Informasjon om eksamenen

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Avsluttende eksamen i IN2120 Informasjonssikkerhet (Høst 2024).

Dato og tidspunkt: **25. november 2024, kl.9:00 - 13:00 (4 timer).**

Ingen hjelpemidler er tillatt.

Merk følgende:

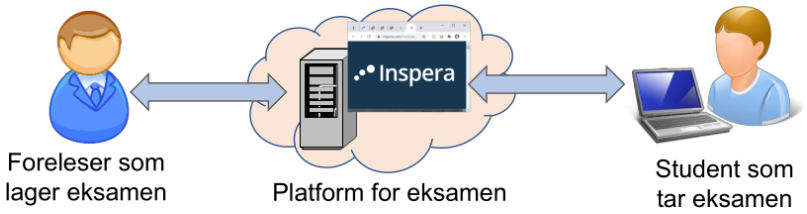
- Oppgavene i denne eksamenen er gruppert i åtte deler. Den første delen dekker grunnleggende aspekter ved informasjonssikkerhet på tvers av pensum, mens de øvrige delene er fra utvalgte områder av pensum.
- Det er mulig å oppnå totalt 100 poeng (= 100%) ved å besvare alle oppgavene korrekt.
- Man kan 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 Generelle sikkerhetsmålsettinger



Anta situasjonen med Inspera-eksamen, som vist på figuren, der vi fokuserer på sikkerhet for selve eksamensoppgavene og besvarelsene (som er verdi/ressurs/asset). Viktigheten av de tre sikkerhetsmålsettingene kan være ulike før eksamen starter, under eksamen, og under sensureringen etter eksamen. For hver av disse tre fasene, velg hvilken sikkerhetsmålsetting som er viktigst. Alle målsettingene er naturligvis viktige, men du skal velge den viktigste i hver fase.

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

Før eksamen er Velg alternativ (konfidensialitet, tilgjengelighet, integritet) viktigst.

Under eksamen er Velg alternativ (konfidensialitet, integritet, tilgjengelighet) viktigst.

Etter eksamen, men før sensureringen er ferdig er Velg alternativ (tilgjengelighet, integritet, konfidensialitet) viktigst.

Maks poeng: 3

2 Oversettelse

Velg riktig oversettelse fra engelsk til norsk.
Poeng: 0,5 for riktig, -0,5 for feil, 0 for ubesvart, maks 2, min 0.

Finn de som passer sammen:

	Visshet	Garanti	Trygghet	Sikkerhet
Safety	○	○	○ ✔	○
Assurance	○	○ ✔	○	○
Security	○	○	○	○ ✔
Certainty	○ ✔	○	○	○

Maks poeng: 2

3 Sikkerhetsmålsettinger

Indiker hvilken sikkerhetsmålsetting som typisk brytes som resultat av hvert angrep.
Poeng: 0,5 for hver riktig; -0,5 for feil/ubesvart; maks 3; minimum 0.
Indiker hvilket sikkerhetsmål som typisk brytes:

	Integritet	Tilgjengelighet	Konfidensialitet
Avlytting av datatrafikk	○	○	○ ✔
Uautorisert sletting av filer og fjerning av backup	○	○ ✔	○
Sende angrepstrafikk med en annens forfalskede IP-adresse til en IPS	○	○ ✔	○
Foreta manuell, men uautorisert endring av filer	○ ✔	○	○
Overdreven passordspraying mot en enkelt brukerkonto (utover systemets terskel for antall feil forsøk)	○	○ ✔	○
Hashkollisjoner i signaturer	○ ✔	○	○

Maks poeng: 3

4 Boksterminologi for testing

I planleggingen av en pentest får du utlevert en skisse over deler av nettverksinfrastrukturen og noe, men ikke all kunnskap 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)
- ○ Svartboks-testing (Blackbox)
- ○ Gulboks-testing (yellow box)
- ○ Gråboks-testing (grey box) ✔

Maks poeng: 1

5 OS privilegienivåer

En prosess kjører i **brukermodus**. Kryss av for hvert privilegienivå om prosessen kan få tilgang til ressurser (f.eks. data og prosess).

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

For hvert privilegienivå, indiker om en bruker-prosess kan få tilgang.

	Kan få tilgang	Kan IKKE få tilgang
Nivå -1	○	○ ✔
Nivå 0	○	○ ✔
Nivå 3	○ ✔	○

Maks poeng: 3

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

Indiker hva hvert utsagn passer beste med.

	Symmetrisk kryptering	Asymmetrisk kryptering	Hash-funksjon	PKI
Er enveis og blir ofte brukt til å sjekke integritet.	○	○	○ ✔	○
Garantere autentisitet av offentlige nøkler ved hjelp digitale sertifikat.	○	○	○	○ ✔
Bruker en felles hemmelig nøkkel	○ ✔	○	○	○
Benytter en privat nøkkel og en offentlig nøkkel.	○	○ ✔	○	○

Maks poeng: 2

7 Asymmetrisk krypto

Poeng: 1 poeng for hvert riktige svar; -1 poeng for feil, 0 poeng for ubesvart; totalt maks 3 poeng; minimum 0 poeng.

Alice har **stjålet en kopi** av Bobs private nøkkel. Hun bruker den til å transformere (kryptere) meldingen, som så blir sendt til Bob. Hvilken nøkkel må Bob bruke for å transformere (dekryptere) teksten for å kunne lese den?

Velg ett alternativ:

- Alice sin private nøkkel
- Bobs private nøkkel
- Alice sin offentlige nøkkel
- Bobs offentlige nøkkel ✔

Bob klarer å lese meldingen med riktig nøkkel. Når han svarer på meldingen, bruker han sin offentlige nøkkel - hvilken nøkkel må da Alice bruke for å lese innholdet av Bobs melding?

Velg ett alternativ

- Bobs private nøkkel ✔
- Alice sin private nøkkel
- Bobs offentlige nøkkel
- Alice sin offentlige nøkkel

Basert på informasjonen nevnt over - hva bør Bob gjøre nå?

Velg ett alternativ

- Revokere sin private nøkkel
- Revokere Alice sin offentlige nøkkel
- Revokere sin offentlige nøkkel ✔
- Revokere Alice sin private nøkkel

Maks poeng: 3

8 Passordknekking

I oblig 2, samt på pentestforelesningen, ble det brukt en parameter i John the ripper for å knekke passord gjennom å lage permutasjoner på ordene i en ordliste. Hva het den?

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

Velg ett alternativ:

- wordspray
- rules ✔
- permute
- all

Maks poeng: 1

9 Sikkerhetsprotokoller

I kurset har vi nevnt en, eller flere protokoller som beskytter mot TLS-stripping. Hvilke(n)?
Poeng: 1 for hvert riktig svar, minus ett per feil - minimum 0 poeng.
Velg riktig alternativ(er)

- TLS
- DNS
- HTTP
- HSTS ✔
- UDP
- IPSEC
- IP

Maks poeng: 1

10 Datanettsikkerhet

Velg det mest passende begrepet i hver setning nedenfor.
Poeng: 1 for hver riktig; -1 for hvert gale svar, 0 for ubesvart; maks 3, minimum 0.

Velg alternativ (TLS-inspeksjon, IDS, ip-tables, autentiseringstjener) er et eksempel på en linux-basert brannmur som beskytter de interne nettverkene mot angrep fra eksterne nettverk, og bestemmer hvilken trafikk som kan passere inn og ut.

Velg alternativ (Diffie-Hellman, Ip-sec, Hashcat, IDS) er et eksempel på en VPN-løsning.

Wireshark er et eksempel på et Velg alternativ (APT, pakkeanalysator, pakkefilter, applikasjonsbrannmur)

Maks poeng: 3

11 Passordkompleksitet

Passordpolicyen har blitt endret fra en passordlengde 10 tegn til 14 tegn. Vi antar at systemet støtter standard (engelsk) 105 forskjellige tegn (store og små bokstaver, tall og spesialtegn). Hvor mye mer komplekst blir passordet?
Poeng: 1 for riktig; 0 for feil eller ubesvart; maks 1, minimum 0.
Velg ett alternativ:

- 105^4 ✔
- 105*4
- 105 ganger
- Umulig å si

Maks poeng: 1

12 Meldingsautentisering

For hver setning nedenfor, velg begrepet som passer inn.
Poeng: 0,5 for hver riktig; -0,5 for hver feil, 0 for ubesvart; maks 3, minimum 0.

Digital signatur bruker Velg alternativ (symmetrisk kryptografi, asymmetrisk kryptografi,

kvantekryptografi, tellermodus-kryptografi) og gir Velg alternativ (ubenektelig, phishingresistent, fremoverhemmelig, enkel) meldingsautentisering.

MAC (Message Authentication Code) bruker Velg alternativ (tellermodus-kryptografi,

symmetrisk kryptografi, kvantekryptografi, asymmetrisk kryptografi) og gir Velg alternativ (enkel, fremoverhemmelig, ubenektelig, phishingresistent) meldingsautentisering.

En privat nøkkel publisert på internett betyr at Velg alternativ (vi må slutte å beregne hash med den kompromitterte nøkkelen., det er uproblematisk, fordi den offentlige nøkkelen kan fremdeles benyttes, vi må stoppe melding autentisert med MAC, vi må slutte å signere digitalt med nøkkelen).

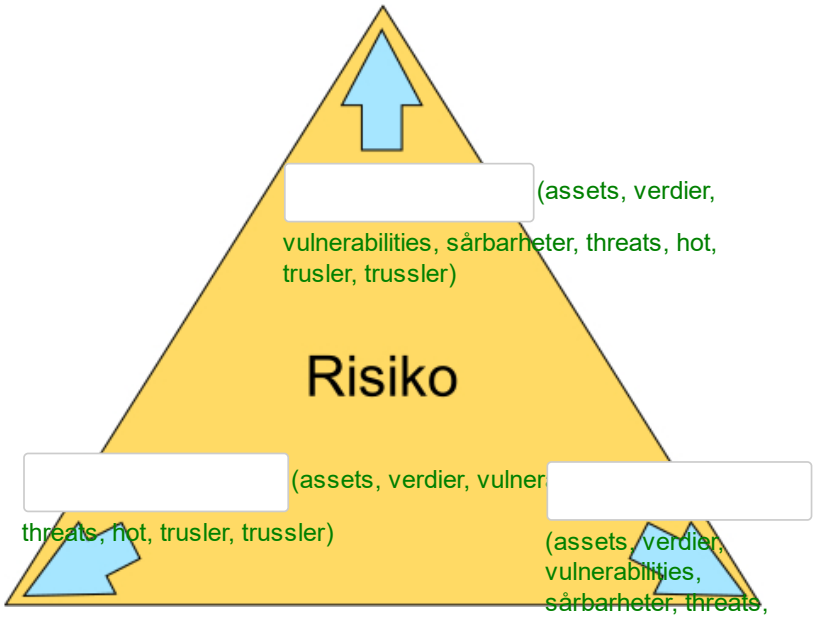
En offentlig nøkkel publisert på internett betyr at Velg alternativ (meldingsautentisering må stoppe, du må lage et nytt nøkkelpar, meldingsautentisering kan fortsette, en angriper kan forfalske meldinger).

Maks poeng: 3

13 Risikotrekanten

Figuren nedenfor viser risikotrekanten der hvert hjørne representerer et fundamentalt risikoaspekt. Skriv navnet på hvert risikoaspekt i hvert sitt hjørne. **Bruk flertallsformen av ordet.** Det spiller ingen rolle hvilket hjørne du skriver hvert ord i. Store eller små bokstaver spiller heller ingen rolle, men pass på å stave ordene riktig.

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



Maks poeng: 3

Del 2: Kryptografi og PKI

14 Egenskaper til krypto

Denne oppgaven gir 1 poeng for hvert riktige svar, -1 for galt, 0 poeng for ubesvart; 3 poeng hvis alt er riktig, og minimum 0 poeng.

Firmaet "Sikkert og visst", har havnet i en konflikt med firmaet "Sorte hull". Du som ekspert i informasjonssikkerhet har du blitt kalt inn for å bistå det juridiske teamet med noen tekniske spørsmål.

En digital signatur som bruker asymmetrisk krypto har blitt brukt på en melding. "Sorte hull" påstår at for en tredjepart, er dette bevis på at "Sikkert og visst" har sendt meldingen. Er denne påstanden riktig?

Velg ett alternativ:

- Påstanden er riktig ✔
- Påstanden er feil

SHA-1 algoritmen har blitt brukt, men "Sorte hull" påstår at denne ikke lenger er sikker så resultatene kan ikke brukes. Hva er riktig om SHA-1?

Velg ett alternativ

- SHA-1 anses som usikker ✔
- SHA-1 anses som sikker

Sensitiv informasjon fra kommunikasjonen mellom "Sikkert og visst" og "Sorte hull" har kommet på avveie. "Sorte hull" sier at de ikke har lekket informasjonen med vilje.

Øktnøklene som er brukt har blitt utvekslet via Diffie-Hellman nøkkelutveksling mellom "Sorte hull" og "Sikkert og visst". "Sorte hull" påstår dermed at siden de ikke brukte noen autentisering så kan kommunikasjonen ha vært utsatt av et mann-i-midten angrep. Hva er riktig om påstanden til "Sorte hull"?

Velg ett alternativ

- Påstanden er riktig siden Diffie-Hellman ble brukt uten digital signatur. ✔
- Påstanden er delvis riktig, Diffie-Hellman gir ikke sterk autentisering, men gir svak autentisering som forebygger mann-i-midten angrep.
- Påstanden er feil siden Diffie-Hellman gir autentisering.

Maks poeng: 3

15 Nøkkelsertifikat

Denne oppgaven omhandler nøkkelsertifikater og du må velge passende svar på nedtrekksmenyen.
Poeng: 1 for hvert riktig; -1 for gale svar, 0 for ubesvart; minimum 0.

Med din nettleser finner du følgende sertifikatsti for en nettside på inspera.no:



inspera.no er et eksempel på [Velg alternativ] (rot-CA, mellomliggende CA, subjeksertifikat).

Hvem har signert inspera.no? [Velg alternativ] (Rot CA, Selv-signert, PKI, Mellomliggende CA)

Maks poeng: 2

16 Nøkkelsertifikat 2

I denne oppgaven skal du skrive inn svaret, som skal være på formatet "-.---" (hvor du må erstatte hver "-" med en bokstav (stor eller liten bokstav spiller ingen rolle) eller et tall.
Poeng: 1 for riktig; 0 for feil eller ubesvart; maks 2; minimum 0.

Hva kalles standarden som brukes for public-key nøkkelsertifikater på Internett ?
Fyll in svaret her:

[ ] (X.509, x509, x 509, x-509)

I dette kurset har vi nevnt en rekke asymmetriske kryptografi algoritmer som kan brukes til signering. For eksempel i en PKI-sammenheng.

Skriv **en, og bare en,** av disse algoritmene i forkortet form (eksempelvis ville kunstig intelligens vært KI) i feltet under:

[ ] (RSA, ECC, DSA, DH, MQV, ECDSA, EdDSA, FFC, IFC, XMSS)

Maks poeng: 2

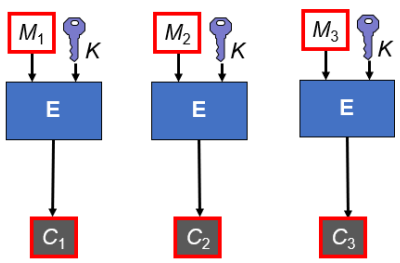
17 Blokkchiffer - operasjonsmoduser

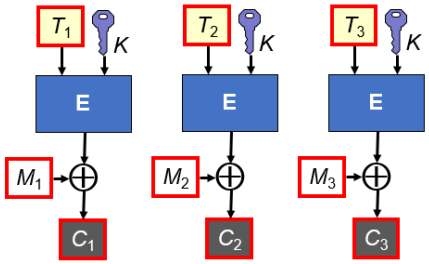
For blokkchiffer brukes ulike operasjonsmoduser for kryptering av mer enn én blokk. Nedenfor ser du diagrammer som illustrerer kryptering for **to ulike** operasjonsmoduser. Sett riktig navn på hver av dem.

Poeng: 1 for hver riktig; -1 for hver feil; 0 for ubesvart; totalt maks 2; totalt minimum 0.

Hjelp

Counter Mode (CTR)	Data Encryption Standard (DES)
Cipher Block Chaining (CBC)	Electronic Code Book (ECB)





Electronic Code Book (ECB) ✔ — Counter Mode (CTR) ✔

Maks poeng: 2

18 Hash-funksjoner

Kryptografiske hashfunksjoner har en rekke krav som må oppfylles. Kryss av de som er korrekte krav og ignorer de som er feil eller ikke gir mening.

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

Velg de alternativene som er krav til en hashfunksjon:

- [ ] Liten offentlig nøkkel
- [ ] Lett å beregne ✔
- [ ] Sterk kollisjonsresistens ✔
- [ ] Salt
- [ ] Tung, men sterk kryptering

Maks poeng: 2

19 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

signerer | private | offentlige | hemmelige | krypterer | verifiserer

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

Maks poeng: 3

i Del 3: Angrepsvektorer og skadevare

20 Phishing

Hva slags phishing-angrep er denne eposten et eksempel på? (Hint: Jeg verken har, eller har noensinne hatt apple pay)

"APPLE PAY har blitt suspendert på enheten din!

