TTY / TIE / Jukka Koskinen

TIE-30100 Tietoturvallisuuden perusteet
Tentti III 16.9.2014

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

Merkitse vastauksesi oheiselle lomakkeelle. Sille pitää kirjoittaa nimi ja opiskelijanumero, joka pitää merkitä myös rastimalla ao. numeromerkit. Tee luonnokset ja korjaukset mieluummin tälle paperille kuin lomakkeelle! Tentin jälkeen voit silloin myös helpommin verrata vastauksiasi kurssisivulta löytyvään oikeaan riviin sekä aikanaan tuloslistassa julkaistaviin vastauksiin, jotka on luettu lomakkeeltasi.

Kussakin tehtävässä 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. **Java-hiekkalaatikko ei voi estää koodilta**
   a. ( ) paikalliselta levyltä lukemista.
   b. (X) nollalla jakamisen yrittämistä.
   c. ( ) uuden prosessin käynnistämistä.
   d. ( ) uuden ohjelmakirjaston lataamista.

2. **Yleisenä turvasuunnittelun periaatteena *avoimen mallin periaate* tarkoittaa**
   a. ( ) tunnettujen ja hyviksi havaittujen turvamekanismien valintaa ja valinnan julkaisemista.
   b. ( ) avoimeen lähdekoodiin perustuvien turvaohjelmistojen suosimista.
   c. ( ) vastaavaa ilmiötä pääsynvalvonnassa kuin julkisen avaimen systeemit ovat kryptografiassa.
   d. ( ) turvallisuuden rakentamista jonkin muun kuin sen varaan, että turvamekanismi pysyy salaisena.

3. **Kaikilla seuraavista on jotain tekemistä redundanssin kanssa. Millä on vähiten tekemistä eheyden tai saatavuuden suojaamiseen käytettävän toisteisuuden kanssa?**
   a. (X) entropia
   b. ( ) datasta laskettu tiivistefunktio
   c. ( ) varmuuskopio
   d. ( ) metatieto eli tieto tiedosta

4. **Haaste-vaste -menetelmässä voidaan käyttää kryptografista tiivistealgoritmia siten, että**
   a. ( ) vain todentaja laskee sillä jotain.
   b. ( ) sekä todentaja että todennettava laskevat sillä saman operaation samaan suuntaan.
   c. ( ) sekä todentaja että todennettava laskevat sillä saman operaation eri suuntaan.
   d. ( ) vain todennettava laskee sillä jotain.

5. **Mitä tekee TPM, Trusted Platform Module?**
   a. ( ) Tarkistaa käynnistyksen yhteydessä BIOS:n ja käynnistyssektorin haittaohjelmien varalta.
   b. ( ) Tarkistaa käyttäjän autentikoitumisdatan.
   c. ( ) Tallentaa palomuurisääntöjen ja haittaohjelmatietokannan tarkistussummat.
   d. ( ) Tekee julkisen avaimen krypto-operaatioita, joissa tarvitaan sen sisältämää yksityistä avainta.

6. **Rikoslain mukaan tiettyjen rikosten yrityskin on rangaistavaa. Mitä seuraavista tämä koskee? (i) Salassapitorikos, (ii) Viestintäsalaisuuden loukkaus, (iii) Tietoliikenteen häirintä, (iv) Tietomurto, (v) Henkilörekisteririkos.**
   a. ( ) (i), (ii) ja (iii)
   b. ( ) (ii) ja (iv)
   c. (X) (i), (iii) ja (iv)
   d. ( ) (i) ja (v)

7. **Oletetaan, että tiivistetään tietoturvallisen *laitteiston* ominaisuudet kahdeksi vaatimukseksi. Jos toinen koskee sitä, että käyttäjä voi vakuuttua laitteiston aitoudesta, niin toinen vaatimus koskee sitä, että laitteisto**
   a. ( ) pystyy erottamaan, ovatko siihen kohdistuvat toimet sallittuja vai eivät.
   b. ( ) pystyy erottamaan, onko sitä etäältä ylläpitävä henkilö autenttinen.
   c. ( ) voi vakuuttaa käyttäjän siitä, ettei mikään erikseen kielletty toimenpide ole päässyt vaikuttamaan siihen.
   d. (X) voi vakuuttaa käyttäjän siitä, ettei mikään sallituista poikkeava toimenpide ole päässyt vaikuttamaan siihen.

8. **Jos www-sivuja julkaisevien osapuolten tietoturvahuolia jaotellaan neljään luokkaan ja sivujen saatavuus on yksi luokka, niin mitkä seuraavista kattavat muut kolme parhaiten?**
   a. ( ) sivujen eheys, asianmukaisen korvauksen saaminen, se että pystyy huolehtimaan vastuista.
   b. (X) sivujen luottamuksellisuus, tekijänoikeuksien puolustaminen, se että pystyy huolehtimaan vastuista.
   c. ( ) sivujen autenttisuus, tekijänoikeuksien puolustaminen, vastuiden kantaminen.
   d. ( ) sivujen eheys, asiakkaan autenttisuus, vastuista vapautuminen.

9. **Varmuuskopiointi on turhaa, jos**
   a. ( ) se tehdään vain kerran viikossa.
   b. ( ) kopiolta ei pysty löytämään palautettavaa tiedostoa.
   c. ( ) kopioita säilytetään samassa huoneessa kuin alkuperäisiä.
   d. (X) kopion toimivuutta ei tarkasteta.

10. **Oletetaan, että salasanan muodostamisen lähtökohtana käytetään tätä titupe-kurssia ja että hyökkääjäkin saattaa asiayhteydestä arvata tämän. Mikä seuraavista salasanoista olisi paras kompromissi muistettavuuden ja entropian välillä (jos niitä ei olisi tässä julkaistu)?**
   a. (X) t.tupe MeiKS 3p
   b. ( ) -t_i/T+u?p*e*
   c. ( ) 71t0p3
   d. ( ) RJeputit!

11. **Henkilötietolain mukaiset arkaluonteiset henkilötiedot jakaantuvat sellaisiin, jotka ovat henkilön omia ominaisuuksia ja sellaisiin, jotka ovat muiden häneen liittämiä, eräänlaisia lokitietoja. Mikä seuraavista kuuluu jälkimmäiseen luokkaan?**
   a. ( ) etninen alkuperä
   b. ( ) uskonnollinen vakaumus
   c. ( ) entisten osoitteiden luettelo
   d. ( ) saadut sosiaalihuollon etuudet

12. **Mitä seuraavista aiheista ei käsitellä Tekijänoikeuslaissa?**
   a. ( ) IPR eli Intellectual Property Rights
   b. (X) DRM eli Digital Rights Management
   c. ( ) Patentit ja tavaramerkit
   d. ( ) Tekijänoikeuden lähioikeudet

13. **Mihin kryptoanalyytikko käyttää tilastollista analyysia?**
   a. ( ) Tiettyyn kryptotekstiin liittyvien mahdollisten selvätekstien haarukointiin.
   b. ( ) Kryptotekstissä olevan redundanssin vähentämiseen.
   c. ( ) Tiettyä algoritmia varten valittujen avainten jakautumisen selvittämiseen.
   d. ( ) Eri kryptoalgoritmien ja -protokollien levinneisyyden tutkimiseen.

14. **Onko laajan turvallisuusselvityksen tarkoitus antaa tietoa työnhakijan (i) rikollisesta toiminnasta, (ii) terveystiedoista, (iii) taloudellisesta tilasta?**
   a. ( ) vain (i):stä ja (ii):sta
   b. ( ) vain (i):stä
   c. ( ) vain (i):stä ja (iii):sta
   d. (X) kaikista

15. **Mitä seuraavista tarvitsee vähiten ottaa huomioon sähköpostin tietoturvallisuutta tarkasteltaessa?**
    a. ( ) viestien sisällön oikeinkirjoitus
    b. ( ) osoitteiden oikeinkirjoitus
    c. ( ) viestien koko
    d. ( ) osoitelistojen koko

16. **Www-selauksessa muualle siirtyviä tietoja ovat yleensä**
    a. (X) yhteen tai useampaan evästeeseen tiivistetty tieto kaikista aiemmista tiedoista, jotka palvelimelle on lähetetty selaimesta.
    b. ( ) selain- ja palvelinkoneen tai niiden proxyjen IP-osoitteet.
    c. ( ) muutama aiempi linkkiä seuraamalla saavutettu sivu omalla koneella olevasta selaimen sivuhistoriasta.
    d. ( ) evästeitä, jotka on saatu sellaisilta muilta palvelimilta, joilta nyt käytetty palvelin kokoaa sivun sisältöä.

17. **Tarkastellaan tietojenkäsittelyrauhan rikkomuksia, joita tietojenkäsittelylaitteeseen fyysisesti käsiksi pääsevä voi aiheuttaa. Mikä seuraavista ei ole *laitteistonäkökulmasta* tietoturvaongelma?**
    a. ( ) laitteen identiteetin muuttaminen
    b. (X) esiintyminen tietoverkossa laitteen käyttäjän nimissä
    c. ( ) laitteessa olevien resurssien käyttö
    d. ( ) laitteen siirtäminen toiseen paikkaan

18. **Jos ilmassa liikkuvat hiukkaset pitää jollain tavalla ottaa huomioon tietoturvauhkia kartoitettaessa, millä seuraavista on vähiten tekemistä asian kanssa?**
    a. ( ) Tietokonelaitteiden mekaanisten osien jumiutuminen
    b. ( ) Tahalliset tietoturvaloukkaukset
    c. ( ) Ylikuumeneminen
    d. (X) Yrityksen imago siistinä työpaikkana

19. **Kun toiminnan kannalta keskeiset tehtävät ja vastuut pilkotaan ja jaetaan eri henkilöille, saadaan aikaan se, että**
    a. ( ) yritys ei ole enää riippuvainen kenestäkään yhdestä henkilöstä.
    b. (X) tarvittavien varahenkilöiden kokonaismäärä pienenee.
    c. ( ) ulkopuolisen social engineering -hyökkääjän on vaikeampi saada riittäviä oikeuksia tavoitteitansa varten.
    d. ( ) henkilöstökoulutuksen tarve vähenee.

20. **Tietokantojen eheystavoitteessa on oleellisesti kolme tasoa, nimittäin**
    a. ( ) fyysinen, rakenteellinen ja tietoalkiokohtainen eheys.
    b. (X) muuttumattomuus, oikeellisuus ja ajantasaisuus.
    c. ( ) looginen, semanttinen ja syntaktinen eheys.
    d. ( ) laitteistotasoinen, pääsynvalvonnallinen ja looginen.

21. **Toimikortin valmistuksessa tapahtuu sulakkeen polttaminen**
    a. ( ) ja tarkoituksena on viimeistellä testaus tiettyjä fyysisiä hyökkäyksiä vastaan.
    b. ( ) heti sen jälkeen kun PIN- ja PUK-koodit on kirjoitettu kortille.
    c. ( ) ennen kuin kortille kirjoitetaan salaiset avaimet.
    d. ( ) viimeisenä vaiheena ennen kuin käyttövaihe alkaa.

22. **Yleisön hallussa olevien tietojen fyysisen kopioinnin ja väärentämisen tuottamia riskejä on tekstissä jaoteltu seuraaviin tilanteisiin: *tekijänoikeuksien puolustaminen -- eheys -- mukana autentikoitumista -- pelkkää oikeutusta.* Jos samat asiat jactaankin viiteen luokkaan, niin luonteva jako olisi:**
    a. ( ) tekijänoikeudet -- eheys -- kiistämättömyys -- saatavuus -- yksityisyys
    b. ( ) yleinen paikkansapitävyys -- autentikoitumisominaisuudet -- pääsyoikeudet -- vaihdantakelpoisuus -- jakelun oikeutus
    c. ( ) tekijänoikeudet -- eheys -- autenttisuus -- kiistämättömyys -- yksityisyys
    d. ( ) yleinen paikkansapitävyys -- autentikoitumisominaisuudet -- pääsyoikeudet -- luottamuksellisuus -- jakelun oikeutus

