Отчет по лабораторной работе № 7.

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

Выполнил студент: Греченко Л.В.

Изучение

1. Изучить лучшие практики по развертыванию SSL/TLS

2. Изучить основные уязвимости и атаки на SSL последнего времени

– POODLE, HeartBleed

POODLE

Этой уязвимости поддвержен SSL-протокол версии 3, который позволяет перехватить содержимое зашифрованное с помощью SSLv3. Этой уязвимости подвержено любое программное обеспечение, использующее для шифрования соединения SSLv3. Это веб-браузеры, веб-серверы, почтовые серверы и тому подобное.

POODLE присутствует, потому что протокол SSLv3 некорректно проверяет содержимое, пересылаемое в зашифрованном виде.

Благодаря этому не происходит верификации со стороны получателя и атакующий может подменять данные и передавать к месту получения. При определенных условиях модифицированные данные могут быть приняты получателем без каких-либо предупреждений.

В среднем, каждый 256-й запрос будет принят получателем и позволит злоумышленнику расшифровать один байт. Это может быть повторено нужное количество раз. Любой злоумышленник, участвуя таким образом в пересылке данных с помощью этого протокола, сможет получить ключ к расшифровке данных за очень короткое время.

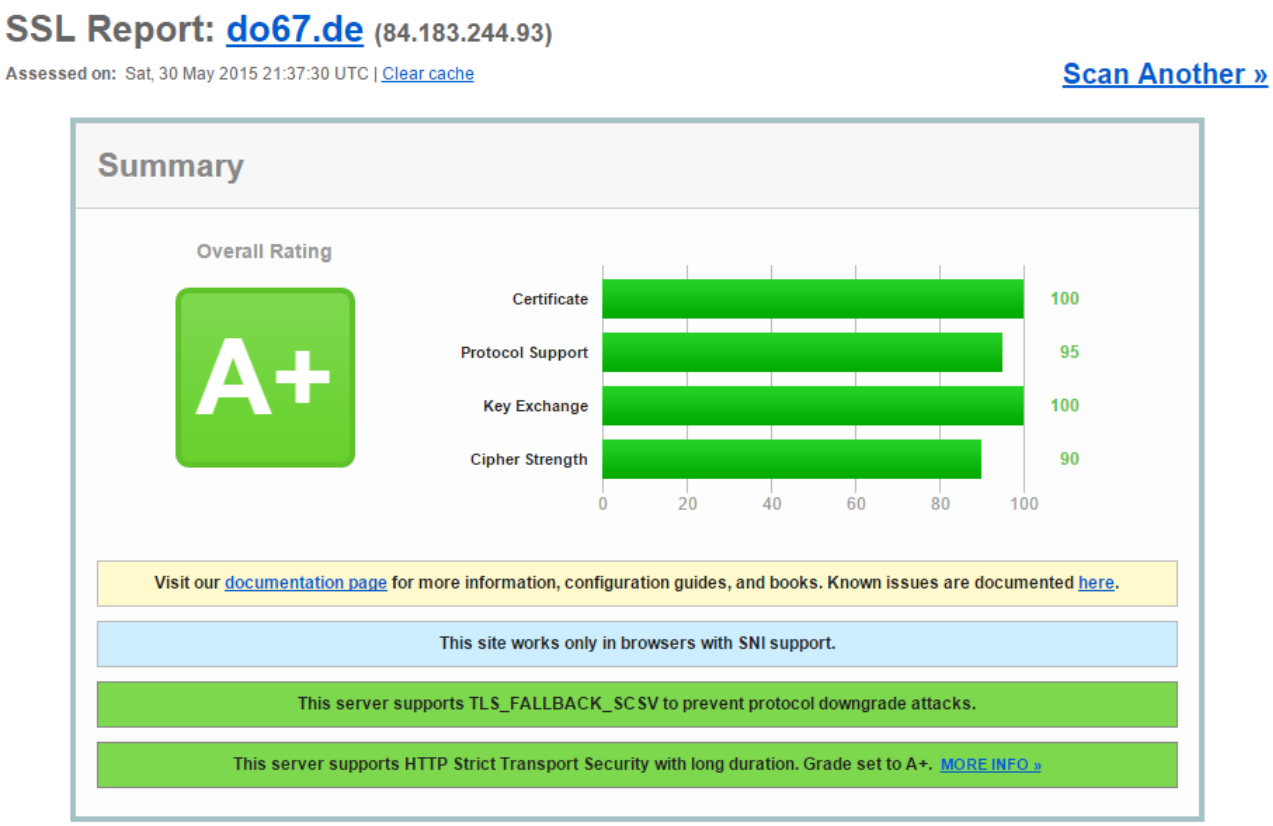
HeartBleed

