Mika Laatikainen

TTY / TIE / J. Harju

TIE-03100 Tietoverkot ja tietoturva

Tentti 7.12.2015

Tentissä ei saa käyttää laskinta. Tätä tehtäväpaperia ei tarvitse palauttaa.

Sekä rastilomake että konseptiarkki pitää palauttaa. Huom. palautus ERI nippuihin: älä sijoita rastilomaketta konseptiarkin sisään!

Kirjoita vastauksesi esseetehtäviin 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.

TEHTÄVÄT 1-3 OVAT ESSEETEHTÄVIÄ, MAX 8p/teht. VASTAA KONSEPTIARKILLE!

---

1. a) Olet tiedustelupalvelun tietotekniikka-asiantuntija ja olet saanut haltuusi käyttäjätunnus- ja salasanatiedoston palvelusta, jonka asiakkaista työnantajasi haluaa tietää mahdollisimman paljon. Tiedostossa tiedot eivät näyttäisi olevan selväkielisiä. Millaisilla menetelmillä lähdet selvittämään tunnuksia ja salasanoja? (4p)

   b) Olet treffipalvelun asiakas ja kuulet, että palvelun asikkaiden tunnukset ja salasanat ovat vuotaneet julkisuuteen. Palveluntarjoaja kuitenkin vakuuttaa, että kaapatussa tiedostossa olleet tiedot oli asianmukaisesti suojattu. Millaisia periaatteita sinun olisi pitänyt salasanan valinnassa noudattaa, jotta voisit olla rauhallisin mielin sikäli, että tämän usein käyttämäsi palvelun salasana tuskin paljastuu hyökkääjille? (4p)

2. Listaa protokollien kerrosmallin kerrokset ylhäältä alaspäin ja luonnehdi lyhyesti kunkin kerroksen tehtävää. Oleellista ei ole se, että muistat kerroksen nimen täsmälleen oikein, vaan yritä kunkin kerroksen kohdalla vastata kysymykseeen: Miksi tämä kerros on tarpeen, jotta tietoliikennejärjestelmä saadaan toimimaan tarkoituksenmukaisella tavalla?

3. 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) Mitä tarkoitetaan mobiiliverkkojen sukupolvilla (generation) ja mitkä sukupolvet tällä hetkellä ovat yleisessä käytössä? (2p)
   d) Miten mobiiliverkot eroavat langattomista lähiverkoista? Tarkastele sekä teknisiä seikkoja että eroavaisuuksia verkkojen käyttötavassa ja hallinnoinnissa. (2p)

MONIVALINTAOSUUS ALKAA TÄSTÄ: VASTAA ERILLISELLE LOMAKKEELLE!

