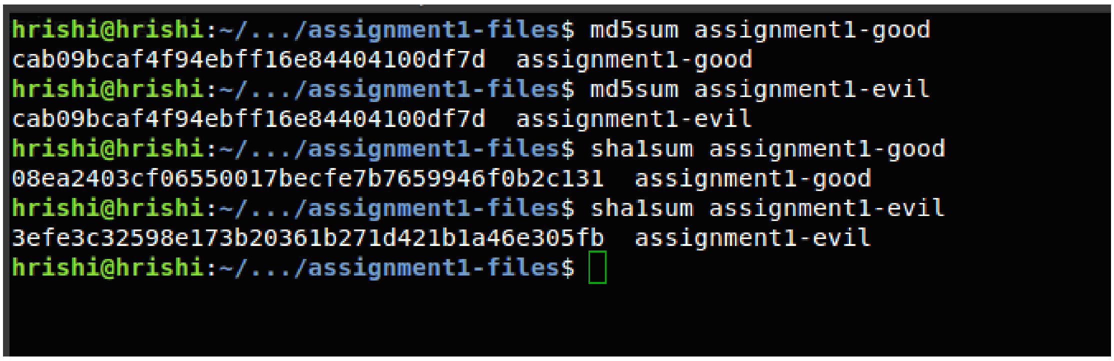
Assignment 1: Question 4:

Hashes for the two files assignment1-evil and assignment1-good are computed and given below :

1. The hashes computed :



```
hrishi@hrishi:~/.../assignment1-files$ md5sum assignment1-good
cab09bcaf4f94ebff16e84404100df7d  assignment1-good
hrishi@hrishi:~/.../assignment1-files$ md5sum assignment1-evil
cab09bcaf4f94ebff16e84404100df7d  assignment1-evil
hrishi@hrishi:~/.../assignment1-files$ sha1sum assignment1-good
08ea2403cf06550017becfe7b7659946f0b2c131  assignment1-good
hrishi@hrishi:~/.../assignment1-files$ sha1sum assignment1-evil
3efe3c32598e173b20361b271d421b1a46e305fb  assignment1-evil
hrishi@hrishi:~/.../assignment1-files$ 
```

2.

a) Md5sum values for both the files are same indicating that they are equal and contain the same data. Comparing hash values is a short cut technique that's usually employed to compare equality of two give files.

b) The sha1sum suggests that the given files here are different.

c) Comparing the hash output of the two files and from referring to the previous two answers we can safely conclude that the md5sum function is wrong and the sha1sum is right. Its long known that the md5sum hash is broken and vulnerable and from running two programs, it is also pretty evident that the programs contain different content. Hence md5sum fails to detect this difference and outputs the two files as the same. However sha1sum shows these two files as different and hence we conclude that md5sum computed here is wrong.

d) The security property that is being violated here is collision resistance.

e) An example may help demonstrate why collision resistance is important.

Hash algorithms are often used for computing digital signatures. The signer of a message runs the original message through a hash algorithm to produce a digest value, then encrypts the digest to produce a signature. Someone verifying the signature will run the message through the same hash algorithm, and will decrypt the attached signature value to ensure the digest it contains matches the one they computed

If collisions are easy to find, they allow an attacker to take an authentic digitally signed message, find a different message that produces the same digest (the collision), then substitute the fake message for the real one while keeping the same signature value. Someone trying to validate the signature won’t be able to tell the difference. This destroys the value of digital signatures.

f) A rough rule of thumb for collisions is the square-root of the range of values. The MD5sum hash is presumably 128 bits long, so you're going to be likely to see collisions above and beyond 2^64 images.

g) There are faster ways to computer md5sum collisions and I am speculating that Prof.Essex must have used such a technique. The best MD5 collision finder is Marc Stevens fastcoll. It can typically find collisions in a couple of seconds using a a variant of the Wang attack. I am sure Prof.Essex has used the above mentioned technique to generate the collisions.

Assignment 2, Question 3:

a) Using Google Chrome, navigate to the website click the green padlock in the URL bar, then click on the Connection tab. Then answer the following questions:

   i. The encryption bit level that the connection is at is 256 bit

   ii. The key exchange mechanism is a strong key exchange mechanism using ECDHE_RSA with P-256