Heartbleed — уязвимость в безопасности программной библиотеки OpenSSL (открытой реализации протокола шифрования SSL/TLS), которая позволяла хакерам получить доступ к содержимому оперативной памяти серверов, в которых в этот момент могли содержаться приватные данные пользователей различных веб-сервисов. Это значит, что на этих сайтах потенциально под угрозой оказались такие личные данные пользователей, как логины, пароли, данные кредитных карт и т.д. Уязвимость также позволяла злоумышленникам получить цифровые ключи, использующиеся, например, для шифрования переписки и внутренних документов во множестве компаний.

Практическое задание

1. Выбрать со стартовой страницы SSL Server Test один домен из списка Recent Best и один домен из списка Recent Worst – изучить отчеты, интерпретировать результаты в разделе Summary

Из списка Recent Best был выбран:



“This site works only in browsers with SNI support.” – Этот сайт работает только с браузерами поддерживающими SNI.

Индикация имени сервера (SNI или Server Name Indication) – это расширение TLS протокола, которое указывает к какому хосту пытается подключиться клиент в начале процесса квитирования (установки соединения). Соответственно это позволяет серверу с самого начала определить корректное имя виртуального хоста для запроса и установки защищенного соединения.

С помощью SNI, можно иметь несколько доменов, привязанных к одному и тому же IP-адресу и порту, и на каждом из этих доменных имен Вы можете установить отдельный SSL сертификат.

