

TLT-3301 Verkon Tietoturva

Tentti 8.4.2010 TTY/TITE/Tuure Vartiainen

1. Ovatko seuraavat väittämät totta vai tarua? Oikeasta vastauksesta saat +1 p, väärästä -1 p, tyhjäksi jätetystä 0 p. Maksimipisteet tästä tehtävästä siis 6 p, minimipistemäärä on 0 p.
 - a) Tietoverkkoon kohdistuvien tai tietoverkon kautta tehtyjen rikosten motiivit eivät juurikaan eroa muiden rikosten motiiveista.
 - b) Tietoliikenneprotokollan tilan huomioon ottava liikenteen suodatus (palomuuraus) on yleisesti suorituskyvyltään parempi kuin tilan suodatus.
 - c) AAA-protokolla mahdollistaa tietoverkon ja -järjestelmien käytön seuraamisen esimerkiksi laskutusta varten.
 - d) Järjestelmän komponenttien kahdentaminen kasvattaa järjestelmän saatavuuden (toimintatodennäköisyys) vähintään kaksinkertaiseksi.
 - e) Offline-tutkimenetelmillä tarkoitetaan sellaisia menetelmiä, joissa tutkinnan kohteena oleva muistilaite, kuten kiintolevy, ei ole käynnissä (eli sille ei syötetä sähköä).
 - f) Tietokoneiden keskusmuistissa oleva data on luonteeltaan ns. volatile-dataa.
2. Minkälaisilla asioilla tietoverkon arkkitehtuuria ja topologiaa suunniteltaessa voidaan parantaa tietoverkon tietoturvaa? (luottamuksellisuus, eheys ja saatavuus) (6 p.)
3. Tietoverkon ja tietojärjestelmien valvonta on olennainen osa niiden turvaamista. Kerro mitä menetelmiä ja tietoliikenneprotokollia valvontaan on olemassa ja kuinka niitä voidaan käyttää tietoturvan tilan valvontaan? (6 p.)
4. VPN-yhteys (Virtual Private Network) mahdollistaa toisistaan etäällä olevien tietoverkkojen yhdistämisen. Kerro mitä tietoliikenneprotokollia voidaan käyttää VPN-yhteyden muodostamiseen ja minkälaisia VPN-yhteyksiä kyseisillä protokollilla voidaan toteuttaa? (6 p.)
5. Kurssin viimeisissä harjoituksissa tutustuttiin lyhyesti ICT-forensiikkatyökaluihin. Miten organisaation tietohallinto/ylläpito voi hyödyntää ICT-forensiikkatyökaluja tietoturvaa kehitettäessä ja toisaalta tapahtuneiden tietoturvapoikkeamatilanteiden selvittämisessä? (5 p.) Olivatko opiskelijoiden harjoituksessa soveltamat menetelmät online- vai offline-tutkiminta? Perustele lyhyesti. (1 p.)