besvarelse:

**Oppgave 1 a**

**1.**

det er for mellom osi modellen og tcp/ip modellen. først hva er osi modellen? osi modellen består av 7 lag som viser en prosess av hvordan datapakker beveger seg. lag 7 er applikasjonslaget dette viser oss nettleseren eller epost, viktig protokoll her er SMTP(secure mail trasnprtation protocol, med funksjoner med funksjoner med hjelp av IMAP,POP3, 250 ok, 550 feil, 354 skriv). lag 6 er presentasjon som viser brukeren hvordan ting er presentert. om det er kryptert eller dekryptert. viktig protokoll her er JPG, TLS (transport layer protokol)og HTTPS(hyper text transmission protcol secure). deretter kommer lag 5 som er session som danner en kommunikasjon mellom enheter. viktig protokoller her er PPTP, som er per to per kommunikasjon som er en til en kommunikasjon. deretter er lag 4 som er trasport laget. her er hva slags måte dataen blir transportert på. viktig protokoll her er TCP(transport) og UDP(user). lag 3 nettverk og det er her ip adresser blir utdelt. det er her nettverket kommuniserer med andre nettverk. derfor er router og switch layer 3 (en switch med evnene til en router) viktige protokoller. layer 2 er datalink som er her mac- adresser blir delt ut. flere enheter kobler seg opp her før det blir vidre sendt i internett trafikken. viktige protokoller her er ethernet og switch. layer 1 som er det nederste laget er fysiske laget det er her signaler og kabler blir sendt. derfor er kabel som kan bli koblet på ulike måter som coax, token ring, tp, og hub er viktige protokoller.

tcp/ip-modelle er at lag 5-7  kombineres til 1 som blir applikasjonslag.det er en fordel siden for eksempel en forespørsel blir sendt så blir alt sett som 5 lag der den øverste kun trenger å sende forespørsel og bekrefte(veldig veldig overfladisk). men osi modellen hjelper oss å se ulike oppgever når dataen går rudnt i internett trafikken for eksempel. det viser oss en enkel format av prossesen.

**2.**

som sagt har jeg sagt litt om viktige protokoller. en forbindelse orientert er en protokoll her er kabel og en forbindelses løs er hub. kabel er når du kobler deg fysisk til en port som da ungår annen forstyring, mens hub er der signaler blir sendt rundt. det er raskt, men alle porter for tilgang til den. begge sender signeler. i lag 2 er forbindelsesorientert switch, mens forbindelses løs er ethernet. begge tar i bruk mac-adresser, men i etherent kan ukjente se mac-adresse trafikken og det er mindre sikkert enn switch. i lag 3 så er router en forbindelses orientert mens, switch layer 2 er forbindelses løst. her er det siden router kun har i oppgave å styre nettverkstrafikken, men i switch layer 3 så må den håndtere mac- adresser også. begge håndterer ip-adresser. i lag 4 er tcp forbindelsesorientert siden den venter på en bekreftelse før dataen blir sendt, mens udp er forbindelsesløst og sender alt fra port. begge transporterer data. lag 5-7 bruker en protokoll som er http som er forbindelses løst siden dataen ikke er

kryptert, mens https har en forbindelse som er krypteret.

**3.**

way handshake er viktig siden i tcp så skal data bli overført så den må bli enig om hvordan den skal bli sendt før det er gjort. det kan bli sett slikt SYN som sender en forbindelse og lager sporing deretter er det ACK+SYN som mottakeren godtar forespørselen. til slutt er det ACK. der forbindelsen er bekreftet.

**OPPGAVE 1 b**

**1.**

dns er en måte som oversetter domene navn til ip adresse. viktige funksjoner her er RFC1149 som dns og www. det fungerer ved at du skriver en domenenavn som www.usn.no, deretter sender det en respons til dns-serveren om ip adressen. responsen sender en forespørsel til rotserveren om .com TDL serveren, responsen serveren svarer med ip adressen til .com serveren. deretter spør responsen spørr da om .com serveren om usn.
no sin navnserveren, da svarer navnserveren med adressen til navnservere. deretter spør navnserveren om ip adressen til usn. no og får ut "192.41.23.01". et eksempel på dette er at en forespørsel blir sendt til applikasjonslaget og her goddtar de det og og sender en handshake, der en kommunikasjon blir dannet. deretter blir det transportert med tcp, før den får en ip-adresse og mac-adresse.

**2.**

a)

overføring overnettverk så burde man ha kryptert data som VPN og en brannmur som sikkere utligjenlig tilgang til innsiden.

b)

for sikkerhet av databasen bør man sikkerhetskopierer i tillfelle angrep som ddos phising eller bufferoverflow skal skje. og man bør ha en overvokningsprogram som kan dettektere utligjenlig oppførsel som zero-day.

c)

for å beskytte mot prossesering som mens man autoriserer. så må man instile zero trust som er at man alltid må bekrefte med en autorisering, eller kan du sikkre med en tredjepert som vasler om det er ukjent aktivitet.

**OPPGAVE 1 C**

i tcp så sende data tregt i forhold til udp. ettersom tcp venter på en bekreftelse fra mottaker. udp sender data med åpne porter eksempler av dette er i radio og livestream, mens tcp er i nettleser og epost. så når man hadde implementert dem så hadde ikke vært bruk for listen() funksjonen i udp, siden den sender alt uansett som er serversocket. mens i tcp så er det både en serversocket og clientsocket siden de kommuniserer med hverandre.

**OPPGAVE 1D**

**1.**

i CSMA så er det 2 måter å håndtere kollisjonene. den ene er CD som er collision detection som skjer i eldre ethernet, dette ungår kolloisjon ved å overåke blandt annet. I CA(collision avoidance) som er mer vanlig nå , som blir brukt i WIFI så unngår den kollisjon, ved hjelp av prediction secutiry blandt annet.

**2**.

i CA blir brukt i WIFI siden det er mer produktivt og effektivt. det er en form for at problemer ikke skal dukke opp, enn detection som skjer i eldre ethernet. den er sårbar siden alt kan ikke bli detected. dette kan gjøre det enkelt for angripere.

**3.**

CA er tryggere der det kan implementeres funksjoner som sikkrer og krypterer, og kan implementere feilkorrigere med fuksjoner som hammerkode. mens i eldre ethernet kan det bli detektert med CRC som er brukt med XOR regneing. der en adresse som 1101 kan brukes for å finne feil på adressen 001101. der de 4 første sifferene addres med 0011 med 1101, som blir 0010 eks, så pusher man talle til venste ut og henter neste siffer i adressen. til slutt kan det bli noe med 100 som da settes bakert slik 001101 100. som da detekterer feil.

**OPPGAVE 2a**

**1.**

man in the middle er der angripere venter med å om justere din retting i nettverks trafikken. der som du ikke har en kryptert nettleser som da er http istedet for https så kan det blir andrep som http tls stripping. der det setter deg over til en side som ser helt lik ut og ser på internetttrafikken din. da kan du gi fra deg passord og andre sensitiv informasjon. det er også i synkornisert nøkkel, der den samme nøkkelen blir brukt for å kryptere og dekryptere. så venter angriperen på å få itak i den nøkelen. derfor er spørsmåle hvordan får du distuburert nøkkelen trygt. det er også asynkroniser nøkkel der alle kan kryptere viktig informasjon , men kun en spesiell nøkkel kan dekryptere den. man in the middel venter på den nøkkelen.

**2.**

det er ulike sikkerhetmekanismer som kan bli tatt i bruk for å unngå disse angrepene. det er som TLS, som blir bedre forklart i neste oppgave. SSL som er secure script der man må ha en sikker programeringspråk, vektøy og sikker kode. det er også HTTPS som da krypterer internett trafikken, koblingen kan ikke komme til angrperen. VPN som sikkrer en tunnel mellom enhetene. monotorering av ukjent aktivitet, som kan bli gjort i brannmur. kontakt nsm om det er alvorlig som er oversikt over alt internetttrafikken i norge(dersom det rammer en bedrift). adt som er en langvarig monottorering av angriperen i forhold til det andre.blir

ofte støttet av staten og er spesifikk, bruker avansert teknologi. det er også 2 typer som kan monotorere som er signertbasert som er brukt i brannmur der de bruker mønste, men den må bli trent opp. mens i den andre er det brukt i nettverk der den oppdager ukjent aktivitet som støtter zero-day.

andre angrep som ikke ble spurt om:

-supplychain er en måte de kommer inn på. dette er ved at de bruker tredjepart for å få tilgang til offeret sitt gjennom en bedrift sin sensitiv info om deg. angrep kan får tilgang på ulike måter. en er før systemet er installert. et annet er gjennom harddisk som en minnepinne som er fysisk. en annen er via phising. det er ulike måter man kan bli lurt på, den typiske er klikke på feil lenke. en er med følelser. en er at de gir feil info og refererer til feil kilde. de kan komme gjennom smart tv som IO. siden det er en bakdør, blir ikke oppdatert, svak passord, ikke kryptert eller har brannmur. det er ulike måter å løse det på når angripen har en 1 fot inne så må adp kunne bruke zero-day for å detektere.når den lager seg en bakdør sånn at den kan komme inn igjen så må den kunne ha en oppstartsystem.
-blockchain er en måte man kan sikre data. den har ikke en main server. den kan ikke endres , ellers må alt endres. dette er på grunn av hash funksjoner som MD5, SHA1 som ikke er brukt så mye nå, men det er brukt SHA-256(svak for passord) og SHA-3(brukt idag oftest). blockchain sine hash funksjoner er som fingeravtrykk. dette brukes i kryptovaluta blant annet siden om noe endre kan det detekteres lett.

