

## TLT-3101 Tietoturvallisuuden perusteet

### Tentti (II) 8. 9. 2008

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 tulostlistassa 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 rasti näistä laittimmaisista ruuduista väärin, menetät yhden pisteen. Jos rasti jommankumman vaihtoehdoista (b) ja (c), saat tai menetät puoli pistettä sen mukaan, mikä on oikea vastaus. Näiden keskivaihtoehtojen tarkoitus on mahdollistaa osittaisen tietämyksen hyvitäminen. Ne eivät siis ole oikeita vastauksia eivätkä edusta mitään osatotuksia.

Normaaleissa neljän vaihtoehdon tehtävissä (24-60) väärä vastaus vähentää pistetiliä 1/3 pisteellä.

- Jos jätetään huomiotta tietoturvamekanismien kuten SSL:n tarvitsemat tiedot, käyttäjä voi estää selaintaan lähettämästä palvelimelle kaiken muun paitsi selain- ja palvelinkoneen IP-osoitteet.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Palomuurien tehtävä on oleellisesti muuta kuin autentikointia.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Haaste-vaste -menetelmässä voidaan käyttää kryptografista tiivistealgoritmia siten, että sekä todentaja että todennettava tulevat tehneeksi saman operaation samaan suuntaan.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- On mahdollista, että jollakulla ei ole oikeutta antaa eikä edes myydä sinulle lupaa itse kirjoittamansa tekstin käyttämiseen kotisivullasi.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Etäkäytön verkkoyhteyden tietoturvatarpeet toteuttaa VPN, kunhan siinä sekä autentikoidaan että salataan luotettavasti.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Jos lohkosalausalgoritmissa olisi syötteenä n bittiä selvätekstiä ja säännönmukaisena tuloksena n+1 bittiä kryptotekstiä, ei salausta välttämättä voisi purkaa.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi

- TTY:n (tai yhtä hyvin TaY:n) yleisen tason tietoturvaliikassa todetaan, että sen ja standardien perusteella laaditaan yliopiston tietoturvasuunnitelma.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Fyysisen peukaloinnin sietokyky ei ole tavanmukaista laitteilla, jotka sijaitsevat turvallisen fyysisen pääsynvalvonnan takana turvallisissa toimitiloissa.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Kahden suuren alkuluvun tulosta pitää ensin laskea jakojäännös kolmannen alkuluvun suhteen, jotta tuloksen voi julkaista ilman että alkuluvut paljastuvat.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Spam-suodatusta ei saa täydellisen osuvaksi avainsanalistojen avulla.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Esimerkki käytettävyyden suhteen tehdystä tiedon turvaluokituksesta on: "I tosiaikainen, II lähes tosiaikainen, III ajantasaisuus ei välttämätön."  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- PICS-järjestelmä ei ota kantaa sivujen varsinaiseen luokitukseen vaan tarjoaa vain kielen sitä varten.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Tietoturvallisuuden käsitteen sisältö tulee määritellyksi, kun esitetään, millä osa-alueilla käsite ilmenee, siis sellaisilla kuin toimitilat, henkilöstö, tietoaaineistot, ohjelmistot jne.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Jos sama viestintätarve halutaan toteuttaa yhtä turvallisesti langattomana kuin se on toteutettu langallisesti, tarvitaan enemmän tai vahvempia turvamekanismeja.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Javan hiekkalaatikko voi estää kirjoittamisen paikalliselle levyille.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- "Web bug" eli seittiötkökkä on seittisivun mukana latautuva näkymätön kuva, johon ei voi liittää evästeiden käyttöä.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Jäännöstietoon liittyvien riskien arvioinnissa on tärkeää huomata, että huolimaton tekstin käsittelijä voi korvata nykyisen dokumentin jollain vanhemmalla versiolla.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Turvallisten oletusarvojen periaate kieltää pääsyn, ellei lupaa erikseen ole myönnetty.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Kaikkiin tietokoneviruksiin on ennemmin tai myöhemmin pystytty kehittämään havaitsemismenetelmä -- siis sellainen, joka löytää ne muutenkin kuin niiden aiheuttaman vahingon kautta.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
- Jos ohjelma ei toteuta täsmällisesti määrityksiään, se ei ole myöskään tietoturvallinen.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi

21. Jos jossain tietoturvaloukkausten luokittelussa kaikkien hyökkäysten yhtenä vaiheena esiintyy tietoon kohdistuva prosessi, niin kyseinen luokittelu pystyy kattamaan vain tahalliset loukkaukset.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
22. Autentikointi on vakuuttumista olion ja tietynlaisten siihen liittyvien odotusten liittämisestä toisiinsa.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
23. Etäyhteyden turvaavia tunteita voidaan muodostaa sekä sovellustasolla verkkoyhteyksien sisään että verkkotasolla sovellustason viestien ympärille.  
a. ( ) Tosi b. ( ) Laulun todeksi c. ( ) Laulun epätodeksi d. ( ) Epätosi
24. Jos pelkän tietojenkäsittelylaitteen näkökulmasta jaotellaan kattavasti ikävyydet, joita siihen fyysisesti käsiksi pääsevä voi aiheuttaa, niin ne ovat särkeminen, varkaus,  
a. ( ) kopioiminen ja virransyötön katkaisu.  
b. ( ) luvaton hyödyntäminen ja muiden pääsyn estäminen.  
c. ( ) siirtäminen ja tietojen paljastaminen.  
d. ( ) muuntelu ja resurssien käyttö.
25. Mitä omistajan kannattaa ensisijaisesti tehdä löytääkseen oman tietojärjestelmänsä haavoittuvuuksia?  
a. ( ) käyttää tunkeutumisen havainnoinnin tekniikoita.  
b. ( ) asentaa jokin root-kit.  
c. ( ) soveltaa automaattisia hyökkäystyökaluja.  
d. ( ) tarjota järjestelmän rinnakkainen version hakkereiden tutkittavaksi.
26. Kurssiaineistossa kartoitettiin tietojenkäsittelyn tulosten uskottavuuden merkitystä. Millainen suhde uskottavuudella käyttäjän näkökulmasta on tietoturvaan?  
a. ( ) Jos tietoturvalle ei ole väliä, ei ole uskottavuudellakaan.  
b. ( ) Jos uskottavuudella ei ole väliä, ei ole tietoturvallakaan.  
c. ( ) Ei ole sellaista tietojenkäsittelyä, jonka uskottavuudella tai tietoturvalle ei olisi väliä.  
d. ( ) Mitään edellisistä väitteistä ei esitetty eikä olisi voitukaan, koska käsitteet eivät ole noin yksinkertaisia.
27. Mikä seuraavista ei ole luonteva sisältö pääsynvalvonnan matriisin solulle?  
a. ( ) tieto useasta pääsyalajista  
b. ( ) pääsyn kieltäminen  
c. ( ) tyhjä  
d. ( ) tieto toimijan ja kohteen ryhmyksestä
28. Toimikortille ladattava digitaalinen raha  
a. ( ) on kopioitavissa, mutta sitä ei kirjanpidon ansiosta silti voi käyttää kahdesti.  
b. ( ) on oleellisesti samanlaista kuin asiakkaan pankkitilillä oleva raha, ja esim. säilyy vaikka kortti tuhoutuisi.  
c. ( ) perustuu siihen, että kortti ei luovuta sitä muille kuin autenttisille maksupäätteille.  
d. ( ) ei ole tavanomaista rahaa siinä mielessä, että se olisi määritelty missään rahayksikössä: arvo määräytyy käyttöyhteydessä tariffin mukaan.

