jussi.puuruner@student.tut.fi

TTY / TIE / J. Harju

TIE-03100 Tietoverkot ja tietoturva

Tentti 10.12.2014

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. Miten yritys voi suojata verkkoaan ja tietoliikennettään hyökkääjiltä? Tarkastele erityisesti seuraavia kahta tilannetta:
   a) yrityksen palvelimia halutaan suojata palvelunestohyökkäyksiltä. Mitä asioita on otettava huomioon ja miten hyökkäykseen varaudutaan? Onko mahdollista saavuttaa täysin kattava suoja palvelunestohyökkäyksiä vastaan?
   b) yrityksellä on useita konttoreita ja niiden välinen tietoliikenne halutaan suojata ulkopuolisilta tahoilta. Millaisilla tekniikoilla liikennettä voidaan suojata ja miten hyvä suoja niiden avulla voidaan saavuttaa?

2. Haluat selata TTY:n työasemalla ulkomaista WWW-sivustoa. Mitä protokollia työasemasi käyttää saadakseen pyytämäsi sivun lautautumaan näytölle? Ota huomioon kaikki tarvittavat pinon protokollat ylhäältä alas asti. Kerro kunkin protokollan toiminnasta keskeiset seikat tiiviissä muodossa.

3. Tarkastellaan kahta eri tilannetta, jossa (taaskin) olet yhteydessä Internetiin, mutta olkoon kohteenasi tällä kertaa vaikka Facebook.
   a) Päätelaitteesi on SIM-kortiton tabletti, joka on langattoman tai langallisen lähiverkon avulla kiinni vanhempaan omakotitaloon tulevassa langallisessa Internet-liittymässä.
   b) Päätelaitteesi on tabletti, jossa on operaattorin SIM-kortti ja olet ulkona paikassa, jossa ei ole langattomia lähiverkkoja.
   Kerro kummassakin tapauksessa, millaisilla yleisnimillä kutsutaan niitä verkkoja, joiden kautta yhteytesi FB:hen kulkee, ja mitä keskeisiä piirteitä ja verkkoelementtejä näillä verkoilla on. Mitkä verkot ovat yhteisiä molemmille tapauksille?

MONIVALINTAOSUUS ALKAA TÄSTÄ: VASTAA ERILLISELLE LOMAKKEELLE!

4. **Mikä seuraavista on tyypillistä tarkistussummille, jotka on tarkoitettu torjumaan erilaisten numeroiden tai merkkijonojen syötössä tapahtuvia näppäilyvirheitä? Se**

   a) ( ) lasketaan yhteenlaskulla muista merkeistä.
   b) ( ) on aina numero, joka sijoitetaan merkkijonon tai numerosarjan loppuun.
   c) ( ) sijoitetaan hajautettuna useamman merkin alueelle.
   d) ( ) lasketaan kaikista muista merkeistä.

5. **Kun yksityisellä avaimella tehtyä allekirjoitusta todennetaan vastaavalla julkisella avaimella, matemaattinen kytkentä varmistaa lähinnä sen, että**

   a) ( ) allekirjoittajalla on ollut hallussaan julkista avainta vastaava yksityinen avain.
   b) ( ) allekirjoittajan henkilöllisyys on sama kuin se, joka on kytketty kyseiseen julkiseen avaimeen varmenteen avulla.
   c) ( ) allekirjoittaja omistaa tai on omistanut kyseisen julkisen avaimen.
   d) ( ) allekirjoittaja, kuka hän onkin, on tulkinnut oikein bittijonon, jonka hän on syöttänyt allekirjoitusalgoritmille.

6. **Symmetrisen salauksen moodi CBC tulee sanoista**

   a) ( ) Crypto Block Cipher
   b) ( ) Code Book Cipher
   c) ( ) Cook Book of Codes
   d) ( ) Cipher Block Chaining

7. **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) ( ) Laitteiston tai ohjelmiston eheys on särkynyt.
   c) ( ) Sisäverkon politiikka sallii hyökkäykset.
   d) ( ) Sisäverkon politiikka on väärin konfiguroitu palomuuriin.

8. **DoS-tyyppisen hyökkäyksen ensisijainen tavoite on**

   a) ( ) varastaa tietoa.
   b) ( ) rikkoa tietokone.
   c) ( ) vakoilla käyttäjää.
   d) ( ) häiritä palvelun toimintaa.

