TTY / TIE / J. Harju, J. Koskinen

TIE-03100 Tietoverkot ja tietoturva
Tentti I 18.12.2013

Tentissä ei saa käyttää laskinta. Tätä tehtäväpaperia ei tarvitse palauttaa.
Sekä rastilomake että konseptiarkki pitää palauttaa.

Kirjoita vastauksesi tehtäviin 1-3 konseptiarkille ja rastitehtäviin 4-39 lomakkeelle. Kirjoita kummallekin nimesi ja opiskelijanumerosi. Lomakkeelle opiskelijanumero pitää merkitä myös rastimalla ao. numeromerkit. Tee rastitehtävien luonnokset ja korjaukset mieluummin tälle paperille kuin lomakkeelle! Tentin jälkeen voit silloin myös helpommin verrata vastauksiasi kurssin Moodlesta löytyvään oikeaan riviin sekä aikanaan tuloslistassa julkaistaviin vastauksiin, jotka on luettu lomakkeeltasi.

Kussakin rastitehtävässä on vain yksi oikea vastaus. Oikeasta vastauksesta tulee 1 piste. Jos rasteja ei ole yhtään tai niitä on enemmän kuin yksi, tehtävästä tulee 0 pistettä. Väärä vastaus vähentää pistetiliä 1/3 pisteellä.

---

1. Yrityksen langallinen lähiverkko koostuu reitittimestä, siihen liitetystä kolmesta Ethernet-kytkimestä, kannettavista tietokoneista, tulostinpalvelimesta, levypalvelimesta ja intranet-palvelimesta, sekä yhteydestä Internetiin. Ethernet-kytkimet on kytketty kukin omaan reitittimen porttiinsa ja päätelaitteet on jaettu kahden kytkimen kesken. Palvelimet on kytketty kolmanteen kytkimeen. Internet-yhteydelle on oma reitittimen porttinsa. Oletetaan sitten, että yrityksen työntekijä A lataa www-sivun oman firmansa intranet-palvelimesta.
   a) Piirrä yhteen kuvaan koko verkon fyysinen toteutus ja toiseen kuvaan www-yhteyden ns. halkileikkaus, jossa näkyvät yhteyden varrella olevat laitteet ja niiden protokollapinot. (4p)
   b) Selosta sanallisesti IP-paketin matka käyttäjän A päätelaitteesta palvelimelle. Vastaa erityisesti seuraaviin kysymyksiin: miten alemmat kerrokset toimivat, mitä osoitteita käytetään missäkin matkan vaiheessa, ja mitä apuprotokollia tarvitaan tai voidaan tarvita? (4p)

2. Reititys ja IP-protokolla ovat Internetin toiminnan keskeisimpiä asioita.
   a) Mitä tarkoitetaan IP-aliverkolla, miten se määritellään IP-osoitteen avulla ja mikä on sen merkitys reitityksen kannalta? (2p)
   b) Mitkä ovat reitittimen perustehtävät? (2p)
   c) Mitä reititysprotokollat tekevät ja missä verkon laitteissa ne yleensä toimivat? (2p)
   d) Mitä tarkoitetaan autonomisella systeemillä (AS) ja miten se liittyy reititykseen ja reititysprotokolliin? (2p)

3. Tarkastellaan erityyppisiä tietoliikenneverkkoja.
   a) Millainen on pääsyverkkojen rakenne ja mitä tiedonsiirtomedioita siellä on käytössä? (2p)
   b) Mitä ovat runkoverkot, miten ne eroavat pääsyverkoista ja mitä tiedonsiirtomedioita niissä käytetään? (2p)
   c) Millainen on mobiiliverkkojen rakenne ja mitä tiedonsiirtomedioita niissä käytetään? (2p)
   d) Miten mobiiliverkot eroavat langattomista lähiverkoista? Tarkastele sekä teknisiä seikkoja että eroavaisuuksia verkkojen käyttötavassa ja hallinnoinnissa. (2p)

---

4. **Mikä on aliverkon 130.230.4.0/25 viimeinen osoite eli broadcast-osoite?**
   a. ( ) 130.230.4.95
   b. (x) 130.230.4.127
   c. ( ) 130.230.7.255
   d. ( ) 130.230.4.255

5. **ADSL-tekniikkaan perustuvan pääsyverkon tiedonsiirtomedia on**
   a. ( ) radiotie.
   b. (x) kierretty parikaapeli.
   c. ( ) optinen kuitu.
   d. ( ) koaksiaalikaapeli.

