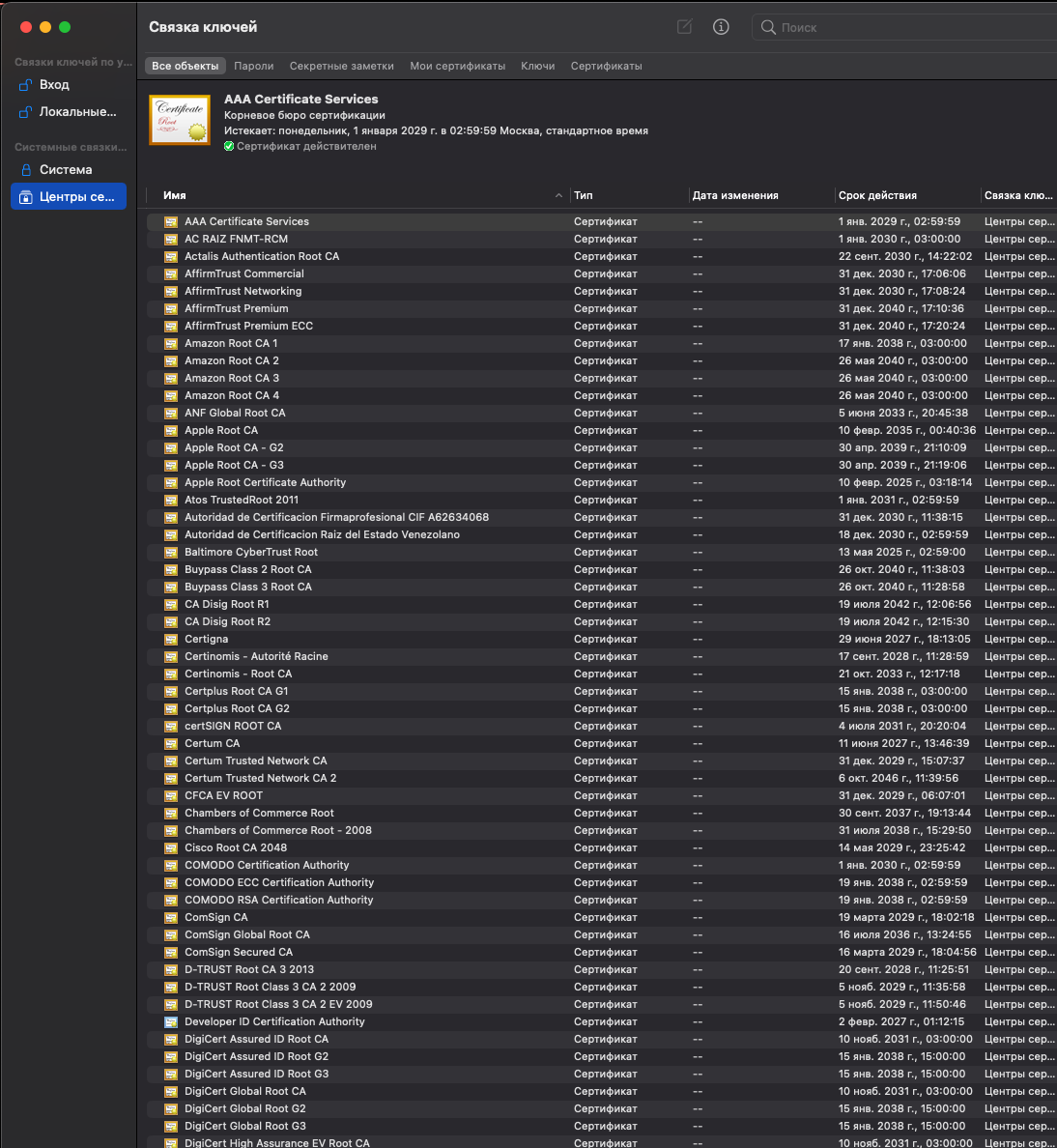
**Примечание**. Меню и графики могут различаться в зависимости от версии браузера Chrome.

