Oppgave 1

Generelt:

Hva er informasjonssikkerhet:

- CIA:
    - CIA er forkortelse for «Konfidensielt (Confidentiality), Integritet (Integrity), Tilgjengelighet (Availability).
    - Vi oppnår konfidensielt ved å omforme data for å gjøre de sikre ved hjelp av kryptografi. Vi sjekker for tilgangskontroll. Videre er det nødvendig med autentisitet for å sikre tilgang for kilder av rett person med de nødvendige tilgang tillatelser. Dette kan vi videre oppnå ved hjelp av «To fase autentisitet» (IMSI).
    - Integritet handler om å unnvike uautoriserte endringer av data samtidig å ha data sikret i en «back up». Man kan også gjøre krypteringer med «Checksum» for å sjekke integritet i de innkommende data.
    - Tilgjengelighet betyr å ha data tilgengelige for autorisert person til rett tid.
    - Data sikkerhet er nedfelt i EU lov om GDPR i 2018 der de som oppbevarer personalopplysninger må sikre tilgang til slike data, inklusive IP adresser.
    - CIA er viktig i forhold til «phising», «malware», «network sniffing», «ARP spoofing», «port scanning», «session hijacking», «DOS Attack», «SQL Injection», «XS Scripting».

Oppgave 2

Konto hijacking og identitetstyveri:

Innbrudd/hijacking av din private epost innebærer et betydelig personlig angrep og brudd på lov om GDPR. Det kan medføre at angriper skaffer seg tilgang til dine data, dine kontakter, din informasjon, dine oppfattinger og meninger.

Vi kan bli utsatt for overvåkning av våre data og web søk der selskaper prøver å påvirke våre oppfattinger, våre vaner, våre meninger og vår adferd. Noen steder fins det «social credit score» der innbyggene er utsatt for overvåkning av hva de har sakt, hva de har skrevet, hva de har gjort og hvor de har vært. Dette påvirker individets rettigheter og muligheter i samfunnet.

- Største trusler:
    - De største trusler i dag er tyveri av identitet, personopplysninger, passord og annet informasjon av personlig karakter slik som bank informasjon og helseopplysninger.

- Mottiltak mot angrep på e-post konto:
    - Vår data sikkerhet kan økes ved hjelp av: «A.A.A.»:
        - Ved autorisasjon som er ikke kompromittert.
        - Opprettholdelse av regler, tillatelser og sikkerhets mekanismer
        - Anonymitet, Proxy server, pseudonymer, oppdatering av programvare, VPN samt andre makansismer som holder vår identitet skult.

    - Videre: «A.C.L.»:
        - Ved hjelp aksess kontroll av bruker gjennom autorisasjon, passord, filbeskyttelse og rolle hierarki som bestemmer tilgangsrettigheter.

    - Videre: «Kryptografi»:
        - Vi sikrer våre kommunikasjoner over sikrede kanaler slik som HTTPS, AES, RSA, Diffie-Hellman, EFS, Public Key Cryptatation, Block Chiffer, Tunneling og likende.

Problemstillinger i forbindelse med identitetstyveri:

- Mine penger kan bli stålet.
- Noen kan kjøpe på min bekostning.
- Noen kan utføre ulovlige handlinger i mitt navn.
- Noen kan legge ut mine private bilder på sosiale medier.
- Noen kan bruke min identitet som basis for spredning av falske nyheter hvis jeg skulle ha en viktig posisjon i samfunnet.
- Generelt misbruke informasjon om meg.

Tyveri av BankID, inklusive tilgang din personlige kode og din kodebrikke:

I dag har alle banker en «to-stegs» sikring av data og tilgang til din personlige konto i banken. Dette for å beskytte banken for uautorisert tilgang til dine data, midler og han/hennes innstilinger. Det gir bruker sikring for at data ikke skal komme i hende på feil person. Bankene insitere på at kodebrikke og personlige kode holdes separat og at personlige kode memoreres og ikke skrives ned.

Skulle din personlige kode og kode brikke komme uvedkommende hende vil tilgang til din bank konto være helt åpen. Du kan miste alle pengen din og du kan skade banken ved overtrekk. Hvis du har vist uaktsomhet ved brudd på kontoavtale kan du holdes ansvarlig. Ved innbrudd, med akseptabel sikring av data kan du få erstatning enten av banken eller forsikringsselskapet jfr. dine poliser.

Oppgave 3

Skadevare:

Det fins mange typer skadevare (Malicious Software). Alle er basert på å skrive uautorisert kode inn i et data program og lage uautoriserte kommandoer.

- Spredning:
  - Et virus kan spres til alle filer. De må ha andre filer hvor de kan gjemme seg.
  - En orm (Worm) kan spre fra maskin til maskin.
- Skjuling:
  - Skadevare kan gjemme seg i rootkit og endre på OS (Operating System).
- Nyttelast:
  - Skadevare kan stjele datakraft og informasjon slik som ID og liknende.

Skadevaren: «ILOVEYOU»:

Denne orm-varianten er kjent for spredning gjennom e-post. 50 millioner PCer ble infisert i løpet av 9 dager. [1]

E-posten inneholdt en lenke. Denne lenken innholdet skadevare som ble laste inn i programmet. Deretter ble tilsvarende melding send til alle kontaktene på data maskinen.

Skadevaren: «Stuxnet»:

Denne skadevaren er en av de mest avanserte skadevarer som er kjent med 20 lag av ormer og viruser for å skade, spre seg, skjule seg og bli nyttelast i SKADA programmer.

Oppdagelsen av Stuxnet i juli 2010 innledet en ny dimensjon i internasjonal krigføring; cyber krig. Det ble den første skadevaren brukt i militær krigføring. Angrepet var rettet mot Irans atomkraftverk som anriket uran. Frykten var at Iran skulle skaffe seg nukleær kapasitet til militært bruk og bruke det mot Israel.

Data koden var tydelig laget av «Old School» programmerere med grunnlag i C og C-påbygg med inngående kunnskaper til Windows operativ systemer, deres svakheter, mulige bakdører gjennom link-lag, ispedd med «multi-Zero day triggers», evnen til å oppdatere seg selv, penetrere registrer-laget og spre seg fra datamaskin til datamaskin. Da Sergey Ulasen oppdaget ormen hadde den spred seg til 100.000 datamaskiner med 12.000 identifisere infeksjoner. [2]

[1] TK2100: Informasjonssikkerhet, Bengt Østby, leksjon 4, side 32, https://kristiania.instructure.com/courses/7866/files/784960?module_item_id=288224.

[2] Kristiania TK2100-1 22V: https://kristiania.instructure.com/courses/7866/files/787885?module_item_id=289340

Skadevaren: «Brain»:

Denne skadevaren krediteres som verden første PC virus (1986) og samme året greide man å infisere exe-filer med Suriv-02. [3]
Virus ble laget i Pakistan for å beskytte programvare som programmererne hadde laget for et hjertemonitor-program. Skadevaren var egentlig ikke designert for spredning. Den skjulte seg i boot sektoren av floppidisker og gjorde datamaskiner saktere enn vanlig (nyttelast). Imidlertid ble alle flopperdisker infisert av viruset som ble brukt i datamaskinen. Derved oppnådde man en utilsiktet, sakte spredning av viruset. [4]

Skadevaren: «WannaCry»:

Denne skadevaren kom fra Nord Korea og er kjent som «Ransomware attack». Skadevaren infiserte operasjons systemet i Windows maskiner. Denne ormen gjorde betydelig skade på mer enn 200 000 maskiner i 150 land. Angriperne låste alle filer og forlangte løsepenger for at bruker igjen skulle få tilgang til sine filer og programvare. Skadevare kan klassifiseres som skadelig nyttelast. Skadevaren utnyttet en svakhet i Windows OS. Alle maskiner som ikke var oppdatert med «Patches» fra Microsoft kunne bli infisert bare ved å være på nettet. [5]

Oppgave 4

Kryptering:

Rivest, Shamir, Adlemann (RSA) skapte en asymmetrisk nøkkelutveksling (Asymmetric key Exchange). Man valgte primtall p, q (1024 bits, minimum 100 desimal tall).
Man kan kalkulerte: n = p*q og z = (p-1)(q-1). Videre selekterte man en kryptisk nøkkel e der e<n og ingen like faktorer med z, der z er et primtall. Man valgte en dekrypteringsnøkkel d slik at e*d er delbar med z (dvs.: e*d mod z = 1). Deretter velger vi en offentlig nøkkel (public key) (n, e) samt en privat nøkkel (private key) (n, d).

Melding m; kryperings tekst c = $m^e \bmod n$
M = $(m^e \bmod n)^d \bmod n$ der $(m^e \bmod n) = c$ [6]

RSA kryptering kan gjøres for å sikre tilgang til en tekst av autoriserte personer (Alice and Bob) uten at en «Man-in-the-Middle» (Eve) får tilgang til den meldingen.

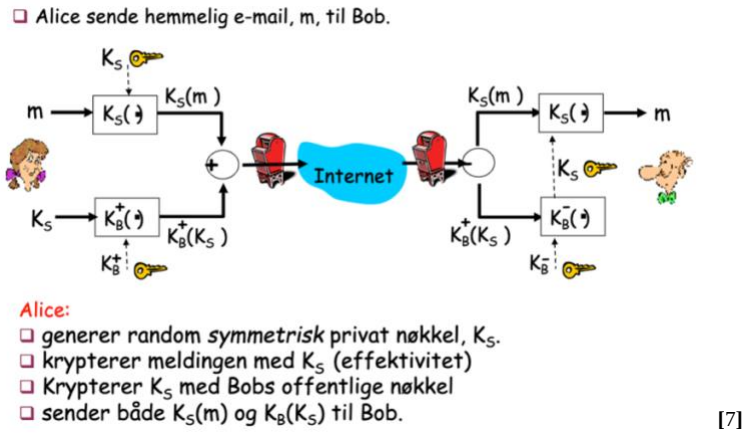
RSA signering brukes for å bekrefte autensitet hos avsender. Dette brukes på dokumenter som skal signeres. Der får man et sertifikat som bekrefter avsender. (Verisign).

[3] TK2100: Informasjonssikkerhet, Bengt Østby, leksjon 4, side 16-17, https://kristiania.instructure.com/courses/7866/files/784960?module_item_id=288224

[4] https://en.wikipedia.org/wiki/Brain_(computer_virus)
[5] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[6] TK2100: Informasjonssikkerhet, Bengt Østby, leksjon 2, side 57-63, https://kristiania.instructure.com/courses/7866/files/770899?module_item_id=277845

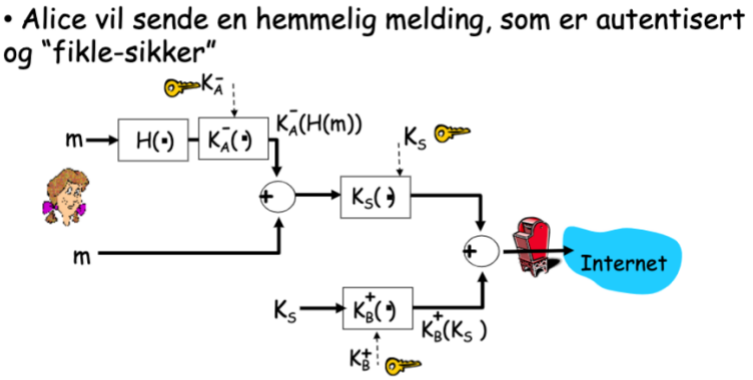
Alice skal sende e-post som både er konfidensiell i innhold og integritet fra avsender. Følgende figurer viser:
figurer 1) konfidensialitet og figurer 2) som viser integritet:

Figur 1)



[7]

Figur 2)



[8]

[7] TK2100: Informasjonssikkerhet, Bengt Østby, leksjon 2, side 64, https://kristiania.instructure.com/courses/7866/files/770899?module_item_id=277845
[8] TK2100: Informasjonssikkerhet, Bengt Østby, leksjon 2, side 67, https://kristiania.instructure.com/courses/7866/files/770899?module_item_id=277845

Oppgave 5

Kryptering:

Vi bruker RSA kryptering der den offentlige nøkkelen er: n = 3233 og e = 17, og den private nøkkelen er n = 3233 og d =2753.

Vi bruker formelen: $M = C^d \bmod n = x \bmod 3233 = y$ = bokstaven 'z' der: [9]
Vi utleder bokstaven « z » fra ASCII tabellen.

x = 1759, 2160 1992, 690, 1632, 2235, 1992, 1859, 2680, 2790.
y = 68, 117, 32, 107, 97, 110, 32, 82, 83, 65.
z = D, u, space, k, a, n, space, R, S, A.

Det betyr at meldingen lyder:
«Du kan RSA»

Oppgave 6

Nettverk:

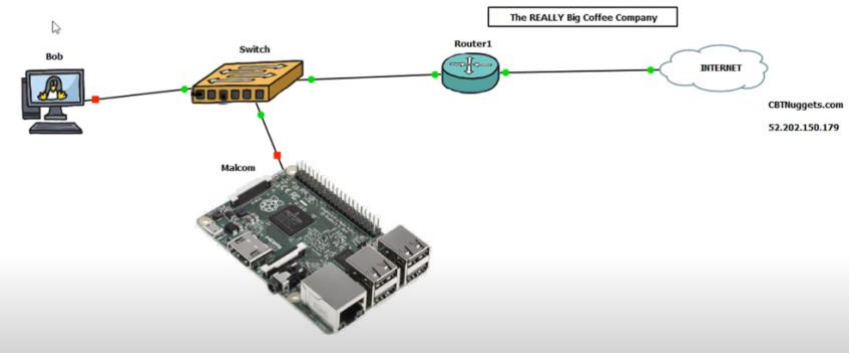
TCP/IP (Transmission Control Protocole) + UTP (UDP) er en multipleksing 16-bit port nummer som sikrer korrekte sekvenser i transmisjoner. Den inneholder sjekksummer, sekvens nummer og mottaker nummer. All HTTP, HTTPS, FTP og SMPT bruker TCP.

Slike sendinger er utsatt for «SYN Flood», dvs. falske sendinger med anonymer SYN/ACK utveklinger for å etablerere kommunikasjoner.
TCP har ingen «bitrate» restriksjoner. Det muliggjør typiske DOS angrep der et TCP-forespørsel er raskere enn serveren kan prosessere. Angriper sender eksepsjonelt mange pakker til severen og setter SYN flagg. Server svarer med SYN/ACK, men oppnår intet svar. Hele serverkapasiteten brukes opp og «socket» forblir åpen i 3 minutter.
Serveren reservere porter for kommunikasjon og bruker opp alle 65279 portene. Dette skaper sårbarheter for DOS angrep. Andre sårbarheter er hastighets-økning slik at router bli overbelastet, «TCP session kidnapping», «port scanning (nmap)», «MAC adresser» og «ARP spoofing og poisoning» [10]

[9] TK2100: Informasjonssikkerhet, Bengt Østby, leksjon 2, side 59, https://kristiania.instructure.com/courses/7866/files/770899?module_item_id=277845

[10] TK2100: Informasjonssikkerhet, Bengt Østby, leksjon 6, side 5-15, https://kristiania.instructure.com/courses/7866/files/800154?module_item_id=292929

Man-in-the-Middle angrep:



Bob skal sende en melding over nettet gjennom en switch og en router. Normalt foregår det ved en forespørsel over nettet gjennom en ARP forespørsel. Angriperen benytter seg av ARP spoofing. Han søker kontroll over Bobs internettrafikk.
ARP protokollen forbinder linkadressen med nettverksadressen og kringkaster forespørselen. Cashen svarer. Bob må igjennom en «default gateway» for å få tak i MAC adressen og dette blir kringkastet. Da kommer svaret som lagres i cashen. Angriper søker å intervenere ved hjelp av ARP spoofing / ARP poisoning. Han søker å legge sin MAC adresse in i cashen slik at Bobs datamaskin kontakter angriper, i stedet for den rettet MAC adressen. Angriper sender forespørsel videre på nettet og sikrer dermed en posisjon i midten der han kan overvåke og kopiere all kommunikasjon mellom Bob og nettet. [11]

Funksjon:

ARP protokollen fungerer ved at linkadressen bli koblet til nettverksadressen gjennom swtcher og routere. Denne forespørselen blir kringkastet. Svaret blir lagret i avsenders cashe som blir oppdatert. I TCP/IP og IPv4 foreligger det ingen sikrings eller autentifikasjonsmekanismer. Dette gjør ARP sårbare for «spoofing og poisoning». I nyere nettverk er IPv4 byttet ut med IPv6 som i stedet for ARP benytter seg av protokollen NDP.[12]