6. **Oletetaan, että päätelaitteen A ja palvelimen B välinen tietoliikenneyhteys koostuu langattomasta lähiverkosta, joka on yhdistetty langalliseen Ethernet-pohjaiseen reititinverkkoon. Mitkä seuraavista laitteista käsittelevät A:n ja B:n välisellä TCP-yhteydellä kulkevan paketin TCP-headeria päätelaitteen ja palvelimen lisäksi? (i) langaton tukiasema, (ii) Ethernet-verkon kytkimet, (iii) verkon reitittimet.**
   a. (x) ei mikään
   b. ( ) vain (i)
   c. ( ) vain (ii)
   d. ( ) vain (iii)

7. **Internetissä tarvitaan luotettavaa yhteydellistä kuljetusprotokollaa, koska**
   a. ( ) yhteyksille olisi muuten mahdotonta taata riittävää tietoturvatasoa.
   b. (x) verkkokerroksen protokolla IP on yhteydetön ja siksi epäluotettava.
   c. ( ) reaaliaikavaatimukset (eli vaatimukset pienestä viiveestä ja viiveenvaihtelusta) edellyttävät luotettavaa kuljetusprotokollaa.
   d. ( ) fyysisellä kerroksella tapahtuneet bittivirheet voi korjata vain kuljetuskerroksella.

8. **IP-aliverkon oletusreititin**
   a. ( ) on reititin, jonka IP-osoite on 0.0.0.0.
   b. (x) on reititin, jolle IP-aliverkon laite lähettää paketit, jotka ovat menossa ulos ko. IP-aliverkosta.
   c. ( ) on reititin, jonka avulla tapahtuu pakettien jakelu IP-aliverkon sisällä.
   d. ( ) on reititin, jolle muualta Internetistä lähetetään paketit, joiden kohde on ko. IP-aliverkossa.

9. **Autonomisen järjestelmän (AS) sisäisessä reitityksessä**
   a. ( ) riittää se, että käytetään MAC-osoitteita ja ARP-protokollaa.
   b. ( ) riittää käyttää staattista reititystä.
   c. (x) pyritään optimoimaan reititystä ja käytetään mm. OSPF-protokollaa.
   d. ( ) reititysprotokollana käytetään BGP:tä.

10. **Sähköpostijärjestelmän SMTP-protokolla**
    a. (x) pyrkii toimittamaan viestit lähettäjän sähköpostipalvelimelta suoraan vastaanottajan sähköpostipalvelimelle.
    b. ( ) sallii sisääntulevat yhteydet vain luotetuiksi todennetuilta SMTP-palvelimilta.
    c. ( ) vie viestit vastaanottajan päätelaitteeseen asti.
    d. ( ) käyttää relay-solmuja ja P2P-tekniikkaa apuna viestien kuljettamisessa.

11. **HTTP:lle ja HTML:lle pätee, että**
    a. ( ) HTTP on kuvauskieli ja HTML on protokolla.
    b. ( ) molemmat ovat protokollia.
    c. ( ) molemmat ovat kuvauskieliä.
    d. (x) HTTP on protokolla ja HTML on kuvauskieli.

12. **Satunnaisuuteen perustuvat MAC-algoritmit (merkityksessä Media Access Control) ovat erityisen tärkeitä**
    a. ( ) point-to-point-yhteyksillä.
    b. ( ) yksisuuntaisissa broadcast-verkoissa.
    c. (x) langattomissa lähiverkoissa.
    d. ( ) aikajakokanavoiduilla yhteyksillä.

13. **Valitse laajin paikkansa pitävä vastausvaihtoehto: Tracerouten avulla laite voi yrittää selvittää,**
    a. ( ) onko kohde liitetty verkkoon.
    b. ( ) minkä reitittimien kautta reitti kohteeseen kulkee.
    c. ( ) mikä on RTT kohteeseen.
    d. (x) kaikki edellä mainitut asiat.

14. **Päätelaitteen pitää lähettää IP-paketti kohdelaitteelle, joka IP-osoitteen mukaan sijaitsee samassa aliverkossa, jossa lähettäjäkin on. Suoran toimitustavan periaatteen mukaisesti päätelaitteen tulee selvittää kohteen MAC-osoite. Tähän se käyttää apunaan protokollaa nimeltä**
    a. ( ) DNS.
    b. ( ) DHCP.
    c. ( ) ICMP.
    d. (x) ARP.

15. **Reititysvirheen sattuessa IP-paketti voi jäädä kiertämään kehää verkossa (ns. reitityssilmukka). Tilanteen pelastaa**
    a. ( ) alemman kerroksen protokolla, joka huomaa tilanteen ja tuhoaa paketin.
    b. (x) time-to-live-laskuri, jonka meneminen nollaksi aiheuttaa paketin tuhoamisen.
    c. ( ) kuljetuskerroksen protokolla, joka raportoi asiasta lähettäjälle.
    d. ( ) ICMP-protokolla, joka huomaa silmukan ja palauttaa paketin lähettäjälle.