- DDoS, som er når når internettrafikken blir manipulert sånn at filer blir trege og ikke tilgjenlige. det er 3 ulike. voulumbasert som er fyller opp internetttrafikken med ip-adresser. apikasjonsbasert som er aplikasjonen som blir rammet og protokollbasert der servern blir utsatt. dette kan bli løst med ikke mange tilgjenlige ip-adresser, redusans. overvåkning og sikkerhetskopiere.
-bufferoverflow som er en måte der angriperen for like priviligere som deg så dem kan endre kode. de kommer inn i minne og tar over. kan løses med ikke skrive minne i stack(no execute), legge til tilfeldige verdier rundt så du kan detektere, trygg prograameringspråk og sterk kode.
-løsepengevirus. det er en måte det angriperen stenger filene og gjør dem utilgjenlig for person/bedrifter. kan sleges til konkurrenter blant annet. dette kan løses med å ikke gi penger, men kontakte nsm. forebyggende tiltak som øvelse, bedrigten setter inn nok penger for sikkerhet. oppgadendetiltak der bedreiften har alarmer, overvokning og autenisering. korrigerende tiltak som forteller at alt går bra, dette er sikkerhetskopiering og kryptering. ulike bot virus kan blir instalert som er sperer virus og kommer inn i applikasjoner, en annen er spion virus som kan bruke kamera.

- man må ta hensyn til personvern. det er en grense mellom overvåkning og personvern man må forholde seg til. for eksempel i en sykehus så trenger de kun viktig informasjon og ikke tilgang til alt. da må man ta i bruk sikkerhetskultur. som er 7 dimensjoner. kommunikasjon, adferd, holdning, overholdelse, normer, kongisjon og ansvar. det blir problemer når norge skal forhandle med utlandet som usa. der de ikke ahr like visjon som det vi har.

**3.**

TLS sikkrer trasnsporten der den går gjennom an sikker lag. trasport layer security forhindrer angrep fra internett ved å bruke handshake. koblingen og sporingen må være godkjent før den blir sendt. det nå også være en serfikat satt av GDPR angående personvern og sikkerhet som den følger. og serfikast av nøkkel, den bruker en privat. TLS ser om det er kryptert, integrert(dataen er uendret) og tilgjenlig.

**OPPGAVE 2B**

**1.**

som sagt er en symetrisk nøkkel bruker samme nøkkel på å dekryptere og kryptere data. mens i anynkroniser blir flere nøkkler delt ut som kan krytrere, mens kun 1 kan dekryptere.

**2.**

dersom du har et sted der du har lagret sensitiv informasjon(huset ditt). så kan motakkeren også har samme nøkkel(huset hans). så begge kn komme seg inn og ut, men man må passe på å ikke miste nøkkelen som passord.

i asynkronisert er det mange som har nøkkelen til postkasse, men kun en har tilgang til å åpne den. men hvordan kan du gi nøkkelen til mottakeren? brukes på krypterete tunneler.

**3.**

moderne systemer bruker begge som i TLS der de først bruker asymetrisk for å være sikker, deretter bytter de til symetrisk siden den er raskere. og kan gi nøkkelen raskere til mottakeren.

**OPPGAVE 3A**

**1.**

A = switch der flere enheter er koblet til, ved help av mac-adresser som sendes vidre i internett trafikken.
B= router som er der internetttrafikken blir styrt. den hondteren ip adresser, VPN og NAT(oversetter ip adresser og porter når den blir sendt ut og inn av nettverket), netmaskt, gateway, interface, ttl, (routing tabell, som forteller om destinasjon i trafikken).
C = brannmur, det er her den filterer internett trafikk. denn følger en brannmur konfigurasjon som forteller den om regler for eksempel allow proto 192.41.10.2  from port 443.
branmur skjer i lag 3,4 og 7. der lag 3 forteller om ip-allokeringen, lag 4 forteller om sikker trasport av pakkene og lag 7 som sikrer nettleser som HTTPS.

