Informasjon om eksamenen

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Avsluttende eksamen i IN2120 Informasjonssikkerhet (Høst 2023).

Dato og tidspunkt: **27. november 2023, kl.9:00 - 13:00 (4 timer).**

Ingen hjelpemidler er tillatt.

Merk følgende:

- Oppgavene i denne eksamenen er gruppert i syv deler. Den første delen dekker grunnleggende aspekter ved informasjonssikkerhet på tvers av pensum, mens de øvrige seks delene er fra utvalgte områder av pensum.
- Det er mulig å oppnå 40 poeng i den første delen av oppgavesettet, og ti poeng for hver av de neste seks delene - totalt 100 poeng (= 100%).
- 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 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, Gudmund og Nils!

Del 1: Generelt

1 Begreper

Figuren nedenfor viser tre typer gjerder/grenser som gir enten sikkerhet (security), trygghet (safety) eller visshet (certainty). Sett inn tekstelementene i tilhørende riktig felt.
Poeng: 1 for hver riktig; 0 for feil/ubesvart; 3 for alle riktig; minimum 0.

Hjelp

Visshet | Sikkerhet | Trygghet

grensemerke

stillas

piggtrådgjerde

Maks poeng: 3

2 Kilder til krav om informasjonssikkerhet

Risikovurdering og regelverk er to ulike kilder til krav om informasjonssikkerhet. For hver type krav, indiker om "forsvarlig nivå" eller "samsvar" avgjør om kravene er oppfylt.
Poeng: 1 for hver riktig; -1 for hver feil; 0 for ubesvart; maks 2; minimum 0.
Indiker hva som avgjør om krav er oppfylt.

	Forsvarlig nivå	Samsvar
Krav om å begrense sikkerhetsrisiko	○	○
Juridiske, lovbestemte, regulatoriske og kontraktsmessige krav	○	○

Maks poeng: 2

3 Sikkerhetsmålsettinger

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

	Konfidensialitet	Integritet	Tilgjengelighet
Løsepenge/krypto-virus	○	○	○
DDoS-angrep	○	○	○
DoS-angrep	○	○	○
Avlytting av datatrafikk	○	○	○
Skadevare genererer tilfeldig input i database	○	○	○
Knekke kryptering	○	○	○

Maks poeng: 3

4 Bokstyper for testing

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

Velg ett alternativ:

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

Maks poeng: 1

5 OS privilegienivåer

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

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

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

	Kan IKKE få tilgang	Kan 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: 1 for hver riktig; 0 for hver feil/ubesvart; maks 4; minimum 0.

Indiker hva hvert utsagn passer beste med.

	Asymmetrisk kryptering	Hash-funksjon	Symmetrisk kryptering	PKI
Krypterer og dekrypter med samme nøkkel	○	○	○	○
Bruker en nøkkel for kryptering og en annen nøkkel for dekryptering	○	○	○	○
Garantere autentisitet av offentlige nøkler og forenkler nøkkeldistribusjonen	○	○	○	○
Er en-veis som betyr at det er praktisk umulig å finne tilbake til input av den	○	○	○	○

Maks poeng: 4

7 Asymmetrisk krypto

I denne oppgaven får du 1 poeng for hvert riktige svar; 0 poeng for hver feil eller ubesvart; totalt maks 2 poeng; minimum 0 poeng.

Bob vil sende en kryptert melding til Alice ved hjelp av asymmetrisk krypto. Hvilken nøkkel bruker han?

Velg ett alternativ:

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

Alice vil dekryptere meldingen fra Bob - da bruker hun hvilken nøkkel?

Velg ett alternativ

- Bobs private nøkkel
- Alice sin offentlige nøkkel
- Bobs offenlige nøkkel
- Alice sin private nøkkel

Maks poeng: 2

8 Programmer

Her er noen programmer som er benyttet i kurset - plasser riktig program til riktig utsagn.
Poeng: 1 for hver riktig; -1 for hver feil; 0 for ubesvart; maks 4; minimum 0.

Hjelp

mimikatz | John the ripper | nmap | Wireshark

Et mye brukt program for å finne ut av hvilke porter som er åpne på en maskin: _____ .

Vi har knekt passord ved hjelp av: _____

Og vi har lastet ned klartekstpassord fra minne ved hjelp av: _____

I tillegg til det har vi undersøkt nettverkspakker ved hjelp av: _____

Maks poeng: 4

9 Passord

Du må bytte passordet ditt. Det gamle passordet var "JuleferienHytte2022" som du endret til "JuleferienHytte2023".
Systemet sier at passordene er for like, hva vet du da om hvordan systemet lagrer passord?

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

Velg ett alternativ:

- MiTM
- Hashet
- Klartekst
- Layered defense

Maks poeng: 1

10 Sikkerhetsprotokoller

Vi har diskutert flere sikkerhetsprotokoller i kurset, der to er nevnt nedenfor. Indiker de to forkortelsene nedenfor som er sikkerhetsprotokoller.
Poeng: 1 for hver riktig; -1 for hver feil; 0 for ubesvart; maks 2; minimum 0.
Velg to alternativer

- [ ] TLS
- [ ] IP
- [ ] IPSEC
- [ ] UDP
- [ ] DNS
- [ ] HTTP

Maks poeng: 2

11 Datanettsikkerhet

Velg det mest passende begrepet i hver setning nedenfor.
Poeng: 1 for hver riktig; 0 for hver feil eller ubesvart; maks 3, minimum 0.

En Velg alternativ (TLS-inspeksjon, IDS, autentiseringstjener, brannmur) er et sjekkpunkt som beskytter de interne nettverkene mot angrep fra eksterne nettverk, og bestemmer hvilken trafikk som kan passere inn og ut.

Velg alternativ (IDS, TLS-inspeksjon, Diffie-Hellman, Anomalideteksjon) brukes av noen organisasjonser for å lese kryptert HTTPS-trafikk som går inn og ut av organisasjonen ved å bryte krypteringen.

Snort er et eksempel på en Velg alternativ (signatur-basert IDS, pakkefilter, applikasjonsbrannmur, APT)

Maks poeng: 3

12 Cyber Kill Chain

For hver beskrivelse nedenfor, velg hvilket steg i cyber-kill-chain som beskrivelsen passer til.
Poeng: 1 for hver riktig; 0 for hver feil eller ubesvart; maks 2; minimum 0.

Som en del av en cyberoperasjon utvikler en trusselaktør en exploit-skadevare som utnytter en sårbarhet som ikke har blitt patchet i en tjeneste som virksomheten din har. Hvilket steg av cyber-kill chain er dette et eksempel på?
Velg ett alternativ:

- Rekognisering
- Bevæpning
- Overlevering
- Utførelse av exploit
- Innstallering
- Kommando og kontroll
- Måloppnåelse

Denne exploiten legges på en USB-minnepinne og en deltidsansatt bestikkes til å koble denne til maskinen til sjefen sin. Hva kalles steget når USB-en settes inn i maskinen?
Velg ett alternativ

- Rekognisering
- Bevæpning
- Overlevering
- Utførelse av exploit
- Innstallering
- Kommando og kontroll
- Måloppnåelse

Maks poeng: 2

13 ID-modeller

Da jeg var i Stockholm tidligere i år logget mobilen min seg på Internett via Eduroam med UiO-brukeren min. Jeg hadde ikke gjort noe for å logge meg på, men standard-pålogging fra UiO fungerte. Hva sier det om ID-modellen som Eduroam bygger på?

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

Velg riktig ID-modell:

- NFC
- Føderert
- Bell-LaPaduala
- Silo

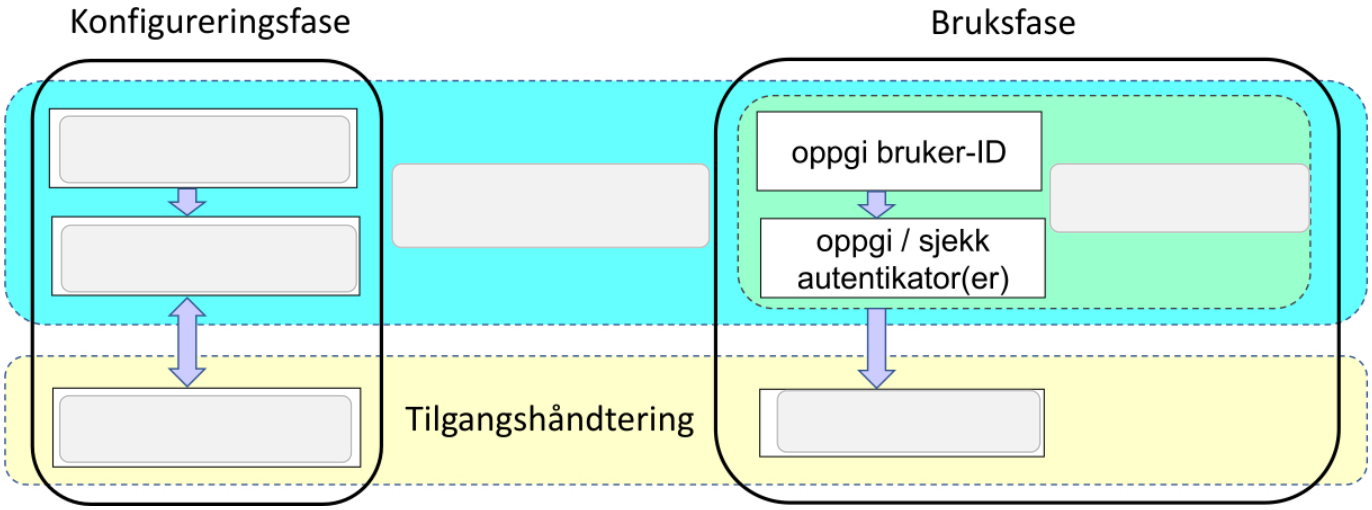
Maks poeng: 1

14 IAM

Figuren nedenfor viser faser og trinn for IAM (dentitets- og tilgangshåndering). Flytt elementene til riktig felt i figuren.
Poeng: 0,5 for hver riktig; 0 for ubesvart/feil; 3 for alle riktig; minimum 0.

Hjelp

Tilgangsautorisering	Tilgangskontroll
Identitetshåndtering	Brukerregistrering
Brukerautentisering	Autentikatorklargjøring



Maks poeng: 3

15 Meldingsautentisering

For hver setning nedenfor, velg begrepet som passer inn.
Poeng: 1 for hver riktig; 0 for hver feil eller ubesvart; maks 3, minimum 0.

Digital signatur gir Velg alternativ (enkel, ubenektelig, fremoverhemmelig, phishingresistent) meldingsautentisering.

MAC (Message Authentication Code) gir Velg alternativ (ubenektelig, enkel, phishingresistent, fremoverhemmelig) meldingsautentisering.

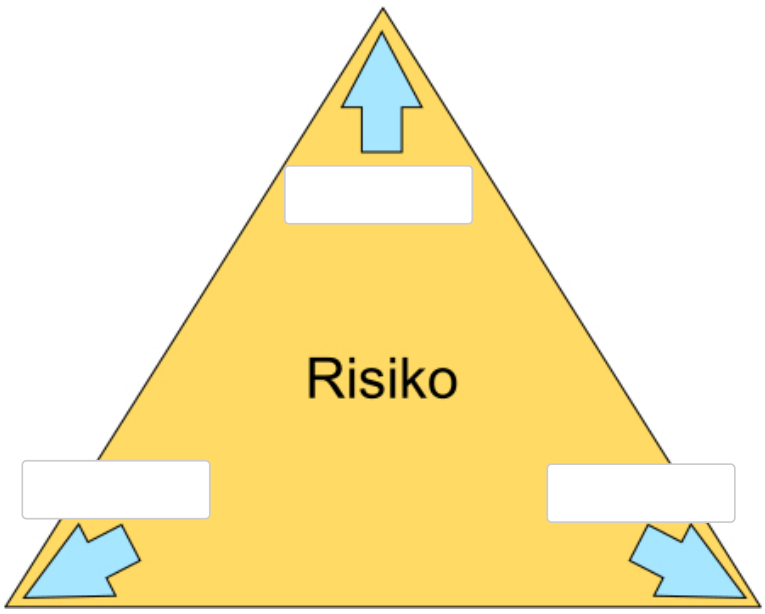
Tap/tyveri av en privat nøkkel gir grunnlag for å Velg alternativ (benekte en phishingresistent meldingsautentisering, benekte en fremoverhemmelig meldingsautentisering, benekte en melding autentisert med MAC, benekte en digitalt signert melding).

Maks poeng: 3

16 Risikotrekanten

Figuren nedenfor viser risikotrekanten der hvert hjørne representerer et fundamentalt risikoaspekt. Skriv navnet på hvert risikoaspekt i hvert sitt hjørne. 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

17 Egenskaper til krypto

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

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

En meldingautentiseringskode (MAC) 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 feil
- Påstanden er riktig

SHA-2 algoritmen har blitt brukt, men "Sorte hull" påstår at denne ikke lenger er sikker så resultatene kan ikke brukes. Hva er riktig om SHA-2?
Velg ett alternativ

- SHA-2 anses som usikker
- SHA-2 anses som sikker

Sensitiv informasjon fra kommunikasjonen mellom "Sikkert og visst" og "Sorte hull" har kommet til avveie. "Sorte hull" sier at de ikke har lekket informasjonen med vilje.
Øktnøklene som er brukt har blitt sendt fra "Sikkert og visst" til "Sorte hull" og har blitt kryptert med "Sorte hull" sin offentlige nøkkel. "Sorte hull" har blitt utsatt for et dataangrep hvor deres private nøkkel har blitt hentet ut. "Sorte hull" påstår dermed at en tredjepart kan ha kunne dekryptert all kommunikasjon. Hva er riktig om påstanden til "Sorte hull"?
Velg ett alternativ

- Påstanden er feil siden man krypterer ikke med offentlige nøkler så dette stemmer ikke.
- Påstanden er feil siden asymmetrisk kryptering er det samme som Diffie-Hellman, så dette stemmer ikke.
- Påstanden er riktig siden måten øktnøkler utveksles ikke gir fremoverhemmelighold.

Maks poeng: 3

18 Nøkkelsertifikat

Denne oppgaven omhandler nøkkelsertifikater og du må velge passende svar på nedtrekksmenyen.
Poeng: 1 for hvert riktig; 0 for ubesvart eller feilt; maks 2; minimum 0.

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

GEANT OV RCC CA 4 er et eksempel på Velg alternativ (mellomliggende CA, rot-CA, subjeksertifikat).

Hvem har signert USERTrust ECC Certification Autohority? Velg alternativ (GEANT OV ECC CA 4, PKI, Selv-signert)

Maks poeng: 2

19 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 1; minimum 0.

Hva kalles standarden som brukes for public-key nøkkelsertifikater på internett ?

Fyll in svaret her:

Maks poeng: 1

20 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.

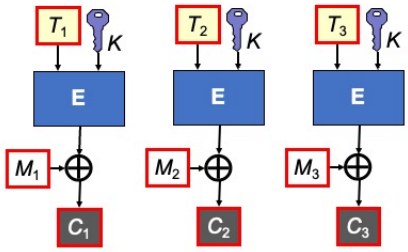
Poeng: 1 for hver riktig; -1 for hver feil; 0 for ubesvart; totalt maks 2; totalt minimum 0.

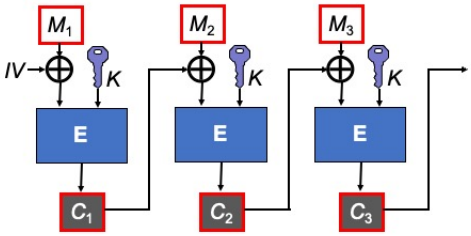
Hjelp

Electronic Code Book (ECB)

Cipher Block Chaining (CBC)

Counter Mode (CTR)





Maks poeng: 2

21 Hash-funksjoner

En kollega av deg har implementert en funksjon H som legger 1 til hvert element fra input.

For å illustrere: H(1)=2, H(3)=4, H(123) = 124 osv.

Du kan anta at hver input generer en unik output-verdi.

Ekte hash-funksjoner har et sett sikkerhetskrav som må oppfylles, og H oppfyller bare 2 av disse. Hvilke?

Poeng: 1 for hver riktig; -1 for hver feil; 0 for ubesvart; maks 2; minimum 0.
Velg de 2 sikkerhetskravene for hashfunksjoner som H oppfyller

- [ ] Kollisjonsresistent
- [ ] Lett å beregne
- [ ] Komprimering til fast størrelse
- [ ] Enveis-funksjon

Maks poeng: 2

Del 3: Angrepsvektorer og skadevare

22 Tilgang for skadevare

Du kjører uheldigvis skadevare på maskinen din med din bruker. Brukerkontoen din har fulle sudo-rettigheter på maskinen din, og kjører følgende kommando:

Hvilke rettigheter får skadevaren da?
Poeng: 1 for riktig, 0 for feil eller ubesvart.
Velg ett alternativ:

- root
- bruker (nilspw)
- administrator
- gjest

Maks poeng: 1

23 Phishing

Hva slags phishing-angrep er dette (Se for deg at du som student får denne teksten i en epost i morgen (altså dagen etter eksamen i IN2120) fra et navn du ikke kjenner)?

"Hei <ditt navn>,
Hvordan gikk eksamen i går? Jeg er ganske fornøyd selv, særlig de første oppgavene gikk greit. Beklager at jeg ikke har tatt kontakt med deg før, men jeg har ikke turt å ta kontakt på forelesningene i høst. Jeg så hvor flink du var i gruppetimene og lurte på om vi kunne samarbeide neste semester. Du finner mer detaljer om min bakgrunn her: https://<langUrl>.<endaLengreUrl>.<noe>"

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

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

Maks poeng: 1

24 Skadevare

Velg den kolonnen som passer best med hver rad.

Poeng: 1 for hver riktig, -1 for hver feil, 0 for ubesvart, 4 for alle riktig, minimum 0.

Finn de som passer sammen:

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

Maks poeng: 4

25 Skadevarebegreper

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

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

Hjelp

Command injection | Rootkit | MiTM | SQL-injection

"aabbasdfj ' or 254 > 55" [ ]

"a && cat /etc/passwd" [ ]

Et program som brukes til å skjule spesielle prosesser: [ ]

Maks poeng: 3

26 Logganalyse

En person fra IT-drift kommer løpende til deg - og sier "Vi er under angrep, se på loggen!" - hva er mest sannsynlig at har skjedd?
Ett poeng for riktig svar, ellers null.

Tid	IP	Trafikk	
21.10.2023 - 20:48:00	10.10.127.34 > 10.1.23.23	User:admin	Pass:Admin
21.10.2023 - 20:48:00	10.10.127.34 > 10.1.23.23	User:admin	Pass:admin
21.10.2023 - 20:48:01	10.10.127.34 > 10.1.23.23	User:admin	Pass:Passw0rd
21.10.2023 - 20:48:01	10.10.127.34 > 10.1.23.23	User:admin	Pass:eeeSSDF
21.10.2023 - 20:48:02	10.10.127.34 > 10.1.23.23	User:admin	Pass:in2120
21.10.2023 - 20:48:02	10.10.127.34 > 10.1.23.23	User:admin	Pass:Sommerferie
21.10.2023 - 20:48:03	10.10.127.34 > 10.1.23.23	User:admin	Pass:Juleferie!
21.10.2023 - 20:48:03	10.10.127.34 > 10.1.23.23	User:admin	Pass:Pentest

Velg ett alternativ:

- Falsk alarm
- Command-injection
- SQL-injection
- Passordspraying

Maks poeng: 1

i Del 4: Pentesting

27 Passordknekking

Du knekker passord ved hjelp av uttømmende søk (I oppgaven benyttes bare tall - tenk koden til et vanlig betalingskort). Systemet har gått fra fire til seks tall. Hvor mye mer komplekst blir passordet?
Poeng: 1 for riktig; 0 for feil eller ubesvart; maks 1, minimum 0.
Velg ett alternativ:

- Hundre ganger
- 10 ganger
- Umulig å si
- 95 Ganger

Maks poeng: 1

28 Matchende begrep

Denne oppgaven gir 1 poeng hvert riktig svar, -1 poeng for hvert gale svar, maks 4 poeng, minimum 0 poeng.
NB: at svarene er i "gåsøyne" er for å unngå konverteringer i inspera - se bort fra dem.

Finn de som passer sammen:

	SQL-injection	Kartlegging	Fuzzing	Phishing	Command-injection
"a' or 1 == 1"	○	○	○	○	○
"ss' or 34 -lt 754"	○	○	○	○	○
"blah && whoami"	○	○	○	○	○
nmap	○	○	○	○	○

Maks poeng: 4

29 Misbruk av sudo

I løpet av en pentest har du funnet passordet til en bruker som kan logge inn på en maskin gjennom ssh. Du logger inn og sjekker rettigheter – se bildet under.

Nevn to måter å misbruke sudo-rettighetene du ser på bildet til å oppnå root-tilgang.
Du trenger ikke å gi uttømmende svar her, skriv en eller maks to setninger for hver måte du nevner.
Hver måte (tekst) gir 2 poeng, men det er mulig å oppnå totalt 5 poeng hvis du skriver en tilnærmet fungerende kode (pseudokode) for å gjennomføre ett av angrepene (altså den delen av angrepet som krever sudo).

Skriv ditt svar her

Format

Words: 0

Maks poeng: 5

Del 5: Nettverkssikkerhet

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

For Velg alternativ (både TLS og IPSec, TLS (men ikke IPSec), IPSec (men ikke TLS)) krypteres all applikasjonsdata.

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

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 innholdet (i klartekst), alt innhold og IP-adresse til endelig destinasjonen, bare IP-adresse til endelig destinasjonen (og ikke ukryptert innhold))

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

Maks poeng: 5

31 Inntrengingsdeteksjon

Firmaet "Detekt i takt" har spesialisert seg på inntrengingsdeteksjon (IDS), og bruker både signatur-basert og anomali-basert inntrengingsdeteksjon. I den forbindelse er det tre spørsmål du må svare på.
Poeng: 1 for hvert riktig; 0 for hver feil eller ubesvart; maks 3; minimum 0.

Hvilken IDS-type er ofte basert på maskinlæring?
Velg ett alternativ

- Anomali-basert
- Signatur-basert

Det går en alarm fra en sårbarhet som nylig har blitt oppdaget men ikke blitt patchet. Hvilken type IDS kan ha generert alarmen?
Velg ett alternativ

- Dette er en kjent sårbarhet som betyr at det må ha vært signatur-basert
- Kan både ha vært fra anomali-basert og signatur-basert
- Det må ha vært fra en anomali-basert siden sårbarheten ikke har blitt patchet

"Detekt i takt" har tidligere laget følgende Snort signatur:

```
alert tcp 1.2.3.4 any -> 5.6.7.8 443 (msg "")
```

Avdelingen for "utvikling av nye signaturer", som du nylig har begynt å jobbe i, har fått i oppdrag å lage mer beskrivende meldinger i signaturene. I dette tilfellet får man ingen informasjon (msg ""), og du har blitt bedt om å forbedre beskrivelsen. Du kan anta standard bruk av portnummer. Velg den mest passende meldingen som beskriver hva signaturen over gjør?
Velg ett alternativ:

- "SSH til IP-adresse 5.6.7.8“
- "Ukryptert trafikk til 5.6.7.8"
- "HTTPS trafikk fra 5.6.7.8 til 1.2.3.4 "
- "HTTPS trafikk fra 1.2.3.4 til 5.6.7.8"

Maks poeng: 3

32 Konfigurasjon av brannmur

Du er innleid som konsulent til firmaet "Frem og tilbake".

"Frem og tilbake" har i nettverket separert forretningslogikken inn i et eget indre segment, mens web-tjeneren står i det ytre segmentet.

Disse segmentene er separert med en dedikert brannmur, som for øyeblikket er stilt inn til å ikke slippe gjennom noe trafikk til det indre segmentet.

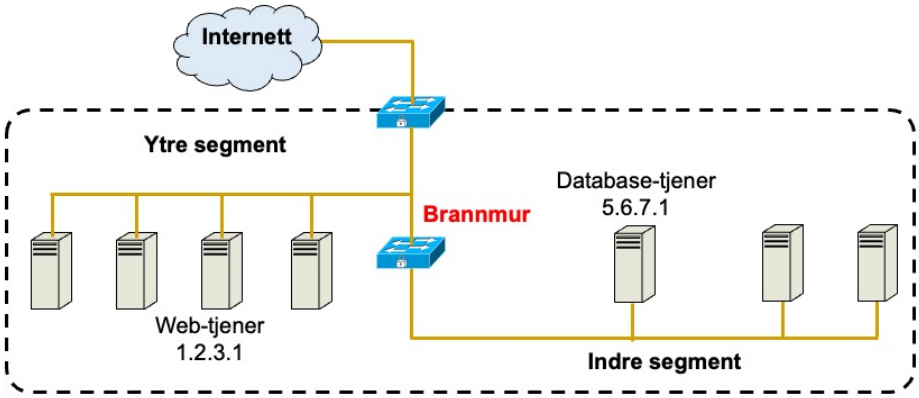
Dette har vist seg å være for restriktivt og du har derfor blitt bedt om å oppdatere brannmuren slik at trafikk fra web-tjeneren (i det ytre segment) til database-tjeneren (i det indre segmentet) skal slippes gjennom.

Du blir gitt følgende informasjon:

- Web-tjeneren har IP-adresse 1.2.3.1
- Database-tjeneren har IP-adresse 5.6.7.1
- Selve database-tjenesten kjører på port 1433 og det er kun trafikk til denne tjenesten som skal godtas.

Brannmuren skal kun slippe gjennom denne trafikken og ikke noe annen trafikk.

Følgende diagram illustrerer denne nettverksarkitekturen:



Brannmuren som brukes er et mye brukt pakkefilter for Linux som du kjenner igjen fra både forelesning og oblig i IN2120. Du husker derimot ikke alle argumentene, så du slår dette opp og finner følgende informasjon om argumentene som kan være nyttig:

- -A <liste> hvor <liste> kan være: OUTPUT, INPUT eller FORWARD
- -s <IP-adresse> spesifiserer IP-adressen(e) til avsender
- -d <IP-adresse> spesifiserer IP-adressen(e) til mottaker
- --sport <portnummer> spesifiserer portnummer til avsender
- --dport <portnummer> spesifiserer portnummer til mottaker
- -p <proto> spesifiserer protokoll brukt
- -j <result> hvor <result> kan være DROP eller ACCEPT

Gi kommando med riktige argumenter for å oppdatere brannmuren som beskrevet over.

Du får 2 poeng for helt riktig svar; 1 poeng for delvis riktig svar; 0 poeng i alle andre tilfeller. Merk at det ikke vil trekkes poeng for feil rekkefølge av argumentene.

Skriv kommando med riktige argumenter her:

Maks poeng: 2

Del 6: Autentisering og IAM

33 Passnøkler

Phishingresistent autentisering med passnøkler (også kalt FIDO eller WebAuthn) er et aktuelt tema. Indiker om hvert av utsagnene nedenfor er sant eller usant.

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

Si om hvert utsagn er sant eller usant.

	Sant	Usant
En passnøkkel inneholder autentiseringstjenerens URL.	○	○
Selv om phishingresistent autentisering gjør at brukeren advares om falske nettsider, kan brukeren i nettleseren velge å ignorere advarselen.	○	○
Hver bruker har kun én passnøkkel som benyttes for ulike nettsteder.	○	○
En passnøkkel er en privat (asymmetrisk) kryptografisk nøkkel.	○	○
Brukere som mister enheter der passnøkler er lagret må generere nye passnøkler.	○	○
Brukerautentisering med passnøkler foregår i to etapper, en lokal, og en online.	○	○

Maks poeng: 3

34 Identitetshåndtering

Si om utsagnene om identitetshåndtering er korrekt eller feil.
Poeng: 0,5 for hver korrekt; -0.5 for for hver feil; 0 for ubesvart; maks 3; minimum 0.

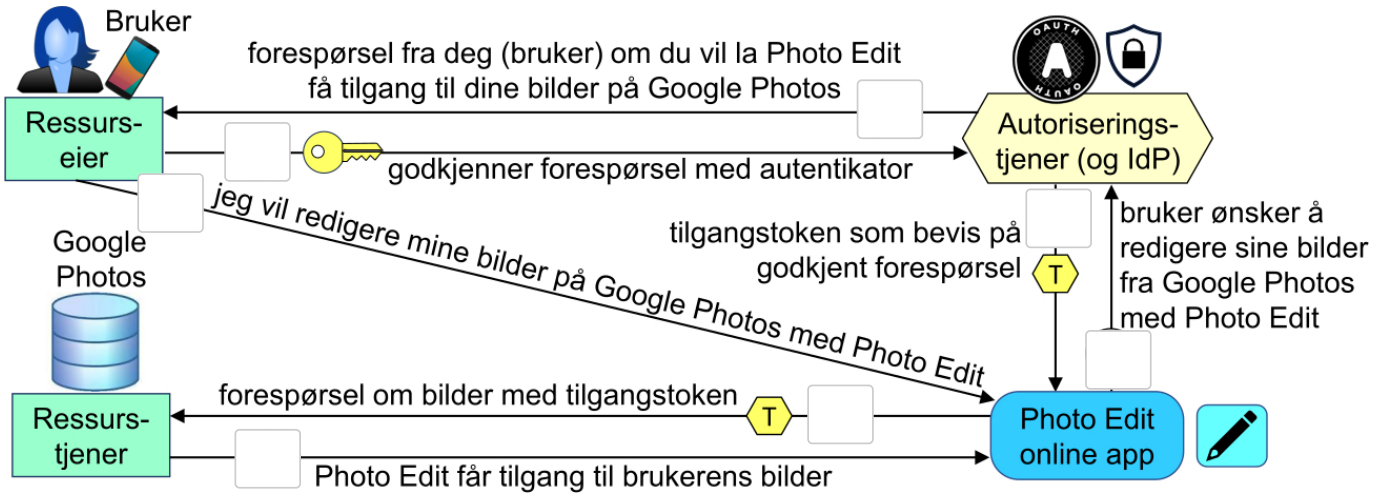
Velg korrekt eller feil for hvert utsagn:

	Korrekt	Feil
Identitet er et sett med attributter.	○	○
Identitetsdomene er et sett med attributter.	○	○
Silo-domener kan bare ha 1-faktorautentisering.	○	○
Fødererte IAM-arkitekturer har alltid distribuerte identitetsdomener.	○	○
Fødererte IAM-arkitekturer har alltid distribuert autentisering.	○	○
En bruker kan ha forskjellige identiteter i forskjellige domener.	○	○

Maks poeng: 3

35 OAuth

Figuren nedenfor viser en forenklet use-case med OAuth der brukeren autoriserer Photo Edit app for tilgang til sine bilder lagret på Google Photos. Skriv riktig meldingsnummer med tall fra 1 til 7 for hver melding.
Poeng: 0,5 for hver riktig; 0 for hver feil eller ubesvart; 4 for alle riktig (0,5 i bonus hvis alt riktig); minimum 0.



Maks poeng: 4

i Del 7: ISMS og risikostyring

36 27K-serien av sikkerhetsstandarder

ISO/IEC publiserer 27K-serien med standarder for informasjonssikkerhet. Indiker hvilket nummer standarden har for hver beskrivelse av en standard nedenfor.

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

Indiker riktig nummer for standard.

	27002	27000	27001	27005
Generell beskrivelse av ISMS (styringssystem for informasjonssikkerhet)	○	○	○	○
Tiltaksbank (beskrivelse av ulike sikkerhetstiltak)	○	○	○	○
Risikostyring for informasjonssikkerhet	○	○	○	○
Krav til ISMS (styringssystem for informasjonssikkerhet)	○	○	○	○

Maks poeng: 2

37 NSMs grunnprinsipper og NIST CSF

NSMs grunnprinsipper for IKT-sikkerhet, og NIST 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 styringsprosesser (f.eks. kartlegge, beskytte, oppdage, håndtere)	○	○	○	○
Standarden/veilederen må kjøpes	○	○	○	○
Er publisert på norsk	○	○	○	○
Kan brukes sammen med ISO/IEC 27001	○	○	○	○

Maks poeng: 2

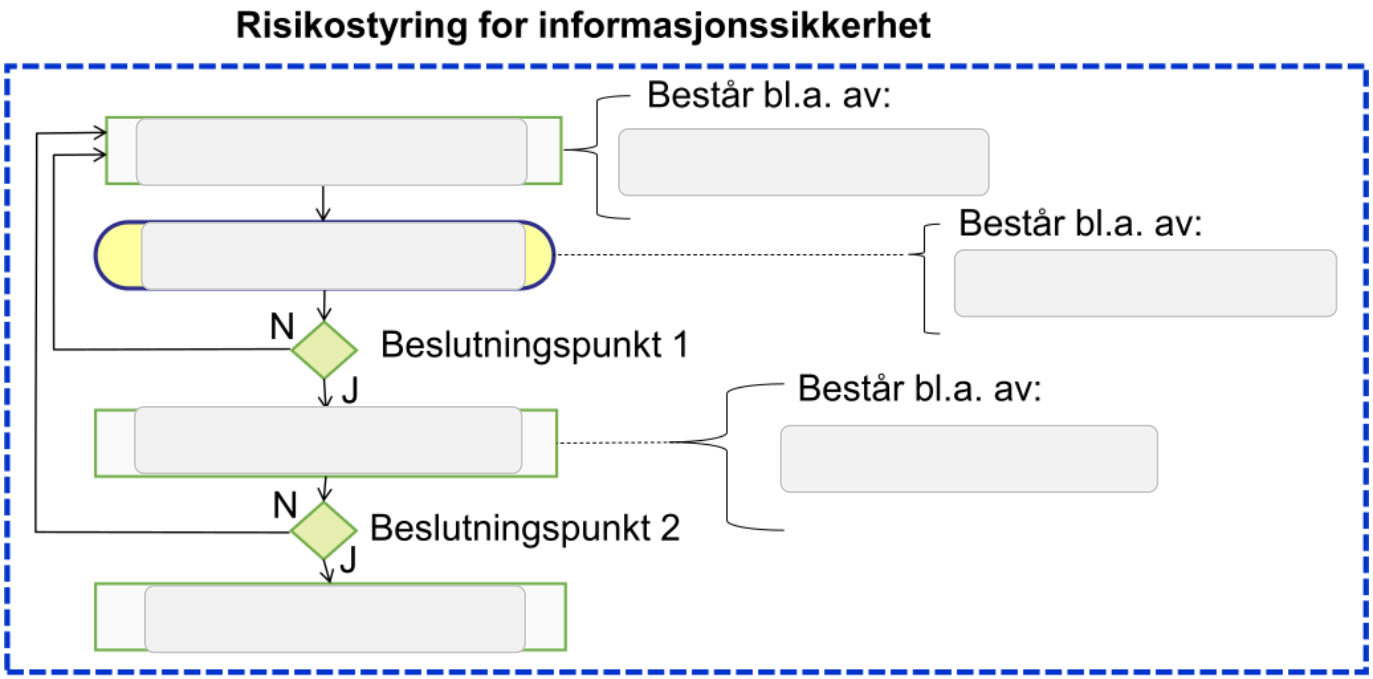
38 Prosess for risikostyring

Figuren nedenfor viser prosess for risikostyring der trinnene mangler beskrivelse. Sett inn elementene i riktig felt for å beskrive trinnene.

Poeng: 0,5 for hver riktig; -0.5 for hver feil; 0 for ubesvart; 4 for alle riktig; minimum 0.

Hjelp

Risikohåndteringsplan	Implementer sikkerhetstiltak
Aksepter risiko	Risikovurdering (ROS)
Bestem risikoeier	Risikoanalyse
Kontekstetablering	



Maks poeng: 4

39 Risikohåndtering

Håndtering av risikoer er en del av risikostyring. For hvert utsagn nedenfor, indiker om det representerer en gyldig metode for å håndtere risiko.

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

Indiker om hvert utsagn er en gyldig metode for risikohåndtering.

	Nei	Ja
Aksepter risikoen, som dermed representerer restrisiko	○	○
Dele eller overføre risiko til andre, f.eks. med tjenesteutsetting eller cyberforsikring	○	○
Reduser risiko ved å implementere sikkerhetstiltak	○	○
Reduser risikonivået fra risikovurderingen ved å endre risikotabellen	○	○

Maks poeng: 2

i Slutt

Slutt på eksamen