Vi la merke til at kortet du bruker på enheten din er knyttet til flere enheter.

Som et sikkerhetstiltak har vi midlertidig blokkert Apple Pay-tjenesten din inntil vi kan bekrefte at du er den legitime eieren av kortet.

Bekreft nå <http://langSensurertUrl>

Apple-ID-en din kan ikke brukes til å foreta betalinger gjennom APPLE PAY før du aktiverer ID-en din på nytt

Sendt av Apple

Copyright 2024 Apple Inc. Alle rettigheter forbeholdt.

Hvis du ønsker å avslutte abonnementet, vennligst klikk her. <http://langSensurertUrl> "

Poeng: 1 for riktig, 0 for feil eller ubesvart.
Velg ett alternativ:

- Masse-phishing ✔
- Direktørsvindel (whaling)
- Spyd-phishing
- Klone-phishing

Maks poeng: 1

21 Skadevare

Velg den kolonnen som passer best med hver rad.

Poeng: 0,25 for hver riktig, -0,25 for hver feil, 0 for ubesvart, 1 for alle riktig, minimum 0.

Finn de som passer sammen:

	Logisk bombe	Virus	Dataorm	Trojaner	Bakdør
Morris er en kjent	○	○	✔	○	○
Skjult passord implementert av programmereren for å kunne logge seg inn senere uten systemeiers viten	○	○	○	○	✔
Fungerende antivirusprogram som inneholder en spesiell skadevare	○	○	○	✔	○
Skadevare som formaterer harddisken din fredag den trettende kl. 12.05	✔	○	○	○	○

Maks poeng: 1

22 Skadevarebegreper

Sett inn riktig begrep for hver beskrivelse. All kode er satt i "gåsøyne" pga innstillinger i inspera - se bort fra dem.

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

Hjelp

Rootkit	Exploit	Kryptoutvinningsbott
Logisk bombe	Løsepengevirus	MiTM
Command injection	trojaner	

Skadevare som skjuler seg i et legitimt, nyttig program	trojaner ✔
Et program som stadig bruker mye CPU-kraft	Kryptoutvinningsb ✔
"a && cat /etc/passwd"	Command injectio ✔
Et program som brukes til å skjule spesielle prosesser	Rootkit ✔

Maks poeng: 2

23 Sårbarhetsutnyttelse

I løpet av en pentest prøver du å logge inn på en nettside. Du har ikke noe passord, men tester og finner ut at følgende angrep funger i passordfeltet:

a' or 1==1

Utvikleren av nettsiden prøver å løse problemet gjennom å lage et filter som blokkerer teksten 1==1.

Oppgave A: Hva heter dette angrepet (1 poeng)?

Oppgave B: Lag et angrep som fungerer, til tross for filteret nevnt over (2 poeng) (du trenger ikke beskrive eller forklare angrepet - bare hva du ville tastet inn i passordfeltet).

Oppgave C: Utvikleren sier han har implementert filteret ved hjelp av script som kjører hos brukerne. Beskriv kort (maks to setninger) hvorvidt dette er en god løsning, og hvorfor/hvorfor ikke (3 poeng).

Skriv ditt svar her

Format

Oppgaven gir maks 6 poeng.

A) 1p for å navngi angrepet: SQL-injection

B) 2p for å lage et angrep som omgår filteret: Her trengs et korrekt logisk uttrykk som passer i et angrep som f.eks. 2==2, eller 345>343.
Angrep: A' or 2==2.

C) 3p
0,5p for å bare svare "nei".

2p for å begrunne påstanden med noe à la:
"Bruker har kontroll over hva som kjører på sin maskin,
og kan dermed omgå, eller la være å kjøre skriptet."

3p for å begrunne påstanden og samtidig å si noe om at dette gjøres gjennom en Proxy, eksempelvis Burp eller Zap (trenger ikke navngi).

Words: 0

Maks poeng: 6

24 Hvilket program er dette?

```
[redacted]# privilege::debug
Privilege '20' OK

[redacted]# sekurlsa::logonpasswords

Authentication Id : 0 ; 515764 (00000000:0007deb4)
Session           : Interactive from 2
User Name         : Gentil Kiwi
Domain            : vm-w7-ult-x
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * LM       : d0e9aee149655a6075e4540af1f22d3b
         * NTLM     : cc36cf7a8514893efccd332446158b1a
         * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
        tspkg :
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * Password : waza1234/
...
```

Hva heter dette programmet? _____ (mimikatz, mimikats, mimmikatz, mimmikats)

Hint: Svaret er IKKE kiwi, som bruker dette programmet. 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 to poeng.

Maks poeng: 2

i Del 4: Nettverkssikkerhet

25 Kommunikasjonssikkerhet

Velg riktig begrep for å danne korrekte utsagn nedenfor.
Poeng: 1 for hver riktig; 0 for hver feil eller ubesvart; maks 5, minimum 0.

Velg alternativ (Alert-protokollen, Handshake-protokollen, Change Cipher Suite-protokollen, Record-protokollen) i TLS brukes til å etablere øktnøkkel (sesjonsnøkkel).

Velg alternativ (Både TLS og IPSec, Bare TLS, Bare IPSec) krypteree all applikasjonsdata.

HSTS beskytter mot Velg alternativ (DOS, XSS, TLS-stripping).

I en sky-VPN kan brukerens ISP (Internet Service Provider) se Velg alternativ (at brukeren har tilgang til sky-VPN men ser ikke innhold eller endelig destinasjon, bare IP-adresse til endelig destinasjonen (og ikke ukryptert innhold), bare innholdet (i klartekst), alt innhold og IP-adresse til endelig destinasjonen)

Velg alternativ (Mitre ATT&CK, OWASP Top 10, Cyber kill chain, APT) rangerer de mest kritiske sikkerhetsrisikoene for nettapplikasjoner.

Maks poeng: 5

26 Standardporter

Velg riktig standardport til hver tjeneste. 0,5 poeng for hvert riktig svar, -0,5 for hvert gale, 0 for ubesvart. Maks 3 poeng.

Finn de som passer sammen:

	21	22	23	53	80	443	3389
SSH	○	✔	○	○	○	○	○
HTTPS	○	○	○	○	○	✔	○
HTTP	○	○	○	○	✔	○	○
FTP	✔	○	○	○	○	○	○
RDP	○	○	○	○	○	○	✔
Telnet	○	○	✔	○	○	○	○

Maks poeng: 3

27 IDS

I kurset har vi gått igjennom enkelte IDS-er. Hvilket program er dette regelsettet et eksempel på? _____ (snort) Riktig svar gir to poeng, galt eller ubesvart gir 0 poeng.

CVE-2017-0147 Detail

Current Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packets, aka "Windows SMB Information Disclosure Vulnerability."

Source: MITRE
Description Last Modified: 03/16/2017
+View Analysis Description

```
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; )
```

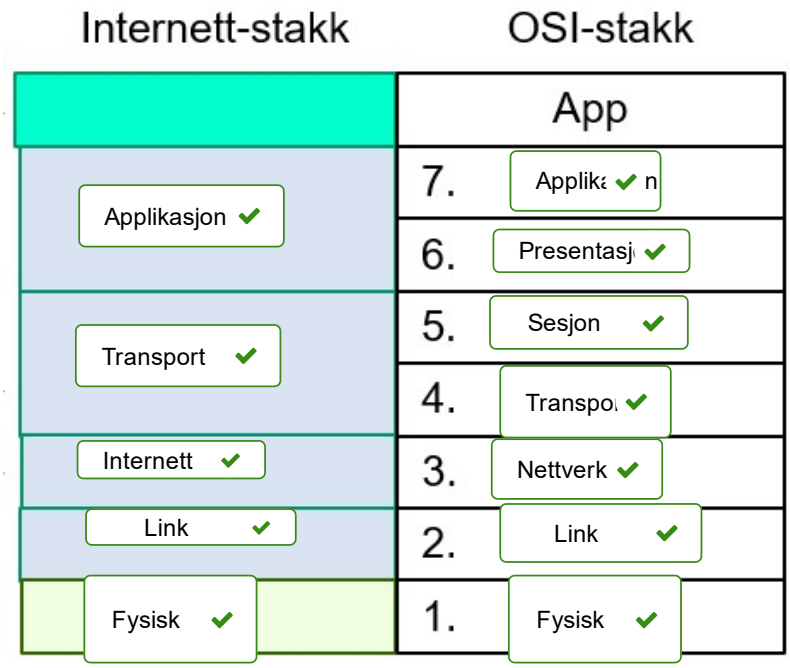
Maks poeng: 2

28 Protokollstack

Flytt protokollnavn til riktig plass i protokollstakkene for internett og OSI. Riktig svar gir 0.5 poeng, galt svar -0.5. Minimum 0, maks 6 poeng.

Hjelp

Link	Presentasjon	Nettverk
Internett	Fysisk	Transport
Applikasjon	Sesjon	



Maks poeng: 6

29 Mørke IP-adresser

Virksomheten din har reservert enkelte ip-adresser mot å bli brukt. Dette kalles mørke ip-adresser, forklar kort (maks 25 ord) hvorfor dette gjøres for å øke sikkerheten.
Oppgaven gir fire poeng.

Skriv ditt svar her

Format

Oppgaven gir totalt 4 poeng.

1p for å navngi, eller beskrive at dette er en honeypotløsning, men 0p hvis svaret tydeligvis viser forvirring mellom dette, og ekte honeypotter (altså faktiske maskiner som er satt opp og som angriperen faktisk kan interagere med).

1p for å nevne at hensikten med dette er deteksjon.

1p for å si at deteksjon gjøres enkelt fordi all trafikk mot IP-adressene er illegitim.

1p for å skrive noe om at dette er en effektiv måte å finne kompromitterte klienter i et nett.

Words: 0/25

Maks poeng: 4

i Del 5: Autentisering og IAM

30 eID-leverandører

BankID, Buypass, Commfides og MinID er såkalte eID-leverandører. Velg om hvert utsagn er sant eller usant.

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

Si om hvert utsagn er sant eller usant.

