

Riittävän pitke & merkittä...
ei redundanssia
ei luonnollista kieltä, EBC
Vaihtaa usein Dictionary attack
ei moneen paikkaan samaa

Vastaa viiteen tehtävään.

12

Kun olet saanut vastaukset valmiiksi, merkitse vastauspaperin alkuun tehtävien numerot siinä järjestyksessä kuin arvioit osanneesi niihin vastata, paras ensimmäiseksi, huonoin viimeiseksi. Jos arvostelu tuottaa saman järjestyksen, saat lisäpisteen.

Man@ger

3p * Esitä salasana-autentikoinnin käyttäjälle ohjeita hyvän salasanan valitsemiseksi ja hyväksi salasanojen käyttötavaksi. Perustele ohjeet (ts. kerro erityisesti mitä salasanojen haavoittuvuuksia niillä vältetään).

5p * (a, 3p) Miten tietokannan eheyttä voidaan edistää datasta laskettavien tarkistussummien avulla?
(b, 2p) Miksi tällaiseen tarkoitukseen sopivat tarkistussummat eivät riitä kryptografisen tiivistämisen tarpeisiin (eli esim. siihen että viestistä laskettu tiiviste allekirjoitetaan viestin sijasta)?
(c, 1p) Mitä hash-funktioissa tehdään asian "korjaamiseksi"?

3. Oletetaan, että saat A:lta salatun PGP-viestin, jonka hän on myös allekirjoittanut.
(a, 2p) Mistä PGP-ohjelmasi saa avaimet salauksen purkuun ja allekirjoituksen todennukseen?
(b, 1p) Kumpaa se tarvitsee ensin?
(c, 3p) Millä perusteilla sinä voit luottaa että juuri A on allekirjoittanut viestin?

5p * (a, 1p) Mitä ovat seittiselauksen evästeet (eli cookiet eli piparit)?
(b, 1p) Miksei niiden kautta voi tapahtua hyökkäystä koneesi eheyttä vastaan?
(c, 2p) Millä tavoin ne voivat aiheuttaa ongelmia yksityisyytesi kannalta?
(d, 2p) Millä tavoin seittiseläus yleisesti heikentää yksityisyyttäsi, evästeistä riippumatta?

5p * Mitä tarkoittaa tietokoneeseen tai tietokoneverkkoon tunkeutuminen ('intrusion') ja mitä keinoja sellaisen havaitsemiseksi on? (Pääpaino on havaitsemiskeinoissa; mainitse ainakin neljä erilaista.)

4p * Common Criteriassa (CC for Information Technology Security Evaluation) vakuuttavuuteen vaikuttavat tekijät jaotellaan seuraaviin luokkiin: konfiguraation hallinta -- järjestelmän toimitus ja toiminta -- kehitystyö -- ohjelmateriaali -- elinkaaren tuki -- testit -- haavoittuvuuden arviointi. Näistä ainoastaan viimeinen näyttäisi nimensä puolesta liittyvän turvallisuuteen. Miten muiden kuuden sisältämät komponentit sitten edistävät vakuuttumista eli antavat perusteita luottaa siihen että evaluoinnin kohteena oleva tuote tai järjestelmä täyttää sille asetetut tietoturvatavoitteet? (Selitä jokaisesta ainakin yksi asia.)

lastlog =

- viitemonitori
- logit | tietämys tapahtuma
- resurssien seuranta
- systeemi kutsujonot.

- ↑ konfiguraation hallinta
- Ympäristön oikein konf oikein ympäristöön
- Järjestelmän toimitus/toiminta
- Asennuksen onnistuminen/valvonta
- kehitystyö
- Bugin korjaaminen (mitkä osien haavoittuvuus arvioidaan osaksi)
- Ohjelmateriaali
- Miten allapäitä ottaa huomioon
- Miten käsitellään turvallisesti
- Elikaaren tuki
- parissa... ei...
- ...