16. **Kuljetusprotokollan headerissa kohdeportin numero identifioi**
    a. ( ) käyttäjän (ihmisen), jolle viesti on tarkoitettu.
    b. (x) sovelluksen, jolle paketin sisältämä data (payload) on tarkoitettu.
    c. ( ) Ethernet-kytkimen porttinumeron kohteena olevassa IP-aliverkossa.
    d. ( ) seuraavan reitittimen portin paketin matkatessa kohti kohdettaan.

17. **Valitse laajin paikkansa pitävä vastausvaihtoehto: DNS-järjestelmästä voi kysyä**
    a. ( ) domain-nimestä vastuussa olevan viranomaisen osoitetta.
    b. (x) IP-osoitteeseen liittyvää domain-nimeä.
    c. ( ) IP-osoitteeseen liittyvän IP-aliverkon omistajan tietoja.
    d. ( ) kaikkia edellä mainittuja asioita.

18. **TCP/IP-pinon kerrokset ylhäältä alaspäin ovat**
    a. ( ) sovellus-, istunto-, kuljetus-, verkko- ja fyysinen kerros.
    b. ( ) sovellus-, esitystapa-, verkko-, siirto- ja fyysinen kerros.
    c. ( ) sovellus-, siirto-, kuljetus-, verkko- ja fyysinen kerros.
    d. ( ) sovellus-, kuljetus-, verkko-, siirto- ja fyysinen kerros.

19. **Mikä seuraavista mobiiliverkkoja ja niiden sukupolvia koskevista väitteistä ei pidä paikkaansa?**
    a. ( ) Ensimmäisen sukupolven mobiiliverkot pohjautuivat analogiatekniikkaan.
    b. ( ) Pakettikytkentäinen datansiirtopalvelu GPRS tuli mukaan 2. sukupolven mobiiliverkkoihin.
    c. (x) Kolmannen sukupolven 3G-verkko pystyy tarjoamaan yli 100 Mbit/s tiedonsiirtonopeuksia.
    d. ( ) Neljännen sukupolven mobiiliverkkotekniikasta käytetään nimeä LTE tai LTE Advanced.

20. **Mikä seuraavista väitteistä ei pidä paikkaansa:**
    a. (x) IEEE 802.3:n mukainen Ethernet-protokolla ja vanhempi Ethernet II -protokolla eivät voi molemmat liikennöidä samassa verkossa.
    b. ( ) Ethernetin osoitteet (ns. MAC-osoitteet) ovat pituudeltaan kuusi tavua.
    c. ( ) Ethernetin MAC-algoritmi on nimeltään CSMA/CD.
    d. ( ) Ethernetin IEEE 802.3 -standardi sallii sen, että kehyksen pituus on ilmoitettu Ethernet-protokollan headerissa.

21. **Pakettikytkentä on tänä päivänä piirikytkentää tehokkaampi, koska**
    a. (x) purskeinen tiedonsiirto sopii hyvin pakettikytkennän periaatteisiin.
    b. ( ) piirikytkentäisessä verkossa ei voi siirtää digitaalista dataa.
    c. ( ) puheensiirron laatuvaatimukset ovat kiristyneet.
    d. ( ) resurssien varaus pakettikytkentäisestä verkosta on helpompaa.

22. **Käsite tietoverkon tietoturva kattaa tietyn osan tietoverkkoon liittyvästä tietoturvasta. Mikä seuraavista kuuluu sen piiriin, selvemmin kuin muut?**
    a. ( ) Julkisen avaimen varmenteita myyvän yrityksen yksityisen avaimen päätyminen hyökkääjän käsiin.
    b. (x) Välimieshyökkäys, jossa verkkoasema tekeytyy toiseksi ja saa haltuunsa liikennettä joka ei ole tarkoitettu sille.
    c. ( ) Sähköpostiviestin salaiseksi tarkoitetun vastaanottajalistan näkyminen kaikille vastaanottajille.
    d. ( ) Työaseman ohjelmistossa oleva haavoittuvuus, joka antaa hyökkääjälle tilaisuuden käyttää työasemaa verkon ylitse ilman lupaa.

