Санкт-Петербургский государственный политехнический университет

Институт компьютерных наук и технологий

Кафедра компьютерных систем и программных технологий

ОТЧЕТ

о лабораторной работе №6

по дисциплине: «Информационная безопасность»

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

Работу выполнил студент

53501/3 *Алексюк Артём*

Преподаватель

_____ *Вылегжанина Карина Дмитриевна*

Санкт-Петербург
2016

1. Цель работы

1) Изучить лучшие практики по развертыванию SSL/TLS

2) Изучить основные уязвимости и атаки на SSL последнего времени - POODLE, HeartBleed

2. Пример правильно настроенного сервера

Возьмем некий сайт h31.ishere.ru. На этом сервере запущен веб-сервер nginx версии 1.4.6 с последними обновлениями безопасности.

Настройки веб-сервера, касаюшиеся TLS:

```
1  listen 80;
2  listen 443 ssl;
3
4  ssl_certificate chain.pem;
5  ssl_certificate_key key.pem;
6
7  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
8  ssl_prefer_server_ciphers on;
9  ssl_ciphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-
       SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:
       DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:
       ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-
       SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-
       AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-
       AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-
       AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!
       EXPORT:!DES:!RC4:!3DES:!MD5:!PSK';
10 ssl_session_cache shared:SSL:10m;
11 ssl_dhparam dhparam.pem;
12 ssl_stapling on;
13 ssl_stapling_verify on;
14 ssl_trusted_certificate chain.pem;
```

Просканируем сервер с помощью SSL Server Test:

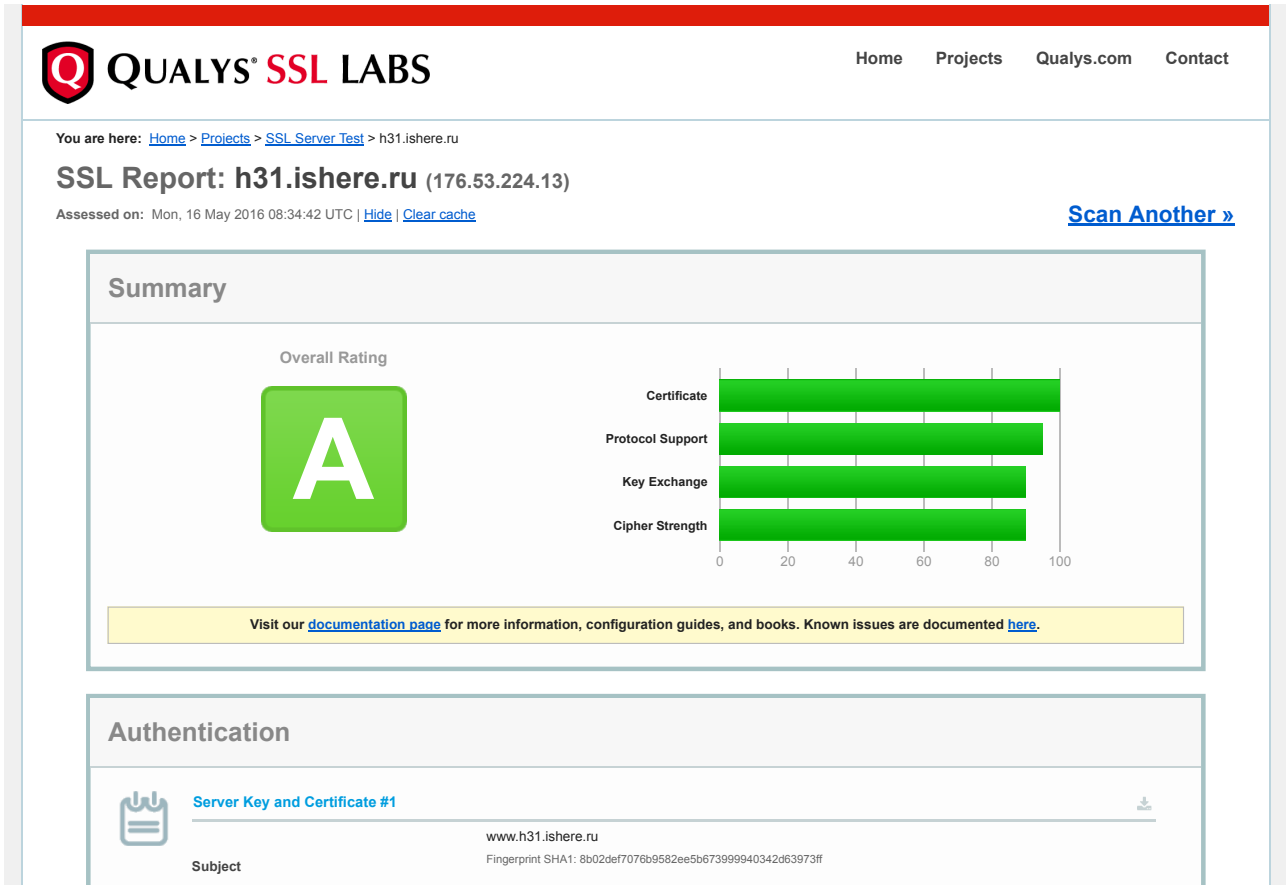

Рис. 1: Отчет SSL Server Test для h31.ishere.ru

В логах веб-сервера можно увидеть обращения от сервиса:

```
1 64.41.200.101 - - [16/May/2016:11:32:33 +0300] "GET / HTTP/1.0" 200
    1773 "-" "SSL Labs (https://www.ssllabs.com/about/assessment.html)"
2 64.41.200.101 - - [16/May/2016:11:32:45 +0300] "GET /?
    SSL_Labs_Renegotiation_Test=User_Agent_May_Not_Show HTTP/1.0" 400 0
     "-" "SSL Labs (https://www.ssllabs.com/about/assessment.html)"
3 64.41.200.101 - - [16/May/2016:11:32:46 +0300] "GET /?
    SSL_Labs_Renegotiation_Test=User_Agent_May_Not_Show HTTP/1.0" 400 0
     "-" "SSL Labs (https://www.ssllabs.com/about/assessment.html)"
```

2.1. Расшифровка аббревиатур

- TLS_ECDHE - алгоритм Диффи-Хэлмана на эллиптических кривых;
- RSA - алгоритм шифрования с открытым ключем;
- AES_128 - алгоритм шифрования с длиной ключа в 128 бит;
- GCM и CBC - режимы блочного шифрования;
- SHA256 - хэш-функция с длиной ключа 256 бит.

2.2. Аутентификация

- Имя основного домена:

```
Subject www.h31.ishere.ru
Fingerprint SHA1: 8b02def7076b9582ee5b673999940342d63973ff
Pin SHA256: Ln8/YgY3VzhA229r6cuXoUd0wzD4XiUoTRzi/NLCq3I=
```

- Сетификат ещё актуален

```
Valid until     Mon, 20 Jun 2016 18:28:00 UTC (expires in 1 month
    and 4 days)
```

- Центр сертификации:

```
Issuer  Let's Encrypt Authority X1
AIA: http://cert.int-x1.letsencrypt.org/
```

- Способ информирования об отзыве сертификата

```
Revocation information  OCSP
OCSP: http://ocsp.int-x1.letsencrypt.org/
```