[11] https://en.wikipedia.org/wiki/Man-in-the-middle_attack,
TK2100: Informasjonssikkerhet, Bengt Østby, leksjon 6, side 5-15,
https://kristiania.instructure.com/courses/7866/files/800154?module_item_id=292929
[12] TK2100: Informasjonssikkerhet, Bengt Østby, leksjon 6, side 5-15,
https://kristiania.instructure.com/courses/7866/files/800154?module_item_id=292929

Oppgave 7

Phishing:

Phishing betyr mottagelse av en e-mail gjennom en falsk webside som ber om logg-in data (som bruker oppgir frivillig uten å vite at forespørsel kommer fra en falsk webside). Dette innebærer at angriper får tilgang til din datamaskin og kan utnytte det for alt det er verdt.

En hacker har stor nytte av kunnskapen han/hun oppnår ved hjelp av phishing. Informasjon slik som brukerdata, ID, bank informasjon, firma hemmeligheter og liknende er verdifulle data for angrepene som kan utnyttes kommersielt, konkurransevridende, i «social engineering» og påvirkning. Videre kan angriper bruke informasjonen for a skade offeret.

Det fins tekniske måter å beskytte seg på:

- TTL field kan settes til kort respons tid og ISP server får et autorativt svar som oppdaterer cashen.
- Vi kan benytte oss av «random ID» ved hjelp av VPN.
- Vi kan bruke «Domain Name System Security Extensions» (DNSSEC) for å få autentiserte svar fra tilbyder som forbedrer integritet og muliggjør trace.
- Vi kan installere Firewall som beskytter private nettverk fra offentlige nettverk. Dette muliggjør «payload inspection» og minsker sårbarheten samtidig som vi opprettholder funksjonaliteten.
- Vi kan benytte oss av White and Black listing. Ved førstnevnte blokkeres alle pakker bortsett fra de som er autoriserte. Ved sistnevnte slippes alle pakker gjennom minus de som er blokkerte.
- Bruk av Tunneling. All payload er kryptert.
- Bruk av IPSec: Den inneholder protokoller for autentisering, såkalt AH-protokoll.
- Bruk av IDS.
- Bruk av port scanning / nmap.

Viktigst av alt er personellopplæring. Her er det mye å hente:

- Unnvik å klikke på lenker som ikke er fra en kjent forbindelse.
- Vær oppmerksom på at i vår konkurranse-utsatte tid har ikke alle på nettet de beste hensikter med sin kontakt.
- Sjekk lenke-adresser før du klikker på dem. [13]

[13] TK2100: Informasjonssikkerhet, Bengt Østby, leksjon 6, side 18-26, https://kristiania.instructure.com/courses/7866/files/787885?module_item_id=289340

Oppgave 8

Hjemmekontor:

Hjemmekontor ble vanlig under koronakrisen og mange ansatte måtte jobbe hjemme i fra. Sårbarheter kom frem på mange plan:

- Ingen sikkerhetsansvarlige å henvende seg til på kort tid.
- Nettverket hjemme innehar ikke de samme sikkerhets-protokoller og tilsvarende utstyr som på den offisielle arbeidsplassen. Tekniske utrustninger og protokoller som nevnt i oppgave 7 er ofte ikke til stede.
- Hjemme har man mindre vakthold som sikrer mot fysiske innbrudd, uautorisert kopiering av ID og data.
- Man kan utsettes for phishing, pharming, ARP spoofing / poisoning, ARP PW tyveri, IP spoofing, smurf angrep ved lav kapasitet, IPv4 sårbarhet, SYN flood, TCP flooding, TCP session angrep, port scanning, DOS angrep med mere.

Ved at «hjemme datamaskiner» kan bli infisert kan dette lett overføres til selskapets servere og da øker selskapets sårbarhet.

Selskaper har således måtte tilpasse seg til den ny «normalen». Følgende sikkerhetstiltak er gjennomført mange steder:

- «Single sign on ID»
- «To step» verifikasjon av bruker mot selskapets server slik som banker nå har som standard.
- «Virtual Desktop Interface»
- Bruk av Citrix protokoll.
- RDC (Remote Desktop Connection)
- Alle data blir «viewed»
- Ingen transmisjoner. Kun «Read Only».
- Ingen «downloads».
- Ingen «print» muligheter samt «print scan» muligheter. Bare tastatur og mus «interface».
- «Hard disk» fullstendig kryptert.
- Tilgang kun akseptert fra lisensiert bruker.
- VPN (Virtual Private Network)
- Sikrede porter. Kun bruk av HTML port.