---

4. **Käsite tietoverkon tietoturva kattaa tietyn osan tietoverkkoon liittyvästä tietoturvasta. Mikä seuraavista kuuluu sen piiriin, selvemmin kuin muut?**
   a. ( ) Arkaluonteisen Word- tai OpenOffice-dokumentin suojaksi asetetun salasanan murtuminen brute-force -hyökkäyksellä.
   b. ( ) Viranomaisten mahdollisuus luoda peiteoperaatioitaan varten anonyymia Bitcoin-verkkorahaa.
   c. ( ) Verkon päätelaitteen käyttöjärjestelmässä oleva haavoittuvuus.
   d. ( ) WWW-palvelimen toiminnan lakkaaminen, kun siihen kohdistetaan DoS-hyökkäys useista eri osoitteista.
5. **Mikä seuraavista kerrosten tehtäviä kuvaavista vaihtoehdoista ei pidä paikkaansa:**
   a. ( ) Internetin verkkokerroksen protokolla IP on yhteydellinen.
   b. ( ) siirtokerros vastaa kehysten siirrosta yhden linkin yli.
   c. ( ) kuljetuskerroksen protokollat ovat ns. päästä-päähän-protokollia.
   d. ( ) fyysinen kerros käsittelee bittejä - ei kehyksiä.
6. **Henkilötietolain mukaan arkaluonteinen henkilötieto on henkilön**
   a. ( ) ammattiliiton nimi
   b. ( ) entinen sukunimi
   c. ( ) lapsen nimi
   d. ( ) vanhemman nimi
7. **Kuljetusprotokollan headerissa kohdeportin numero identifioi**
   a. ( ) Ethernet-kytkimen porttinumeron kohteena olevassa IP-aliverkossa.
   b. ( ) sovelluksen, jolle paketin sisältämä data (payload) on tarkoitettu.
   c. ( ) seuraavan reitittimen portin paketin matkatessa kohti kohdettaan.
   d. ( ) käyttäjän (ihmisen), jolle viesti on tarkoitettu.
8. **Mikä on välttämätöntä, jotta kahden suuren alkuluvun p ja q tuloa voi käyttää julkisen avaimen kryptografiassa julkisena avaimena?**
   a. ( ) Kyseiset alkuluvut eivät saa olla muiden kuin omistajansa tiedossa.
   b. ( ) Pitää tarkistaa onko kyseisiä alkulukuja vastaavaa yksityistä avainta olemassa.
   c. ( ) Täytyy julkaista myös p*p modulo q, tai q*q modulo p.
   d. ( ) Pitää tarkistaa, ovatko myös p-1 ja q-1 alkulukuja.
9. **Internetissä yhteydetönkin (ja siten epäluotettava) kuljetusprotokolla on hyödyllinen, koska**
   a. ( ) sovelluksille on se ja sama onko kuljetuskerroksella käytössä yhteydellinen vai yhteydetön kuljetusprotokolla.
   b. ( ) bittivirheet ja pakettien katoamiset tapahtuvat fyysisellä kerroksella ja ne korjataan siirtokerroksella.
   c. ( ) reaaliaikavaatimukset (eli vaatimukset pienestä viiveestä ja viiveenvaihtelusta) usein edellyttävät yhteydetöntä kuljetusprotokollaa.
   d. ( ) verkkokerroksen protokolla IP on yhteydellinen.
10. **Mikä seuraavista väitteistä ei ole totta käytettäessä UDP-protokollaa?**
    a. ( ) Pakettien perille saapuminen ei ole taattu.
    b. ( ) Paketti osoitetaan aina johonkin porttiin, jonka numero kulkee paketin otsikkokentässä.
    c. ( ) Paketit eivät saavu perille välttämättä lähetysjärjestyksessä.
    d. ( ) Paketin vastaanottaja lähettää ACK-sanoman lähettäjälle, jos paketti tuli perille.