* + 1. Откройте веб-обозреватель Chrome на своем ПК.
    2. Щелкните значок с тремя точками в дальнем правом конце адресной строки, чтобы отобразить параметры Chrome.



* + 1. Нажмите **Settings** (Настройки), а затем нажмите **Show Advanced Settings** (Показать дополнительные параметры).
    2. Прокрутите страницу вниз и нажмите кнопку **Manage certificates…** (Настроить сертификаты...) в разделе **HTTPS/SSL**.
    3. В открывшемся окне **Certificates** (Сертификаты) выберите вкладку **Trusted Root Certification Authorities** (Доверенные корневые центры сертификации). Откроется окно, в котором показаны все сертификаты и ЦС, которым доверяет Chrome.

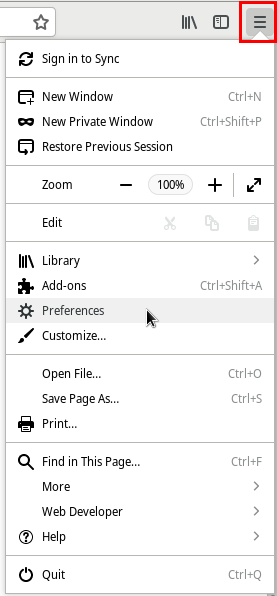




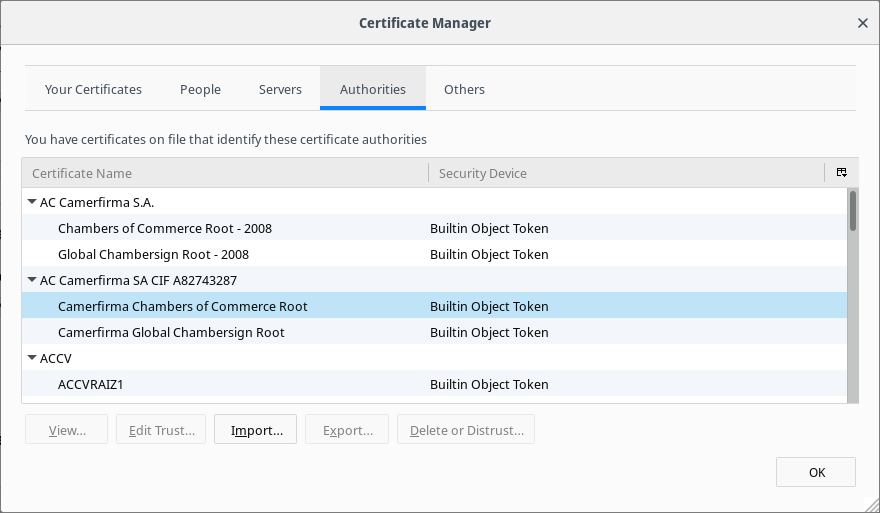
* 1. Отображение сертификатов в хранилище ЦС в Firefox.

**Примечание**. Меню и графики могут различаться в зависимости от версии браузера Firefox и используемой операционной системы. **Firefox 59** на виртуальной машине рабочей станции CyberOps показан на этом этапе.

* + 1. Откройте Firefox и щелкните значок меню. Значок **Menu** (Меню) находится в крайней правой части окна Firefox рядом с адресной строкой.



* + 1. Нажмите **Preferences > Privacy & Security** (Предпочтения > Безопасность и конфиденциальность).
    2. Прокрутите вниз до раздела безопасности и нажмите **View Certificates** (Просмотреть сертификаты).
    3. Откроется окно, в котором показаны сертификаты и ЦС, которым доверяет Firefox.



1. Выявление атаки через посредника

Эта часть выполняется с использованием рабочей станции виртуальной машины CyberOps.

Хеши широко используются для проверки целостности данных, но они также могут использоваться для выявления атак через посредника HTTPS.