- Можно ли доверять сертификату

```
Trusted Yes
```

- Цепочка сертификатов

```
1       Sent by server  www.h31.ishere.ru
Fingerprint SHA1: 8b02def7076b9582ee5b673999940342d63973ff
Pin SHA256: Ln8/YgY3VzhA229r6cuXoUd0wzD4XiUoTRzi/NLCq3I=
RSA 2048 bits (e 65537) / SHA256withRSA
2       Sent by server  Let's Encrypt Authority X1
Fingerprint SHA1: 3eae91937ec85d74483ff4b77b07b43e2af36bf4
Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=
RSA 2048 bits (e 65537) / SHA256withRSA
3       In trust store  DST Root CA X3   Self-signed
Fingerprint SHA1: dac9024f54d8f6df94935fb1732638ca6ad77c13
Pin SHA256: Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys=
RSA 2048 bits (e 65537) / SHA1withRSA
Weak or insecure signature, but no impact on root certificate
```

2.3. Аутентификация

- Версии TLS. Безопасные - поддерживаются, небезопасные - отключены.

```
Protocols
TLS 1.2 Yes
TLS 1.1 Yes
TLS 1.0 Yes
SSL 3   No
SSL 2   No
```

- Протоколы шифрования. Предпочитается AES-GCM с обменом ключами с помощью ECDHE.

```
1  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)   ECDH secp256r1 (
     eq. 3072 bits RSA)   FS         128
2  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)   ECDH secp256r1 (
     eq. 3072 bits RSA)   FS         256
3  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)   DH 2048 bits   FS
     128
4  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)   DH 2048 bits   FS
     256
5  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)   ECDH secp256r1 (
     eq. 3072 bits RSA)   FS         128
6  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)   ECDH secp256r1 (eq.
      3072 bits RSA)   FS   128
7  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)   ECDH secp256r1 (
     eq. 3072 bits RSA)   FS         256
8  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)   ECDH secp256r1 (eq.
      3072 bits RSA)   FS   256
9  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)   DH 2048 bits   FS
     128
10 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)   DH 2048 bits   FS
     128
11 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)   DH 2048 bits   FS
     256
12 TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)   DH 2048 bits   FS
     256
```

- Проверка основных уязвимостей. Ни одна из них не может быть применена к этому сайту.

```
1  DROWN (experimental)    No, server keys and hostname not seen
     elsewhere with SSLv2
2  (1) For a better understanding of this test, please read this
     longer explanation
3  (2) Key usage data kindly provided by the Censys network search
     engine; original DROWN test here
4  (3) Censys data is only indicative of possible key and
     certificate reuse; possibly out-of-date and not complete
5  Secure Renegotiation    Supported
6  Secure Client-Initiated Renegotiation   No
7  Insecure Client-Initiated Renegotiation No
8  BEAST attack    Not mitigated server-side (more info)   TLS 1.0:
     0xc013
9  POODLE (SSLv3)  No, SSL 3 not supported (more info)
10 POODLE (TLS)    No (more info)
11 Downgrade attack prevention     Yes, TLS_FALLBACK_SCSV supported
     (more info)
12 SSL/TLS compression     No
13 RC4     No
14 Heartbeat (extension)   Yes
15 Heartbleed (vulnerability)      No (more info)
16 OpenSSL CCS vuln. (CVE-2014-0224)       No (more info)
```

- Forward Secrecy - при взломе сервера и получении приватного ключа не получится расшифровать старые соединения (установленные до взлома)

```
1  Forward Secrecy Yes (with most browsers)   ROBUST (more info)
```

Итого: сервер не уязвим к основным атакам. Можно и дальше повышать безопасность, но потеряется совместимость со старыми клиентами.

3. Пример неправильно настроенного сервера

Просканируем people.epfl.ch.