11. **Jos palomuuri hylkää jonkin paketin,**
    a. ( ) se lähetetään takaisin sinne, mistä se tulikin.
    b. ( ) sen kryptografinen tiiviste kirjoitetaan lokitiedostoon.
    c. ( ) voidaan jättää lokimerkintä myös tekemättä.
    d. ( ) se kirjoitetaan lokitiedostoon.
12. **Koska SSL/TLS toimii sovelluskerroksen alapuolella, se**
    a. ( ) ei tiedä, millaista dataa sen avulla suojataan.
    b. ( ) ei pysty suojaamaan selaimeen kirjoitettua salasanaa sen matkatessa palvelimelle.
    c. ( ) pystyy suojaamaan sovellustasolla toimivan liiketoiminnan kokonaisuuden.
    d. ( ) ei pysty järjestämään salattua yhteyttä sovellusten välille.
13. **Mikä seuraavista ei päde reitityksessä:**
    a. ( ) reititystaulunsa perusteella reititin päättelee, mikä on seuraava etappi IP-paketin matkatessa kohti kohdettaan.
    b. ( ) reititin voi hylätä paketin, jos sille ei löydy reittiä eteenpäin.
    c. ( ) reititystaulunsa perusteella reititin muodostaa vastaavuuden paketin lähettäjän ja kohdelaitteen MAC-osoitteiden välille.
    d. ( ) runkoverkon reitittimen reititystaulu voi sisältää yli 300.000 kohdealiverkkoa.
14. **Epäsymmetristen kryptosysteemien avaimiin liittyvä termi PKI tulee sanoista**
    a. ( ) Public Key Infrastructure
    b. ( ) Private Key-ring Integrity
    c. ( ) Private Key Integrity
    d. ( ) Public Keys for Internet
15. **Mikä seuraavista on tyypillistä tarkistussummille, jotka on tarkoitettu torjumaan erilaisten numeroiden tai merkkijonojen syötössä tapahtuvia näppäilyvirheitä? Se**
    a. ( ) sijoitetaan hajautettuna useamman merkin alueelle.
    b. ( ) lasketaan yhteenlaskulla muista merkeistä.
    c. ( ) lasketaan kaikista muista merkeistä.
    d. ( ) sijoitetaan aina numerosarjojen alkuun tai loppuun.
16. **Materiaalissa sanotaan: "Avaintenvaihto on yksi tärkeimmistä kryptografisista protokollista." Mitä avaintenvaihto, eli 'key exchange' tässä tarkoittaa?**
    a. ( ) Julkinen avain peruutetaan ja uusi varmennetaan.
    b. ( ) Vanha symmetrinen avain päivitetään.
    c. ( ) Symmetrisestä avaimesta sovitaan.
    d. ( ) Päivitetty julkinen avain rekisteröidään.
17. **Ethernet-kytkin on laite, joka**
    a. ( ) toimii kuljetuskerroksen tasolla.
    b. ( ) reitittää lähiverkon paketteja IP-aliverkkojen välillä.
    c. ( ) oppii välittämiensä kehysten perusteella sen, minkä portin takana mitkäkin MAC-osoitteet sijaitsevat.
    d. ( ) toistaa sisääntulevat kehykset aina kaikkiin ulosmeneviin portteihin.
18. **Mikä on aliverkon 130.230.4.64/26 viimeinen osoite eli broadcast-osoite?**
    a. ( ) 130.230.4.95
    b. ( ) 130.230.4.255
    c. ( ) 130.230.4.127
    d. ( ) 130.230.7.255
19. **Mikä on todennäköisin syy, jos sisä- ja ulkoverkon väliin asennetun palomuurin läpi voi päästä hyökkäämään sisäverkon järjestelmiä vastaan?**
    a. ( ) Laitteiston tai ohjelmiston valmistuksessa on tapahtunut virhe.
