Лабораторная работа №7. Сервис тестирования корректности настройки SSL на сервере Qualys SSL Labs - SSL Server Test

Никитина Анна

18 мая 2016 г.

Оглавление

1 Цель работы

- Изучить лучшие практики по развертыванию SSL/TLS.
- Изучить основные уязвимости и атаки на SSL последнего времени - POODLE, HeartBleed.

2 Ход работы

2.1 Изучение

Лучшие практики по развертыванию SSL/TLS

SSL/TLS обманчиво кажется простой технологией. Он прост в развертывании, а потом он просто работает, не обеспечивая достаточного уровня безопасности. Но основная проблема заключается в том, что SSL/TLS нелегко правильно развернуть. Для того чтобы TLS обеспечивал необходимый уровень безопасности, системные администраторы и разработчики должны приложить дополнительные усилия в настройке своих серверов и в разработке приложений.

1. Приватный ключ и сертификат

   Качество защиты, обеспечиваемой TLS полностью зависит от секретного ключа, закладывающего основу безопасности, и сертификата, который сообщает о подлинности сервера для его посетителей.

   (a) Используйте 2048-битные закрытые ключи

   (b) Защитите закрытый ключ
   Рекомендуемые меры:

   - Генерируйте закрытые ключи и запросы на сертификат (CSRs) на доверенном компьютере.
   - Используйте парольную защиту закрытых ключей, чтобы предотвратить их компрометацию в тех случаях, когда они хранятся в резервных системах.
   - После компрометации отзывайте старые сертификаты и генерируйте новые ключи.
   - Обновляйте сертификаты каждый год и всегда с новыми закрытыми ключами.

   (c) Обеспечьте охват всех используемых доменных имен

   (d) Приобретайте сертификаты у надежного удостоверяющего центра

   (e) Используйте надежные алгоритмы подписи сертификата

2. Конфигурация
   Если вы правильно настроили на сервере TLS, то можете быть уверены, что данные вашего сайта корректно отображаются для посетителей сайта, используются только безопасные алгоритмы.

   (a) Используйте безопасные протоколы. К ним относятся TLS v1.0, v1.1 и v1.2

   (b) Используйте безопасные алгоритмы шифрования

   (c) Контроль за выбором алгоритма шифрования

   (d) Отключите Renegotiation по инициативе клиента
   В SSL / TLS renegotiation позволяет сторонам остановить обмен данными, с тем чтобы повторно инициировать его для обеспечения безопасности. Есть некоторые случаи, в которых renegotiation должен быть инициирован сервером, но нет никакой известной необходимости позволять инициировать renegotiation клиентом. Кроме того это может облегчить организацию DDoS-атаки на ваши сервера.

   (e) Снижение известных проблем
   В какой-то момент могут возникнуть проблемы с безопасностью с любым продуктом. Хорошо, если вы всегда в курсе событий в мире информационной безопасности.

Уязвимости POODLE, HeartBleed

POODLE - это уязвимость в SSLv3, она позволяет злоумышленнику, имеющему какую-либо возможность отправлять свои данные на сервер по SSLv3 от имени жертвы, расшифровывать по 1 байту за 256 запросов. Происходит это из-за того, что в SSLv3 не учитывается MAC адрес.
Теоретически, реализовать атаку POODLE можно на любой сервис, где есть возможность влиять на отправляемые данные со стороны атакуемого. Для этого атакующему необходимо:

- Иметь возможность прослушивать и подменять трафик атакуемого
- Иметь возможность совершать запросы от имени атакуемого с известным атакующему текстом

HeartBleed - это уязвимость в безопасности программной библиотеки OpenSSL (открытой реализации протокола шифрования SSL/TLS), которая позволяет хакерам получить доступ к содержимому оперативной памяти серверов, в которых в этот момент могут содержаться приватные данные пользователей различных веб-сервисов.
Уязвимость позволяет взломщику получить доступ к 64 килобайтам оперативной памяти сервера и осуществлять атаку вновь и вновь вплоть до полной потери данных. Это означает, что утечке подвержены не только логины и пароли, но и данные файлов cookie, которые веб-серверы и сайты используют для отслеживания действий пользователя и упрощения авторизации.

2.2 Практическое задание

В качестве Recent Best был проанализирован сайт forum.anfs.eu. Отчет представлен на рисунке 1. Сайт имеет оценку A.

В качестве Recent Worst был проанализирован сайт synata.com. Отчет

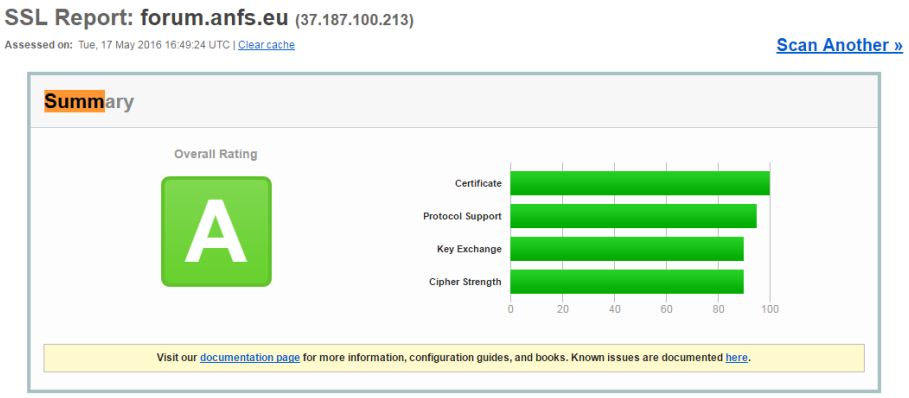

Рис. 1: Отчет для сайта forum.anfs.eu

представлен на рисунке 2. Сайт имеет оценку F.
Замечания отчета:

- Сайт поддерживает анонимный (небезопасный) набор алгоритмов. Оценка F.
- Сайт поддерживает слабые Диффи-Хеллмана (DH) параметры обмена ключа. Оценка B.
- Сайт поддерживает только старые протоколы, а не текущие TLS 1.2. Оценка C.
- Сайт принимает шифр RC4, но только с более старыми версиями протокола. Оценка B.
- Сайт не поддерживает Forward Secrecy

Выберем для самостоятельного анализа домен github.com. Домен защищен SSL шифровнием.

Summary. Отчет для выбранного домена представлен на рисунке 3. Сайт имеет оценку A+ (наивысшую). Дополнительных замечаний на домен не было обнаружено.

Configuration. Расшифруем шифры в этом разделе.

```
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
256
```