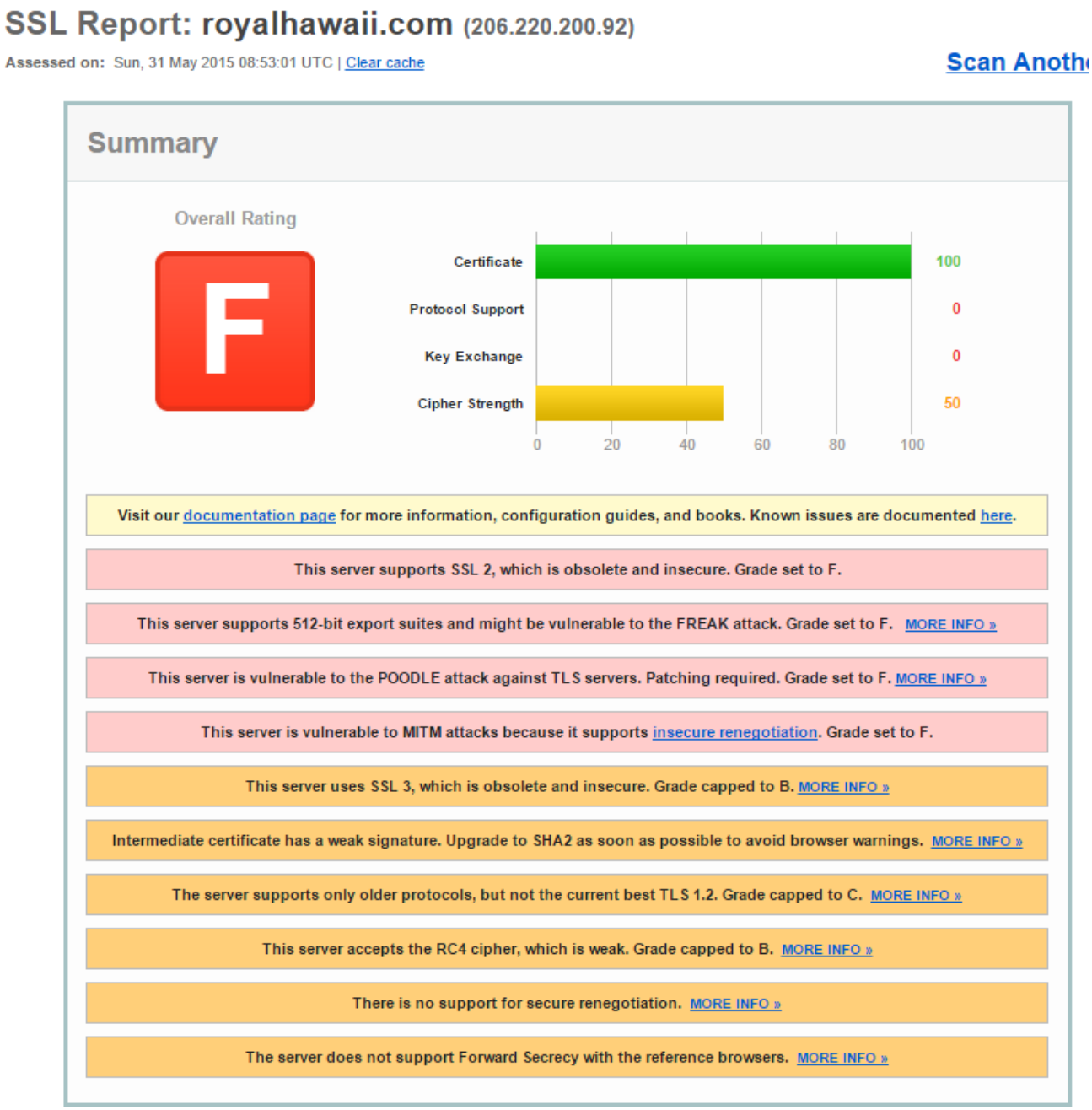
This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks. - Этот сервер поддерживает TLS_FALLBACK_SCSV, чтобы предотвратить атаки протокола более ранней версии.

Специалисты по безопасности опубликовали подробности об уязвимости в дизайне протокола SSL 3.0. Уязвимость под кодовым названием POODLE позволяет расшифровать содержимое защищённого канала коммуникации. В общем, на всех системах необходимо блокировать использование SSL 3.0, потому что работающего способа обойти эксплоит не существует. Но злоумышленник может умышленно принудить клиента подключиться именно по SSL 3.0, эмулируя разрывы связи, и после этого эксплуатировать уязвимость. Рекомендуемый способ обхода — поддержка механизма TLS_FALLBACK_SCSV, который не позволяет злоумышленнику снизить защиту канала до SSL 3.0. Механизм также предотвращает снижение защиты с TLS 1.2 до 1.1 или 1.0, что может помочь в предотвращении будущих атак.

This server supports HTTP Strict Transport Security with long duration. - Этот сервер поддерживает HTTP Strict Transport Security с большой продолжительностью.

HTTP Strict Transport Security (HSTS) — механизм, активирующий форсированное защищённое соединение по HTTPS. Данная политика безопасности позволяет сразу же устанавливать безопасное соединение, вместо использования HTTP. Механизм использует особый заголовок HTTP Strict-Transport-Security, для переключения пользователя, зашедшего по HTTP, на HTTPS-сервер.

Из списка Recent Worst был выбран:



«This server supports SSL 2, which is obsolete and insecure» - Этот сервер поддерживает SSL 2, который является устаревшим и небезопасным.