Для защиты пользовательских данных все больше веб-сайтов переключаются на зашифрованный трафик. В соответствии с подходом, известным как HTTPS, сайты используют такие протоколы, как TLS/SSL, для шифрования пользовательского трафика от начала до конца. После того как трафик надежно зашифрован, очень сложно кому бы то ни было, кроме пользователя и данного сайта, просмотреть содержимое зашифрованного сообщения. Это полезно для пользователей, но создает проблемы организациям, которые хотят заглянуть в трафик. Компании и организации часто стремятся просматривать трафик своих сотрудников в целях контроля. Им необходимо иметь возможность просматривать TLS/SSL-зашифрованный трафик. Это делается с помощью прокси-сервера HTTPS.

Веб-обозреватели доверяют удостоверению посещаемого веб-сайта, если сертификат, представленный этим веб-сайтом, подписан одним из ЦС, установленных в хранилище сертификатов браузера. Для того чтобы иметь возможность просматривать TLS/SSL-зашифрованный трафик пользователей, компания или организация просто добавляет еще один ЦС в список установленных ЦС браузера пользователя.

Рассмотрим следующий сценарий: компания X нанимает нового сотрудника и предоставляет ему ноутбук. Перед передачей ноутбука ИТ-отдел компании устанавливает все необходимое для работы программное обеспечение. Наряду с установленными программным обеспечением и процессами ИТ-отдел включает в список доверенных ЦС один дополнительный ЦС. Этот дополнительный ЦС указывает на управляемый компанией компьютер, известный как прокси-сервер HTTPS. Поскольку компания контролирует трафик, прокси-сервер HTTPS можно поместить в середину любого подключения. Принцип действия следующий.

1. Пользователь пытается установить защищенное соединение с использующим протокол HTTPS веб-сайтом H, размещенным в Интернете. H может быть любой HTTPS-сайт: банк, интернет-магазин, сервер электронной почты и т. д.
2. Поскольку компания управляет трафиком, она делает это таким образом, чтобы весь пользовательский трафик проходил через прокси-сервер HTTPS. Затем прокси-сервер HTTPS *олицетворяет* веб-сайт H и представляет самоподписанный сертификат, чтобы доказать, что это H. В сущности, прокси-сервер HTTPS говорит: «Привет, я есть HTTPS-сайт H. Вот мой сертификат. Он подписан... мною».
3. Поскольку представленный сертификат подписан одним из ЦС, включенных в хранилище ЦС ноутбука (следует помнить, что он был добавлен ИТ-отделом), веб-обозреватель ошибочно считает, что действительно обменивается данными с H. Обратите внимание, что, если бы дополнительный ЦС не был добавлен в хранилище ЦС, ноутбук не доверял бы сертификату и немедленно распознал, что кто-то другой пытается *олицетворять* H.
4. Ноутбук доверяет подключению и устанавливает безопасный канал связи с прокси-сервером HTTPS, ошибочно полагая, что безопасно обменивается данными с H.
5. Теперь прокси-сервер HTTPS устанавливает второе безопасное подключение с H, веб-сайтом, к которому пользователь пытался получить доступ с самого начала.
6. Прокси-сервер HTTPS теперь является конечной точкой двух отдельных безопасных подключений: одного, установленного с пользователем, и другого, установленного с H. Поскольку HTTPS ― конечная точка обоих подключений, можно расшифровать трафик обоих подключений.
7. Теперь прокси-сервер HTTPS может получить TLS/SSL-зашифрованный трафик пользователя, предназначенный для H, расшифровать его, проинспектировать, повторно зашифровать с помощью TLS/SSL и отправить H. Когда H отвечает, прокси-сервер HTTPS выполняет обратный процесс перед пересылкой трафика пользователю.

Обратите внимание, что процесс в основном прозрачен для пользователя, который считает подключения TLS/SSL-зашифрованными (зеленые значки в браузере). Соединение безопасное (TLS/SSL-зашифрованное), но установлено через ложный веб-сайт.

