Aiheita tietoturvallisuuden jatkokurssin harjoitustyöhön

Tässä on noin 43 aihetta. Omia aiheita voi ehdottaa ja joissakin aiheissa on tekemistä kahdellekin.

Kokeilut, vertailut, käytäntö

Laadi valmistajien tiedotteiden, ohjelmia vertailevien sivustojen tai lehtien avulla **katsaus** tyypin X ohjelmistoihin. Valitse niistä kaksi tai kolme, jotka ovat jonkin **asettamasi** kriteerin mukaan sopivimpia ja kokeiltavissa. Valittujen ohjelmien pitää löytyä vähintään kahdesta erilaisesta lähteestä. Kokeile ohjelmia ja kirjoita katsauksen jatkeeksi oma **raporttisi**. Tässä X voi olla jokin seuraavista

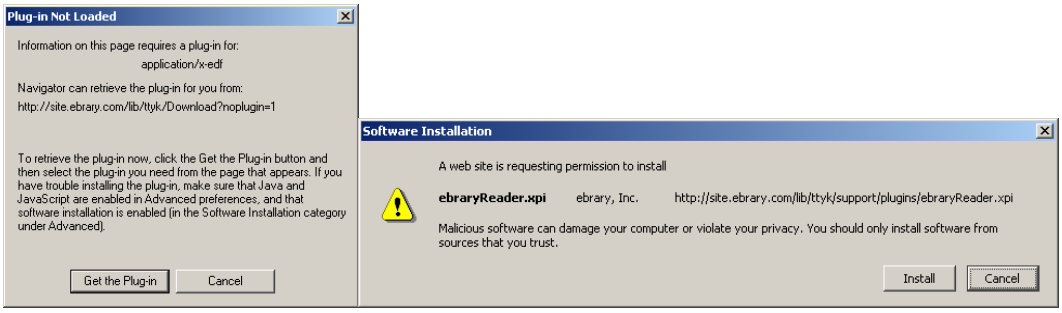
- ► Jälkien siivoaminen
- ► Vakoiluohjelmien poistaminen (esim. Tietokone 2/2005 s. 80)
- ► Seittisisällön suodatus
- ► Henkilökohtaiset palomuurit
- ► VPN
- ► Tiedoston, levyosion tai levyn salaus
- ► Sähköpostin salaus
- ► Roskapostin suodatus
- ► Anonymisointi
- ► Varmuuskopiointi
- ► Ilmaisten SQL-tietokantamoottoreiden pääsynvalvonta
- ► P2P
- ► Sanakirjahyökkäys

Seuraavissa aihepiireissä voi olla vaikeampi löytää kokeiltavaa. Ota silti selvää samassa hengessä kuin eo. tehtävissä:

- ► Biometriikka
- ► Vesileimaus (www.infosec-technologies.com/covert.htm)
- ► Ohjelmistosuojaus, esim. HASP (www.ids.fi/Hasp/SUOJAUS.HTM)
- ► Forensiikka, esim. Encase (www.guidancesoftware.com). Löytyykö sharewarena tai demona?
- ► Visuaaliset salasanat
- ► Salasanalaskurit (SecurID ym.)
- ► Avainten varmuustallennus (key escrow)

► Laadi ohjeet henkilökohtaisessa käytössä olevien toimisto-ohjelmien turva-asetuksille. Oletetaan, että käyttöjärjestelmän ja verkkoyhteyksien asetukset on pannut kuntoon joku muu, eikä käyttäjä niistä paljon ymmärräkään. Hän tarvitsee siis ohjeet tietyn valmistajan ohjelmistoille, joilla hän toimittaa seuraavia tehtäviä: tekstinkäsittely, lomakkeet (PDF), taulukkolaskenta, tietokanta ja sähköposti.

► Laadi eo. tehtävän hengessä ohjeet, miten alla kuvattujen tilanteiden kanssa pitää menetellä:



►► Valitse jokin avoimen koodin ohjelmassa ollut haavoittuvuus, jota jokin hyökkäys tai haittaohjelma on voinut käyttää hyväksi. Näytä kooditasolla, mistä oli kyse, millainen korjaus tarvittiin, miten se muodostui avoimen koodin yhteisössä.

► Network Magazine -lehden 8/2005 artikkeli The Threat From Within käsittelee tietokantojen luottamuksellisuutta, kun uhkana on oikeutetun käyttäjän vilpillisyys. Tiivistä artikkelin esitettämät suositukset ja kaiva kahdesta tietokantatuotteesta esille suosituksia tukevat ominaisuudet.

