Part 1:

1. Go to the website

Output: It works!

Download the netsec root certificate :

1: What is the reason or security warning ?

Ans: Someone is trying to impersonate this website, so don’t continue. Certificate issuer is unknown – The certificate is self signed – server sin’t sending the correct certificates.

1. Who is the issuer of the certificate

Ans. Issuer of ceritificate: NetSec CA

1. To whom is the certificate issued: Chalmers with CN NetSec
2. Why is there no security warning any more? Explain using the following terms: web browser, root certificate, web server certificate, signature, verification : Because we added the certificate
3. What is the reason connection failed: failed to verify 1st certificate

COMMAND: openssl s\_client -connect localhost:443 -tls1\_2

s\_client : test SSL/TLS connections, -connect : to define the host and port to connect to, -

tls1\_2 : tls version 1.2

We get Verificatioon code 12

1. Command: openssl s\_client -tls1\_2 -connect theoden.se.chalmers.se:443 -CAfile <netsec.pem file from the website>

**-CAfile file**

A file containing trusted certificates to use during server authentication and to use when attempting to build the client certificate chain.

We uploaded the certificate and the corresponding website. This solved the issue.

1. Algorithm used for key exchange: Diffie hellman

Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) is a key exchange algorithm that allows two parties to establish a shared secret over an insecure communication channel. It is a variant of the Diffie-Hellman key exchange that uses elliptic curve cryptography to provide stronger security with smaller key sizes.

The “ephemeral” part of the name refers to the fact that the key used in the key exchange is only used once and then discarded. This provides forward secrecy, which means that if an attacker were to compromise the private key of one party later, they would not be able to use it to decrypt past communications.

RSA (Rivest–Shamir–Adleman): A widely used public-key encryption algorithm, used in this case for server authentication.

AES256 (Advanced Encryption Standard with a 256-bit key): A symmetric block cipher that uses a 256-bit key size to provide strong encryption of data.

GCM: Block cipher –

AES and GSM is used for key exchange

Authentication of server : RSA

1. RSA isn’t popularly used, why?

RSA is a relatively slow algorithm and needs more computation resources compared to

symmetric encryption algorithms such as AES. Because of this, it is not commonly used to directly encrypt user data.

Type the big command in a new terminal: Wireshark will start sniffing packets –

There is 3 way handshake happening, then they will exchange key and cipher. Then send encrypted handshake message . Then data is sent.

1. Don’t know – Verification code 10 : Certificate has expired.
2. Yes, message sent successfully – As we get ACK packet in return. Technically this wasn’t supposed to happen because the certificate had expired. But the message was transmitted. However, there’s no guarantee that someone wasn’t eavesdropping.

Step 1: TCP Handshake

Step 2: Client Hello – TLS version, ciphers etc are exchanged. Server sends ACK.

Step 3: Server Hello – Random number, cipher and TLS version is exchanged. Along with certificates. Server hello is done . Client sends ACK.

Step 3: Client Key exchange – Server decrypts the pre-master secret and then finds out the master secret with the random secret. Then it sends it. This means authentication is done. All messages from now on are authenticated. Then ACK is sent and then Application Data is exchanged.

1. In client Hello message 🡪 TLS V1.2 🡪 Handshake Protocol 🡪 Cipher Suites
2. Server Hello shows which cipher is shown -- Why is it selected? --- Same as before
3. Application data
4. Making a private key public means anyone can access the encrypted data / session – loss of confidentiality, security breach.
5. CA’s certificate is shared publically so that users can verify that the certificate is issued by a trusted CA
6. A. TLS Version – whether it’s the same or not

B. Checks the certificate, if it is valid, expired, is the CA is trusted etc

C. Hostname in the URL matches the Common Name

Client sends hello with random number,version cipher etc

Server responds with info and creates a pre-master secret

This is used to create master secret key

Then they create session keys

2 pairs of 4 keys :

Q18: There is a difference in the signed and unsigned stuff

Q19:

1. It implies that the CA was issued by a trusted CA and and the information contained in the CA is verified
2. No we cannot trust this server.

Q20: Differences: We can now see tls1.3.

Q21:

Client hello

TLS 1.2 --🡪 After server hello, there is encrypted handshake message. After that, there is encrypted alert --- this has 2 way handshake which is slower and may cause delays

TLS1.3 🡪 During server hello, change cipher spec, and Application Data : (maybe encrypted message?)

Here we have 1 way handshake which is faster , same session key

Q22: