Høyskolen Kristiania

HJEMME EKSAMEN VÅR 2022
TK2100 Informasjonssikkerhet

Tillatte hjelpemidler: Alle **Varighet:** 24 timer **Dato:** 7. juni 2022

Karakterskala/vurderingsform: Bestått / ikke bestått

Oppgavesettet består av 3 sider, og inneholder totalt 10 oppgaver som skal besvares.

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 eller Chicago (forfatter, år) standardene anbefales brukt for kilder. For topp score bør svarene underbygges med relevante kilder utover ordinær pensumlitteratur.

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

Oppgave 1. Generelt (10 %)

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

Oppgave 2. Konto hijacking og identitetstyveri (10 %)

Drøft hva en hacker kan gjøre hvis han/hun får kontroll over (hijacker) din private epost-konto. Reflekter over mottiltak mot slike angrep. Se problemstillingen i sammenheng med identitetstyveri, og diskuter også hva en hacker kan bruke din BankID til hvis angriperen får tilgang til din personlige kode og din kodebrikke.

Husk å oppgi kandidatnummer på din besvarelse, ikke studentnummer.

Høyskolen Kristiania

Oppgave 3. Skadevare (10 %)

Det finnes flere måter å klassifisere skadevare (malware), historisk har vi delt inn i klasser basert på følgende egenskaper: Spredning, Skjuling og Nyttelast.

Basert på denne metoden klassifiser følgende skadevare, og begrunn hvorfor du har valgt den klassifiseringen (oppgi kilder du har brukt for å underbygge svaret):

- ILOVEYOU
- Stuxnet
- Brain
- WannaCry

Oppgave 4. Kryptering (10 %)

Forklar forskjellen på RSA kryptering og RSA signering, forklar hvordan de to anvendelsene fungerer.

En avsender Alice ønsker å sende en epost til Bob og ønsker både å oppnå konfidensialitet og integritet, tegn og forklar hvordan dette kan oppnås.

Oppgave 5. Kryptering (utregning) (10 %)

I denne oppgaven skal du manuelt regne med algoritmene for RSA kryptering (men med mye mindre nøkkelstørrelser slik at vi kan bruke en vanlig kalkulator). Gitt at du har en public key hvor n = 3233 og e = 17, og din privat key er n = 3233 og d = 2753.

Bob har brukt din public key for å kryptere en melding til deg, dekrypter denne meldingen med din private key. Meldingen du mottar er:

1759 2160 1992 690 1632 2235 1992 1859 2680 2790

Vis fremgangsmåte og forklar formelen som er brukt.

Oppgave 6. Nettverk (10 %)

Forklar hvilke sikkerhetsutfordringer vi har på linklaget i TCP/IP modellen. Tegn og forklar hvordan en angriper kan utføre «Man-in-the-Middle» angrep mot et mål som er koblet til samme switch som angriperen, og vis hvorfor dette er mulig ved å forklare hvordan ARP protokollen fungerer.

Høyskolen Kristiania

Oppgave 7. Phishing (10 %)

Forklar hva phishing er og hvordan en hacker kan utnytte dette for å angripe et selskap. Drøft tekniske og personellmessige løsninger på denne angrepsvinkelen.

Oppgave 8. Hjemmekontor (10 %)

Under pandemien har det blitt vanlig med hjemmekontor for de fleste selskaper og ansatte med typisk «kontorarbeid». Drøft hvilke utfordringer dette utgjør for datasikkerheten i selskapene. Hva mener du må endres for å ivareta sikkerheten hvis hjemmekontor blir den «nye normalen» også etter pandemien?

Oppgave 9. Praktisk SSL analyse (10 %)

Du skal utføre en analyse av «Usikre TLS ciphers» ved hjelp av standard verktøy for dette. Du skal teste følgende domene:

`https://demo.testfire.net`

Dette er et test-domene som er laget for å lære seg om penetrasjonstesting, og eiet av IBM. (Du skal ikke besøke URLen selv, kun bruke standard verktøy for SSL/TLS analyse, du har heller ikke tillatelse til å bruke andre typer hacker/pentest verktøy.) Vurder hvor sikker krypteringen (TLS) er på denne webserveren, trekk spesielt frem svake algoritmer som brukes i kryptert kommunikasjon med serveren.

Oppgave 10. 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/?page_id=3950, 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.

Slutt på oppgavesettet.