29. Henkilötietolaki antaa henkilörekisteriin merkitylle tiettyjä oikeuksia kieltää omien tietojensa käsittely. Olettaen että rekisteri sinänsä on lainmukainen, hän ei voi ko. lain perusteella kieltää käsittelyä  
a. ( ) suoramainontaa varten.  
b. ( ) viranomaistarkistusta varten.  
c. ( ) henkilömatrikkeliä varten.  
d. ( ) sukututkimusta varten.
30. Tietokantojen eheystavoitteessa on oleellisesti kolme tasoa, nimittäin  
a. ( ) looginen, semanttinen ja syntaktinen eheys.  
b. ( ) muuttumattomuus, oikeellisuus ja ajantasaisuus.  
c. ( ) fyysinen, rakenteellinen ja tietoalkiokohtainen eheys.  
d. ( ) laitteistotasoinen, pääsynvalvonnallinen ja looginen.
31. EDI, jota vastaava lyhenne suomeksi on OVT, tulee sanoista  
a. ( ) enterprise data interchange  
b. ( ) enterprise digital interface  
c. ( ) electronic data interchange  
d. ( ) electronic data interface
32. Oletetaan, että olet keksinyt seittipalveluun salasanan unohtamisen varalle turvakysymyksen ja sille vastauksen, joka sinun on helppo muistaa. Jos ne ovat "Ystävä Unkarissa?" ja "Dorotyya", niin mikä seuraavista olisi turvallisuuden kannalta heikoin modifikaatio niille?  
a. ( ) "Ystävä Unkarissa? Sulje teet." ja "Doro([tt])ya"  
b. ( ) "Ystävä Unkarissa? Siirrä hitu ja ajoita." ja "Epspuuzb57v"  
c. ( ) "Ystävä Unkarissa? o=0" ja "D0r0ttaa"  
d. ( ) "Ystävä Unkarissa? Kasvata vokaaleita." ja "D1r1tTYA"
33. Kansalaisvarmenteen myöntäjä VRK julkaisee varmennepolitiikan, jotta  
a. ( ) varmenteisiin luottavat osapuolet osaavat hoitaa todennuksen turvallisesti.  
b. ( ) muut osapuolet voivat päättää, kannattaako varmenteisiin luottaa.  
c. ( ) varmenteiden haltijat osaavat käyttää varmenteitaan turvallisesti.  
d. ( ) varmenteen todentamisessa käytetty VRK:n oma avain saisi kansainvälisen varmenteen.
34. Kaikilla seuraavista on jotain tekemistä redundanssin kanssa. Millä on vähiten tekemistä eheyden suojaamiseen käytettävän redundanssin kanssa?  
a. ( ) tiedoston kompressio  
b. ( ) varmuuskopio  
c. ( ) datasta laskettu tiivistefunktio  
d. ( ) metatieto eli tieto tiedosta
35. Rikoslain mukaan tiettyjen rikosten yritys on rangaistavaa. Mitä seuraavista tämä koskee? (i) Salassapitorikos, (ii) Viestintäsalaisuuden loukkaus, (iii) Tietoliikenteen häirintä, (iv) Tietomurto, (v) Henkilörekisteririkos.  
a. ( ) (i) ja (v)  
b. ( ) (i), (iii) ja (iv)  
c. ( ) (ii) ja (iv)  
d. ( ) (i), (ii) ja (iii)

