Лабораторная работа №5.
SSL/TSL

Евсеев Дмитрий

20 июня 2016 г.

Оглавление

1 Цель работы

Сервис тестирования корректности настройки SSL на сервере Qualys SSL Labs – SSL Server Test

2 Ход работы

2.1 Лучшие практики по развертыванию SSL

- Использовать 2048-битные закрытые ключи. Использовать 2048-битный RSA или 256-битные ECDSA закрытые ключи для всех серверов. Ключи такой крепости безопасны и будут оставаться безопасными в течение значительного периода времени.
- Защитить закрытый ключ. Относитесь к закрытым ключам как к важным активам, предоставляя доступ к как можно меньшей группе сотрудников.
- Обеспечить охват всех используемых доменных имен. Убедитесь, что ваши сертификаты охватывают все доменные имена, которые вы хотите использовать на сайте.
- Приобретать сертификаты у надежного удостоверяющего центра (CA).
- Использовать надежные алгоритмы подписи сертификата. Безопасность сертификата зависит от длины закрытого ключа и прочности используемой функции хеширования. Сегодня большинство сертификатов используют алгоритм SHA1, который считается слабым.
- Использовать безопасные протоколы. (TLS v1.0/v1.1/v1.2)
- Использовать безопасные алгоритмы шифрования. В данном случае подойдут симметричные алгоритмы с ключами более 128 бит.
- Контролировать выбор алгоритма шифрования. В SSL версии 3 и более поздних версиях протокола, клиенты отправляют список алгоритмов шифрования, которые они поддерживают, и сервер выбирает один из них для организации безопасного канала связи. Не все сервера могут делать это хорошо, так как некоторые выбирают первый поддерживаемый алгоритм из списка.
- Использование Forward Secrecy. Forward Secrecy — это особенность протокола, который обеспечивает безопасный обмен данными, он не зависит от закрытого ключа сервера. С алгоритмами шифрования, которые не поддерживают Forward Secrecy, возможно расшифровать ранее зашифрованные разговоры с помощью закрытого ключа сервера.
- Отключить проверку защищенности по инициативе клиента.

2.2 Основные уязвимости и атаки на SSL

POODLE

Атака POODLE(Padding Oracle On Downgraded Legacy Encryption) работает по следующему сценарию: Взломщик отправляет свои данные на вервер по протоколу SSL3 от имени взламываемой структуры, что позволяет ему постепенно расшифровывать данные из запросов. Это возможно, так как в SSL3 нету привязки к MAC адресу.

Heartbleed

Ошибка (переполнение буфера) в криптографическом программном обеспечении OpenSSL, позволяющая несанкционированно читать память на сервере или на клиенте, в том числе для извлечения закрытого ключа сервера. Информация об уязвимости была опубликована в апреле 2014 года, ошибка существовала с конца 2011 года.

2.3 Домен из списка Recent Best

Со стартовой страницы SSL Server Test выбран один домен из списка Recent Best (рисунок 1).

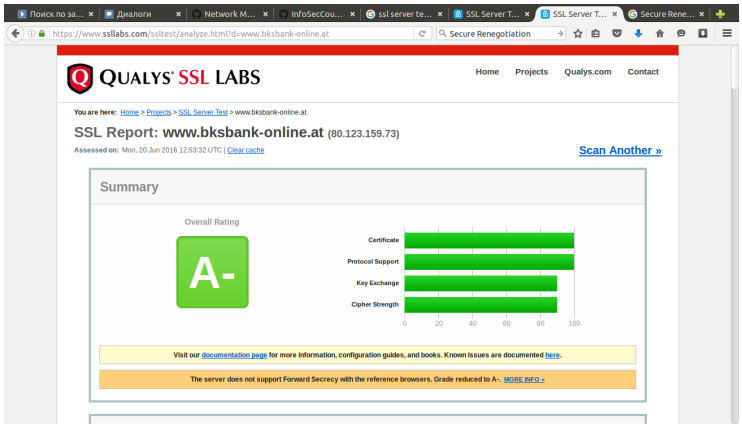

Рис. 1: Summary для recent best.

Recent Best

- Поддержка TLS 1.2
- Не поддерживает небезопасный SSL v3
- Поддержка Secure Renegotiation

2.4 Домен из списка Recent Worst

Summary для домена из Recent worst (рисунок 2)

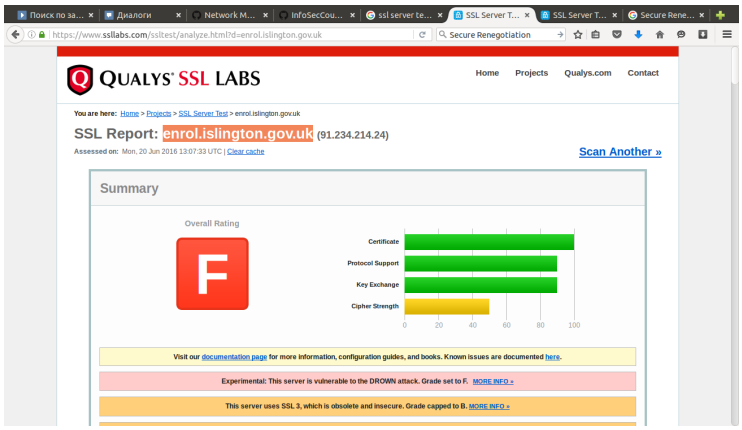

Рис. 2: Summary для recent worst.

Recent Worst

- Поддерживает небезопасный SSL v3
- Подвержен DROWN атакам
- Использует небезопасный RC4
- Не поддерживает Forward secrecy

2.5 Выбор интернет-домена, защищенного SSL-шифрованием.