«This server supports 512-bit export suites and might be vulnerable to the FREAK attack» - Сервер может быть уязвим к атаке FREAK.

Название уязвимости «атака FREAK» происходит от фразы «Factoring attack on RSA-EXPORT Keys», означающей способ подбора открытых ключей к «экспортному» шифрованию RSA. Суть уязвимости заключается в том, что злоумышленники могут заставить браузеры использовать более слабое шифрование, чем принято обычно. Тогда они смогут взломать его за считанные часы, получив не только доступ к чужим личным данным, но и возможность управлять содержимым страниц в браузере

«This server is vulnerable to the POODLE attack against TLS servers» - Этот сервер является уязвимым для POODLE нападения на TLS.

This server is vulnerable to MITM attacks because it supports insecure renegotiation. Этот сервер является уязвимым для атак MITM.

Атака «человек посередине», MITM-атака (англ. Man in the middle) — термин в криптографии, обозначающий ситуацию, когда криптоаналитик (атакующий) способен читать и видоизменять по своей воле сообщения, которыми обмениваются корреспонденты, причём ни один из последних не может догадаться о его присутствии в канале.

This server uses SSL 3, which is obsolete and insecure. - Этот сервер использует SSL 3, который является устаревшим и небезопасным.

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. - Промежуточный сертификат имеет слабую подпись.

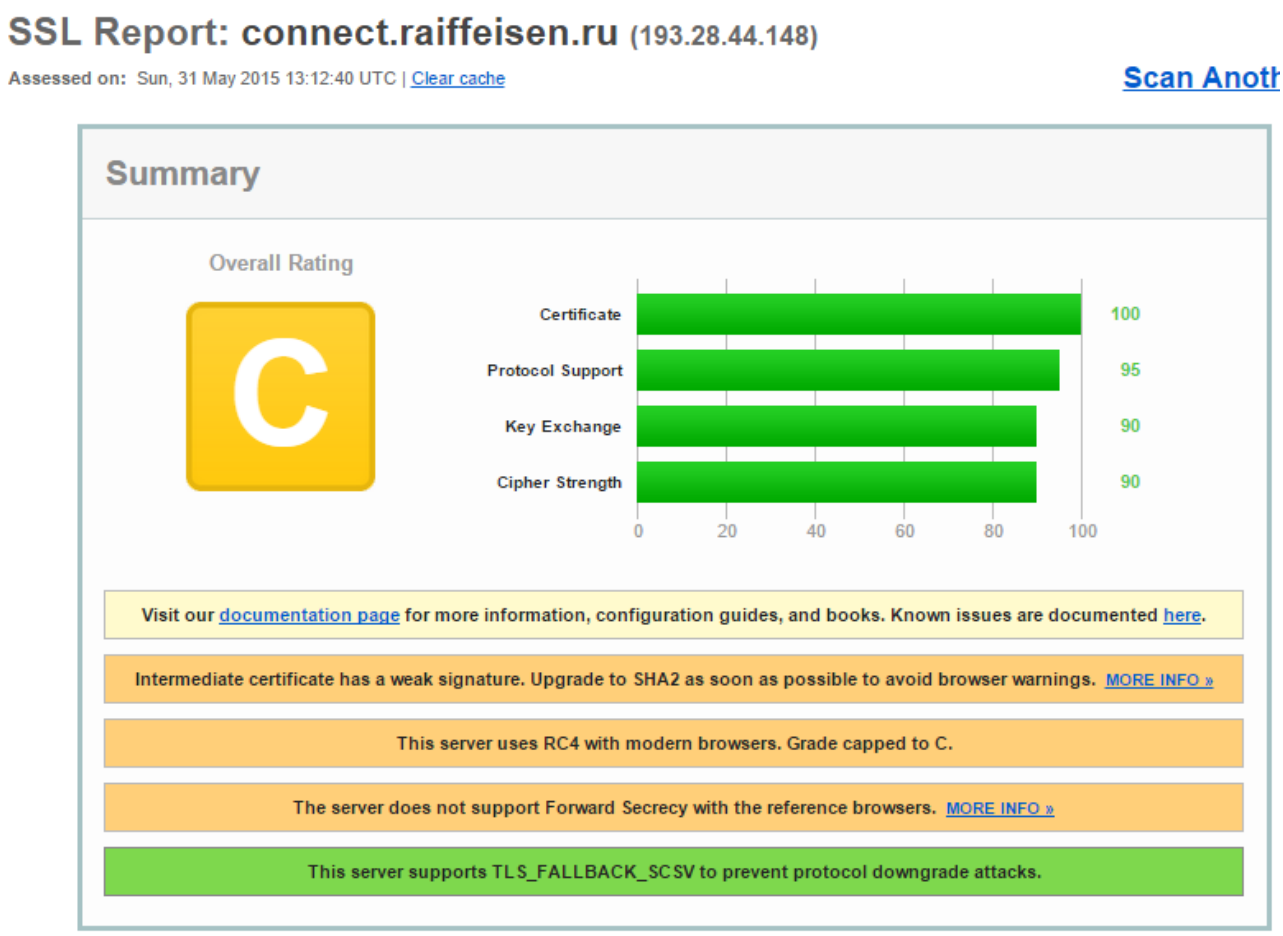
The server supports only older protocols, but not the current best TLS 1.2. - Сервер поддерживает только старые протоколы, но не текущий лучший TLS 1.2.

