SSL/TLS for sysadmin

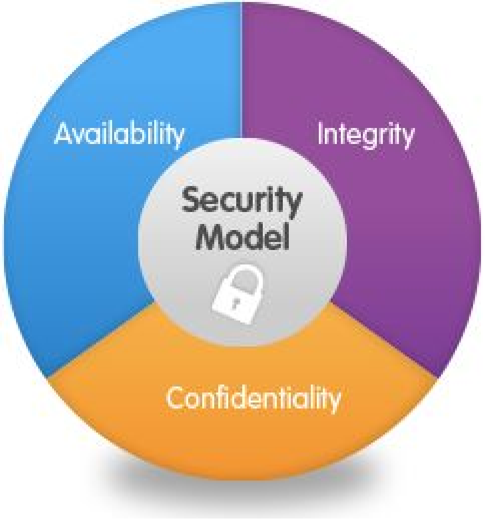
XMPP Hackfest

https://xmpp.hackfest.ca

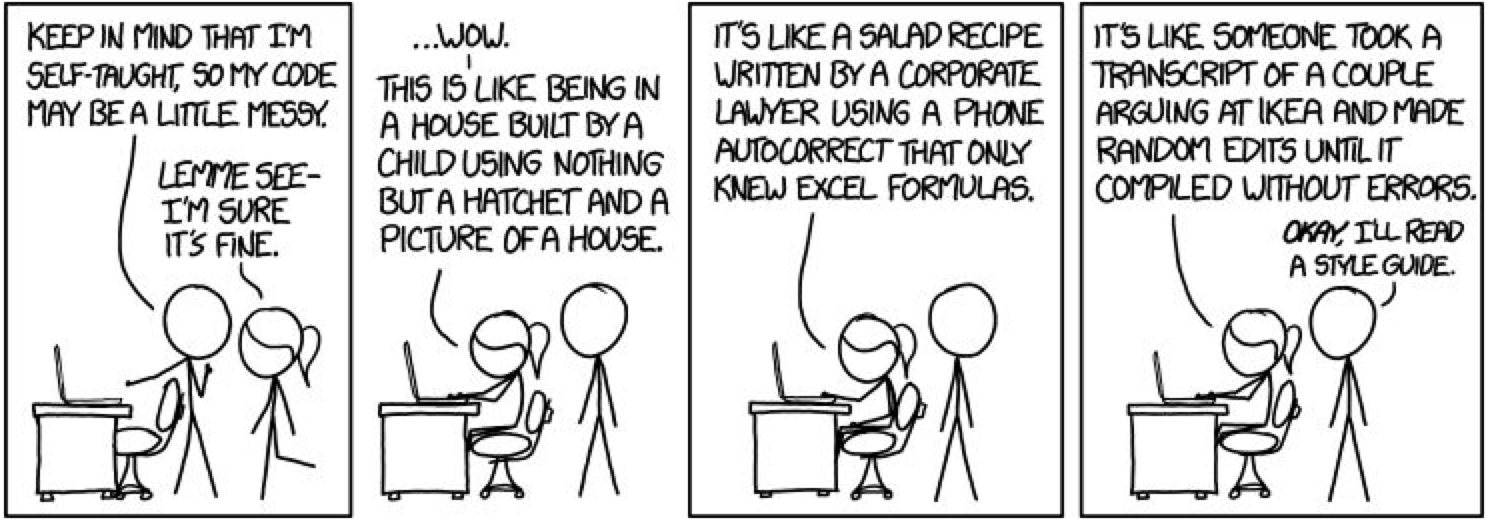
1) connect with browser
2) register
3) Have fun :)

OpenSource : https://github.com/sdelements/lets-chat

What is SSL/TLS?



What is NOT SSL/TLS?


KEEP IN MIND THAT I'M SELF-TAUGHT, SO MY CODE MAY BE A LITTLE MESSY.
LEMME SEE- I'M SURE IT'S FINE.
...WOW.
THIS IS LIKE BEING IN A HOUSE BUILT BY A CHILD USING NOTHING BUT A HATCHET AND A PICTURE OF A HOUSE.
IT'S LIKE A SALAD RECIPE WRITTEN BY A CORPORATE LAWYER USING A PHONE AUTOCORRECT THAT ONLY KNEW EXCEL FORMULAS.
IT'S LIKE SOMEONE TOOK A TRANSCRIPT OF A COUPLE ARGUING AT IKEA AND MADE RANDOM EDITS UNTIL IT COMPILED WITHOUT ERRORS.
OKAY, I'LL READ A STYLE GUIDE.

SSL history

1994: SSL v1.0 Developed by Netscape will stay in draft
February 1995: SSLv2
November 1996: SSLv3
January 1999: TLS 1.0
April 2006: TLS 1.1
August 2008: TLS 1.2
April 2014: Draft of TLS 1.3

March 2011: Prohibiting Secure Sockets Layer (SSL) Version 2.0 RFC6176
April 2015: In PCI 3.1, SSLv2, SSLv3 and TLSv1.0 are not trust has secure protocol
June 2015: Prohibiting Secure Sockets Layer (SSL) Version 3.0 RFC7568

Asymmetric encryption VS symmetric encryption

Asymmetric(Certificate, PGP):

-Private key : sign data, decrypt data

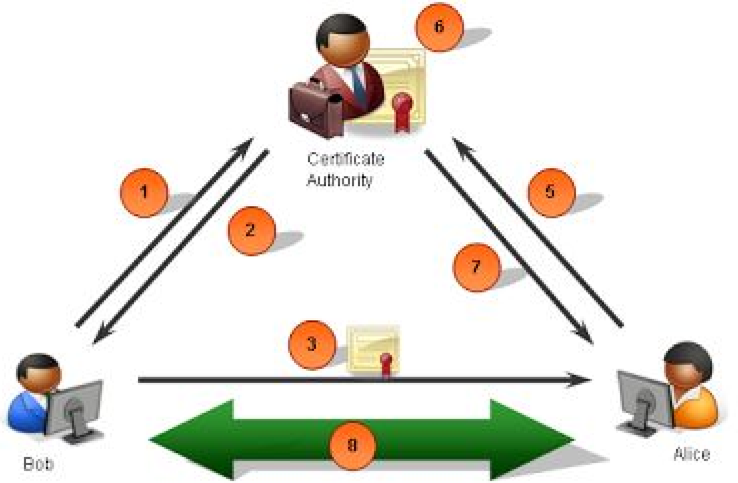
-Public key: encrypt data, verify signature

Symmetric(WPA,ZIP):

