TTY / TLT / J.Koskinen

TLT-3101 Tietoturvallisuuden perusteet
Tentti (III) 7. 9. 2009

Merkitse vastauksesi oheiselle lomakkeelle. Sille pitää kirjoittaa nimi ja opiskelijanumero, joka pitää merkitä myös rastimalla ao. numeromerkit. Tätä tehtäväpaperia ei tarvitse palauttaa. 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.

Tosi-epätosi -tehtävissä väittämät ovat joko tosia tai epätosia eli oikea vastaus on joko (a) tai (d). Jos rastit näistä laitimmaisista ruuduista väärän, menetät yhden pisteen. Jos rastit jommankumman vaihtoehdoista (b) ja (c), saat tai menetät puoli pistettä sen mukaan, mikä on oikea vastaus. Näiden keskivaihtoehtojen tarkoitus on mahdollistaa osittaisen tietämyksesi hyvittäminen. Ne eivät siis ole oikeita vastauksia eivätkä edusta mitään osatotuuksia.

Normaaleissa neljän vaihtoehdon tehtävissä (20-60) väärä vastaus vähentää pistetiliä 1/3 pisteellä.

---

1. **Lokijärjestelmän täytyy olla tyyppiä read-only, jotta voidaan olla varmoja siitä, ettei hyökkääjä pääse peittämään jälkiään.**
   o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
2. **Kun harrastat seittiselausta, et voi välttää sitä, että hakemasi URL ja koneesi IP-osoite lähtevät koneeltasi verkkoon ja näkyvät jossain muualla.**
   o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
3. **Kun korostetaan, että tietoturvallisuus on prosessi, ei tarkoiteta samanlaisuutta teollisuusprosessien kanssa (sellaisten kuin puunjalostus tai kemia).**
   o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
4. **Toimikortin valmistuksessa tapahtuu sulakkeen polttaminen ennen kuin kortille kirjoitetaan salaiset avaimet.**
   o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
5. **Javan hiekkalaatikko on ohjelmointimenetelmä, jolla Java-ohjelmista saadaan luotettavia myös tietoturvan kannalta.**
   o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
6. **Jos salausalgoritmissa tehtäisiin niin, että selkotekstin bittien järjestystä vain muutettaisiin, mutta se tehtäisiin satunnaisella, avaimesta riippumattomalla tavalla, tuloksena olevasta salatekstistä ei voisi enää purkaa selkotekstiä takaisin.**
   o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi

7. **Vain noin viidennes viruksista on peräisin levykkeiltä ja CD:iltä.**
   o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
8. **Jos tunkeutumisen havainnoinnin perustana käytetään tietoa siitä, miten käyttäjät normaalisti toimivat, saadaan yleensä enemmän vääriä hälytyksiä, kuin jos hyökkäyksiksi tulkitaan tunnusmerkkianalyysilla kaikki lokitiedoista löytyvät hahmot, jotka sopivat tunnettujen hyökkäysten rakenteeseen.**
   o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
9. **Tarkkaan ottaen samassa koneessa sijaitseva rinnakkainen kiintolevy ei riitä varmuuskopioinnin tarpeisiin.**
   o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
10. **PGP:ssä käytetään sekä symmetrisiä että epäsymmetrisiä kryptoalgoritmeja.**
    o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
11. **Jäännöstietoon liittyvien riskien arvioinnissa on tärkeää huomata, että huolimaton tekstin käsittelijä voi korvata nykyisen dokumentin jollain vanhemmalla versiolla.**
    o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
12. **Yksityisyys koskee vain pysyvämpiä henkilöön liittyviä tietoja kuin esimerkiksi sitä, missä hän kulloinkin sijaitsee.**
    o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
13. **Kun epäsymmetristä algoritmia sovelletaan hash-funktion tai symmetrisen salausavaimen kautta suureen määrään dataa, tarvitaan silti pidentävää täydennystä ('padding').**
    o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
14. **Sähköinen kaupankäynti tarkoittaa sitä, että rahaliikenne tapahtuu bitteinä.**
    o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
15. **Jos kohteiden pääsyluettelo edustaa riviä pääsynvalvonnan kokonaisesityksen taulukossa, niin toimijoiden kykyluettelo vastaa taulukon saraketta.**
    o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
16. **Myös ilman luotettua kolmatta osapuolta on mahdollista joissakin kryptografisissa protokollissa havaita, että tietoturvatavoite ei tullut saavutetuksi.**
    o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
17. **Verkosta ladattavan ohjelman alkuperästä ja eheydestä voidaan vakuuttua sellaisten allekirjoitusten perusteella, joita esimerkiksi Object Signing tai Authenticode tarjoavat, mutta nämä eivät takaa, että koodi olisi turvallista.**
    o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
18. **Tietoturvallisuus on laajasti ymmärrettynä niin monitahoinen kokonaisuus, että yleisen yritysturvallisuuden osa-alueet voidaan katsoa sen erityistapauksiksi.**
    o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
19. **Tietokantojen eheystavoitteessa on kaksi tasoa: tietokantaohjelmiston ja tietoalkioiden eheys.**
    o a. ( ) Tosi b. ( ) Luulen todeksi c. ( ) Luulen epätodeksi d. ( ) Epätosi
20. **Jos seittipalvelussa pitää salasanan unohtamisen varalle keksiä kysymys ja vastaus, mikä seuraavista on turvallisuuden kannalta tärkeintä?**
    1. ( ) kysymyksen entrooppisuus
    2. ( ) vastauksen muistettavuus
    3. ( ) kysymyksen ja vastauksen yhteensopivuus
    4. ( ) vastauksen entrooppisuus