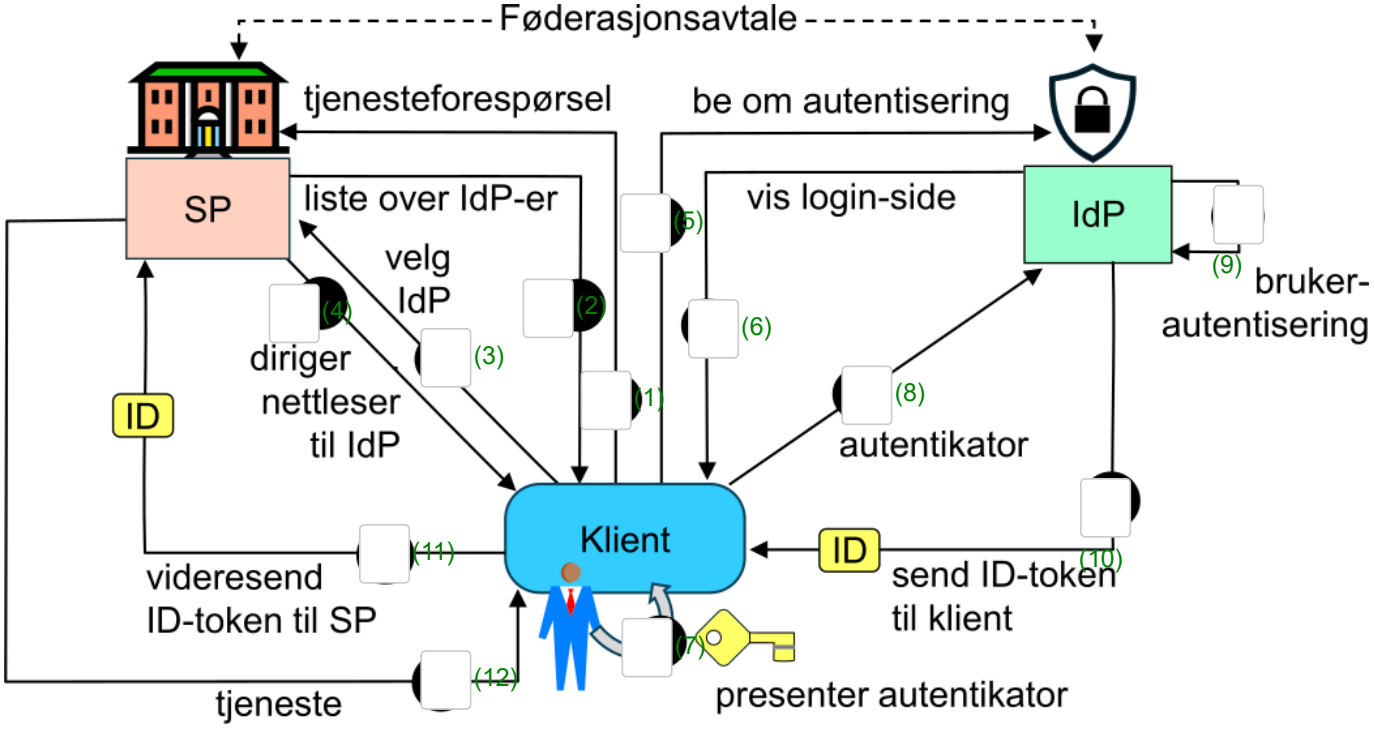
	Usant	Sant
Alle disse eID-leverandørene er statlige tjenester.	✔	
Alle disse eID-leverandørene kan brukes for å logge på nettbanker.	✔	
Alle offentlige tjenester på internett krever autentiseringsnivå HØYT.	✔	
Alle disse eID-leverandørene kan brukes for å logge seg på offentlige tjenester på internett (e-forvaltning).		✔

Maks poeng: 2

31 Open ID Connect

Figuren viser scenarioet for brukerautentisering med OIDC. Sett inn tall 1 - 12 i hver melding for å vise rekkefølgen av meldingene i scenarioet.

Poeng: 0,25 for korrekt tall, 0 for for feil eller intet tall, maks 3, minimum 0.



Maks poeng: 3

i Del 6: ISMS og risikostyring

32 NSMs grunnprinsipper og NIST CSF

NSMs grunnprinsipper for IKT-sikkerhet, og NIST CSF (Cybersecurity Framework) er to standarder/veiledere for informasjonssikkerhet. Indiker om hvert utsagn nedenfor gjelder for NSM, NIST, begge eller ingen.

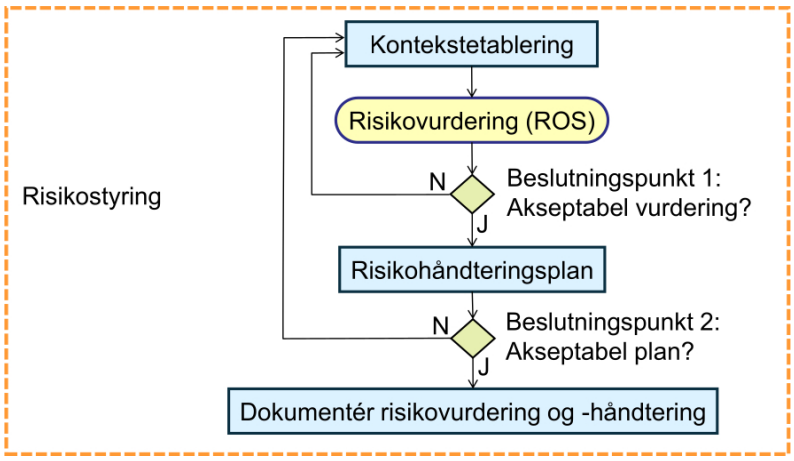
Poeng: 0,5 for hver riktig; -0,5 for hver feil; 0 for ubesvart; maks 2, minimum 0.

Indiker hva som gjelder for hvert utsagn.

	NSM	NIST	begge	ingen
Kategoriserer sikkerhetstiltak etter sikkerhetsfunksjoner/prosesser (f.eks. kartlegge, beskytte, oppdage, håndtere)	○	○	○ ✔	○
Standarden/veilederen må kjøpes	○	○	○	○ ✔
Er publisert på norsk	○ ✔	○	○	○
Kan brukes sammen med ISO/IEC 27001	○	○	○ ✔	○

Maks poeng: 2

33 Beslutningspunkter for risikostyring



Figuren for risikostyring viser to beslutningspunkter.

Velg relevant(e) grunn(er) til å svare "Nei" på beslutningspunkt 1
Velg ett eller flere alternativer

- [ ] Virksomheten må først gjennomføre OSINT.
- [ ] Relativt dårlig spredning av risikonivåer. ✔
- [ ] Det hersker fremdeles stor uvisshet rundt en eller flere høye risikoer. ✔
- [ ] Utilstrekkelig budsjett for å innføre sikkerhetstiltak.

Nevn relevant(e) grunn(er) til å svare "Nei" på beslutningspunkt 2.
Velg ett eller flere alternativer

- [ ] Det må først gjennomføres OSINT.
- [ ] Det er for mange aksepterte risikoer. ✔
- [ ] Alle risikoene har omtrent samme nivå.
- [ ] Utilstrekkelig budsjett til foreslåtte sikkerhetstiltak. ✔

Poeng: 0,5 for riktig, -0,5 for feil, 0 for ubesvart, minimum 0.