Хотя его присутствие обычно является прозрачным для пользователя, TLS-прокси можно легко обнаружить с помощью хешей. В приведенном выше примере, поскольку прокси-сервер HTTPS не имеет доступа к частным ключами сайта H, сертификат, представленный пользователю, отличается от сертификата, представленного сайтом H. В каждый сертификат входит значение, известное как *отпечаток.* В сущности, хеш рассчитывается и подписывается издателем сертификата, а отпечаток выступает в качестве уникальной сводки всего содержимого сертификата. Если хотя бы одну буква сертификата изменена, вычисленный отпечаток будет иметь совершенно другое значение. Из-за этого свойства отпечатки используются для быстрого сравнения сертификатов. Возвращаясь к приведенному выше примеру, пользователь может запросить сертификат H и сравнить включенный в него отпечаток с отпечатком, предоставленным, когда было установлено подключение к веб-сайту H. Если отпечатки совпадают, соединение действительно установлено с H. Если отпечатки не совпадают, значит, подключение установлено с какой-то другой конечной точкой.

Выполните следующие действия, чтобы выяснить, есть ли прокси-сервер HTTPS в вашем соединении.

* 1. Сбор правильных и неизмененных отпечатков сертификата.
     1. Первый шаг ― собрать отпечатки нескольких сайтов. Это важно, поскольку они будут использоваться для сравнения позже. В приведенной ниже таблице содержится несколько отпечатков сертификатов популярных сайтов.

**Примечание**. Отпечатки SHA-1, показанные в таблице 1, возможно, больше недействительны, так как организации регулярно обновляют свои сертификаты. Отпечаток (fingerprint) также называется thumbprint в компьютерах Windows.

**Таблица 1. Популярные сайты и их отпечатки сертификата SHA-1**

|  |  |  |
| --- | --- | --- |
| Сайт | Домены, на которые распространяется сертификат | Отпечаток сертификата SHA-1 (по состоянию на апрель 2018 г.) |
| [www.cisco.com](http://www.cisco.com) | [www.cisco.com](http://www.cisco.com) | 64:19:CA:40:E2:1B:3F:92:29:21:A9:CE:60:7D:C9:0C:39:B5:71:3E |
| [www.facebook.com](http://www.facebook.com) | \*.facebook.com | BD:25:8C:1F:62:A4:A6:D9:CF:7D:98:12:D2:2E:2F:F5:7E:84:FB:36 |
| [www.wikipedia.org](http://www.wikipedia.org) | \*.wikipedia.org | 4B:3E:D6:B6:A2:C7:55:E8:56:84:BE:B1:42:6B:B0:34:A6:FB:AC:24 |
| [twitter.com](http://www.twitter.com/) | twitter.com | 26:5C:85:F6:5B:04:4D:C8:30:64:5C:6F:B9:CF:A7:D2:8F:28:BC:1B |
| [www.linkedin.com](http://www.linkedin.com) | [www.linkedin.com](http://www.linkedin.com) | 3A:60:39:E8:CE:E4:FB:58:87:B8:53:97:89:8F:04:98:20:BF:E3:91 |
| Сайт | Домены, на которые распространяется сертификат | Отпечаток сертификата SHA-1 (по состоянию на апрель 2022 г.) |
| [www.cisco.com](http://www.cisco.com) | [www.cisco.com](http://www.cisco.com) | ﻿50:D7:FF:4B:D7:CD:45:1C:56:BE:E0:ED:8A:92:36:80:E2:33:AC:B1 |
| [www.facebook.com](http://www.facebook.com) | \*.facebook.com | 2D:FA:C1:32:75:7E:6C:76:1A:B1:7D:8D:20:3B:7E:DF:93:89:00:29 |
| [www.wikipedia.org](http://www.wikipedia.org) | \*.wikipedia.org | D6:06:82:CE:7D:BA:8A:1A:BD:8E:83:D2:38:D5:44:23:D9:D5:54:ED |
| [twitter.com](http://www.twitter.com/) | twitter.com | 37:63:F4:77:39:1F:19:EF:D1:63:ED:67:74:1B:92:83:0F:9E:D4:93 |
| [www.linkedin.com](http://www.linkedin.com) | [www.linkedin.com](http://www.linkedin.com) | D3:5E:97:06:63:31:26:47:DB:76:E7:48:95:15:52:5F:88:98:9A:88 |

Что такое отпечатки? Почему они важны?

