Cezzar

TTY / TLT / M.Helenius

TLT-3201 Tietoturvallisuuden jatkokurssi
Tentti I 18. 1. 2010

Tentissä ei saa käyttää oheismateriaalia eikä laskinta.

Merkitse vastauspaperiin nimesi viereen sitova valinta, oletko tekemässä A- vai AB-tenttiä. Sen mukaan määräytyy, kumpi versio tehtävästä 5 vaaditaan. Muissa tehtävissä on [B]:llä merkittyjä kohtia, jotka edellytetään vain AB:n tenttijöiltä. Niissä on mainittu myös maksimipistemäärä. Se vähentää AB-tentissä saman tehtävän muiden kohtien osuutta 6 pisteestä, joka on kaikissa tehtävissä maksimipistemäärä. Kyseisten muiden kohtien vaativuus pysyy silti samana kuin se on pelkässä A-tentissä.

1. Tässä ovat tutkielmakysymykset. Tarkoitus on, että jokainen saa valita seitsemästä muita kuin omaa työtä koskevasta kysymyksestä *kuusi*, joihin vastaa. Jos oma kysymyksesi ei ole kysymysten (1) – (7) joukossa, valitse niistä kuusi ja vastaa niihin. Muussa tapauksessa valitse kysymyksistä (1) – (8) kuusi muuta kuin omasi ja vastaa niihin.

(1) Mitä tarkoitetaan mobiilivarmenteella ja mihin sitä käytetään?
(2) Mikä on asiakaskoneiden merkitys tietoturvan kannalta NAS- ja SAN-verkoissa?
(3) Kerro biometristen henkilökorttien tietoturvan puutteista ja niistä johtuvista ongelmista.
(4) Mitä merkitystä matkapuhelimen Bluetooth-nimellä on tietoturvan kannalta?
(5) Miten saastunut kone voi heikentää verkon toimintaa ja miten sellainen havaitaan verkkopelitapahtumassa?
(6) Miten sähköisessä äänestyksessä voidaan yrittää taata, ettei ääntä ole annettu painostuksen alla?
(7) Mihin SPF:n (Sender Policy Framework), DomainKeysin ja SenderID:n toiminta perustuu ja mitä niiden avulla pyritään estämään?
(8) Mitä asioita HTTP API:n tietoturvan suunnittelussa kannattaa ottaa huomioon?

2. Miten RAID ja sen eri tasot toimivat? Mikä vaikutus eri tasoilla on luotettavuuteen ja suorituskykyyn?

3. (i) Bell LaPadula sekä Biba ovat eräänlaisia pääsynvalvonnan malleja. Kuvaa mallien periaatteet.

(ii) [B, 2p] Miten RBAC toimii ja mitkä ovat sen etuja verrattuna perinteiseen pääsynvalvontaan?

4. (i) Mitä salasanatietokannan toteutuksessa tulee ottaa huomioon?

(ii) [B, 2p] Miten EKE-protokollalla toteutetaan salasanan vahventaminen?

5. [A] Mitä bittiin sitoutuminen tarkoittaa ja miten se toteutetaan? Vastauksessa kaivataan paitsi toimintaperiaatteita myös matemaattista mallia.

5. [B] Mitä tarkoittaa kieltämätön allekirjoitus ja miten se toteutetaan? Vastauksessa kaivataan paitsi toimintaperiaatteita myös matemaattista mallia.