**2.**

jeg skal lage en pseudo konfigurasjon av relevante enheter i maskinen som gir internett

tilgang til port 8081 på pc3. først sendes datapakken til switchen der den får en mac-adresse som 12a:13b:c4 deretter blir den sendt til router. her blir pakken sendt vidre med en routing tabell. Jeg sender med VPN som er en sikker tunnel, hvis du ikke vil det så blir det en ip adresse på interface.ttl forteller om tidsrommet for datapakken. routing tabell forteller om destinasjoenen og måten den blir sendt på. så vis nettverket sin ip adresse er 192.41.1.0/24. så er destinasjoenen til internet sendt slikt:

| Destinasjon | Gateway | Interface | Nettmask | TTL |
|---|---|---|---|---|
| 192.41.2.1 | 192.41.1.10 | VPN12 | 255.255.255.0 | 64 |

det er flere ting som har en faktor under routingtabellen. hvordan subnettene er delt opp. som man ser har jeg laget en leid linje mellom routeren som ahr id på vpn12. det er her dataen sin port blir sendt til. den porten kommer fra gateway. som man ser har jeg i eksemplet mitt brukt ip adresse klasse c som er for små nettverk som denne og hjemme. ip adressene starter fra 192- 223, privat er xxx.xxx.xxx, nettmask er 255.255.255.xxx. a er for store der 1-126, 10 er privat, nettmask er 255.xxx.xxx..xxx. 127 er loopback, mens 255.255.255.255 er broadcast. klasse b er for mellomstore kontorer som er 128-191, 172 er privat, det nettmask er 255.255.xxx.xxx. der som serveren vil stenge adgang ved og fordele foreksempel sikkerhetskopieringen så må det bli gjort med VLAN i router. men kan man må ha tilgang til dan så de gjøres det med en VLAN inter connect. en annen sikkerhets metode man kan gjøre i internette er DMZ som skiller mellom det eksterne og interne. dette er LAN som er lokal area nettverk. NAT er en annen sikkerhetstiltak som er effektiv som skjer i routeren.

brannmur konfigurasjonen skal gi det en sikker tilgang så den bruker ikke http port 80, men http port 443, for en sikker side. brannmuren skal gi tilgang til pc3 gjennom en port 8081. det blir da allow proto 192.41.10 port 8081.

**OPPGAVE 3B**

er skrevet i vedlegg

**Oppgave 3C**

**1.**

man finner ganske mye informajon i wireharrk. man finner router tabellen som forteller om koblingen. den viser hvor den skal til(destinasjon), id, tid, kilde, ip-adressen, protokoll, størrelse og info. dette er nyttig info for å se statusen til koblingen. andre måter å detektere er PING som ser fra node til node. Kretskabel som ser koblingen. netstat som viser tilkoblinger av porter tilgjenlig. tracerout som er sporing fra a til å. så er det brannmur som viser statusen til dataen.

nærmere på wireshark vises det frame som er statusen for det hele. ethernet som viser mac-

adresser(lag 2). ip-adresser som skjer i lag 3. tcp som er hvordan den blir trasportert i lag 4. og aplikkaasjonslaget http.

**2.**

denne wireshar loggen viser oss data pakken for psudo koden som ble laget. denne tar imot add og substract fra http/1.1, altså en webserver. detter blir da brukt med hhtp. ip adressen 10.0.0.2 er da oss og koblingen er godtatt, med 200 ok. dette er statuskoder på hhtp. der 500 er intern feil, og 404 er error. den skal til ip adresse 10.0.0.1. som sagt blir id, tiden og lengden av data pakkene nevnt. resultatet av adderingen var 8 og subtraheringen 2.

framen forteller oss at pakken kjøres på 100 bit på kabel, men 880 uten.
ethernet viser source port, hvor vi sender fra som har mac-adresse på 00:0c:29:11:22:23. destinasjonsporten, er der den skal til som har mac-adresse 00:0c:29:aa:bb:cc.
internett protocol version 4,forteller  om nettverkstrafikken. som man ser er ipv4 brukt. den viser lengden fav header og total. den har ikke fragment. ttl er 64. den er en tcp. destination er 10.0.0.1, mens vi er 10.0.0.2. detter er altså routngtabellen som styrer internett trafikken.
transmission control protocol, tcp er hvordan datapakkene blir transpotert. dette forteller oss hvilken port som blir brukt her blir den sendt fra 52344 til 8080, med lengden 47. andre porter som er ofte i bruk er 8000 og 8800.
til slutt er hypertext transfer protocol, http. aplikasjonslaget. metoden som blir brukt er subtract.  forespørselen fra nettsiden er /calculate?a=5&b=3. og det vi ser er host som er er 10.0.0.1:8080. dette viser oss koblingen og hvordan den blir presentert.