T-110.4200 Tietoturvallisuustekniikka
Tentti 9.3.2008

1 Selitä lyhyesti seuraavat tietoturvallisuuteen liittyvät käsitteet. (6 p)
   a) Intrusion Detection
   b) MAC
   c) Malware
   d) Puskurin ylivuoto (Buffer overflow)
   e) Biometriikka
   f) CIA-malli

2 Perustele lyhyesti mitkä seuraavista väitteistä pitävät paikkansa ja mitkä eivät. (6 p)
   a) Tietoturva ei välttämättä edellytä vahvojen salausalgoritmien käyttöä.
   b) Yrityksen kannattaa tallettaa itselleen kopiot tärkeistä salausavaimista.
   c) Verkkokauppa voidaan suunnitella siten, että edustalla olevan WWW-palvelimen turvan murtuminen ei avaa pääsyä koko järjestelmään.
   d) Tietoturvan tason mittaaminen on mahdollista.
   e) Kun on aihetta epäillä tietomurtoa, tärkeintä on irrottaa yrityksen verkko Internetistä.
   f) Internetin IP-osoitteita ei voi jäljittää.

3 a) Kuvaa kaksi etua palomuuriohjelmiston sijoittamisesta työasemaan, yrityksen lähiverkon ja Internetin yhdistävän palomuurin lisäksi. (2 p)
   b) Mitä tarvitaan yrityksen lähiverkon Internetiin yhdistävältä palomuurilta, jotta se pystyisi torjumaan sähköpostiviestissä olevan viruksen? (2p)
   c) Kuvaile lyhyesti yksi tietoturvaan liittyvä standardi, josta on hyötyä suunniteltaessa organisaation tietoturvaa. (1 p)
   d) Kuvaile lyhyesti jokin tietoturvaan liittyvä ammatillinen pätevöitymistutkinto. (1 p)

4 Tiedon salaus ja suojaus (6 p)
   a) Mitä salausavaimia tarvitaan salatun ja allekirjoitetun sähköpostiviestin lähettämiseen, kun oletetaan käytännön tilanne ja viesti on kooltaan suuri? Kuvaile kunkin salausavaimen käyttö ja mistä ko. avain saadaan. (3 p)
   b) Kuvaile yksi tapa murtaa järjestelmän salasana, jos käytettävissä on salasanojen tiivistetiedosto (hash file)? (1 p)
   c) Kuvaile jokin WWW-järjestelmän lomakkeiden syötteen kautta suoritettava hyökkäys ja miten sitä vastaan puolustaudutaan suunniteltaessa ja toteutettaessa järjestelmää. (2 p)

5 Palvelinohjelmistossa, esimerkiksi WWW- tai sähköpostipalvelimessa voi olla haavoittuvuuksia tai turva-aukkoja, joiden kautta hyökkääjä saa pääsyn palvelinkoneeseen. Miten tällaisia aukkoja syntyy? Kuvaile kaksi erityyppistä aukkoa ja niiden hyväksykäyttö yleisellä tasolla. Miten estäisit turva-aukkojen synnyn johtamassasi ohjelmistoprojektissa (kerro ainakin kaksi menetelmää, joita hyödynnät)? (6 p)