T-110.4200 Tietoturvallisuustekniikka
Tentti 11.5.2007

1 Selitä lyhyesti seuraavat tietoturvallisuuteen liittyvät käsitteet. (6 p)
a) Varmenne
b) Salaisen avaimen salaus
c) Tiivistefunktio
d) BS 7799 (ISO 17799)
e) Julkisen avaimen salaus
f) Puskurin ylivuoto

2 Perustele lyhyesti mitkä seuraavista väitteistä pitävät paikkansa ja mitkä eivät. (6 p)
a) Rootkit on joukko ohjelmia, joilla murtautuja piilottaa jälkensä
b) Vanhoista WWW-palveluista voidaan tehdä turvallisia suojaamalla kone palomuurilla ja yhteys SSL:llä
c) Common Criteria -hyväksynnän saanutta tuotetta voidaan käyttää missä tahansa ympäristössä ilman pelkoa turvan pettämisestä
d) Yksi ACL:n (access control list) hyvistä puolista on, että sen avulla on helppo selvittää yhden objektin kaikki oikeudet.
e) Helpoin ja kokonaistaloudellisin tapa suojata verkkoon palveluita tarjoava ohjelma on pitää sen koodi salaisena
f) Varmenteella ei ole mitään merkitystä, jos sen voimassaoloa ei tarkasteta CRL-listasta

3 Palomuurit (6 p)
Miten pakettisuodattavat ja sovellustason palomuurit toimivat? Mitkä ovat tärkeimmät erot niiden tarjoamassa suojassa? Anna esimerkki tilanteesta, johon pakettisuodatin soveltuu paremmin ja toinen esimerkki, johon sovellustason palomuuri on sopivampi

4 Salasanat (6 p)
a) Nimeä ja kuvaa kaksi hyökkäystä, joiden tarkoitus on selvittää *kenen tahansa* järjestelmän käyttäjän salasana. (2 p)
b) Nimeä ja anna esimerkki kahdesta hyökkäyksestä joiden tarkoitus on selvittää *tietyn käyttäjän* salasana ja jotka eroavat a-kohdan hyökkäyksistä. (2 p)
c) Salasana on esimerkki todentamismenetelmästä joka perustuu periaatteelle "mitä käyttäjä tietää". Nimeä kaksi muuta periaatetta ja anna esimerkki niihin liittyvistä todentamismenetelmistä. (2 p)

5 Monitasomallit ja multilateraalin turvan mallit (6 p)
Kurssilla on esitelty useita formaaleja tai puoliformaaleja turvamalleja (BLP, Biba, jne.). Kuvaa kaksi näistä malleista. Liitä kuvaukseesi:
- Mallissa käytettävät säännöt, formaalisti jos mahdollista.
- Anna esimerkki siitä, mihin mallia voidaan käyttää ja mitkä olisivat tällöin sen subjektit ja objektit.