

**Verkkovarmenteet yrityskäytössä**

Tatu Erkinjuntti, Jussi Isosomppi, Eino Kupias, Saku Kähäri

Tietoturvan hallinta -kurssi

Tietojenkäsittelyn koulutusohjelma

11.9.2017

|  |  |
| --- | --- |
| **Tekijä(t)**  Tatu Erkinjuntti, Jussi Isosomppi, Eino Kupias, Saku Kähäri | |
| **Koulutusohjelma** | |
| **Raportin nimi** Verkkovarmenteet yrityskäytössä | **Sivu- ja liitesivumäärä**  19 + 2 |
| Tiivistelmä edellytetään pääsääntöisesti vain opinnäytetöissä.  Opinnäytetyön tiivistelmässä esitetään työn keskeiset kohdat siten, että lukija ymmärtää tiivistelmän luettuaan työn sisältämät pääasiat. Tiivistelmässä esitetään selvitettävän asian tausta, työn tavoite ja rajaus, työn toteutustapa ja mahdolliset menetelmät, työn tekemisen ajankohta sekä tulokset ja päätelmät. Tiivistelmä etenee raportin mukaisessa järjestyksessä.  Tiivistelmä on enintään yhden sivun pituinen. Käytä tiivistelmässä asiatyyliä eli kirjoita tiiviisti, ymmärrettävästi ja kieliopillisesti oikein. Käytä kokonaisia lauseita ja virkkeitä. Jaa teksti muutaman virkkeen mittaisiin kappaleisiin ja erota kappaleet toisistaan ylimääräisellä rivinvaihdolla. Aloita uusi kappale siirtyessäsi uuteen asiaan. Tiivistelmä ei saa sisältää lähdeviitteitä.  Tiivistelmä on siis kuin itse opinnäytetyö pienoiskoossa. Tiivistelmän pitää olla itsenäinen kokonaisuus, joka on ymmärrettävissä itse opinnäytetyötä lukematta. | |
| **Asiasanat**  SSL/TLS, Sertifikaatti, Verkkoselain, | |

Sisällys

[1 Johdanto 1](#_Toc531958376)

[2 Projektin työsuunnitelma 2](#_Toc531958377)

[3 Varmenteiden tutkimus 3](#_Toc531958378)

[3.1 Yleinen käsite PKI 3](#_Toc531958379)

[3.2 CA/WOT 3](#_Toc531958380)

[3.3 Heikkoudet hyödyt 3](#_Toc531958381)

[4 Testaus 4](#_Toc531958382)

[4.1 OCSP 4](#_Toc531958383)

[4.1.1 Muutos 4](#_Toc531958384)

[4.1.2 Blokkaus 4](#_Toc531958385)

[4.2 Root cert asennus 4](#_Toc531958386)

[4.3 CA DOS 4](#_Toc531958387)

[4.4 Moxy 4](#_Toc531958388)

[4.5 Ettercap / bettercap 4](#_Toc531958389)

[4.6 Tulosten yhteenveto 4](#_Toc531958390)

[5 Ohjeistus 5](#_Toc531958391)

[5.1 Kenelle miksi 5](#_Toc531958392)

[5.2 Koonti / tarina kehityksestä 5](#_Toc531958393)

[6 Suositukset varmenteiden käyttöön 6](#_Toc531958394)

[7 Yhteenveto 7](#_Toc531958395)

[Lähteet 8](#_Toc531958396)

[Liitteet 9](#_Toc531958397)

[Liite 1: Tuotekortti: Tietoturvan peruskartoitus 9](#_Toc531958398)

[Liite 2. Kartoituskysymykset vastauksineen 10](#_Toc531958399)

# Johdanto

Projektin tarkoitus

# Projektin työsuunnitelma

Työsuunnitelma

# Varmenteiden tutkimus

Kuva

## Yleinen käsite PKI

Dsdsds

## CA/WOT

Fdsfds

## Heikkoudet hyödyt

# Testaus

Suunnittelu!

## OCSP

Mikä

### Muutos

### Blokkaus

## Root cert asennus

## CA DOS

## Moxy

Arp spoof sslstrip

## Ettercap / bettercap

## Tulosten yhteenveto

# Ohjeistus

Yleinen

## Kenelle miksi

Fds

## Koonti / tarina kehityksestä

# Suositukset varmenteiden käyttöön ( vai meneekö yhteenvetoon?)

Yhteenvedon voit halutessasi myös jättää pois.

# Yhteenveto

# Lähteet

# Liitteet

## Liite 1: Tuotekortti: Tietoturvan peruskartoitus

## Liite 2. Kartoituskysymykset vastauksineen