

Welcome to

# Internet Self Defense

Protect yourself peacefully

Henrik Lund Kramshøj, internet samurai  
[hlk@solido.net](mailto:hlk@solido.net)

<http://www.solidonetworks.com>

# Kontaktinformation og profil



- Henrik Lund Kramshøj, IT-sikkerhed og internet samurai
- Email: [hlk@solido.net](mailto:hlk@solido.net)      Mobil: +45 2026 6000
- Cand.scient fra Datalogisk Institut ved Københavns Universitet, DIKU
- CISSP certificeret
- 2003 - 2010 Selvstændig sikkerhedskonsulent
- 2010 Stifter og partner i Solido Networks ApS

## Del 1: Beskyt dig selv

- Kl 10:00-12:30
- Mindre foredrag mere workshop
- Mindre enetale, mere interaktion

## Del 2: Hacking, Hackerværktøjer, undersøg sikkerhed

- Kl 13:00-16:30
- Mindre foredrag mere workshop
- Mindre enetale, mere interaktion

Send gerne spørgsmål senere

Et demokrati fordrer borgere med frihed som har evnen til at tage beslutninger, som ikke skal være bange for overvågning.

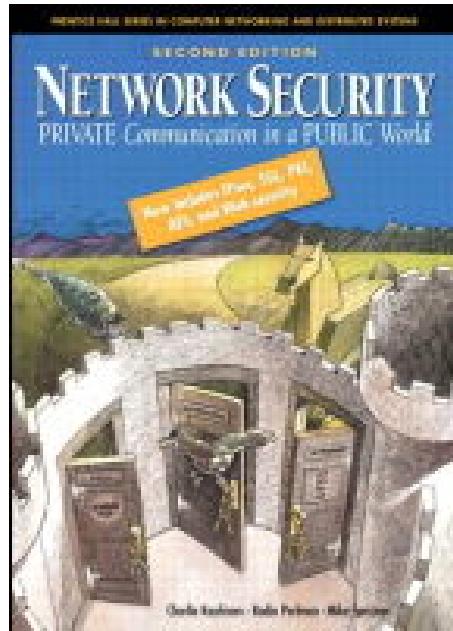
Et demokrati fordrer borgere som aktivt vælger hvornår de afgiver personlige data om deres liv og færdens.

Kryptografi er en fredelig protest mod indsamling af data som misbruges enten til kriminelle formål, kommercielle formål eller under dække af beskyttelse mod terror, ekstremisme, nazisme, misbrug af børn, ... Le mal du jour / dagens onde.

## Du bestemmer - det er demokrati

Derudover stalking, ekskærester, arbejdsgivere, forældre, ...

Hvor skal vi nu starte denne rejse?



## Private Communications in an Public World

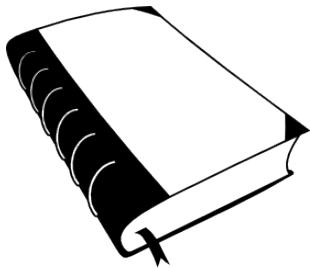
Anbefalelsesværdig bog som gennemgår grundlaget for kryptering, teknikker og protokollerne der bruges på internet idag, herunder: IPsec, SSL/TLS, PGP, PKI, AES m.fl.



Vores data er overalt

Vi er afhængige af computere Vi er afhængige af netværk

Vi er afhængige af andres computere - servere og services



Free graphics by Lumen Design Studio

Dette materiale består af flere dele:

- Kursusmaterialet - præsentationen til undervisning - dette sæt
- Øvelseshæfte med øvelser
- Hertil kommer diverse ressourcer fra internet

Øvelserne er valgfrie ☺

# Why think of security?



Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world. A Cypherpunk's Manifesto by Eric Hughes, 1993

Copied from <https://cryptoparty.org/wiki/CryptoParty>



## Don't Panic!

Hacking betyder idag indbrud, kriminalitet, hærværk m.v.

Oprindeligt betød hacking at man udforskede, undersøgte, involverede sig

Vi skal bruge ånden fra hacking til forskning, udvikling

Mange regler om at man ikke må noget er imod hacking.

Lad være med at bryde love, men bøj gerne regler ☺



- Nmap, Nping - tester porte, godt til firewall admins <http://nmap.org>
- Metasploit Framework gratis på <http://www.metasploit.com/>
- Wireshark avanceret netværkssniffer - <http://www.wireshark.org/>
- Burpsuite <http://portswigger.net/burp/>
- Skipfish <http://code.google.com/p/skipfish/>
- OpenBSD operativsystem med fokus på sikkerhed <http://www.openbsd.org>
- Metasploit Pro fra <http://www.rapid7.com>

Kilde: Angelina Jolie fra Hackers 1995



BackTrack er baseret på Linux og må kopieres frit :-)

<http://www.backtrack-linux.org/>

Wireshark - <http://www.wireshark.org>

Er det fornuftigt at man kan hente dem?

hacking backtrack – YouTube  
[http://www.youtube.com/results?search\\_query=hacking%20backtrack](http://www.youtube.com/results?search_query=hacking%20backtrack) DuckDuckGo

YouTube hacking backtrack Search results for **hacking backtrack** About 6,650 results

Filter ▾ Sort by: Relevance ▾

**IEFD Ep. 12 - Hacking Basics - Backtrack Part 1**  
On the forums, there has been many questions concerning **Backtrack**. Therefore, we decided to make a video that tries to answer as many as these ...  
by Gregorpm | 4 years ago | 155,410 views

**Security Awareness - Hacking Windows 7 with BackTrack 4....**  
This short tutorial provides an insight into network security and how quickly and easily a windows 7 machine can be compromised with a small ...  
HD by eastmidlandsit | 1 year ago | 12,188 views

**Facebook Hacking with BackTrack 5**  
Facebook **Hacking** with **BackTrack** 5 Sorry guys, i had to open a new account again as my older account was banned by youtube due to various **hacking** ...  
by MauritianHacker | 6 months ago | 68,523 views

**Hacking - BackTrack 4 Linux / VMware - For Beginners**  
View in HD and Fullscreen!! In this video I explain how to download **BackTrack** Linux 4 R2, and VMware. This video is for beginners. To Download ...  
HD by Raventattoo | 11 months ago | 7,407 views

**How to Hack (BackTrack & VMware Player)**  
"What will happen if my child becomes a **Hacker**?" Maybe what you should really be asking yourself is, "What if my child does not become a **Hacker** ...  
by J2897Tutorials | 2 years ago | 33,394 views

Featured Videos

**Cracking Router Logins**  
Attacking router logins If you like it, comment.  
by linuxstyles | 61,526 views

**How to Hack Free Int...**  
THIS IS LINUX Wanna hack the router login after u hack t...  
by theorignalfatdonkey | 46,749 views

**How To Hack Wireles...**  
This is very easy(Noob-Friendly) yet detailed tutorial on how to ha...  
by mushroomHEADBANGERS | 151,490 views

**Linux / Win7 - VMWar...**  
pc-addicts.com - 1of2 - I briefly demonstrate how to use a Linksys USB...  
by PCAddictsLive | 12,071 views

Botnets spreder sig ved at inficere så mange systemer som muligt

Botnets idag vokser gerne langsommere - ingen ny Code Red hastighedsrekord

Spreder sig via SMTP, HTTP, SMB, ... alle protokoller der kan overføre data

Bannerkampagner og 3. parts kilder til elementer på din side?!

Når først der er kommet malware på systemet udvides med moduler

Malware idag er sofistikeret

Modulært opbygget

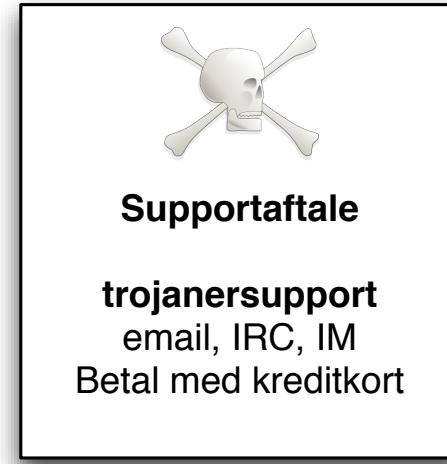
Benytter stærk kryptering til at sikre administrationen af inficerede computere

Benytter seneste sikkerhedshuller - 0 days til at sprede sig

Benytter de seneste rootkit metoder til at holde sig skjult

Muterer efter alle kendte metoder for at undgå opdagelse

Larmer mindre end tidligere



Malware programmører har lært kundepleje

"Køb denne version og få gratis opdateringer"

Lej vores botnet med 100.000 computere

# Phishing - Receipt for Your Payment to mark561@bt....com



Mark Willson  
145 Church Lane East  
Aldershot, Hampshire, GU11 3ST  
United Kingdom

Important Note: Mark Willson has provided an Unconfirmed Address. If you are planning on shipping items to Mark Willson, please check the Transaction Details page of this payment to find out whether you will be covered by the PayPal Seller Protection Policy.

Note:

If you haven't authorized this charge ,click the link below to cancel transaction

Cancel Transaction:

[https://www.paypal.com/cgi-bin/webscr/cgi-bin/webscr?login-run.websrcmd=\\_account-run.CaseIDNumberPP-046-631-789](https://www.paypal.com/cgi-bin/webscr/cgi-bin/webscr?login-run.websrcmd=_account-run.CaseIDNumberPP-046-631-789)

\*SSL connection:

PayPal automatically encrypts your confidential information in transit from your computer to ours using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available)

[http://paypal-co.uk.dt6.pl/?login-run.websrcmd=\\_account-run.CaseIDNumberPP-046-631-789](http://paypal-co.uk.dt6.pl/?login-run.websrcmd=_account-run.CaseIDNumberPP-046-631-789)

## Kan du selv genkende Phishing

# Zip files?

zspam — hlk@kramse.dk (473 unread)

Entire Message

474 messages

	From	Subject	Date Received
●	maynard stipek	Experience convenient online shopping ...	Today 2.24
●	Merrill H. Schumacher	online Pharmcy..ADIPEX,SOMA,etc !!	Today 2.52
●	Forest Salgado	Critical Service Pack 2 update . March 10th	Today 4.00
●	Vanessa J. Smith	Windows XP + Office XP = \$89.95	Today 6.19
●	Norah Kelley	Sale on All AutoCAD software	Today 6.55
●	Heidi Forbes	Better than Viagra	Today 7.25
●	<a href="#">randi@indocrafts.com</a>	Re: Delivery Protection	Today 8.41
●	<a href="#">km@roval-photo.dk</a>	Mail Delivery failure hlk@kramse.dk	Today 8.43

From: [randi@indocrafts.com](mailto:randi@indocrafts.com)  
Date: 14. marts 2005 19.23.01 MET  
To: [hlk@kramse.dk](mailto:hlk@kramse.dk)  
Subject: Re: Delivery Protection

Protected message is attached.

 message.zip (39.9 KB)

In (63 unread)

Entire Message

From	Subject	Date Received
Charlie Root	betty.kramse.dk daily output	14. marts 2005 1.37
Charlie Root	betty.kramse.dk daily insecurity output	14. marts 2005 1.37
Henrik Root	phoenix.devoteam.dk daily output	14. marts 2005 1.43
Charlie Root	betty.kramse.dk weekly output	12. marts 2005 3.37
Henrik Root	phoenix.devoteam.dk weekly output	12. marts 2005 3.43
Qualys, Inc.	@RISK: The Consensus Security Vulnerability Alert - Week 10 2005	12. marts 2005 3.15
Washington Mutual Online Banking	Confirm Your Washington Mutual Online Banking	12. marts 2005 2.21

From: Washington Mutual Online Banking <personalbanking@erms-02.wamu.com>  
Subject: Confirm Your Washington Mutual Online Banking  
Date: 12. marts 2005 2.19.18 MET  
To: hlk@kramse.dk

wamu.com A Washington Mutual, Inc. Web site Customer Service Contact Us Locations

Dear Washington Mutual customer,

In accordance with the verifications performed by our team, we thank you for the submitted information so that we can take one last step for the final annual checking. Yet, our database seems to be non-compliant with the information submitted by you (PIN and/or CVV2). Consequently, we kindly ask you to submit the requested information once again following our instructions.



[Explanation](#)

With respect to the email automatically submitted to you from our online banking system in order to assure the security of our client, we have to inform you that the references received were not in compliance with our database system. Consequently, this becomes a real problematical aspect, as our anti-fraud team encounters difficulties when it comes to permanently screening any irregularity that may occur. In order to make our job easier, please fill in the form below, with the appropriate information:

<https://login.personal.wamu.com/registration/CreateLogonEntry.asp>

If you believe you have provided personal or account information in response to a fraudulent e-mail or Web site, please contact Washington Mutual at 800.788.7000 and contact the other financial institutions with which you have accounts

Thank you for trusting our services.

zspam — hlk@kramse.dk (464 unread)

Entire Message

474 messages

From	Subject	Date Received
hlk@kramse.dk	Mail Delivery (failure hlk@kramse.dk)	3/3-2005 10.50
viba@fa.dk	Mail Delivery (failure hlk@kramse.dk)	3/3-2005 21.23
Larry Martin	Institutions are buying Homeland Security,, ...	4/3-2005 5.37
info@opinionsland.co	Re: your data	4/3-2005 10.02
peter@bluesky.se	Mail Delivery (failure hlk@kramse.dk)	4/3-2005 10.02
everett wetterer	Quality meds without any hassel headquarter	4/3-2005 2.19
Jodie Harding	Protect your children	6/3-2005 16.10
Brandi Dutton	Re: susceptance baud where hines ideology	6/3-2005 6.50

From: [info@opinionsland.co](mailto:info@opinionsland.co)  
Date: 4. marts 2005 10.02.43 MET  
To: [hlk@kramse.dk](mailto:hlk@kramse.dk)  
Subject: Re: your data

Please read the important document.

  
[data.scr \(28,9 KB\)](#)

## SCR er screensaver files - programmer

## The Mobile Network in 2010 and 2011

Global mobile data traffic grew 2.6-fold in 2010, nearly tripling for the third year in a row. The 2010 mobile data traffic growth rate was higher than anticipated. Last year's forecast projected that the growth rate would be 149 percent. This year's estimate is that global mobile data traffic grew 159 percent in 2010.

...

Last year's mobile data traffic was three times the size of the entire global Internet in 2000. Global mobile data traffic in 2010 (237 petabytes per month) was over three times greater than the total global Internet traffic in 2000 (75 petabytes per month).

...

There will be 788 million mobile-only Internet users by 2015. The mobile-only Internet population will grow 56-fold from 14 million at the end of 2010 to 788 million by the end of 2015.

Kilde: *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010 - 2015*

## Hvad kendetegner håndholdte enheder

- små - kan typisk ligge i en lomme
- meget lille lager til rådighed
- Begrænset processorkapacitet
- begrænset funktionalitet
- kan synkroniseres med en stationær computer ■
- meget stor lagerkapacitet i moderne udgaver!
- udvidet funktionalitet
- *viewer programmer* til Word, Excel, PDF m.fl.
- alt er forbundet idag, typisk netværk uover GPRS/telefoni

Brug teknologien

Lær teknologien at kende - læs manualen!

Tænk på følsomheden af data I gemmer og overfører

- Slå ting fra som I ikke bruger
- Slå bluetooth fra når I ikke bruger den
- Opdater softwaren på enheden
- Slå kryptering til hvor I kan: IMAPS, POP3S, HTTPS og over bluetooth
- Brug låsekode fremfor tastaturlås uden kode på mobiltelefonen
- Stol ikke for meget på fingertryksaflæsere

Gælder alle enheder og steder I gemmer data

Kryptografi - brug så vidt muligt kryptering og kryptoværktøjer

Sikre protokoller - som ofte bruger kryptering

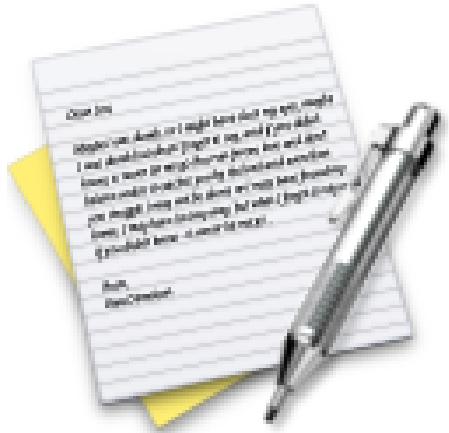
Backup - jævnligt

Tal frit

Lær og lær fra dig

Følg med i nyhederne

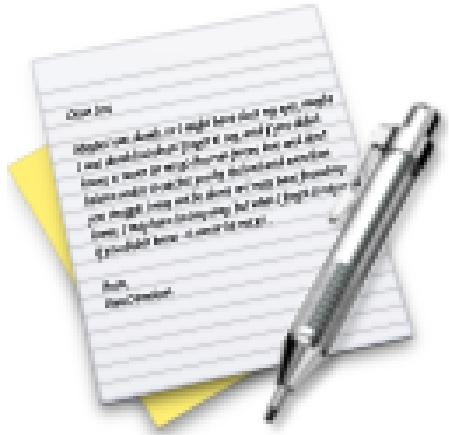




Vi laver nu øvelsen

## Installation af alternativ browser

som er øvelse **1** fra øvelseshæftet.



# Vi laver nu øvelsen

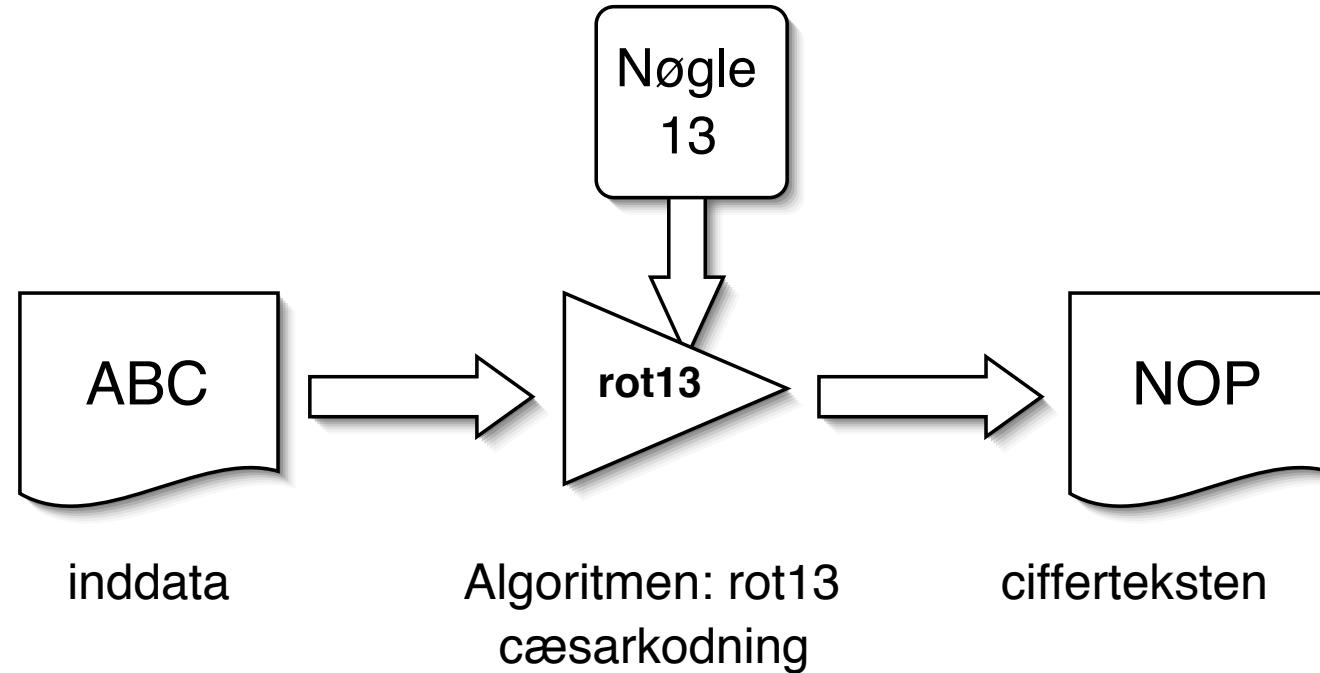
# Installation af Thunderbird

som er øvelse 2 fra øvelseshæftet.

Er det tid til en lille pause?

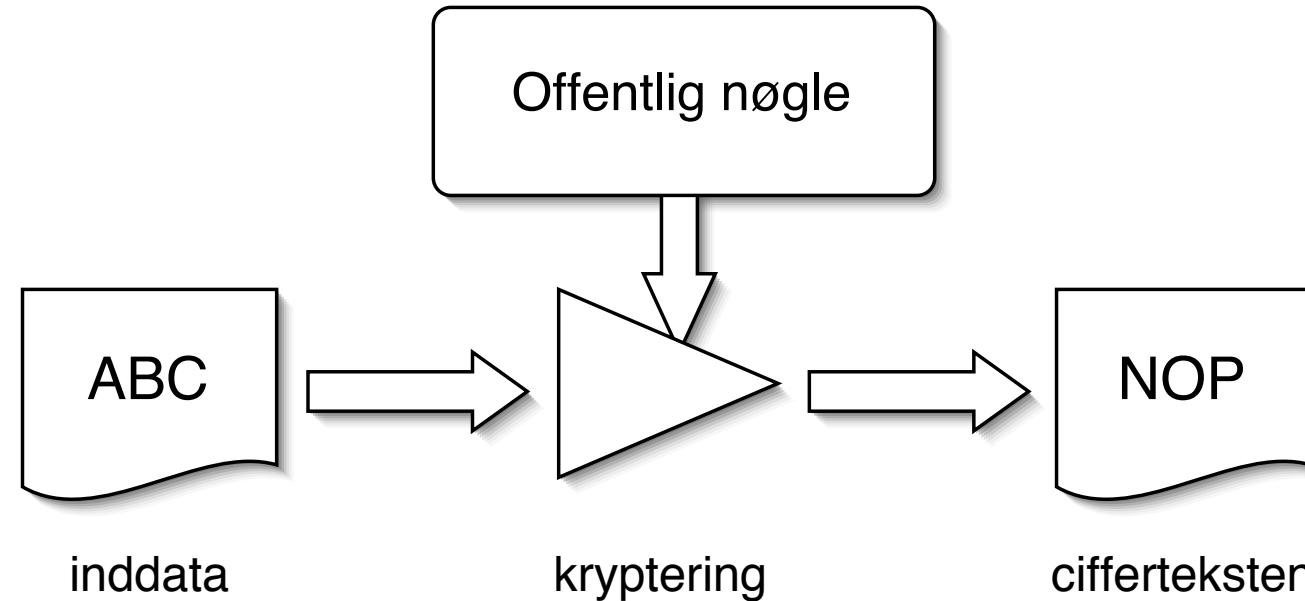


Vi vil nu snakke overordnet om kryptering - uden matematik ☺



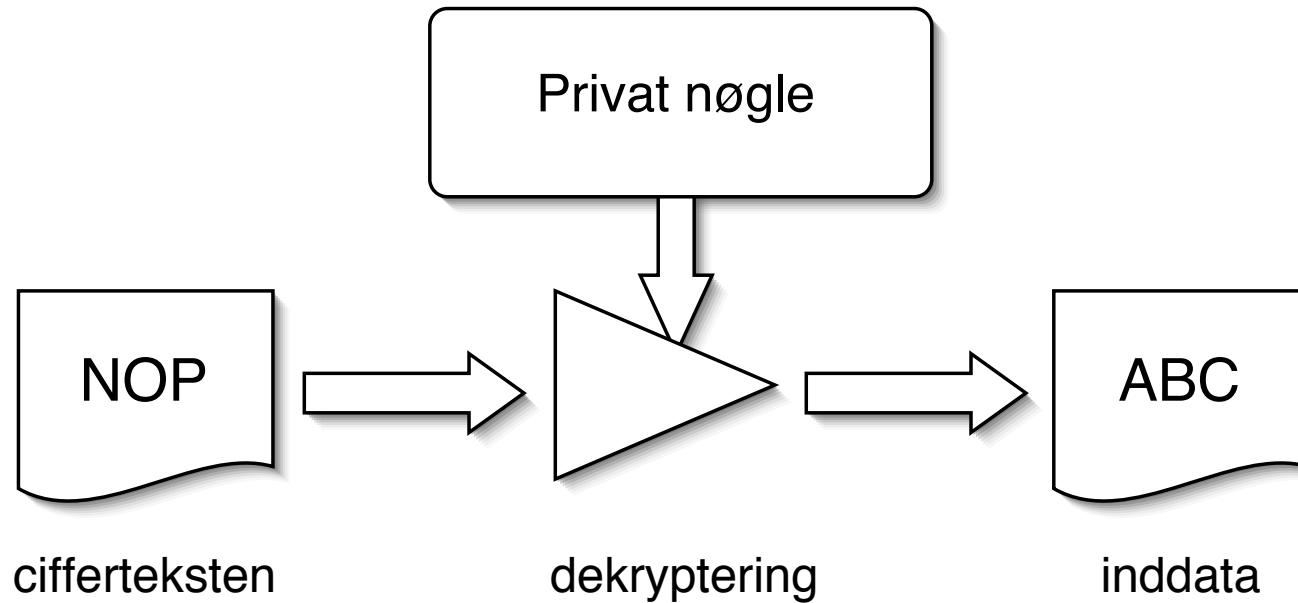
Kryptografi er læren om, hvordan man kan kryptere data

Kryptografi benytter algoritmer som sammen med nøgler giver en ciffertekst - der kun kan læses ved hjælp af den tilhørende nøgle



privat-nøgle kryptografi (eksempelvis AES) benyttes den samme nøgle til kryptering og dekryptering

offentlig-nøgle kryptografi (eksempelvis RSA) benytter to separate nøgler til kryptering og dekryptering



offentlig-nøgle kryptografi (eksempelvis RSA) bruger den private nøgle til at dekryptere man kan ligeledes bruge offentlig-nøgle kryptografi til at signere dokumenter - som så verificeres med den offentlige nøgle

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

Et successfult angreb på en krypto-algoritme er enhver genvej som kræver mindre arbejde end en gennemgang af alle nøglerne

Nye algoritmer, programmer, protokoller m.v. skal gennemgås nøje!

Se evt. Snake Oil Warning Signs: Encryption Software to Avoid

<http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>

Formålet med kryptering

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

## AES

---

Advanced Encryption Standard

DES kryptering baseret på den IBM udviklede Lucifer algoritme har været benyttet gennem mange år.

Der er vedtaget en ny standard algoritme Advanced Encryption Standard (AES) som afløser Data Encryption Standard (DES)

Algoritmen hedder Rijndael og er udviklet af Joan Daemen og Vincent Rijmen.

[http://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)  
<http://csrc.nist.gov/encryption/aes/>

NIST announced a public competition in a Federal Register Notice on November 2, 2007 to develop a new cryptographic hash algorithm called SHA-3. The competition is NIST's response to advances made in the cryptanalysis of hash algorithms.

...

Based on the public comments and internal review of the candidates, NIST announced **Keccak** as the winner of the SHA-3 Cryptographic Hash Algorithm Competition on October 2, 2012, and ended the five-year competition.

