TIEA222 Tietoturva
2. viikkoharjoitus
30.9.2010

Vastaukset on palautettava 6.10.2010 mennessä.

Ohjeet

Kurssiin kuuluu 4 viikkoharjoitusta. Viikkoharjoitukset jakautuvat tehtäviin, joista jaettavat pisteet käyvät ilmi ☕-merkkien määrästä. Yhteensä pisteitä on jaossa 32. Kurssin suoritukseen vaaditaan 16 pistettä.

Tehtävistä annetaan hyvityspisteitä tenttiin seuraavan taulukon mukaisesti:

pisteitä	hyvitys
16,0	0
20,0	+1
22,0	+2
24,0	+3
26,0	+4
28,0	+5
30,0	+6

Vastaukset palautetaan sähköpostilla 6.10.2010 mennessä. Mikäli vastaukset ovat ryhmältä, mainitse selkeästi myös muiden ryhmän jäsenten nimet. Lähetä sähköposti osoitteeseen `tietoturva@zouppen.iki.fi`, otsikkona `Viikkoharjoitus 2`.

Vastaukset voi kirjoittaa sähköpostiviestiin joko sellaisenaan tai sisällyttää PDF-liitteenä. Muut tiedostomuodot eivät käy. Mikäli vastauksiin liittää kuvankaappauksia, ne kannattaa sijoittaa PDF-tiedostoon tekstin joukkoon. Mikäli kirjoitat vastauksesi suoraan sähköpostiviestiin, kuvat voi toimittaa liitetiedostoina PNG- tai JPEG-muodossa.

Tehtävät tarkistetaan käsin ja Korppiin kirjataan viikkoharjoituksista myönnetyt pistemäärät viikon kuluessa palautuksen takarajasta.

Tehtävä 1 ☕☕

Kerro lyhyesti miten Ciscon verkkolaitteissa käyttäjien salasanat pidetään salassa? Mikä heikkous Ciscon laitteiden salasanoissa on esiintynyt aiemmin ja mistä se johtui? Mitä tarkoittavat komennot `enable password` ja `enable secret` ja miten ne liittyvät Ciscon laitteiden salasanojen turvallisuuteen? Selvitä lopuksi alla olevan Ciscon käyttäjätunnuksen heikko salasana.

```
username admin password 7 00271A150754
```

Vinkki: Netistä löytyy useita ohjelmia heikkojen salasanojen purkamiseen, joissakin työkaluissa on virheitä tai eroja, jolloin purettu salasana ei ole oikea, mutta oikea salasana on helposti pääteltävissä siitä.

Tehtävä 2 ☕☕

Selitä lyhyesti mitä tarkoittaa Cisco Port Security? Anna esimerkki, mitä vastaan Port Security suojaa? Onko Port Security päällekkäinen 802.1x- standardin kanssa vai täydentävätkö ne toisiaan?

Tehtävä 3 ☕☕

Selitä lyhyesti mikä on Spanning Tree Protocol (lyh. *STP*) ja miten sen avulla voidaan toteuttaa DoS-hyökkäys? Tietoja aiheesta voit löytää standardista IEEE 802.1D, jossa STP on määritelty.

Tehtävä 4 ☕☕

Tutki sivun `https://www.jyu.fi` varmenteita. Löydät ne Web-selaimestasi sivun tietojen yhteydestä.

a) Tiedoissa mainitaan *Sonera*. Mitä tekemistä tällä yrityksellä on sivun kanssa?

a) Mihin asti sertifikaatti on voimassa ja mitä salausalgoritmejä käytetään?

b) Miten ja millaisia hierarkioita PKI:n CA:ssa on ja mikä on hierarkian globaali juuritaso?

Tehtävä 5 ☕☕☕☕☕☕

Tämä tehtävä on bonustehtävä, josta voi saada korkeintaan 6 pistettä riippuen vastauksen perusteellisuudesta.

Tässä työssä sinun tulee tutustua WLAN:n yhteydenmuodostukseen verkossa, joka käyttää joko WPA- tai WPA2-salausmenetelmää. Kaappaa WLAN-tukiaseman ja oman tietokoneesi välistä liikennettä ja esittele yhteyden muodostuksen vaiheet, mukaanlukien salausavainten vaihdon. Käytä esimerkkinä kaappaamaasi liikennettä.

Tehtävässä apuna voit käyttää *aircrack-ng*-sovelluksen liikenteen kaappaukseen työkaluja, *Wiresharkin* analysointityökaluja tai muita tarkoitukseen sopivia työkaluja.

Voit kaapata liikennettä haluamastasi WLAN-verkoista. Myös `jyu-student` soveltuu, kunhan huomioit, että et vastaanota muille tarkoitettua liikennettä etkä häiritse verkon normaalia toimintaa. Myösään verkon salausta ei tule purkaa, vaan seurata yhteydenmuodostusta.

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!