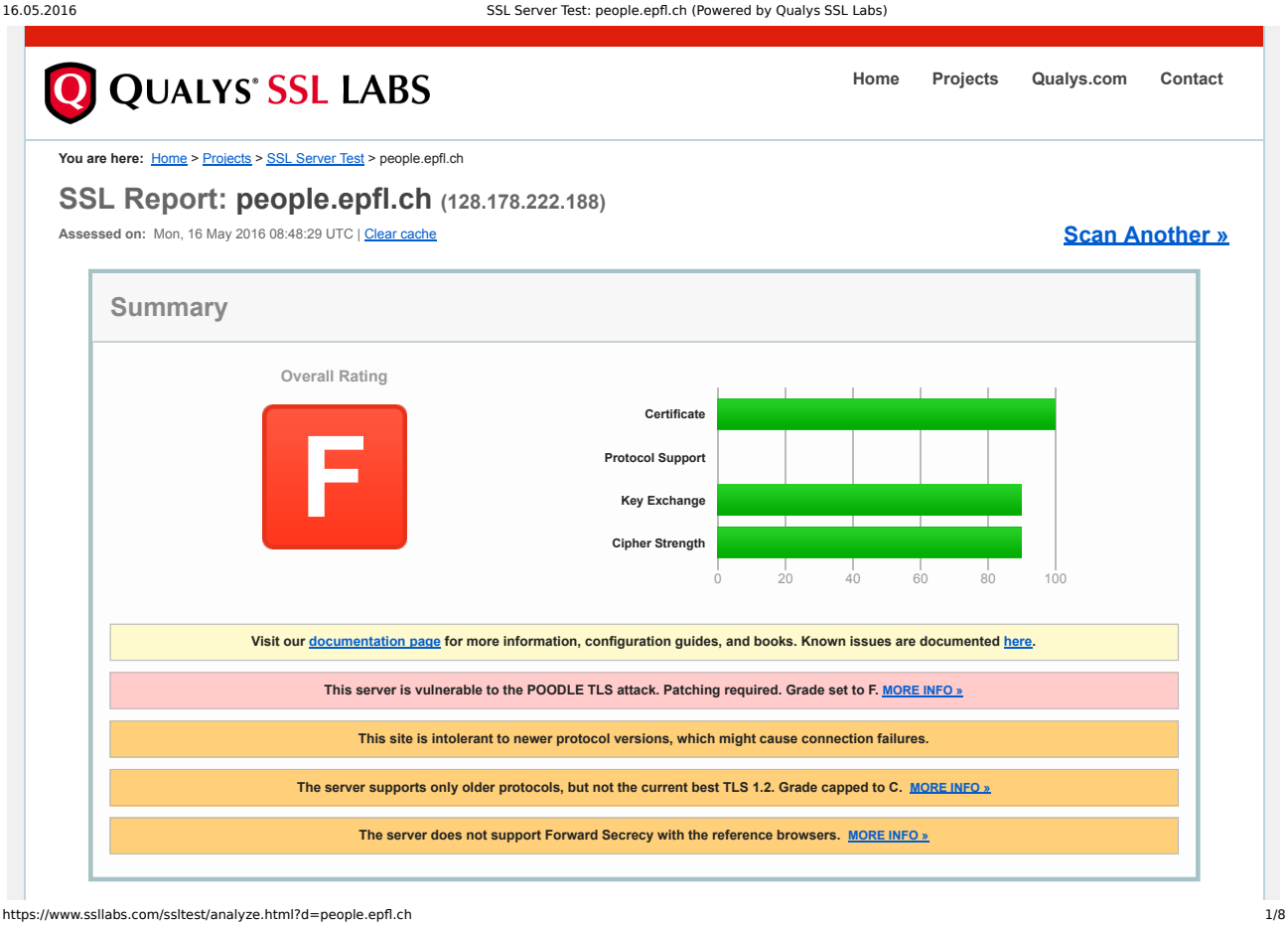

Рис. 2: Отчет SSL Server Test для people.epfl.ch

Этот сервер уязвим к атаке POODLE, не поддерживает Forward Secrecy и поддерживает только старые версии TLS.

4. Выводы

В данной лабораторной работе был использован сервис SSL Server Test от Qualys SSL Labs. Этот сервис выдает достаточно полную информацию о поддержке SSL выбранным сервисом. Кроме того, сервис показывает основные атаки, которые могут быть применены для данного сервиса.

С помощью сервиса было проанализировано два сайта, правильно настроенного и неправильного.