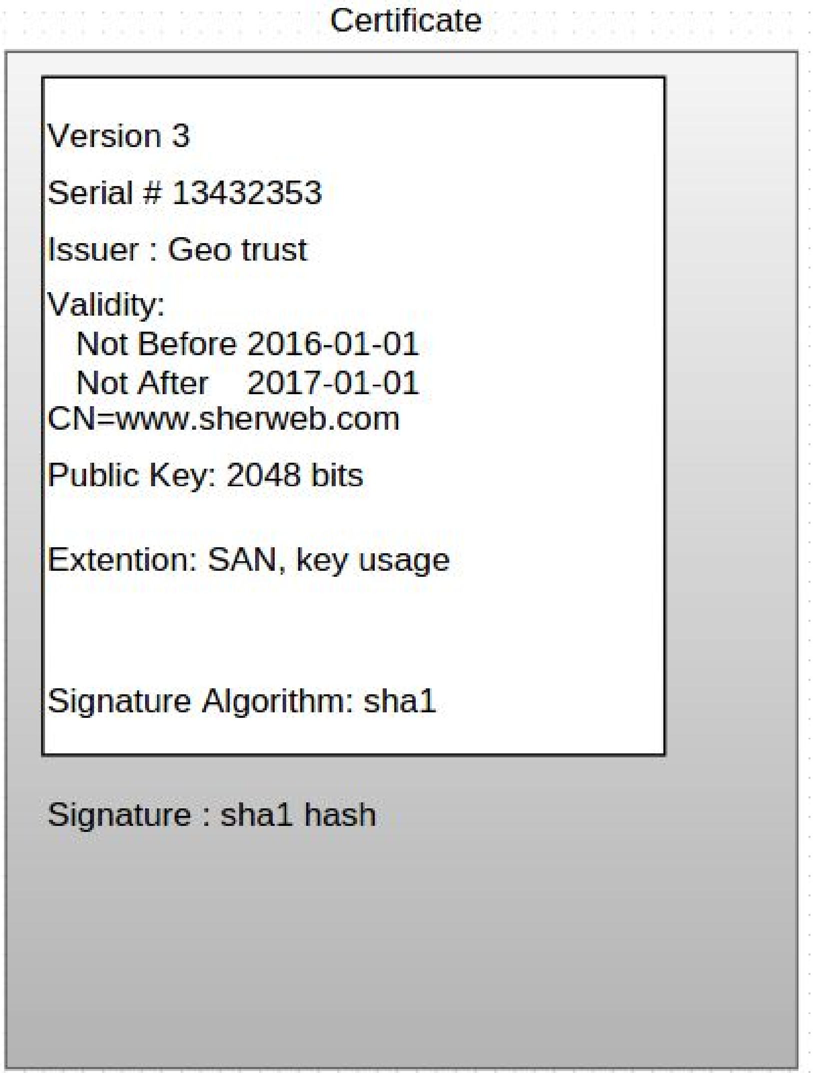
PSK: encrypt data and decrypt data

Why using encryption internally?

PKI infrastructure



1. Bob ask the Certificate Authority to issue a certificate in his name
2. The Certificate Authority validates Bob identity and then issues a certificate to Bob
3. Bob present a certificate containing his identity to Alice
5. Alice ask the Certificate Authority to verify Bob identity
6. The Certificate Authority checks that Bob certificate is valid (has not been altered, has not expired and other checks)
7. The certificate Authority tells Alice that Bob certificate is valid
8. Alice now trusts Bob and she can request the Certificate Authority in case of dispute



Certificate

Version 3

Serial # 13432353

Issuer : Geo trust

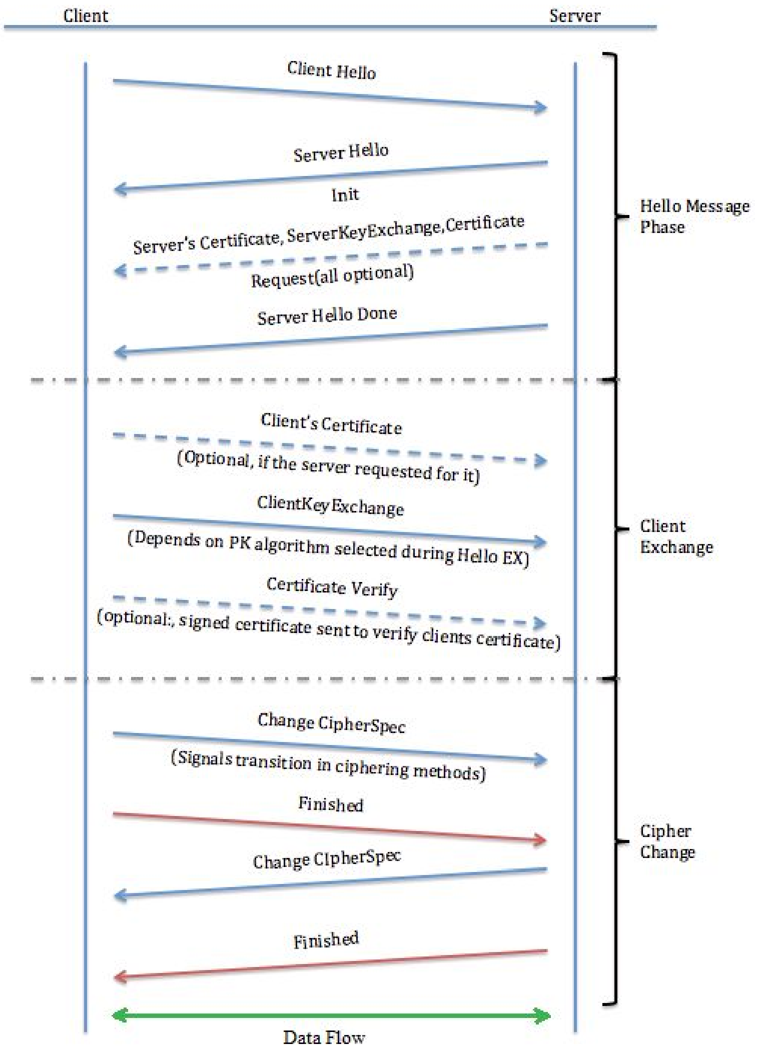
Validity:
   Not Before 2016-01-01
   Not After   2017-01-01
CN=www.sherweb.com