36. Mikä seuraavista ei päde luettavana olleeseen tekstiin "Lukitse ovesi ja tietokoneesi, kun lähdet muualle"?
- Teksti käsittelee myös kirjautumismenetelmiä julkisen avaimen kryptografian keinoin.
  - Teksti muistuttaa siitä, ettei suojamekanismeja kannata ylimitoittaa suojattavan kohteen arvoon nähden.
  - Tekstissä annetaan useita käytännön ohjeita mm. ohjelmien sammuttamisesta ja näytönsäätäjistä.
  - Teksti soveltaa vanha totuutta, että lukot eivät ole varkaita vaan rehellisiä ihmisiä varten, ja suosittelee harkitsemaan salakirjoitusta tietojen suojaksi.
37. Mikä seuraavista toteuttaa huonoimmin varsinaisen varmuuskopioinnin tavoitteita?
- muistitikujen käyttö
  - ajoittainen inkrementaalikopiointi täyskopioiden sijasta
  - sellainen päivittäinen kopiointi, jota ei joka kerta tarkisteta
  - RAID-tekniikkaa käyttävä tiedostojärjestelmä
38. Eräässä suomalaisyritysten tietoturva tarkastelevassa tutkielmassa on tällainen toteamus: "Tietosuojalainsäädännön puutteiden vuoksi piratismi on riski Venäjällä, erityisesti Pietarin ja Moskovan alueilla toimiville yrityksille." Mikä seuraavista pohdintoista on eniten oikeassa?
- Mainitulla lainsäädännön puutteella ei ole mitään tekemistä mainitun riskin kanssa.
  - Piratismiin riski päinvastoin on melko pieni, kun siitä kerran on säädetty Venäjän laissa puutteellisesti.
  - Piratismi on suomalaisyritykselle riski vasta, kun se tuo Venäjältä hankkimiaan laittomia kopioita Suomeen.
  - Lainsäädännön puutteella tarkoitetaan Suomen lainsäädännössä olevaa puutetta.
39. Hot site -tyyppisessä varatilassa tavallisesti
- on laitteisto valmiina mutta ei paikalla olevaa henkilökuntaa.
  - on tuotantokäytössä olevan tietojärjestelmä ja sen rinnalla ovat käynnissä identtiset varalaitteet, joissa ajetaan kaikki samat toiminnot.
  - ajetaan samoilla varalaitteilla usean yrityksen tietojärjestelmien reaaliaikaisia kopioita.
  - on valmiina sekä laitteisto että paikalla oleva henkilökunta.
40. Yksi mahdollinen toiminta IPSecillä on, että se lisää datapakettiin kentän, jossa on
- paketista lähettäjän avaimella laskettu allekirjoitus.
  - paketin otsikkokentistä laskettu varmenne.
  - pakettia varten generoitu julkinen avain ja sen varmenne.
  - paketista ja symmetrisestä avaimesta laskettu tiivistä
41. Mikä on tiivistämisen rooli digitaalisessa allekirjoituksessa?
- Dokumentteille tehdään aina palautettava kompressio ennen allekirjoitusta.
  - Epäsymmetristä algoritmia ei sovelleta dokumenttiin vaan sen yksisuuntaiseen tiivistäseen.
  - Allekirjoituksesta lasketaan yksisuuntainen tiiviste.
  - Allekirjoituksen yhteydessä ei yleensä käytetä tiivistämistä.
42. Mihin seuraavista luokista kuuluu selkeimmin myös sellaista tietoa, jonka eheydestä sinun pitää huolehtia, mutta joka ei sinänsä ole lainkaan arvokasta sinulle itsellesi edes silloin kun sitä käytetään?
- lokitiedot
  - kryptoavaimet
  - jäännöstiedot
  - kopiot
43. Kertakirjautuminen
- on turvallisuutta lisäävä mekanismi, koska siinä käytetään vahvempaa autentikointia kuin salasanaa.
  - voi tuottaa pääsyn useaan resurssiin, mutta on voimassa vain jonkin rajoitetun aikamäärän tai istunnon ajan.
  - tuottaa pääsyn koko istunnon ajaksi yhteen tiettyyn resurssiin.
  - tuottaa pääsyn mihin tahansa yhteen resurssiin yhdeksi käyttökerraksi.
44. Mikä on pahin ongelma biometrisessä autentikoinnissa, jonka pitäisi toimia internetin kaltaisen turvattoman verkon yli?
- Joku voi saada haltuunsa palvelimella olevan vertailudatan.
  - Verkossa kulkevan datan eheys tai salaus voi särkyä matkalla.
  - Virheellisten hyväksymisten osuutta ei voi pienentää uusintojen avulla.
  - Ei tiedetä, onko autentikointidatan syöttäjä sama kuin se, jota data koskee.
45. Haittaohjelma voi käynnistyä oikean ohjelman sijasta tai silloin kun mitään ohjelmaa ei ollut tarkoitus käynnistää. Millä seuraavista on tämän kanssa vähiten tekemistä?
- samanaikaiset koneen muut käyttäjät
  - dokumenttitiedoston avaaminen
  - käyttöjärjestelmän monipuolisuus
  - tiedostonimet
46. Verkkoympäristössä tapahtuvaa viestintää koskevat uhkat tiivistetään viiteen keskeiseen tapaukseen, joista yksi on etäresurssin luvaton käyttö verkon yli. Muut neljä käsittelevät viestien "kohtaloa". Jos ne luokitellaan ongelmiksi luottamuksellisuuden, eheyden ja saatavuuden kannalta, niin mihin näistä luokista tulee kaksi?
- sekä eheyteen että luottamuksellisuuteen
  - saatavuuteen
  - sekä eheyteen että saatavuuteen
  - eheyteen
47. Mikä laki sanoo tähän tapaan: teknisenä välittäjänä toimiva palvelun tarjoaja ei joudu vastuuseen, kunhan hän viipymättä havaitsee ja poistaa aineiston, joka sisältää ... ?
- Ei mikään laki
  - Sähköisen viestinnän tietosuojalaki
  - Laki tietoyhteiskunnan palvelujen tarjoamisesta
  - Rikoslaki
48. Millä seuraavista on vähiten tekemistä perinteisten GSM-puhelujen kanssa?
- salausalgoritmit
  - pakettisuodatin
  - haaste-vaste -menetelmä
  - tietoturvaliikenne