9. **Mitä seuraavista lähinnä tarkoittaa julkisen avaimen kryptosysteemin salaluukku?**

a) ( ) algoritmia diskreetin logaritmin laskemiseksi modulo n, kun n on kahden suuren alkuluvun tulo
b) ( ) keinoa suorittaa julkisen avaimen salausoperaatioita ilman että tuntee avaimia
c) ( ) julkisen avaimen salauksen purkuavainta tai allekirjoituksen laadinta-avainta
d) ( ) jotain julkisessa avaimessa olevaa salaista rakennetta, kuten kahta suurta alkutekijää

10. **Materiaalissa sanotaan: "Avaintenvaihto on yksi tärkeimmistä kryptografisista protokollista." Mitä avaintenvaihto, eli 'key exchange' tässä tarkoittaa?**

a) ( ) Vanha symmetrinen avain päivitetään.
b) ( ) Julkinen avain peruutetaan ja uusi varmennetaan.
c) ( ) Symmetrisestä avaimesta sovitaan.
d) ( ) Päivitetty julkinen avain rekisteröidään.

11. **Ethernet-kytkin on laite, joka**

a) ( ) toistaa sisääntulevat kehykset aina kaikkiin ulosmeneviin portteihin.
b) ( ) oppii välittämiensä kehysten perusteella sen, minkä portin takana mitkäkin MAC-osoitteet sijaitsevat.
c) ( ) toimii kuljetuskerroksen tasolla.
d) ( ) reitittää lähiverkon paketteja IP-aliverkkojen välillä.

12. **Mikä on aliverkon 130.230.4.0/22 viimeinen osoite eli broadcast-osoite?**

a) ( ) 130.230.4.255
b) ( ) 130.230.4.127
c) ( ) 130.230.7.255
d) ( ) 130.230.4.95

13. **Internetissä yhteydetönkin (ja siten epäluotettava) kuljetusprotokolla on hyödyllinen, koska**

a) ( ) verkkokerroksen protokolla IP on yhteydellinen.
b) ( ) reaaliaikavaatimukset (eli vaatimukset pienestä viiveestä ja viiveenvaihtelusta) usein edellyttävät yhteydetöntä kuljetusprotokollaa.
c) ( ) bittivirheet ja pakettien katoamiset tapahtuvat fyysisellä kerroksella ja ne korjataan siirtokerroksella.
d) ( ) sovelluksille on se ja sama onko kuljetuskerroksella käytössä yhteydellinen vai yhteydetön kuljetusprotokolla.

14. **TCP/IP-pinon kerrokset ylhäältä alaspäin ovat**

a) ( ) sovellus-, istunto-, kuljetus-, verkko- ja fyysinen kerros.
b) ( ) sovellus-, kuljetus-, verkko-, siirto- ja fyysinen kerros.
c) ( ) sovellus-, esitystapa-, verkko-, siirto- ja fyysinen kerros.
d) ( ) sovellus-, siirto-, kuljetus-, verkko- ja fyysinen kerros.

15. **Sähköpostijärjestelmän SMTP-protokolla tarkistaa aina, että**

a) ( ) lähettäjä (kenttä "Mail from:") on juuri se, joka väittääkin olevansa.
b) ( ) viestin sisältöosuus ei sisällä viruksia.
c) ( ) vastaanottajan sähköpostipalvelin on olemassa ja kiinni verkossa.
d) ( ) viestin otsikkotiedoissa mainittu lähettäjä (kenttä "From:") on sama kuin SMTP-protokollan "Mail from:"-kentän lähettäjä.

16. **Jos samaan dataan sovelletaan sekä SSL:ää että IPseciä (joko AH:ta tai ESP:tä), niin siinä vaiheessa kun dataa operoi IPsec, datassa**

a) ( ) on SSL:n muokkaamia kenttiä, joille IPsec tekee omat operaationsa riippumatta kenttien sisällöstä.
b) ( ) ei ole SSL:stä jälkeäkään.
c) ( ) on SSL:n muokkaamia kenttiä, joille IPsec ei tee mitään.
d) ( ) on SSL:n muokkaamia kenttiä, joille IPsec tekee omat operaationsa, joissa se tarvitsee SSL:n avaimia.

17. **Traceroute-komennon generoimille peräkkäisille ICMP Echo-paketeille on tyypillistä, että niiden**

a) ( ) sisältämän datan määrä pienenee.
b) ( ) TTL-kentän arvo IP-headerissa pienenee.
c) ( ) TTL-kentän arvo IP-headerissa kasvaa.
d) ( ) sisältämän datan määrä kasvaa.

