

# Paranoia and government hacking workshop

Henrik Lund Kramshøj

hlk@solido.net

25. oktober 2013



# Indhold

<b>1</b>	<b>Wireshark installation</b>	<b>3</b>
<b>2</b>	<b>Sniffing network packets</b>	<b>4</b>
<b>3</b>	<b>Installation af alternativ browser</b>	<b>5</b>
<b>4</b>	<b>Installation af Thunderbird</b>	<b>6</b>
<b>5</b>	<b>Installation af GPG GNU Privacy Guard</b>	<b>7</b>
<b>6</b>	<b>Installation af Truecrypt</b>	<b>8</b>
<b>7</b>	<b>Installation af Enigmail plugin</b>	<b>9</b>
<b>8</b>	<b>Lav en PGP-kompatibel nøgle</b>	<b>10</b>
<b>9</b>	<b>Hent en nøgle fra en anden</b>	<b>11</b>
<b>10</b>	<b>Send en krypteret mail</b>	<b>12</b>
<b>11</b>	<b>Signer en nøgle</b>	<b>13</b>
<b>12</b>	<b>Installation af FileZilla</b>	<b>14</b>
<b>13</b>	<b>Discover active systems ping sweep</b>	<b>15</b>
<b>14</b>	<b>Execute nmap TCP and UDP port scan</b>	<b>16</b>
<b>15</b>	<b>Perform nmap OS detection</b>	<b>17</b>
<b>16</b>	<b>Perform nmap service scan</b>	<b>18</b>
<b>17</b>	<b>Find systems with SNMP</b>	<b>19</b>
<b>18</b>	<b>Try Hydra brute force</b>	<b>20</b>
<b>19</b>	<b>Try Cain brute force</b>	<b>21</b>

# Forord

Dette kursusmateriale er beregnet til brug på kurset *Paranoia and government hacking 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 kursusedtagerne et indblik i hvordan Paranoia and government hacking praksis ser ud og opfører sig.

Formålet med workshoppen er at give deltagerne en praktisk erfaring med emnet og information til at implementere i egne miljøer.

## Forudsætninger og ordliste

Dette kursusmateriale forudsætter at deltageren har kendskab til internet og e-mail på brugerniveau. Det betyder at begreber som <http://www.solido.net>, [hk@solido.net](mailto:hk@solido.net) ikke bør være ukendte.

## 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:

- UNIX - herunder Linux, OpenBSD, NetBSD, FreeBSD og Mac OS X
- Microsoft Windows 7 - primært som klientoperativsystem

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

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

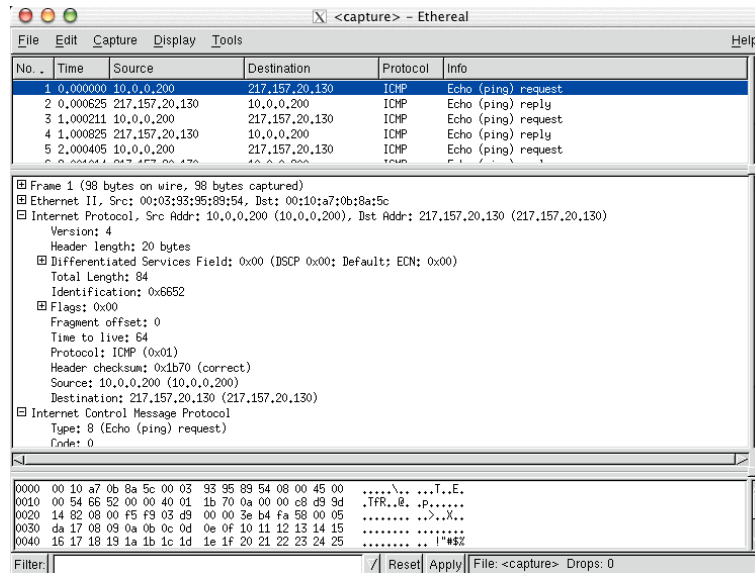
# Indholdet i øvelserne

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

## Wireshark installation



### Objective:

Install the program Wireshark locally on the Windows workstation

### Purpose:

Installing Wireshark will allow you to analyse packets and protocols

### Suggested method:

Download and install the program, either download from web server locally or from <http://www.wireshark.org> Wireshark requires a Windows Capture library to be installed, which is included in the Wireshark installation, but can none the less be downloaded from <http://www.winpcap.org/>

### Hints:

PCAP is a packet capture library allowing you to read packets from the network. Wireshark is a graphical application to allow you to browse through traffic, packets and protocols.

### Solution:

When Wireshark is installed sniff some packets, also see next exercise.

### Discussion:

Wireshark is just an example other packet analyzers exist, some commercial and some open source like Wireshark

## Øvelse 2

# Sniffing network packets

**Objective:**

Sniff packets and dissect them using Wireshark

**Purpose:**

See real network traffic, also know that a lot of information is available and not encrypted.

