Informasjon om eksamenen

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Avsluttende eksamen i IN2120 Informasjonssikkerhet (Høst 2025).

Dato og tidspunkt: **16.desember 2025, kl.15:00 - 19:00 (4 timer).**

Ingen hjelpemidler er tillatt.

Merk følgende:

- Oppgavene i denne eksamenen er gruppert i ni deler. Den første delen dekker grunnleggende aspekter ved informasjonssikkerhet på tvers av pensum, mens de øvrige delene er fra utvalgte områder av pensum.
- Det er mulig å oppnå totalt 100 poeng (= 100%) ved å besvare alle oppgavene korrekt.
- Man kan navigere frem og tilbake mellom oppgavene.
- Skåring for hver oppgave angis eksplisitt. Det kan gis negative poeng for feil svar/valg, men total poengsum for hele oppgaven er minimum 0 (selv om summen over alle svarene er negativ).
- Vær kortfattet når du skriver tekst som svar på en tekstoppgave. Svaret kan skrives på norsk, svensk, dansk eller engelsk.
- Les oppgaveteksten nøye og spesielt der du skal fylle inn verdier i en tekstboks.
- I navigasjonslinjen nederst på skjermen indikeres fullførte oppgaver med blå søyler.

Tips! Siden du kan gå frem og tilbake kan det være lurt og først svare på oppgavene du syns er lette, og deretter gå tilbake til vanskelige oppgaver hvis du har tid.

Lykke til, hilsen Audun, Åvald og Nils!

Del 1: Generelt

1 Begrepsforståelse

Velg begrepet som betegner sutuasjonen ved hvert utsagn. Hvert begrep skal velges bare én gang.
Poeng: 0,5p for riktig, -0,5p for feil, 0p for ubesvart, maks 2p, min 0p.

Finn de som passer sammen:

	Usikkerhet	Unøyaktighet	Utrygghet	Uvisshet
Kjørehastighet = 200 km/t	○	○	✔	○
Knipse mynt og kron med sannsynliget p = 0,5	○	○	○	✔
Passord = 123456	✔	○	○	○
Måle avstand med øyemål	○	✔	○	○

Maks poeng: 2

2 Sikkerhetsmålsettinger

Indiker hvilken sikkerhetsmålsetting som typisk brytes som resultat av hvert angrep.

Poeng: 0,5p for hver riktig; -0,5p for feil, 0p for ubesvart; maks 3p; minimum 0p.

Indiker hvilket sikkerhetsmål som typisk brytes:

	Konfidensialitet	Integritet	Tilgjengelighet
Lese av pakkestrøm i wireshark	✔		
Kryptovirus (AES-256)			✔
DDoS-angrep			✔
Hashkollisjoner i signaturer		✔	
Installere en keylogger	✔		
Endre eksamensbesvarelsen din etter at du har sendt den inn		✔	

Maks poeng: 3

3 Krypteringsalgoritmer

Angi om disse krypteringsalgoritmene er symmetriske eller asymmetriske

0.5 poeng for hvert riktig svar, -0.5 for gale, 0 for ubesvart. Maks 2 poeng, min 0.

Finn de som passer sammen:

	Symmetrisk	Asymmetrisk
ECC		✔
RSA		✔
AES	✔	
Caesar	✔	

Maks poeng: 2

4 Boksterminologi for testing

I planleggingen av en pentest får du ingen informasjon om systemet du skal teste Hva kalles denne typen testing?
Poeng: 1 for riktig; 0 for feil eller ubesvart.

Velg ett alternativ:

- ○ Hvitboks-testing (white box)
- ○ Gulboks-testing (yellow box)
- ○ Svartboks-testing (Blackbox) ✔
- ○ Gråboks-testing (grey box)

Maks poeng: 1

5 OS privilegienivåer

En prosess kjører i **hypervisormodus**. Kryss av for hvert privilegienivå om prosessen kan få tilgang til ressurser (f.eks. data og prosess).
Poeng: 0.5p for hver riktig; -0.5p for feil, 0p for ubesvart; maks 1p; minimum 0p.
For hvert privilegienivå, indiker om en bruker-prosess kan få tilgang.

	Kan få tilgang	Kan IKKE få tilgang
Nivå -1	○ ✔	○
Nivå 0	○ ✔	○

Maks poeng: 1

6 Krypto- og PKI-begreper

Hvert utsagn nedenfor passer til et bestemt begrep innenfor krypto/PKI. Indiker hvilket begrep hvert utsagn passer best til.
Poeng: 0,5p for riktig;, -0,5p for feil, 0p for ubesvart; maks 2p; minimum 0p.
Indiker hva hvert utsagn passer beste med.

	PKI	Symmetrisk kryptering	Asymmetrisk kryptering	Hash-funksjon
AES-512 er et eksempel på	○	○ ✔	○	○
OS lagrer gjerne passord ved hjelp av	○	○	○	○ ✔
Deler offentlige nøkler	○ ✔	○	○	○
Er den raskeste måten å kryptere store mengder data	○	○ ✔	○	○

Maks poeng: 2

7 NSM

A) Hva står forkortelsen NSM (og nå snakker vi om den norske organisasjonen som blant annet står bak grunnprinsippene) for? (Hint: Svaret er to ord, og kan skrives på bokmål eller nynorsk).

Svar [ ] (Nasjonal sikkerhetsmyndighet, Nasjonalt tryggingsorgan) her.