    b. ( ) Sisäverkon politiikka on väärin konfiguroitu palomuuriin.
    c. ( ) Sisäverkon politiikka sallii hyökkäykset.
    d. ( ) Laitteiston tai ohjelmiston eheys on särkynyt.
20. **Minkä verkoista (i) LAN, (ii) MAN, (iii) WAN voi yksittäinen käyttäjä pystyttää ilman lupahakemuksia?**
    a. ( ) vain (i):n
    b. ( ) ei mitään
    c. ( ) vain (i):n ja (ii):n
    d. ( ) vain (i):n ja (iii):n
21. **Jos selaimesi tarjoaa sinulle mahdollisuuden tallentaa juuri syöttämäsi salasana vastaista käyttöä varten, minkä ehdon seuraavista olisi tärkeintä täyttyä, jotta sinun kannattaa tehdä talletus?**
    a. ( ) Salasanan takana ei ole mitään arvokasta.
    b. ( ) Selaimesi salasanat ovat suojattuja muilta.
    c. ( ) Salasana on niin entrooppinen, ettet pystyisi sitä muistamaan.
    d. ( ) Et tarvitse salasanaa miltään muulta koneelta.
22. **Tietosuojan keskeinen merkitys on**
    a. ( ) yksityisten ihmisten salaisten tietojen suojaamisessa.
    b. ( ) yritysten salaisten tietojen suojaamisessa.
    c. ( ) yksityisten ihmisten erilaisille tiedonkerääjille kertomien tietojen suojaamisessa.
    d. ( ) yritysten erilaisille tiedonkerääjille kertomien tietojen suojaamisessa
23. **RSA-allekirjoitus muodostetaan korottamalla viesti tiettyyn potenssiin ja laskemalla jakojäännös julkisen moduulin suhteen. Mikä seuraavista on mahdollinen eksponentti?**
    a. ( ) 3
    b. ( ) 1000-bittinen satunnaisluku
    c. ( ) 2
    d. ( ) 1/2 (eli lasketaan viestistä neliöjuuri)
24. **IPsecin voi asentaa myös reitittimien välille. Mitä seuraavista voi sen avulla tällaisessa yhteydessä toteuttaa: (i) haittaohjelmasuodatin, (ii) roskapostisuodatin, (iii) VPN? Vain**
    a. ( ) (i)
    b. ( ) (ii) ja (iii)
    c. ( ) (i) ja (ii)
    d. ( ) (iii)
25. **Mikä seuraavista sopii huonoimmin bot-verkon käsitteeseen?**
    a. ( ) Bot-verkolla voidaan toteuttaa palvelunestohyökkäys.
    b. ( ) Bot-verkon koneet ovat yleensä saman organisaation omistuksessa.
    c. ( ) Bot-verkossa olevien koneiden käyttäjät eivät yleensä tiedä verkon olemassaolosta.
    d. ( ) Bot-verkon koneissa on etäkäytettävä ohjelma.
26. **Kuljetuskerroksen protokollan ohjaustietokenttään (header) lähetyspäässä sijoitettava tieto, kuten esimerkiksi porttinumero, on tarkoitettu**
    a. ( ) verkkokerroksen käyttöön vastaanottavassa päässä.
    b. ( ) verkkokerroksen käyttöön lähettävässä päässä.
    c. ( ) sovelluskerroksen käyttöön vastaanottavassa päässä.
    d. ( ) kuljetuskerroksen käyttöön vastaanottavassa päässä.
27. **Mikä seuraavista on yleisesti ottaen vaarallisinta salasanojen yhteydessä? Käyttäjä**
    a. ( ) kirjoittaa salasanan paperille.
    b. ( ) valitsee salasanan, jossa on vähän entropiaa.
    c. ( ) ei vaihda salasanaansa koskaan.
    d. ( ) käyttää samaa salasanaa useassa paikassa.