23. **Yksityistä avaintaan soveltamalla avaimen haltija pystyy muodostamaan vastaavan julkisen avaimen K ja oman identiteettinsä välille kytkennän,**
    a. (x) josta voi olla se hyöty, että toiset tietävät, että kytkennän muodostaja tuntee K:ta vastaava yksityisen avaimen.
    b. ( ) josta ei ole hyötyä, jos pitää kasvattaa muiden tietoa siitä, kenen hallussa K:ta vastaava yksityinen avain mahdollisesti on.
    c. ( ) jonka perusteella toiset saavuttavat luottamuksen siihen, kenen hallussa K:ta vastaava yksityinen avain on.
    d. ( ) jonka avulla toiset voivat luottaa väitteisiin siitä, kenen hallussa K on.

24. **Mikä seuraavista pätee matkapuhelinten 2G- ja 3G-järjestelmissä? Tässä "puhelin autentikoituu" tarkoittaa, että sen SIM/USIM autentikoituu.**
    a. ( ) Puhelin autentikoituu puhelinverkolle 3G:ssä mutta ei 2G:ssä.
    b. ( ) Puhelin autentikoituu 3G:ssä vastaanottavalle 3G-puhelimelle, mutta vastaavaa ei tapahdu 2G:ssä.
    c. ( ) Molemmissa puhelinverkko autentikoituu puhelimelle.
    d. (x) Molemmissa puhelin autentikoituu puhelinverkolle.

25. **Henkilötietolain mukaan arkaluonteinen henkilötieto on henkilön**
    a. (x) osoite.
    b. ( ) lapsen nimi.
    c. ( ) entinen sukunimi.
    d. ( ) ammattiliiton nimi.

26. **Digitaalinen allekirjoitus ei ole lainvoimainen, jos se todentuu teknisesti, mutta**
    a. (x) sillä allekirjoitettua sähköistä tietoa on muutettu.
    b. ( ) jälkeenpäin tehty uusi allekirjoitus kumoaa sen.
    c. ( ) allekirjoittaja ilmoittaa, että hän on tehnyt sen erehdyksessä.
    d. ( ) allekirjoittajalla ei ole enää hallussaan välinettä, jota hän käytti allekirjoituksen tekoon.

27. **Hyökkääjän pääsy tietoverkon kautta aiheuttamaan harmia toteutuu neljän vaiheen kautta, jotka ovat tiivistettyinä aakkosjärjestyksessä haavoittuvuus, prosessi, tieto ja valtuuttamaton toimi. Mikä on oikea yleispätevä järjestys?**
    a. ( ) Tieto haavoittuvuudesta antaa hyökkääjälle mahdollisuuden käynnistää valtuuttamattomasti prosessi.
    b. ( ) Haavoittuvuus käynnistää prosessin, jonka hyökkääjä saa haltuunsa ja voi siten vahingoittaa/saada selville tietoa.
    c. (x) Haavoittuvuus antaa mahdollisuuden valtuuttamattomaan toimeen, jossa hyökkääjä saa käyntiin prosessin, joka kohdistuu tietoon.
    d. (x) Hyökkääjän käynnistämä prosessi käyttää haavoittuvuutta valtuuttamattomaan toimeen tietoa kohtaan.

28. **Tutki väitettä: "Palvelimen lähettämän varmenteen voi asentaa selaimeen siten, että SSL/TLS voi käyttää sitä jatkossa saman palvelimen yksityisen avaimen todentamiseen." Väite on**
    a. ( ) tosi, mutta selain täytyy ensi sammuttaa ja käynnistää uudelleen.
    b. (x) tosi, eikä selainta tarvitse käynnistää uudelleen.
    c. ( ) epätosi, sillä SSL/TLS ei todenna palvelimen yksityistä avainta vaan yksityisellä avaimella tehdyn allekirjoituksen.
    d. ( ) epätosi, sillä selaimeen ei voi asentaa varmenteita vaan julkisia avaimia.

29. **Mikä on julkista RSA:ssa eli Rivestin, Shamirin ja Adlemanin julkisen avaimen kryptosysteemissä?**
    a. (x) vain salauksen moduuli eli luku jonka suhteen lasketaan jakojäännös
    b. ( ) salauseksponentti ja luku jonka suhteen korotuksen tuloksesta otetaan jakojäännös
    c. ( ) vain salauseksponentti
    d. ( ) alkuluvut, joiden suhteen voidaan laskea neliöjuuria mutta ei diskreettejä logaritmeja

30. **Mikä seuraavista toteuttaa huonoimmin varsinaisen varmuuskopioinnin tavoitteita?**
    a. (x) ajoittainen inkrementaalikopiointi täyskopioiden sijasta
    b. ( ) Snapshot-tekniikkaa käyttävä tiedostojärjestelmä
    c. ( ) kirjoitettavien CD-levyjen käyttö
    d. ( ) sellainen päivittäinen varmuuskopiointi, jota ei joka kerta tarkisteta

31. **Suojamekanismeja valittaessa on otettava huomioon tietoturvaprosessin eri vaiheita, joihin ne voivat soveltua. Mitkä kolme?**
    a. (x) välttäminen, estäminen ja havaitseminen.
    b. ( ) politiikan muodostaminen, uhkien torjunta ja vahinkojen korjaaminen.
    c. ( ) suunnittelu, toteutus ja valvonta.
    d. ( ) ehkäisy, havaitseminen ja reagointi.