B) Hva heter NSMs nasjonale koordinerende enhet for sikkerhetshendelser med hensyn til deteksjon, hendelsesrespons og koordinering? Svar enten forkortelsen eller fullt navn (begge gir lik uttelling). Hint: NorCERT-funksjonen er en del av dette, men ikke i navnet.

[ ] (NCSC, Nasjonalt cybersikkerhetssenter, National cyber security center, National cyber security centre)

Begge deloppgavene gir 1p for riktig svar, 0p for galt eller ubesvart, maks 2p, minimum 0p.

Maks poeng: 2

i Del 2: Kryptografi og PKI

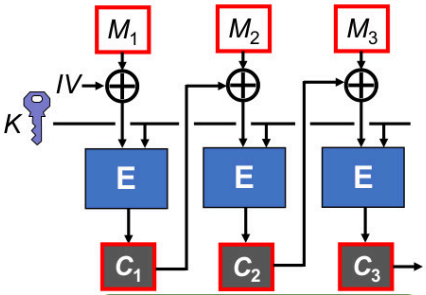
8 Blokkchiffer - operasjonsmoduser

For blokkchiffer brukes ulike operasjonsmoduser for kryptering av mer enn én blokk. Nedenfor ser du diagrammer som illustrerer kryptering for **tre ulike** operasjonsmoduser. Sett riktig navn på hver av dem.

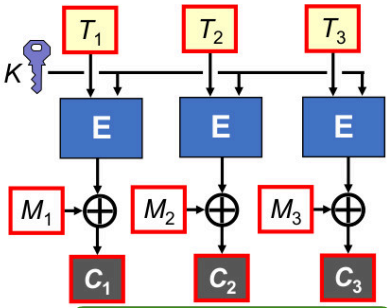
Poeng: 1p for hver riktig; -1p for feil; 0p for ubesvart; maks 3p; minimum 0p.

Hjelp

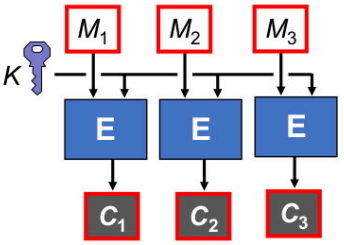
Electronic Code Book (ECB) | Cipher Block Chaining (CBC) | Output Feedback (OFB) | Counter Mode (CTR)



Cipher Block Chaining (C ✔)



Counter Mode (CTR) ✔



Electronic Code Book (E ✔

Maks poeng: 3

9 Nøkler

I denne oppgaven skal du flytte inn riktig begrep på riktig plass i teksten.
Poeng: 0,5 for riktig, -0,5 for feil, 0 for ubesvart, maks 3, minimum 0. Boksene kan gjenbrukes.

Hjelp

krypterer | private | signerer | offentlige | verifiserer | hemmelige

Bob [krypterer] en melding med Alice sin [offentlige] nøkkel. Deretter signerer han med sin [private] nøkkel. og sender over meldingen. Alice [verifiserer] signaturen med Bobs [offentlige] nøkkel, og dekrypterer meldingen med sin [private] nøkkel.

Maks poeng: 3

10 Kerckhoffs prinsipp

Hva er Kerckhoffs' prinsipp?
Forklar kort med egne ord, skriv maks fem setninger.
Maks 3p.
Skriv svaret ditt her. Endringer blir lagret automatisk.

Format

Kerckhoffs prinsipp lyder: «Utformingen av apparatet skal ikke kreve hemmelighold, og tap av apparatet til fienden skal ikke ødelegge sikkerheten for korrespondentene .»

Kryptografisk sikkerhet skal følgelig ikke være avhengig av algoritmen holdes hemmelig, kun krypteringsnøkkelen må holdes hemmelig.

To poeng for å ha forstått prinsippet, og ett poeng ekstra for å få nevne at kryptonøkler må være hemmelige.

Words: 0

Maks poeng: 3

11 Vigenèrechiffer

Du skal sende en norsk bok over Internett og ønsker å kryptere den. Du velger, som i oblig1, å bruke Vigenèrechiffer.

A) Tall og spesialtegn holdes her utenfor, og det er ingen forskjell mellom store og små bokstaver. Hvor stort blir dette nøkkelrommet? (Du trenger selvsagt ikke regne det ut, men sett opp begrepet.) Denne delen gir ett poeng.

B) Hva er svakheten med denne type chiffer - kort sagt, hvordan kan det eventuelt knekkes?
Skriv maks tre linjer her. Denne delen gir maks to poeng.

Skriv svaret ditt her. Endringer blir lagret automatisk.

Format

A) Vigenérechifferet benytter et sett standard alfabeter som er forskjøvet, der første bokstav er lik hver bokstav i kodeordet. Anta alfabeter med 29 bokstaver og at kodeordet (nøkkellengden) har K bokstaver. Størrelsen på nøkkelrommet blir da 29^K. Dette gir 1 poeng, siden oppgaven presiserer en norsk bok - så gi 0.5 poeng hvis de skriver 26^K og sier at det er 26 bokstaver (som jo er engelsk...) 1 poeng.

B) Vigenèrechiffer knekkes trivielt med frekvensanalyse. Bokstaven 'e' utgjør for eks 15,38% av det norske språket, noe som gjør den til den mest frekvente bokstaven.

Godkjenn frekvensanalyse, samt alle forklaringer om hva frekvensnanalyse er, eller hvordan det kan gjøres. 2 poeng.