21. **Mikä on välttämätöntä, jotta kahden suuren alkuluvun p ja q tuloa voi käyttää julkisen avaimen kryptografiassa julkisena avaimena?**
    1. ( ) Pitää tarkistaa onko kyseisiä alkulukuja vastaavaa yksityistä avainta olemassa.
    2. ( ) Pitää tarkistaa, ovatko myös p-1 ja q-1 alkulukuja.
    3. ( ) Kyseiset alkuluvut eivät saa olla muiden kuin omistajansa tiedossa.
    4. ( ) Täytyy julkaista myös p*p modulo q, tai q*q modulo p.
22. **Vaikka kukin seuraavista kohdista edustaakin tietoturvattomuutta, mikä niistä aiheuttaa yleisesti ottaen vähiten vahinkoa tiedoille? Käyttäjä**
    1. ( ) käyttää samaa salasanaa useassa paikassa, joista yhteen hyökkääjä murtautuu.
    2. ( ) unohtaa salasanansa ja hyökkääjä havaitsee tämän.
    3. ( ) kirjoittaa salasanat paperille, joka joutuu hyökkääjän haltuun.
    4. ( ) ei vaihda salasanaansa rittävän usein ja hyökkääjä ehtii murtaa sen.
23. **Sähköpostiviesteihin tai www-dokumentteihin liitettäviä metatietoja (oheistietoja, jotka sijaitsevat otsikkokentässä eivätkä näy normaalisti, mutta jotka saa näkyviin) voidaan käyttää**
    1. ( ) palomuureissa tunkeutumisen havainnointiin tai estämiseen.
    2. ( ) roskasähköpostin havaitsemiseen ja suodatukseen.
    3. ( ) ei-toivotun www-aineiston suodatukseen selaimessa.
    4. ( ) makrovirusten havaitsemiseen.
24. **Tarkastellaan tietojenkäsittelyrauhan rikkomuksia, joita tietojenkäsittelylaitteeseen fyysisesti käsiksi pääsevä voi aiheuttaa. Mikä seuraavista ei ole *laitteistonäkökulmasta* tietoturvaongelma?**
    1. ( ) laitteen siirtäminen toiseen paikkaan
    2. ( ) laitteen identiteetin muuttaminen
    3. ( ) laitteen fyysisten suojausten poistaminen
    4. ( ) esiintyminen tietoverkossa laitteen käyttäjän nimissä
25. **Tietoturvapolitiikka on johdon hyväksymä näkemys tietoturvallisuuden**
    1. ( ) merkityksestä, periaatteista ja toteutuksen yksityiskohdista.
    2. ( ) merkityksestä, vastuista ja toteutussuunnitelmasta.
    3. ( ) rakenteista, vastuista ja toteutuksesta.
    4. ( ) päämääristä, periaatteista ja toteutuksesta.
26. **Mitä seuraavista ei ole käytetty www-termin 'cookie' suomennoksena?**
    1. ( ) keksi
    2. ( ) kokki
    3. ( ) kuitti
    4. ( ) pipari
27. **Haittaohjelma voi käynnistyä oikean ohjelman sijasta tai silloin kun mitään ohjelmaa ei ollut tarkoitus käynnistää. Millä seuraavista on tämän kanssa vähiten tekemistä?**
    1. ( ) tiedostonimet
    2. ( ) samanaikaiset koneen muut käyttäjät
    3. ( ) dokumenttitiedoston avaaminen
    4. ( ) käyttöjärjestelmän monipuolisuus