<http://csrc.nist.gov/groups/ST/hash/sha-3/index.html>

## Kryptering af e-mail

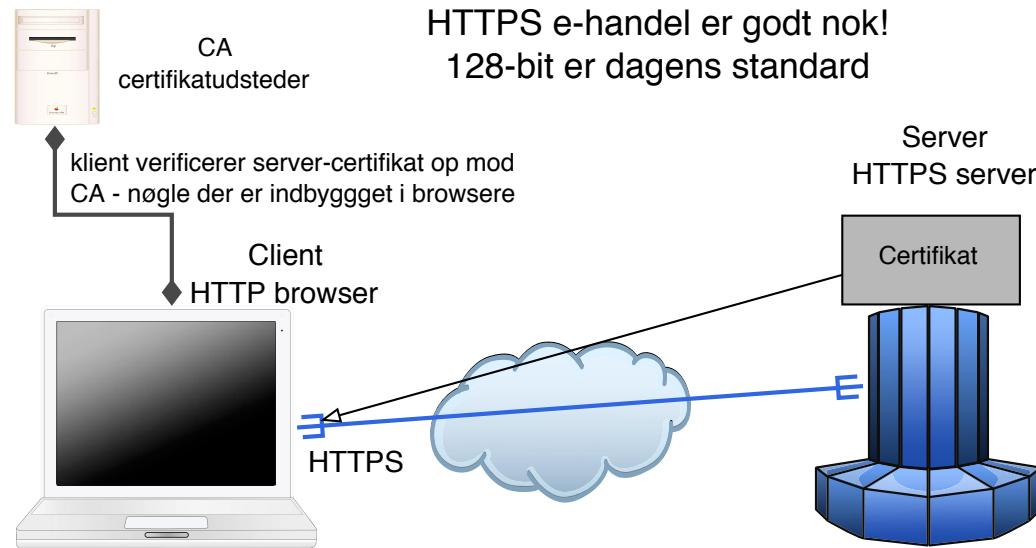
- Pretty Good Privacy - Phil Zimmermann
- PGP = mail sikkerhed

## Kryptering af sessioner SSL/TLS

- Secure Sockets Layer SSL / Transport Layer Services TLS
- krypterer data der sendes mellem webservere og klienter
- SSL kan bruges generelt til mange typer sessioner, eksempelvis POP3S, IMAPS, SSH m.fl.

## Kryptering af netværkstrafik - Virtual Private Networks VPN

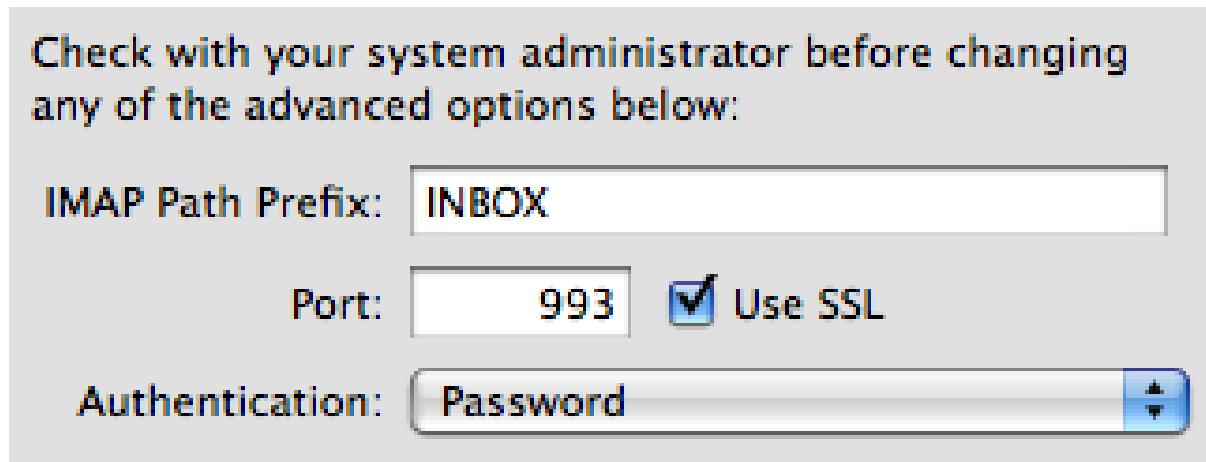
- VPN **IPsec IP Security Framework**, se også L2TP
- VPN **PPTP Point to Point Tunneling Protocol** - dårlig og usikker, brug den ikke mere!
- SSL VPN, OpenVPN m.fl.



Oprindeligt udviklet af Netscape Communications Inc.

Secure Sockets Layer SSL er idag blevet adopteret af IETF og kaldes derfor også for Transport Layer Security TLS. TLS er baseret på SSL Version 3.0.

RFC-2246 The TLS Protocol Version 1.0 fra Januar 1999



Mange protokoller findes i udgaver hvor der benyttes SSL

HTTPS vs HTTP

IMAPS, POP3S, osv.

Bemærk: nogle protokoller benytter to porte IMAP 143/tcp vs IMAPS 993/tcp

Andre benytter den samme port men en kommando som starter:

SMTP STARTTLS RFC-3207



## Hvad er Secure Shell SSH?

Oprindeligt udviklet af **Tatu Ylönen** i Finland,  
se <http://www.ssh.com>

SSH afløser en række protokoller som er usikre:

- Telnet til terminal adgang
- r\* programmerne, rsh, rcp, rlogin, ...
- FTP med brugerid/password

Når vi skal hente post sker det typisk med POP3 eller IMAP

- POP3 Post Office Protocol version 3 RFC-1939
- Internet Message Access Protocol (typisk IMAPv4) RFC-3501

Forskellen mellem de to er at man typisk med POP3 henter posten, hvor man med IMAP lader den ligge på serveren

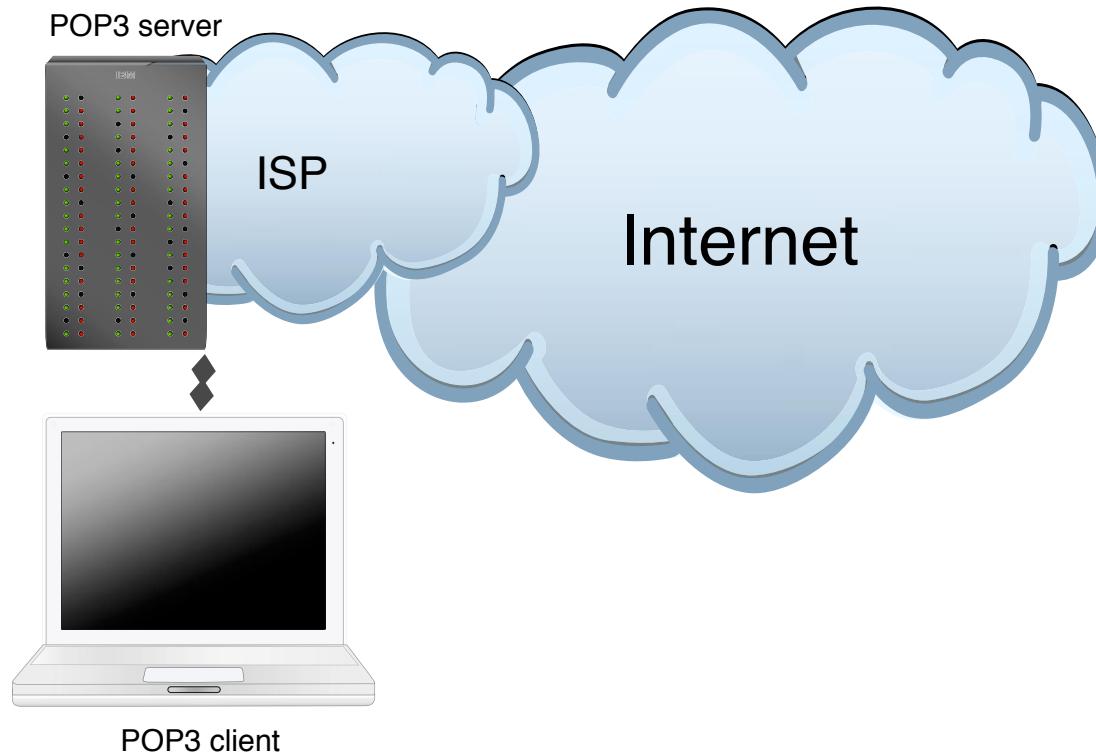
POP3 er bedst hvis kun en klient skal hente

IMAP er bedst hvis du vil tilgå din post fra flere systemer

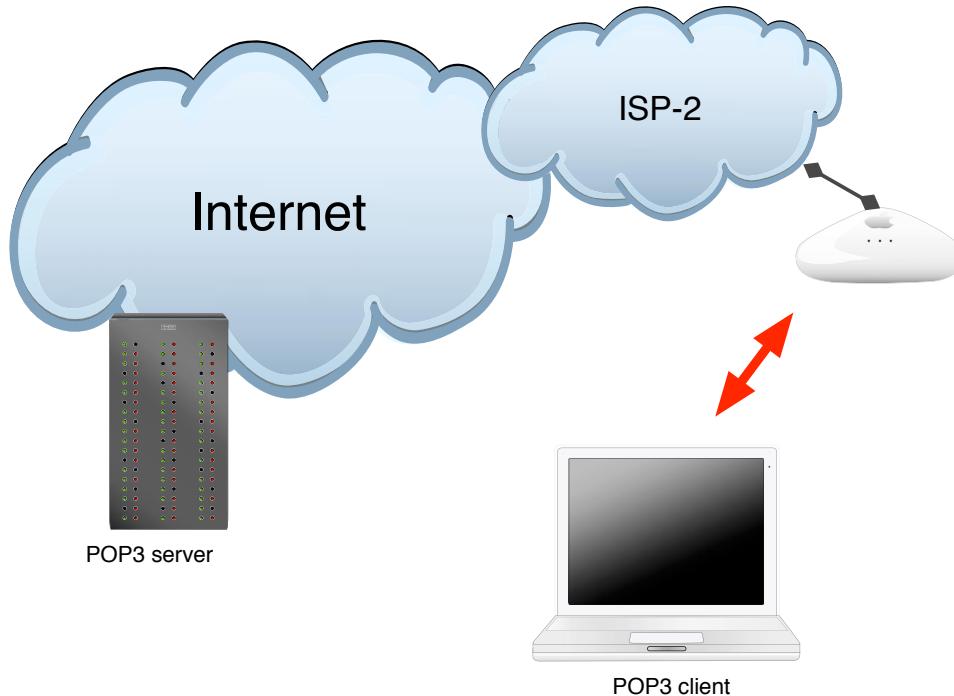
Jeg bruger selv IMAPS, IMAP over SSL kryptering - idet kodeord ellers sendes i klartekst

SMTP bruges til at sende mail mellem servere

POP3 sender brugernavn og kodeord i klartekst - ligesom FTP  
bruges dagligt af næsten alle privatkunder  
alle internetudbydere og postudbydere tilbyder POP3  
der findes en variant, POP3 over SSL/TLS



Man har tillid til sin ISP - der administrerer såvel net som server



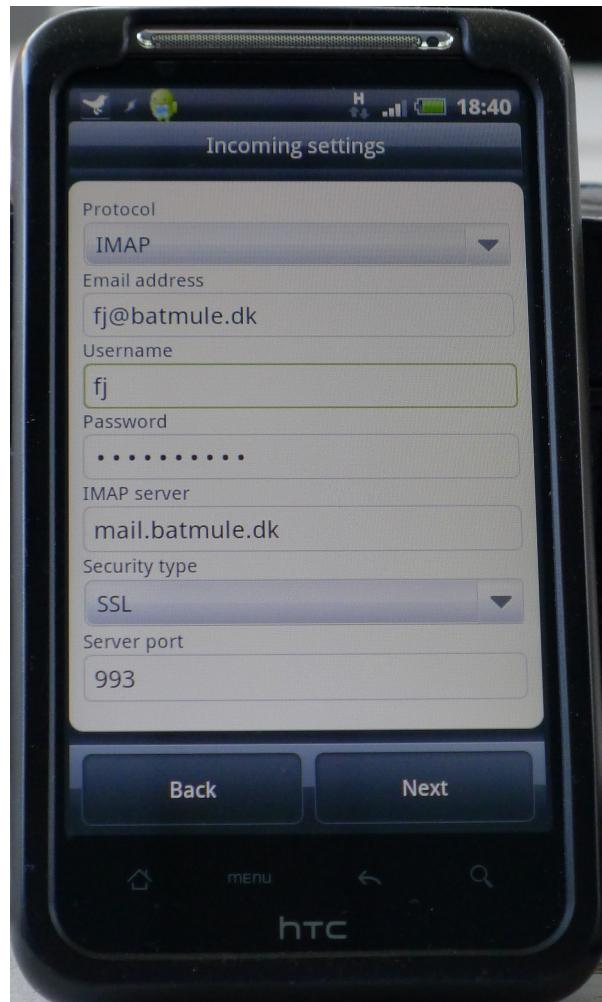
Har man tillid til andre ISP'er? Alle ISP'er?

Deler man et netværksmedium med andre?

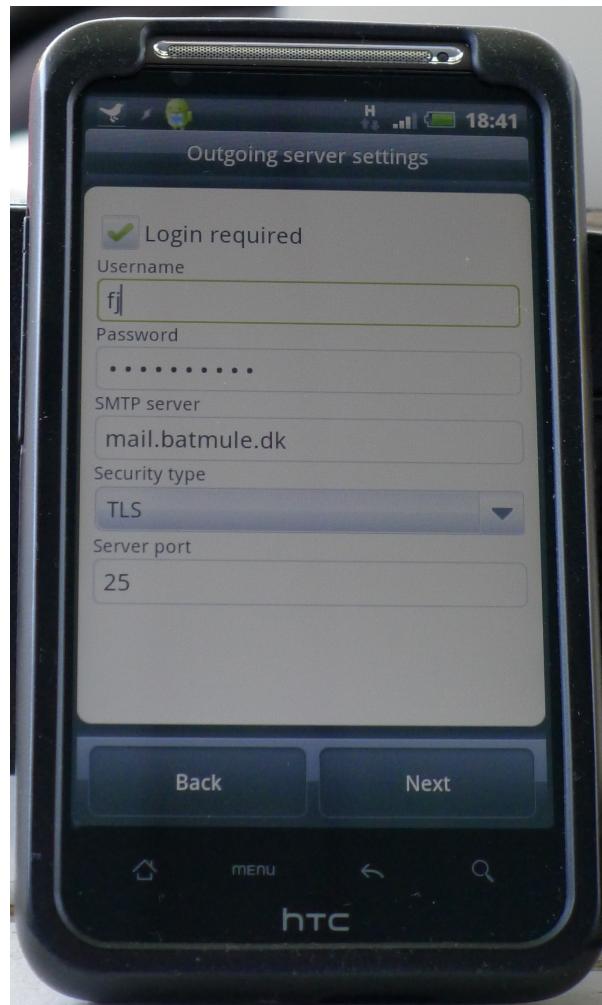
Brug de rigtige protokoller!

Brug de krypterede udgaver af protokollerne

Istedet for POP3 brug POP3s, Istedet for IMAP brug IMAPs



SMTP kan erstattes med SMTP+TLS





Vi laver nu øvelsen

## Installation af Thunderbird

som er øvelse **2** fra øvelseshæftet.



Vi laver nu øvelsen

## Installation af GPG GNU Privacy Guard

som er øvelse **3** fra øvelseshæftet.



Vi laver nu øvelsen

## Installation af Enigmail plugin

som er øvelse **4** fra øvelseshæftet.

The 'S' in HTTPS stands for 'secure' and the security is provided by SSL/TLS. SSL/TLS is a standard network protocol which is implemented in every browser and web server to provide confidentiality and integrity for HTTPS traffic.

Nu vi snakker om kryptering - SSL overalt?

Kan vi klare det på vores servere? ■

Google kan:

<http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html>

Men alt for få gør det

■ Næste spørgsmål er så hvilke rod-certifikater man stoler på ...

# Kryptering step 2 - data at rest

Mange glemmer at låse bilen når de skal hente børn - travlhed

Mange lader deres baggage være ubevogtet i lufthavnen - sult tørst

Mange lader deres bærbare stå på kontoret - frit fremme

Mange forlader deres bærbare på et bord under konferencer

... simpelt tyveri er ofte muligt

eller er det industrispionage?

Et laboris cillum. Tia non  
ob ea soluad inco. quae egen ium im<sup>per</sup> end. Officia deserunt mollit a<sup>et</sup> orum Et  
harumd dereud fac<sup>er</sup> expedit distinct. Gothicā quam nunc putamus parum<sup>us</sup> aposuerit  
litterarum formas humanitatis per seacula quarta; modo typi is videntur parum clari flant  
sollemnes in futurum; litterarum f<sup>ac</sup> humanitatis per seac<sup>ula</sup> cima et quinta decima, modo typi  
qui nu<sup>tur</sup> parur sollemnes in futuru rit ! Nam liber te conscient to factor  
tum p<sup>ro</sup> ioque civi eque pecun moc honor et imper r et,  
conse<sup>ting</sup> elit, seu ut dolore magna aliquam is nostrud exercitatio lo  
conse<sup>te</sup> :e in voluptate ve<sup>rit</sup> esse cillum dolore eu fugiat nulla pariatur. At vver e am  
dignissum qui blandit est praesent.

# Stjålet laptop

## Slittede eller ødelagte data

- og hvordan sletter man data? Huskede du mini SD kortet med dine private billeder?

## Kom igang!

- Skriv på DVD - DVD brændere i mange laptops idag
- Gem på netværket - Dropbox, husk en yderligere backup!
- Brug Duplicity på egen server, eller tilsvarende services

Mat Honan epic hacking :-(

<http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/>

## What is it?

Duplicity backs directories by producing encrypted tar-format volumes and uploading them to a remote or local file server. Because duplicity uses librsync, the incremental archives are space efficient and only record the parts of files that have changed since the last backup. Because duplicity uses **GnuPG** to encrypt and/or sign these archives, they will be safe from spying and/or modification by the server.

<http://duplicity.nongnu.org/> duplicity home page

<http://www.gnupg.org/> The GNU Privacy Guard

## The 5<sup>th</sup> Wave

By Rich Tennant



**"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."**



## Kryptering findes i alle de gængse klient operativsystemer

- Microsoft Windows Bitlocker - kryptering af disken Ultimate eller Enterprise
- Apple Mac OS X - krypterer nemt med FileVault og FileVault2
- FreeBSD GEOM og GBDE - giver mulighed for at kryptere enheder generelt
- PGP disk - Pretty Good Privacy - laver en virtuel krypteret disk
- Truecrypt <http://www.truecrypt.org/>
- Nogle producenter har kodeord på disken - IBM harddisk BIOS kodeord

Hvad man vælger afhænger af operativsystemet og pengepungen

Tvind brugte Safeguard Easy fra det tyske firma Utimaco

Politiet *knækkede* harddiskene ved brug af kodeord som de enten gættede eller fik - ikke selve krypteringen

**En god algoritme i et godt produkt med en god nøgle kan ikke brydes**

<http://www.sophos.com/en-us/products/encryption/safeguard-privatecrypto.aspx>



Vi laver nu øvelsen

## Installation af Truecrypt

som er øvelse **5** fra øvelseshæftet.

# Kryptering step 3 - email data in transit



Selvom du kommunikerer sikkert med din mail server sendes email som postkort over internet.

En måde at beskytte data er at bruge PGP, pretty good privacy



- Pretty Good Privacy - PGP
- Oprindeligt udviklet af Phil Zimmermann
- nu kommersielt, men der findes altid en freeware version <http://www.pgp.com>
- Eksporteret fra USA på papir og scannet igen - det var lovligt
- I dag kan en masse information om PGP findes gennem: <http://www.pgpi.org>



Gnu Privacy Guard, forkortes GnuPG eller GPG

brug linket: <http://www.gnupg.org/>

Open Source med GPL licens.

Kan bruges på alle de gængse operativsystemer

```
$ cd /userdata/download/src/postfix/  
$ ls -l *.sig  
-rw-r--r-- 1 hlk admin 152 13 Sep 2003 postfix-2.0.16.tar.gz.sig  
-rw-r--r-- 1 hlk admin 152  3 May 13:34 postfix-2.1.1.tar.gz.sig  
$ gpg --verify postfix-2.1.1.tar.gz.sig  
gpg: Signature made Mon May  3 19:34:08 2004 CEST using RSA key ID D5327CB9  
gpg: Good signature from "wietse venema <wietse@porcupine.org>"  
gpg:                               aka "wietse venema <wietse@wzv.win.tue.nl>"  
$
```

**Det er nødvendigt at verificere arkiver med kildekode!**

## Generering af key

```
$ gpg --gen-key
```

- Vælg "DSA and Elgamal"
- Vælg passende keysize - 4096 skader næppe
- Vælg passende udløbsdato - "no expire" vil virke for de fleste
- Brug din officielle mailadresse i forbindelse med dit navn, så Email klienter kan finde din key automatisk
- Brug en god passphrase.  
En lang sætning som du kan huske, og som ikke kan gættes udfra kendskab til dig.
- Når nøglen genereres, så hjælp med at generere "randomness" i systemet. Det får genereringen til at gå hurtigere, og det giver en bedre key.

samme spørgsmål i GUI programmerne, **og husk at lave et revoke certifikat!**

Du har nu en GnuPG key klar til at blive signeret

Er du **sikker** på at du kan huske din passphrase?

Når nøglen er genereret bliver der vist et kort sammendrag af indholdet  
Dette *fingerprint* kan også fås frem med:

```
$ gpg --fingerprint addr@domain.dk
pub 1024D/D1EFBA6 2003-01-20
      Key fingerprint = OFAE F19D DB46 DF2E D93D  9B05 21A6 469B D1EF BAA6
uid                         Henrik Lund Kramshoej (work email) <hlk@security6.net>
uid                         Henrik Lund Kramshoej (Kramse) <hlk@kramse.dk>
uid                         [jpeg image of size 14412]
sub 2048g/6D08E6E6 2003-01-20
```

Vi sætter defaults der sikrer:

- Ingen brok over usikker brug af hukommelsen (at låse sider kræver root, dvs. SUID på UNIX)
- Valg af default keyserver
- Valg af default key (hvis du har flere)
- Valg af karaktersæt

```
$ tail ~/.gnupg/gpg.conf
no-secmem-warning
keyserver hkp://pgp.mit.edu/
default-key D1EFBAA6
charset ISO-8859-1
```

Det gör livet lidt lettere

# Upload af keys

For at andre kan signere din key skal de have en kopi af din publickey.

Dette kan enten gøres ved at du eksporterer den til en fil og sender filen via Email, diskette, scp, USBkey, etc.:

```
gpg -a --export addr@domain.dk
```

Eller det kan gøres ved at den uploads til keyserverne, hvorfra alle kan hente den:

```
gpg --send-keys 47A33XXX
```

## Download af keys

Download kan enten foretages via en webside med søgemuligheder

<http://pgp.mit.edu/>

Herfra kan en publickey gemmes i en fil, og importeres med:

```
gpg --import FILE
```

Download kan også foretages direkte hvis keyid kendes:

```
gpg --recv-keys DC9C7XXX
```

Keys signeres med:

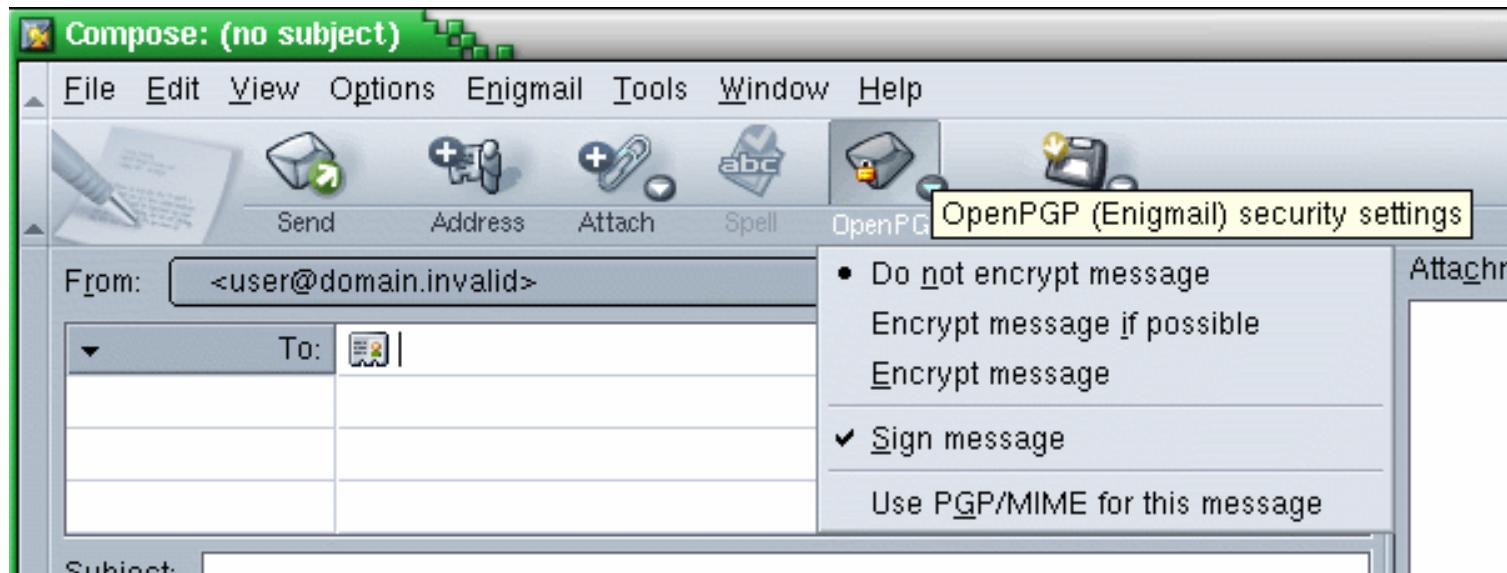
```
gpg --sign-key addr@domain.dk # Eller keyid
```

Husk at sikre at det nu også er den korrekte key i signerer

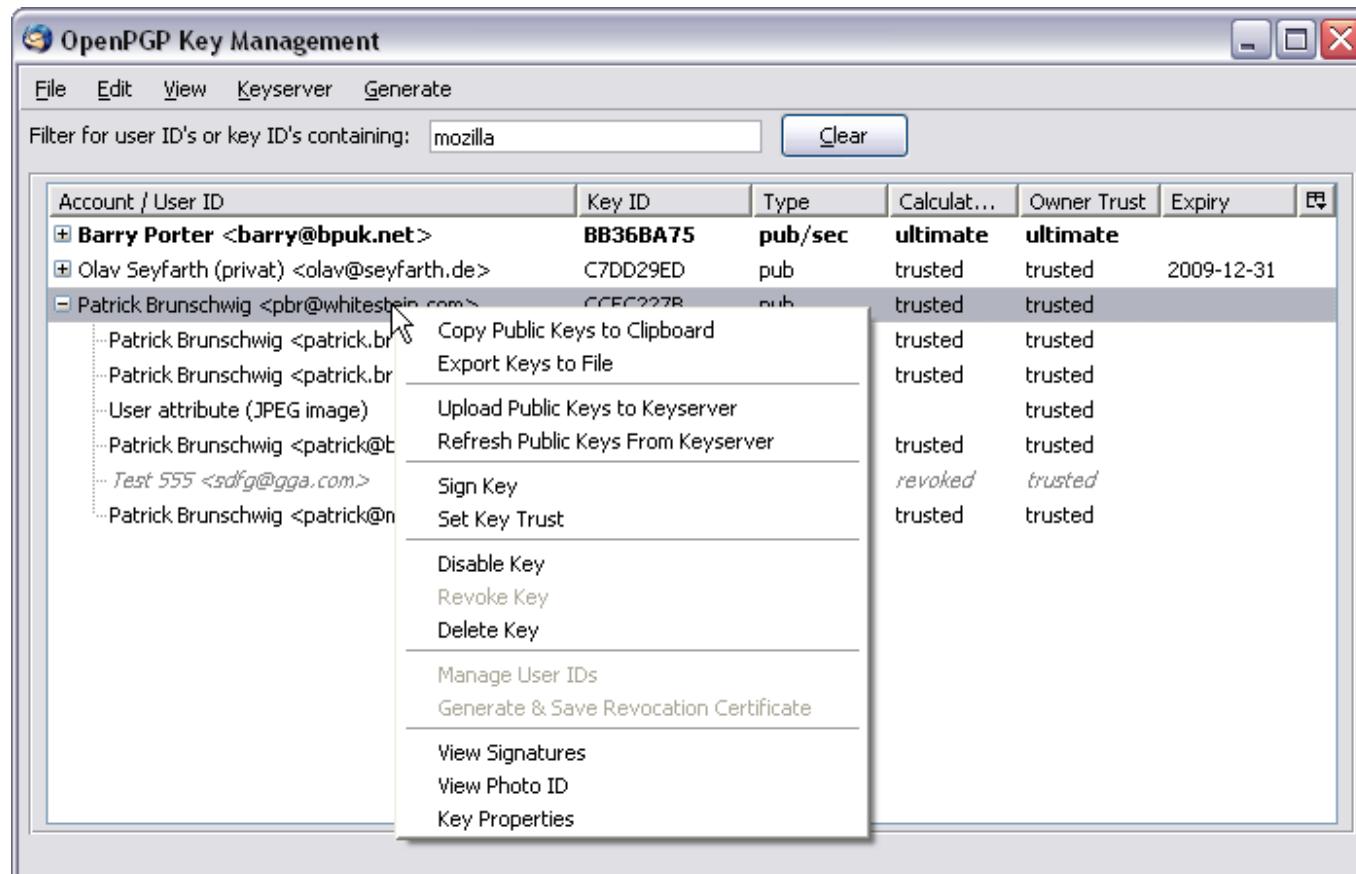
Kontroller med:

```
gpg --fingerprint addr@domain.dk
```

