

Tietoturvan perusteet: Oppimistavoitteet

30. maaliskuuta 2010

Pääalue	Esitiedot	Lähestyy oppimistavoitteita	Saavuttaa oppimistavoitteet	Syventää oppimistavoitteita
Yleiskuva tietoturvasta		<ul style="list-style-type: none"> • Osaa luetella, mistä osa-alueista yleinen ja tietoturvasuus koostuvat. • Tietää turvallisuuteen liittyvät tärkeimmät lait ja osaa kuvailla, minkälaisissa tilanteissa niitä sovelletaan. 	<ul style="list-style-type: none"> • Osaa luetella turvallisuuteen liittyvät tärkeimmät organisaatiot ja hallintostandardit. • Osaa selittää turvalliseen ohjelmistosuunnittelun pääperiaatteet. 	
Pääsynvalvonta	Unix-käyttöjärjestelmien perusteet.	<ul style="list-style-type: none"> • Osaa valita salasanat oikein ja tietää, minkälaisia salasanoja tulee välttää. • Osaa asettaa pääsyoikeudet Unix-tiedostoihin. • Tuntee eri haittaohjelmatyypit ja tietää niiden torjunnan perusteet. 	<ul style="list-style-type: none"> • Osaa selittää, miten salasana-tiedosto muodostetaan ja miten sateenkaaritauluja vastaan puolustaudutaan. • Tuntee Unix:in tiedostotyypit ja osaa käyttää niitä. • Osaa selittää Unix:in UID-tunnusten käytön ja tietää niihin liittyvistä ongelmista. • Tietää laajasti haittaohjelmien torjunnasta. 	<ul style="list-style-type: none"> • Osaa kuvailla Unix:in inoderakenteen. <p>Osaa käyttää erilaisia tiedostoviittauksia ja symbolisia linkkejä Unix:ssa.</p>

Pääalue	Esitiedot	Lähestyy oppimistavoitteita	Saavuttaa oppimistavoitteet	Syventää oppimistavoitteita
Ohjelmien turvallisuus	Java-ohjelmointitaito, kyky ymmärtää yksinkertaisia C-kielen rakenteita, SQL.	<ul style="list-style-type: none"> • Osaa luetella muutamia tyypillisiä ohjelmistovirheitä, jotka vaarantavat turvallisuuden. • Osaa antaa esimerkkejä ohjelmointikielten ominaisuuksista, jotka vaikuttavat tietoturvaan. • Osaa luetella muutamia turvallisessa ohjelmoinnissa huomioon otettavia seikkoja. 	<ul style="list-style-type: none"> • Osaa luetella tyypillisimmät turvallisuutta vaarantavat ohjelmistovirheet. • Osaa luetella turvallisessa ohjelmoinnissa huomioon otettavat seikat ja osaa antaa esimerkkejä turva-aukoista, joita voi syntyä, jos periaatteita ei ole noudatettu. • Osaa antaa esimerkkejä Javan ja C:n heikkouksista. • Tuntee Javan turvamekanismeja. 	<ul style="list-style-type: none"> • Osaa käyttää Javan turvamekanismeja. • Osaa käyttää C:n osoittimia turvallisesti.
Datan turvallisuus		<ul style="list-style-type: none"> • Osaa luokitella tietoja ja tietää valtionhallinnon tietojen luokitusperiaatteista. • Osaa käyttää oikein tiedostojen poisto- ja kopiointiopeeraatioita. 	<ul style="list-style-type: none"> • Osaa selittää eheystekniikkojen periaatteet, kun käytetään salausta, tiivistefunktioita ja MAC-funktioita. • Osaa selittää jono- ja lohkosalaaajien eron ja osaa valita sopivat avainpituudet eri tarkoituksiin. • Osaa valita sopivat salalohkojen ketjutustekniikat, joita sovelletaan käytännön tilanteissa. 	

Pääalue	Esitiedot	Lähestyy oppimistavoitteita	Saavuttaa oppimistavoitteet	Syventää oppimistavoitteita
Verkkojen tietoturva	Tietoliikenteen perusteet	<ul style="list-style-type: none"> • Osaa selittää tyypillisen hyökkäyksen etenemisen. • Osaa antaa muutamia esimerkkejä palvelunestohyökkäyksistä. • Osaa selittää palomuurin toiminnan. • Osaa selittää IPsec:in ja SSL:n roolin ja niiden käyttötapoja. 	<ul style="list-style-type: none"> • Tuntee erilaisia teoreettisia menetelmiä vaikeuttaa palvelunestohyökkäyksiä ja osaa valita niistä sopivimmat eri tilanteisiin. • Tuntee erilaisia palomuuriratkaisuja ja osaa selittää niiden käyttötarkoituksen ja tyypilliset käyttötilanteet. • Osaa selittää RSA:n toiminnan, digitaalisen allekirjoituksen RSA:n avulla ja X.509-varmennestandardin hyvät ja huonot puolet. 	<ul style="list-style-type: none"> • Osaa käsitellä varmenteita turvallisesti.
Riskianalyysi		<ul style="list-style-type: none"> • Tuntee muutamia riskianalyysiin liittyviä tapaustutkimuksia. 	<ul style="list-style-type: none"> • Osaa arvioida yksinkertaisten järjestelmien riskejä. 	