Для анализа защищенности SSL шифрованием был выбран домен youtube.com (рисунок 3).

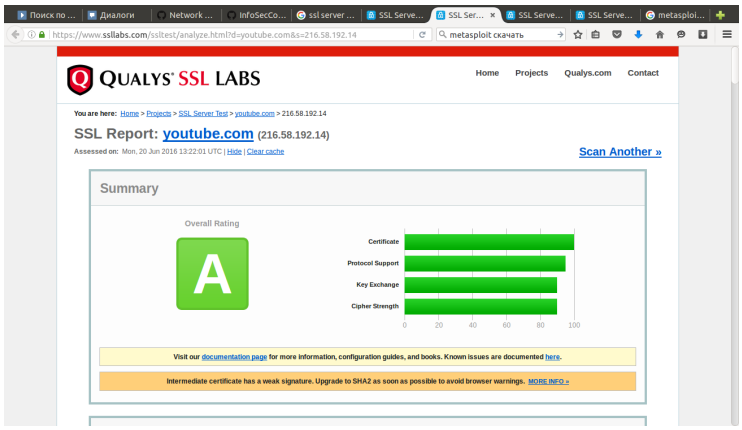

Рис. 3: Summary для youtube.com.

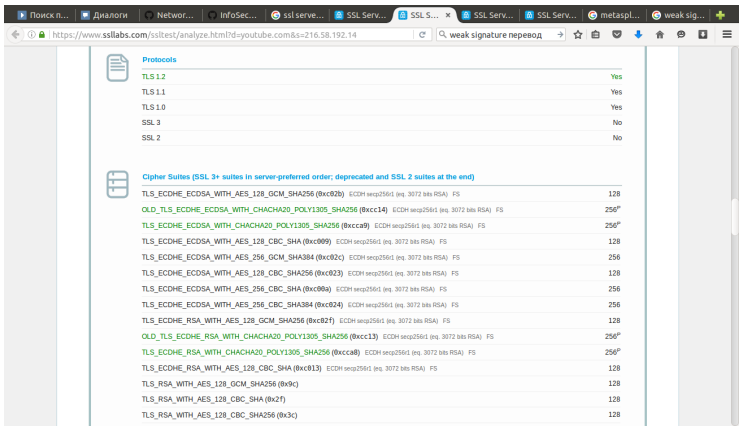

Рис. 4: Configuration для youtube.com.

Configuration

- ECDH - Elliptic curve Diffie–Hellman - Протокол Диффи-Хеллмана на эллиптических кривых
- RSA - Rivest, Shamir, Adleman - криптографический алгоритм
- RC4 - Rivest Cipher 4 - потоковый шифр 4-й версии
- SHA/SHA256/384 - Secure Hash Algorithm - Алгоритм хэширования. Цифра - длина ключа
- AES - Advanced Encryption Standard - симметричный алгоритм блочного шифрования
- GCM и CBC это два режима блочного шифрования
- TLS - Transport Layer Security - криптографический протокол
- 3DES - Digital Encryption Standard - алгоритм блочного шифрования
- EDE - Encrypt, Decrypt, Encrypt - режим работы алгоритма 3DES

Protocol details

- Secure Renegotiation - Возобновление подлючения TLS
- Secure Client-Initiated Renegotiation, Insecure Client-Initiated Renegotiation - подверженность процесса проверки сертификата атаке.
- BEAST attack, POODLE (SSLv3), POODLE (TLS) - проверка уязвимости к данным атакам.
- Downgrade attack prevention - атака, при которой клиента принудительно заставляют использовать предыдущие (менее надежные) версии протоколов

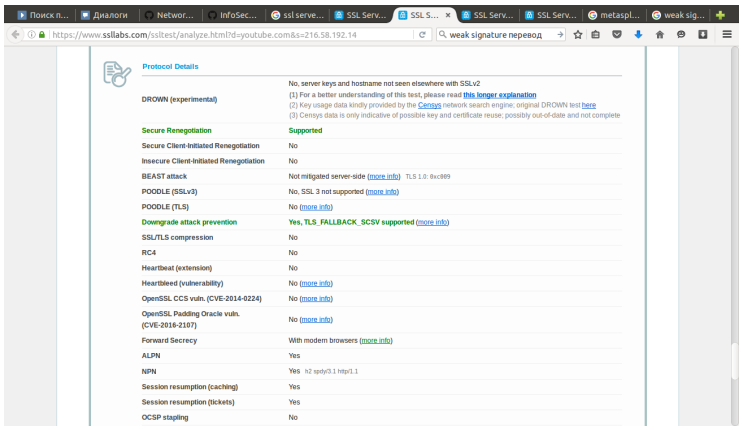

Рис. 5: Protocol details для youtube.com.

- SSL/TLS compression - сжатие SSL/TLS не используется
- RC4 - Не спользуется слабый шифр RC4
- Heartbeat (extension), Heartbleed (vulnerability), OpenSSL CCS vuln. (CVE-2014-0224) - уязвимости OpenSSL Heartbleed и тд.
- Forward Secrecy - совместимость Forward Secrecy с новыми браузерами.
- Strict Transport Security (HSTS) - форсированное переключение на HTTPS
- SSL 2 handshake compatibility - Совместимость с SSL 2 handshake

2.6 Вывод о реализации SSL на youtube.com

Общую защищенность сервера можно оценить как отличную. Все характеристики удовлетворяют лучшим практикам развертывания SSL.

3 Выводы

В результате выполнения работы были изучены лучшие практики по развертыванию SSL серверов, а так же средство для проверки SSL серверов Qualys SSL Server Test, которое позволяет подробно изучить любой домен. Полученные данные помогут получить действительную картину защищенности сервера и понять какие действия необходимо препринять для улучшения стабильности и безопасности сервера.