Words: 0

Maks poeng: 3

12 Fremoverhemmelighold

Forklar (på maks fem linjer) hvorfor Diffie-Hellman gir fremoverhemmelighold, og hvorfor hybrid kryptering ikke gjør det.

Skriv svaret ditt her. Endringer blir lagret automatisk.

Format

Diffie-Hellman gir fremoverhemmelighold fordi den genererer unike øktnøkler for hver sesjon uavhengig av hverandre. Siden nøklene er uavhengig av hverandre, vil ikke en nøkkel kunne brukes til å utlede en annen.

Ett poeng for å nevne, eller beskrive øktnøkler. Ett poeng for å nevne eller beskrive at de skal være uavhengig av hverandre, og ett for å skrive noe om at nøklene derfor ikke kan brukes til å utlede tidligere eller senere nøkler og dermed sesjoner.

Words: 0

Maks poeng: 3

i Del 3: Angrepsvektorer og skadevare

13 Strafferamme ulovlig datainnbrudd

I henhold til straffelovens § 204 – hva er strafferammen for gjennomføring av ulovlig datainnbrudd? (I denne oppgaven må svaret være helt korrekt - hvis korrekt svar er "bøter og fengsel" og du svarer "bøter" - så er svaret altså feil.)

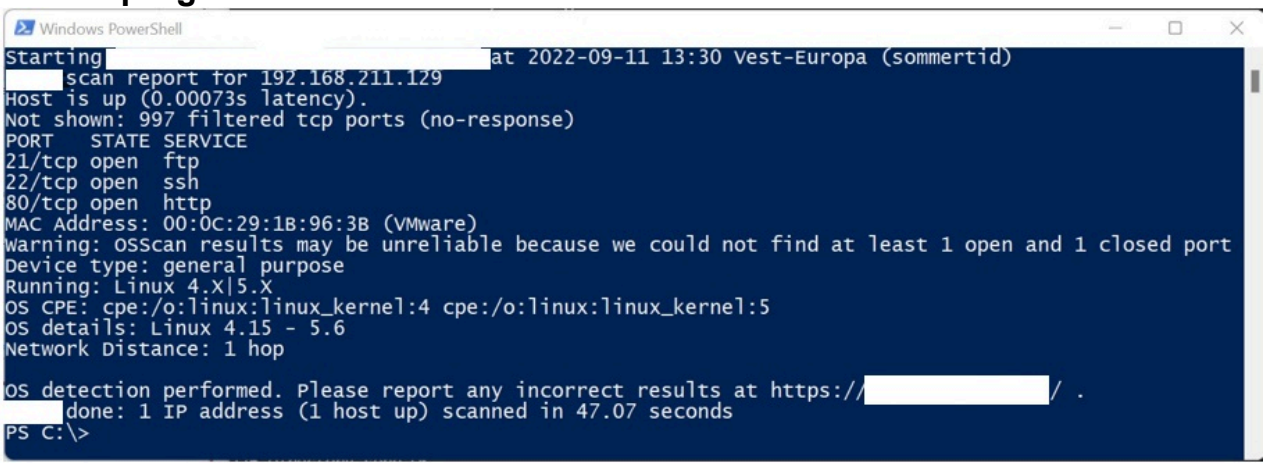
Poeng: 1 for riktig, 0 for feil eller ubesvart.

Velg ett alternativ:

- Fengsel i inntil fem år
- Bøter eller fengsel i inntil ti år
- Bøter
- Bøter eller fengsel i inntil to år ✔

Maks poeng: 1

14 Hvilket program er dette?



Hva heter dette programmet? [ ] (nmap, n map, network mapper)

Hint: Svaret skrives i ETT ord, og husk at svaret rettes automatisk. Er du i tvil om skrivemåten, så spør faglærer om du har skrevet det riktig når han går runden.
Riktig svar gir ettpoeng.

Maks poeng: 1

15 Sentrifuger

Hva heter skadevaren vi snakket om i kurset som ødela sentrifuger for å ødelegge det iranske atomprogrammet?

Skriv svaret ditt [ ] (stuxnet, stuxnett, stuksnett, stuksnet) her.

Poeng: 1p for riktig, 0p for galt eller ubesvart.

Maks poeng: 1

16 Hack et filter

I svarfeltet nedenfor er det implementert et filter som forhindrer deg å skrive mer enn to ord.
Du skal lure filteret - slik at du kan skrive og få frem hele setningen nedenfor:
"Filteret kan lures"
Du skal vise to måter å lure filteret, og det gir 1 poeng (du må gi to løsninger for å få poeng).
Skriv svaret ditt her. Endringer blir lagret automatisk.

Format

Godta alle løsningen som får frem setningen - eksempelvis;
FilteretKanLures.
Filteret_kan_lures.

To løsninger gir 1 poeng, ett gir ingen.

Words: 0/2

Maks poeng: 1

17 OSINT 1

Hva er OSINT [ ] (Open Source Intelligence, Open Source Inteligence, Open Source Intelligense, Open Source Inteligense, OpenSource Intelligence, Open SourceIntelligence) forkortelse for?

Hint: Det er en engelsk forkortelse, så du må svare på engelsk. Hvis du er i tvil om stavemåte - så spør faglærer.

Oppgaven gir ett poeng for riktig svar.

Maks poeng: 1

18 OSINT 2

Hva ER egentlig OSINT?