This server accepts the RC4 cipher, which is weak. Этот сервер принимает шифр RC4, который является слабым.

The server does not support Forward Secrecy with the reference browsers. Сервер не поддерживает Forward Secrecy с исходных браузеров.

Forward Secrecy - свойство некоторых протоколов согласования ключа (Key-agreement), которое гарантирует, что сессионные ключи, полученные при помощи набора ключей долговременного пользования, не будут скомпрометированы при компрометации одного из долговременных ключей.

2. Выбрать для анализа интернет-домен защищенный SSL-шифрованием (старайтесь выбрать что-то достаточно известное, но не слишком очевидное), проделать следующие шаги:
    a. **Интерпретировать результаты в разделе Summary**



Промежуточный сертификат имеет слабую подпись. Необходимо обновление до SHA2 как можно скорее, чтобы избежать предупреждений браузера. Этот сервер использует RC4 с современными браузерами. Сервер не поддерживает Forward Secrecy с контрольными браузерами. Этот сервер поддерживает TLS_FALLBACK_SCSV, чтобы предотвратить атаки протокола более ранней версии.

b. Расшифровать все аббревиатуры шифров в разделе Configuration

TLS_RSA_WITH_RC4_128_SHA (0x5) WEAK 128

Для обмена ключами и проверки их подлинности применяется алгоритм: RSA

Для симметричного шифрования: RC4 с длиной ключа 128 бит

Для хеш-функций: SHA

TLS_RSA_WITH_RC4_128_MD5 (0x4) WEAK 128

Для обмена ключами и проверки их подлинности применяется алгоритм: RSA

Для симметричного шифрования: RC4 с длиной ключа 128 бит

Для хеш-функций: MD5

TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) 256

Для обмена ключами и проверки их подлинности применяется алгоритм: RSA

Для симметричного шифрования: AES с длиной ключа 256 бит с использованием блочных шифров

Для хеш-функций: SHA с длиной ключа 256 бит

TLS_RSA_WITH_AES_256_CBC_SHA (0x35) 256

Для обмена ключами и проверки их подлинности применяется алгоритм: RSA

Для симметричного шифрования: AES с длиной ключа 256 бит с использованием блочных шифров

Для хеш-функций: SHA

TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) 128

Для обмена ключами и проверки их подлинности применяется алгоритм: RSA

Для симметричного шифрования: AES с длиной ключа 128 бит с использованием блочных шифров

