IN1020 - Nettverkskommunikasjon og datasikkerhet: Øvingsoppgaver gruppetime 2 (uke 36)

1 Datasikkerhet

1. Hvordan kommer data på avveie? Tenk gjennom og diskuter ulike scenarier.
2. Kapittel 2.4 i Jøsang (Cybersikkerhet: Teknologier og styring): Oppg. 1
3. Case-oppgave:

   Et stort spillutviklingsselskap er i full sving med sitt neste AAA-spill i en populær serie (et AAA-spill er et høyprofil-spill med høye budsjetter for utvikling og markedsføring). Selskapet involverer 500 ansatte gjennom hele utviklingsprosessen, som inkluderer mange mindre team der noen f.eks. jobber med ting som animasjoner, og andre programmerer ulike deler av spillet.

   (a) Hvilke verdier kan dere identifisere i dette scenarioet?
   (b) Hvem/hva er mulige trusselaktører? Hva kan gå galt?
   (c) Hvilke sikkerhetsmål bør prioriteres, og hvorfor?
   (d) Hvordan ville dere sikret selskapet mot det dere kom frem til i b)? Hvilke sikkerhetstiltak bør benyttes?

4. Behandling av data:

   Gjør en vurdering av hvordan du lagrer og behandler egne data/informasjon. Private, på UiO/Ifi, jobb. Ta utgangspunkt i mulige sikkerhetstrusler og sikkerhetstiltak du allerede har eller bør iverksette, og kikk gjerne på UiOs veiledning for klassifisering av data og Lagringsguide:

   (a) https://www.uio.no/tjenester/it/sikkerhet/lsis/tillegg/infoklasser.html
   (b) https://www.uio.no/tjenester/it/sikkerhet/lsis/tillegg/lagringsguide.html

5. Sikkerhetskopi (backup) som sikkerhetstiltak.

   (a) Hva kjennetegner gode rutiner for sikkerhetskopiering (backup) i en virksomhet eller for en privatperson, og hvorfor er den fysiske eller nettverksmessige plasseringen av disse kopiene så kritisk?
   (b) Hvilket av de tre klassiske sikkerhetsmålene (konfidensialitet, integritet eller tilgjengelighet) er det sikkerhetskopiering primært er ment å ivareta? Begrunn svaret kort med utgangspunkt i trusler som løsepengevirus.

6. Eksamensoppgaver 11 fra eksamenssettet H20.
7. Hva kan hackere oppnå gjennom et angrep basert på SQL-injeksjon?
8. Hva kan hackere oppnå gjennom et angrep basert på Cross Site Scripting (XSS)?

9. Dataangrep:

   Kalenderen viser mai 2017. På jobben din er bruk av datamaskiner en essensiell del av arbeidet. En dag blir du plutselig møtt med denne meldingen på skjermen til arbeidsstasjonen din:

   `"Ooops, your important files are encrypted"`

   Videre ber meldingen deg å kjøre en dekrypteringsprogramvare som allerede har poppet opp. I dekrypteringsprogramvaren ser du en klokke som teller ned, og en melding som ber om 300 bitcoin (som var mye penger i 2017). Du ser rundt deg og flere og flere av kollegaene dine ser ut til å bli rammet. Full panikk! Hva nå?

   (a) Hvordan tror dere hovedpersonen ble rammet av denne skadevaren? Har de gjort noe dumt eller kan dette skje uansett hvor påpasselig man er selv? Og har du hørt om, eller kan finne informasjon om dette angrepet, som er basert på en ekte hendelse?

   (b) Diskuter hva slags skadevare det er snakk om her.

   (c) Hvordan kunne arbeidsplassen forhindret angrepet? (Kunne de det i det hele tatt?) Hva er lurt å gjøre når angrepet først har startet?

   (d) Hvilke sikkerhetsmål er svekket av angrepet?

10. Sosial manipulasjon

    (a) Hvilke sårbarheter er det vanlig å utnytte i det vi kaller phishing attacks?

    (b) Foreslå sikkerhetstiltak for å forebygge slike angrep (phishing attacks).

    (c) Kom med forslag til hvordan en angriper kan bruke sosial manipulering til å:

        i. få uautorisert tilgang til en virksomhets/en bedrifts lokaler/bygg

        ii. installert skadevare på de personlige datamaskinene til selskapets direktør

11. Innsamling av fritt tilgjengelige data benyttes ofte av hackere for mer rettet phishing. Her er noen oppgaver du kan forsøke deg på.

    (a) Hva er brukernavnet til Universitetsdirektøren til UiO? (Og hvordan fant du det?) Hvordan kan kjennskap til noens brukernavn potensielt misbrukes?

    (b) På semestersiden til IN1020 finner dere et bilde:
    https://www.uio.no/studier/emner/matnat/ifi/IN1020/h26/ukeoppgaver/vinterblomst.jpg

        i. Finn ut hvor bildet er tatt ved å se på metadataene som følger med i bildefilen.

        ii. Finner du annen interessant informasjon i bildets metadata?

2 Datanettverk

1. Beskriv kort forskjellene mellom linjesvitsjing (circuit switched) og beskjedssvitsjing (message switched) i nettverk. Hva ligner mest på Internett i dag?

2. Hva er en protokoll, og hvorfor trenger vi det i datakommunikasjon?

3. Hvilke nettverkstopologier er mest vanlige i dag?

4. Diskusjonsoppgave:

   Hvilke sikkerhetsutfordringer har de mest brukte nettverkstopologiene, og hvordan kan vi løse dem?