28. **Voiko sähköpostiviestin loppuun lisätyllä lähettäjän nimellä olla oikeudellista merkitystä?**
    1. ( ) Kyllä, sopimusvapauden ja vapaan todistusharkinnan periaatteiden mukaan.
    2. ( ) Ei, sillä laki sähköisistä allekirjoituksista määrittelee vain varmenteeseen perustuvan allekirjoituksen.
    3. ( ) Ei, sillä sen voi helposti väärentää.
    4. ( ) Kyllä, sillä laki sähköisistä allekirjoituksista rinnastaa sen faxitse lähetettyyn käsinkirjoitettuun allekirjoitukseen.
29. **Kaikkia seuraavista voidaan tarvita särkyneen eheyden paikkaamisessa, mutta mikä on konkreettisinta?**
    1. ( ) proaktiivisuus
    2. ( ) politiikka
    3. ( ) reagointi
    4. ( ) redundanssi
30. **Henkilötietolaki antaa henkilörekisteriin merkitylle tiettyjä oikeuksia omia tietojaan koskien. Olettaen että rekisteri sinänsä on lainmukainen, mikä seuraavista ei kuulu näihin?**
    1. ( ) Oikeus korjata tietonsa.
    2. ( ) Oikeus tarkastaa tietonsa.
    3. ( ) Oikeus kieltää käsittely suoramainontaa varten.
    4. ( ) Oikeus poistaa osa tiedoista.
31. **Mikä piirre yleisessä tietoturvatavoitteessa "saatavuus" (eli käytettävyys eli availability) poikkeaa sekä luottamuksellisuudesta että eheydestä?**
    1. ( ) Tavoitteessa on mukana aikaraja, jonka puitteissa asioiden pitäisi tapahtua.
    2. ( ) Tavoite ottaa huomioon sekä vahingossa että tahallaan syntyneet ongelmat.
    3. ( ) Tavoitetta ei voi saavuttaa ilman, että molemmat muut on ensin saavutettu.
    4. ( ) Tavoite ei riipu siitä, kenen näkökulmasta asioita tarkastellaan.
32. **Jos pitää välillä käydä keventymässä, julkisella paikalla olevan (kiinteän) tietokoneen lukitseminen salasanalla suojatulla joutonäytöllä riittää varotoimenpiteeksi**
    1. ( ) saatavuutta varten.
    2. ( ) jatkuvuutta varten.
    3. ( ) luottamuksellisuutta varten.
    4. ( ) eheyttä varten.
33. **Mihin kryptoanalyytikko käyttää tilastollista analyysia?**
    1. ( ) Kryptotekstissä olevan redundanssin vähentämiseen.
    2. ( ) Eri kryptoalgoritmien ja -protokollien levinneisyyden tutkimiseen.
    3. ( ) Tiettyyn kryptotekstiin liittyvien mahdollisten selvätekstien haarukointiin.
    4. ( ) Tiettyä algoritmia varten valittujen avainten jakautumisen selvittämiseen.
34. **Yksi kolmesta yleisimmästä ohjelmistojen tietoturvaan liittyvästä virheestä on puutteellinen tiedonkulun hallinta (yhdeltä käsittelyrutiinilta toiselle; "incomplete mediation"). Tästä esimerkkinä on**
    1. ( ) vanhan tiedon käyttö, vaikka uusi tieto on jo talletettu toiseen muuttujaan.
    2. ( ) sellaisen aliohjelman kutsuminen, joka ei palauta mitään arvoa vaikka suorittaakin jonkin laskutoimituksen.
    3. ( ) taulukon alkion kirjoittaminen taulukon ulkopuolelle, vaikka taulukon rajat ovatkin tiedossa.
    4. ( ) syötteen tarkistuksen jättäminen tekemättä, vaikka siihen olisi

mahdollisuus.