23. **Kun GSM-puhelinverkko autentikoi vierasrekisterin (VLR:n) alueella olevan soittajan, SIM-kortilla olevasta avaimesta Ki tiedetään:**
    a. ( ) autentikointihaasteeseen tullut vastaus lähetetään kotirekisteriin (HLR) tarkistettavaksi Ki:n avulla.
    b. ( ) VLR tarkistaa autentikointihaasteeseen tulleen vastauksen vertaamalla sitä ennalta Ki:n avulla laskettuun arvoon.
    c. ( ) sen kopio on VLR:n tiedossa, mutta avainta vaihdetaan seuraavaa puhelua varten.
    d. ( ) VLR käyttää sitä lähettämäänsä haasteeseen tulleen vastauksen tarkistamiseen.

24. **Miten sähköinen henkilökortti ja biometrinen passi vertautuvat (Suomessa)?**
    a. ( ) Kummassakin on sähköisessä muodossa olevia tietoja, joita toisessa ei ole.
    b. ( ) Ne otettiin käyttöön samoihin aikoihin 2010-luvun alussa.
    c. ( ) Molemmat kelpaavat maahantuloon oikeuttavana matkustusasiakirjana kaikkialla, missä ei edellytetä viisumia.
    d. ( ) Molemmat kelpaavat maahantuloon oikeuttavana matkustusasiakirjana kaikkialla, missä digitaalisia biometrisiä tietoja ei edellytetä.

25. **Tietoaineistoturvallisuuden kohteena oleva *tietoaineiston käsite* rajautuu yleisesti sen mukaan,**
    a. ( ) minkä turvaluokan käsittelysääntöjä pitää noudattaa.
    b. ( ) missä paikassa tiedot sijaitsevat.
    c. ( ) mitä asiakokonaisuutta tiedot koskevat
    d. ( ) minkälaisella tallennusvälineellä tiedot ovat.

26. **EDI, electronic data interchange, on organisaatioiden väliseen tiedonsiirtoon tarkoitettu**
    a. ( ) menettely, jolla paperiliikennettä voidaan korvata biteillä.
    b. ( ) protokolla, jota voi käyttää tiedonsiirron turvaamiseen myös asiakkaiden suuntaan.
    c. ( ) perinteinen menettely, jonka on sittemmin korvannut HTTP yhdessä TLS:n ja IPsecin kanssa.
    d. ( ) protokolla, joka kattaa sekä verkko- että kuljetuskerroksen.

27. **Mikä laki lähinnä vaikuttaa teknisin menetelmin toteutettuun valvontaan työpaikoilla?**
    a. ( ) Laki valvonnan ja tietoverkon käytön järjestämisestä työelämässä
    b. ( ) Henkilötietolaki
    c. (X) Laki yksityisyyden suojasta työelämässä
    d. ( ) Sähköisen viestinnän tietosuojalaki

28. **Koska SSL/TLS toimii sovelluskerroksen alapuolella, se ei tiedä, millaista dataa sen avulla suojataan. Tästä huolimatta**
    a. ( ) viestinnän molempien päiden autentikointi kuuluu aina sen tuottamiin turvapalveluihin.
    b. ( ) ei sovellu VPN:n muodostamisessa tarvittavaan tunnelointiin.
    c. ( ) tarjoaa suojan asiakaskoneen käyttäjän identiteetille.
    d. ( ) se voi ottaa huomioon kaupankäynnin eri transaktioiden muodostaman kokonaisuuden, kunhan osapuolia on enintään kolme.

29. **Millaista lainsäädäntöä on valtion viranomaisten kanssa tapahtuvasta sähköisestä asioinnista? (Lyhennetään: L = Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista)**
    a. ( ) Siitä ei ole omaa lakia, mutta asiaa koskee L.
    b. ( ) Siitä on omakin lakinsa, mutta asiaa koskee myös L.
    c. ( ) Siitä ei ole omaa lakia eikä L vaikuta asiaan, vaan säännöksiä löytyy muista laieista.
    d. ( ) Siitä on oma lakinsa eikä L vaikuta asiaan.