# Enigmail - GPG plugin til Mail

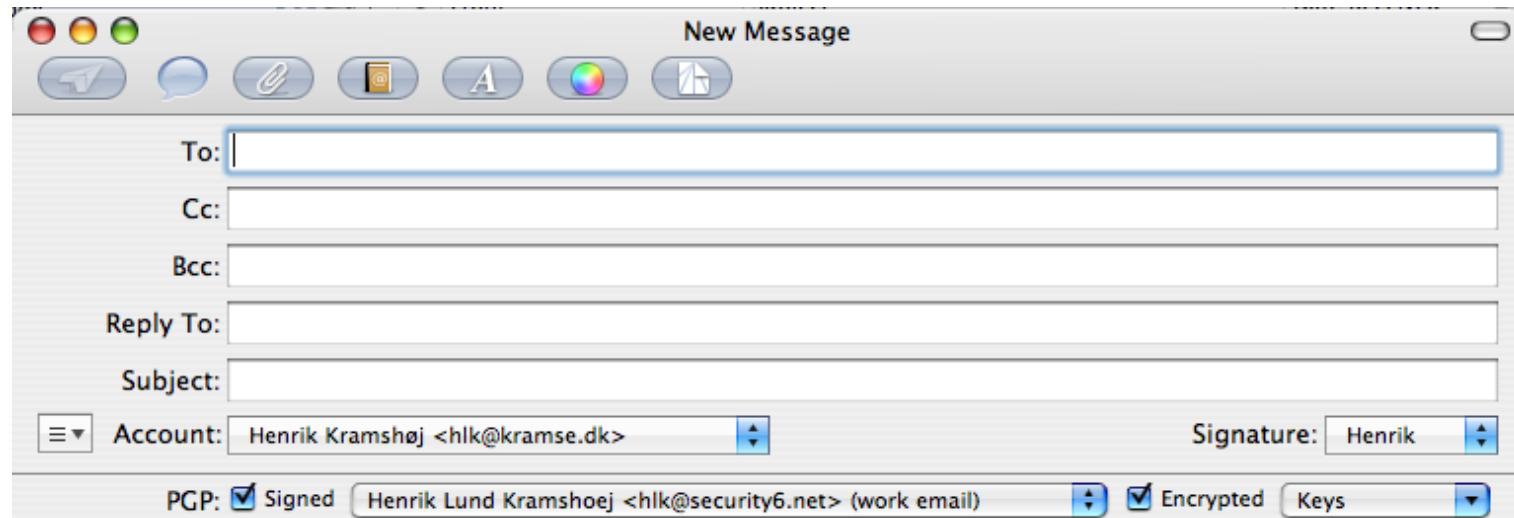


- Enigmail er en udvidelse til
- mailklienten i Mozilla/Netscape
- standalone mailklienten Thunderbird
- Billede fra <http://enigmail.mozdev.org>



Key Manager funktionaliteten i Enigmail kan anbefales

# GPGMail plugin til Mac OS X Mail.app



- Bruger GPG
- kilde: <http://www.sente.ch/software/GPGMail/English.lproj/GPGMail.html>



Vi laver nu øvelsen

## Lav en PGP-kompatibel nøgle

som er øvelse **6** fra øvelseshæftet.



Vi laver nu øvelsen

## Hent en nøgle fra en anden

som er øvelse **7** fra øvelseshæftet.



Vi laver nu øvelsen

## Send en krypteret mail

som er øvelse **8** fra øvelseshæftet.



Vi laver nu øvelsen

## Signer en nøgle

som er øvelse **9** fra øvelseshæftet.

# Kryptering step 4 - network data in transit



## File Transfer Protocol - filoverførsler

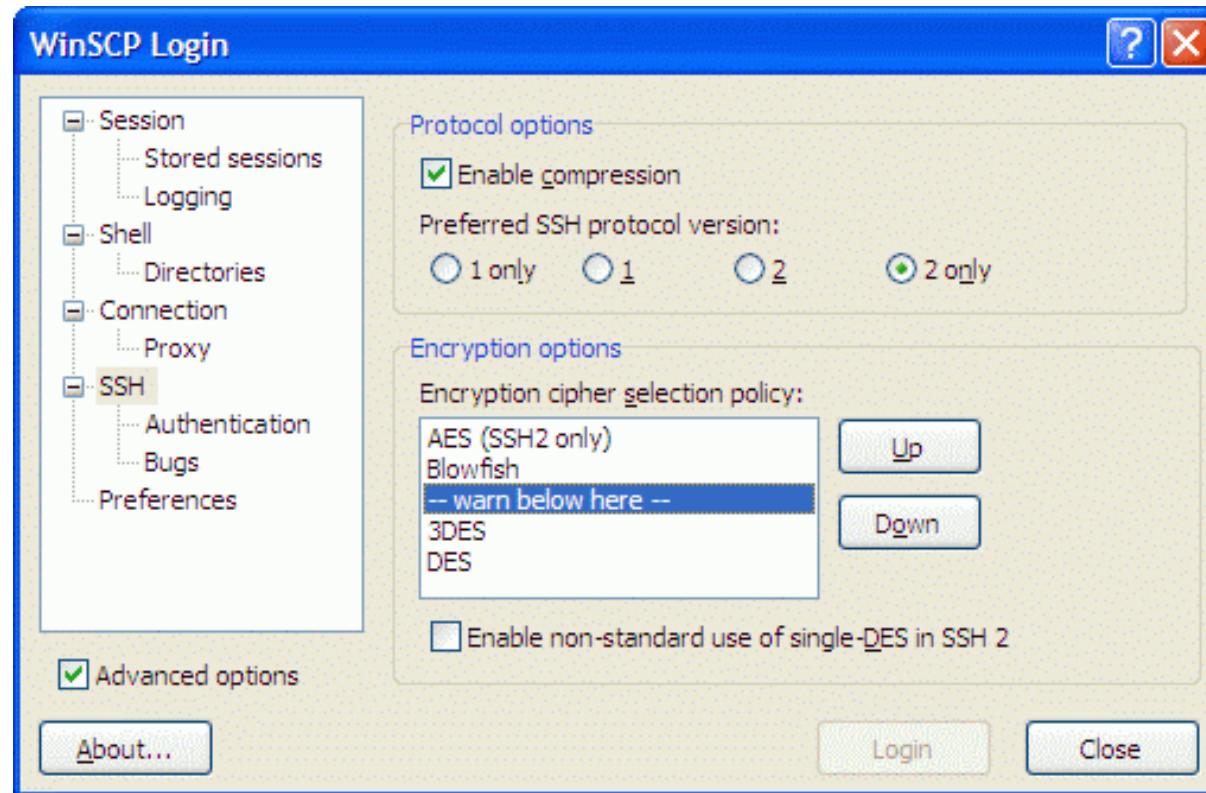
FTP bruges især til:

- FTP - drivere, dokumenter, rettelser - Windows Update? er enten HTTP eller FTP
- Opdatering af websites
- Overførsel af data mellem virksomheder
- Serveren er indbygget i de fleste serveroperativsystemer

FTP sender i klartekst

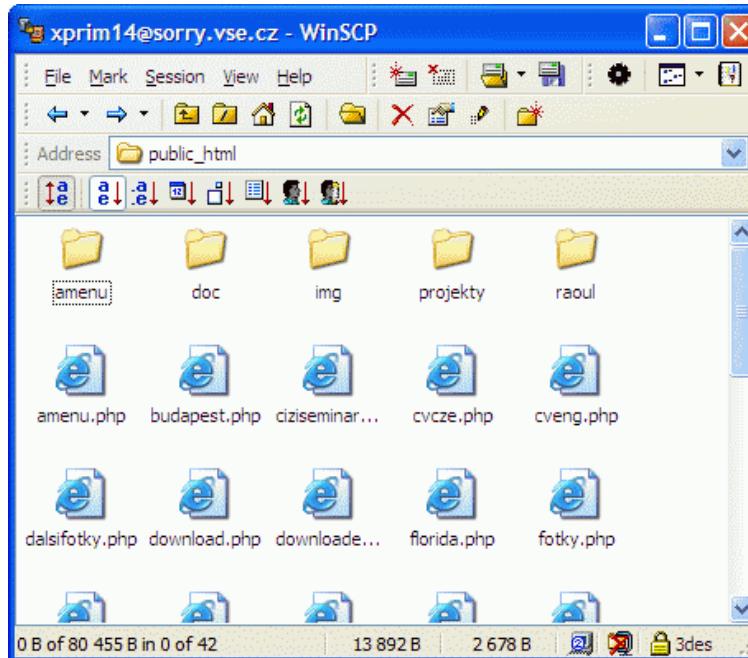
**USER brugernavn** og

**PASS hemmeligt-kodeord**



screenshot fra

<http://winscp.vse.cz/eng/screenshots/large/advanced.gif>



benytter Secure Shell protkollen (SSH)

screenshot fra

<http://winscp.vse.cz/eng/screenshots/large/explorer.gif>

## FileZilla Features

### ❖ Overview

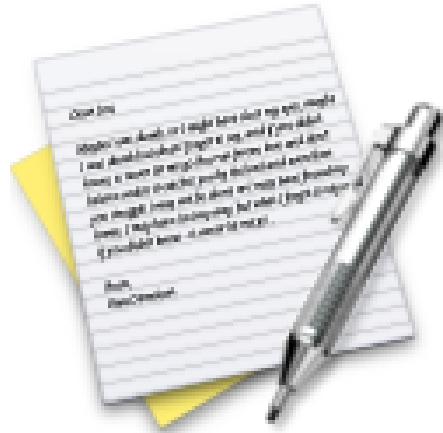
FileZilla Client is a fast and reliable cross-platform FTP, FTPS and SFTP client with lots of useful features

### ❖ Features

Among others, the features of FileZilla include the following:

- Easy to use
- Supports FTP, FTP over SSL/TLS (FTPS) and SSH File Transfer Protocol (SFTP)
- Cross-platform. Runs on Windows, Linux, \*BSD, Mac OS X and more
- IPv6 support
- Available in many languages
- Supports resume and transfer of large files >4GB
- Tabbed user interface
- Powerful Site Manager and transfer queue
- Bookmarks
- Drag & drop support
- Configurable transfer speed limits

<http://filezilla-project.org/>



Vi laver nu øvelsen

## Installation af FileZilla

som er øvelse **10** fra øvelseshæftet.

VPN [http://en.wikipedia.org/wiki/Virtual\\_private\\_network](http://en.wikipedia.org/wiki/Virtual_private_network)

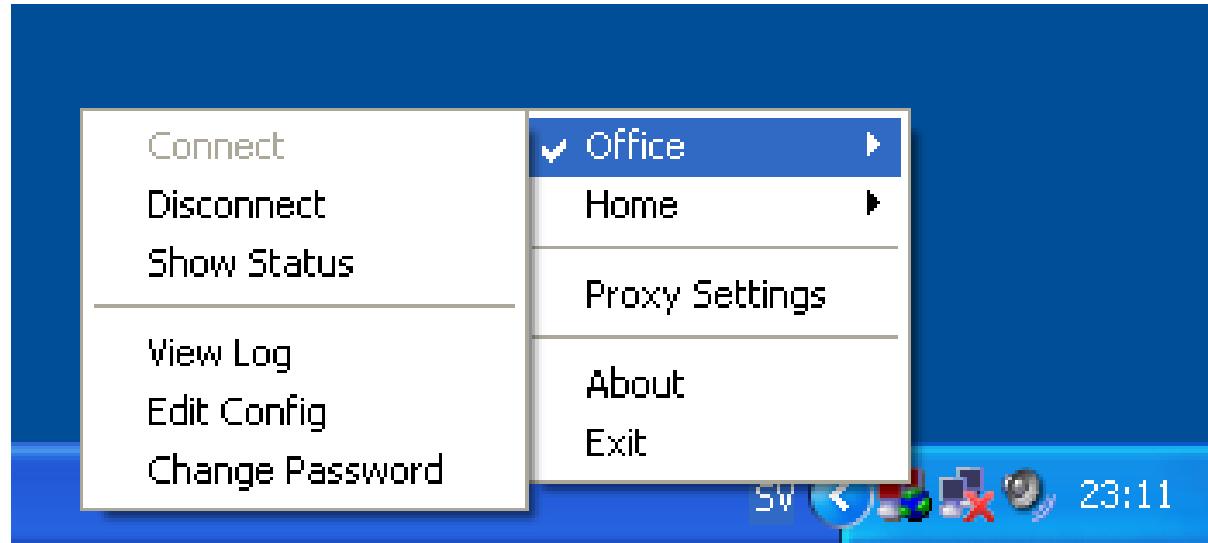
SSL/TLS VPN - Generelt koncept. Adskillige leverandører: Cisco, Juniper, F5 Big IP

De snakker ikke ret godt sammen på tværs. Brug IPSec for dette.

IPsec er desværre blokeret mange steder og man skal bruge en klient  
(I praksis bruger SSL VPN ofte en klient, men den downloades fra web)

Open source variant: OpenVPN

Der findes idag mange billige services så man kan sikre sin trafik ☺  
og derved kan man bruge services der kræver man bor/kommer fra USA osv.



OpenVPN GUI - easy to use

Ægypten, Sudan, Tunesien, ...

Den der kontrollerer ISPerne kontrollerer trafikken

Facebook revolutionerne

Blokering er umulig, men det forsøges

Spredning af falsk information

Diginotar Dutch Certificate Authority

Kilde: <http://irevolution.net/2011/02/10/facebook-for-repressive-regimes/>



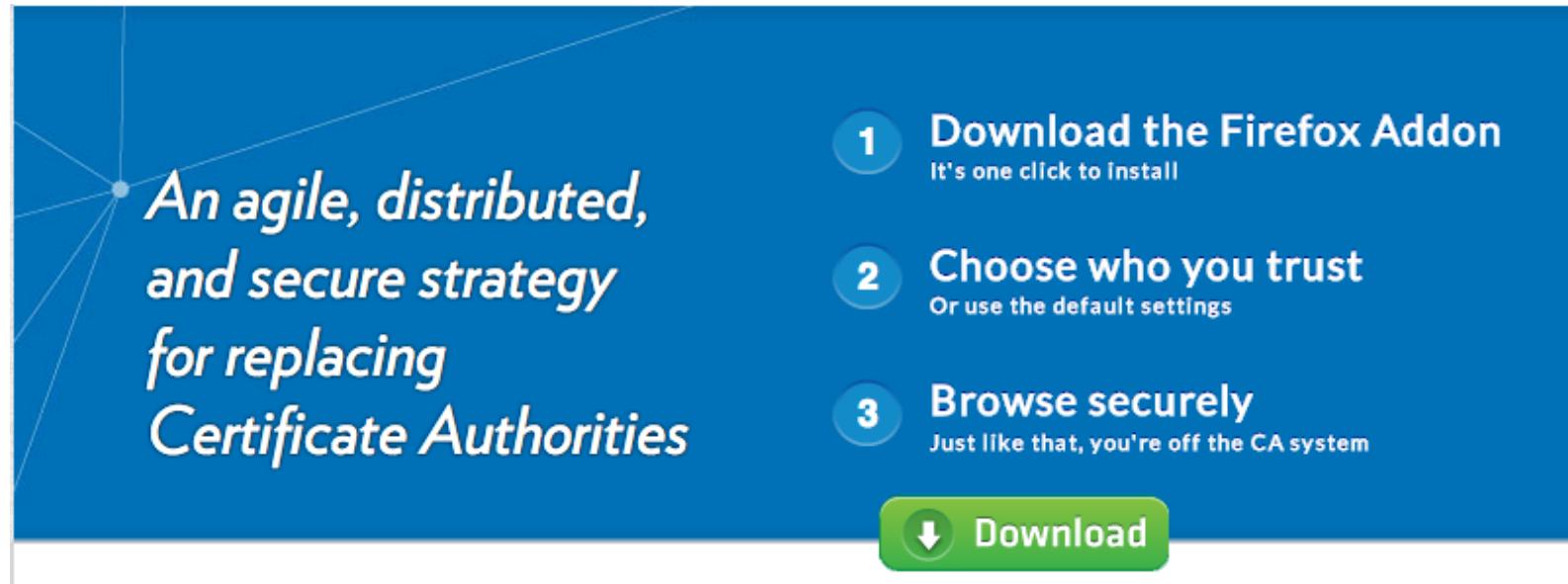
HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

<http://www.eff.org/https-everywhere>



An add-on formerly considered paranoid: CertPatrol implements "pinning" for Firefox/Mozilla/SeaMonkey roughly as now recommended in the User Interface Guidelines of the World Wide Web Consortium (W3C).

<http://patrol.psyced.org/>



*An agile, distributed, and secure strategy for replacing Certificate Authorities*

- 1 Download the Firefox Addon**  
It's one click to install
- 2 Choose who you trust**  
Or use the default settings
- 3 Browse securely**  
Just like that, you're off the CA system

 Download

<http://convergence.io/>

Warning: radical change to how certificates work

## Objective:

Specify mechanisms and techniques that allow Internet applications to establish cryptographically secured communications by using information distributed through DNSSEC for discovering and authenticating public keys which are associated with a service located at a domain name.

### DNS-based Authentication of Named Entities (dane)

<https://datatracker.ietf.org/wg/dane/charter/>

<http://googleonlinesecurity.blogspot.dk/2011/04/improving-ssl-certificate-security.html>

**DNSSEC er ved at være godt udbredt - undtagen i DK**

(findes på .dk zonen, men næsten ingen resolvere)

<http://www.censurfridns.dk>

Velkommen til www.censurfridns.dk.

Du er velkommen til at benytte:

ns1.censurfridns.dk / 89.233.43.71 / 2002:d596:2a92:1:71:53::

ns2.censurfridns.dk / 89.104.194.142 / 2002:5968:c28e::53

som DNS server for at undgå DNS censur.

Se venligst blog.censurfridns.dk for mere info.

**Det er uacceptabelt at pille ved DNS - punktum!**



Der findes mange DNSSEC programmer, blandt andet DNSSEC-trigger som er en navneserver til din lokale PC

- **DNSSEC Validator for firefox**  
<https://addons.mozilla.org/en-us/firefox/addon/dnssec-validator/>
- **OARC tools** <https://www.dns-oarc.net/oarc/services/odvr>
- <http://www.nlnetlabs.nl/projects/dnssec-trigger/>

# Kryptering step 5 - anonymous access to internet

## Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

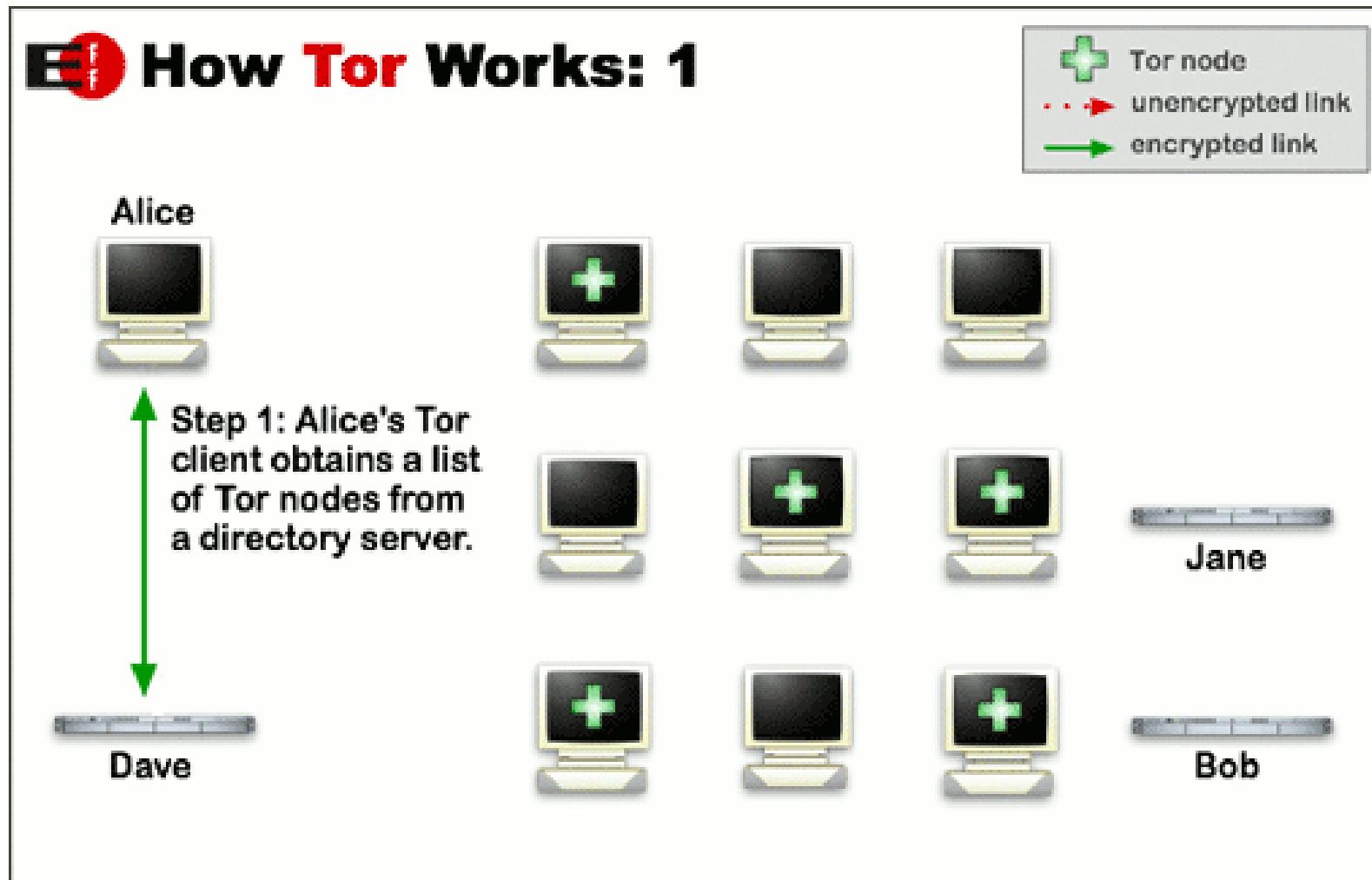


Download Tor 

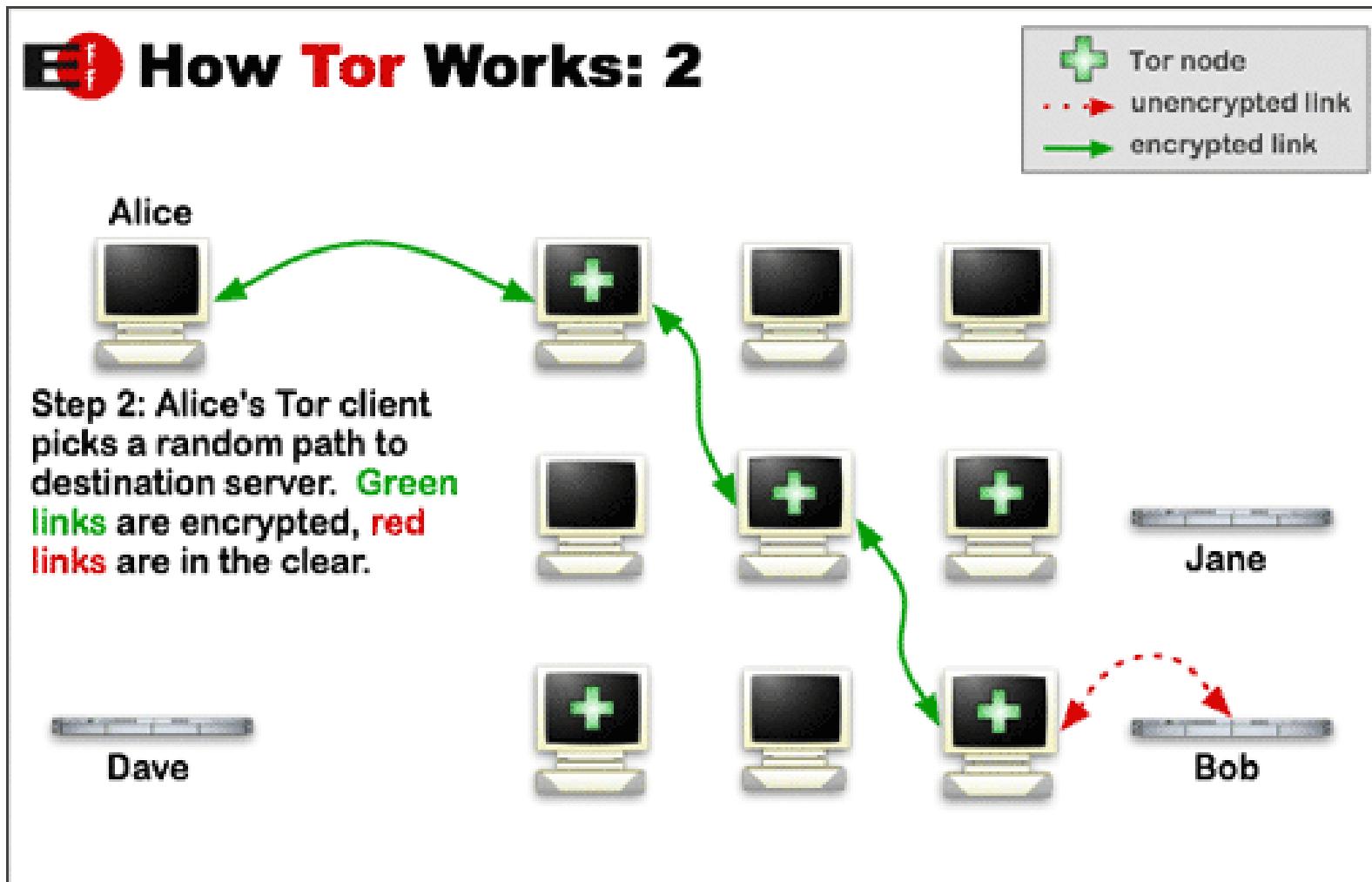
- ➔ Tor prevents anyone from learning your location or browsing habits.
- ➔ Tor is for web browsers, instant messaging clients, remote logins, and more.
- ➔ Tor is free and open source for Windows, Mac, Linux/Unix, and Android

<https://www.torproject.org/>

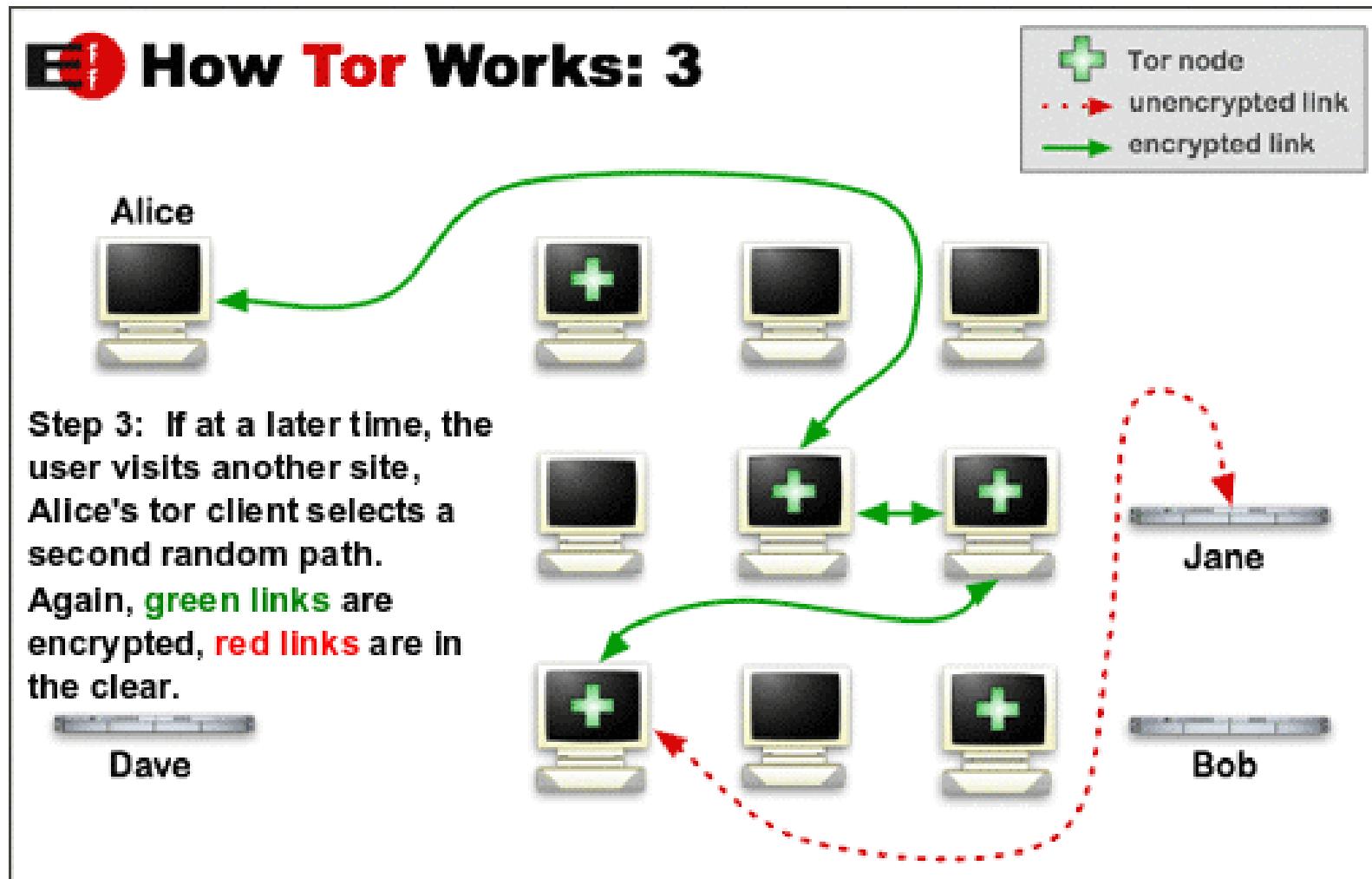
Der findes alternativer, men Tor er mest kendt



pictures from <https://www.torproject.org/about/overview.html.en>



pictures from <https://www.torproject.org/about/overview.html.en>



pictures from <https://www.torproject.org/about/overview.html.en>



Der findes diverse tools til Tor, Torbutton on/off knap til Firefox osv.

