TTY / TLT / J. Koskinen

Ei laskimia. Kysymyspaperin saa pitää.

TLT-3201 Tietoturvallisuuden jatkokurssi

Tentti (I) 10. 12. 2012

1. Millainen rakenne on turvallisella tietoverkolla? (Nimittäin jonkin organisaation tietoverkolla.)

2. Mitä sääntöjä noudattamalla ohjelmointi tuottaa tavallista turvallisemman tuloksen? (Luonnehdi jotain kokoelmaa tai esittele joitain keskeisiä sääntöjä.)

3. Olisiko vielä teorioita, joista olisi apua TT:n erityisongelmien ratkomisessa? (Eli: Millaisia Bell-LaPadulan mallin tapaisia muita teorioita on olemassa?)

4. Millaisen "pahimman" varalle pitäisi olla suunnitelmia? (Kontekstina tietoturvaan liittyvät eritasoiset suunnitelmat.)

5. Syksyllä 2013 alkavan uudistetun Tietoturvallisuuden jatkokurssin (8 op) osaamistavoitteet ovat tällaiset:

Opintojakson suoritettuaan opiskelija

(i) osaa kuvailla, mitä kaikkea tietoturvallisuuden insinööritaitoon kuuluu, osaa esittää pääpiirteet useimmista alan tekniikoista, mutta osaa myös tunnistaa taitojensa rajat ja esittää arvion, miten kehittyminen olisi mahdollista tai miksei se olisi tarpeellista.

(ii) on kehittänyt tietoturvan puolustajan tarvitseman hyökkäävän ajattelutavan. Hän osaa ehdottaa murtokeinoja erityyppisiin hänelle esitettyihin tietojärjestelmiin ja niiden turvamekanismeihin.

(iii) osaa neuvoa kuvitteellista kokematonta työntekijää tunnistamaan erityyppisiä, myös sosiaalista vaikuttamista käyttäviä, hyökkäyksiä ja havainnollistamaan niitä esimerkeillä.

(iv) osaa esittää periaatteet, joilla voidaan arvioida hänelle esitetyn tietojärjestelmän tietoturvallisuutta sinänsä, sen kustannuksia ja sen käytettävyyttä.

(v) pystyy kuvailemaan hänelle esitetystä tunnetusta tai uudenlaisesta tietoturvauhkasta, miten puolustajan kannattaisi siihen suhtautua, olipa ilmiö tietokoneen laitteiston tai yhteiskunnan kriittisten järjestelmien tasolla tai jossain niiden välillä.

(vi) on hankkinut oman kiinnostuksensa mukaista syventävää tietämystä, jonka varassa hänellä on hyvät valmiudet aloittaa itsenäinen työskentely tietoturvaprojektissa. Tätä varten hän pystyy myös kuvailemaan järjestelmien turvallisen suunnittelun periaatteet.

a) Mikä näistä saa eniten tukea jo nykyisen kaltaiselta jatkokurssilta? Perustele. Toteutuuko asia myös sinulle?
b) Mitä tavoitetta nykyinen kurssi tukee heikoimmin? Perustele.
c) Valitse jokin muu nykyisellään heikosti toteutuva tavoite kuin b-kohdassa ja luonnostele, miten uuden kurssin kannattaisi siihen pyrkiä. (Kohdat a ja c tuovat max. 2 pistettä ja b max. 1 pisteen.)

6. Vertaile SSH:ta ja Kerberosta käyttötarkoituksen ja toteutusperiaatteiden suhteen.

7. Mihin sokeaa allekirjoitusta voidaan soveltaa? Miksi voidaan tarvita "puolisokeutta"?

8. Harjoitustyökysymykset. Tarkoitus on, että jokainen saa valita kuudesta muuta kuin omaa työtä koskevasta kysymyksestä viisi, joihin vastaa. Tätä varten muistuta ensin lukijaa, mikä olikaan tutkielmasi aihe. Jos sitä koskeva kysymys ei ole kysymysten (1)–(6) joukossa, valitse niistä viisi ja vastaa niihin. Muussa tapauksessa valitse kysymyksistä (1)–(7) viisi muuta kuin omasi ja vastaa niihin.

(1) Minkä turvallisuuden KLJN ja QKD takaavat? Miten se eroaa Diffie-Hellmanin takaamasta turvasta?
(2) Miten penetraatiotestauksen tuloksista tulisi raportoida?
(3) Mistä aiheista System Security Group (ETH Zürich) on julkaissut ja millaista näkyvyyttä se on saanut?
(4) Mitä salaisuuksia EMV-kortit tallettavat?
(5) Kuinka social engineer voi käyttää hyväkseen mikroilmeitä?
(6) Millaisia testejä Codenomiconin ohjelmat tekevät?
(7) Miten DNSSEC turvaa DNS:n toimintaa?