LTKK/Tite
Pekka Jäppinen

Ti5313500 Tietoturvan perusteet
Tentti 22.12.2006

1. Ennen vastaamista lue koko tentti läpi ajatuksella läpi ja mieti mitä oikeasti kysytään.

2. Ovatko seuraavat lauseet totta vai tarua? **Perustele vastauksesi?**
Oikea vastaus +1p, oikea/hyvä perustelu +2p, väärä vastaus huonolla tai puuttuvalla perustelulla -1p

a) Biometriikkaan perustuva autentikointi on parempi kuin polettiin perustuva autenikointi
b) Matojen avulla voidaan hankkia zombieita.
c) Kekseillä (cookie) voidaan levittää viruksia
d) Liikenneanalyysiä vastaan ei auta edes 512-bittinen symmetrinen salaus.
(**12p**)

3. Matti saa sähköpostissa liitteenä viestin Maijalta. Matti tallentaa viestin koneensa kovalevylle salattuna symmetrisellä AES algortimilla käyttäen 256-bittistä avainta. Salausavain on tallennettuna USB tikulla, josta tiedon lukeminen vaatii biometrisen autentikoinnin. Määrittele Matin saaman viestin turvallisuus. Mitä muuta Matin kannattaisi tehdä tiedon turvaamiseksi? Olisiko jotain mitä Matin tulisi tehdä toisella tavalla? Tarvittaessa voit itse määrittää mahdollisia lisädetaljeja kuten käytetyn prosessorin merkki ja Matin kenkien väri.
(**18p**)

4. Mitä on Phishing ja kuinka sitä vastaan voi itse suojautua?
(**6p**)

5. Pelit&Vehkeet myy verkokaupassa omia tuotteitaan verkossa. Yrityksellä on kaksi toimipistettä, toinen Helsingissä (myynti ja markkinointi) ja toinen Rovaniemellä (tuotekehitys ja tuotanto). Kuinka yrityksen tulisi suojata verkkonsa ja verkkoyhteytensä? Tarvittaessa voit itse määrittää mahdollisia lisädetaljeja kuten käytettyjen laitteiden merkin ja yrityksen myymien tuotteiden värin.
(**14p**)

6. Varmista että olet laittanut vastauspaperin ensimmäiselle sivulle nimesi ja opiskelijanumerosi. Kirjoita näiden jälkeen ensimmäiselle sivulle teksti: Olen lukenut kaikki tehtävät läpi ja jätä tekstin jälkeen ainakin kymmenen tyhjää riviä.

EI LASKIMIA
EI MATERIAALIA