Det anbefales at bruge bundles fra <https://www.torproject.org/>

Pause mens dem som vil installere gør det

# Bonus: brug Bitcoins?

## BITCOIN NORDIC

Instant Bitcoins

[Buy Bitcoins](#) [Sell Bitcoins](#) [News](#) [About us](#)



Credit card



Pay through eWire which accepts VISA, VISA Electron, MasterCard, Maestro, and DanKort issued in Scandinavian countries.  
Delivery time: 1 minute.

Bank transfer



Domestic, SEPA (European Union) or international wire transfers to our Danish bank account.  
Delivery time: 0-48 hours.

Cash or check



Cash or check by mail or in-person deposit at various locations.  
Delivery time: 5 minutes.

Husk: hvis du bruger kryptering fra starten er det nemmere at slette data - slet nøglen

Computer Forensics involves the preservation, identification, extraction, documentation and interpretation of computer data.

*Computer Forensics: Incident Response Essentials*, Warren G. Kruse II og Jay G. Heiser, Addison-Wesley, 2002



Inspireret af TCT har Brian Carrier fra Atstake lavet flere værktøjer til forensics analyse

Det officielle hjem for TASK og autopsy er nu: [www.sleuthkit.org](http://www.sleuthkit.org)

TASK kan betragtes som en erstatning for TCT the coroners toolkit lavet af Dan Farmer og Wietse Venema

Autopsy er en Forensic Browser - et interface til TASK

- Filsystemer skal være hurtige - skal ikke lave unødvendige operationer
- En harddisk er en fysisk disk med en arm der skal bevæges og et læse/skrivehoved som skal tændes og slukkes
- Hvis man kan undgå at skulle skrive over hele filen ved sletning er det hurtigere
- De fleste operativsystemer sletter derfor kun metadata og overskriver derfor ikke alle datablokke for filer
- Eksempel DOS FAT  
Når man slettede en fil på MS-DOS fjernede man reelt kun det første bogstav i filnavnet  
undelete bestod i at skrive det første bogstav i filnavnet - og håbe på at alle datablokke der hørte til filen stadig var at finde på disken

*Secure Deletion of Data from Magnetic and Solid-State Memory* Peter Gutmann, 1996

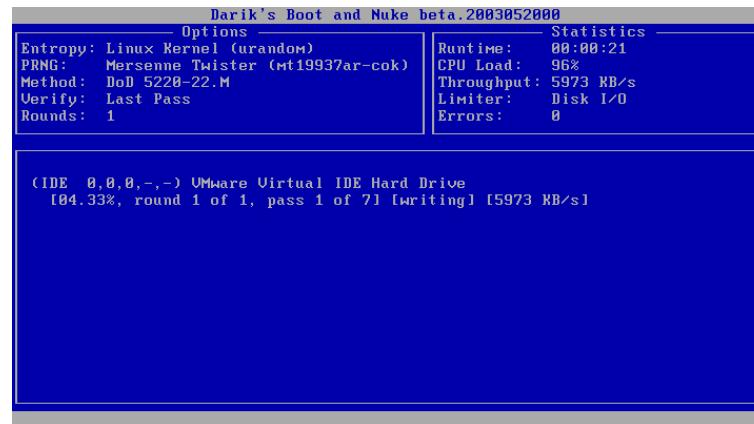
Det er et klassisk paper om sletning af data som man bør læse

[http://www.cs.auckland.ac.nz/~pgut001/pubs/secure\\_del.html](http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html)

Der findes mange kommercielle værktøjer til sletning og en del Open Source - baseret på Guttman's dokument

DBAN er efter min mening et af de bedste

<http://dban.sourceforge.net/> USB



- ad-hoc oprydning, formatering og sletning af filer giver ingen sikkerhed!
- Free. Fast. Rapid deployment in emergency situations.
- Easy. Start the computer with DBAN and press the ENTER key.
- Safe. Irrecoverable data destruction. Prevents most forensic data recovery techniques.
- <http://dban.sourceforge.net/>
- NB: Brug <http://unetbootin.sourceforge.net/> til at skrive CD-image til

# Opsummering Del 1



Hey, Lets be careful out there!

Kilde: Michael Conrad <http://www.hillstreetblues.tv/>

Nødvendigt eller er det ekstreme teknikker vi har diskuteret?

```
main(int argc, char **argv)
{
    char buf[200];
    strcpy(buf, argv[1]);
    printf("%s\n", buf);
}
```



## Teknisk hvad er hacking - og værktøjer

Mere frit - vi undersøger nogle af emnerne fra del 1, som hackere

(Vi når IKKE alle opgaverne fra øvelseshæftet)



## Don't Panic!

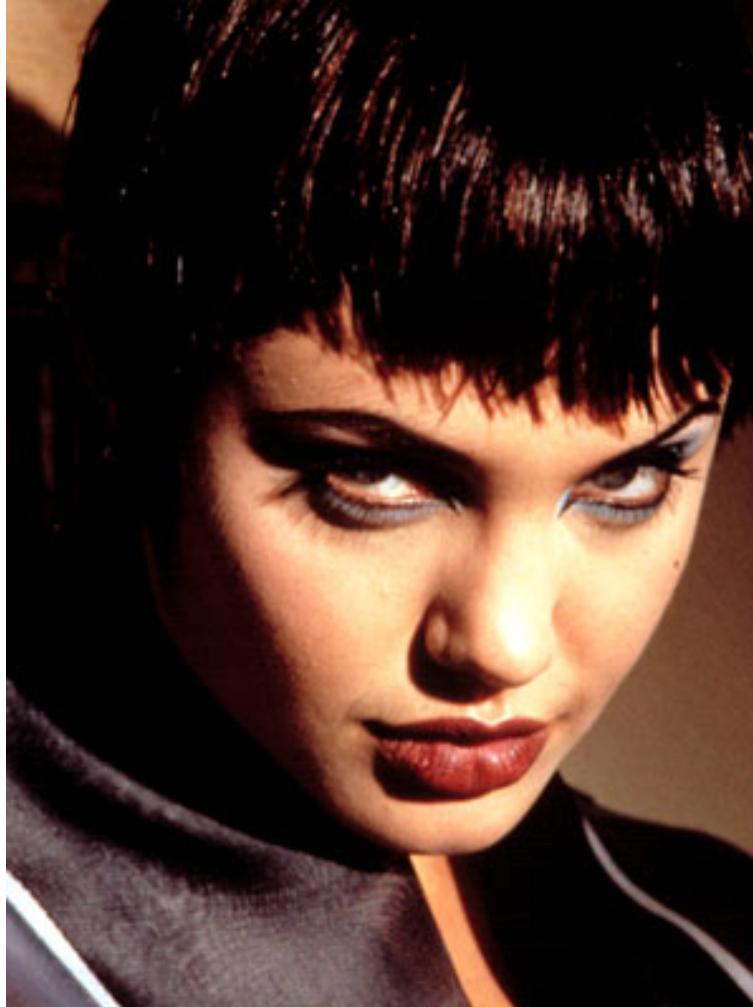
Introduce hacking and a couple of hacker tools

List some tools that can be used to protect your computer and data

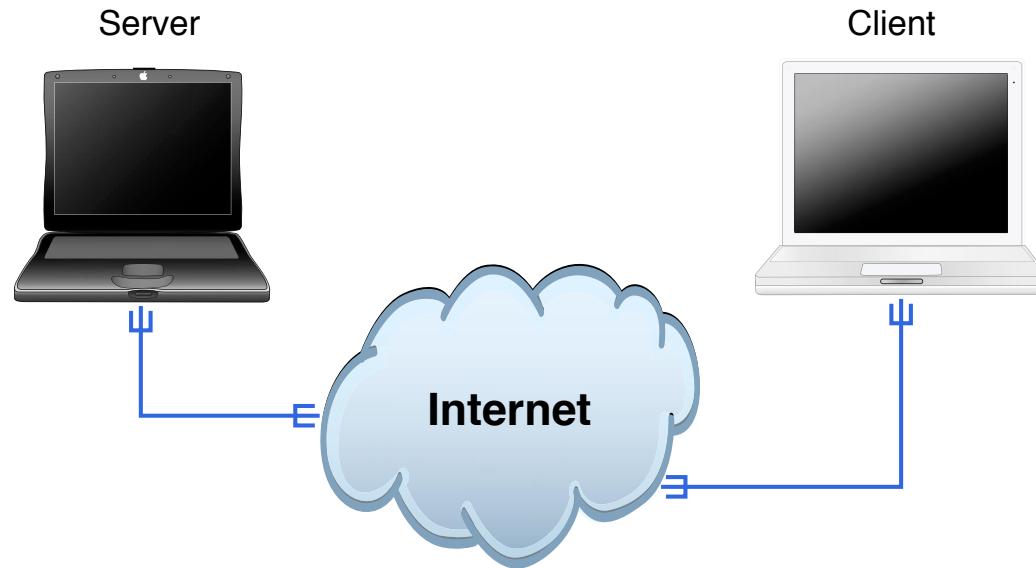
PS Sorry about the many TLAs ... og danglish

præsentationen er meget teknisk, men foredraget behøver ikke at blive det ☺

# Introduktion til hacking



<http://www.imdb.com/title/tt0113243/> Hackers (1995)



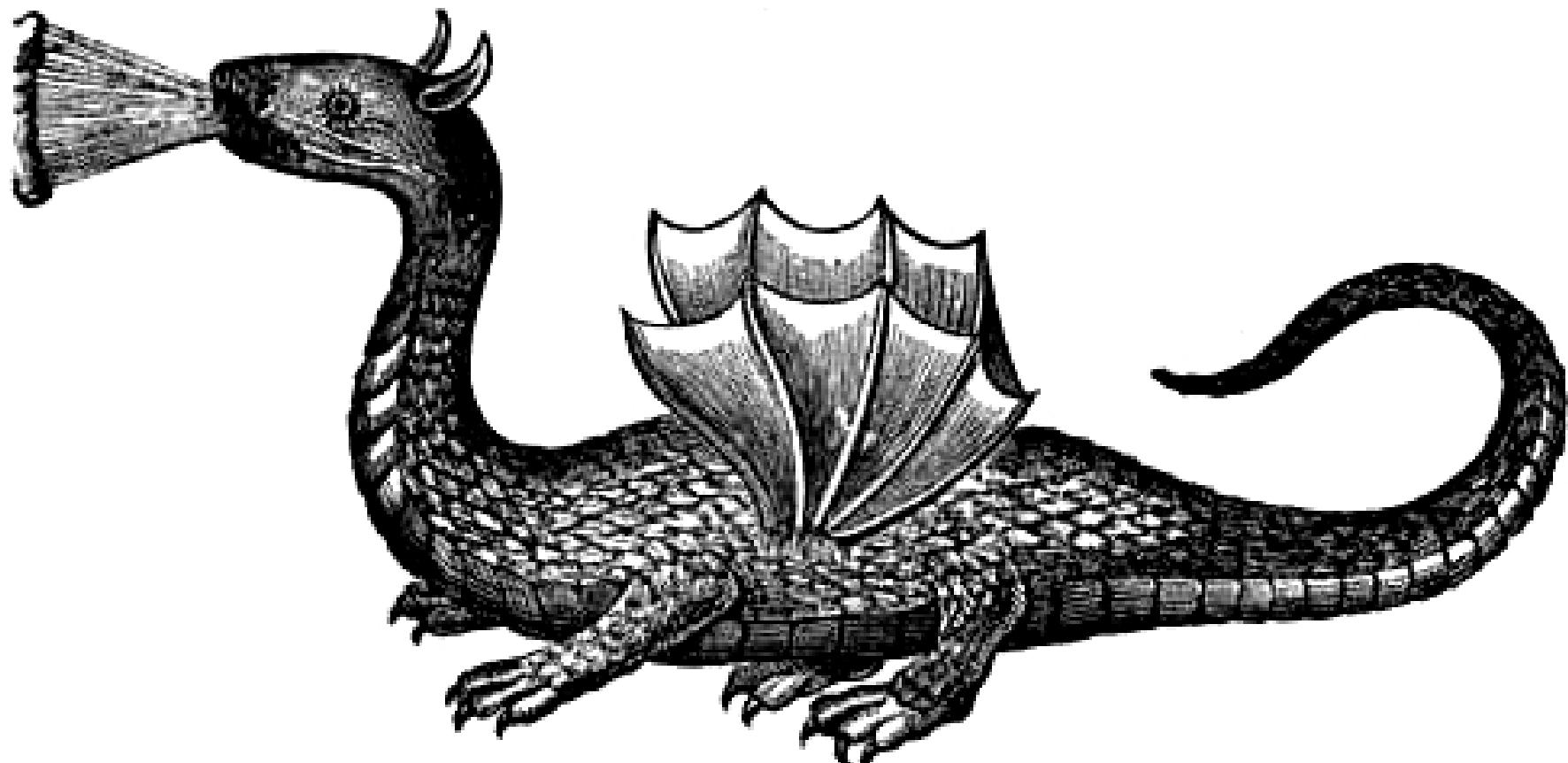
Clients and servers

Rooted in academic networks

Protocols which are more than 20 years old, moved to TCP/IP in 1981

Trying to migrate to IPv6 - a lot of hacking opportunities here

# Internet - Here be dragons



# Matrix style hacking anno 2003



# Trinity breaking in

```
80/tcp      open     http  
81/tcp      open     hostx2_anc  
10 [REDACTED] ( mobile)  
11 $ nmap -v -sS -O 10.2.2.2  
11  
13 Starting nmap 0. 2.54BETA25  
13 Insufficient responses for TCP sequencing (3). OS detection is  
13 inaccurate  
14 Interesting ports on 10.2.2.2:  
14 (The 1539 ports scanned but not shown below are in state: cle  
51 Port      State       Service  
51 22/tcp    open        ssh  
58  
68 No exact OS matches for host  
68  
24 Nmap run completed -- 1 IP address (1 host up) scanned  
50 $ sshhuhnke 10.2.2.2 -rootpw="Z10H0101"  
Connecting to 10.2.2.2:ssh ... successful.  
Re  
IP Attempting to exploit SSHv1 CRC32 ... successful.  
Reseting root password to "Z10H0101".  
System open: Access Level <9>  
Hn $ ssh 10.2.2.2 -l root  
root@10.2.2.2's password: [REDACTED]  
[REDACTED] RIF CONTROL [REDACTED]  
[REDACTED] ACCESS GRANTED [REDACTED]
```

<http://nmap.org/movies.html>

Meget realistisk [http://www.youtube.com/watch?v=511GCTgqE\\_w](http://www.youtube.com/watch?v=511GCTgqE_w)

## Det korte svar - drop diskussionen

Det havde oprindeligt en anden betydning, men medierne har taget udtrykket til sig - og idag har det begge betydninger.

**Idag er en hacker stadig en der bryder ind i systemer!**

ref. Spafford, Cheswick, Garfinkel, Stoll, ... - alle kendte navne indenfor sikkerhed

- *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Clifford Stoll
- *Hackers: Heroes of the Computer Revolution*, Steven Levy
- *Practical Unix and Internet Security*, Simson Garfinkel, Gene Spafford, Alan Schwartz

Eric Raymond, der vedligeholder en ordbog over computer-slang (The Jargon File) har blandt andet følgende forklaringer på ordet hacker:

- En person, der nyder at undersøge detaljer i programmerbare systemer og hvordan man udvider deres anvendelsesmuligheder i modsætning til de fleste brugere, der bare lærer det mest nødvendige
- En som programmerer lidenskabligt (eller enddog fanatisk) eller en der foretrækker at programmere fremfor at teoretiserer om det
- En ekspert i et bestemt program eller en der ofter arbejder med eller på det; som i "en Unixhacker".

Kilde: Peter Makholm, <http://hacking.dk>

Benyttes stadig i visse sammenhænge se <http://labitat.dk>

We reject kings, presidents, and voting.  
We believe in rough consensus and running code.  
– The IETF credo Dave Clark, 1992.

Request for comments - RFC - er en serie af dokumenter

RFC, BCP, FYI, informational  
de første stammer tilbage fra 1969

Ændres ikke, men får status Obsoleted når der udkommer en nyere version af en standard

Standards track:  
Proposed Standard → Draft Standard → Standard

Åbne standarder = åbenhed, ikke garanti for sikkerhed

## Udnyttede følgende sårbarheder

- buffer overflow i fingerd - VAX kode
- Sendmail - DEBUG
- Tillid mellem systemer: rsh, rexec, ...
- dårlige passwords

## Avanceret + camouflage!

- Programnavnet sat til 'sh'
- Brugte fork() til at skifte PID jævnligt
- password cracking med intern liste med 432 ord og /usr/dict/words
- Fandt systemer i /etc/hosts.equiv, .rhosts, .forward, netstat ...

Lavet af Robert T. Morris, Jr.

Medførte dannelsen af CERT, <http://www.cert.org>

Der benyttes en del værktøjer:

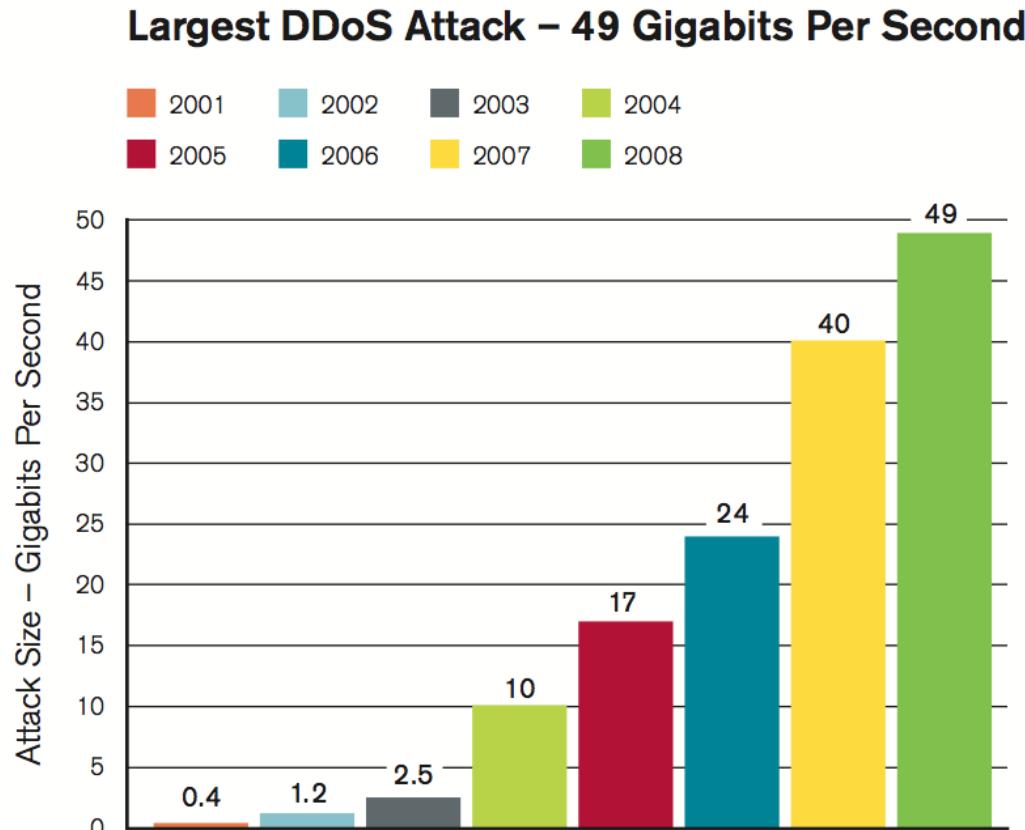
- nmap - <http://www.insecure.org> portscanner
- Wireshark - <http://www.wireshark.org/> avanceret netværkssniffer
- OpenBSD - <http://www.openbsd.org> operativsystem med fokus på sikkerhed
- BackTrack <http://www.remote-exploit.org/backtrack.html>
- Putty - <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>  
terminal emulator med indbygget SSH

Er det fornuftigt at man kan hente dem?

**Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling.**

Hacking kan betyde:

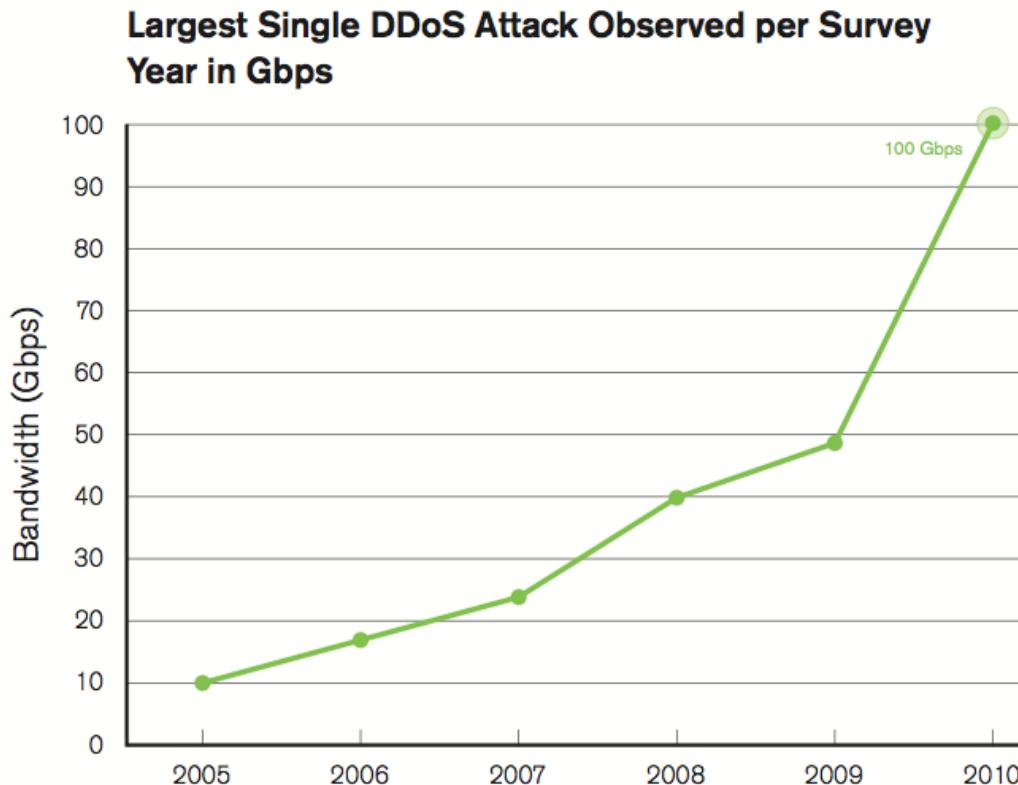
- At man skal betale erstatning til personer eller virksomheder
- At man får konfiskeret sit udstyr af politiet
- At man, hvis man er over 15 år og bliver dømt for hacking, kan få en bøde - eller fængselsstraf i alvorlige tilfælde
- At man, hvis man er over 15 år og bliver dømt for hacking, får en plettet straffeattest. Det kan give problemer, hvis man skal finde et job eller hvis man skal rejse til visse lande, fx USA og Australien
- Frit efter: <http://www.stophacking.dk> lavet af Det Kriminalpræventive Råd
- Frygten for terror har forstærket ovenstående - så lad være!



**Figure 1: Largest DDoS Attack – 49 Gigabits Per Second**

Source: Arbor Networks, Inc.

Kilde: <http://www.arbornetworks.com/report> 2009 rapporten



*Figure 1*  
Source: Arbor Networks, Inc.

Kilde: <http://www.arbornetworks.com/report> 2010 rapporten

- Application-Layer DDoS Attacks Are Increasing in Sophistication and Operational Impact
- Mobile/Fixed Wireless Operators Are Facing Serious Challenges to Maintaining Availability in the Face of Attacks
- Firewalls and IPS Devices Are Falling Short on DDoS Protection
- DNS Has Broadly Emerged as an Attack Target and Enabler
- Lack of Visibility into and Control over IPv6 Traffic Is a Significant Challenge
- Chronic Underfunding of Operational Security Teams
- Operators Continue to Express Low Confidence in the Efficacy of Law Enforcement
- Operators Have Little Confidence in Government Efforts to Protect Critical Infrastructure

Kilde: <http://www.arbornetworks.com/report> februar 2011

Der er mange pointer at lære fra de mange hacking historier

Social Engineering rockz! Uddannelse!

Alle er et mål, evt. som springbrædt ind til andre

Anonymous er en flok forkælede møgunger? helte? egoer? løst knyttet gruppe, tæt knyttet gruppe?

Hacktivism er okay, bare det rammer Scientology?

... flere pointer?