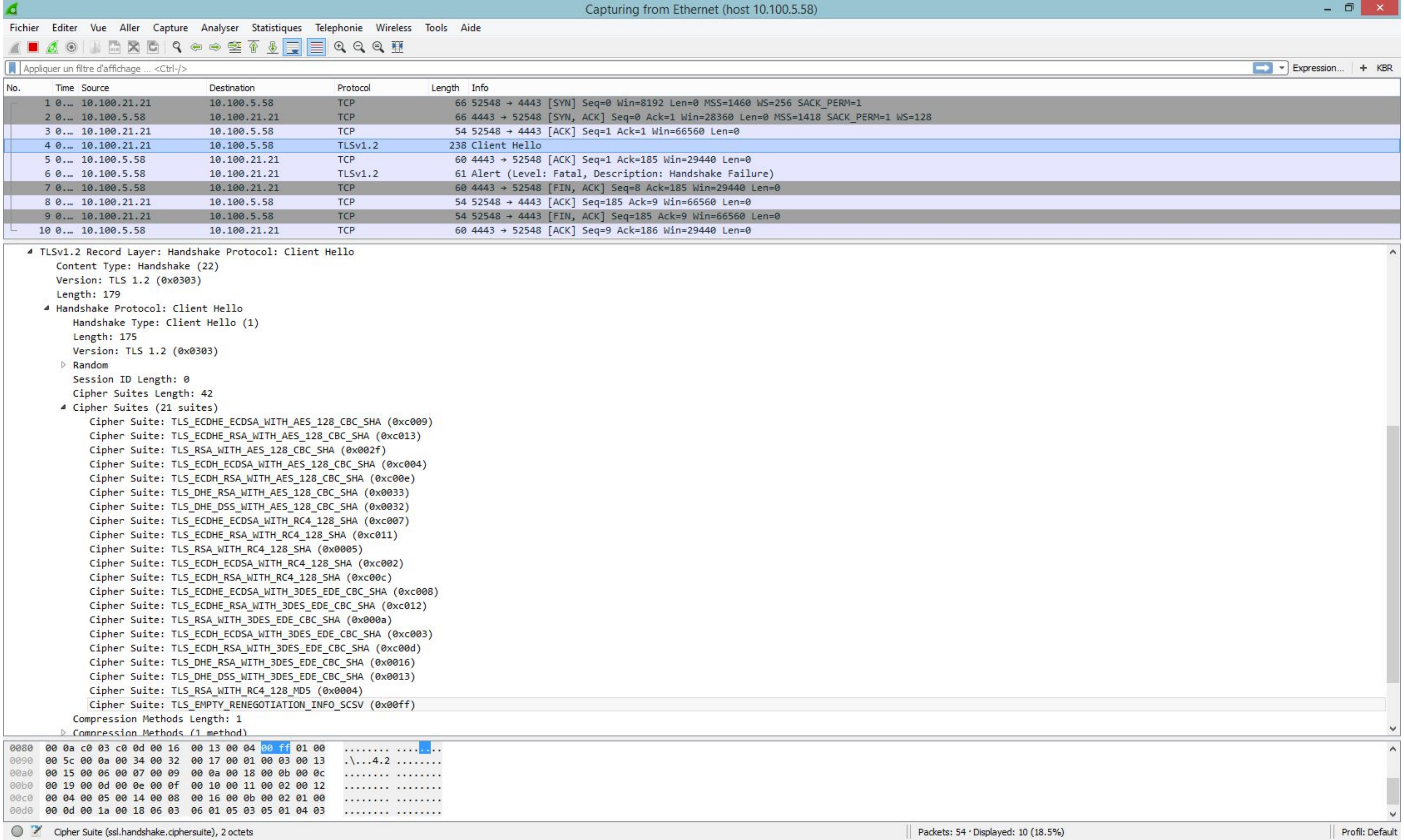
Public Key: 2048 bits

Extention: SAN, key usage

Signature Algorithm: sha1

Signature : sha1 hash


Client
Server
Client Hello
Server Hello
Init
Server's Certificate, ServerKeyExchange,Certificate
Request(all optional)
Server Hello Done
Hello Message Phase
Client's Certificate
(Optional, if the server requested for it)
ClientKeyExchange
(Depends on PK algorithm selected during Hello EX)
Certificate Verify
(optional:, signed certificate sent to verify clients certificate)
Client Exchange
Change CipherSpec
(Signals transition in ciphering methods)
Finished
Change CipherSpec
Finished
Cipher Change
Data Flow



```
No.   Time Source         Destination    Protocol    Length Info
  1 0... 10.100.21.21    10.100.5.58    TCP             66 52548 → 4443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  2 0... 10.100.5.58     10.100.21.21   TCP             66 4443 → 52548 [SYN, ACK] Seq=0 Ack=1 Win=28360 Len=0 MSS=1418 SACK_PERM=1 WS=128
  3 0... 10.100.21.21    10.100.5.58    TCP             54 52548 → 4443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
  4 0... 10.100.21.21    10.100.5.58    TLSv1.2        238 Client Hello
  5 0... 10.100.5.58     10.100.21.21   TCP             60 4443 → 52548 [ACK] Seq=1 Ack=185 Win=29440 Len=0
  6 0... 10.100.5.58     10.100.21.21   TLSv1.2         61 Alert (Level: Fatal, Description: Handshake Failure)
  7 0... 10.100.5.58     10.100.21.21   TCP             60 4443 → 52548 [FIN, ACK] Seq=8 Ack=185 Win=29440 Len=0
  8 0... 10.100.21.21    10.100.5.58    TCP             54 52548 → 4443 [ACK] Seq=185 Ack=9 Win=66560 Len=0
  9 0... 10.100.21.21    10.100.5.58    TCP             54 52548 → 4443 [FIN, ACK] Seq=185 Ack=9 Win=66560 Len=0
 10 0... 10.100.5.58     10.100.21.21   TCP             60 4443 → 52548 [ACK] Seq=9 Ack=186 Win=29440 Len=0
```

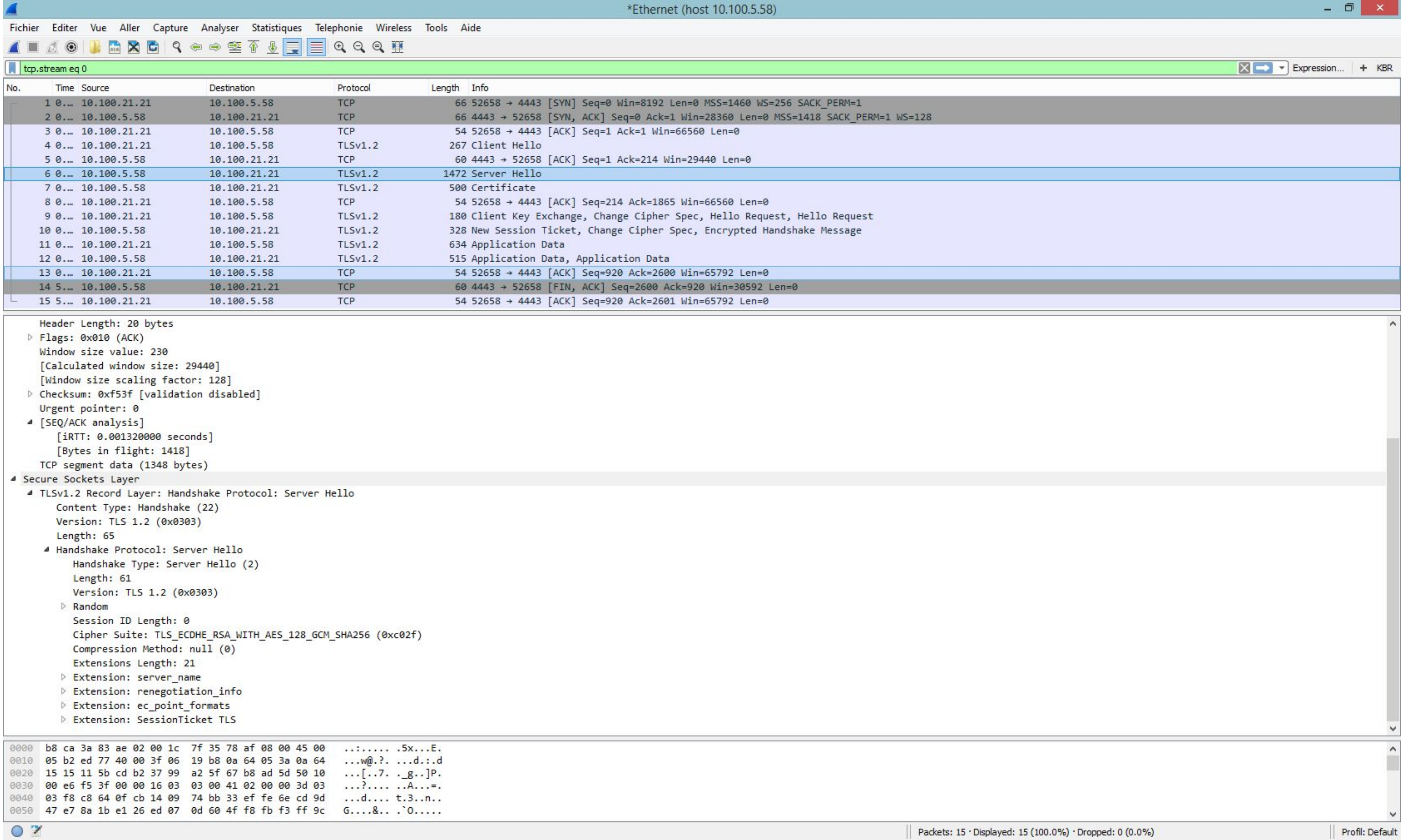
```
◢ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 179
  ◢ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 175
      Version: TLS 1.2 (0x0303)
    ▷ Random
      Session ID Length: 0
      Cipher Suites Length: 42
    ◢ Cipher Suites (21 suites)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
        Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
        Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
        Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
        Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
        Cipher Suite: TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
        Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
        Cipher Suite: TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
        Cipher Suite: TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
        Cipher Suite: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
        Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
        Cipher Suite: TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)
        Cipher Suite: TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
        Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
        Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
        Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
        Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
      Compression Methods Length: 1
    ▷ Compression Methods (1 method)
```

```
0080  00 0a c0 03 c0 0d 00 16  00 13 00 04 00 ff 01 00   ........ ........
0090  00 5c 00 0a 00 34 00 32  00 17 00 01 00 03 00 13   .\...4.2 ........
00a0  00 15 00 06 00 07 00 09  00 0a 00 18 00 0b 00 0c   ........ ........
00b0  00 19 00 0d 00 0e 00 0f  00 10 00 11 00 02 00 12   ........ ........
00c0  00 04 00 05 00 14 00 08  00 16 00 0b 00 02 01 00   ........ ........
00d0  00 0d 00 1a 00 18 06 03  06 01 05 03 05 01 04 03   ........ ........
```