35. **Viitemonitorin tehtävänä luotetussa tietojenkäsittelyssä on**
    1. ( ) asettaa käyttäjien oikeudet resursseihin pääsynvalvonnan tauluihin.
    2. ( ) hallinnoida epäsuorien muistiviittausten osoitetauluja.
    3. ( ) välittää kaikki vuorovaikutus käyttäjien ja resurssien välillä.
    4. ( ) tehdä lokimerkintä tietoturvapolitiikan vastaisesta tietoliikenteestä.
36. **Mikä seuraavista on muita tärkeämpää VPN:ssä, jonka pitää täyttää etäkäytön verkkoyhteyden tietoturvatarpeet?**
    1. ( ) autentikointi
    2. ( ) virtuaalisuus
    3. ( ) tunnelointi ja päätepisteiden kätkentä
    4. ( ) verkon toimivuus läpinäkyvästi
37. **Henkilöstöturvallisuus ei tavanomaisten määritelmien mukaan kata kaikkia organisaation kanssa tekemisissä olevia. Ketä seuraavista se ei kata?**
    1. ( ) Päivittäistavarakaupan asiakasta.
    2. ( ) Yrityksen alihankkijaa, joka vierailee yrityksessä.
    3. ( ) Etätyöntekijää, joka ei asioi yrityksen toimipisteissä.
    4. ( ) Yrityksen tiloissa korjausta tekevää putkimiestä.
38. **Yleisenä turvasuunnittelun periaatteena avoimen mallin periaate tarkoittaa**
    1. ( ) turvallisuuden rakentamista jonkin muun kuin sen varaan, että turvamekanismi pysyy salaisena.
    2. ( ) avoimeen lähdekoodiin perustuvien turvaohjelmistojen suosimista.
    3. ( ) vastaavaa ilmiötä pääsynvalvonnassa kuin julkisen avaimen systeemit ovat kryptografiassa.
    4. ( ) tunnettujen ja hyviksi havaittujen turvamekanismien valintaa ja valinnan julkaisemista.
39. **Jos käyttäjän oman koneen julkinen SSH-avain on usean kohdekoneen tiedossa, ja hänellä on niissä tunnus, kirjautuminen niihin kaikkiin SSH:lla edellyttää, että**
    1. ( ) jokaisen kohdekoneen julkinen avain on sama.
    2. ( ) jokaisen kohdekoneen julkinen avain on käyttäjän koneessa.
    3. ( ) käyttäjän salasana on sama jokaisessa kohdekoneessa.
    4. ( ) käyttäjän salasana on erilainen jokaisessa kohdekoneessa.
40. **Mikä seuraavista olisi kaikkein tiukin vaatimus, kun henkilöitä koskevasta tietokannasta saa hakea monenlaisia yhteenvetotietoja, mutta jokin kenttä on yksilön tasolla arkaluonteinen? Hakutuloksissa ei saa paljastaa edes**
    1. ( ) luetteloa niistä, joilla ylipäätään on merkintä kyseisessä kentässä.
    2. ( ) onko kyseisen tiedon arvo tietyllä henkilöllä jokin muu kuin hakuehdoissa annettu.
    3. ( ) onko tietokannassa kyseistä kenttää vai ei.
    4. ( ) karkeaa vaihteluväliä, jolla kyseinen kentän arvo sijaitsee tietyllä henkilöllä.
41. **Materiaalissa jaoteltiin sähköpostin turvakysymyksiä kahdeksaan osaan. Mihin niistä kuuluu tämä kysymyskokoelma: "Millaiset nimiöt, yhteystiedot, motot yms. tarvitaan ja kenelle? Huomaako/muistaako lähettäjä aina, mitä automatiikka liittää mukaan viestiin?" ?**
    1. ( ) Turvamekanismit
    2. ( ) Kirjeenvaihto
    3. ( ) Kuljetus, postilaatikko
    4. ( ) Osoitteet