**Hacking er ikke cool og koster mange resourcer!**



Hacking ligner indimellem magi



Hacking kræver blot lidt ninja-træning

MAC filtrering på trådløse netværk

Alle netkort har en MAC adresse - BRÆNDT ind i kortet fra fabrikken

Mange trådløse Access Points kan filtrere MAC adresser

Kun kort som er på listen over godkendte adresser tillades adgang til netværket ■

Det virker dog ikke ☺

De fleste netkort tillader at man overskriver denne adresse midlertidigt

Eksemplet med MAC filtrering er en af de mange myter

Hvorfor sker det?

Marketing - producenterne sætter store mærkater på æskerne

Manglende indsigt - forbrugerne kender reelt ikke koncepterne

Hvad *er* en MAC adresse egentlig

Relativt få har forudsætningerne for at gennemskue dårlig sikkerhed

Løsninger? ■

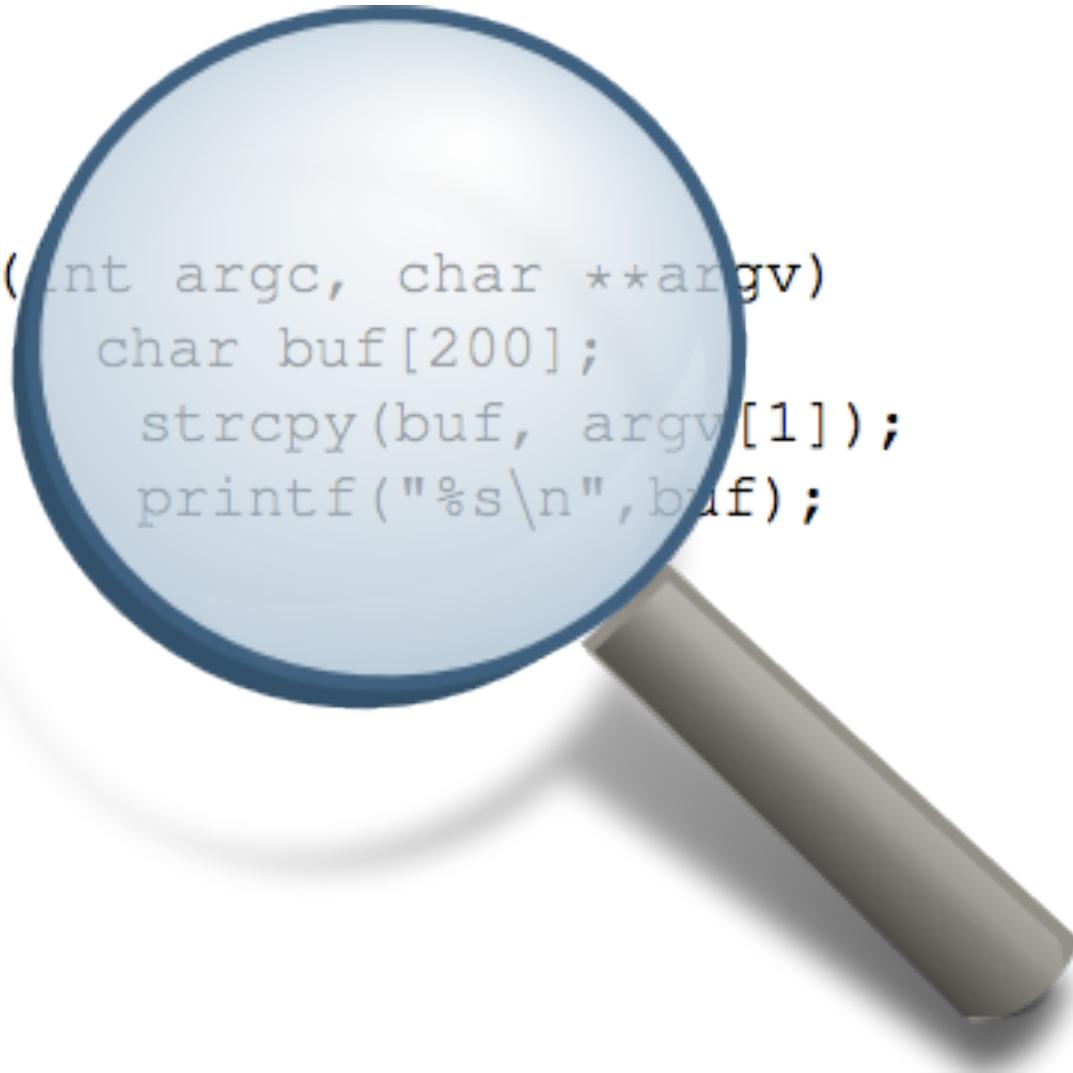
Udbrede viden om usikre metoder til at sikre data og computere

Udbrede viden om sikre metoder til at sikre data og computere

# MAC filtrering

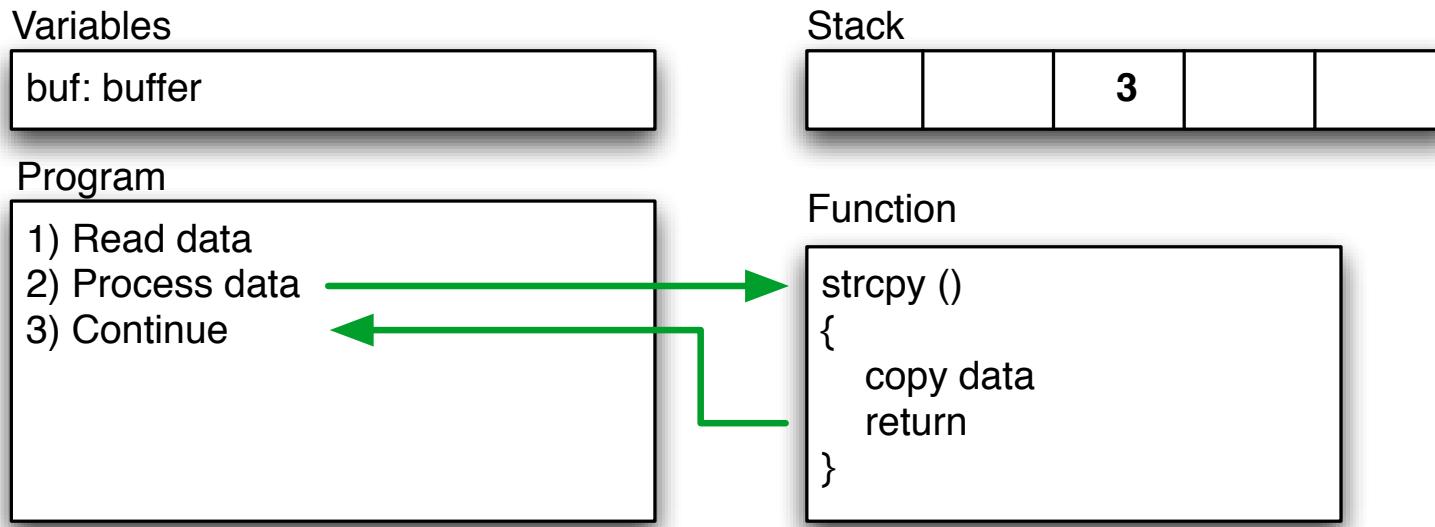


```
main(int argc, char **argv)
{
    char buf[200];
    strcpy(buf, argv[1]);
    printf("%s\n", buf);
}
```



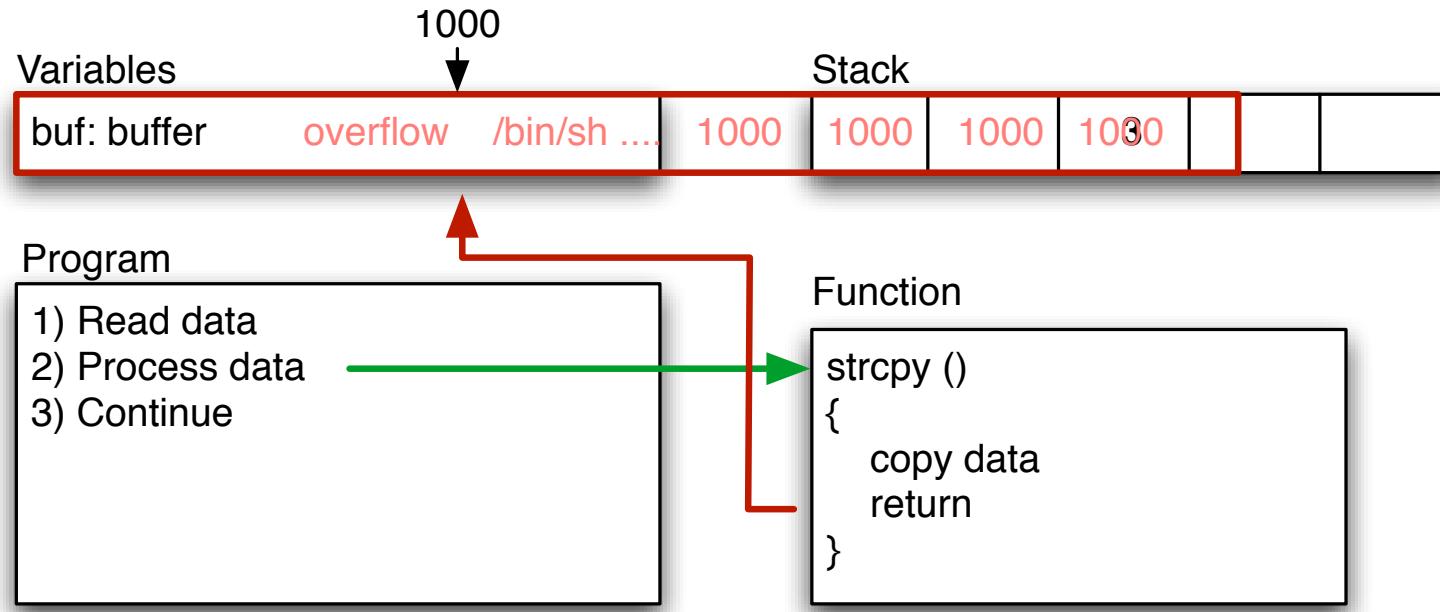
**Et buffer overflow** er det der sker når man skriver flere data end der er afsat plads til i en buffer, et dataområde. Typisk vil programmet gå ned, men i visse tilfælde kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

**Stack protection** er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.



```
main(int argc, char **argv)  
{  
    char buf[200];  
    strcpy(buf, argv[1]);  
    printf("%s\n", buf);  
}
```

# Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

```
$buffer = "";
$null = "\x00"; █
$nop = "\x90";
$nopsize = 1; █
$len = 201; // what is needed to overflow, maybe 201, maybe more!
$the_shell_pointer = 0xdeadbeef; // address where shellcode is
# Fill buffer
for ($i = 1; $i < $len;$i += $nopsize) {
    $buffer .= $nop;
}█
$address = pack('l', $the_shell_pointer);
$buffer .= $address;█
exec "$program", "$buffer";
```

## Demo exploit in Perl

Black box testing

Closed source reverse engineering

White box testing

Open source betyder man kan læse og analysere koden

Source code review - automatisk eller manuelt

Fejl kan findes ved at prøve sig frem - fuzzing

Exploits virker typisk mod specifikke versioner af software

# The Exploit Database - dagens buffer overflow



The screenshot shows the homepage of The Exploit Database. At the top, there's a navigation bar with links like [ home ], [ news ], [ remote ], [ local ], [ web ], [ dos ], [ shellcode ], [ papers ], [ search ], [ D ], [ submit ], and [ rss ]. To the right of the navigation, it says "Currently Archiving 10343 Exploits". The main content area features a banner with the text "The Exploit Database" and a subtext about being an archive of exploits and vulnerable software. It also mentions a cleanup and submission policy. Below this, there's a section titled "Remote Exploits" with a table listing various exploits. The table columns include Date, D, A, V, Description, Plat., and Author. The table rows list the following information:

Date	D	A	V	Description	Plat.	Author
2010-01-27	D	A	✓	CamShot v1.2 SEH Overwrite Exploit	windows	technik
2010-01-25	D	-	✓	AOL 9.5 Phobos.Playlist 'Import()' Buffer Overflow Exploit (Meta)	windows	Trancer
2010-01-22	D	A	✓	IntelliTamper 2.07/2.08 (SEH) Remote Buffer Overflow	windows	loneferret
2010-01-21	D	-	✓	EFS Easy Chat server Universal BOF-SEH (Meta)	windows	FB1H2S
2010-01-20	D	-	✓	AOL 9.5 ActiveX 0day Exploit (heap spray)	windows	Dz_attacker
2010-01-19	D	-	✓	Pidgin MSN <= 2.6.4 File Download Vulnerability	multiple	Mathieu GASPARD
2010-01-18	D	A	✓	Exploit EFS Software Easy Chat Server v2.2	windows	John Babio

<http://www.exploit-db.com/>

## What is it?

The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide. The framework is written in the Ruby programming language and includes components written in C and assemblers.

Idag findes der samlinger af exploits som milw0rm

Udviklingsværktøjerne til exploits er idag meget raffinerede!

<http://www.metasploit.com/>

<http://www.fastandeasyhacking.com/> Armitage GUI til Metasploit

<http://www.offensive-security.com/metasploit-unleashed/>

Bemærk: alle angreb har forudsætninger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

Kan du bryde kæden af forudsætninger har du vundet!

Computeren skal være tændt

Funktionen der misbruges skal være slået til

Executable stack

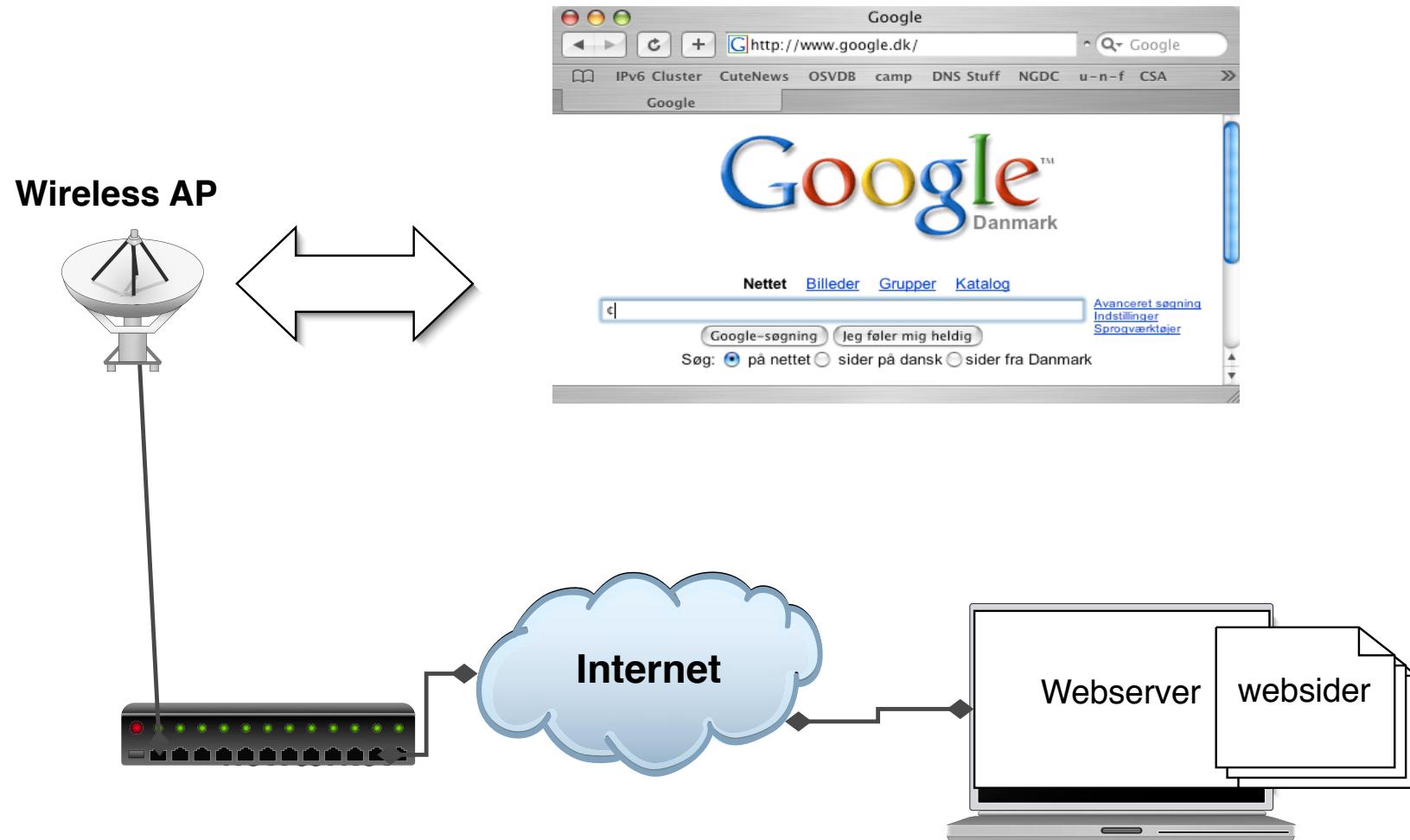
Executable heap

Fejl i programmet

|

**alle programmer har fejl**

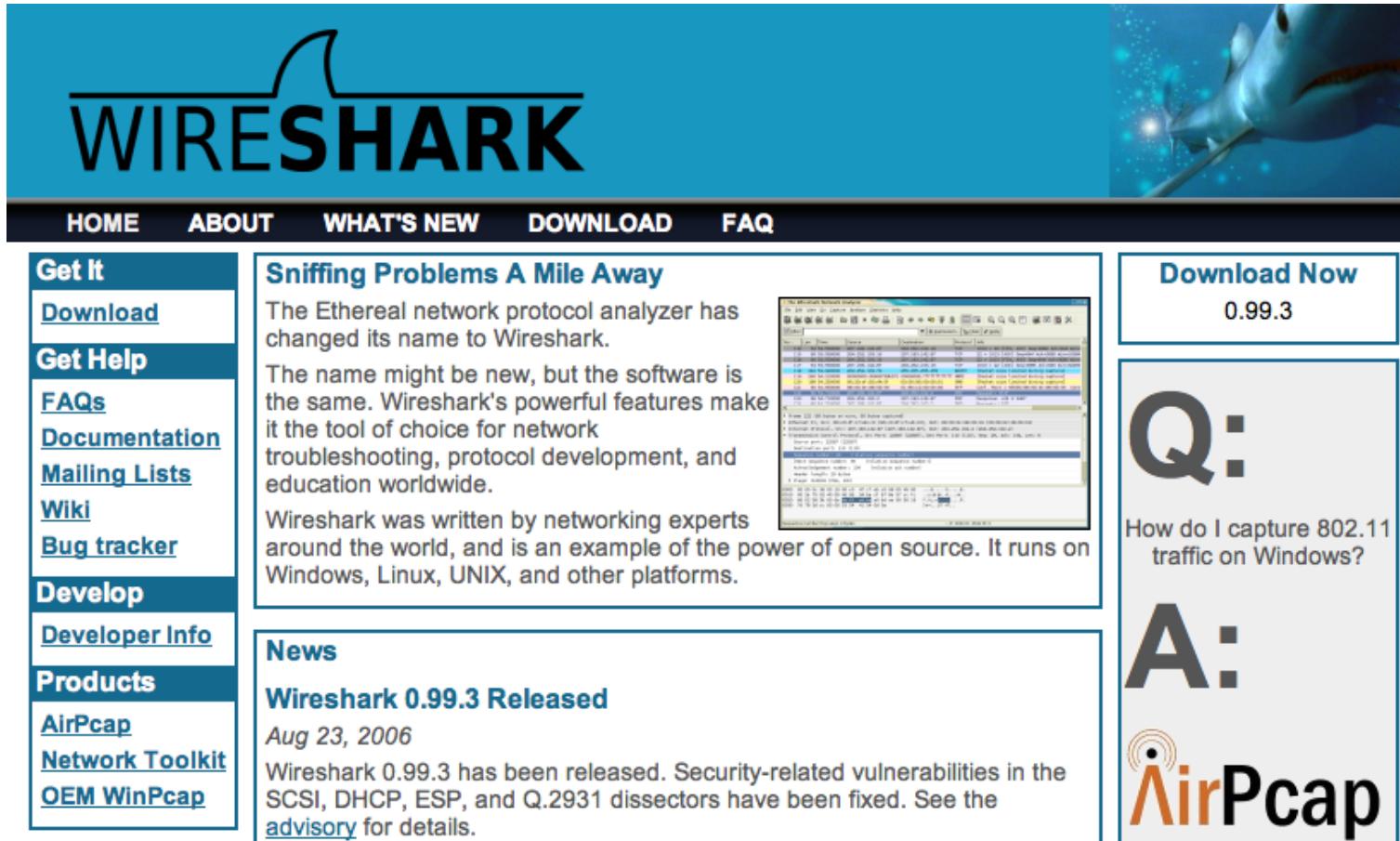
# Normal wireless brug





Wireshark - <http://www.wireshark.org> avanceret netværkssniffer  
bruger vi til at sniffe, vi bruger Wireshark til primære demo, nævner Ettercap osv.

BackTrack <http://www.backtrack-linux.org/>



The screenshot shows the official Wireshark website. At the top, there's a navigation bar with links for HOME, ABOUT, WHAT'S NEW, DOWNLOAD, and FAQ. Below the navigation is a large banner featuring the Wireshark logo and a shark swimming in water. To the left, there's a sidebar with sections for 'Get It' (links to Download, Get Help, FAQs, Documentation, Mailing Lists, Wiki, Bug tracker), 'Develop' (links to Developer Info, Products, AirPcap, Network Toolkit, OEM WinPcap), and 'Sniffing Problems A Mile Away'. This section discusses the name change from Ethereal to Wireshark and highlights its powerful features for network troubleshooting, protocol development, and education. In the center, there's a news section about the release of Wireshark 0.99.3, dated Aug 23, 2006, which fixed security-related vulnerabilities. To the right, there's a 'Download Now' section for version 0.99.3, a Q&A section about capturing 802.11 traffic, and the AirPcap logo.

<http://www.wireshark.org>  
både til Windows og UNIX, tidligere kendt som Ethereal

Download, installer - kør! - farligt!

Sådan gøres det:

- download program OG signaturfil/MD5
- verificer signatur eller MD5
- installer
- brug programmet
- hold programmet opdateret!

Det anbefales at afvikle BackTrack i en virtuel maskine, på klient med VMware Player, Virtualbox eller tilsvarende

BackTrack kan også benyttes som pentest server i netværket, med eller uden virtualisering

BackTrack <http://www.backtrack-linux.org/>

# Chaosreader

## Chaosreader Report

Created at: Sun Nov 16 21:04:18 2003, Type: snoop

[Image Report](#) - Click here for a report on captured images.

[GET/POST Report](#) (Empty) - Click here for a report on HTTP GETs and POSTs.

[HTTP Proxy Log](#) - Click here for a generated proxy style HTTP log.

### TCP/UDP/... Sessions

1.	Sun Nov 16 20:38:22 2003	30 s	192.168.1.3:1368 <-> 192.77.84.99:80	web	383 bytes	• <a href="#">as html</a>
2.	Sun Nov 16 20:38:22 2003	29 s	192.168.1.3:1366 <-> 192.77.84.99:80	web	381 bytes	• <a href="#">as html</a>

Med adgang til et netværksdump kan man læse det med chaosreader

Output er HTML med oversigter over sessioner, billeder fra datastrømmen osv.

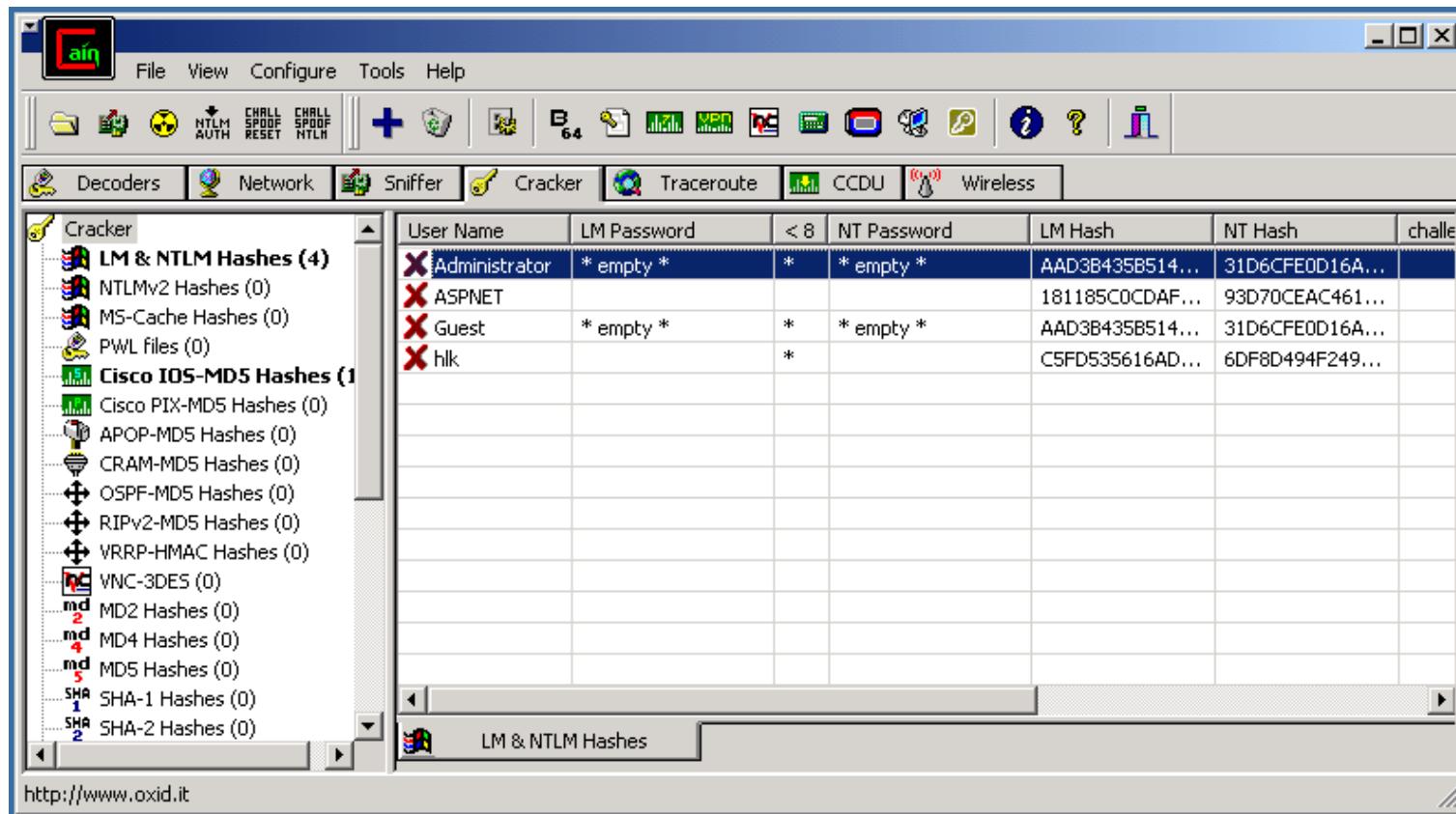
<http://chaosreader.sourceforge.net/>

## The 5<sup>th</sup> Wave

By Rich Tennant



**"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."**



Cain og Abel anbefales ofte istedet for l0phcrack <http://www.oxid.it>

John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.

UNIX passwords kan knækkes med alec Muffets kendte Crack program eller eksempelvis John The Ripper <http://www.openwall.com/john/>

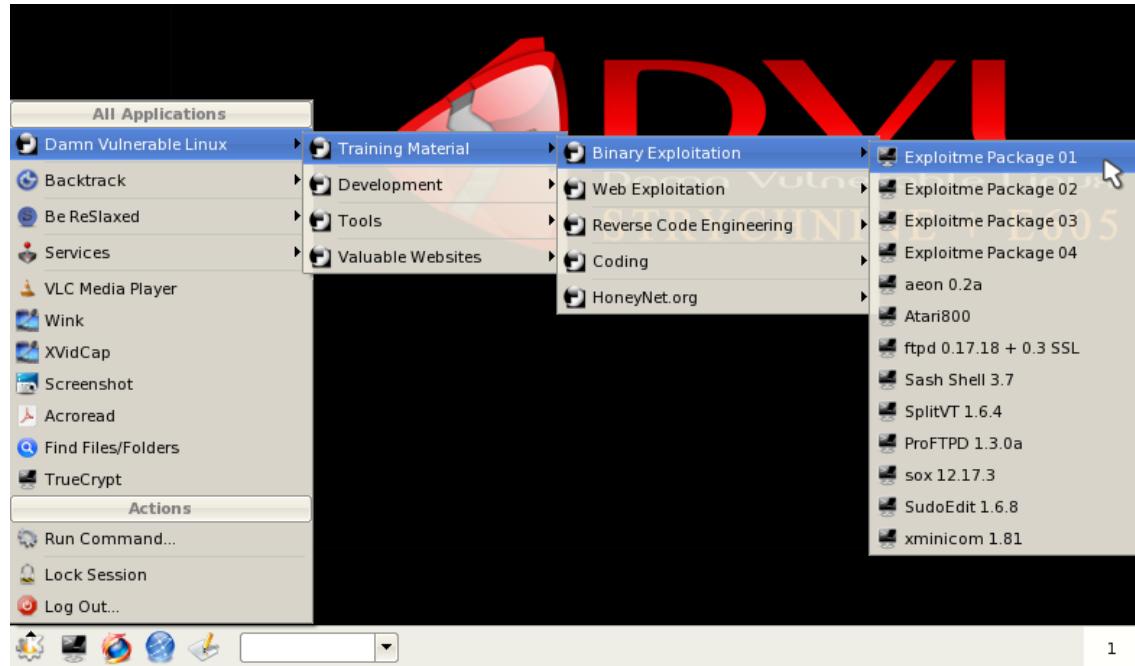
Jeg bruger selv John The Ripper

# What to do?



What do we do?

# Damn Vulnerable Linux boot CD'er



Damn Vulnerable Linux <http://www.damnvulnerablelinux.org/>  
DVL er baseret på Linux og må kopieres frit :-)

Brug DVD'en eller VMware player til den

Da UNIX indgår er her et lille *cheat sheet* til UNIX

- DOS/Windows kommando - tilsvarende UNIX, og forklaring
- dir - ls - står for list files, viser filnavne
- del - rm - står for remove, sletter filer
- cd - cd - change directory, skifter katalog
- type - cat - concatenate, viser indholdet af tekstudefiler
- more - less - viser tekstudefiler en side af gangen
- attrib - chmod - change mode, ændrer rettighederne på filer

Prøv bare:

- **ls** list, eller long listing med **ls -l**
- **cat /etc/hosts** viser hosts filen
- **chmod +x head.sh** - sæt execute bit på en fil så den kan udføres som et program med kommandoen **./head.sh**



WebGoat fra OWASP, <http://www.owasp.org>

Træningsmiljø til webhacking

Downloads som Zipfil og kan afvikles direkte på en Windows laptop

Tænk som en hacker

## Rekognoscering

- ping sweep, port scan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

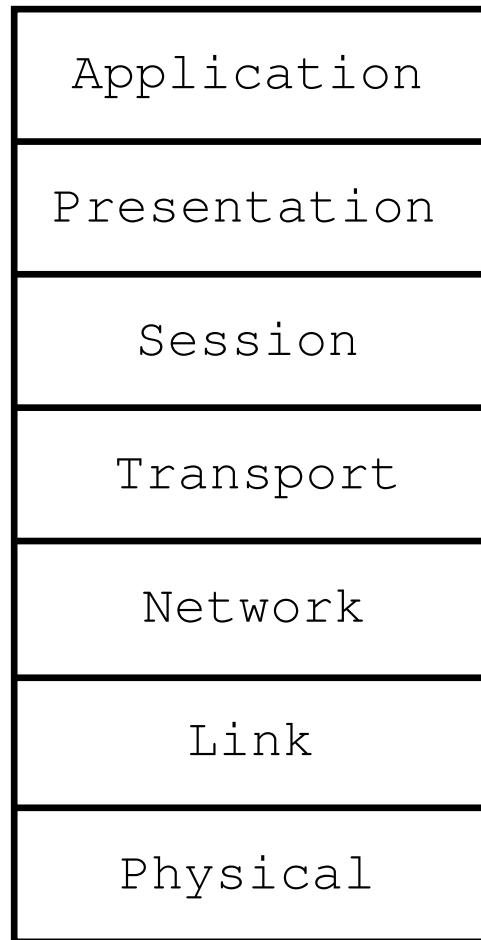
Udnyttelse/afprøvning: OpenVAS, nikto, exploit programs

Oprydning vises ikke på kurset, men I bør i praksis:

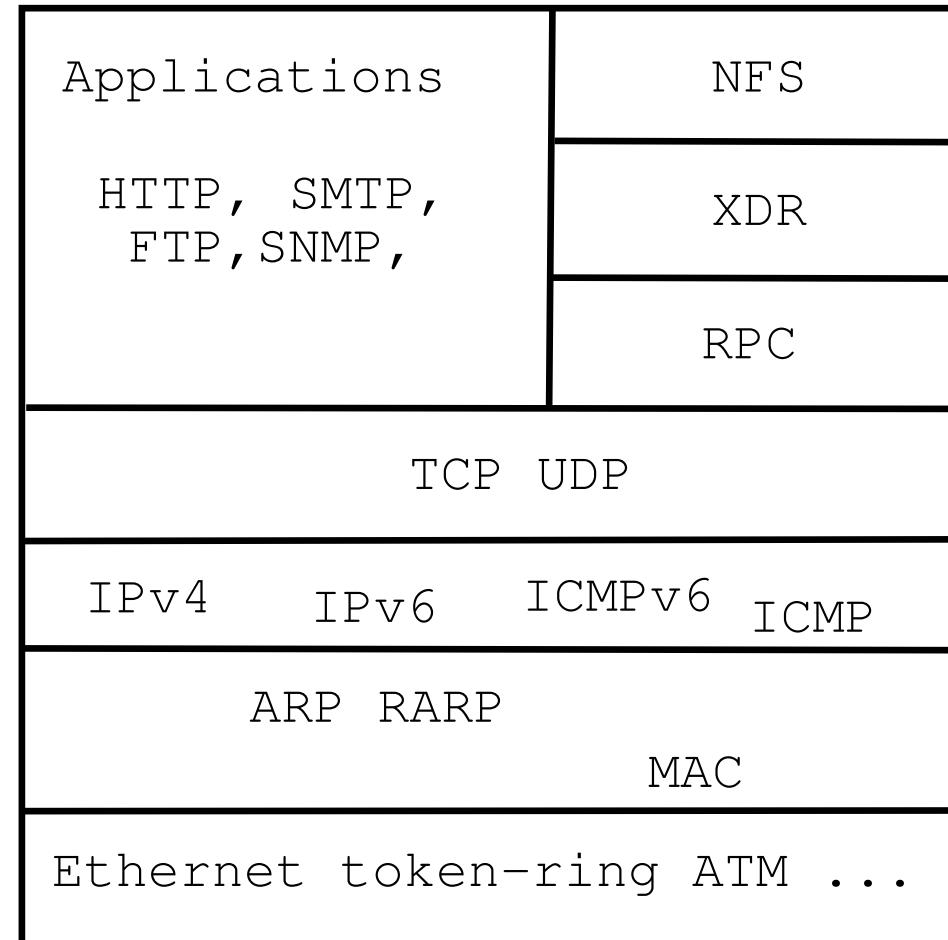
- Lav en rapport
- Gennemgå rapporten, registrer ændringer
- Opdater programmer, konfigurationer, arkitektur, osv.

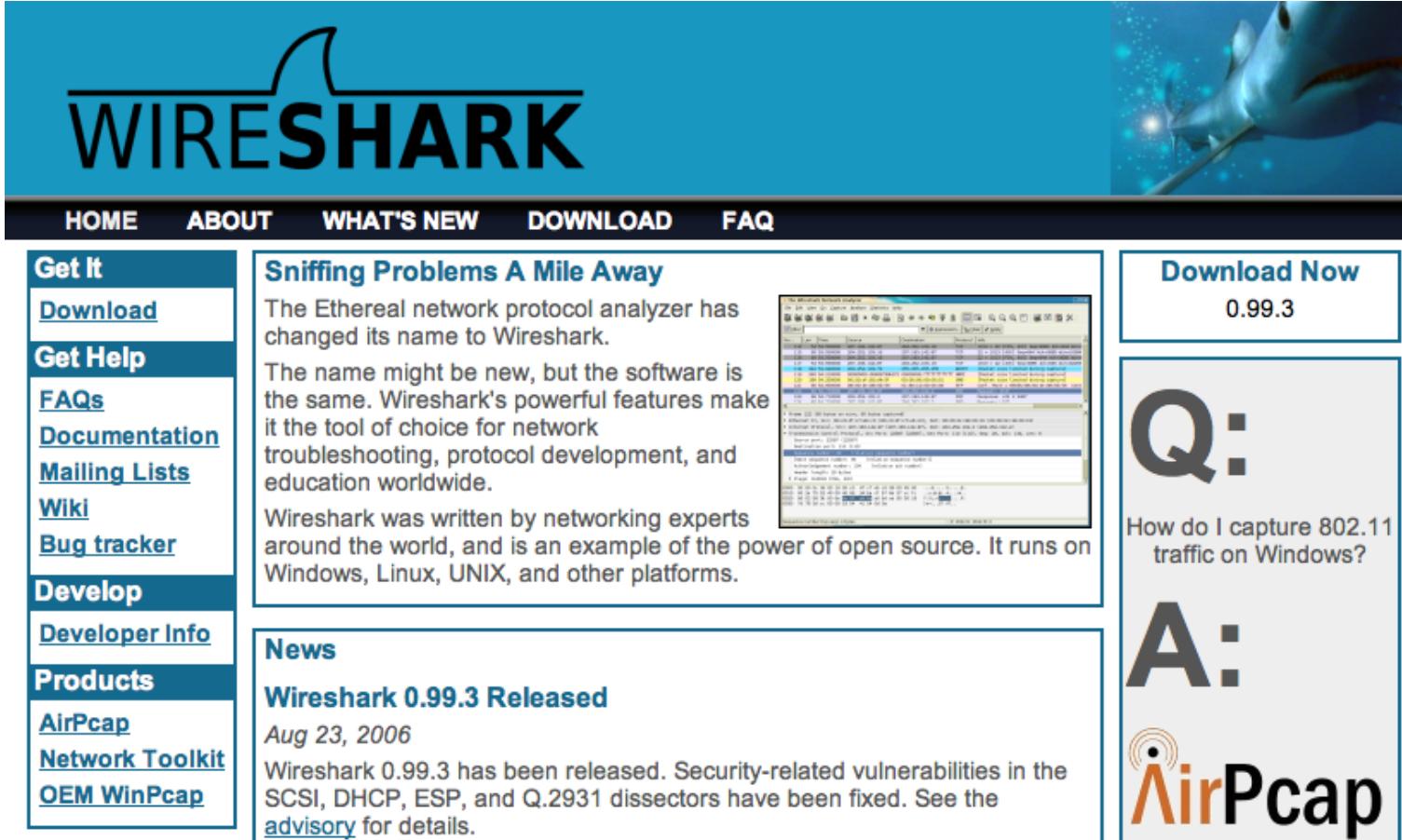
I skal jo også VISE andre at I gør noget ved sikkerheden.

OSI Reference Model



Internet protocol suite





The screenshot shows the official Wireshark website. At the top, there's a large blue header with the "WIRESHARK" logo. Below it is a black navigation bar with links for HOME, ABOUT, WHAT'S NEW, DOWNLOAD, and FAQ. To the right of the navigation is a background image of a shark swimming in water. On the left side, there's a sidebar with a dark blue background containing links under categories like "Get It", "Get Help", "Develop", and "Products". The main content area has several sections: one about name changes, news about the 0.99.3 release, and a Q&A section about capturing 802.11 traffic.

**Sniffing Problems A Mile Away**

The Ethereal network protocol analyzer has changed its name to Wireshark.

The name might be new, but the software is the same. Wireshark's powerful features make it the tool of choice for network troubleshooting, protocol development, and education worldwide.

Wireshark was written by networking experts around the world, and is an example of the power of open source. It runs on Windows, Linux, UNIX, and other platforms.

**News**

**Wireshark 0.99.3 Released**

Aug 23, 2006

Wireshark 0.99.3 has been released. Security-related vulnerabilities in the SCSI, DHCP, ESP, and Q.2931 dissectors have been fixed. See the [advisory](#) for details.

**Download Now**

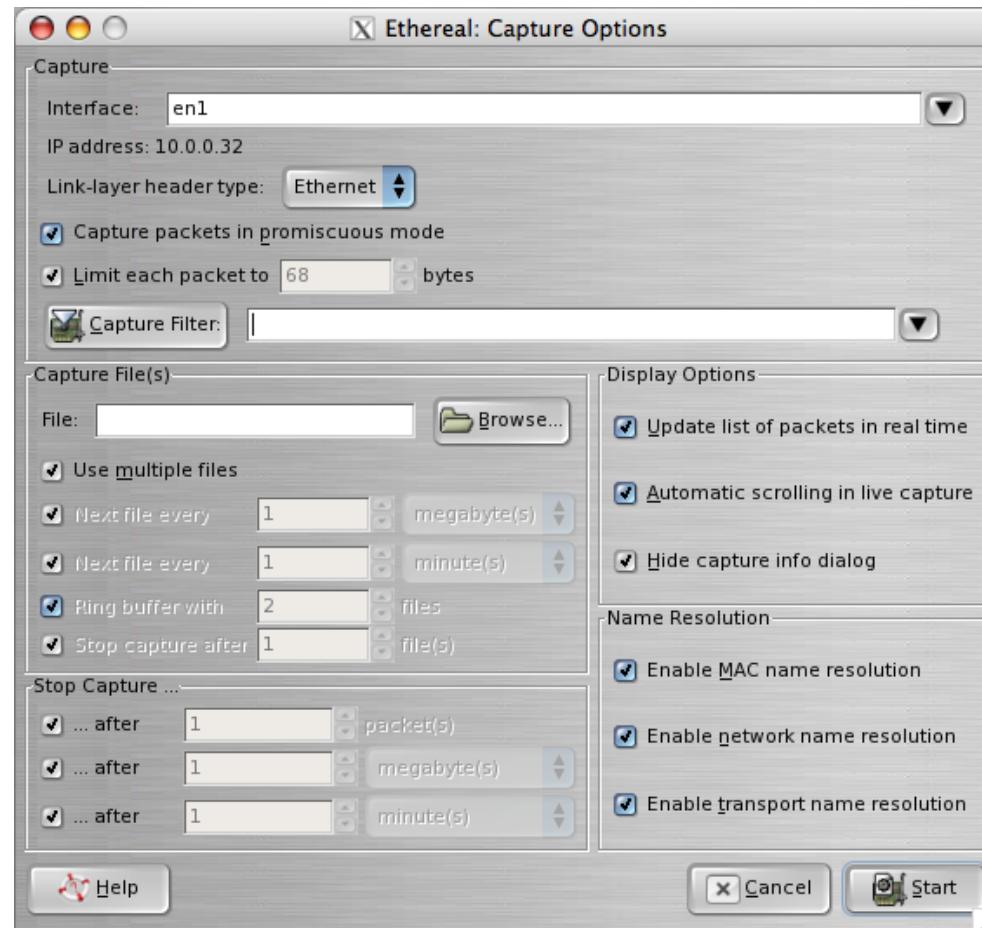
0.99.3

**Q:**  
How do I capture 802.11 traffic on Windows?

**A:**  

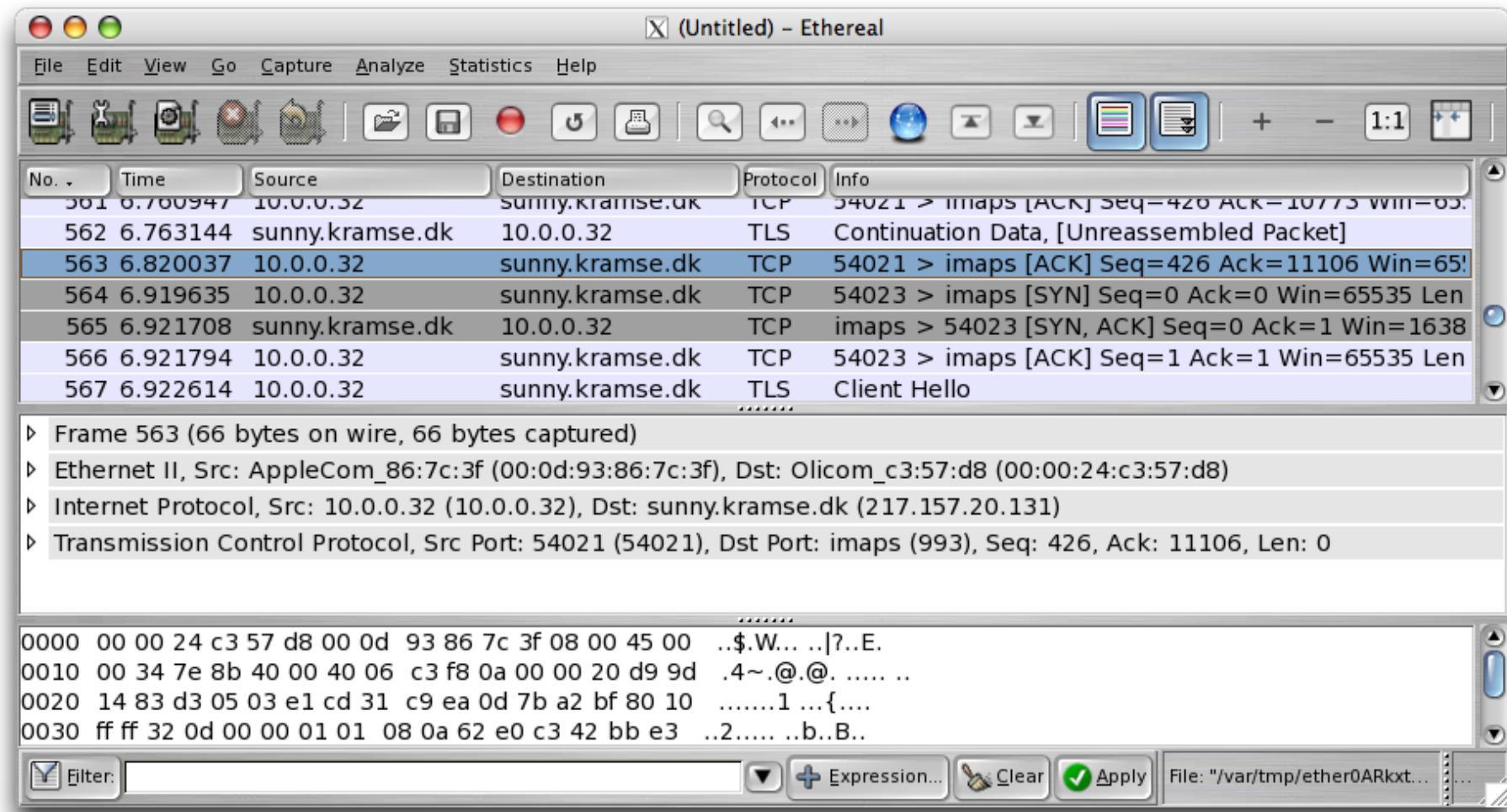

<http://www.wireshark.org>

både til Windows og UNIX, tidligere kendt som Ethereal



Man starter med Capture - Options

# Brug af Wireshark



Læg mærke til filtermulighederne

en sniffer til mange usikre protokoller

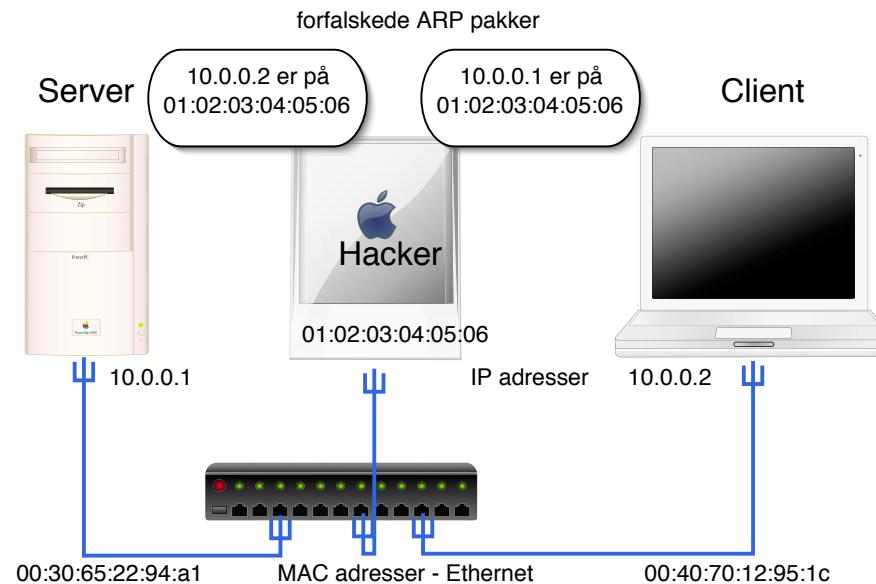
inkluderer **arpspoof**

Lavet af Dug Song, [dugsong@monkey.org](mailto:dugsong@monkey.org)

dsniff is a password sniffer which handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP, MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL\*Net, Sybase and Microsoft SQL protocols.

Der er visse forudsætninger der skal være opfyldt

- Man skal have trafikken
- Det kan gøres gennem arp spoofing eller ved at hacke ind i et system/router på netværksvejen



# Kommenteret dsniff

```
[root@hlk hlk]# dsniff
dsniff: listening on fxp0
-----
05/20/03 08:53:38 tcp client.49154 -> server.110 (pop)
USER hlk
PASS secr3t! Her er opsamlet et kodeord til e-mail
-----
05/20/03 08:54:11 tcp client.49155 -> server.23 (telnet)
[poppe]

hlk
secr3t! Her er opsamlet kodeord og
kommandoer fra en session
ls
exit

-----
05/20/03 08:55:33 tcp client.49156 -> server.23 (telnet)
[poppe]

an ja
an jnaan ja
an ja
```

## Hvad kan man gøre for at få bedre netværkssikkerhed?

- bruge switcher - der skal ARP spoofes og bedre performance
- opdele med firewall til flere DMZ zoner for at holde utsatte servere adskilt fra hinanden, det interne netværk og Internet
- overvåge, læse logs og reagere på hændelser

# Chaosreader

## Chaosreader Report

Created at: Sun Nov 16 21:04:18 2003, Type: snoop

[Image Report](#) - Click here for a report on captured images.

[GET/POST Report](#) (Empty) - Click here for a report on HTTP GETs and POSTs.

[HTTP Proxy Log](#) - Click here for a generated proxy style HTTP log.

### TCP/UDP/... Sessions

1.	Sun Nov 16 20:38:22 2003	30 s	192.168.1.3:1368 <-> 192.77.84.99:80	web	383 bytes	• <a href="#">as html</a>
2.	Sun Nov 16 20:38:22 2003	29 s	192.168.1.3:1366 <-> 192.77.84.99:80	web	381 bytes	• <a href="#">as html</a>

Med adgang til et netværksdump kan man læse det med chaosreader

Output er HTML med oversigter over sessioner, billeder fra datastrømmen osv.

<http://chaosreader.sourceforge.net/>



SSH afløser en række protokoller som er usikre:

- Telnet til terminal adgang
- r\* programmerne, rsh, rcp, rlogin, ...
- FTP med brugerid/password

kommandoerne er:

- ssh - Secure Shell
- scp - Secure Copy
- sftp - secure FTP

Husk: SSH er både navnet på protokollerne - version 1 og 2 samt programmet ssh til at logge ind på andre systemer

SSH tillader også port-forward, tunnel til usikre protokoller, eksempelvis X protokollen til UNIX grafiske vinduer

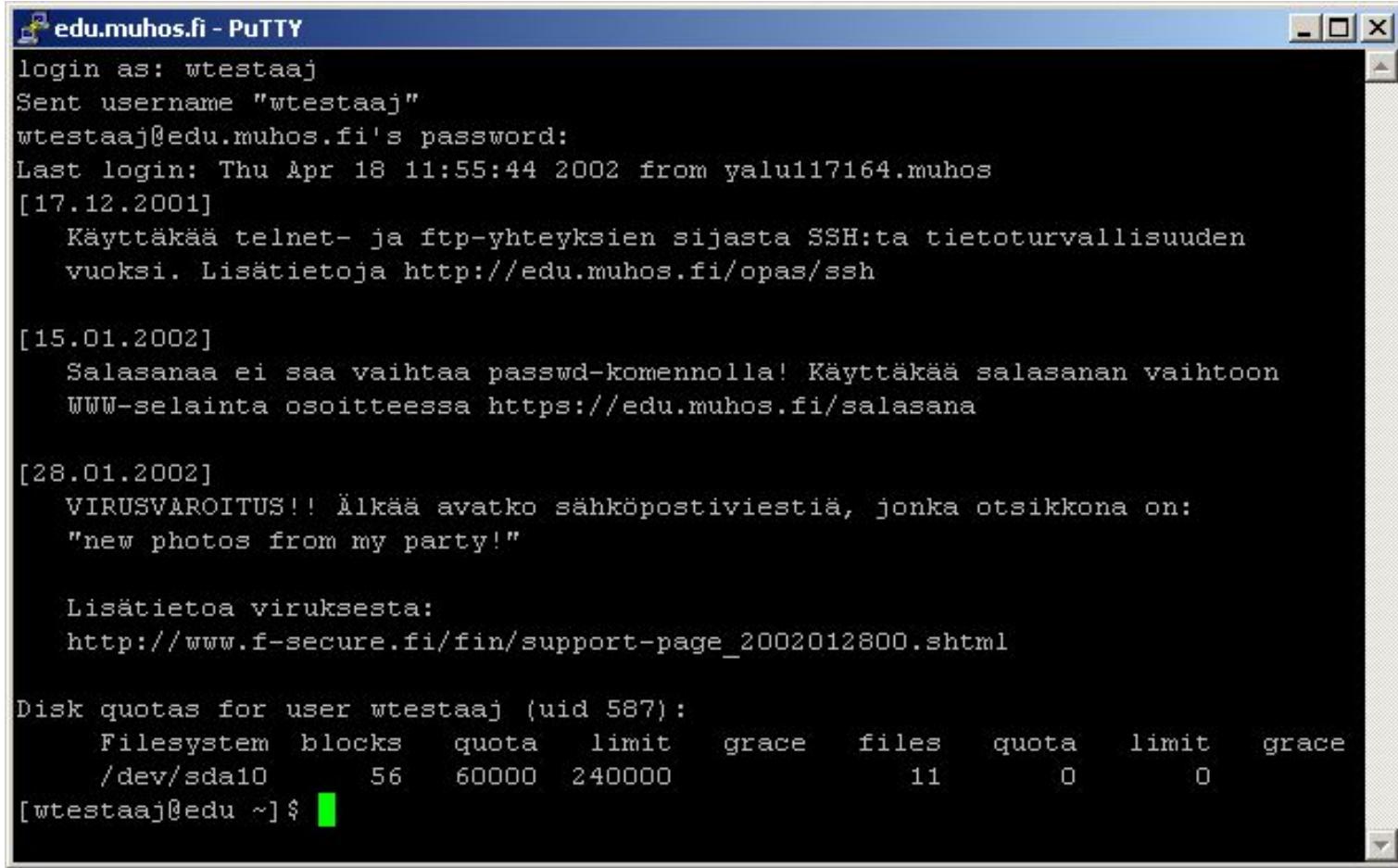
**NB: Man bør idag bruge SSH protokol version 2!**