Cipher Suite (ssl.handshake.ciphersuite), 2 octets

Packets: 54 · Displayed: 10 (18.5%)

Profil: Default



tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.…	10.100.21.21	10.100.5.58	TCP	66	52658 → 4443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.…	10.100.5.58	10.100.21.21	TCP	66	4443 → 52658 [SYN, ACK] Seq=0 Ack=1 Win=28360 Len=0 MSS=1418 SACK_PERM=1 WS=128
3	0.…	10.100.21.21	10.100.5.58	TCP	54	52658 → 4443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
4	0.…	10.100.21.21	10.100.5.58	TLSv1.2	267	Client Hello
5	0.…	10.100.5.58	10.100.21.21	TCP	60	4443 → 52658 [ACK] Seq=1 Ack=214 Win=29440 Len=0
6	0.…	10.100.5.58	10.100.21.21	TLSv1.2	1472	Server Hello
7	0.…	10.100.5.58	10.100.21.21	TLSv1.2	500	Certificate
8	0.…	10.100.21.21	10.100.5.58	TCP	54	52658 → 4443 [ACK] Seq=214 Ack=1865 Win=66560 Len=0
9	0.…	10.100.21.21	10.100.5.58	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
10	0.…	10.100.5.58	10.100.21.21	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
11	0.…	10.100.21.21	10.100.5.58	TLSv1.2	634	Application Data
12	0.…	10.100.5.58	10.100.21.21	TLSv1.2	515	Application Data, Application Data
13	0.…	10.100.21.21	10.100.5.58	TCP	54	52658 → 4443 [ACK] Seq=920 Ack=2600 Win=65792 Len=0
14	5.…	10.100.5.58	10.100.21.21	TCP	60	4443 → 52658 [FIN, ACK] Seq=2600 Ack=920 Win=30592 Len=0
15	5.…	10.100.21.21	10.100.5.58	TCP	54	52658 → 4443 [ACK] Seq=920 Ack=2601 Win=65792 Len=0

```
    Header Length: 20 bytes
  ▷ Flags: 0x010 (ACK)
    Window size value: 230
    [Calculated window size: 29440]
    [Window size scaling factor: 128]
  ▷ Checksum: 0xf53f [validation disabled]
    Urgent pointer: 0
  ◢ [SEQ/ACK analysis]
      [iRTT: 0.001320000 seconds]
      [Bytes in flight: 1418]
    TCP segment data (1348 bytes)
◢ Secure Sockets Layer
  ◢ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 65
    ◢ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 61
        Version: TLS 1.2 (0x0303)
      ▷ Random
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Method: null (0)
        Extensions Length: 21
      ▷ Extension: server_name
      ▷ Extension: renegotiation_info
      ▷ Extension: ec_point_formats
      ▷ Extension: SessionTicket TLS
```

```
0000  b8 ca 3a 83 ae 02 00 1c  7f 35 78 af 08 00 45 00   ..:..... .5x...E.
0010  05 b2 ed 77 40 00 3f 06  19 b8 0a 64 05 3a 0a 64   ...w@.?. ...d.:.d
0020  15 15 11 5b cd b2 37 99  a2 5f 67 b8 ad 5d 50 10   ...[..7. ._g..]P.
0030  00 e6 f5 3f 00 00 16 03  03 00 41 02 00 00 3d 03   ...?.... ..A...=.
0040  03 f8 c8 64 0f cb 14 09  74 bb 33 ef fe 6e cd 9d   ...d.... t.3..n..
0050  47 e7 8a 1b e1 26 ed 07  0d 60 4f f8 fb f3 ff 9c   G....&.. .`O.....
```

Packets: 15 · Displayed: 15 (100.0%) · Dropped: 0 (0.0%)

Profil: Default

FILE ??

Encodings

-PEM : Privacy Enhanced Mail (Base64 ------ BEGIN XXXX --------)

-DER : Distinguished Encoding Rules (Binary)

Common Extensions

.crt, .cer, .csr, .key

Container

-PKCS#7: contain only Certificates & Chain certificates (.p7b, .p7c)

-PKCS#12: storing the Server certificate, any Intermediate certificates & Private key in one encryptable file (.pfx, .p12)