A) Forklar med egne ord hva OSINT er.

B) Gi to eksempler på hvorfor man bruker OSINT (altså hvilken nytte har man av det)

Skriv svaret ditt her. Endringer blir lagret automatisk.

Format

A) Ett poeng for å beskrive hva osint er.

OSINT, eller åpen kildeanalyse, er at man samler inn og analyserer data fra åpne kilder - eksempelvis Internett.

B) Ett for hver fornuftig målsetning de kommer opp med.

Målsetningen kan være å hente inn informasjon til bruk i phishing, eller som informasjonsinnhenting for eksempelvis å finne ut av hva slags teknologi som brukes i en virksomhet

Words: 0

Oppgaven gir tre poeng.

Maks poeng: 3

19 Skadevare

Du er sikkerhetssjef i et selskap. I nettverksloggene sine har IT funnet ut at ên, og bare ên, spesifikk maskin sender kryptert datatrafikk ut på Internett til gitte tider av døgnet. Det er for tiden ingen som fysisk har tilgang til, eller bruker maskinen. Problemet viste seg å fortsette selv etter å ha rebootet maskinen. IT har undersøkt maskinen og har ikke funnet tegn til at den kjører noe annet enn standard OS-applikasjoner. De har verifisert at disse er identiske med filene som leveres fra produsenten. (De har gjort dette riktig, så filene er altså ikke manipulert). Antivirusløsningen deres finner ingen skadevare.

Maskinen fortsetter imidlertid å sende ut data. Du installerer en annen antivirusløsning - den finner og fjerner skadevaren. Du sjekker maskinens logger nøye, men finner ingen spor til at filen hverken kjører eller noensinne har kjørt (dette gjør du både før og etter at du installerte ny antivirusløsning, og svaret var identisk begge gangene).

IT trenger maskinen og ønsker å sette den tilbake i produksjon siden antivirusløsningen tross alt har fjernet viruset.

A) Hva kalles denne typen skadevare?

B) Hva bør du gjøre nå?

C) Kan IT sette maskinen tilbake i drift nå som skadevaren er borte? Begrunn svaret,

Svar maks en linje på oppgave A (1p), fem linjer på oppgave B (3p) og fem linjer på oppgave C (3p).

Skriv svaret ditt her. Endringer blir lagret automatisk.

Format

A) Rootkit - ett poeng.

B) Her bør de få med noe om å verifisere at skadevaren ikke er spredt til øvrige deler av virksomheten - to poeng.

De bør også skrive noe om å analysere hvordan skadevaren kom inn i systemet (ett poeng).

C) Her må de få med at maskinen må reinstalleres for å være sikker.

Hensikten med rootkit, er å skjule skadevare. Selv om skadevaren nå tilsynelatende er borte, så kan det være bakdører eller annen skadevare der.

Ett poeng for å få med at maskinen må reinstalleres, og to poeng for begrunnelsen.

Words: 0

Maks poeng: 7

i Del 4: Nettverkssikkerhet

20 Snortregel

```
alert tcp $HOME_NET 445 -> any any ( msg:"OS-WINDOWS Microsoft Windows SMB possible leak of kernel
heap memory"; flow:to_client,established; content:"Frag",fast_pattern; content:"Free";
content:"|FA FF FF|"; content:"|F8 FF FF|",within 3,distance 5; content:"|F8 FF FF|",within
3,distance 5; metadata:policy balanced-ips alert,policy security-ips drop,ruleset community;
service:netbios-ssn; reference:cve,2017-0147; reference:url,technet.microsoft.com/en-
us/security/bulletin/MS17-010; classtype:attempted-recon; sid:42339; rev:2; )
```

Lag en snort-regel som generer en alarm for utgående TCP-basert SSH-trafikk fra domenekontrolleren 10.10.23.23. Husk å få med riktig portnummer for SSH (vi forutsetter at standardporten er i bruk).

Skriv svaret ditt her. Endringer blir lagret automatisk.

alert tcp 10.10.23.23 22 -> any any (msg “Utgående SSH-trafikk mot DC“)
Det svaret gir to poeng, se bort fra enkle syntaksfeil (feil retning for trafikken er helt feil svar,
og gir null poeng) og feil rekkefølge i brukte parametere. Trekk dem ett poeg for mangel på følgende ord: "alert", "tcp" og mangel på, eller bruk av feil portnr (som skal være 22).

Oppgaven gir maks to, minimum null poeng.

Maks poeng: 2

21 IDS

A) Hva er en IDS, og hva står forkortelsen for?

Skriv maks en setning (ett poeng)

B) Du setter opp en anomalibasert IDS-løsning i løpet av mars. I samme måned har virksomheten din en større pentest av nettet sitt.

Er det noe problem å gjøre dette samtidig?

Begrunn svaret ditt, skriv maks fem linjer tekst - denne delen av oppgaven gir maks to poeng.

Skriv svaret ditt her. Endringer blir lagret automatisk.

Format

A) Intrusion detection system - innbruddsdeteksjonssystem (godta begge). (0,5 poeng)

Godta enhver forklaring som gir mening på hva IDS er. (0,5 poeng).

B) Gi 0.5 poeng for å bare si at det er potensielt problematisk.

