Informasjon om eksamen

Høgskolen i Østfold

EKSAMEN

Emnekode: ITF15015

Emnenavn: Innføring i datasikkerhet

Dato: 16/05-2018

Eksamenstid: 09.00-13.00, 4 timer

Hjelpemidler: Ingen

Faglærer: Tom Heine Nätt

Om eksamensoppgaven:
Oppgavesettet er inndelt i 2 deler. Det er på hver del, og deloppgavene i del 2, angitt hvor mye disse teller av totalen. Karakter fastsettes dog på basis av en helhetsvurdering av besvarelsen.

Gjør dine egne forutsetninger dersom du mener noe er uklart.

Takk for et hyggelig semester - beklager at jeg har gjort dere paranoide.

Lykke til!

Sensurfrist: 06/06-2018
Karakterene er tilgjengelige for studenter på Studentweb.

Del 1

Del 1. Faktaspørsmål (65 %)

Alle disse oppgavene har et slags forventet svar, selv om det ikke er noen eksakt fasit. Hver deloppgave (a,b,c,d osv.) teller i utgangspunktet like mye. Det kan likevel være variasjoner i vektingen av deloppgaver basert på omfang og vanskelighetsgrad.

Selv om det kan være mulig å svare på flere av deloppgavene samlet, ønskes det at du er nøye med å skille svarene på deloppgavene fra hverandre i din besvarelse.

Husk at det ikke er mengden tekst, men innholdet, som er viktig. Svar derfor gjerne som stikkord/korte setninger og punktlister. Det viser god kompetanse i et tema at man klarer å svare kort og konsist. Pass imidlertid på at det ikke blir så kort at innholdet forsvinner eller blir utydelig.

Mange av oppgavene vil også ha flere ulike momenter (for eksempel teknikker eller farer) som mulige svar. Å kun nevne ett moment vil da ikke gi full uttelling, selv om det i seg selv er riktig.

1 Oppgave 1.1

Oppgave 1.1 – Cookies, sesjoner og sesjonskapring

a) Forklar med dine egne ord hvordan nettjenester med sesjoner som baserer seg på cookies (informasjonskapsler) fungerer.
b) Hvordan kan en hacker overta en sesjon ved å få kjennskap til brukerens cookie/cookies?
c) Hvilke muligheter/begrensninger er det for hackeren på en slik sesjonskapring?
d) Gjennom hvilke metoder kan en hacker få kjennskap til en brukers cookie/cookies?
e) Hva kan brukere og tjenesteutviklere gjøre for at det ikke skal være like lett å utføre og missbruke en sesjonskapring?

Skriv ditt svar her...

2 Oppgave 1.2

Oppgave 1.2 - CSRF

a) Forklar ved hjelp av et eget eksempel hva CSRF (cross-site request forgery) er.
b) Hva kan brukerne gjøre for å beskytte seg mot CSRF-angrep?
c) Hva kan utviklerne gjøre for å (forsøke) forhindre CSRF-angrep?

Skriv ditt svar her...

3 Oppgave 1.3

Oppgave 1.3 - Skadevare

a) Hvilke ulike overordnede metoder kan et "antivirusprogram" benytte for å oppdage
skadevare, og hvordan (i korte trekk) fungerer disse?
b) Hvilke årsaker kan det være til at et "antivirusprogram" ikke advarer oss om en faktisk skadevare?
c) Hva er et hoax i forbindelse med skadevare, og hvordan kan det utgjøre en sikkerhetsrisiko?
d) Hvordan kan social engineering benyttes av hackere for å få utført sin nyttelast på tross av at brukeren har et "antivirusprogram" (her er det flere fremgangsmåter)?

Skriv ditt svar her...

4 Oppgave 1.4

Oppgave 1.4 – Trådløse nett / VPN

a) Du kobler til et ukjent trådløst nett (altså et nett du ikke tidligere har koblet til). Hvilke ulike farer kan det innebære å koble til dette nettet?
b) Hvorfor kan man ikke stole på et kjent trådløst nett (SSID som du har benyttet deg av før)?
c) Forklar hvordan VPN kan minimere farene du nevner i oppgave a.
d) Hvilke sikkerhetsutfordringer kan det være ved å benytte VPN?

Skriv ditt svar her...

5 Oppgave 1.5

Oppgave 1.5 – Daglig drift / Diverse

a) Hva bør man tenke på (sett fra et sikkerhetsperspektiv) når man skal utføre en oppdatering av programvare/firmware/drivere, og hvorfor er det viktig å oppdatere?
b) Forklar hvorfor det ikke nødvendigvis er tilstrekkelig å slette en fil på en minnepenn før man gir fra seg minnepennen til andre.
c) Hva kan man gjøre om man vil være sikker på at informasjonen i en fil er permanent fjernet?
d) Hvordan kan tofaktorautentisering øke sikkerheten i en innlogging, og hvilke generelle "faktorer" består dette av?

Skriv ditt svar her...

Del 2

Del 2. Åpne spørsmål (35 %)

Disse oppgavene har ikke noe "fasitsvar", og det er opp til deg hvordan du vil angripe de. Du vil bli bedømt på hvordan svaret ditt viser at du behersker datasikkerhet. Det er her viktig å vise sensor at du har en forståelse for anvendelse av det du har lært i emnet, ikke at du kan gjenta mest mulig som er pugget. Pass på at svaret ditt har noe med problemstillingen i oppgaven å gjøre.

Det er angitt på hver oppgave hvor mye de teller av totalen. Dette indikerer også til en viss grad hvor mye tid det er forventet at du skal benytte oppgaven.

Også her er innholdskvalitet viktigere enn tekstmengde, men husk at du skriver såpass utfyllende at sensor forstår hva du mener.

6 Oppgave 2.1

Oppgave 2.1 (20 %)

Mediene skriver til stadighet om personer som har blitt "hacket". En av de store sakene i 2017/2018 var Nora Mørk sine private bilder som hadde kommet på avveie.

Alt vi vet ut i fra mediene er at Nora Mørk har tatt noen private bilder som hun har oppbevart på sin mobiltelefon, og at disse så er blitt spredt ukontrollerbart rundt på nett av andre.

Skisser opp ulike scenarioer for hvordan bildene kan ha kommet på avveie. Husk å tenke hele bredden fra menneskelige feil og bevisste handlinger til tekniske feil og "angrep". Del svaret ditt tydelig opp i disse scenarioene, for eksempel ved å benytte overskrifter.

For hvert av scenariene kan du gjøre forutsetninger dersom nødvendig. F.eks. at bildene er sendt som privat melding til noen utvalgte mottakere.

Svært mye av pensum passer i denne oppgaven, og det forventes at du gjør litt ut av den. Husk igjen på at det ikke er mengden tekst som er avgjørende. Sørg imidlertid for at du skriver såpass utdypet at sensor forstår hva du vil frem til.

Skriv ditt svar her...

7 Oppgave 2.2

Oppgave 2.2 (10 %)

a) Forklar hva sammenhengen **potensielt tap * sannsynlighet < kostnaden til mottiltak** innebærer, og hva det har å si for bedrifters håndtering av datasikkerhet.

b) Hvordan kan innføringen av GDPR påvirke bedrifters håndtering av datasikkerhet? Koble gjerne deler av svaret ditt til oppgave a.

Skriv ditt svar her...

8 Oppgave 2.3

Oppgave 2.3 (5%)

I kurset har vi sett på verktøypakken Kali. Hva vil det si for datasikkerhet generelt at slike ferdige verktøypakker for hacking finnes åpent tilgjengelig.
(Gi svaret ut i fra flere perspektiver)

Skriv ditt svar her...