# Putty en SSH til Windows



Login skærmen til Putty terminal programmet

# Putty terminaladgang



The screenshot shows a PuTTY terminal window titled "edu.muhos.fi - PuTTY". The session is logged in as the user "wtestaaaj". The terminal displays the following text:

```
login as: wtestaaaj
Sent username "wtestaaaj"
wtestaaaj@edu.muhos.fi's password:
Last login: Thu Apr 18 11:55:44 2002 from yalui117164.muhos
[17.12.2001]
    Käyttäkää telnet- ja ftp-yhteyksien sijasta SSH:ta tietoturvallisuuden
    vuoksi. Lisätietoja http://edu.muhos.fi/opas/ssh

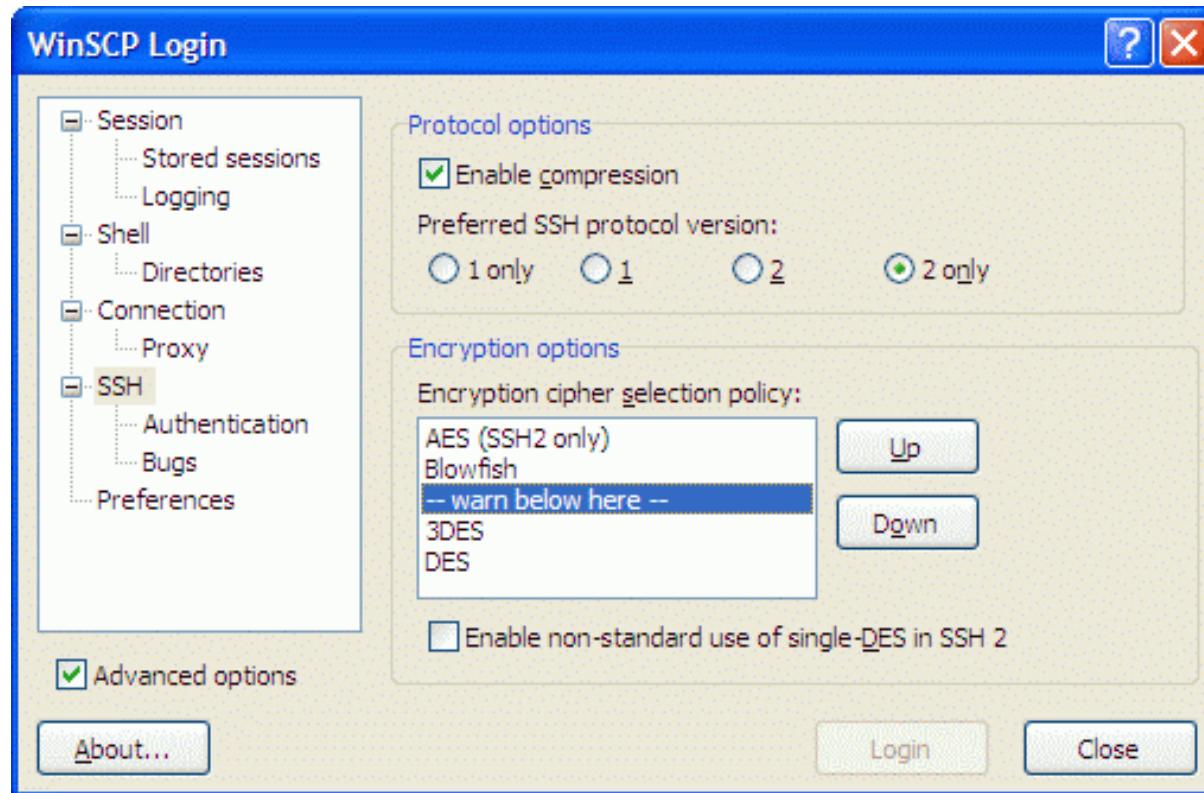
[15.01.2002]
    Salasanaa ei saa vaihtaa passwd-komennoilla! Käyttäkää salasanan vaihtoon
    WWW-selainta osoitteessa https://edu.muhos.fi/salasana

[28.01.2002]
    VIRUSVAROITUS!! Älkää avatko sähköpostiviestiä, jonka otsikkona on:
    "new photos from my party!"

    Lisätietoa viruksesta:
    http://www.f-secure.fi/fin/support-page_2002012800.shtml

Disk quotas for user wtestaaaj (uid 587):
  Filesystem  blocks   quota   limit   grace   files   quota   limit   grace
    /dev/sda10      56    60000   240000           11        0        0        0
[wtestaaaj@edu ~] $
```

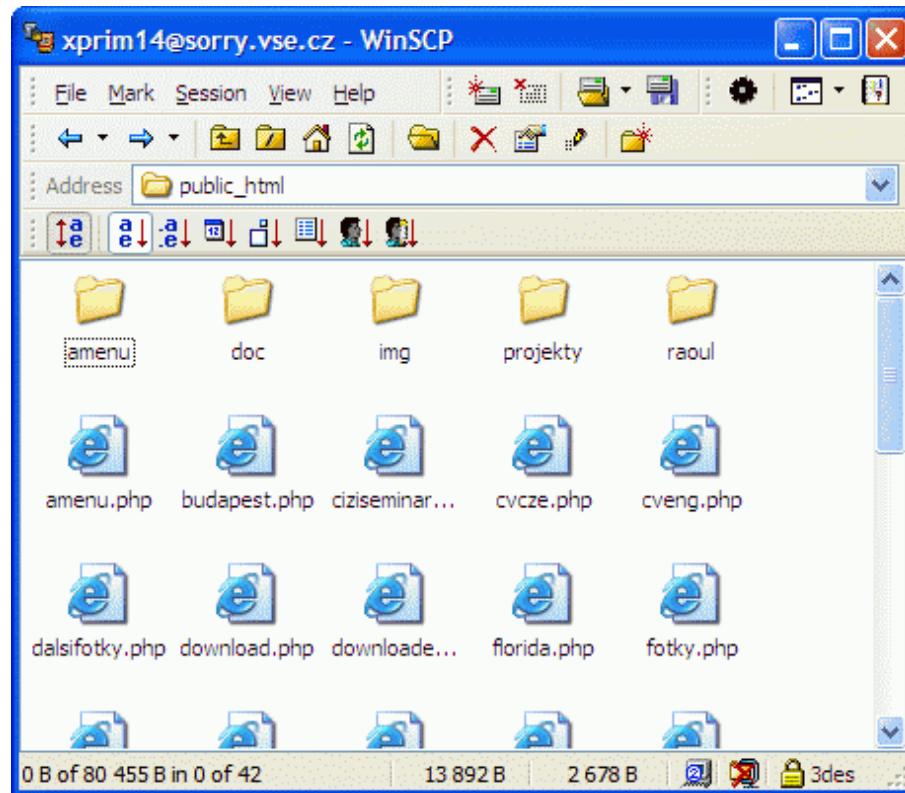
Billede fra <http://edu.muhos.fi/opas/ssh/putty-ohje.htm>



screenshot fra

<http://winscp.vse.cz/eng/screenshots/large/advanced.gif>

# Grafisk Secure Copy - WinSCP



screenshot fra

<http://winscp.vse.cz/eng/screenshots/large/explorer.gif>



Vi laver nu øvelsen

## Putty installation - Secure Shell login

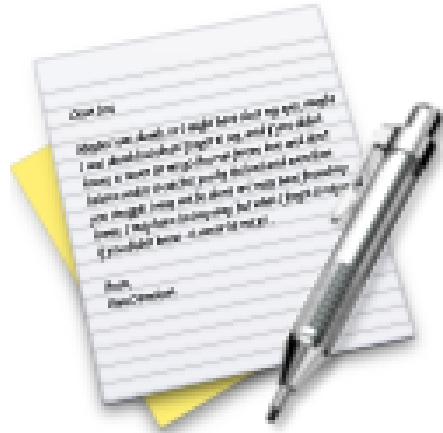
som er øvelse **11** fra øvelseshæftet.



## Vi laver nu øvelsen

# WinSCP installation - Secure Copy

som er øvelse **12** fra øvelseshæftet.



Vi laver nu øvelsen

## Login to Unix server

som er øvelse **13** fra øvelseshæftet.



Vi laver nu øvelsen

## Get to know some Unix

som er øvelse **14** fra øvelseshæftet.



Vi laver nu øvelsen

## Access the root on Unix

som er øvelse **15** fra øvelseshæftet.



Vi laver nu øvelsen  
**Unix boot DVD**  
som er øvelse **16** fra øvelseshæftet.



Vi laver nu øvelsen

## Wireshark installation

som er øvelse **17** fra øvelseshæftet.



Vi laver nu øvelsen

## Sniffing network packets

som er øvelse **18** fra øvelseshæftet.

traceroute programmet virker ved hjælp af TTL

levetiden for en pakke tælles ned i hver router på vejen og ved at sætte denne lavt opnår man at pakken *timer ud* - besked fra hver router på vejen

default er UDP pakker på Unix

default er ICMP pakker på Windows, tracert kommandoen

BackTrack giver mulighed for at bruge UDP, TCP, ICMP

# traceroute - med UDP

```
# tcpdump -i en0 host 217.157.20.129 or host 10.0.0.11
tcpdump: listening on en0
23:23:30.426342 10.0.0.200.33849 > router.33435: udp 12 [ttl 1]
23:23:30.426742 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.436069 10.0.0.200.33849 > router.33436: udp 12 [ttl 1]
23:23:30.436357 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.437117 10.0.0.200.33849 > router.33437: udp 12 [ttl 1]
23:23:30.437383 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.437574 10.0.0.200.33849 > router.33438: udp 12
23:23:30.438946 router > 10.0.0.200: icmp: router udp port 33438 unreachable
23:23:30.451319 10.0.0.200.33849 > router.33439: udp 12
23:23:30.452569 router > 10.0.0.200: icmp: router udp port 33439 unreachable
23:23:30.452813 10.0.0.200.33849 > router.33440: udp 12
23:23:30.454023 router > 10.0.0.200: icmp: router udp port 33440 unreachable
23:23:31.379102 10.0.0.200.49214 > safri.domain: 6646+ PTR?

200.0.0.10.in-addr.arpa. (41)
23:23:31.380410 safri.domain > 10.0.0.200.49214: 6646 NXDomain* 0/1/0 (93)
14 packets received by filter
0 packets dropped by kernel
```

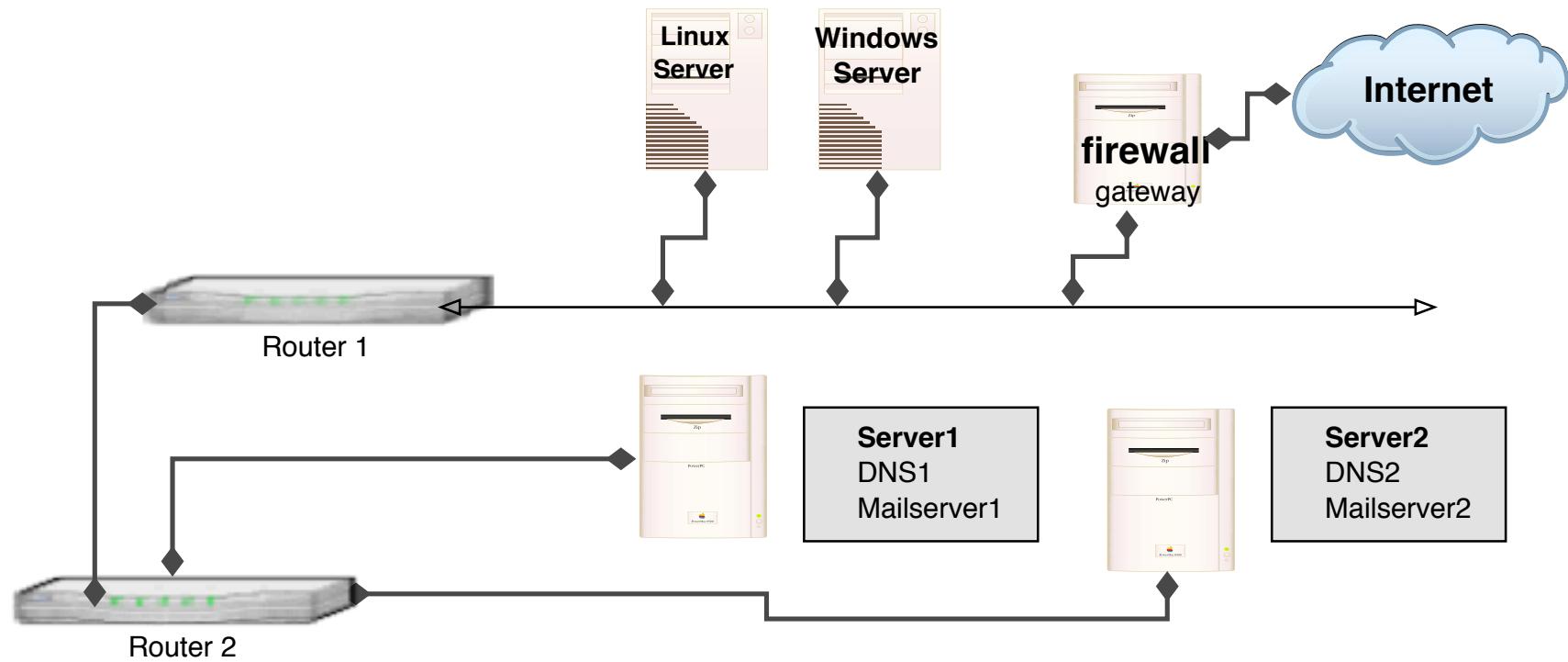
diagnosticering af netværksproblemer - formålet med traceroute

indblik i netværkets opbygning!

svar fra hosts - en modtaget pakke fremfor et *sort hul*

traceroute er ikke et angreb - det er også vigtigt at kunne genkende normal trafik!

# Network mapping



Ved brug af traceroute og tilsvarende programmer kan man ofte udlede topologien i det netværk man undersøger

Der findes mange specialiserede trace programmer til diverse formål

Eksempel: dnstracer information om DNS servere

```
# dnstracer -r . www.security6.net
Strange amount of retries, setting to default
Tracing to www.security6.net via 10.0.0.11, timeout 15 seconds
10.0.0.11 (10.0.0.11)
|__ H.GTLD-SERVERS.net [net] (192.54.112.30)
|   |__ NS6.GANDI.net [security6.net] (80.67.173.196) * * *
|   __ NS1.security6.net [security6.net] (217.157.20.130)
|       |__ B.GTLD-SERVERS.net [net] (192.33.14.30)
|       |   |__ NS6.GANDI.net [security6.net] ...
```

mtr My traceroute - grafisk <http://www.bitwizard.nl/mtr/>

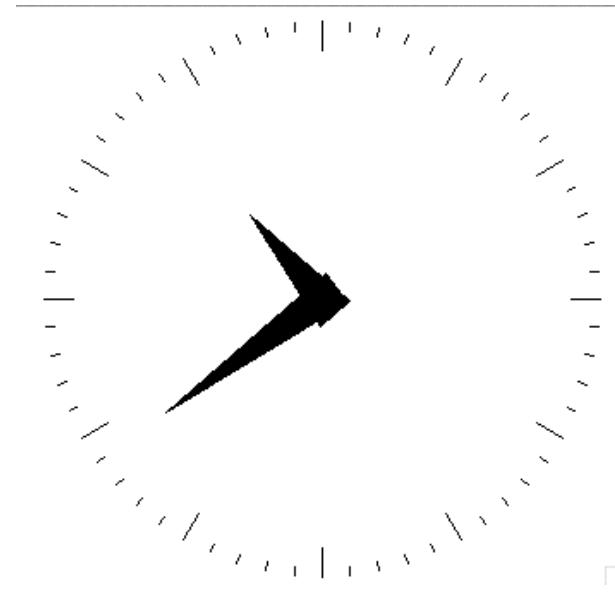
Ift - *layer four trace* benytter TCP SYN og FIN prober

trace ved hjælp af TCP og andre protokoller findes

paratrace - *Parasitic Traceroute via Established TCP Flows and IPID Hopcount*

Der findes webservices hvor man kan trace fra, eksempelvis:

<http://www.traceroute.org>



Hvad er klokken?

Hvad betydning har det for sikkerheden?

Brug NTP Network Time Protocol på produktionssystemer

ICMP timestamp option - request/reply

hvad er klokken på en server

Slayer icmpush - er installeret på server

viser tidstempel

```
# icmpush -v -tstamp 10.0.0.12
```

```
ICMP Timestamp Request packet sent to 10.0.0.12 (10.0.0.12)
```

```
Receiving ICMP replies ...
```

```
fischer          -> 21:27:17
```

```
icmpush: Program finished OK
```



Vi laver nu øvelsen

## Discovery using ping and traceroute

som er øvelse **19** fra øvelseshæftet.



Vi laver nu øvelsen

## ICMP tool - icmpush

som er øvelse **20** fra øvelseshæftet.

Det vi har udført er informationsindsamling

Indsamlingen kan være aktiv eller passiv indsamling i forhold til målet for angrebet  
passiv kunne være at lytte med på trafik eller søge i databaser på Internet  
aktiv indsamling er eksempelvis at sende ICMP pakker og registrere hvad man får af svar

00-03-93	(hex)	Apple Computer, Inc.
000393	(base 16)	Apple Computer, Inc. 20650 Valley Green Dr. Cupertino CA 95014 UNITED STATES

Netværksteknologierne benytter adresser på lag 2

Typisk svarende til 48-bit MAC adresser som kendes fra Ethernet MAC-48/EUI-48

Første halvdel af adresserne er Organizationally Unique Identifier (OUI)

Ved hjælp af OUI kan man udlede hvilken producent der har produceret netkortet

<http://standards.ieee.org/regauth/oui/index.shtml>

# IPv4 pakken - header - RFC-791

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1
Version   IHL   Type of Service		Total Length	
Identification   Flags   Fragment Offset			
Time to Live   Protocol   Header Checksum			
Source Address			
Destination Address			
Options		Padding	

## Example Internet Datagram Header



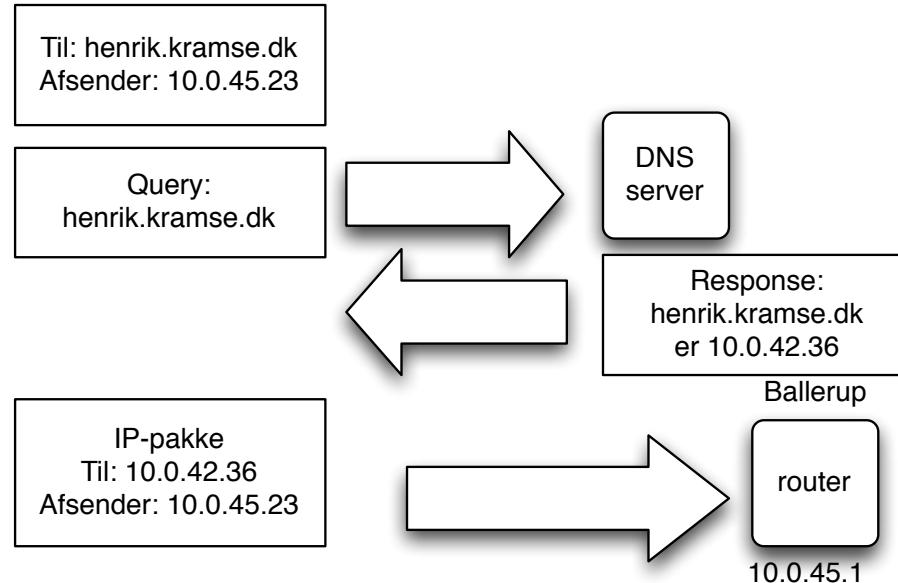
IANA vedligeholder en liste over magiske konstanter i IP

De har lister med hvilke protokoller har hvilke protokol ID m.v.

En liste af interesse er port numre, hvor et par eksempler er:

- Port 25 SMTP Simple Mail Transfer Protocol
- Port 53 DNS Domain Name System
- Port 80 HTTP Hyper Text Transfer Protocol over TLS/SSL
- Port 443 HTTP over TLS/SSL

Se flere på <http://www.iana.org>



En DNS server kan slå navne, domæner og adresser op

Foregår via query og response med datatyper kaldet resource records

DNS er en distribueret database, så opslag kan resultere i flere opslag

navneopslag på Internet

tidligere brugte man en **hosts** fil

hosts filer bruges stadig lokalt til serveren - IP-adresser

UNIX: /etc/hosts

Windows c:\windows\system32\drivers\etc\hosts

Eksempel: www.solido.net har adressen 91.102.95.20

skrives i database filer, zone filer

ns1	IN	A	91.102.95.95
IN	AAAA	2a02:9d0:10::9	
www	IN	A	91.102.95.20
IN	AAAA	2a02:9d0:10::9	

består af resource records med en type:

- adresser A-records, fra navn til IP
- PTR reverse records, fra IP til navn
- IPv6 adresser AAAA-records
- autoritative navneservere NS-records
- post, mail-exchanger MX-records
- flere andre: md , mf , cname , soa , mb , mg , mr , null , wks , ptr , hinfo , minfo , mx ....

IN	MX	10	mail.security6.net.
IN	MX	20	mail2.security6.net.

## Root-servere - 13 stk geografisk distribueret fordelt på Internet

I.ROOT-SERVERS.NET.	3600000	A	192.36.148.17
E.ROOT-SERVERS.NET.	3600000	A	192.203.230.10
D.ROOT-SERVERS.NET.	3600000	A	128.8.10.90
A.ROOT-SERVERS.NET.	3600000	A	198.41.0.4
H.ROOT-SERVERS.NET.	3600000	A	128.63.2.53
C.ROOT-SERVERS.NET.	3600000	A	192.33.4.12
G.ROOT-SERVERS.NET.	3600000	A	192.112.36.4
F.ROOT-SERVERS.NET.	3600000	A	192.5.5.241
B.ROOT-SERVERS.NET.	3600000	A	128.9.0.107
J.ROOT-SERVERS.NET.	3600000	A	198.41.0.10
K.ROOT-SERVERS.NET.	3600000	A	193.0.14.129
L.ROOT-SERVERS.NET.	3600000	A	198.32.64.12
M.ROOT-SERVERS.NET.	3600000	A	202.12.27.33

bestyrer .dk TLD - top level domain

man registrerer ikke .dk-domæner hos DK-hostmaster, men hos en registrator

Et domæne bør have flere navneservere og flere postservere

autoritativ navneserver - ved autoritativt om IP-adresse for maskine.domæne.dk findes

ikke-autoritativ - har på vegne af en klient slået en adresse op

Det anbefales at overveje en service som <http://www.gratisdns.dk> der har 5 navneservere distribueret over stor geografisk afstand - en udenfor Danmark

```
#!/bin/sh
# Try to get version info from BIND server
PROGRAM=`basename $0`
. `dirname $0`/functions.sh
if [ $# -ne 1 ]; then
    echo "get name server version, need a target! "
    echo "Usage: $0 target"
    echo "example $0 10.1.2.3"
    exit 0
fi
TARGET=$1
# using dig
start_time
dig @$1 version.bind chaos txt
echo Authors BIND er i versionerne 9.1 og 9.2 - måske ...
dig @$1 authors.bind chaos txt
stop_time
http://www.kramse.dk/files/tools/dns/bind-version
```

# Små DNS tools dns-timecheck - Perl script

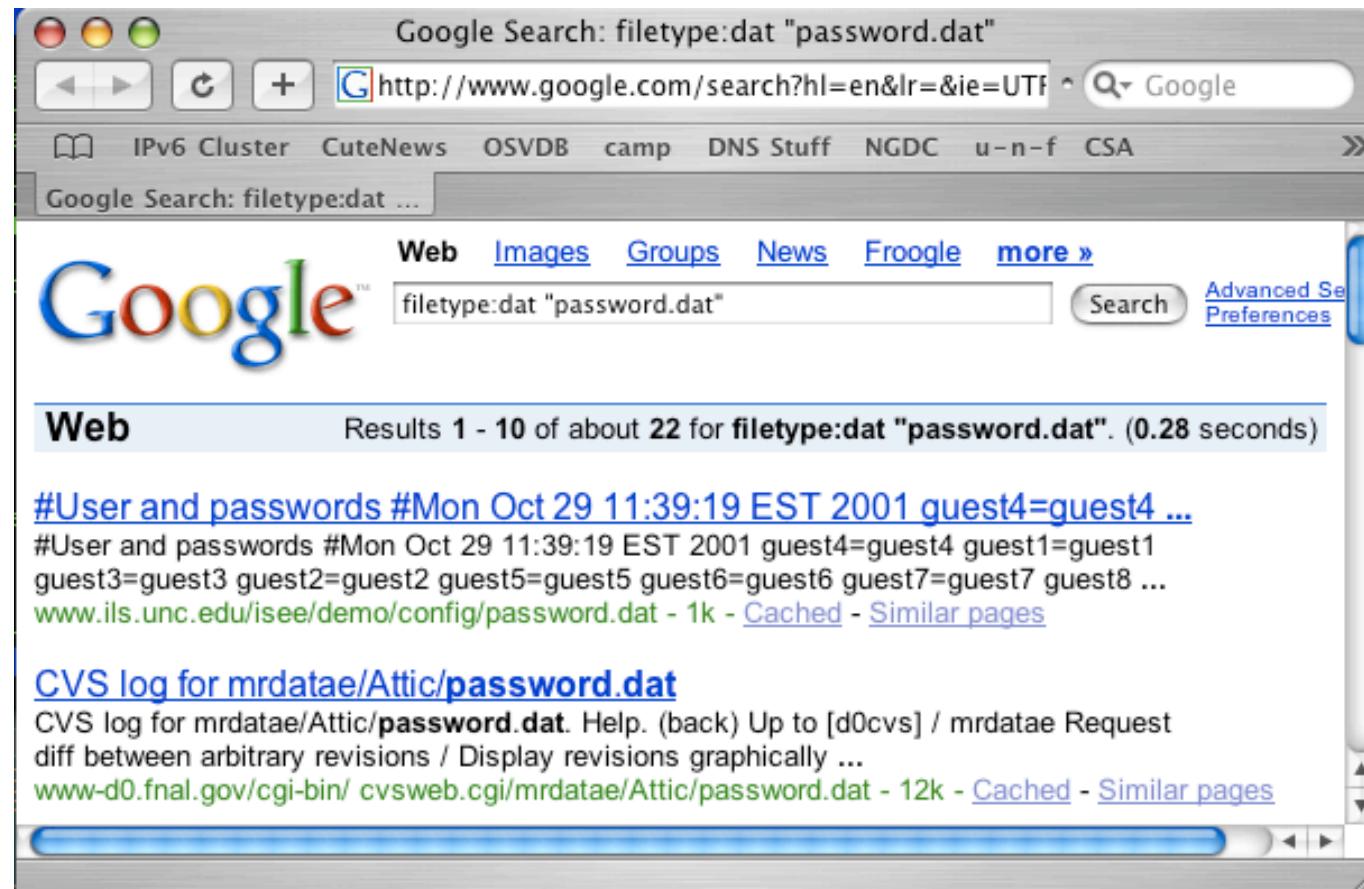
```
#!/usr/bin/perl
# modified from original by Henrik Kramshøj, hlk@kramse.dk
# 2004-08-19
#
# Original from: http://www.rfc.se/fpdns/timecheck.html
use Net::DNS;

my $resolver = Net::DNS::Resolver->new;
$resolver->nameservers ($ARGV[0] );

my $query = Net::DNS::Packet->new;
$query->sign_tsig("n", "test");

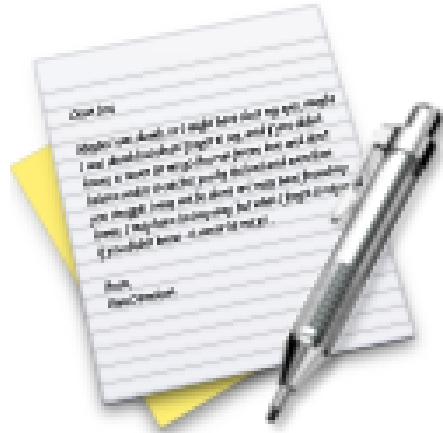
my $response = $resolver->send($query);
foreach my $rr ($response->additional)
    print "localtime vs nameserver $ARGV[0] time difference: ";
    print $rr->time_signed - time() if $rr->type eq "TSIG";
```

<http://www.kramse.dk/files/tools/dns/dns-timecheck>



Google som hacker værktøj?