49. Jos pöly ja lika pitää jollain tavalla ottaa huomioon tietoturvaohjeita kartoitettaessa, millä seuraavista on vähiten tekemistä asian kanssa?
- Ylikuumeneminen
  - Tietokonelaitteiden mekaanisten osien jumiutuminen
  - Liikenneanalyysi
  - Työntekijöiden altistumisesta aiheutuva sairauspoissaolot
50. Tiedon hävittäminen voi olla ongelmallista, kun ei tiedetä missä kaikkialla on kopioita tai muita jäänteitä. Vähiten tätä ongelmaa aiheuttaa todennäköisesti
- tietojen jakelu paperilla.
  - tietojen lähettäminen salattuna sähköpostina.
  - eheyden säilyttämiseen tähtäävä toisteisuus.
  - tietojen siirtäminen eri ohjelmistojen ja tiedostomuotojen välillä.
51. Toimikorttien kytkentänastoja
- ei normaalisti käytetä kaikkia ja ylimääräisistä aiheutuu riski hyökkääjän käsissä.
  - on liian vähän, jotta tietoturvallinen tiedonsiirto voisi toteutua.
  - on yleensä käytössä kaksi tai kolme.
  - on toteutettu useampia kuin tavallisesti käytetään.
52. SSH-autentikoinnissa voidaan tarvita sormenjälkien tarkistusta
- käyttäjän varmistaessa, mikä on kohdekoneen julkinen avain.
  - etäkoneen varmistaessa, että salauslauseella on tullut puretuksi oikea yksityinen avain.
  - käyttäjän varmistaessa, mikä on hänen käytössään olevan etäkoneen julkinen avain.
  - kohdekoneen varmistaessa, mikä on etäkoneen julkinen avain.
53. Oletetaan, että salasanan muodostamisen lähtökohtana käytetään tätä titupekurssia ja että hyökkääjäkin saattaa asiayhteydestä arvata tämän. Mikä seuraavista salausnoista olisi paras kompromissi muistettavuuden ja entropian välillä (jos niitä ei olisi tässä julkaistu)?
- t-t-p: 3 po/Nts
  - reputiPAS
  - 71t0p3
  - T(iT{ \_uu-peE£
54. Mikä piirre yleisessä tietoturvatavoitteessa "saatavuus" (eli käytettävyys eli availability) poikkeaa sekä luottamuksellisuudesta että eheydestä?
- Tavoitetta ei voi saavuttaa ilman, että molemmat muut on ensin saavutettu.
  - Tavoite ottaa huomioon sekä vahingossa että tahallaan syntyneet ongelmat.
  - Tavoitteessa on mukana aikaraja, jonka puitteissa asioiden pitäisi tapahtua.
  - Tavoite ei riipu siitä, kenen näkökulmasta asioita tarkastellaan.
55. Epäsymmetristen kryptosysteemien avaimiin liittyvä termi CA tulee sanoista
- Certificate of Authority
  - Certified Authentication
  - Certificate Authority
  - Certificate Authentication
56. Selaa ja pyrkii johonkin luottamusta edellyttävään seittiosoitteeseen ja selain saa seittipalvelimelta SSL-käytelyssä ennalta näkemättömän julkisen avaimen K, jonka pitäisi olla kyseisen palvelimen oma. Mitä sitten?
- Selain varoittaa asiasta ja käyttäjän pitäisi laskea kyseisen avaimen sormenjälki, tallettaa se ja käynnistää selain uudelleen.
  - Käyttäjä voi näennäisesti edetä haluamalleen seittisivulle vastattuaan "ok" selaimen kysymykseen, mutta palvelin on todennäköisesti jokin muu kuin hän luulee.
  - Selain etsii K:lle varmenteen varmennepalveluista ja jos sellainen löytyy, selain antaa käyttäjälle mahdollisuuden asentaa K selaimen.
  - Käyttäjä pääsee haluamalleen seittisivulle suoraan, jos selaimessa on luottamus avaimen, jolla K on varmennettu.
57. Tietosuojavaltuutetun toimistossa on työntekijöitä
- 10-29
  - 50 tai enemmän
  - alle 10
  - 30-49
58. Mikä standardi sisältää arviointiluokat D, C1, C2, B1, B2, B3 ja A1?
- European Criteria for Information Technology Security
  - Common Criteria for Information Technology Security Evaluation
  - Trusted Computer System Evaluation Criteria
  - USA:n puolustusministeriön "Yellow book".
59. TCB eli Trusted Computing Base sisältää
- myös luotetun käyttöhenkilöstön.
  - vain laitteita.
  - vain ohjelmistoa.
  - vain ohjelmistoa ja laitteita.
60. Lyhyellä tähtäimellä toteutettu social engineering on hyökkäyskeino, jossa yritetään saada aikaan tietovuoto tai muu tulos lähinnä
- tekeytymällä työyhteisöön tai sen lähelle kuuluvaksi ja käyttämällä hyväksi ihmisten auttamishalua.
  - työyhteisön ihmissuhteisiin aiheutetuilla ristiriidoilla, kateudella, kilpailutilanteilla tms.
  - soveltamalla yrityksen tietoturvaliittikkeen reverse engineering -tekniikkaa.
  - soluttautumalla työyhteisön jäseneksi.