18. **Mikä seuraavista verkkotopologioista soveltuu langallisena versiona huonosti lähiverkkoon:**

a) ( ) väylä.
b) ( ) tähti.
c) ( ) mesh.
d) ( ) rengas.

19. **Mikä seuraavista ei kuulu käsitteen kryptoalgoritmi piiriin?**

a) ( ) avaimellinen tiivistefunktio
b) ( ) hash-funktio
c) ( ) haaste-vaste -menetelmä
d) ( ) satunnaislukugeneraattori

20. **Autonomisen järjestelmän (AS) sisäisessä reitityksessä**

a) ( ) pyritään optimoimaan reititystä ja käytetään mm. OSPF-protokollaa.
b) ( ) reititysprotokollana käytetään BGP:tä.
c) ( ) riittää käyttää staattista reititystä.
d) ( ) riittää se, että käytetään MAC-osoitteita ja ARP-protokollaa.

21. **Tietosuojan keskeinen merkitys on**

a) ( ) yksityisten ihmisten erilaisille tiedonkerääjille kertomien tietojen suojaamisessa.
b) ( ) yritysten salaisten tietojen suojaamisessa.
c) ( ) yksityisten ihmisten salaisten tietojen suojaamisessa.
d) ( ) yritysten erilaisille tiedonkerääjille kertomien tietojen suojaamisessa.

22. **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) ( ) ei mikään
b) ( ) vain (i)
c) ( ) vain (iii)
d) ( ) vain (ii)

23. **Valitse laajin paikkansa pitävä vastausvaihtoehto: Tracerouten avulla laite voi yrittää selvittää,**

a) ( ) minkä reitittimien kautta reitti kohteeseen kulkee.
b) ( ) onko kohde liitetty verkkoon
c) ( ) mikä on RTT kohteeseen.
d) ( ). kaikki edellä mainitut asiat.

24. **Mikä seuraavista ei päde avaimellisille kryptografisille tiivisteille?**

a) ( ) Niitä voi käyttää viestin autentikointiin.
b) ( ) Niistä käytetään myös nimitystä Cyclic Redundancy Check (syklinen toisteisuustarkiste).
c) ( ) Niiden pituuden pitää olla reilusti enemmän kuin 24 bittiä.
d) ( ) Niiden laskennassa voidaan käyttää apuna avaimettomia tiivistefunktioita, kuten SHA-1.

25. **Miten salausalgoritmien informaatioteoreettinen tavoite *konfuusio* ilmenee käytännössä?**

a) ( ) Se tiivistää salatekstin lyhyemmäksi bittijonoksi kuin alkuperäinen selväteksti oli.
b) ( ) Se hämärtää selvä- ja salatekstin välistä yhteyttä lisäämällä salatekstiin ylimääräisiä ns. "suolabittejä".
c) ( ) Se hajottaa selvätekstin jakaumia koko kryptotekstiin permutaatioiden avulla.
d) ( ) Se hämäännyttää selvä- ja salatekstin välistä yhteyttä suorittamalla korvauksia.

26. **Jossain lukujärjestelmässä luvun kertominen itsellään on sillä tavoin yksisuuntainen operaatio, että sitä voidaan käyttää lukuun koodatun tiedon salaamiseen. Mitä ominaisuuksia tässä järjestelmässä on sen lisäksi, että luvut ovat hyvin suuria eli monibittisiä?**

a) ( ) Kertolaskuna on vektoritulo hyvin moniulotteisessa lineaariavaruudessa.
b) ( ) Laskenta tapahtuu ottamalla jakojäännös jonkin kiinteän jakajan eli moduulin suhteen.
c) ( ) Luvut muodostuvat tavallisten kompleksilukujen pareista.
d) ( ) Luvut ovat rationaalilukuja eli kokonaislukujen osamääriä.

27. **Mikä seuraavista on yleisesti ottaen vaarallisinta salasanojen yhteydessä? Käyttäjä**

a) ( ) kirjoittaa salasanan paperille.
b) ( ) ei vaihda salasanaansa koskaan.
c) ( ) käyttää samaa salasanaa useassa paikassa.
d) ( ) valitsee salasanan, jossa on vähän entropiaa.

28. **Yksi mahdollinen toiminta IPsecillä on, että se lisää datapakettiin kentän, jossa on**

a) ( ) pakettia varten generoitu julkinen avain ja sen varmenne.
b) ( ) paketista ja symmetrisestä avaimesta laskettu tiiviste
c) ( ) paketista lähettäjän avaimella laskettu allekirjoitus.
d) ( ) paketin otsikkokentistä laskettu varmenne.