Отпечатки - это хэш сертификата, вычисляемый по всем данным сертификата и его подпись. Отпечатки используются в качестве уникальных идентификаторов для сертификатов, в приложениях при принятии решений о доверии, в файлах конфигурации и отображаются в интерфейсах.

Кто вычисляет отпечатки? Как найти их?

Отпечатки вычисляет Центр сертификации, они содержатся в описании сертификата

* 1. Получите отпечаток сертификата, используемый ВМ рабочей станции CyberOps.

Теперь, когда у нас есть действительные отпечатки, настало время получить отпечатки из локального хост-компьютера и сравнить значения. Если отпечатки не совпадают, используемый сертификат НЕ принадлежит к проверяемому сайту HTTPS. Это означает, что имеется прокси-сервер HTTPS между хост-компьютером и проверяемым HTTPS-сайтом. Совпадение отпечатков означает, что прокси-сервер HTTPS отсутствует.

* + 1. Используйте три приведенные ниже конвейерные команды, чтобы получить отпечаток для Cisco.com. В показанной ниже строке OpenSSL используется для подключения к cisco.com через порт 443 (HTTPS), запроса сертификата и его сохранения в текстовом файле с именем **cisco.pem**. Для контекста также показан результат.

[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

ГОТОВО

* + 1. При необходимости используйте команду **cat** для отображения содержимого сертификата, полученного и сохраненного в текстовом файле **cisco.pem**.

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

---НАЧАЛО СЕРТИФИКАТА---

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

---КОНЕЦ СЕРТИФИКАТА---

[analyst@secOps ~]$

* + 1. Теперь, когда сертификат сохранен в текстовом файле **cisco.pem**, используйте приведенную ниже команду для его извлечения и отображения его отпечатков.

[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 ~]$

**Примечание**. Существует две причины, по которым отпечатки могут иметь разные значения. Во-первых, ваша операционная система может отличаться от ОС на ВМ рабочей станции CyberOps. Во-вторых, сертификаты регулярно обновляются, а значения отпечатков меняются.

Какой алгоритм хеширования использовался OpenSSL для расчета отпечатка?

sha1

Почему был выбран именно этот алгоритм? Это важно?

Данный алгоритм прост в использовании и имеет достаточно хорошую стойкость к коллизиям. Это важно, так как благодаря этому сложно замаскироваться «посреднику», так как вычислительно сложно подобрать такой же хэш

* 1. Сравните отпечатки

Используйте таблицу 1 для сравнения отпечатка сертификата, полученного на HTTPS-сайте Cisco, с отпечатком, полученным внутри своей сети. Напоминаем, что отпечатки могут меняться со временем.

Отпечатки совпадают?

Совпадают отпечатки между браузером, cli и корневыми в системе

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Что это означает?

Сертификаты подлинны. При этом сертификаты не совпадают с приведенными в табл, так как их срок действия закончен.

Обеспечивает ли этот метод полную надежность?

В целом полного технического доверия добиться невозможно, так как сертификатам, забитым в нашей системе мы доверяем по умолчанию.

Вопросы для повторения

Какие условия необходимы для работы прокси-сервера HTTPS?

* Компании и организации, которые хотят отслеживать трафик HTTPS, достигают этого доверия, устанавливая сертификат прокси-сервера HTTPS в корневое хранилище сертификатов локального компьютера. В этом сценарии локальные машины будут доверять прокси-серверу HTTPS, позволяя ему расшифровывать трафик без каких-либо предупреждений.