Høyskolen Kristiania

Emnekode:	**TK2100 – eksamen (Oslo)**
Emnenavn:	**Informasjonssikkerhet**
Vurderingskombinasjon:	**24 timer hjemmeeksamen**
Vurderingsform:	**Bestått / ikke bestått**
Innleveringsdato:	**29. april 2025**
Filformat:	**PDF**

Oppgavesettet består av 3 sider, og inneholder totalt 10 oppgaver som skal besvares. (Du kan svare på norsk eller engelsk.)

Det er 24 timers frist på denne hjemmeeksamen, men forventet arbeidsmengde er 4-6 timer så det er ikke meningen å «jobbe gjennom natten». Vær obs på at eksamen MÅ leveres innen fristen som er satt, og må leveres via eksamensplattformen WISEFLOW. Det vil ikke være mulig å få levert oppgaven etter fristen – det betyr at du bør levere i god tid slik at du kan ta kontakt med eksamenskontoret eller brukerstøtte hvis du har tekniske problemer.

Da dette er en hjemmeeksamen er det viktig å vise helhetlig forståelse, og oppgavene har et større preg av drøfting. Det forventes derfor utfyllende og forklarende svar på alle oppgaver. Figurer og skisser kan du velge å tegne i tekstbehandleren, eller ved å tegne på papir og laste opp bilde – husk å sette inn bilde på riktig sted i besvarelsen. (Bilder som er vedlegg, men ikke satt inn i besvarelsen anses ikke som en del av besvarelsen.)

Det presiseres at studenten skal besvare eksamen selvstendig og individuelt, samarbeid mellom studenter og plagiat er ikke tillatt. All bruk av tekst, bilder og illustrasjoner som er hentet fra forelesninger, lærebøker eller internett skal føres med kildehenvisning slik at det kommer tydelig frem hva som er studentens eget arbeid, APA7 standarden anbefales brukt for kilder. For topp score på oppgaver bør svarene underbygges med relevante kilder utover ordinær pensumlitteratur. (Vær obs på at å kopiere tekst fra en egen tidligere innleverte oppgave/eksamen kan bli ansett som «selvplagiering» hvis du ikke oppgir deg selv riktig som kilde.)

Det presiseres også at det i henhold til skolens eksamensreglement ikke er tillatt å presentere andres arbeid som ditt eget – dette inkluderer arbeid utført av kunstig intelligens (som tekst- eller kode-genereringsmodeller).

Besvarelsen skal ikke være på mer enn 15 A4 sider, med font størrelse 12, normale marger og linjeavstand 1.0.

Husk å oppgi kandidatnummer på din besvarelse, ikke studentnummer.

Høyskolen Kristiania

Oppgave 1. Generelt (10 %)

Definer «informasjonssikkerhet». Ta utgangspunkt i CIA-modellen.

Oppgave 2. Overvåkning (10 %)

Drøft hvordan nasjonale myndigheter kan bruke din nettverkstrafikk til å kartlegge deg som privatperson, og dine bevegelser og handlinger. Drøft hvordan Etterretningstjenesteloven kapittel 7 kan påvirke privatpersoner i Norge.

Sett deg inn i begrepet «nedkjølingseffekt» (engelsk: «chilling effect») i denne sammenhengen, og drøft etiske problemstillinger knyttet til denne lovhjemmelen.

Oppgave 3. Skadevare (10 %)

Forklar forskjellen mellom et virus og en orm. Du skal vise til minimum ett eksempel av hver av disse to typene skadevare, og forklare hvordan disse spredde seg.

Oppgave 4. Kryptering (10 %)

Forklar hvordan data kan signeres med asymmetrisk kryptering, gi minimum et eksempel på algoritme som kan gjøre dette og forklar hvordan denne algoritmen fungerer når brukt for signering.

Forklar konseptuelt hvordan et dokument kan digitalt signeres på denne måten, forklar hvilke deler av CIA modellen dette ivaretar og drøft om også andre sikkerhetskrav oppfylles ved dette.

Oppgave 5. Personlig sikkerhet (10 %)

Forklar 5 tekniske grep du kan gjøre for å styrke din personlige sikkerhet innenfor det digitale domenet (dette kan være grep du allerede har gjort). Forklar hvilke problemer hvert av disse grepene løser og hvorfor dette er viktig for deg.

Oppgave 6. Web sikkerhet (10 %)

Forklar hvordan Cross Site Request Forgery fungerer, og hva som skiller dette angrepet fra andre web baserte angrep. Drøft konkrete bruksområdet for CSRF angrep, og hvordan man kan forsvare seg mot slike angrep.

Høyskolen Kristiania

Oppgave 7. Nettverk (10 %)

Forklar hvilke sikkerhetsutfordringer vi har på linklaget i TCP/IP modellen.

Oppgave 8. Hjemmekontor (10 %)

Under COVID pandemien ble det vanlig med hjemmekontor for de fleste selskaper og ansatte med typisk «kontorarbeid». Drøft hvilke utfordringer dette utgjør for informasjonssikkerheten i selskapene. Hva mener du må endres for å ivareta sikkerheten nå som hjemmekontor fremover blir den «nye normalen» i mange selskap?

Oppgave 9. Praktisk anti-virus (10 %)

I denne oppgaven skal du demonstrere din kunnskap om bruk av anti-virus programvare. Last ned test filen EICAR fra https://www.eicar.org/download-anti-malware-testfile/, du kan enten laste ned en av filene eller du kan opprette en ny fil med de 68 karakterene som utgjør «virusets» signatur som beskrevet nederst på siden (og som brukt i øvingstimene). Du skal videre demonstrere følgende:

- Scan filen med ditt anti-virus program, vis at anti-virus programmet oppdager filen og rapporterer den som skadevare
- Gå inn i ditt anti-virus program sin karantene (quarantine) funksjon, finn den detekterte filen og eksporter den ut av karantene (for noen anti-virus programmer er det mulig du må skru av sanntidsbeskyttelse først)

Dokumenter de to stegene med skjermbilder fra ditt anti-virus program, forklar hva du gjør og hvorfor.

Hvis du (til tross for det du har lært i dette faget) ikke har anti-virus program på din maskin må du installere det for denne oppgaven.

Oppgave 10. Praktisk server-side angrep (10 %)

Du skal i denne oppgaven bruke web applikasjonen «Boris Lockpicks» som dere installerte i øvingstimene til leksjon 8 Web Sikkerhet. Demonstrer mot denne web applikasjonen hvordan man utfører et «local file inclusion» angrep.

Simuler angrepet ved å få printet ut innholdet av filen 'backend/sendemail.c' på skjermen. Dokumenter med skjermbilder og forklar din fremgangsmetode. Husk å sette inn skjermbilde på riktig sted i besvarelsen.

Slutt på oppgavesettet