**Suggested method:**

Open Wireshark and start a capture - either from Windows or BackTrack

Then in another window execute the ping program while sniffing

**Hints:**

When running on Linux the network cards are named eth0 for the first Ethernet and wlan0 for the first Wireless network card. In Windows the names of the network cards are long and if you cannot see which cards to use then try them one by one.

**Solution:**

When you have collected some packets you are done.

**Discussion:** Is it ethical to collect packets from an open wireless network?

## Øvelse 3

# 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:

### Forslag til løsning:

Hent setup programmet 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 indstilling.

Mac brugere kan derefter bruge Safari, mens Windows brugere kan fortsætte med Internet Explorer til NemID/Netbank og sites man stoler på. Jeg stoler ikke selv på NemID og har lavet en virtuel VMware med Ubuntu til dette specifikke formål.

## Øvelse 4

# 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:**

Der findes følgende installationsfiler:

- Thunderbird Setup

**Diskussion:**

Thunderbird anbefales fremfor eksempelvis Outlook og Apple Mail grundet de gode muligheder for udvidelser, herunder GPG 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 GPG.

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



## Øvelse 5

# Installation af GPG GNU Privacy Guard

### THE GNU PRIVACY GUARD

GnuPG is the GNU project's complete and free implementation of the OpenPGP standard as defined by RFC4880. GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications. A wealth of frontend applications and libraries are available. Version 2 of GnuPG also provides support for S/MIME.

GnuPG is Free Software (meaning that it respects your freedom). It can be freely used, modified and distributed under the terms of the GNU General Public License.

GnuPG comes in two flavours: 1.4.15 is the well known and portable standalone version, whereas 2.0.22 is the enhanced and somewhat harder to build version.

Project Gpg4win provides a Windows version of GnuPG. It is nicely integrated into an installer and features several frontends as well as English and German manuals.

Project GPGTools provides a Mac OS X version of GnuPG. It is nicely integrated into an installer and features all required tools.

Project Aegypten developed the S/MIME functionality in GnuPG 2.

### 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 6

# 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 7

# 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 8

# 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 9

# 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 10

# 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 11

# 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 12

# 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:

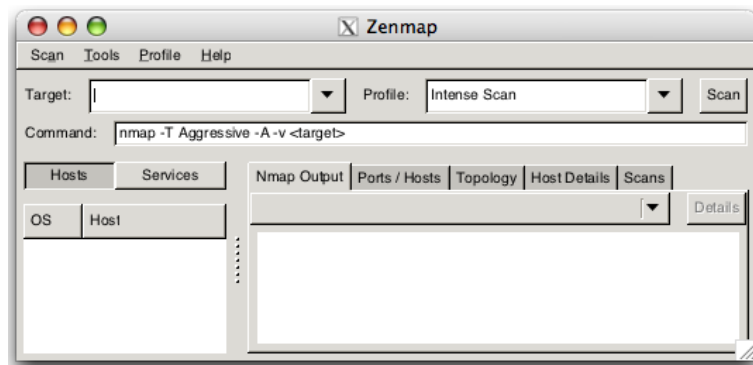
### Diskussion:

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



## Øvelse 13

# Discover active systems ping sweep



### Objective:

Use nmap to discover active systems

### Purpose:

Know how to use nmap to scan networks for active systems.

### Suggested method:

Try different scans,

- Ping sweep to find active systems
- Port sweeps to find active systems with specific ports

### Hints:

Try nmap in sweep mode

### Solution:

Use the command below as examples:

- Ping sweep `nmap -sP 10.0.45.*`
- Port sweeps `nmap -p 80 10.0.45.*`

### Discussion:

**You can also use the graphical interface to nmap called Zenmap.**

## Øvelse 14

# Execute nmap TCP and UDP port scan

**Objective:**

Use nmap to discover open ports on active systems

**Purpose:**

Finding open ports will allow you to find vulnerabilities on these ports.

**Suggested method:**

Use `nmap -p 1-1024 server` to scan the first 1024 TCP ports

Try to use `nmap -sU` to scan using UDP ports, not really possible if a firewall is in place.

If a firewall blocks ICMP you might need to add `-P0` or even `-PN` to make nmap scan even if there are no Ping responses

**Hints:**

Sample command: `nmap -P0 -sU -p1-1024 server` UDP port scanning 1024 ports without doing a Ping first

**Solution:**

Discover some active systems and you are done.

**Discussion:**

There is a lot of documentation about the nmap portscanner, even a book by the author of nmap. Make sure to visit <http://www.nmap.org>

TCP and UDP is very different when scanning. TCP is connection/flow oriented and requires a handshake which is very easy to identify. UDP does not have a handshake and most applications will not respond to probes from nmap. If there is no firewall the operating system will respond to UDP probes on closed ports - and the ones that do not respond must be open.

When doing UDP scan on the internet you will almost never get a response, so you cannot tell open (not responding services) from blocked ports (firewall drop packets). Instead try using specific service programs for the services, sample program could be `nsping` which sends DNS packets, and will often get a response from a DNS server running on UDP port 53.