Для хеш-функций: SHA с длиной ключа 256 бит

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) 128

Для обмена ключами и проверки их подлинности применяется алгоритм: RSA

Для симметричного шифрования: AES с длиной ключа 128 бит с использованием блочных шифров

Для хеш-функций: SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) 112

Для обмена ключами и проверки их подлинности применяется алгоритм: RSA

Для симметричного шифрования: 3DES операции шифровка-расшифровка-шифровка с тремя разными ключами, с использованием блочных шифров

Для хеш-функций: SHA

3. Прокомментировать большинство позиций в разделе Protocol Details

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info) TLS 1.0: 0x5
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
TLS compression	No
RC4	Yes **WEAK** (more info)
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	No **WEAK** (more info)
Next Protocol Negotiation (NPN)	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
Public Key Pinning (HPKP)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	-
Uses common DH prime	No
SSL 2 handshake compatibility	Yes

Secure Renegotiation	Поддерживает возобновление подключения TLS.
Secure Client-Initiated Renegotiation	Нет. Есть некоторые случаи, в которых возобновление должно быть инициировано сервером, но нет никакой известной необходимости для клиентов, чтобы сделать это. Кроме того, возобновление по инициативе клиента может сделать сервер более уязвимым к атакам с помощью отказа в обслуживании (DoS).
Insecure Client-Initiated Renegotiation	Нет.
BEAST attack	Смягчено со стороны сервера
POODLE (SSLv3)	Нет, SSL3 не поддерживается.
POODLE (TLS)	Нет

Downgrade attack prevention	**Да, TLS_FALLBACK_SCSV поддерживается**
TLS compression	Нет
RC4	**Да**
Heartbeat (расширение)	Да. Предоставляет новый протокол для TLS / DTLS, позволяющий использование функциональности Keep-Alive, не выполняя возобновления.
Heartbleed (уязвимости)	Нет.
OpenSSL CCS vuln. (CVE-2014-0224)	Нет. Возможность выполнить MITM атаку.
Forward Secrecy	**Нет.**
Next Protocol Negotiation (NPN)	Нет.
Возобновление сессии (кэширование)	Да.
Session resumption (tickets)	Да. Протокол SSL /TLS включает в себя сеанс кэширование, чтобы сократить количество дорогостоящих криптографических операций, если клиент ранее посетил его.
OCSP stapling	Нет, OCSP (или Online Certificate Status Protocol) – это протокол, проверяющий, был ли отозван SSL-сертификат. Используя OCSP, браузер посылает запрос к OCSP URL и получает ответ, содержащий состояние достоверности сертификата.
Strict Transport Security (HSTS)	Нет, механизм, активирующий форсированное защищённое соединение по HTTPS. Данная политика безопасности позволяет сразу же устанавливать безопасное соединение, вместо использования HTTP.
Public Key Pinning (HPKP)	Нет, Реализовано HTTP-расширение для механизма привязки открытых ключей (Public Key Pinning), позволяющего явно определить сертификаты каких удостоверяющих центров допустимо использовать для заданного сайта. Если для установки защищённого соединения применён достоверный сертификат выписанный иным удостоверяющим центром, соединение будет отвергнуто из-за подозрения в атаке "man-in-the-middle" с использованием поддельного сертификата.
Long handshake intolerance	Нет.
TLS extension intolerance	Нет.
TLS version intolerance	Нет.
Incorrect SNI alerts	-
Uses common DH prime	No
SSL 2 handshake compatibility	Yes

3. Сделать итоговый вывод о реализации SSL на заданном домене.

Оценка C. Есть проблемы с обменом ключей и шифрованием.

Вывод:

В данной лабораторной работе были изучены возможности **Qualys SSL Labs SSL Server Test** . Сервис позволяет проверить SSL-сертификат, который используется на вашем (или чужом) веб-сайте, и получить его полную диагностику. Первым делом проверили интернет-банкинг своего банка.