30. **Oletetaan, että salasanatiedosto ei voi päästä asiattomien käsiin ja salasanat on tallennettu sinne salaamattomina. Mitä tällaisesta seuraisi?**
    a. ( ) Tavalliset käyttäjät eivät pystyisi vaihtamaan salasanaansa.
    b. (X) Kaikkien salasanat jouduttaisiin silti vaihtamaan ylikäyttäjän vaihtuessa.
    c. ( ) Salasanojen ei tarvitsisi olla yhtä pitkiä kuin yleensä.
    d. ( ) Salasanoja ei tarvitsisi salata siirron aikana.

31. **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. ( ) Kerrottavien lukujen pitää olla alkulukuja.
    b. ( ) Kertolaskuna on skalaaritulo hyvin moniulotteisessa lineaariavaruudessa.
    c. ( ) Luvut näyttävät positiivisilta kokonaisluvuilta, mutta tulon itseisarvo on pienempi kuin tulon tekijät.
    d. ( ) Luvut muodostuvat tavallisten kompleksilukujen pareista.

32. **Mikä seuraavista pätee matkapuhelinten 2G- ja 3G-järjestelmissä?**
    a. ( ) Puhelu salataan kahden 3G-puhelimen välillä päästä päähän, kun 2G:ssä salaus vaihtuu puhelinkeskuksessa.
    b. ( ) Puhelu salataan kahden 3G-puhelimen välillä päästä päähän, kun 2G:ssä salaus on vain laitteen ja tukiaseman välillä.
    c. ( ) Puhelu salataan 3G:ssä mutta ei 2G:ssä.
    d. ( ) Sekä 2G- että 3G- puheluissa on salaus, mutta kummassakaan se ei ulotu päästä päähän.

33. **Mistä vuodesta asti sähköinen henkilökortti on ollut Suomessa käytössä (aikaisintaan)?**
    a. ( ) 1995
    b. ( ) 1990
    c. ( ) 2005
    d. ( ) 2000

34. **Miten toimikortit suhtautuvat symmetrisen avaimen kryptografiaan? Niiden prosessorit**
    a. ( ) eivät ole yleensä tarpeeksi nopeita, jotta järkevää salauskäyttöä voisi ajatella.
    b. (X) kykenevät siihen, mutta tiedonsiirto on epäkäytännöllisen hidasta suurelle salattavalle datamäärälle.
    c. ( ) kykenevät siihen, mutta eivät kestä suurten datamäärien salausta kuumentumatta pilalle.
    d. ( ) eivät ole yleensä tarpeeksi monipuolisia siihen.

35. **Millainen eroavalla/erotetulla työntekijällä muistissaan oleva tietämys voi helpoimmin aiheuttaa kaikkia kolmea tyyppiä olevia tietoturvariskejä, joita työsuhteen päättymiseen yleisesti liittyy?**
    a. ( ) Konepajayrityksen asiakasrekisteri.
    b. ( ) Verkon turvatekniikkaa kehittävän yrityksen tutkimusverkon rakenne.
    c. ( ) Kemianteollisuuden yrityksen raaka-ainetoimittajien tiedot.
    d. (X) Pankkialan yrityksen konsernitason turvajärjestelyt.

36. **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. ( ) käytettävyys edellyttää myös sitä, että tiedot eivät ole hallitsemattomasti muuttuneet.
    b. (X) termiä käytettävyys ei pidä käyttää samassa merkityksessä kuin termiä saatavuus.
    c. ( ) saatavuus edellyttää, että tietoihin päästään käsiksi jonkin asetetun aikarajan puitteissa.
    d. ( ) tietoturvamielessä saatavuus koskee vain tietoja ja käytettävyys vain palveluja.

37. **Tietojärjestelmää koskevia turvavaatimuksia on kahta päätyyppiä -- yleensäkin, mutta erityisesti Common Criteria -standardin mukaan, nimittäin**
    a. ( ) tahallisiin ja tahattomiin tietoturvaloukkauksiin liittyviä.
    b. ( ) toiminnallisia ja vakuuttavuutta edistäviä.
    c. ( ) aktiivisia ja passiivisia.
    d. (X) painotuksena on joko eheys ja saatavuus tai luottamuksellisuus ja yksityisyys.

38. **Oletetaan, että julkisen avaimen infrastruktuurissa on yksi juurivarmentaja, sillä joukko alivarmentajia (2-taso) ja kullakin niistä joitakin alivarmentajia (3-taso), jotka ainoastaan myöntävät varmenteita yksilöille. Jos varmennehierarkia on tiukasti top-down -tyyppiä, niin**
    a. ( ) kukin varmentaja saa avaimelleen varmenteen välittömästä yläpuolellaan olevalta varmentajalta paitsi juurivarmentaja, joka antaa itse itselleen varmenteen.
    b. ( ) ylimmän tason varmentaja myöntää varmenteet 2-tason varmentajien avaimille ja varmentaa näiden varmentajien väliset ristiinvarmenteet. Vastaavasti 2-tason varmentajat tekevät saman omille alaisilleen eli 3-tason varmentajille.
    c. ( ) ristiinvarmenteita ei esiinny, vaan kukin varmentaja saa avaimelleen varmenteen omilta alivarmentajiltaan sekä välittömästi yläpuolellaan olevalta varmentajalta (juurivarmentaja tulkittuna omaksi "yläisekseen").
    d. ( ) ylimmän tason varmentaja myöntää varmenteet 2-tason varmentajille ja varmentaa näiden 3-tason varmentajille antamat varmenteet.

39. **Suojamekanismeja valittaessa on otettava huomioon tietoturvaprosessin eri vaiheita, joihin ne voivat soveltua. Mitkä kolme?**
    a. ( ) toipuminen, korjaaminen ja syyllisten rankaisu.
    b. ( ) välttäminen, pelottaminen ja estäminen.
    c. (X) ehkäisy, havaitseminen ja reagointi.
    d. ( ) politiikan muodostaminen, uhkien torjunta ja vahinkojen korjaaminen.

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

41. **Jos lohkosalausalgoritmissa tehtäisiin niin, että**
    a. ( ) syötteen bittejä sekä korvattaisiin toisilla että vaihdettaisiin niiden järjestystä, tuloksena olevasta salatekstistä ei voisi enää purkaa selkotekstiä takaisin.
    b. ( ) syötelohko olisi pitempi kuin tulos eli kryptolohko, salausta ei välttämättä voisi purkaa.
    c. ( ) selkotekstilohkoon ensin liitettäisiin tarkistussumma, salauksen murtaminen vaikeutuisi.
    d. ( ) selkoteksti ensin zip-tiivistettäisiin, salauksen murtaminen helpottuisi.

42. **Aiempaan arvioon verrattuna kokonaisriski pienenee, jos tiettyyn riskiin liittyvän**
    a. ( ) torjuntamekanismin olemassaolo jätetään laskuissa huomiotta.
    b. ( ) kohteen arvo merkitään laskuissa todellista suuremmaksi.
    c. ( ) kohteen arvo todetaan entistä pienemmäksi.
    d. ( ) uhkan todennäköisyys asetetaan laskuissa todellista pienemmäksi.

43. **Yksi mahdollinen toiminta IPsecillä on, että se**
    a. ( ) salaa myös alkuperäisen vastaanottajan IP-osoitteen.
    b. ( ) purkaa datasta ylemmän protokollakerroksen tekemän salauksen.
    c. ( ) lähettää paketin mukana purkuavaimen digitaalisessa kirjekuoressa.
    d. ( ) kompressoi datapaketin.