29. **Tutki väitettä: "Palvelimen lähettämän varmenteen voi asentaa selaimeen siten, että SSL/TLS voi käyttää sitä jatkossa saman palvelimen yksityisen avaimen todentamiseen." Väite on**

a) ( ) epätosi, sillä SSL/TLS ei todenna palvelimen yksityistä avainta vaan yksityisellä avaimella tehdyn allekirjoituksen.
b) ( ) epätosi, sillä selaimeen ei voi asentaa varmenteita vaan julkisia avaimia.
c) ( ) tosi, eikä selainta tarvitse käynnistää uudelleen.
d) ( ) tosi, mutta selain täytyy ensi sammuttaa ja käynnistää uudelleen.

30. **IP-aliverkon oletusreititin**

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

31. **Yksi tietosuojan perusteita on henkilörekistereiden laatimista ja käyttöä koskeva lainsäädäntö. Sitä koskevan lain nimenä on nykyään**

a) ( ) Tietosuojalaki.
b) ( ) Henkilörekisterilaki.
c) ( ) Henkilötietolaki.
d) ( ) Laki yksityisyyden suojasta työelämässä.

32. **Pääsyverkolla tarkoitetaan sitä tietoliikenneverkon osaa, joka**

a) ( ) yhdistää yritysten hajallaan olevat toimipisteet toisiinsa.
b) ( ) yhdistää operaattoreiden verkkoja toisiinsa.
c) ( ) yhdistää käyttäjän operaattorin runkoverkkoon.
d) ( ) on käyttäjän kotona ja hänen omassa hallinnassaan.

33. **Mikä seuraavista on lähinnä sellainen tehtävä, jonka hoitamiseen voidaan käyttää kryptografista protokollaa?**

a) ( ) sähköpostiviestin muuttaminen salatekstiksi
b) ( ) salausavaimesta sopiminen
c) ( ) salausavaimen turvallinen säilytys
d) ( ) salausavaimen generointi hyvien satunnaislukujen perusteella

34. **Mikä seuraavista mobiiliverkkoja ja niiden sukupolvia koskevista väitteistä ei pidä paikkaansa?**

a) ( ) Neljännen sukupolven mobiiliverkkotekniikasta käytetään nimeä LTE tai LTE Advanced.
b) ( ) Ensimmäisen sukupolven mobiiliverkot pohjautuivat analogiatekniikkaan.
c) ( ) Pakettikytkentäinen datansiirtopalvelu GPRS tuli mukaan 2. sukupolven mobiiliverkkoihin.
d) ( ) Kolmannen sukupolven 3G-verkko pystyy tarjoamaan yli 100 Mbit/s tiedonsiirtonopeuksia.

35. **Kuljetusprotokollan headerissa kohdeportin numero identifioi**

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

36. **Viestistä laskettu kryptografinen tiiviste edustaa koko viestiä sikäli, että**

a) ( ) pienet muutokset viestissä muuttavat tiivistettä vain vähän.
b) ( ) on erittäin epätodennäköistä löytää jotain muuta viestiä, jolla olisi sama tiiviste.
c) ( ) sitä ei voi saada mistään muusta viestistä.
d) ( ) missä tahansa kohdassa tapahtunut muutos voidaan korjata tiivisteen perusteella.

37. **ICMP-protokollan avulla laite voi lähettää ns. pingin eli Echo Request -viestin. Kun kohdelaite vastaanottaa pingin, niin se**

a) ( ) lähettää Echo Reply -viestin takaisin lähettäjälle.
b) ( ) lähettää välittömästi pingin kaikille saman IP-aliverkon laitteille.
c) ( ) jää odottamaan seuraavaa pingiä, mitaten siitä vasteajan.
d) ( ) lähettää Echo Reply -viestin lähimmän reitittimen IP-osoitteeseen.

38. **Mitä seuraavista ei voi toteuttaa TCP-protokollalla?**

a) ( ) ruuhkanhallinta
b) ( ) tietoturvallinen tiedonsiirto
c) ( ) vuonvalvonta
d) ( ) luotettava yhteyden lopetus

39. **Jos henkilökohtaisessa tietokoneessa on palomuuri, se on tyypillisesti**

a) ( ) verkkojohdossa sijaitseva lisälaite.
b) ( ) yksi prosessi muiden joukossa.
c) ( ) osa verkkokortilla olevaa hardwarea.
d) ( ) selainprosessin lisäosa.