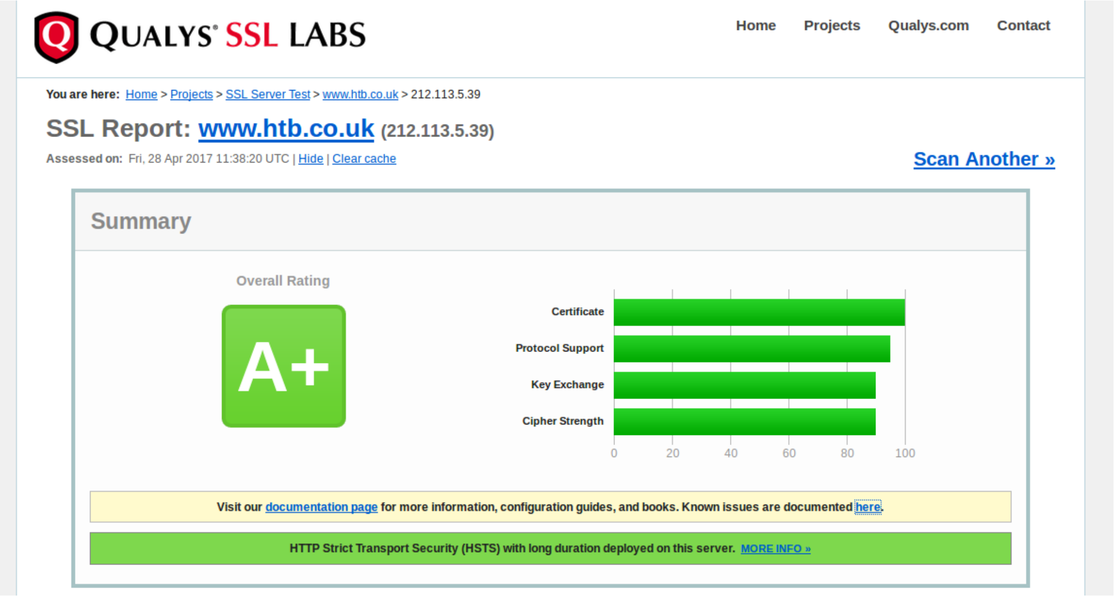
   iii. Digital Certificate mechanism – PKCS #1 SHA-256 With RSA Encryption

   iv. The symmetric key mechanism is AES_256_GCM. It is AES 256 and is used in the Galois Counter Mode operation

   v. The authentication mechanism is using a strong protocol - TLS 1.2

b) Qualsys SSL Server Test:

   i. SSL report for the IP 212.113.5.39:



You are here: Home > Projects > SSL Server Test > www.htb.co.uk > 212.113.5.39

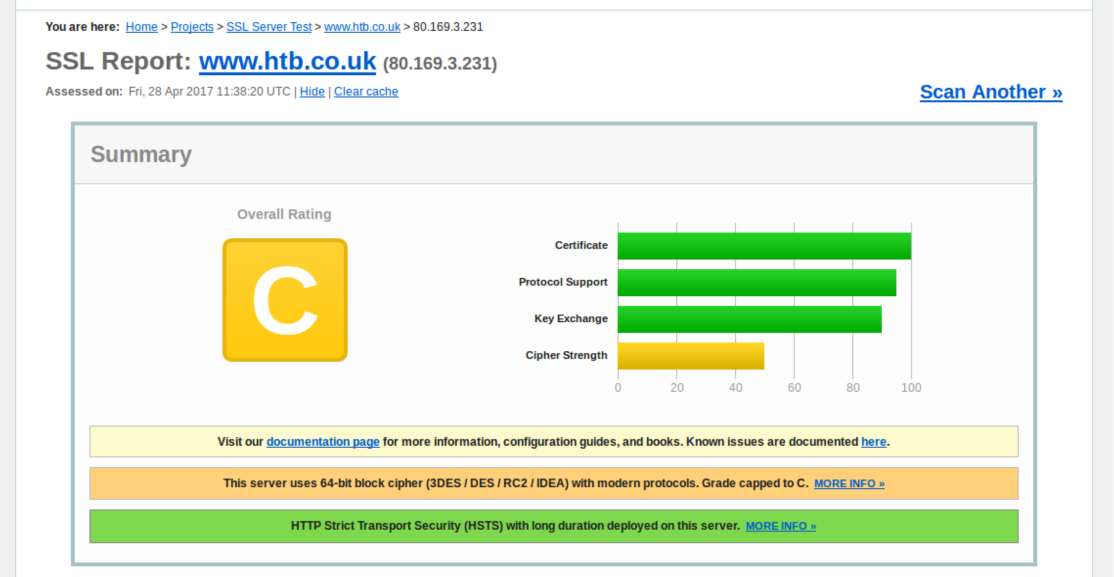
SSL Report: www.htb.co.uk (212.113.5.39)

Assessed on: Fri, 28 Apr 2017 11:38:20 UTC | Hide | Clear cache

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

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

SSL report for the IP 80.169.3.121:



You are here: Home > Projects > SSL Server Test > www.htb.co.uk > 80.169.3.231

SSL Report: www.htb.co.uk (80.169.3.231)

Assessed on: Fri, 28 Apr 2017 11:38:20 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

C

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

This server uses 64-bit block cipher (3DES / DES / RC2 / IDEA) with modern protocols. Grade capped to C. MORE INFO »

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

In the first IP test SSL report is an A+ whereas in the second it's a C. In the second the server uses 64-bit block cipher (3DES / DES / RC2 / IDEA) with modern protocols. Hence the Grade capped to C. Such block ciphers are prone to birthday attacks and hence vulnerable.

ii. The versions of TLS supported are 1.2, 1.1 and 1.0. SSL version 3 and 2 are not supported by the website

iii. The most preferred cipher suite by the website is TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

c) The TLS cipher suite I choose would be TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. This cipher suite uses TLS 1.2 most advanced version of the encryption protocol. It uses elliptic curve diffie-hellman key exchange which is significantly faster than Diffie - Hellman exchange and establishes secure communication channel. It uses a combination of RSA and AES 256 in GCM mode for secure key exchange and communication. For the hash algorithm it uses SHA384 which is one of the most advanced and secure hashing algorithms. The cipher suite test further more shows that it is graded A+ and is very secure.