44. **"Käyttäjän syötteeseen luottaminen on turmioksi." Tämä on yleinen muistutus ja ohjelmoijan perussääntö numero 1. Mitkä kaksi muista säännöistä ovat tämän sovelluksia: (i) Suojaudu puskurin ylivuotoja vastaan. (ii) Estä sivuston komentosarjakäyttö. (iii) Älä edellytä järjestelmänvalvojan oikeuksia. (iv) Jätä salauskoodin tuottaminen ammattilaisille. (v) Vähennä hyökkäyskohteita.**
    a. ( ) (iv) & (v)
    b. ( ) (ii) & (iii)
    c. (X) (i) & (ii)
    d. ( ) (iii) & (iv)

45. **Mikä seuraavista ei kuulu symmetrisen kryptosysteemin avaimenhallintaan?**
    a. ( ) avaimen asettaminen sulkulistalle
    b. ( ) avaimen varmuuskopiointi/palauttaminen
    c. ( ) avaimen käyttötarkoituksen kontrolli
    d. ( ) avaimen pakkoluovutus (key escrow)

46. **Oletetaan, että joku on asentanut SSH:n omalle koneelleen ja on jo käyttänytkin sitä kohdekoneelle kirjautumiseen. Mikä seuraavista on kaikissa tapauksissa välttämätöntä, jotta seuraavakin kirjautuminen SSH:lla olisi mahdollinen? Hänellä tai hänen omalla koneellaan pitää olla tallessa**
    a. ( ) oma yksityinen tai julkinen avain.
    b. (X) oma yksityinen avain tai oma salasana kohdekoneeseen.
    c. ( ) oma tai kohdekoneen julkinen avain.
    d. ( ) oma tai kohdekoneen yksityinen avain.

47. **Mikä seuraavista sopii huonoimmin bot-verkon käsitteeseen?**
    a. (X) Bot-verkossa olevien koneiden käyttäjät ovat sopineet yhteistyöstä verkon ylläpitäjän kanssa.
    b. ( ) Bot-verkolla voidaan toteuttaa palvelunestohyökkäys.
    c. ( ) Bot-verkon koneet ovat harvoin saman organisaation omistuksessa.
    d. ( ) Bot-verkon koneissa on etäkäytettävä ohjelma.

48. **Epäsymmetristen kryptosysteemien avaimiin liittyvä termi PKI tulee sanoista**
    a. (X) Private Key Integrity
    b. ( ) Private Key-ring Initiative
    c. ( ) Public Key Infrastructure
    d. ( ) Public Key Initiative

49. **Feistelin periaatteessa yhden kierroksen sisällä lohkon puolikkaille tapahtuu seuraavaa:**
    a. ( ) salausavain ei vaikuta lainkaan toisen puoliskon seuraavalle kierrokselle tuottamaan tulokseen.
    b. ( ) molemmille tehdään jokin muunnos ennen sijoitusta seuraavan vaiheen lähtökohdaksi.
    c. ( ) kumpikin vaikuttaa molempiin seuraavan vaiheen puolikkaisiin.
    d. ( ) toinen puolikas kopioidaan eteenpäin sellaisenaan eikä se vaikuta toisen puoliskon tuottamaan tulokseen.

50. **Tietoturvamekanismeja laajasti mutta abstraktisti esittelevässä käsitekartassa mainitaan**
    a. (X) tunkeutumisen havainnointi.
    b. ( ) virustorjunta.
    c. ( ) roskapostin suodatus.
    d. ( ) varmuuskopiointi.

51. **Tietoturva.fi-sivuston haittaohjelmien esittelyssä ei käsitellä**
    a. ( ) root-kittejä
    b. ( ) takaportteja
    c. ( ) bot-verkkoja
    d. (X) loogisia pommeja

52. **Tietoturvallisuus on yksi kohta yleisessä turvallisuusjaottelussa, jonka monilla muillakin kohdilla on yhtymäkohtia tietoturvallisuuteen. Millä seuraavista yleisen turvallisuuden osa-alueista on *vähiten* tekemistä sen kanssa, mitä tietoturvallisuudessa tavoitellaan?**
    a. ( ) Kiinteistö- ja toimitilaturvallisuus
    b. (X) Ympäristönsuojelu
    c. ( ) Valmiussuunnittelu
    d. ( ) Rikosturvallisuus