32. **Minkä yritys on säädetty rangaistavaksi: (i) Salassapitorikos, (ii) Salassapitorikkomus, (iii) Viestintäsalaisuuden loukkaus, (iv) Törkeä viestintäsalaisuuden loukkaus?**
    a. (x) (i) - (iv)
    b. (x) (i) & (iii) & (iv)
    c. ( ) (i) & (ii)
    d. ( ) (iii) & (iv)

33. **Www-sivuja julkaisevien palveluntuottajien tietoturvahuolten neljä luokkaa kurssimateriaalissa ovat (i) palvelun saatavuus, (ii) palvelun eheys, (iii) maksun saaminen ja (iv) vastuut. Palveluja käyttävät selaajat voivat tuottaa ongelmia tuottajalle kaikissa näissä luokissa. Missä luokassa tämä voi tapahtua helpoimmin ilman pienintäkään pahuutta?**
    a. (x) (i)
    b. (x) (iii)
    c. ( ) (iv)
    d. ( ) (ii)

34. **Mikä on yhteinen piirre kaikille pahoille ohjelmille?**
    a. (x) Ne pystyvät samankaltaisiin toimiin kuin muut niiden ajoympäristön ohjelmat.
    b. ( ) Ne leviävät ohjelmistoissa olevien haavoittuvuuksien kautta.
    c. ( ) Ne on suunnattu jonkin taloudellisen tavoitteen toteuttamiseen.
    d. ( ) Ne on suunnattu johonkin kohteeseen, vaikka ne yleensä leviävät muuallekin.

35. **Oletetaan, että sinulla on julkisesti nähtävillä olevat www-kotisivut. Tietosuojasäännökset kieltävät**
    a. ( ) www-palvelimen ylläpitäjää luovuttamasta kotisivusi tietoja arkistoitaviksi.
    b. ( ) sinua ylläpitämästä vieraskirjaa, johon pyydät kävijöitä kirjoittamaan henkilökohtaiset terveisensä.
    c. (x) sinua ylläpitämästä osoitemuistiotasi kotisivulla.
    d. ( ) sinua sijoittamasta sivuillesi mainoksia sellaisilta tahoilta, jotka käyttävät cookie-tekniikkaa käyttäjien seurantaan monien eri sivustojen alueella.

36. **Mitä palomuurin tulee yleisimmin tehdä, kun se on hylännyt jonkin paketin muusta kuin siitä syystä että se ei ole standardin mukainen?**
    a. ( ) Lähettää hälytys tunkeutumisen havaitsemisjärjestelmään.
    b. ( ) Antaa käyttäjälle varoitus.
    c. ( ) Käsitellä seuraava paketti erilaisella säännöllä.
    d. (x) Kirjoittaa paketin tunnisteet lokitiedostoon.

37. **Missä IPsecin toimintamoodeista salataan koko alkuperäinen IP-paketti?**
    a. ( ) autentikointimoodissa
    b. ( ) kuljetusmoodissa
    c. (x) tunnelointimoodissa
    d. ( ) turvamoodissa

38. **Mikä seuraavista ei kuulu käsitteen kryptoalgoritmi piiriin?**
    a. ( ) haaste-vaste -menetelmä
    b. ( ) hash-funktio
    c. ( ) avaimellinen tiivistefunktio
    d. (x) satunnaislukugeneraattori

39. **Tutki väitettä: Tietoturvatavoitteena saatavuus tai käytettävyys tarkoittaa, että tiedot tai palvelut ovat tallella ja niihin pääsee käsiksi ennemmin tai myöhemmin. Se on epätosi, koska**
    a. ( ) termiä käytettävyys ei pidä käyttää samassa merkityksessä kuin termiä saatavuus.
    b. ( ) saatavuus edellyttää, että tietoihin päästään käsiksi jonkin asetetun aikarajan puitteissa.
    c. ( ) tietoturvamielessä saatavuus koskee vain tietoja ja käytettävyys vain palveluja.
    d. (x) käytettävyys edellyttää myös sitä, että tiedot eivät ole hallitsemattomasti muuttuneet.