42. **Rabin-allekirjoitus muodostetaan korottamalla viesti tiettyyn potenssiin ja laskemalla jakojäännös julkisen moduulin suhteen. Mikä seuraavista on mahdollinen eksponentti?**
    1. ( ) 1/2 (eli lasketaan viestistä neliöjuuri)
    2. ( ) 3
    3. ( ) 1000-bittinen satunnaisluku
    4. ( ) 2
43. **Jos tietoturvapolitiikka on järkevä ja sen mukaan jokin tieto pitää hävittää moninkertaisella päällekirjoituksella, niin mitä muuta pitäisi sen lisäksi tai sijasta tehdä?**
    1. ( ) kohdella samoin kaikkia ko. tiedon kopioita.
    2. ( ) poistaa tiedon omistajan käyttöoikeudet.
    3. ( ) tehdä kattavat tietokanta- ja www-haut, joilla selviää, onko tieto jo olemassa muualla, josta sitä ei voida hävittää. Tällöin päällekirjoituskin on turhaa.
    4. ( ) salata ko. tiedon varmuuskopiot avaimella, jota ei kirjoiteta levylle ja joka pyyhitään muistista käytön jälkeen.
44. **Epäsymmetristen kryptosysteemien avaimiin liittyvä termi PKI tulee sanoista**
    1. ( ) Private Key Integrity
    2. ( ) Private Key-ring Integrity
    3. ( ) Public Key Infrastructure
    4. ( ) Public Keys for Internet
45. **Mikä seuraavista ei päde tarkistussummille, jotka on tarkoitettu torjumaan numeroiden tai merkkijonojen syötössä tapahtuvia näppäilyvirheitä?**
    1. ( ) Se voidaan sijoittaa muualle kuin merkkijonon loppuun.
    2. ( ) Yhden tarkistusmerkin sijasta voidaan käyttää useampaa.
    3. ( ) Se lasketaan kaikista muista merkeistä, eikä operaationa yleensä ole pelkkä yhteenlasku.
    4. ( ) Alle 10-numeroisissa luvuissa voidaan päätellä, mikä numero on väärin, kun tarkistumerkkinä oleva numero ei täsmää.
46. **Mikä seuraavista ei kuulu tavanomaisiin tietolähteisiin, joita tunkeutumisen havaitsemisen järjestelmät käyttävät analyysinsa perustana?**
    1. ( ) aiemman normaalin toiminnan piirteet.
    2. ( ) lokimerkinnät palomuurista tai palvelimista.
    3. ( ) nykyisen järjestelmän verkkoliityntöjen asetukset.
    4. ( ) aiemmin toteutuneiden hyökkäysten kohdeosoitteet.
47. **Miten autentikointi alkaa suomalaisten verkkopankkien käyttäessä SSL:ää?**
    1. ( ) Pankkipalvelin autentikoi asiakkaan tämän antamien ja asiakasohjelman SSL:llä allekirjoittaminen tunnisteiden (esim. kertakäyttösalasana) avulla.
    2. ( ) Pankkipalvelin autentikoi asiakasohjelman tämän SSL-varmenteen avulla.
    3. ( ) Asiakas ja pankkipalvelin autentikoivat toisensa samassa SSL-kättelyssä toistensa varmenteiden perusteella.
    4. ( ) Asiakasohjelma autentikoi pankkipalvelimen tämän SSL-varmenteen avulla.
48. **Tietosuojavaltuutetun toimistossa on työntekijöitä**
    1. ( ) 35-70
    2. ( ) 10-30
    3. ( ) 75 tai enemmän
    4. ( ) 3-8