Oppgave 9

Praktisk SSL analyse:

Jeg benytte meg av SSL scan. Jeg fikk ikke tilgang til SSL Labs som ble referert til i forelesningene. [14]

Jeg kom frem til følgende konklusjoner:

- Testen ble gjennomført på port 443
- Serveren støttet ikke TLS fallback SCSV
- «Session renegotiation» var støttet og funnet sikker.
- TLSv1.2 var ikke sårbar for «heartbleed»
- Server Ciphers støttet ECDHE-RSA-AES256-GCM-SHA384
- Signatur Algoritmene var støttet ved: sha256WithRSAEncryption med en bit styrke på 2048.

Konklusjonen ble at serveren var godt sikret med høyeste verdier som kreves.

Detaljene på testen er gjengitt nedenfor.

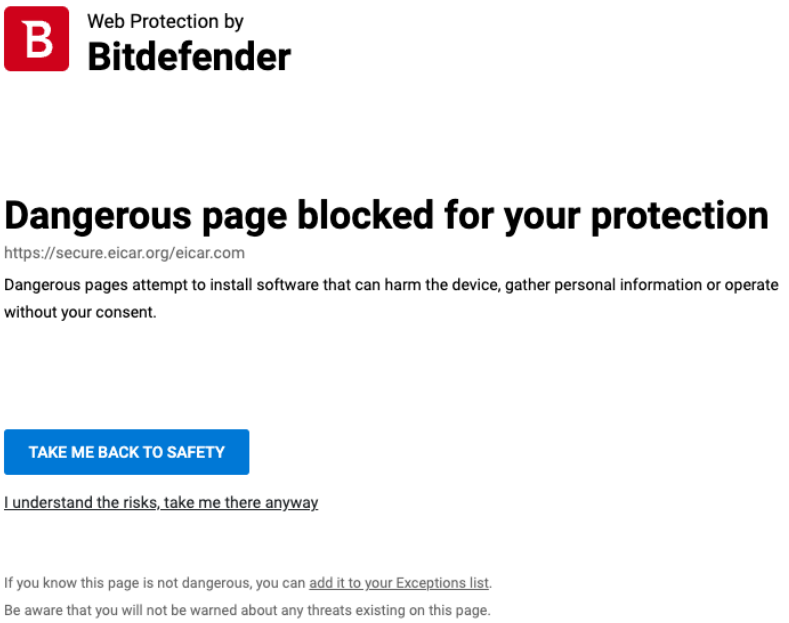
```
└─$ sslscan https://demo.testfire.net
Version: 2.0.12-static
OpenSSL 1.1.1n-dev  xx XXX xxxx

Connected to 65.61.137.117

Testing SSL server demo.testfire.net on port 443 using SNI name demo.testfire.net

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 1024 bits
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256     DHE 1024 bits
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 1024 bits
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA256         DHE 1024 bits
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  demo.testfire.net
Altnames: DNS:demo.testfire.net, DNS:altoromutual.com
Issuer:   Sectigo RSA Domain Validation Secure Server CA

Not valid before: May 22 00:00:00 2020 GMT
Not valid after:  May 22 23:59:59 2022 GMT
```

[14] TK2100: Informasjonssikkerhet, Bengt Østby, leksjon 12, side 37, https://kristiania.instructure.com/courses/7866/files/832074?module_item_id=303432

Oppgave 10

Praktisk anti-virus:

Jeg lastet EICAR filen fra https://www.eicar.org/?page_id=3950. Jeg scannet filen med mitt virus program. Virus programmet oppdaget filen og rapporterte den som skadevare. Følgende rapport ble mottatt:



Jeg gikk deretter inn i antivirus programmet sin karantene funksjon. Det er ikke aktuelt for meg å skru av sanntidsbeskyttelsen og eksportere den ut av karantenen. Dette vil innebærer risiko for min datamaskin og mine programvarer. Jeg fikk følgende analyse av mitt antivirus program.