De bør skrive at et anomalibasert IDS da trenes opp til at angrepstrafikk er vanlig (1p).
Kartlegging og skadevare vil da være normaltillstand for IDSen,
og reelle angrep vil derfor ikke generere alarmer. (1 p)

Words: 0

Maks poeng: 3

22 Protokollstack

I denne oppgaven skal du fylle ut enkelte protokoller du har vært borti i kurset på riktig sted i Internettstacken.

NB: Grunnet begrensninger i inspera står står nederste lag (fysisk) helt til venstre, og så går lagene oppover mot høyre. Kan være lurt å dobbeltsjekke at du ikke har tenkt feil.

Hvert riktig svar gir 0,5 poeng, ubesvart gir 0, og hvert gale gir -0,5 poeng.



Plasser protokollene på riktig nivå

	Fysisk	Link	Internett	Transport	Applikasjon	App
TLS Record	○	○	○	✔	○	○
Outlook	○	○	○	○	○	✔
UDP	○	○	○	✔	○	○
TLS Handshake	○	○	○	○	✔	○
ARP	○	✔	○	○	○	○
IP	○	○	✔	○	○	○
HTTP	○	○	○	○	✔	○
Telnet	○	○	○	○	✔	○

Maks poeng: 4

23 Kryptert trafikk?

Angi hvilke av disse protokollene som er henholdsvis kryptert, eller ikke kryptert.
Hvert riktig svar gir 0,5 poeng, hvert gale -0,5. 0 for ubesvart.

Finn de som passer sammen:

	Ukryptert	Kryptert
SSH	○	○ ✔
Telnet	○ ✔	○
HTTP	○ ✔	○
FTP	○ ✔	○
RDP	○	○ ✔
ARP	○ ✔	○

Maks poeng: 3

24 Brannmurregler

I denne oppgaven skal du svare om trafikken slippes igjennom en tilstandsløs brannmur med følgende regelsett:

```
iptables –A FORWARD –s 131.234.142.33 -p tcp --dport 80 –j accept
iptables -A INPUT   -s 131.234.142.33 -j drop
iptables -A FORWARD -s 129.240.31.23 -p tcp -j drop
iptables -A FORWARD -s 129.240.31.23  -p tcp --dport 23 -j accept
iptables –A FORWARD –s 131.234.142.33 –p tcp -—dport 22 –j accept
iptables –A FORWARD –s 131.234.142.33 –j drop
```

Vil følgende trafikk slippes igjennom?

	Ja	Nei
RDP-trafikk fra 131.234.142.33	○	○ ✔
HTTPS-trafikk fra 131.234.142.33	○	○ ✔
SSH-trafikk fra 131.234.142.33	○ ✔	○
HTTP-trafikk fra 129.240.31.23	○	○ ✔
HTTP-trafikk fra 141.10.10.10	○	○ ✔
HTTP-trafikk fra 131.234.142.33	○ ✔	○
Telnet-trafikk fra 129.240.31.23	○	○ ✔
UDP-trafikk fra 129.240.31.23	○	○ ✔

Hvert riktig svar gir 0,25 poeng, hvert gale gir -0,25 og ubesvart gir 0 poeng. Minimum 0 poeng.

Maks poeng: 2

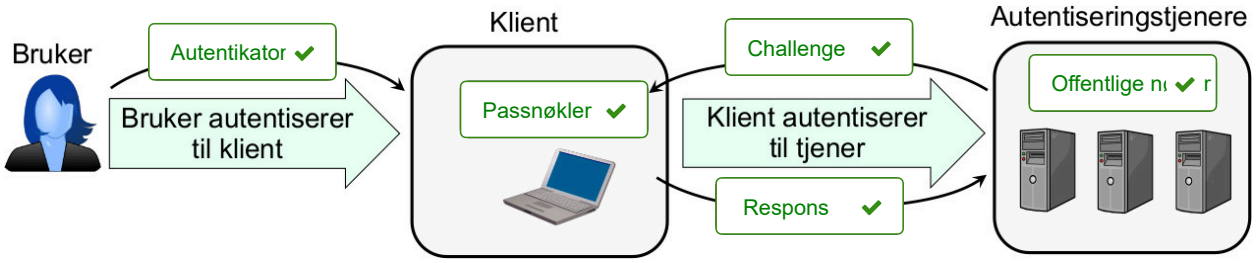
i Del 5: Autentisering og IAM

25 Passnøkler 1

Figuren viser en enkel arkitektur for online brukerautentisering med passnøkler. Flytt tekstelementene til riktig plass i figuren.
Poeng: 0,5p for hver riktig, -0,5p for feil, 0p for ubesvart, 3p for alle riktig, minimum 0p.

Hjelp

Respons	Offentlige nøkler	Passnøkler	Challenge
Autentikator			



Maks poeng: 3

26 Passnøkler 2

Velg riktig(e) svar på spørsmålene nedenfor. Hvert spørsmål kan ha flere enn ett riktig svar.
Poeng: 0.5p for hver riktig, -0.5p for feil, 0p for ubesvart, Maks 2p, minimium 0p.

1) Hva er en phishing-melding?
Velg ett eller flere alternativer

- [ ] En melding som lurer brukeren til å utføre en handling som bryter sikkerheten ✔
- [ ] En melding med reklame, enten den er ønsket eller uønsket.
- [ ] En melding med uønsket reklame, men som ellers ikke lurer brukeren..
- [ ] En melding med lenke til en falsk nettside som lurer brukeren til å oppgi brukernavn og autentikator(er). ✔

2) Hva gjør at autentisering med passnøkler regnes som phishingresistent?
Velg ett eller flere alternativer.