Vulnerability

Protocole

sslv2

sslv3

TLS 1.0

-CRIME: Compression Ratio Info-leak Made Easy

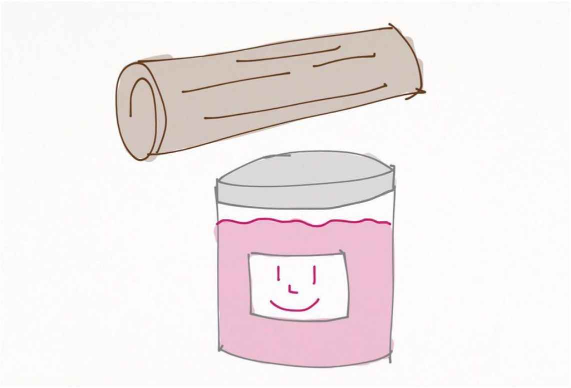
-

Implementation

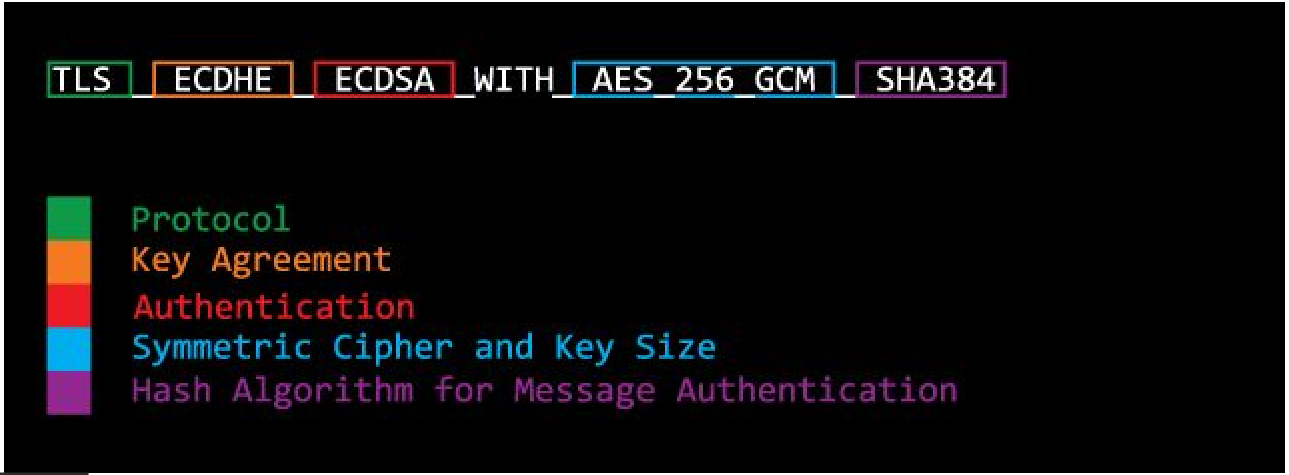
-Certificate Validation Flaw (François Gagnon Android)

-CVE-2016-0701(OpenSSL weak key)

-MS04-011 Microsoft Private Communications Transport Overflow (Remote code execution)

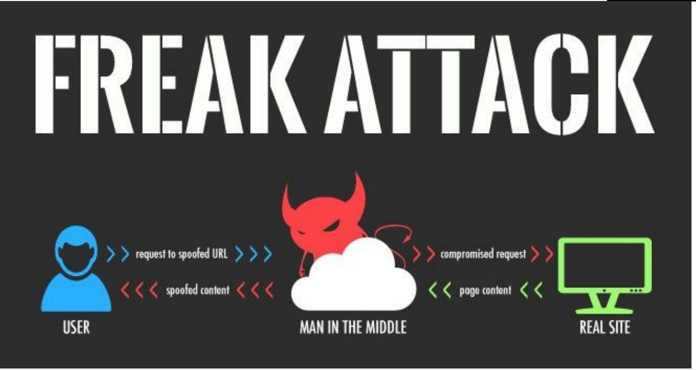


Cipher strength



TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

🟩 Protocol
🟧 Key Agreement
🟥 Authentication
🟦 Symmetric Cipher and Key Size
🟪 Hash Algorithm for Message Authentication



What to look at ?

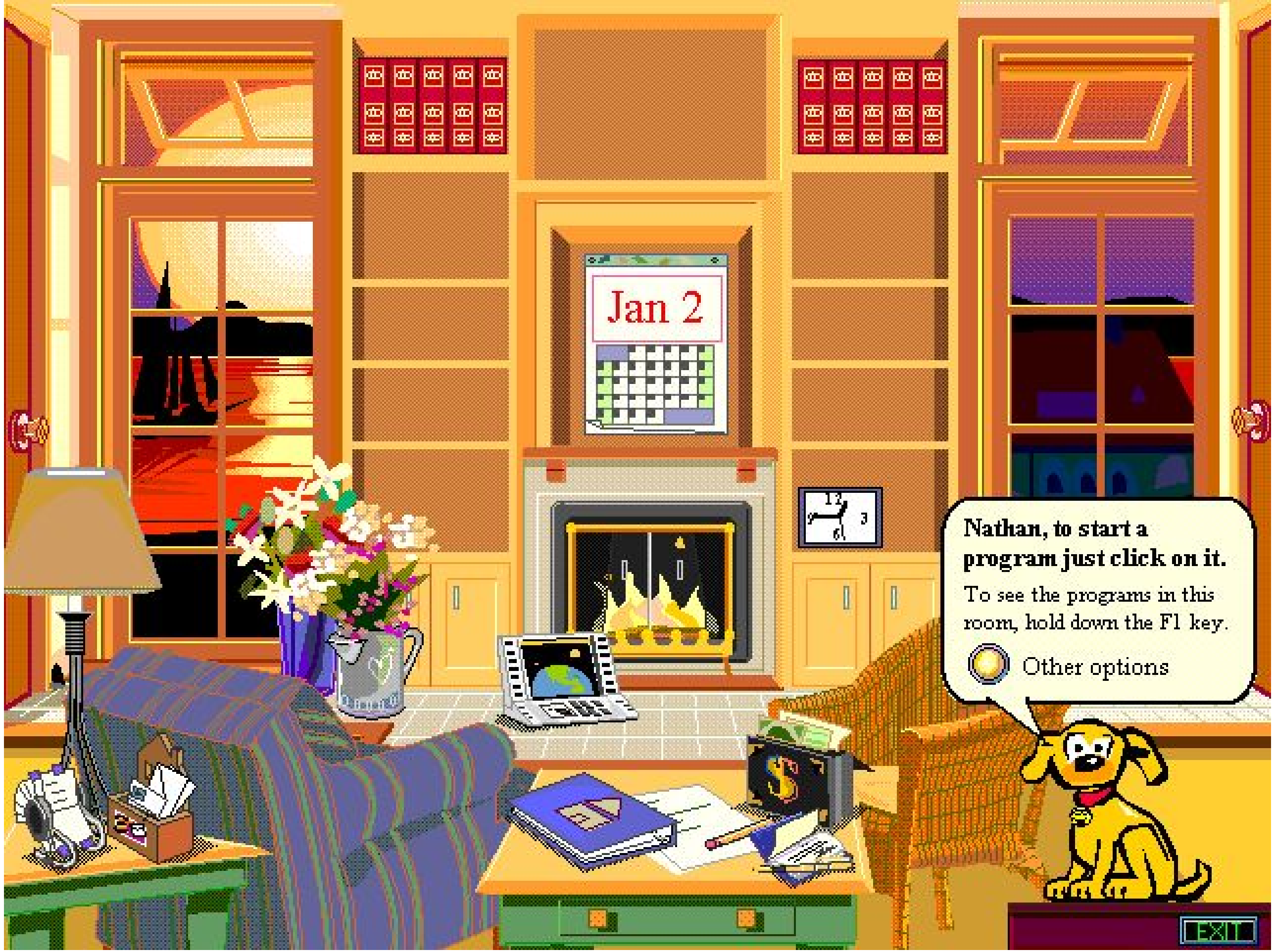
Protocole : GOOD: TLSv1.1, TLSv1.2 BAD: SSLv2, SSLv3, TLS 1.0

Cipher: RC4, MD5, 3DES

Patch: Openssl, microsoft, apache …..

key size : 2048 or 4096

Hash method: Sha256



Nathan, to start a program just click on it.