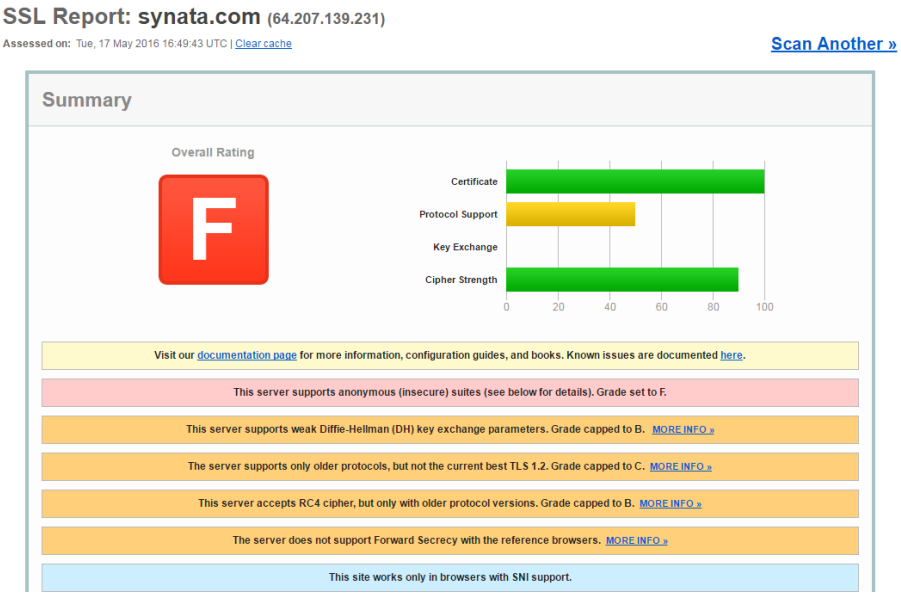

Рис. 2: Отчет для сайта synata.com

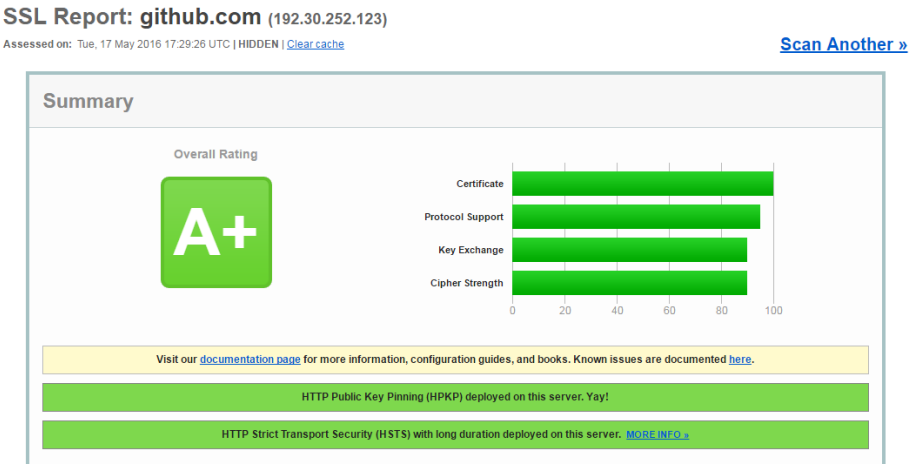

Рис. 3: Отчет для сайта github.com

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) 128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) 256
```

```
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) 128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) 128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) 256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) 256
```

- TLS - протокол защищенной передачи данных;
- ECDHE - алгоритм Диффи-Хэлмана на эллиптических кривых;
- RSA - алгоритм шифрования с открытым ключем;
- GCM - режим блочного шифрования;
- CBC - режим блочного шифрования;
- AES_128 - алгоритм шифрования с длиной ключа в 128 бит;
- SHA256 - хэш-функция с длиной ключа 256 бит;
- SHA384 - хэш-функция с длиной ключа 384 бит.

Protocol Details. Просмотрим детали протокола подробнее
Сайт защищен от атак DROWN, BEAST, POODLE (SSLv3, TLS)

```
DROWN (experimental) No, server keys and hostname not seen elsewhere with SSLv2
BEAST attack Not mitigated server-side (more info)   TLS 1.0: 0xc013
POODLE (SSLv3) No, SSL 3 not supported (more info)
POODLE (TLS) No (more info)
```

Поддерживается технология привязки ключей

```
Public Key Pinning (HPKP) Yes
```

Сайт поддерживает функцию Heartbeat, но защищен от уязвимости Heartbleed, основанной на этой функции.

```
Heartbeat (extension) Yes
Heartbleed (vulnerability) No (more info)
```

Поддержка Forward Security для современных браузеров.

```
Forward Secrecy With modern browsers (more info)
```

Поддерживает ALPN и не поддерживает NPN.

```
ALPN Yes
NPN No
```

Поддержка возобновления сессии, используя механизм кеширования.

```
Session resumption (caching) Yes
Session resumption (tickets) No
```

Перенаправление на HTTPS при помощи HSTS

```
Strict Transport Security (HSTS) Yes
HSTS Preloading
```

Предотвращение атаки Downgrade attack, с помощью которой злоумышленник может понизить версию используемых протоколов.

```
Downgrade attack prevention Yes, TLS_FALLBACK_SCSV supported
```

Протокол Диффи-Хеллмана не поддерживается.

```
Uses common DH primes No, DHE suites not supported
DH public server param (Ys) reuse No, DHE suites not supported
```

Итоговый вывод. Домен github.com имеет наивысшую оценку (A+) по реализации SSL. Сайтом поддерживается технология привязки ключей, функция Heartbeat(при этом осуществлена защита от уязвимости Heartbleed, основанной на этой функции). Также поддерживаются: Forward Security для современных браузеров, ALPN, возможность возобновления сессии при помощи механизма кеширования и другое. Данный домен является надежным.

3 Вывод

В ходе данной лабораторной работы были изучены возможности сервиса SSL Labs, анализирующего качество защиты домена.
Были просмотрены отчеты для двух типов сервисов: имеющих наибольшую оценку и наименьшую.
Также был проанализирован домен github.com. Был просмотрен отчет по данному домену, содержащий конкретные детали: используемые способы шифрования, защита от уязвимстей и другое. На основе полученной информации был сделан вывод, что сайт github.com является хорошо защищенным.