- [ ] Under autentisering vil autentiseringstjeneren sjekke at passnøkkelen passer sammen med den offentlige nøkkelen.
- [ ] Under autentiseringen vil klienten sjekke at passnøkkelen inneholder domenenavnet til nettsiden som foretar brukerautentisering. ✔
- [ ] Hver passnøkkel inneholder domenenavnet til nettsiden som foretar brukerautentisering. ✔
- [ ] Under autentisering vil klienten sjekke at passnøkkelen passer sammen med den offentlige nøkkelen.

Maks poeng: 2

27 Passnøkler 3

Oppgave 1. En bruker benytter en passordbank som støtter synkronisering av passnøkler mellom brukerens ulike enheter. Forklar kort et realistisk phishing-scenario som gjør at brukerens passnøkler kan bli stjålet eller misbrukt. Skriv maks tre setninger.

Poeng: 2p for et realistisk scenario.

Skriv svaret ditt her. Endringer blir lagret automatisk.

Oppgave 1 (2p). Tilgang til passordbanken er ikke phishingresistent fordi den ikke kan benytte passnøkler (som ellers ville være lagret i passordbanken). Angriperen kan dermed sende phishing som lurer brukeren til å oppgi autentikator(er) til passordbanken.

Oppgave 2. NIST SP 800-63-4 "Retningslinjer for digital identitet" er en veileder for brukerautentisering i amerikansk e-forvaltning. Veilederen definerer tre "Assurance Levels" for autentisering, dvs. AL1, AL2, og AL3. For at en autentiseringsordninger med passnøkler skal tilfredsstille krav til AL3 (høyeste nivå), hva sier veilederen om synkronisering av passnøkler? Skriv maks tre setninger.

Poeng: 1p for korrekt beskrivelse.

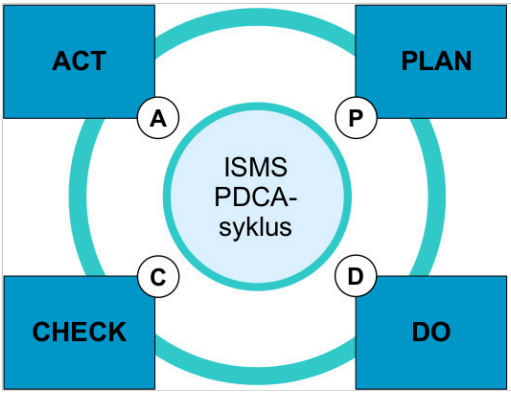
Skriv svaret ditt her. Endringer blir lagret automatisk.

Oppgave 2 (1p). Passnøkler kan ikke synkroniseres. Dvs. at hver passnøkler kun er lagret i, og bundet til enheten, som typisk er en autentiseringsbrikke.

Maks poeng: 3

i Del 6: ISMS og risikostyring

28 **ISMS**



Kapitlene i ISO/IEC 27001 ISMS - Krav	
1 Omfang (dvs. virkeområde)	6 Planlegging
2 Normative referanser	7 Støtte
3 Termer og definisjoner	8 Drift
4 Organisasjonens kontekst	9 Prestasjonsevaluering
5 Ledelse	10 Forbedring

Standarden **ISO/IEC 27001 ISMS - Krav** inneholder 10 kapitler, hvorav kapitlene 4 - 10 beskriver krav til ISMS. Tabellen viser titlene på alle kapitlene. ISMS tolkes ofte etter den velkjente PDCA-modellen (Plan Do Check Act) for kvalitetsforbedring, som vist på figuren.

Å tolke ISMS etter PDCA betyr å tilordne hvert av kapitlene 4 - 10 til en av PDCA-fasene. I tillegg er en av fasene naturlig for drift av sikkerhet basert på f.eks. NSMs grunnprinsipper for IKT-sikkerhet.

Velg riktig PDCA-fase for hvert av kapitlene 4 - 10, samt for NSMs grunnprinsipper for IKT-sikkerhet.

	P	D	C	A
4 Organisasjonens kontekst	✔			
5 Ledelse	✔			
6 Planlegging	✔			
7 Støtte	✔			
8 Drift		✔		
9 Prestasjonsevaluering			✔	
10 Forbedring				✔
NSMs grunnprinsipper for IKT-sikkerhet		✔		

Poeng: 0,5p for hver riktig, -0,5p for feil, 0p for ubesvart. Maks 4p, minimum 0p.

Maks poeng: 4

29 NSMs grunnprinsipper og ISO27001

NSMs grunnprinsipper for IKT-sikkerhet, og ISO27001 er to standarder/veiledere for informasjonssikkerhet. Indiker om hvert utsagn nedenfor gjelder for NSM, ISO27001, begge eller ingen.

Poeng: 0,5 for hver riktig; -0,5 for hver feil; 0 for ubesvart; maks 2, minimum 0.

Indiker hva som gjelder for hvert utsagn.

	NSM	ISO27001	begge	ingen
Kategoriserer sikkerhetstiltak etter sikkerhetsfunksjoner/prosesser (f.eks. kartlegge, beskytte, oppdage, håndtere)	✔			
Standarden/veilederen må kjøpes		✔		
Tilgang er avgrenset til offentlige myndigheter				✔
Kan brukes sammen med ISO/IEC 27002			✔	

Maks poeng: 2

30 Risikoanalyse

Oppgave 1: Angi korrekt matematisk formel (som tekst) for beregning av risikonivå når sannsynlighet og konsekvens uttrykkes kvantitativt. Hva kalles den matematiske operatoren?