To see the programs in this room, hold down the F1 key.

Firefox 1, Chrome 1, IE 7, Opera 5 and Safari 1

Tools

Online

https://www.ssllabs.com/ (Check SSL server implementation)

https://badssl.com/ (Example of BAD implementation)

https://secure.comodo.net/utilities/decodeCSR.html (Decode CSR)

https://www.digicert.com/csr-creation.htm (CSR cli generator)

good doc :

https://wiki.mozilla.org/Security/Server_Side_TLS

Check supported protocol and ciphers

nmap --script=ssl-enum-ciphers www.sherweb.com -p 443

https://testssl.sh/ (linux)

SSLYZE (linux)

Security@git: get-TLSVersion.py

openssl s_client -connect xmpp.hackfest.ca [-tls1/tls1_1/tls1_2/-ssl3/-ssl2]
(check openssl for sslv2 compilation)

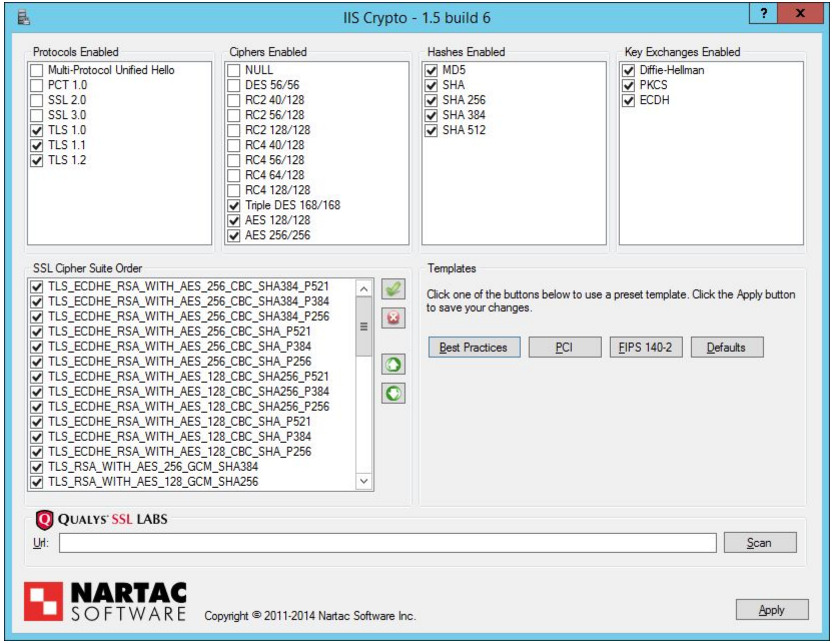
Certificate Grabing

```
nmap --script=ssl-cert www.google.ca -p 443 -vv
```

Security@git : get-certificate.py

Configure Windows

https://www.nartac.com/Products/IISCrypto



IIS Crypto - 1.5 build 6

Protocols Enabled

- ☐ Multi-Protocol Unified Hello
- ☐ PCT 1.0
- ☐ SSL 2.0
- ☐ SSL 3.0
- ☑ TLS 1.0
- ☑ TLS 1.1
- ☑ TLS 1.2

Ciphers Enabled

- ☐ NULL
- ☐ DES 56/56
- ☐ RC2 40/128
- ☐ RC2 56/128
- ☐ RC2 128/128
- ☐ RC4 40/128
- ☐ RC4 56/128
- ☐ RC4 64/128
- ☐ RC4 128/128
- ☑ Triple DES 168/168
- ☑ AES 128/128
- ☑ AES 256/256

Hashes Enabled

- ☑ MD5
- ☑ SHA
- ☑ SHA 256
- ☑ SHA 384
- ☑ SHA 512

Key Exchanges Enabled

- ☑ Diffie-Hellman
- ☑ PKCS
- ☑ ECDH

SSL Cipher Suite Order

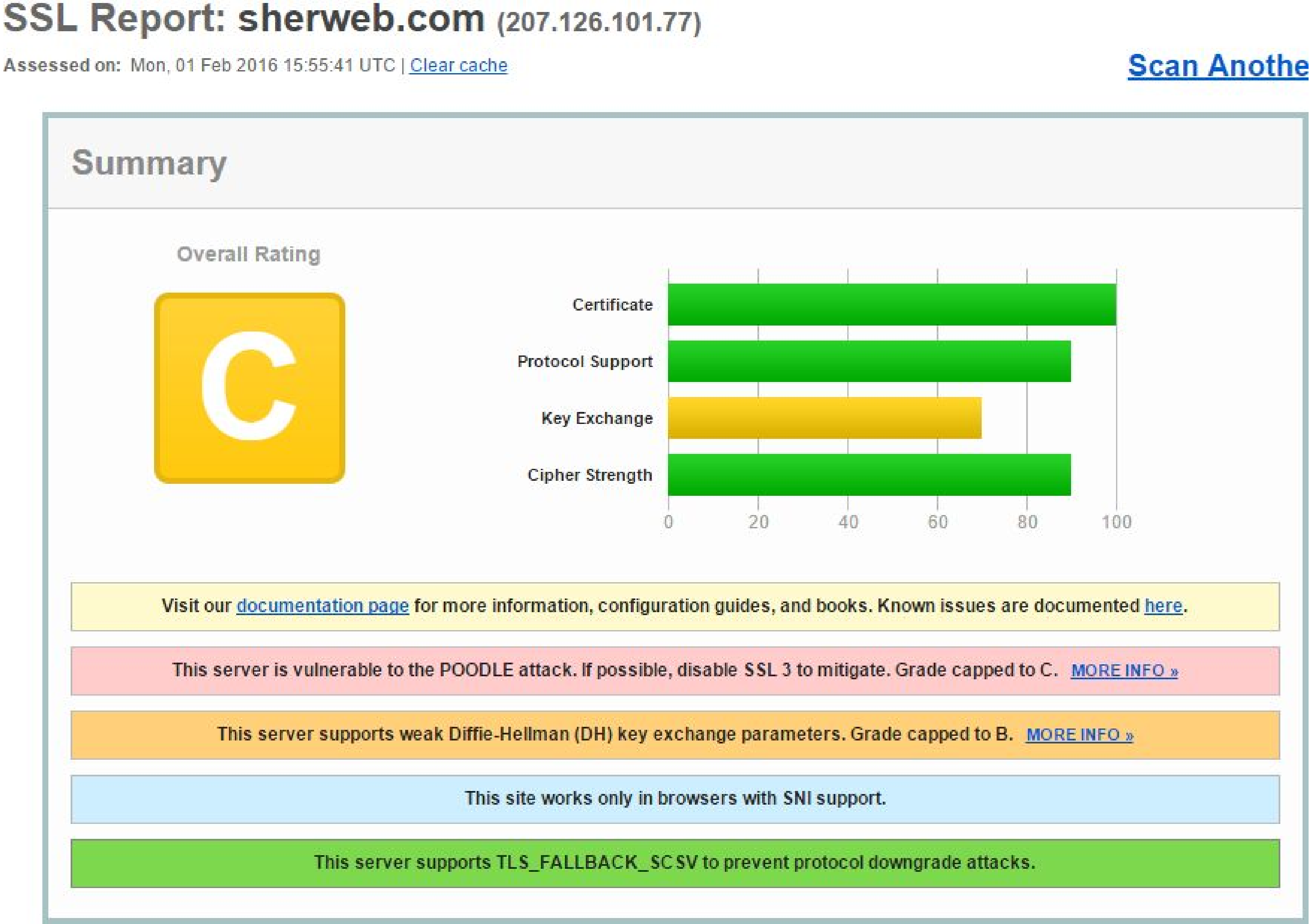
- ☑ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521
- ☑ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
- ☑ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
- ☑ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521
- ☑ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
- ☑ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
- ☑ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521
- ☑ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
- ☑ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
- ☑ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521
- ☑ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
- ☑ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
- ☑ TLS_RSA_WITH_AES_256_GCM_SHA384
- ☑ TLS_RSA_WITH_AES_128_GCM_SHA256