49. **IPsec salaa tietopaketteja protokollakerroksella, joka on**
    1. ( ) ylempi kuin SSL:ssä.
    2. ( ) joissain toiminnoissa sama, joissain alempi kuin SSL:ssä.
    3. ( ) sama kuin SSL:ssä.
    4. ( ) alempi kuin SSL:ssä.
50. **Mikä laki sanoo tähän tapaan: teknisenä välittäjänä toimiva palvelun tarjoaja ei joudu vastuuseen, kunhan hän viipymättä havaitsee ja poistaa aineiston, joka sisältää ... ?**
    1. ( ) Julkisuuslaki
    2. ( ) Ei mikään laki
    3. ( ) Laki tietoyhteiskunnan palvelujen tarjoamisesta
    4. ( ) Sähköisen viestinnän tietosuojalaki
51. **Minkä paljastuminen GSM-tekniikan hallitsevalle hyökkääjälle johtaisi helpoimmin siihen, että hän pystyisi soittamaan sinun laskuusi?**
    1. ( ) Puhelinnumerosi ja IMEI-koodisi (International Mobile Equipment Identity)
    2. ( ) GSM-verkon ja SIM-korttisi yhteisen salaisuuden
    3. ( ) Puhelusi salaukseen käytetyn avaimen
    4. ( ) SIM-korttisi
52. **Symmetrisen salauksen moodi ECB tulee sanoista**
    1. ( ) Encrypting Chain of Blocks
    2. ( ) Electronic Code Book
    3. ( ) Encrypting Code Block
    4. ( ) Electronic Cipher Block
53. **Toimikorttien kytkentänastoille pätee, että**
    1. ( ) tietoliikenteeseen käytetään eri nastaa kuin käyttöjännitteen syötölle.
    2. ( ) kortti pystyy julkisen avaimen kryptologiaan vain, jos kaikki nastat ovat käytössä.
    3. ( ) yksi niistä on tarkoitettu kortilla olevien kryptoavainten siirtoon, kun krypto-operaatio tehdään kortin ulkopuolella.
    4. ( ) oikosulkuun joutuessaan ne voivat vaurioittaa kortilla olevaa prosessoria.
54. **Virus ei voi tehdä mitään, jos sen koodia vain luetaan mutta ei ajeta. Miksi Wordin makrovirus sitten käynnistyy, vaikka sen sisältävä dokumentti vain luetaan levyltä Wordiin?**
    1. ( ) Virus on tarttunut myös Wordin ohjelmakoodiin.
    2. ( ) Saastunut dokumentti sisältää ohjelmakoodia, jonka lukeminen saa Wordissa aikaan puskurin ylivuodon, jolloin koodi kuitenkin päätyy ajettavaksi.
    3. ( ) Virus on muistinvarainen ja tarttuu avattaviin dokumentteihin.
    4. ( ) Saastunut dokumentti sisältää ohjelmakoodia, jonka Word ajaa luettuaan dokumentin.
55. **Mitä seuraavista pakettisuodatin voi tehdä: (i) virustorjuntaa, (ii) ylisuurten sähköpostiliitteiden poistoa, (iii) salausta tai purkua?**
    1. ( ) vain (ii) ja (iii)
    2. ( ) ei mitään näistä
    3. ( ) vain (iii)
    4. ( ) vain (i) ja (ii)

56. **Aiempaan arvioon verrattuna kokonaisriski pienenee, jos tiettyyn riskiin liittyvän**
    1. ( ) kohteen arvo todetaan entistä pienemmäksi.
    2. ( ) kohteen arvo merkitään laskuissa todellista suuremmaksi.
    3. ( ) torjuntamekanismin olemassaolo jätetään laskuissa huomiotta.
    4. ( ) uhkan todennäköisyys asetetaan laskuissa todellista pienemmäksi.
57. **Mikä seuraavista edustaa sellaista fyysistä tiedon tallennetta, jonka väärentäminen vaikuttaa toimijan oikeuksiin mutta ei autenttisuuteen?**
    1. ( ) huvipuiston ranneke
    2. ( ) musiikki-CD
    3. ( ) matkakortti, jolla on arvolippu
    4. ( ) kirjaston lainauskortti
58. **Paketinnuuskijan ('packet sniffer') tarkoituksena on**
    1. ( ) poistaa verkkoliikenteestä asiaankuulumattomia paketteja.
    2. ( ) kaapata (kopioida) verkkoliikennettä myöhempää analyysia varten.
    3. ( ) jäljittää verkkoyhteyksiä ulkoisiin kohteisiin.
    4. ( ) skannata verkon segmenttejä kaapelointivaurioiden varalta.
59. **Kerberoksessa käyttäjän salasana**
    1. ( ) purkaa lippupalvelulta tulleen salausavaimen asiakasohjelman käytettäväksi.
    2. ( ) toimii salausavaimena, kun asiakasohjelma lähettää lipun kohdepalveluille.
    3. ( ) pitää lähettää useiden kohdepalveluiden sijasta vain lippupalvelulle.
    4. ( ) lähetetään kohdepalveluille lippupalvelun salaamana.
60. **Oletetaan, että tieto on alunperin oikeaa ja säilynyt eheänä, kun olet sen luvallisesti hankkinut julkaistusta lähteestä. Mikä seuraavista on tällöin epätodennäköisin uhka, jonka sinä voisit aiheuttaa?**
    1. ( ) luvaton käyttö
    2. ( ) väärä tulkinta
    3. ( ) väärinkäyttö
    4. ( ) paljastuminen