

TIEA222 Tietoturva
1. viikkoharjoitus
22.9.2010

Vastaukset on palautettava 29.9.2010 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 29.9.2010 mennessä. Mikäli vastaukset ovat ryhmältä, mainitse selkeästi myös muiden ryhmän jäsenten nimet. Lähetä sähköposti osoitteeseen `tietoturva@zouppen.iki.fi`, otsikkona Viikkoharjoitus 1.

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 myönnetty pistemäärät viikon kuluessa palautuksen takarajasta.

Tehtävä 1 ☕☕

Lue Phishing-artikkeli ja kerro tutkimuksen päätulokset.

http://users.jyu.fi/~timoh/TIEA222/why_phishing_works.pdf

Tehtävä 2 ☕☕

Tässä tehtävässä tutustutaan tunnistetietoihin, joita selaimesi välittää HTTP-kyselyn yhteydessä. Asenna koneellesi jokin protokolla-analysaattori, kuten Wireshark. Sovellus löytyy osoitteesta <http://www.wireshark.org/> ja Linux-jakeluiden pakettihallinnasta.

Laita analysaattori tallentamaan liikennettä ja vieraile kahdella WWW-sivulla, joista ensimmäinen käyttää HTTP:tä ja toinen HTTPS:ää. Lopeta yhteyden kaappaus ja tarkastele yhteyden muodostumista palvelimille. Vastaa seuraaviin kysymyksiin lyhyesti perustellen:

- a) Mitä tunnistetietoja selain välittää palvelimelle HTTP-kyselyn ohessa? Millä tavoin selaimen lähettämiä tietoja voidaan hyödyntää tietoturvahyökkäyksissä?
- b) Mitä tunnistetietoja palvelin lähettää selaimelle HTTP-kyselyyn vastatessa? Millä tavoin palvelimen lähettämiä tietoja voidaan hyödyntää tietoturvahyökkäyksissä?
- c) Miten tulokset eroavat HTTPS:llä liikennöitäessä? Suojaako HTTPS:n käyttö osapuolia tunnistetietojen keräilyltä? Perustele.

Liitä vastaukseen kuvankaappaus protokolla-analysaattorista, jossa näkyy ainakin osa jonkin HTTP-kyselyn sisältämistä tunnistetiedoista.

Tehtävä 3 ☕☕

Tutustu Tor-ohjelmistoon osoitteessa <http://www.torproject.org/>. Asenna www-selaimesi tuki Tor:lle. Ohjeet eri käyttöjärjestelmille:

Mac OS X: <http://www.torproject.org/docs/tor-doc-osx.html.en>
Ubuntu Linux: <http://wiki.ubuntu-fi.org/Tor>
Windows: <http://www.torproject.org/docs/tor-doc-windows.html.en>

- a) Mitä Tor-ohjelmisto tekee ja miten se toimii? Mitä hyötyjä ja haittoja sen käytöstä on?
- b) Tutki Tor:n aiheuttamaa liikennettä käyttäen protokolla-analysaattoria. Miten liikennöinti poikkeaa edellisen tehtävään verrattuna?
- c) Liitä vastaukseen yksi Tor:n välittämä paketti. Otsikkotiedot riittävät.

Huom! Tor:n käyttö on Suomessa sallittua. Kannattaa kuitenkin kytkeä Tor pois käytöstä tämän tehtävän suorittamisen jälkeen, koska se käyttää paljon tietoliikennekapasiteettia.

Tehtävä 4 ☕☕

Kerää HTTP-liikennettä protokolla-analysaattorilla. Mikäli teit edellisen tehtävän, kannattaa uusiokäyttää siinä keräämääsi HTTP-liikennettä.

- a) Selitä, mitä tarkoittaa TCP-yhteyden kaappaus (engl. *TCP-hijacking*) ja kuinka siltä voidaan suojautua?

- b) Kuinka kaappaus toteutetaan käytännössä? Käytä esimerkkinä keräämääsi dataa ja kerro, mitä hyökkääjän tulisi tehdä yhteyden kaappaamiseksi. Liitä paketteja vastaukseesi.

Kohtaan *b* vastaaminen edellyttää pakettien kaappaamista. Pakettien liittäminen vastaukseen onnistuu Wiresharkissa siten, että käyttää *mark*-toimintoa haluttujen pakettien valitsemiseen, jonka jälkeen niiden tallentaminen tekstitiedostoon onnistuu toiminnolla *File...Export...as plain text*. Paketit voi liittää joko vastausten joukkoon tai tekstimuotoisena (.txt) liitteenä.

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!