INDIVIDUELL HJEMME EKSAMEN
TK2100 Informasjonssikkerhet

Tillatte hjelpemidler: Alle **Varighet:** 24 timer **Dato:** 2020-04-30

Karakterskala/vurderingsform: Bestått / ikke bestått

Oppgavesettet består av 3 sider, og inneholder totalt 8 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 færre spørsmål enn på en ordinær eksamen, og oppgavene har et preg av drøfting for å vise forståelse av temaet. Det forventes derfor utfyllende og forklarende svar på alle oppgaver.

Det presiseres at studenten skal besvare eksamen selvstendig og individuelt, samarbeid mellom studenter og plagiat er ikke tillatt.

Oppgave 1. Generelt (10 %)

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

Oppgave 2. Trusler for personer (15 %)

Drøft hva som er de største truslene mot din egen informasjonssikkerhet. Beskriv de viktigste tiltakene for å redusere risiko.

Oppgave 3. Kryptering (15 %)

3.1 Teoretisk oppgave

Forklar kort hva som skiller asymmetrisk (public key) kryptering fra symmetrisk kryptering. Forklar hva som er den vanligste block cipher krypteringsmetoden, og hva som er den vanligste asymmetriske krypteringsmetoden– og bruk disse i forklaringen.

3.2 Praktisk oppgave

Følgende tekst er resultatet av at en plain tekst er kryptert med AES-256-CBC med en nøkkel derivert fra et passord som er et tall under 100 (det vil si fra «00» til «99»).

Passordet er saltet. Svaret er enkodet med BASE64. Knekk koden med brute force ved bruk av openssl på kommandolinje. (Alt ble gjort i 1 kommandolinje operasjon når plain tekst ble kryptert.)

U2FsdGVkX1//didoayE/MomTlg2iyU6HJMVx8gVWhnzVQGBYvhLNtalm2j4w9Y/X
q1sMC97+NUqBinS8E8FmB6SypsCqvHk9kEFEAkEvqQI=

Hva er passordet («koden»), hva er plain teksten, og hvordan gikk du frem?

Oppgave 4. Operativsystemet og fysisk (10 %)

I utgangspunktet sier man innen informasjonssikkerhet at en angriper som kan få fysisk tilgang til en maskin har full kontroll – og for eksempel bærbare maskiner kan være enkle mål. Forklar hvordan man kan beskytte en datamaskin på best mulig måte, ta utgangspunkt i en bærbar maskin som står på en kontorpult og lag sikkerhetsmodellen din rundt dette. Beskriv en løsning som omfatter både operativsystemsikkerhet, brukerpolicyer, og fysisk sikkerhet.

Oppgave 5. Nettverk (15 %)

Forklar hvordan og hvorfor TCP/IP modellen resulterer i så store sikkerhetssvakheter, og hvilke praktiske problemer dette resulterer i. Herunder skal du forklare problemer med protokoller som HTTP og Telnet, du skal forklare om TCP hijacking, og du skal vise hvordan ARP poisioning og MAC flooding fungerer.

Hvis du skal jobbe med å sikre nettverket hos et selskap, hva har dette å si for deg og din jobb?

Oppgave 6. Penetrasjonstest (15 %)

Tenk deg at du skal angripe en stor norsk bank, formålet ditt er å enten stjele penger eller finne bedriftshemmeligheter du kan utnytte senere. Dette er en penetrasjonstest og det er selskapets CIO og CEO som har bedt deg utføre testen, og ingen andre er informert. Beskriv hvordan du ville gått frem for å komme deg inn i banken. Din begrensning er at du ikke har lov til å true ansatte på noen måte, og du har ikke lov til å oppsøke noen ansatte eller deres familier utenfor bankens lokaler – ellers skal du fullt ut bruke en kriminell sine metoder for å utføre angrepet.

Beskriv din fremgangsmetode trinn for trinn, i så stor detalj som tiden tillater. Beskriv også eventuelle forutsetninger og antagelser du tar. (Obs; du skal ikke utføre oppdraget i praksis…)

Oppgave 7. Kopibeskyttelse (10 %)

Drøft fordeler og ulemper med patent og kopibeskyttet software.

Hvem tjener på det og hvem taper? Kan en aktør både tjene og tape på streng håndheving av kopibeskyttelse?

Oppgave 8. Refleksjon (10 %)

Forklar hvordan du føler emnet Informasjonssikkerhet har vært, hvordan kan du bruke kunnskaper og ferdigheter fra dette emnet i ditt planlagte yrkesvalg? Våren 2020 har vært preget av tilnærmet unntakstilstand i Norge og resten av verdenen, hvordan har det preget din studiehverdag? Hva har vært positivt og hva har vært negativt med å ha siste del av semesteret i et digitalt klasserom, hvordan føler du det har fungert i dette faget?

Slutt på oppgavesettet.