Templates

Click one of the buttons below to use a preset template. Click the Apply button to save your changes.

Copyright © 2011-2014 Nartac Software Inc.

Example Sherweb



SSL Report: sherweb.com (207.126.101.77)

Assessed on: Mon, 01 Feb 2016 15:55:41 UTC | Clear cache

Scan Anothe

Summary

Overall Rating

C

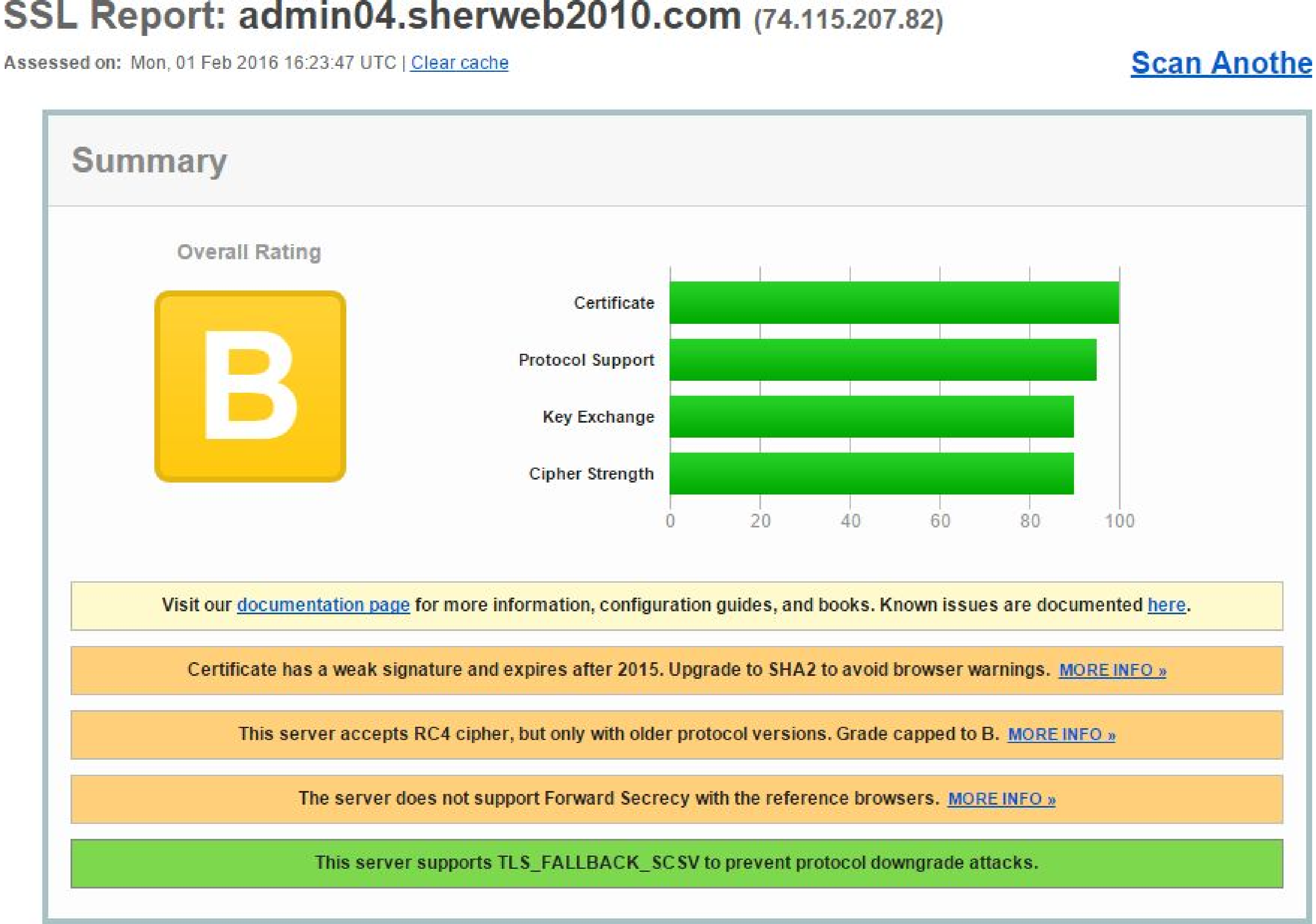
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

This site works only in browsers with SNI support.

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.



SSL Report: admin04.sherweb2010.com (74.115.207.82)