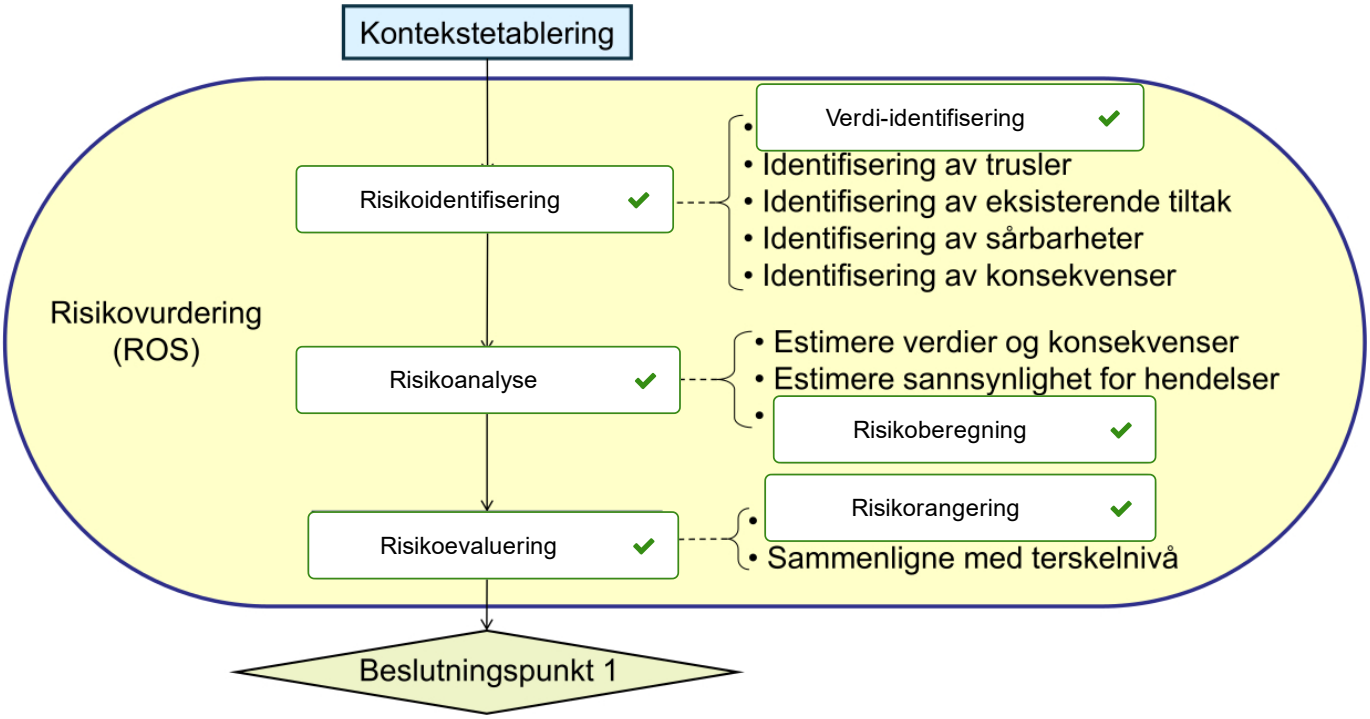
Maks poeng: 2

34 Prosess for risikovurdering

Figuren nedenfor viser prosess for risikovurdering der noen av trinnene mangler beskrivelse.
Sett inn elementene i riktig felt for å beskrive trinnene.
Poeng: 0,5p for hver riktig; -0.5p for hver feil; 0p for ubesvart; 3p for alle riktig; minimum 0p.

Hjelp

Risikoanalyse	Risikorangering	Verdi-identifisering
Risikoidentifisering	Risikoevaluering	Risikoberegning



Maks poeng: 3

35 ISMS

Hva er riktig om ISMS (Information Security Management System)?
Poeng: 0,5 for riktig, -0,5 for feil, 0 for ubesvart.
Velg ett eller flere alternativer

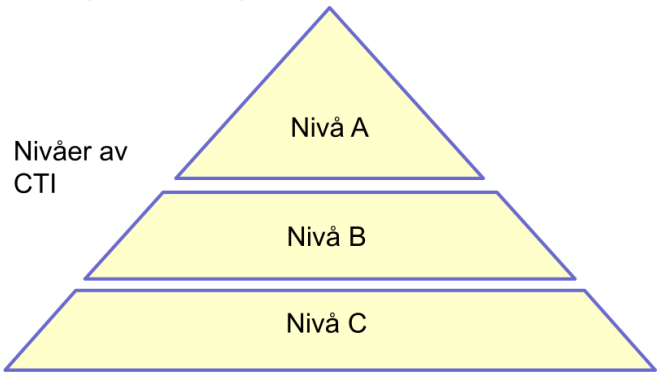
- [ ] Det er et sett med policyer og prosedyrer for informasjonssikkerhet. ✔
- [ ] NSMs grunnprinsipper for IKT-sikkerhet er et ISMS.
- [ ] Det betyr det samme som ledelsessystem for informasjonssikkerhet. ✔
- [ ] Det er en applikasjon som styrer sikkerheten i virksomheter.

Maks poeng: 1

Del 7: Cyberoperasjoner

36 CTI

CTI (Cyber Threat Intelligence - digital trusseletterretning) deles typisk inn i tre hovednivåer, som vist på figuren nedenfor. Bokstavene A, B og C er bare uspesifikke navn, som representerer egentlige spesifikke typer CTI for hvert nivå. Poeng: 0,5p for hver riktig, 0p for feil eller ubesvart, maks 3p, minimum 0p.



Nivå A kalles [ ] (strategisk, strategic) CTI.

Nivå B kalles [ ] (taktisk/operasjonell, taktisk, operasjonell, tactical/operational, tactical, operational, TTP, operativ) CTI.

Nivå C kalles [ ] (teknisk, angrepsindikatorer, attackidentifierare, angrebsindikatorer, indicators of compromise, technical) CTI.

Er du i tvil om stavemåte for oppgavene over, spør faglærer.

MITRE ATT&CK beskriver CTI-elementer på [Velg alternativ] (nivå A, nivå B, nivå C).

