

Verkon tietoturva TLT-3301

Laskin ei ole sallittu!

Tentti 21.5.2013 TTY/TIE/Joona Kannisto & Matti Tiainen

Tentti sisältää sanaselitystehtävän, neljä lyhyttä esseettä ja pitkän soveltavan tehtävän. Tehtävien yhteydessä on annettu pistemäärät, joista tentin tekijä voi arvioida vastauksen laajuutta.

Tehtävä 1: Sanaselitystehtävä. Myyntiosaston geelitukka on eksynyt väärille messuille ja haluaa nyt tietää mitä ovat seuraavat termit. Selitä termit ja niiden käyttötarkoitukset:

Kerrospuolustus, meidän toimitalossa on kaksi kerrosta, kumpaakin pitää vahtia, eikö? (1p)

Pakettisuodatus, tämän tiedänkin, eikös tämä ole palomuuuri? (1p)

IDS, autossani on ABS ja ESP, onko tämä parempi vai huonompi? (1p)

Manuaalinen penetraatiotestaus, ??? (1p)

VPN (1p)

DNSSEC (1p)

Tehtävä 2:

Kirjoita lyhyt essee organisaation lokinkäsittelystä (3p)

- Mistä asioista tavanomaisessa organisaatioverossa kannattaa kerätä lokia?
- Mitä kerätyllä tiedolla saa/kannattaa tehdä?
- Mitä hyökkääjä haluaa lokeista?

Kirjoita lyhyt essee keskitetystä autentikoinnista ja käyttöoikeuksien hallinnasta (3p)

- Miksi monissa ympäristöissä käyttäjänhallinta on repaleista?
- Mitä tietoturvahaukia voidaan torjua käyttäjänhallintaa keskittämällä?
- Mitä hyötyä saadaan liiketoimintaan?

Tehtävä 3: Lyhyt essee seuraavista aiheista (3p/kohta):

- IPv6 hyökkäykset ja niiden torjunta pääsyverkossa. (3p)
- Vertaile eri verkonvalvonnan keinoja ja protokollia. Mitä niillä yritetään saavuttaa? (3p) *SNMP*
SYLOG

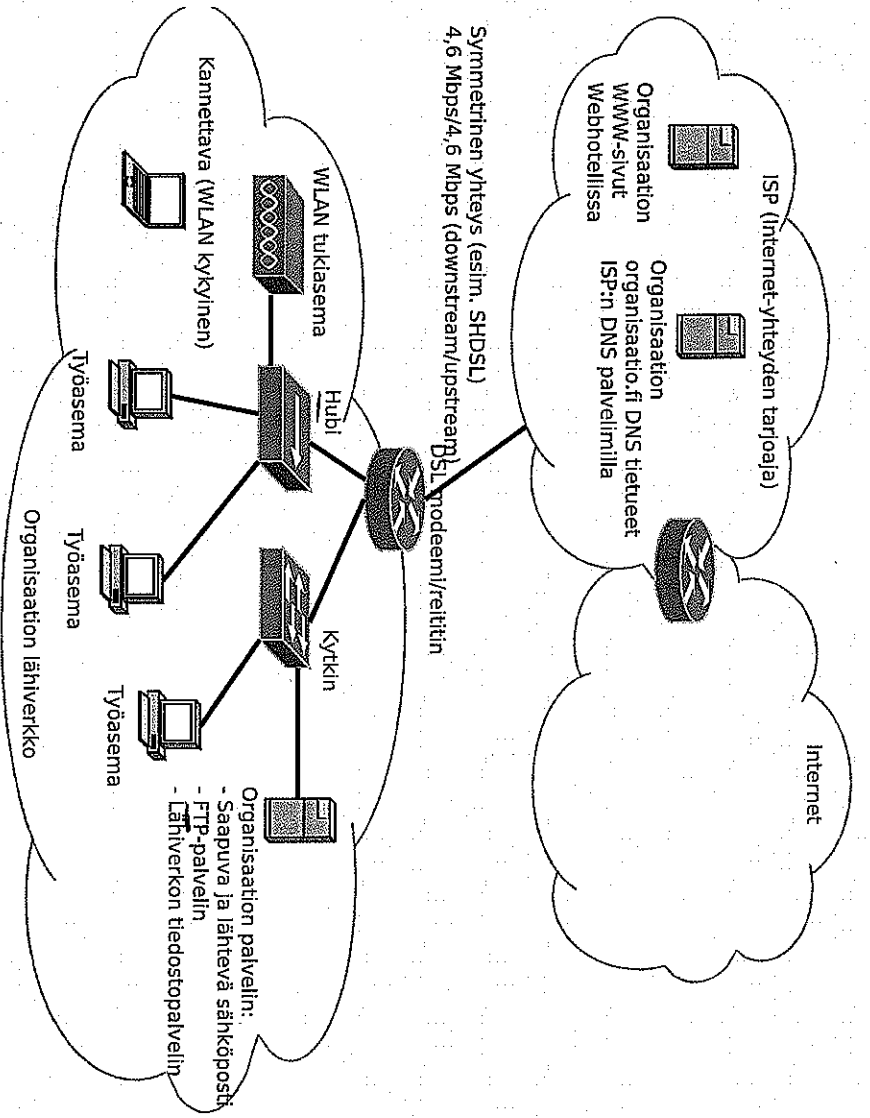
Tehtävä 4: Verkon suunnittelu ja topologiat tietoturvamielessä (6p)

Arvioi liitekuvan verkkoa tietoturvan kannalta

- Miten luottamuksellisuuden ja eheyden tavoitteita voitaisiin parantaa verkossa?
- Miten taas saatavuutta?
- Entäpä liiketoiminnan varsinaisten tavoitteiden saavuttaminen?

Tee havaintojesi pohjalta uusi verkkosuunnitelma. Piirrä kuva ja merkitse selvästi kuvaan laittamasi elementit siten että myös tarkastaja ymmärtää ne.

Fyysinen topologia



Looginen topologia (Verkkoerros)

