TIEA222 Tietoturva
3. viikkoharjoitus
12.10.2010

Vastaukset on palautettava 19.10.2010 mennessä.

Ohjeet

Viikkotehtävät läpikäydään luennon alussa ja opiskelija merkitsee tekemänsä tehtävät salissa kiertävään listaan. Merkitsemällä tehtävän tehdyksi on valmis esittämään vastauksensa muille opiskelijoille. Tehtävistä saa lähtökohtaisesti merkitsemänsä pisteet. Käytäntö on tuttu matematiikan harjoituksista.

Vastaukset palautetaan etukäteen sähköpostitse riippumatta siitä, pääseekö itse paikalle. Pelkästään sähköpostilla palautetut vastaukset arvostellaan kuitenkin tarkemmin ja yksi kerrallaan.

Demotilaisuuteen ei tarvitse valmistautua millään tavalla. Ohjaaja löytää vastaukset sähköpostista, jotka opiskelija esittelee ja tarvittaessa ohjaaja kysyy tarkentavia kysymyksiä.

Lähetä vastaukset sähköpostilla osoitteeseen `tietoturva@zouppen.iki.fi`, otsikkona `Viikkoharjoitus 3`. Palautus viimeistään 19.10.2010 klo 12.00 mennessä.

Tehtävä 1 ☕☕☕

Lue artikkeli *Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure*. Kerro artikkelissa mainituista kymmenestä riskistä pääkohdat.

`http://www.schneier.com/paper-pki.pdf`

1. Keihin luotamme ja miksi?
2. Kuka voi käyttää salaista avaintani?
3. Kuinka turvallinen todentava tietokone on?
4. Samannimiset henkilöt. kuka on kukin?
5. CA:n auktoriteetti, onko CA valtuutettu?
6. Loppukäyttäjän rooli, onko käyttäjä osa tietoturvaa?
7. CA- ketjun turvallisuus/luottamus, yksi CA vai CA ja RA?
8. Miten CA indentifioi sertifikaatin haltijan, ja yksityisen avaimen omistajan?
9. Kuinka turvallisia sertifikaattien käytänteet ja myönnöt ovat (avaimet, serifikaattien tarkistus)?
10. Miksi käytämme koko CA-prosessia?

Tehtävä 2 ☕

Selvitä osoitteesta `http://www.jyu.fi/` löytyvän HTTP-palvelinohjelmiston nimi ja versio. Kerro miten hyökkääjä voi hyötyä näistä tiedoista. Voit käyttää selvityksessä apuna netcat-ohjelmaa (komentorivillä `nc`).

Netcat löytyy Linux-jakeluiden pakettihallinnasta. Se on myös valmiiksi asennettuna myös `jalava.cc.jyu.fi`-palvelimella.

Tehtävä 3 ☕☕

Selitä lyhyesti Teardrop-hyökkäys. Mitä käyttöjärjestelmiä ongelma koski? Selitä lyhyesti LAND-palvelunestohyökkäys. Koska se havaittiin ja mitkä järjestelmät olivat haavoittuvia?

Tehtävä 4 ☕☕

Selitä Kerberos-autentikointiprotokollan toimintaperiaate yleisellä tasolla sekä sen toiminta Windows 2000 Active Directoryn yhteydessä.
`http://msdn.microsoft.com/en-us/library/aa378747%28VS.85%29.aspx`

Tehtävä 5 ☕☕☕☕☕☕

Tästä bonustehtävästä on jaossa enintään 6 pistettä riippuen raportin perusteellisuudesta.

Asenna Radius-palvelin koneellesi (esim. Free Radius, `http://freeradius.org/`) ja konfiguroi se toimimaan siten, että NAS:na toimii WLAN- tukiasemasi. Tällöin tukiaseman kautta verkkoon liittyvät langattomat käyttäjät autentikoidaan RADIUS-palvelimessa.

Testaa toiminnallisuus ja raportoi tarvittavat konfiguraatiot sekä liitä raporttiin testitrace, josta käy ilmi NAS:n ja Radiuksen välinen kommunikaatio. Viestinnän kaappaamiseen soveltuu esimerkiksi Wireshark.

Jos et halua koskea oman tietokoneesi asetuksiin, voit käyttää suoraan cd-levyltä käytettävää pfSense-ohjelmistoa. `http://www.pfsense.org/`.

Jos sinulla ei ole mahdollista tehdä tätä harjoitusta oikealla laitteistolla, niin voit raportoida työn teoreettisesti eli kuvailemalla Free Radiuksen toiminnallisuudet ja työvaiheet toimintakuntoon saattamiseksi.

Vinkki: Laboratoriotyössä 2 oppimasi taidot ja työohje auttavat.

Palaute

Palautteesta ei myönnetä pisteitä, mutta se auttaa kurssin suunnittelussa.

a) Kuinka paljon näihin viikkotehtäviin kului aikaa?

b) Oliko jokin tehtävistä huomattavasti vaikeampi kuin pistemäärästä arvaisi?

c) Muuta viikkotehtäviin liittyvää palautetta?

Kiitos!