Vähemmän omakohtaisia aiheita

►► Tutki jonkin tuoreen tunnetun viruksen koodia, sen variointia ja siihen liittyviä kirjoitustyökaluja.

► Etsi tietoa haittaohjelmista, jotka voivat häiritä tietojenkäsittelyä alueilla, jotka ovat toistaiseksi enimmäkseen säästyneet, nimittäin älypuhelimet ja autot (ja muutkin alueet jos jotain löytyy).

► Lähtien liikkeelle esim. artikkelista A.Whitten, J.Tygar: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0 etsi lisää tutkimuksia tietoturvamekanismien käytettävyydestä.

► Toimikorttien ja niiden lukulaitesysteemien turvallisuus: tuoreimmat tiedot.

► Käytännön tekniikoita suojautumiseen hajasäteilyn aiheuttamilta tietovuodoilta.

►► Jokin sopiva luku Furhtin ja Kirovskin toimittamasta kirjasta: Multimedia Security Handbook (2005), joka on TTY:n kirjastossa elektronisesti.

Hallinto

► Mobiilivarmenteiden tekniikka pintaa syvemmältä + SMS-maksaminen.

► Network Magazine -lehden 8/2005 viimeinen artikkeli (kolumni, otsikolla ”Take My Social Security Number--Please!”) ehdottaa Yhdysvalloissa kaavaillun henkilökorttihankkeen sijalle jotain kovin toisenlaista. Yhtenä ideana siinä on hajautus ja toisena yksilöiden mahdollisuus ikäänkuin käydä kauppaa yksityisyyden ja käytettävyyden välillä. Ota selvää, mitä USA:n hallitus suunnittelee ja mistä tässä ehdotuksessa on kyse. Punnitse ehdotuksen ominaisuuksia ja tarkastele, olisiko vastaava mahdollinen tai tarpeellinen Suomessa.

► Verkkosivujen kävijämäärälaskureiden luotettavuus mainosten hinnoittelun/laskutuksen kannalta.

► Jokin todellinen äänestysprotokolla.

Tietoaineistot ja tietokannat

► Tutki verkkotallennuksen tietoturvaominaisuuksia: perinteinen NFS (network file system), NAS (netw. attached storage), SAN (storage area netw.) ja ISCSI (Internet SCSI (small computer system interface)). Saatavuuden lisäksi tarkastele, pitääkö yhteyksien olla sinänsä turvallisia vai onko käytettävissä turvaprotokollia? (Tietokone 2/2005)

►Varmuuskopioinnin, tarkastamisen ja palauttamisen menettely käytännössä. ”Kokeiluaiheeseen” verrattuna tässä on kyse isosta tietojärjestelmästä ja mukaan tarvitaan hallinnollisia ohjeita.

► Miten torjutaan bit rot -ilmiötä, esimerkkinä Dspace-hanke? Mitä muuta kuin tiedon säilyminen on otettava huomioon? (IEEE Spectrum July /2005)

Tietoverkot

►WPA eli WiFi Protected Access.

Network Magazine myönsi toukokuussa 2005 30 IT-hankkeelle innovaatiopalkinnon. Kolme näistä on tietoturvan alueelta (kohta ”Security Goes to Business School”) ja yksi voitti myös koko ”kisan”.

- ► Ciscon NAC-systeemi (Network Admission Control)
- ► Skybox View: Riskien mittaaminen
- ► Spam-palomuuri

► Onko portinkoputuksessa jotain tolkkua? (www.portknocking.org)

► Selvitä, mistä tässä oli ja on kyse:

> Tomorrow, on Tuesday 27.9.2005 starting at 13.15 in TC148 Dr. Andrei Gurtov <http://www.cs.helsinki.fi/u/gurtov> from HIIT <http://www.hiit.fi/> will give a talk with the following title:
>
> Hi3: An Efficient and Secure Networking Architecture for Mobile Hosts
>
> **Abstract:**
> The Host Identity Indirection Infrastructure (Hi3) is a networking architecture for mobile hosts, derived from the Internet Indirection Infrastructure (i3) and the Host Identity Protocol (HIP). Hi3 has efficient support for secure mobility and multihoming, which both are crucial for future Internet applications. Compared to Mobile IP, Hi3 achieves better resilience, scalability and security. Considering all capabilities Hi3 provides, its implementation is much simpler than a corresponding implementation based on existing or proposed IETF standards. We present analytical analysis of scalability of the Hi3 control plane, and show preliminary performance measurement results.