

TIEA222 Tietoturva
4. viikkoharjoitus
20.10.2010

Vastaukset on palautettava 26.10.2010 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 4. Palautus viimeistään 26.10.2010 klo 12.00 mennessä.

Tehtävä 1 ☕

IPSec:n tunnelimoodissa muodostetaan paketille uusi IP-otsikko. Mitkä uuden IP-otsikon kentät ovat riippuvaisia alkuperäisistä kentistä ja millä tavalla?

Tehtävä 2 ☕

Millä tavoin IPSec antaa suojan toistohyökkäystä vastaan?

Tehtävä 3 ☕☕☕

Tässä tehtävässä on tarkoitus muodostaa palomuuuri Linuxin Iptables-pakettisuodatimen sääntöjen avulla. Voit luetella sääntöjen laadintaan tarvittavat komennot käsin tai laatia skriptin, joka on yhteensopiva komennon `iptables-restore` kanssa. Voit käyttää myös muun järjestelmän käyttämää syntaksia, jos haluat. Tällöin liitä vastaukseesi lähde käyttämästäsi järjestelmästä ja sääntöjen formaatista.

Seikkaperäiset ohjeet Iptablesin käyttämästä syntaksista löytyvät osoitteesta http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO:_Ch14:_Linux_Firewalls_Using_iptables. Tehtävässä sääntöjen laadinnan pohjana voit halutessasi käyttää osoitteessa <http://www.mista.nu/iptables/> sijaitsevaa sääntögeneraattoria.

Vaikka esimerkissä oleva verkkoalue on yksityiseen käyttöön tarkoitettulta alueelta *10.0.0.0/8*, voit käsitellä sitä tässä tehtävässä kuin se olisi osa julkista Internetiä. Toisin sanoen sääntöjä laatiessasi ei tarvitse kiinnittää huomiota osoitteenmuutoksiin (NAT).

Määrittele Iptables-järjestelmän mukaiset palomuurisäännöt seuraavaan ympäristöön:

- Palomuuuri sijaitsee yksityisen verkon ja Internetin rajalla, suodattaen kumpaankin suuntaan kulkevaa liikennettä.
- Yksityinen verkko koostuu verkkoalueesta *10.0.0.0/24*
- Sisäverkon laitteilta tulee sallia seuraavien palveluiden toiminta kohteesta riippumatta:
 - ssh
 - smtp
 - dns
 - http
 - pop
 - imap
- Sisäverkossa toimii seuraavat palvelimet, joihin tulee päästä käsiksi Internetistä käsin.:
 - ssh-palvelin osoitteessa *10.0.0.104*
 - http-palvelin osoitteessa *10.0.0.105*
 - smtp-palvelin osoitteessa *10.0.0.110*
- Kaikki muu liikenne tulee estää.
- Palomuuriin tulee konfiguroida myös Smurf-hyökkäysten esto, eli se, että Internetistä ei sallita broadcast-lähetyksiä sisäverkkoon. Kirjoita tämä sääntö, vaikka se sisältyisikin muihin sääntöihin.

Tehtävä 4 ☕☕

Lue artikkeli Unicode-merkistön avulla tehtävästä NIDS-laitteiden (Network Intrusion Detection Systems) huijaamisesta. Selitä, miten huijaus tapahtuu, ja kuinka se voidaan torjua.

Eräs mahdollinen lähde: <http://www.securityfocus.com/infocus/1232>

Tehtävä 5 ☕☕☕

Tutustu johonkin Unicode-merkistön tai sen koodauksen (UTF-8, UTF-16, ...) käsitteeseen liittyvään tietoturva-aukkoon. Kerro, miten haavoittuvuus ilmenee ja pohdi sitä, kuinka paljon mielestäsi syyksi voidaan laskea puutteet merkistön määrittelyssä tai koodaustavassa? Vai voiko kyseisen haavoittuvuuden laskea kokonaan sovelluksen ohjelmoijan huolimattomuuden piikkiin?

Riippuen vastauksen perusteellisuudesta, tästä tehtävästä voi saada enintään 3 pistettä. Liitä vastaukseesi käyttämäsi lähteet.

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!