Assessed on: Mon, 01 Feb 2016 16:23:47 UTC | Clear cache

Scan Anothe

Summary

Overall Rating

B

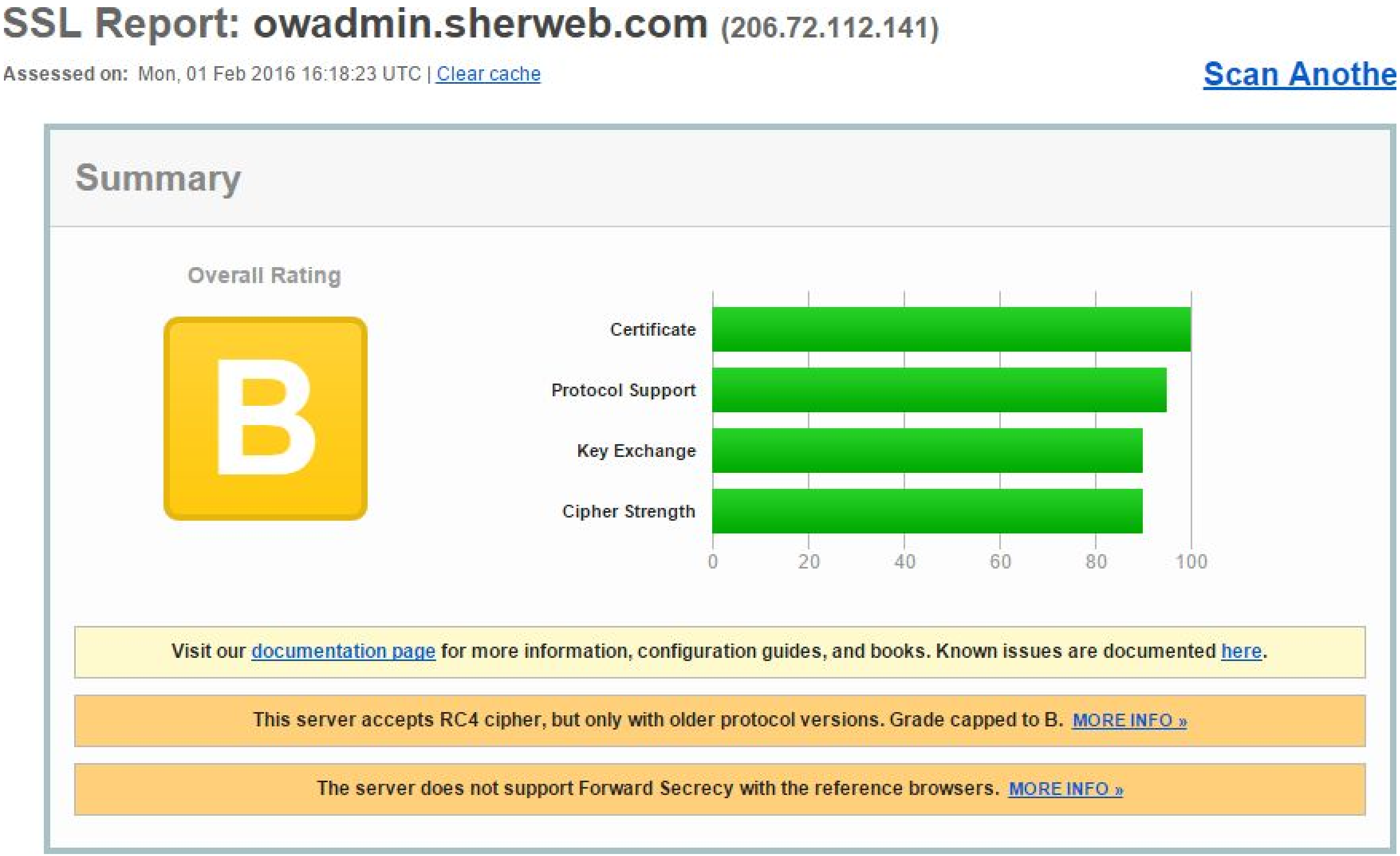
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Certificate has a weak signature and expires after 2015. Upgrade to SHA2 to avoid browser warnings. MORE INFO »

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.



SSL Report: owadmin.sherweb.com (206.72.112.141)

Assessed on: Mon, 01 Feb 2016 16:18:23 UTC | Clear cache

Scan Anothe

Summary

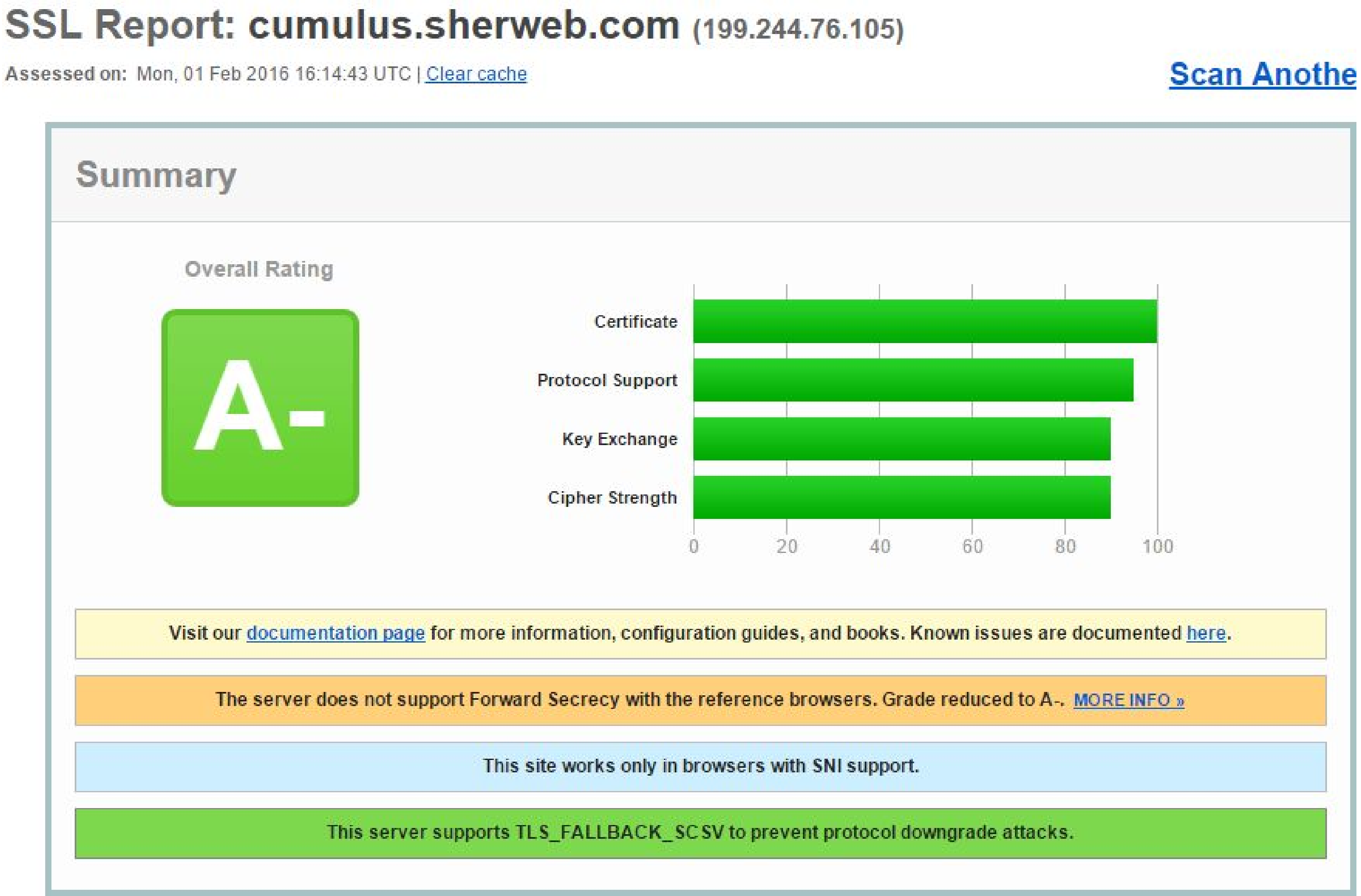
Overall Rating

B

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »



SSL Report: cumulus.sherweb.com (199.244.76.105)

Assessed on: Mon, 01 Feb 2016 16:14:43 UTC | Clear cache

Summary

Overall Rating

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

The server does not support Forward Secrecy with the reference browsers. Grade reduced to A-. MORE INFO »

This site works only in browsers with SNI support.

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

And what’s next ?

Applicatif

-HTTP Strict Transport Security

-Certificate and Public Key Pinning

-Secure flags coockie

Audit

-Audit your configuration for any change(Bad change)

-Monitor Certificate expiration date

Keep updated

-to day security is not tomorrow security!