Sikker browsing, plugins og Tor project workshop

Henrik Lund Kramshøj

hlk@solido.net

16. februar 2014

Indhold

Forord

Dette kursusmateriale er beregnet til brug på kurset *Sikker browsing, plugins og Tor project workshop*. Materialet er lavet af Henrik Lund Kramshøj, http://www.solido.net
Materialet skal opfattes som øvelseshæfte til kurset, og indeholder derfor ikke en fuldstændig beskrivelse af emnet. Der henvises istedet til andet materiale om emnet som nævnt i litteraturlisten.
Til workshoppen hører desuden en præsentation som udleveres.
God fornøjelse

Oversigt

Materialet er inddelt i et antal øvelser som er beregnet til at give kursusdeltagerne et indblik i hvordan Sikker browsing, plugins og Tor project praksis ser ud og opfører sig.

Formålet med workshoppen er at give deltagerne en praktisk erfaring med emnet og information til selv at komme igang.

Forudsætninger og ordliste

Dette kursusmateriale forudsætter at deltageren har kendskab til internet og e-mail på brugerniveau. Det betyder at web adresser som http://www.solido.net, og email adresser som hlk@solido.net ikke bør være ukendte.

Bemærk at til de fleste værktøjer findes god information på internet, eksempelvis videoer på Youtube.com.

Værktøjer

Dette materiale er udarbejdet ved hjælp af en masse værktøjer, og er beregnet på at kunne udføres i et almindeligt kursuslokale med netværksopkoblede pc'er.

De praktiske øvelser benytter i vid udstrækning Open Source og kan derfor afvikles på blandt andet følgende platforme:

- Microsoft Windows 7
- Mac OS X
- Linux

Det anbefales at benytte virtualiseringsplatforme til hackerværktøjer, herunder Kali Linux. Der findes flere alternativer som:

- VMware Player https://www.vmware.com/products/player/
- VirtualBox https://www.virtualbox.org/
- Xen http://www.xen.org/

Indholdet i øvelserne

De fleste af øvelserne har følgende indhold:

- **Opgave:** Hvad går øvelsen ud på
- **Formål:** Hvad forventes det at man lærer ved at løse opgaven
- **Forslag til fremgangsmåde:** er en hjælp til at komme igang
- **Hjælp:** er flere tips eller beskrivelser af hvordan man kan løse opgaven
- **Forslag til løsning:** en mulig løsning til opgaven
- **Diskussion:** er oplæg til diskussion efter løsning af opgaven. Der er mulighed for at sammenligne og diskutere de valgte løsninger.

Øvelse 1

Installation af alternativ browser

Opgave:
Installer en alternativ browser på din PC, eksempelvis Firefox eller Chrome

Forslag til fremgangsmåde:
Hent installationsprogrammet fra http://www.mozilla.org eller http://www.google.com/chrome

Hjælp:
En ekstra browser giver mulighed for nemt at have sikre indstillinger når man surfer på internet.

Forslag til løsning:
Hent installationsprogrammet og udfør installationen

Diskussion:
Vi bruger Firefox for at have en alternativ browser, som kan indstilles mere paranoidt, kan udvides med plugins, Flash blocker m.v.

Det er valgfrit hvilken browser man vælger, men en alternativ browser giver muligheder for bedre sikkerhedsindstillinger.

Mac brugere kan derefter bruge Safari, mens Windows brugere kan fortsætte med Internet Explorer til NemID/Netbank og sites man stoler på.

Husk at installere plugins som:

- Firefox CertPatrol
- Firefox / Chrome - HTTPS Everywhere
- Firefox NoScripts/ Chrome NotScripts

Øvelse 2

Installation af Thunderbird

Opgave:
Installer Thunderbird mailklienten på din PC

Forslag til fremgangsmåde:
Hent installationsprogrammet lokalt eller fra http://www.mozilla.org

Hjælp:

Forslag til løsning:
Hent installationsprogrammet og udfør installationen.

Diskussion:
Thunderbird anbefales fremfor eksempelvis Outlook og Apple Mail grundet de gode muligheder for udvidelser, herunder Enigmail OpenGPG plugin.