28. **Kehen pääasiassa luotat, jos ulkomaalaisen esittämän passin perusteella päättelet, mikä hänen nimensä on? Passin**
    a. ( ) valmistajaan
    b. ( ) tarkastaneisiin rajaviranomaisiin
    c. ( ) esittäjään
    d. ( ) myöntäneeseen viranomaiseen
29. **Mikä seuraavista on mahdollinen merkintä niin sanotun C-luokan aliverkon 198.230.4.0 verkkomaskille? (i) /24, (ii) 11111111 11111111 11111111 00000000, (iii) 255.255.255.0.**
    a. ( ) vain (ii) ja (iii)
    b. ( ) (i), (ii) ja (iii)
    c. ( ) vain (i) ja (iii)
    d. ( ) vain (i)
30. **Yksi mahdollinen toiminta IPsecillä on, että se**
    a. ( ) kompressoi datapaketin.
    b. ( ) purkaa datasta ylemmän protokollakerroksen tekemän salauksen.
    c. ( ) lähettää paketin mukana purkuavaimen digitaalisessa kirjekuoressa.
    d. ( ) salaa myös alkuperäisen vastaanottajan IP-osoitteen.
31. **Mikä seuraavista ei päde yksityiseen käyttöön varatuille IP-osoitteille (ns. harmaille osoitteille)?**
    a. ( ) Jotta yksityisen IP-osoitteen omaava päätelaite voisi kommunikoida julkisessa Internetissä olevan laitteen kanssa, tarvitaan väliin osoitemuunnos eli NAT.
    b. ( ) Osoitelohko 10.0.0.0/8 on varattu yksityisille osoitteille.
    c. ( ) Eri yksityisissä IP-aliverkoissa ei voi käyttää samaa IP-osoitetta ilman, että siitä on haittaa verkon toiminnalle.
    d. ( ) Julkisessa Internetissä oleva palvelin ei voi lähettää IP-pakettia yksityisen verkon päätelaitteelle siten, että kohdeosoitekentässä on yksityinen IP-osoite.
32. **Minkä seuraavista pitäisi lähinnä kyetä palomuurin tapaiseen pakettien suodatukseen?**
    a. ( ) modeemi
    b. ( ) kytkin
    c. ( ) reititin
    d. ( ) toistin
33. **Paketinnuuskijan ('packet sniffer') tarkoituksena on**
    a. ( ) poistaa verkkoliikenteestä asiaankuulumattomia paketteja.
    b. ( ) skannata verkon segmenttejä kaapelointivaurioiden varalta.
    c. ( ) kaapata (kopioida) verkkoliikennettä myöhempää analyysia varten.
    d. ( ) jäljittää verkkoyhteyksiä ulkoisiin kohteisiin.
34. **Oletetaan, että päätelaitteen A ja palvelimen B välinen tietoliikenneyhteys koostuu langattomasta lähiverkosta, joka on yhdistetty langalliseen Ethernet-pohjaiseen reititinverkkoon. Mitkä seuraavista laitteista aina 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. ( ) vain (iii)
    b. ( ) vain (ii)
    c. ( ) vain (i)
    d. ( ) ei mikään
35. **Mikä seuraavista ei kuulu IP-paketin ohjaustietokenttään (headeriin):**
    a. ( ) protokollanumero, joka identifioi ylemmän kerroksen protokollan.
    b. ( ) time-to-live (toiselta nimeltään hop count) -laskuri.
    c. ( ) paketin kokonaispituus.
    d. ( ) kuittausnumero, joka kuittaa ko. numerolla varustetun aiemman paketin vastaanotetuksi.
36. **Epäsymmetristen kryptosysteemien avaimiin liittyy keskeisesti termi CA. Sen merkitys on**
    a. ( ) Certificate Authority eli sertifikaattiauktoriteetti.
    b. ( ) Certified Authentication eli sertifioitu autentikointi.
    c. ( ) Certificate Authentication eli sertifikaatin autentikointi.
    d. ( ) Certificate of Authority eli auktoriteetin sertifikaatti.
37. **Reititysvirheen sattuessa IP-paketti voi jäädä kiertämään kehää verkossa (ns. reititysslmukka). Tilanteen pelastaa**
    a. ( ) time-to-live-laskuri, jonka meneminen nollaksi aiheuttaa paketin tuhoamisen.
    b. ( ) alemman kerroksen protokolla, joka huomaa tilanteen ja tuhoaa paketin.
    c. ( ) kuljetuskerroksen protokolla, joka raportoi asiasta lähettäjälle.
    d. ( ) ICMP-protokolla, joka huomaa silmukan ja palauttaa paketin lähettäjälle.
38. **Mikä seuraavista asioista liittyy mobiiliverkkoihin, mutta ei yrityksen tai organisaation WLAN-verkkoihin?**
    a. ( ) Verkon käyttäjät on pystyttävä tunnistamaan luotettavasti.
    b. ( ) Tiedonsiirron käytöstä on pystyttävä keräämään laskutustietoa.
    c. ( ) Yhteyksien täytyy toimia siirryttäessä yhden tukiaseman alueelta toisen tukiaseman peittoalueelle.
    d. ( ) Turvallisuussyistä liikenne päätelaitteen ja tukiaseman välillä on syytä salata.
39. **Pääsyverkolla tarkoitetaan sitä tietoliikenneverkon osaa, joka**
    a. ( ) yhdistää käyttäjän operaattorin runkoverkkoon.
    b. ( ) on käyttäjän kotona ja hänen omassa hallinnassaan.
    c. ( ) yhdistää yritysten hajallaan olevat toimipisteet toisiinsa.
    d. ( ) yhdistää operaattoreiden verkkoja toisiinsa.