## Øvelse 15

# Perform nmap OS detection

**Objective:**

Use nmap OS detection and see if you can guess the devices on the network

**Purpose:**

Getting the operating system of a system will allow you to focus your next attacks.

**Suggested method:**

Look at the list of active systems, or do a ping sweep.

Then add the OS detection using the option `-O`

**Hints:**

Use the manual page

The nmap can send a lot of packets that will get different responses, depending on the operating system.

**Solution:**

Use a command like `nmap -O -p1-100 10.0.45.45`

**Discussion:**

nmap OS detection is not a full proof way of knowing the actual operating system, but in most cases it can detect the family and in some cases it can identify the exact patch level of the system.

Another tool which does the same is Xprobe.

## Øvelse 16

# Perform nmap service scan

**Objective:**

Use more advanced features in nmap to discover services.

**Purpose:**

Getting more intimate with the system will allow more precise discovery of the vulnerabilities and also allow you to select the next tools to run.

**Suggested method:**

Use `nmap -A` option for enabling service detection

**Hints:**

Look into the manual page of nmap or the web site book about nmap scanning

**Solution:**

Run nmap and get results.

**Discussion:**

Some services will show software versions allowing an attacker easy lookup at web sites to known vulnerabilities and often exploits that will have a high probability of success.

Make sure you know the difference between a vulnerability which is discovered, but not really there, a false positive, and a vulnerability not found due to limitations in the testing tool/method, a false negative.

A sample false positive might be reporting that a Windows server has a vulnerability that you know only to exist in Unix systems.

## Øvelse 17

# Find systems with SNMP

**Objective:**

Use snmpwalk to research SNMP systems

**Purpose:**

Learn that gathering information can help an attacker.

**Suggested method:**

Log into the Unix server provided and run snmpwalk which is using UDP port 161.

**Hints:**

We are running in a LAN environment with less firewalls, so doing nmap UDP scan is possible.

When discovering an IP then use the snmpwalk program to show a lot of information.

**Solution:**

- Use the command `snmpwalk -v 2c -c public 10.0.45.34 | less`

The command less will show output one screen at a time.

**Discussion:**

In real networks SNMP is being used a lot, but new equipment is starting NOT to allow access using the community string public.

## Øvelse 18

# Try Hydra brute force

**Objective:**

Try a brute force program named hydra/Xhydra

**Purpose:**

Learn that some protocols allow brute forcing.

**Suggested method:**

Log into the Unix server or use the BackTrack.

Make a short list of usernames and a short list of passwords and use hydra to brute force your way into a system. Use the editor kate, using `kate users.txt` and `kate pass.txt` followed by a command similar to this:

```
$ hydra -V -t 1 -L users.txt -P pass.txt 10.0.45.2 ssh
```

**Hints:**

When learning tools create a nice environment and check that things are working before trying to hack. So with brute forcing an account, create and test it!

**Solution:**

There is an FTP server with an easy to guess administrator password.

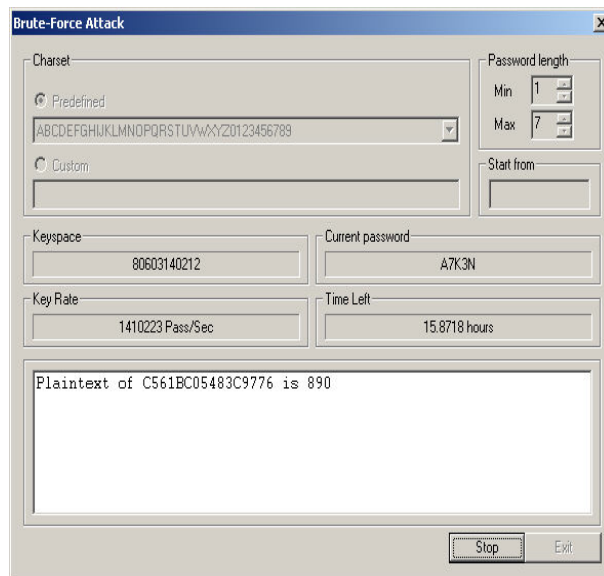
**Discussion:**

The hydra program can brute force a lot of different protocols and also allow a lot of tuning.

The hydra program does an online brute force attack, in some cases you can get access to data like password databases, or hash values that can be cracked in off-line brute force attacks.

## Øvelse 19

# Try Cain brute force



### Objective:

Try a brute force program named Cain

### Purpose:

Learn that some algorithms allow for easier brute forcing.

### Suggested method:

Download and install the Windows program Cain

Then try cracking some local accounts, access to hash is only allowed if you are administrator.

### Hints:

When learning tools create a nice environment and check that things are working before trying to hack. So with Cain use a system where you are administrator and crack local accounts.

Then later get hash values from real systems, or by doing google searches.

### Solution:

See that some algorithm can do 100.000s keys/second and others only allow 100s keys/second.

### Discussion:

Cain is built for cracking passwords in off-line brute force attacks, but also includes other features like sniffing.