På Mac OS X kan benyttes den indbyggede Mail.app med GPGMail plugin - hvis man kan leve med at den ikke altid findes til nyeste version af Mac OS X.

På andre UNIX varianter er Mutt mail reader populær og integrerer nemt til OpenGPG.

Thunderbird giver også mulighed for nem mail filtrering med eksempelvis Sieve og Dovecot.

Øvelse 3

Installation af GPG GNU Privacy Guard

Opgave:
Installer GNU Privacy Guard på jeres PC.

Forslag til fremgangsmåde:
Hent installationsprogrammet og installer - brug pakkesystemerne hvis I bruger Linux

Mac OS X brugere kan med fordel benytte https://www.gpgtools.org/

Hjælp:

Forslag til løsning:

Diskussion:

Øvelse 4

Installation af Enigmail plugin

Opgave:
Installer Enigmail plugin til Thunderbird

Forslag til fremgangsmåde:
Hent installationsprogrammet og installer

Hjælp:

Forslag til løsning:
Det nemmeste er at gå til hjemmesiden for Enigmail

http://enigmail.mozdev.org/

Diskussion:
Enigmail kræver at GNU Privacy Guard er installeret

Øvelse 5

Lav en PGP-kompatibel nøgle

Opgave:
Brug et valgfrit program til at lave en PGP-kompatibel nøgle

Forslag til fremgangsmåde:
Brug Enigmail Key Manager eller PGP pakken til at generere en nøgle

Hjælp:
Sørg for at lave din første nøgle med udløbsdato!

Sørg for at lave et revocation certificate på din første nøgle - så kan du altid trække den tilbage - selvom du glemmer kodeordet.

Forslag til løsning:
Brug det lokale mailsetup som eksempel og lav en nøgle

Diskussion:
Husk at hvis det skal være en rigtig nøgle skal du helst bruge din rigtige mailadresse

Jeg vil ikke anbefale at der uploades ”testnøgler”til keyservere, da man ikke kan slette sine nøgler.

Øvelse 6

Hent en nøgle fra en anden

Opgave:
Find en nøgle og indlæs den i din nøglering

Forslag til fremgangsmåde:
Brug enten en keyserver http://pgp.mit.edu eller en USB nøgle til at overføre en elektronisk udgave af nøglen til din PC

husk at verificere fingerprint

Hjælp:

Forslag til løsning:

Diskussion:

Øvelse 7

Send en krypteret mail

Opgave:
Send en krypteret mail

Forslag til fremgangsmåde:
Brug PGP pakken eller Thunderbird til at sende en krypteret mail til en af de andre

Hjælp:

Forslag til løsning:

Diskussion:

Øvelse 8

Signer en nøgle

Opgave:
Find ud af hvordan du laver en signatur på en nøgle og returnerer den

Forslag til fremgangsmåde:

Hjælp:

Forslag til løsning:

Diskussion:
Det er en god politik KUN at signere nøgler hvor man har fået fremvist officielle papirer som kørekort og pas.

Læg yderligere mærke til at det som signaturen angiver er om den nøgle tilhører vedkommende - ikke om vedkommende er troværdig!

Øvelse 9

Installation af Truecrypt

Opgave:
Installer Truecrypt pakken fra http://www.truecrypt.org/

Forslag til fremgangsmåde:
Hent installationsprogrammet og installer

Hjælp:

Forslag til løsning:

Diskussion:

Øvelse 10

Installation af FileZilla

Opgave:
Installer FileZilla pakken fra http://filezilla-project.org/

Forslag til fremgangsmåde:
Hent installationsprogrammet og installer FileZilla, alternativt WinSCP eller et andet program der forstår SFTP

Hjælp:

Forslag til løsning:

Diskussion:
Det er vigtigt at bruge sikre protokoller når man overfører data, eksempelvis til opdatering af websites

Øvelse 11

Installation af Torbrowser

Opgave:
Installer Torbrowser pakken fra http://www.torproject.org/

Forslag til fremgangsmåde:
Hent installationsprogrammet og installer

Hjælp:

Forslag til løsning:

Diskussion:

