Yhteenveto kokeeseen tulevista asioista

Seuraavassa käydään läpi moniste luku luvulta ja katsotaan, missä muodossa asiat tulee hallita. Lukuja IPSec ja SSL ei ehditty käsitellä luennoilla, joten niitä ei myöskään tule kokeeseen.

Luku 1: Yleistä tietoturvasta I

- Kokonaisturvallisuudesta: tiedettävä, mitä asioita siihen kuuluu.
- Tietoturvallisuus: osa-alueet osattava luetella.
- Lait ja viranomaiset: muistettava rikoslakiin kuuluvat lakien nimet, jotka liittyvät tietoturvallisuuteen. Samoin pakkokeinolaista. Harjoitukset 1.4 ja 1.5 vastauksineen kuuluvat kurssiin.
- Vientivalvonta: Kuka Suomessa valvoo?
- Oletetaan, että osaa nimetä muutamia tietoturvaorganisaatioita. Tuntee standardeista SSE-CMM, Common Criteria, BS7799, mihin ne liittyvät.
- Turvallisen suunnittelun periaatteet kokonaan.

Pääsynvalvonta I

- Politiikan ja mekanismin erottaminen.
- Pääsynvalvontatyypit
- Salasanatiedosto ja suolaus.
- Salasanan valinta
- Sateenkaaritaulujen idea
- Tiedostonimityypit Unixissa
- Symboliset linkit
- Erilaiset UID:t, setuid ja salasanan vaihtoesimerkki
- Pääsyoikeuksien asettaminen Unixissa
- Haittaohjelmien luokittelu yleisesti (kertalukemisella), botnetit yleisesti. Ei virusten luokittelua.
- Haittaohjelmilta suojautuminen: pääasiat

Ohjelmien turvallisuus I

- Tyypilliset ohjelmistovirheet esimerkkeineeen
- Implementointi- ja hallintosäännöt
- Ohjelmointikielten turvallisuuspiirteistä
- Javan hyvät puolet (eli miten sovelmia käsitellään)
- Ei Javan huonoja puolia, eikä C:tä

Datan turvallisuus I

- Esimerkki datan luokittelusta organisaatiossa, valtionhallinnon luokitukset.
- Tiedostojen poisto Unixissa, huomioon otettavat seikat. Samoin kopiointi
- Tiivistefunktioilta vaadittavat ominaisuudet, tunnetuimmat tiivistefunktiot.
- MAC-funktion käsite.
- Eheyden käsite ja sen toteuttaminen (MAC-funktion avulla, tiivistefunktion ja digitaalisen allekirjoituksen avulla)
- One time pad eli Vernamin salaus
- Jonosalauksen idea. Ei tarvitse muistaa rekursioyhtälöitä.
- Symmetrisen lohkosalauksen idea. Salausstadardin nimi (AES) ja sen avainten pituudet.
- Ketjutustekniikat

Verkkoturvallisuus I

- Tyypillisen (kohdistetun) hyökkäyksen eteneminen verkossa pääpiirteittäin.
- Käsitteet sormenjäljet, tunnustelu ja skanneri.
- Palvelunestohyökkäysten torjunta: ehdotettuja ratkaisuja protokolliin. Ei tarvitse muistaa luetteloa vanhoista palvelunestohyökkäyksistä.
- Palomuurityypit ja tyypilliset palomuurikonfiguraatiot.
- Hyökkäysyritukset paketteja suodattavaa palomuuria vastaan.
- Julkisen avaimen salauksen idea.
- RSA: miten salataan ja puretaan, kun n, e ja d on annettu.
- Avainten pituudet symmetrisessä ja epäsymmetrisessä salauksessa erilaisissa ympäristöissä ja eri aikaväleillä.
- Digitaalinen allekirjoitus RSA:n avulla: periaate.
- Julkisen avaimen infrastruktuuri: X.509.

Verkkoturvallisuus II

- Varmenteen rakenne, varmennepolut, versio 3 vs versio 2.
- Julkisen avaimen infrastruktuurin ongelmat.
- OCSP