Maks 1p.

Skriv svaret ditt her. Endringer blir lagret automatisk.

Kvantitativ: (1p) for minst ett av de to svarene nedenfor:
Risikonivå = Sannsynlighet x Konsekvens
Produkt/multiplikativ

Oppgave 2: Angi korrekt matematisk formel (som tekst) for beregning av risikonivå når sannsynlighet og konsekvens uttrykkes som (kvalitative) logaritmiske nivåer. Hva kalles den matematiske operatoren?

Maks 1p.

Skriv svaret ditt her. Endringer blir lagret automatisk.

Kvalitativ: (1p) for minst ett av de to svarene nedenfor:
Risikonivå = Sannsynlighet + Konsekvens
Sum/additiv

Maks poeng: 2

i Del 7: Sikker utvikling

31 STRIDE

STRIDE er et hjelpemiddel for trusselmodellering ved programvareutvikling. Hver av de seks bokstavene i STRIDE er forbokstaven for et engelsk trusselbegrep. For hver av de seks bokstavene, nevn 1) trusselbegrepet på engelsk eller norsk, og 2) hvilken sikkerhetmålsetting trusselen medfører brudd på (f.eks. brudd på konfidensielitet, integritet, tilgjengelighet, autentisering etc.).

Maks 6p.

Skriv svaret ditt her. Endringer blir lagret automatisk.

For hver bokstav, 0,5p for begrepet til bokstaven, og 0,5p for sikkerhetsmålet som brytes.

S Spoofing (Identitetstyveri) Brudd på autentisitet
T Tampering (Tukling) Brudd på integritet
R Repudiation (Benekting) Brudd på sporbarhet
I Information disclosure (Datatyveri og -lekkasje) Brudd på konfidensialitet
D Denial of service (Tjenestenekt) Brudd på tilgjengelighet
E Elevation of privilege (Utvidede tilganger) Brudd på tilgangskontroll

Maks poeng: 6

32 OWASP Top 10

Gi en kort beskrivelser av OWASP Top 10, Når ble siste utgave publisert? Bruk maks fire setninger.

Skriv svaret ditt her. Endringer blir lagret automatisk.

–Rangerer de 10 mest kritiske sikkerhetsrisikoene for nettapplikasjoner
–Gir råd om hvordan sårbarhet og risiko kan reduseres
–Siste utgave fra november 2025
Opp til 3p for tilsvarende dekkende beskrivelse

Maks poeng: 3

i Del 8: Fysisk sikkerhet

33 SJA

Hva står forkortelsen SJA for [ ] (sikker jobbanalyse, sikker jobb analyse) .

Maks poeng: 1

34 SJA - del 2

A) Hva er vitsen med SJA (1p)

B) Hvordan skal prosesesn med å lage en SJA gjøres?

Maks 3p.

Skriv svaret ditt her. Endringer blir lagret automatisk.

Format

Hensikten med sikker jobbanalyse er å forhindre arbeidsulykker (1p).

En potensielt farlig arbeidsoppgave deles opp i små deler, hvor risikoen i hver deloppgave analyseres for å eventuelt finne måter å redusere risikoen for ulykker
(1p for å nevne oppdeling, 1p for å analysere risiko for å redusere risiko.
Risiko må nevnes, ikke bare skrive å forhindre ulykker - hvis ikke gir oppgaven maks to poeng.

Words: 0

Maks poeng: 3

35 Emisjonssikkerhet

Hva heter NATO-spesifikasjonen læreboken beskriver for å avlytte elektromagnetisk stråling for å kunne gjenskape signaler?

Fyll inn ditt [ ] (TEMPEST) her.

Riktig svar gir 1p.

Maks poeng: 1

36 Bytte lyspære

Du skal bytte en lyspære. Den er tre meter opp i luften, og det skal benyttes en lift (personløfter).

Bruk det du har lært i kurset til å besvare, og begrunne følgende spørsmål (bruk relevante regler som du har lært om i kurset og du kan se bort fra SJA):

"Hvor mange IN2120-studenter trengs for å bytte en lyspære?"

Ps: Du trenger ikke finne på en vits her.
PPs: Du får lov.

Maks 4p.

Skriv svaret ditt her. Endringer blir lagret automatisk.

Format

Det skal være minst to personer, hvorav minst en må være på bakken.

Begge må ha gyldig opplæring i bruken av lift.

Gi to poeng for å skrive at det må være to personer, ett poeng for å skrive at en må være på bakken, og ett poeng for å skrive at begge må ha opplæring.

Words: 0

Maks poeng: 4

i Del 9: Bobs passord

37 Bobs passord

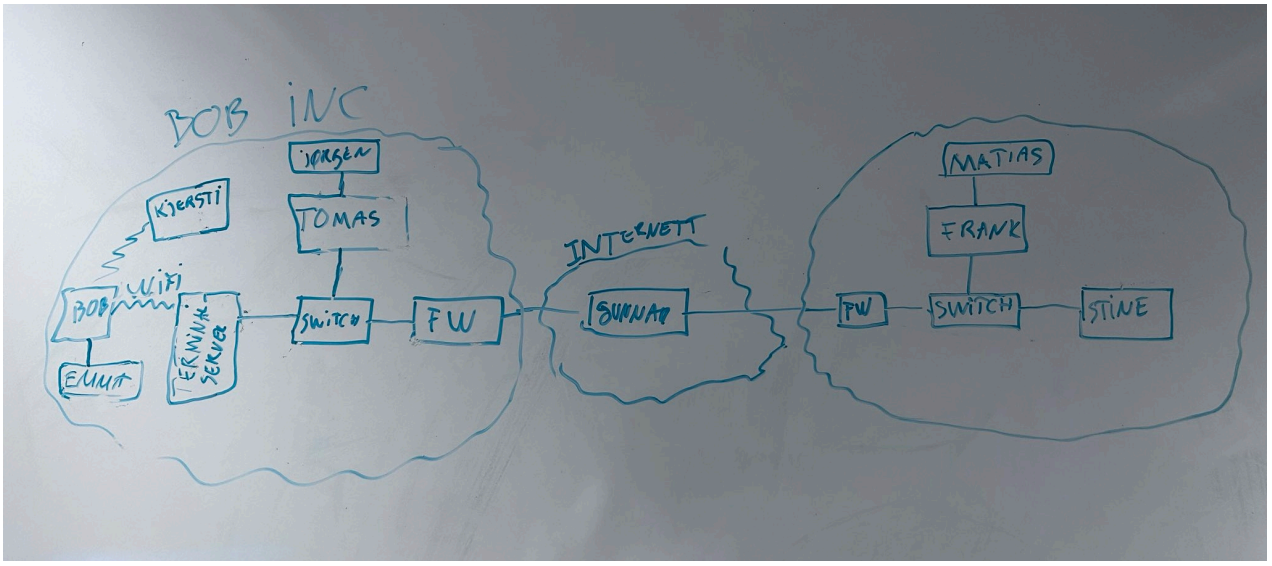
Bob er toppsjef for det store konsernet Bob Inc.
Bob er opptatt av passordsikkerhet, og bytter passord hvert sjette måned (du kan se helt bort fra evt trussel fra kvantedatamaskiner i denne oppgaven).

Bob har funnet Stines nettside som sjekker passordstyrke. Passordet sjekkes av et script som kjører på serveren som hoster nettsiden.

Nettsiden ser slik ut (forenklet - forutsett at nettsiden ser ut som en legitim fullstendig nettside) og Bob har tastet inn passordet sitt. Passordet til Bob er: "DettePassordetErLangtSomEtVondtÅr688AS%!@" Nettsiden er satt opp med TLS, og HSTS er implementert. Det er ikke første gang Bob bruker nettsiden med samme nettleser.



Nettverket som benyttes ser slik ut:



Som vi ser av tegningen (nettverket er større, men vi fokuserer på denne delen) er Bob pålogget en terminalserver via wifi. Emma har en keylogger på Bobs maskin. Kjersti avlytter wifi-trafikken mellom Bob og terminalserveren. Tomas har foretatt et vellykket man in the middle-angrep, og står mellom terminalserveren og brannmuren i Bobs nett. Jørgen har hacket Tomas sin maskin, men er ikke admin på den.

Gunnar er systemadministrator hos teleleverandøren, og all trafikken går igjennom hans utstyr.

I nettverket til Stine (det er hennes server), er Frank MiTM mellom brannmuren og Stines server og Matias har hacket Franks maskin. Matias har fått root-tilgang på Franks maskin.

Oppgave: Hvem, hvis noen av disse personene (bortsett fra Bob) kan nå ha få fatt i Bobs passord.
Begrunn svaret (både hvorfor, og hvorfor ikke) for hver person, og hvis begrunnelsen er lik for flere personer - så kan de selvsagt grupperes (person x, y og z har/ikke passordet fordi <begrunnelse>.)

Maks 9p.

Skriv svaret ditt her. Endringer blir lagret automatisk.

Format

Denne oppgaven inneholder mange personer...

Emma, som har en keylogger vil kunne fange opp passordet - da en keylogger fungerer før TLS slår inn.

Kjerstis avlytting av åpne wifi-signaler plukker uansett bare opp TLS-kryptert tekst.

Frank og Tomas sine tilgang (MitM), ser også bare kryptert tekst. Signalene går her gjennom Gunnars maskiner, og blir helt tilsvarende.

Jørgen vil potensielt plukke opp Franks signaler, men vil bare se samme krypterte teksten som Frank får.
Matias har root- og vil plukke opp Franks signaler, men Frank har som kjent ikke det ukrypterte passordet...

Stine eier serveren, og siden serveren dekrypterer - så vil hun kunne plukke opp passordet til Bob.

Oppgaven gir 1 poeng for å si at Emma kan finne passordet, og to poeng til for å begrunne med at tastetrykkene jo kommer før TLS-kryptering.

Videre gis 1 poeng for å navngi Stine, og 2 til for å begrunne (terminering av TLS, eller på annen måte si at serveren ser teksten i klartekst).

0,5 poeng for å nevne alle som ikke får tilgang til passordet (totalt tre) hvis de nevner noe om at disse personene uansett bare får tilgang til kryptert tekst (enten nevner TLS,
eller sier noe om ende til ende-kryptering),

Words: 0

1 poeng for å si nevne ende-til endekryptering, enten med ord eller forklaring.

Maks poeng: 9

Slutt

Slutt på eksamen. Takk for nå, og ha god jul når du er ferdig med siste eksamen!