53. **Mikä seuraavista väitteistä on tosi?**
    a. ( ) Jos joku keksii samasta tekstistä kaksi variaatiota, joilla on sama tiiviste, hän voi allekirjoittaa digitaalisesti yhden tekstin ja väittää myöhemmin että allekirjoittikin toisen.
    b. ( ) Viestistä laskettu yksisuuntainen tiivistefunktio edustaa koko viestiä sikäli, että ei ole olemassa mitään muuta viestiä, jolla olisi sama tiiviste.
    c. ( ) Yksisuuntaisen tiivistefunktion tuottama tulos ei voi olla pitempi kuin siihen syötetty teksti.
    d. ( ) Kryptografisen tiivistealgoritmin rakentamisessa käytetään kutistusfunktiona palautettavissa olevaa kompressiota.

54. **Mitä omistajan kannattaa ensisijaisesti tehdä löytääkseen oman tietojärjestelmänsä haavoittuvuuksia?**
    a. ( ) soveltaa automaattisia hyökkäystyökaluja.
    b. ( ) tarjota järjestelmän rinnakkainen versio hakkereiden tutkittavaksi.
    c. ( ) asentaa jokin root-kit.
    d. (X) käyttää tunkeutumisen havainnoinnin tekniikoita.

55. **Mitä merkitsee käytettävyyden kannalta, jos turvallisen järjestelmän suunnittelussa otetaan yhdeksi tavoitteeksi, että väärinkäyttö tehdään todella hankalaksi?**
    a. ( ) Järjestelmästä tulee todennäköisesti käyttökelvoton.
    b. ( ) Järjestelmän turvallisuus muodostuu osana käytettävyyttä.
    c. ( ) Järjestelmää ei voida tältä osin saada turvalliseksi.
    d. (X) Tavoitteella on hyvin vähän tekemistä käytettävyyden kannalta.

56. **Vertaillaan uhkia 1. tiedon väärinkäyttö, 2. tiedon luvaton käyttö ja 3. tiedon varastaminen.**
    a. ( ) Uhkat 1 ja 2 ovat erilaiset ja kumpikin edustaa uhkan 3 erikoistapausta.
    b. ( ) Mikään uhkista ei ole toisen erikoistapaus.
    c. ( ) Uhkien 1 ja 2 merkitys on lähes sama ja uhka 3 on erilainen.
    d. ( ) Uhkat 1 ja 2 ovat erilaiset ja tarkalleen toinen niistä edustaa mahdollista seurausta uhkan 3 toteutumisesta.

57. **Mikä standardi sisältää arviointiluokat D, C1, C2, B1, B2, B3 ja A1?**
    a. ( ) USA:n puolustusministeriön "Yellow book".
    b. ( ) Trusted Computer System Evaluation Criteria
    c. ( ) European Criteria for Information Technology Security
    d. (X) Common Criteria for Information Technology Security Evaluation

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

59. **Spam-viestinnän alajakoa voi tehdä sen mukaan, (i) meneekö viesti suoraan uhrille, (ii) meneekö uhri itse viestin luo, vai (iii) onko mukana hakukoneen kaltainen välittäjä. Missä seuraavista luetteloista on kaikkia kolmea tyyppiä olevia spam-viestinnän keinoja?**
    a. ( ) spamdexing, sblog, spit
    b. ( ) sosiaalinen media, sms-spam, pharming
    c. (X) smishing, vishing, pharming
    d. ( ) sblog, wiki, spim

60. **"Erot langattoman ja langallisen tietojenkäsittelyn tietoturvassa johtuvat tietoliikennekanavan erilaisista ominaisuuksista." Väite on**
    a. ( ) yleensä epätotta; jos kanava on autentikoitu ja salattu, muut erot ovat merkittävämpiä.
    b. ( ) yleensä totta; on muitakin eroja, jotka eivät ole lainkaan niin merkittäviä kuin kanavan aiheuttamat.
    c. ( ) epätotta lähes aina; muiden erojen rinnalla kanavan erilaisuus ei paljon merkitse.
    d. ( ) totta lähes aina, poikkeukset ovat vähäisiä.