Den mest detaljerte CTI er på [Velg alternativ] (nivå A, nivå B, nivå C).

Den mest kortvarige CTI er på [Velg alternativ] (nivå A, nivå B, nivå C)

Maks poeng: 3

37 Cyberkrigføring

Land A har et begrenset budsjett for å drifte sin militære cyberavdeling. Velg realistisk praksis som cyberavdelingen kan benytte for å bli selvfinansiert, slik at den ikke belaster statsbudsjettet. Du kan anta at land A ikke har etiske eller moralske skrupler med hensyn til cyberkrigføring.

Velg ett eller flere alternativer

- [ ] Gjennomføre OSINT mot andre land
- [ ] Angrip andre land med løsepengevirus ✔
- [ ] Drifte en TOR-node
- [ ] Selge nulldagssårbarheter ✔

Anta at land A planlegger et militært angrep på land B. Den militære cyberavdelingen i land A har et begrenset arsenal av exploits. Velg den/de mest fornuftige måten(e) blant alternativene under for land A å benytte sitt exploit-arsenal.

Velg ett eller flere alternativer

- [ ] Benytt exploit-arsenalet i innledende fase av militærangrepet ✔
- [ ] Benytt exploit-arsenalet for å svekke land B i ukene og månedene før militærangre ✔
- [ ] Benytt exploit-angrepet for å angripe land B med NMAP.
- [ ] Selg exploit-arsenalet for å tjene penger.

Poeng: 0,5 for riktig, -0,5 for feil, 0 for ubesvart.

Maks poeng: 2

ℹ Del 8: Retten er satt

38 Retten er satt

Alice (10.0.0.15), Bob(10.0.0.33, mac-adresse: 34-24-d8-02-24), Charlie (10.0.0.155) og Stine (10.0.0.184) kommuniserer på et internt datanett. De signerer meldingene sine med en å legge med en MAC (Message Authentication Code), generert med felles nøkkel.

En dag får Alice en melding (per TCP), som tilsynelatende kommer fra Bob. Meldingen er signert, og kommer fra Bobs IP-adresse (10.0.0.33). Bob nekter for å ha sendt denne meldingen.

Bobs venn Charlie har lagt med en kopi av sin arp-tabell fra tiden da pakkene ble sendt.

```
PS C:\Users\charlie> arp -a
Internet Address      Physical Address      Type
10.0.0.15             98-77-e7-ef-06-27     dynamic
10.0.0.33             28-47-d7-ff-06-57     dynamic
10.0.0.155            44-00-4e-00-00-fc     static
10.0.0.184            28-47-d7-ff-06-57     dynamic
```

Du skal hjelpe Bobs advokat med å frikjenne Bob. Du må med andre ord hjelpe til med å finne alternative, men rimelige løsninger som skaper rimelig tvil om saken.
Løsningen bør beskrive beskrive hvem andre enn Bob som kan stå bak.

Du skal altså beskrive hvordan angrepet har blitt gjennomført, basert på hva du har lært i IN2120. En god løsning bør håndtere både bruken av signatur og Bobs IP-adresse.

"Rimelig tvil i straffesaker" er her definert som: "Det er ikke enhver teoretisk tvil som skal komme tiltalte til gode, men kun dersom det er en fornuftig rimelig tvil ved det faktum som må legges til grunn for at handlingen er straffbar. Med andre ord at det er en reell og ikke bare en teoretisk mulighet for at faktum ikke er riktig, slik aktor har lagt det frem." (jusinfo.no)

Oppgave A: Beskriv hvorfor bruken av denne typen signaturer ikke kan brukes til å sikkert identifisere Bob (hvem kan ha generert MAC-signaturen) (2poeng).

Oppgave B; Beskriv en annen, og sikrere, metode som hadde unikt kunnet identifisere avsender (1 poeng). (Svar kort)

Oppgave C: Navngi angrepet som er blitt benyttet (2 poeng) (svar kort)

Oppgave D: Identifiser hvem som (mest trolig) står bak (3 poeng). (Begrunn, men maks to setninger)

Oppgave E: Navngi ett verktøy som kan ha vært brukt til å gjennomføre angrepet (1 poeng).

Oppgave F: Navngi ett verktøy som kan brukes til å generere falske pakker (1 poeng).

Skriv ditt svar her

Format

Oppgaven gir totalt 10 poeng.

A) 2p for å forklare at alle de fire aktuelle personene kan ha laget signaturen - da signaturen lages med samme felles nøkkel som alle har.

B) 1p for å navngi, eller beskrive PKI og asymmetriske signaturer.

C) 2p
2p for å beskrive hvordan dette er et Man-in-the-middle-angrep (MiTM). Bare 1p for å si at dette er et IP-spoofingangrep, med en mer eller mindre legitim grunn til at Bob i Charlies ARP-tabell har Stines MAC-adresse.

D) 3p
2p for å forklare hvordan Stine mest sannsynlig står bak, da Bobs IP-adresse har Stines MAC-adresse.

1p For å skriver noe om alternative, men potensielt riktige løsninger, eksempelvis at Charlie står bak og at han har forfalsket outputen fra sin ARP-tabell for å legge skylden på Stine.

Selve oppgaveteksten sier de skal hjelpe til med å frikjenne Bob, så svar som viser stakkars Bobs skyld gir 0p.

E) 1p for Ettercap, Bettercap, eller andre relevante verktøy.

F) 1p for Hping3, Scapy, men også svar som "genererer falske pakker i programmeringsspråk x ved hjelp av pakke y", eller annet relevant.

Words: 0

Ps: Til studenter med juridisk kompetanse - Bobs advokat snakker flytende jus, og trenger ingen juridisk hjelp. Ikke bruk tid eller plass på juridiske betraktninger, de gir ingen poeng i oppgaven. I oppgaven ønskes et rent IT-teknisk svar.

Maks poeng: 10

Slutt

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