Googledorks <http://johnny.ihackstuff.com/>



Vi laver nu øvelsen

## Discover using DNS

som er øvelse **21** fra øvelseshæftet.



Vi laver nu øvelsen

## Try the bind-version shell script

som er øvelse **22** fra øvelseshæftet.



## Vi laver nu øvelsen

# Try the dns-timecheck Perl program

som er øvelse **23** fra øvelseshæftet.

Hvad er portscanning

afprøvning af alle porte fra 0/1 og op til 65535

målet er at identificere åbne porte - sårbare services

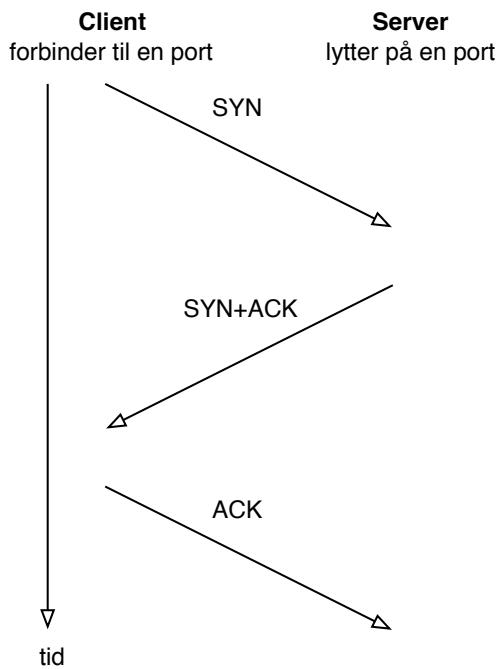
typisk TCP og UDP scanning

TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

# TCP three way handshake



- **TCP SYN half-open scans**
- Tidligere loggede systemer kun når der var etableret en fuld TCP forbindelse - dette kan/kunne udnyttes til *stealth*-scans
- Hvis en maskine modtager mange SYN pakker kan dette fylde tabellen over connections op - og derved afholde nye forbindelser fra at blive oprette - **SYN-flooding**

scanninger på tværs af netværk kaldes for sweeps

Scan et netværk efter aktive systemer med PING

Scan et netværk efter systemer med en bestemt port åben

Er som regel nemt at opdage:

- konfigurerer en maskine med to IP-adresser som ikke er i brug
- hvis der kommer trafik til den ene eller anden er det portscan
- hvis der kommer trafik til begge IP-adresser er der nok foretaget et sweep - bedre hvis de to adresser ligger et stykke fra hinanden

## Port 80 TCP er webservere

```
# nmap -p 80 217.157.20.130/28
```

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on router.kramse.dk (217.157.20.129):
```

Port	State	Service
80/tcp	filtered	http

```
Interesting ports on www.kramse.dk (217.157.20.131):
```

Port	State	Service
80/tcp	open	http

```
Interesting ports on (217.157.20.139):
```

Port	State	Service
80/tcp	open	http

# nmap port sweep after port 161/UDP

Port 161 UDP er SNMP

```
# nmap -sU -p 161 217.157.20.130/28
```

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on router.kramse.dk (217.157.20.129):
Port      State       Service
161/udp   open        snmp
```

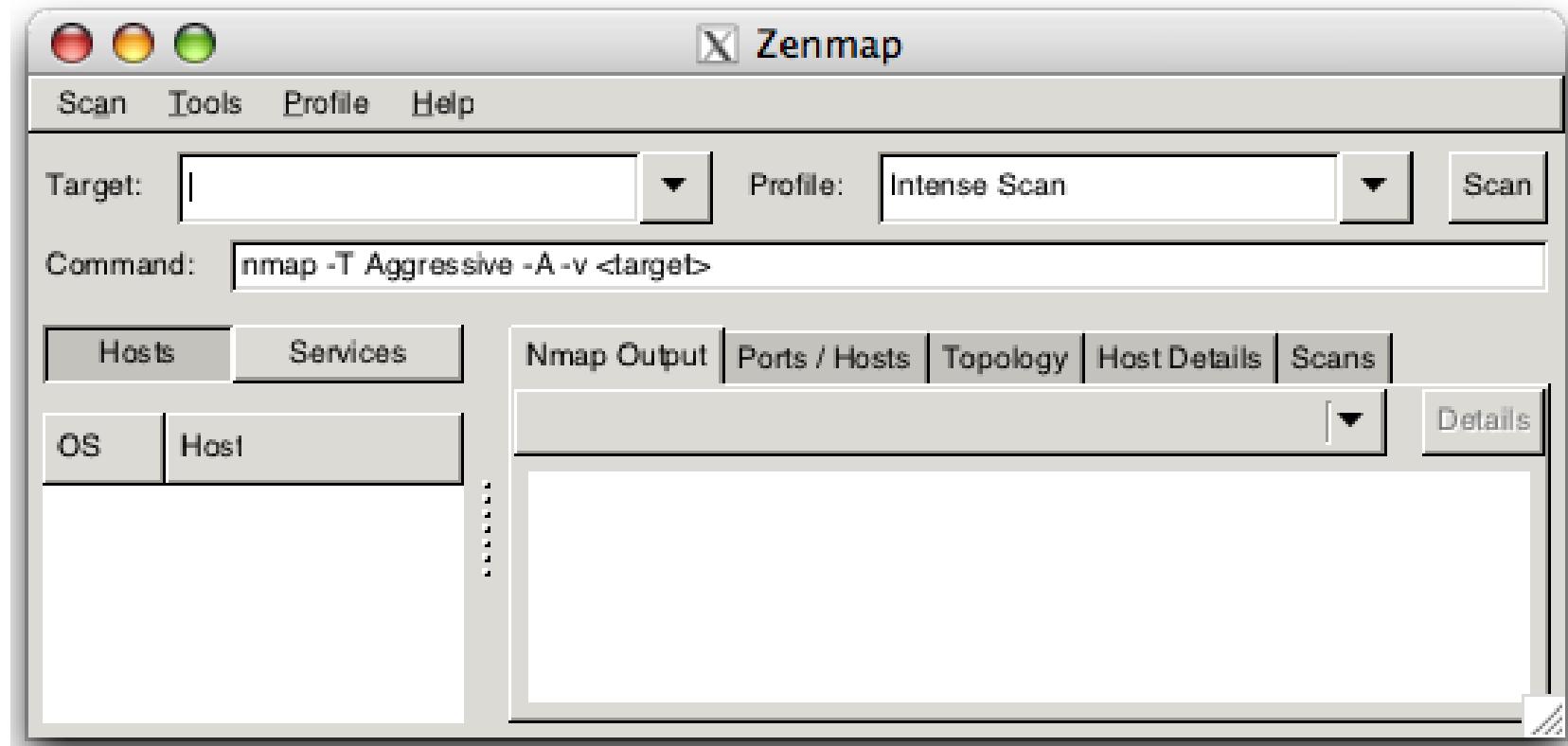
The 1 scanned port on mail.kramse.dk (217.157.20.130) is: closed

```
Interesting ports on www.kramse.dk (217.157.20.131):
Port      State       Service
161/udp   open        snmp
```

The 1 scanned port on (217.157.20.132) is: closed

```
# nmap -O ip.adresse.slet.tet scan af en gateway
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-03 11:31 CET
Interesting ports on gw-int.security6.net (ip.adresse.slet.tet):
(The 1653 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1080/tcp  open  socks
5000/tcp  open  UPnP
Device type: general purpose
Running: FreeBSD 4.X
OS details: FreeBSD 4.8-STABLE
Uptime 21.178 days (since Wed Nov 12 07:14:49 2003)
Nmap run completed -- 1 IP address (1 host up) scanned in 7.540 seconds
```

- lavniveau måde at identificere operativsystemer på
- send pakker med *anderledes* indhold
- Reference: *ICMP Usage In Scanning* Version 3.0, Ofir Arkin  
<http://www.sys-security.com/html/projects/icmp.html>



Vi bruger Zenmap til at scanne med, GUI til Nmap



Vi laver nu øvelsen

## Discover active systems ping sweep

som er øvelse **24** fra øvelseshæftet.



Vi laver nu øvelsen

## Execute nmap TCP and UDP port scan

som er øvelse **25** fra øvelseshæftet.



Vi laver nu øvelsen

## Perform nmap OS detection

som er øvelse **26** fra øvelseshæftet.



Vi laver nu øvelsen

## Perform nmap service scan

som er øvelse **27** fra øvelseshæftet.

mange oplysninger

kan man stykke oplysningerne sammen kan man sige en hel del om netværket

en skabelon til registrering af maskiner er god

- svarer på ICMP:  echo,  mask,  time
- svarer på traceroute:  ICMP,  UDP
- Åbne porte TCP og UDP:
- Operativsystem:
- ... (banner information m.v.)

Mange små pakker kan oversvømme store forbindelser og give problemer for netværk

hvor og hvordan kan I bruge penetrationstest

hvis man vil have et andet indblik i netværket, TCP, UDP, ICMP, portscanning og samle puslespil udfra få informationer

Netværksadministratorer kan bruge pentesting til at sikre egne netværk ved brug af samme teknikker som hackere

Pentesting er ikke kun til test af produktionsnetværk

man skal ofte vurdere nye produkter - sikkerhedsmæssigt og funktionalitetsmæssigt - yder det beskyttelse, forbedrer det sikkerheden m.v.

Man står med en server der er kompromitteret - hvordan skete det? - hvordan forhindrer vi det en anden gang.

Problem:

Ønsker et simpelt CGI program, en web udgave af finger

Formål:

Vise oplysningerne om brugere på systemet

Vi bruger Web applikationer som eksempel!

ASP, PHP, Ruby on Rails m.fl.

- server scripting, meget generelt - man kan alt

SQL

- databasesprog - meget kraftfuldt
- mange databasesystemer giver mulighed for specifik tildeling af privilegier "grant"

JAVA

- generelt programmeringssprog
- bytecode verifikation
- indbygget sandbox funktionalitet

Perl og andre generelle programmeringssprog

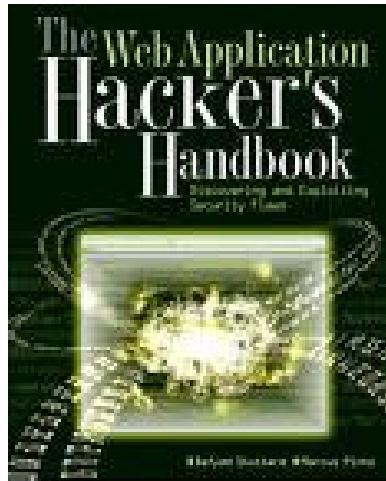
Pas på shell escapes!!!

Demo af et sårbart system - badfinger

Løsning:

- Kalde finger kommandoen
- et Perl script
- afvikles som CGI
- standard Apache HTTPD 1.3 server

```
print "Content-type: text/html <html>";
print "<body bgcolor=#666666 leftmargin=20 topmargin=20";
print <<XX;
<h1>Bad finger command!</h1>
<HR COLOR=#000>
<form method="post" action="bad_finger.cgi">
Enter userid: <input type="text" size="40" name="command">
</form>
<HR COLOR=#000>
XX
if (&ReadForm(*input))
    print "<pre>";
    print "will execute: /usr/bin/finger $input{'command'}";
    print "<HR COLOR=#000>";
    print '/usr/bin/finger $input{'command'}';
    print "<pre>";
```



*The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws*  
Dafydd Stuttard, Marcus Pinto, Wiley 2007 ISBN: 978-0470170779

# Hvordan udnyttes forms nemmest?

Manuelt download form:

```
<FORM ACTION="opret.asp?mode=bruger?id=doopret"  
METHOD="POST" NAME="opret"  
ONSUBMIT="return validate(this)">
```

fjern kald til validering:

```
<FORM ACTION="opret.asp?mode=bruger?id=doopret"  
METHOD="POST" NAME="opret">
```

Tilføj 'BASE HREF' i header, findes med browser - højreklik properties i Internet Explorer

# Hvordan udnyttes forms nemmest?

Den form som man bruger er så - fra sin lokale harddisk:

```
<HEAD>
<TITLE>Our Products</TITLE>
<BASE href="http://www.target.server/sti/til/form">
</HEAD>
...
<FORM ACTION="opret.asp?mode=bruger?id=doopret"
METHOD="POST" NAME="opret">
```

Kald form i en browser og indtast værdier

Man bliver hurtigt træt af at ændre forms på den måde

Istedet anvendes en masse proxyprogrammer

Nogle af de mest kendte er:

- Burp proxy
- Parox proxy
- Firefox extension tamper data
- OWASP WebScarab

webroot er det sted på harddisken, hvorfra data der vises af webserveren hentes.

Unicode bug:

`http://10.0.43.10/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:`

Kilde:

`http://www.cgisecurity.com/archive/misc/unicode.txt` - rain forest  
puppy

`http://online.securityfocus.com/bid/1806/info/` - securityfocus info

Hvorfor er programmerne stadig sårbare?

RFP exploits - adgang til kommandolinien via database

? :\Program Files\Common Files\System\Msadc\msadcs.dll

Unicode - fejl i håndtering af specialtilfælde

double decode - flere fejl i håndtering af nye specialtilfælde

Dark spyrit jill.c - Internet Printing Protocol IPP. Ny funktionalitet som implementeres med fejl

**Programmer idag er komplekse!**

## IIS track record

- meget funktionalitet
- større risiko for fejl
- alvorlige fejl - arbitrary code execution

## Apache track record

- typisk mindre funktionalitet
- typisk haft mindre alvorlige fejl

## PHP track record?

Sammenligning IIS med Apache+PHP, idet en direkte sammenligning mellem IIS og Apache vil være unfair

## **Meget få har idag små websteder med statisk indhold**

Både IIS version 6 og Apache version 2 anbefales idag, fremfor tidligere versioner



# w3af

Web Application Attack and Audit Framework

Vi afprøver nu følgende programmer sammen:

Nikto web server scanner <http://cirt.net/nikto2>

W3af Web Application Attack and Audit Framework <http://w3af.sourceforge.net/>

Begge findes på BackTrack



Scanner version: 1.00b Scan date: Thu Mar 18 12:04:42 2010  
Random seed: 0x75573a02 Total time: 0 hr 16 min 46 sec 841 ms

### Crawl results - click to expand:

-  **http://www.example.com/** 0 3 0 2 0 171  
Code: 200, length: 438, declared: text/html, detected: text/html, charset: UTF-8 [[show trace](#) +]  
New 404 signature seen  
1. Code: 404, length: 285, declared: text/html, charset: iso-8859-1 [[show trace](#) +]  
New 'Server' header value seen  
1. Code: 200, length: 438, declared: text/html, charset: UTF-8 [[show trace](#) +]  
Memo: Apache/2.2.3 (CentOS)
-  **error** 0 3 0 5  
Code: 403, length: 288, declared: text/html, detected: text/html, charset: iso-8859-1 [[show trace](#) +]
-  **include** 0 2 0 3  
Code: 403, length: 296, declared: text/html, detected: text/html, charset: iso-8859-1 [[show trace](#) +]
-  **README** 0 0 1  
Code: 200, length: 1979, declared: text/plain, detected: text/plain, charset: UTF-8 [[show trace](#) +]
-  **icons** 0 164  
Code: 200, length: 30034, declared: text/html, detected: text/html, charset: ISO-8859-1 [[show trace](#) +]

### Document type overview - click to expand:

-  **application/xhtml+xml** (1)
-  **image/gif** (5)
-  **image/png** (2)

Vi afprøver nu følgende program sammen:

Skipfish fully automated, active web application security reconnaissance tool.

Af Michal Zalewski <http://code.google.com/p/skipfish/>

Husk hidden fields er ikke mere skjulte end "view source"-knappen i browseren  
serverside validering er nødvendigt

SQL injection er nemt at udføre og almindeligt

Cross-site scripting kan have uanede muligheder

Brug top 10 listen fra <http://www.owasp.org>

Brug WebGoat fra OWASP til at lære mere om Websikkerhed

## Hacking, buffer overflows, scannerværktøjer

SNMP er en protokol der supporteres af de fleste professionelle netværksenheder, såsom switcher, routere

hosts - skal slås til men følger som regel med

SNMP bruges til:

- *network management*
- statistik
- rapportering af fejl - SNMP traps

**sikkerheden baseres på community strings der sendes som klartekst ...**

det er nemmere at brute-force en community string end en brugerid/kodeord kombination

## hvad betyder bruteforcing? afprøvning af alle mulighederne

Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>

Syntax: hydra [[[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]  
[-o FILE] [-t TASKS] [-g TASKS] [-T SERVERS] [-M FILE] [-w TIME]  
[-f] [-e ns] [-s PORT] [-S] [-vV] server service [OPT]

Options:

- S connect via SSL
- s PORT if the service is on a different default port, define it here
- l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
- p PASS or -P FILE try password PASS, or load several passwords from FILE
- e ns additional checks, "n" for null password, "s" try login as pass
- C FILE colon seperated "login:pass" format, instead of -L/-P option
- M FILE file containing server list (parallizes attacks, see -T)
- o FILE write found login/password pairs to FILE instead of stdout

...

routing table - tabel over netværkskort og tilhørende adresser

default gateway - den adresse hvortil man sender *non-local* pakker  
kaldes også default route, gateway of last resort

routing styres enten manuelt - opdatering af route tabellen, eller konfiguration af adresser og subnet maske på netkort

eller automatisk ved brug af routing protocols - interne og eksterne route protokoller

de lidt ældre routing protokoller har ingen sikkerhedsmekanismer

source routing - mulighed for at specificere en ønsket vej for pakken

Hvis en angriber kan fortælle hvilken vej en pakke skal følge kan det give anledning til sikkerhedsproblemer

maskiner idag bør ikke lytte til source routing, evt. skal de droppe pakkerne

falske routing updates til protokollerne

sende redirect til maskiner

Der findes (igen) specialiserede programmer til at teste og forfalske routing updates, svarende til icmpush programmet

Det anbefales at sikre routere bedst muligt - eksempelvis Secure IOS template der findes på adressen:

<http://www.cymru.com/Documents/secure-ios-template.html>

All your packets are belong to us - Attacking backbone technologies

Daniel Mende & Enno Rey fra ERNW i Tyskland <http://www.ernw.de>



Vi laver nu øvelsen

## Find systems with SNMP

som er øvelse **28** fra øvelseshæftet.



Vi laver nu øvelsen

## Try Hydra brute force

som er øvelse **29** fra øvelseshæftet.



Vi laver nu øvelsen

## Try Cain brute force

som er øvelse **30** fra øvelseshæftet.

## Cisco routere - ude af drift angreb - juli 2003

- Med en bestemt sekvens af pakker til routerens egen adresse på et interface kan den bringes i en tilstand hvor den ikke sender pakker videre - dødt interface
- *This issue affects all Cisco devices running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets. This includes routers as well as switches and line cards which run Cisco IOS software. Cisco devices which do not run Cisco IOS software are not affected.*
- kræver genstart
- pakkerne kan sågar genereres med et shellscript (batch fil) og programmer som hping

## Kilder:

<http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml>  
<http://www.cert.org/advisories/CA-2003-15.html>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0567>

```
#!/bin/sh
# 2003-07-21 pdonahue
# cisco-44020.sh
# -- this shell script is just a wrapper for hping (http://www.hping.org)
# with the parameters necessary to fill the input queue on
# exploitable IOS device
# -- refer to "Cisco Security Advisory: Cisco IOS Interface Blocked by
# IPv4 Packets"
# (http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml)
#for more information
...
for protocol in $PROT
do
    $HPING $HOST --rawip $ADDR --ttl $TTL --ipproto $protocol
    --count $NUMB --interval u250 --data $SIZE --file /dev/urandom
done
```

Hvorfor afvikle applikationer med administrationsrettigheder - hvis der kun skal læses fra eksempelvis en database?

**least privilege** betyder at man afvikler kode med det mest restriktive sæt af privileger - kun lige nok til at opgaven kan udføres

Dette praktiseres ikke i webløsninger i Danmark - eller meget få steder

**privilege escalation** er når man på en eller anden vis opnår højere privileger på et system, eksempelvis som følge af fejl i programmer der afvikles med højere privilegier. Derfor HTTPD servere på UNIX afvikles som nobody - ingen specielle rettigheder.

En angriber der kan afvike vilkårlige kommandoer kan ofte finde en sårbarhed som kan udnyttes lokalt - få rettigheder = lille skade

når vi scanner efter services går det nemt med at finde dem

Giv jer selv mere tid til at omkonfigurere og opdatere ved at undgå standardindstillinger

Tiden der går fra en sårbarhed annonceres på bugtraq til den bliver udnyttet er meget kort idag!

Ved at undgå standard indstillinger kan der måske opnås en lidt længere frist - inden ormene kommer

NB: ingen garanti - og det hjælper sjældent mod en dedikeret angriber

# Matrix the movie Trinity breaking in

```
80/tcp      open     http  
81/tcp      open     hostx2_anc  
10  [mobile]  
11 $ nmap -v -sS -O 10.2.2.2  
11  
13 Starting nmap 0.2.54BETA25  
13 Insufficient responses for TCP sequencing (3). OS detection is  
13 inaccurate  
14 Interesting ports on 10.2.2.2:  
14 (The 1539 ports scanned but not shown below are in state: cle  
51 Port      State       Service  
51 22/tcp    open        ssh  
58  
68 No exact OS matches for host  
68  
24 Nmap run completed -- 1 IP address (1 host up) scanned  
50 $ sshhuhnke 10.2.2.2 -rootpw="Z10H0101"  
Connecting to 10.2.2.2:ssh ... successful.  
Re  
IP Attempting to exploit SSHv1 CRC32 ... successful.  
Reseting root password to "Z10H0101".  
System open: Access Level <9>  
Hn $ ssh 10.2.2.2 -l root  
root@10.2.2.2's password: 
```

<http://nmap.org/movies.html>

Meget realistisk [http://www.youtube.com/watch?v=Zy5\\_gYu\\_isg](http://www.youtube.com/watch?v=Zy5_gYu_isg)

**Et buffer overflow** er det der sker når man skriver flere data end der er afsat plads til i en buffer, et dataområde. Typisk vil programmet gå ned, men i visse tilfælde kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

**Stack protection** er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

exploit/exploitprogram er

- udnytter eller demonstrerer en sårbarhed
- rettet mod et specifikt system.
- kan være 5 linier eller flere sider
- Meget ofte Perl eller et C program

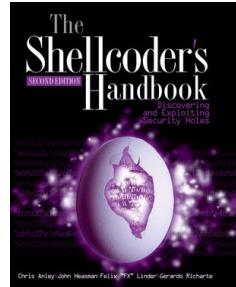
Eksempel:

```
#!/usr/bin/perl
# ./chars.pl | nc server 31337
print "abcdefghijkl";
print chr(237);
print chr(13);
print chr(220);
print chr(186);
print "\n";
```

**local vs. remote** angiver om et exploit er rettet mod en sårbarhed lokalt på maskinen, eksempelvis opnå højere privilegier, eller beregnet til at udnytter sårbarheder over netværk

**remote root exploit** - den type man frygter mest, idet det er et exploit program der når det afvikles giver angriberen fuld kontrol, root user er administrator på UNIX, over netværket.

**zero-day exploits** dem som ikke offentliggøres - dem som hackere holder for sig selv. Dag 0 henviser til at ingen kender til dem før de offentliggøres og ofte er der umiddelbart ingen rettelser til de sårbarheder



Hvis man vil lære at lave buffer overflows og exploit programmer er følgende dokumenter et godt sted at starte

*Smashing The Stack For Fun And Profit* Aleph One

*Writing Buffer Overflow Exploits with Perl - anno 2000*

Følgende bog kan ligeledes anbefales: *The Shellcoder's Handbook : Discovering and Exploiting Security Holes* af Jack Koziol, David Litchfield, Dave Aitel, Chris Anley, Sinan "noir" Eren, Neel Mehta, Riley Hassell, John Wiley & Sons, 2004

NB: bogen er avanceret og således IKKE for begyndere!

[ home ] [ contents ] [ platforms ] [ shellcode ] [ search ] [ cracker ] [ links ] [ rss ] [ archive ]

# MILWORM

[ highlighted ]

-::DATE	-::DESCRIPTION	-::HITS	-::AUTHOR
2009-03-05	Winamp <= 5.541 Skin Universal Buffer Overflow Exploit	3128	R D SkD
2009-02-26	Coppermine Photo Gallery <= 1.4.20 (BBCode IMG) Privilege Escalation	7338	R D StAkeR
2009-02-25	Apple MACOS X xnu <= 1228.x Local Kernel Memory Disclosure Exploit	4111	R D mu-b
2009-02-23	Adobe Acrobat Reader JBIG2 Local Buffer Overflow PoC #2 0day	17652	R D Guido Landi
2009-02-23	MLdonkey <= 2.9.7 HTTP DOUBLE SLASH Arbitrary File Disclosure Vuln	4225	R D Michael Peselnik
2009-02-23	Multiple PDF Readers JBIG2 Local Buffer Overflow PoC	7781	R D webDEVIL

[ remote ]

-::DATE	-::DESCRIPTION	-::HITS	-::AUTHOR
2009-03-05	SupportSoft DNA Editor Module (dnaedit.dll) Code Execution Exploit	1093	R D X Nine:Situations:Group
2009-03-04	Easy File Sharing Web Server 4.8 File Disclosure Vulnerability	1424	R D Stack
2009-03-04	EFS Easy Chat Server Authentication Request Buffer Overflow Exploit (pl)	969	R D Dr4sh
2009-03-04	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (fast)	3965	R D Ahmed Obied
2009-03-03	EFS Easy Chat Server (XSRF) Change Admin Pass Vulnerability	1215	R D Stack
2009-03-03	Imera ImeraIEPlugin ActiveX Control Remote Code Execution Exploit	1020	R D Elazar

[ local ]

-::DATE	-::DESCRIPTION	-::HITS	-::AUTHOR
2009-03-05	Media Commands (m3u File) Universal SEH Overwrite Exploit	669	R D His0k4
2009-03-05	Media Commands .m3l File Local Buffer Overflow Exploit	621	R D Stack

<http://milw0rm.com/> - men ingen opdateringer

# The Exploit Database - dagens buffer overflow



The screenshot shows the homepage of The Exploit Database. At the top, there is a navigation bar with links: [ home ], [ news ], [ remote ], [ local ], [ web ], [ dos ], [ shellcode ], [ papers ], [ search ], [ D ], [ submit ], and [ rss ]. To the right of the navigation bar, it says "Currently Archiving 10343 Exploits". The main content area features a banner with the text "The Exploit Database" and a subtext about being an archive of exploits and vulnerable software. It also mentions a cleanup and submission policy. Below this, there is a section titled "Remote Exploits" with a table listing various exploits. The table has columns for Date, D, A, V, Description, Plat., and Author. The exploits listed are:

Date	D	A	V	Description	Plat.	Author
2010-01-27	D	A	✓	CamShot v1.2 SEH Overwrite Exploit	windows	technik
2010-01-25	D	-	✓	AOL 9.5 Phobos.Playlist 'Import()' Buffer Overflow Exploit (Meta)	windows	Trancer
2010-01-22	D	A	✓	IntelliTamper 2.07/2.08 (SEH) Remote Buffer Overflow	windows	loneferret
2010-01-21	D	-	✓	EFS Easy Chat server Universal BOF-SEH (Meta)	windows	FB1H2S
2010-01-20	D	-	✓	AOL 9.5 ActiveX 0day Exploit (heap spray)	windows	Dz_attacker
2010-01-19	D	-	✓	Pidgin MSN <= 2.6.4 File Download Vulnerability	multiple	Mathieu GASPARD
2010-01-18	D	A	✓	Exploit EFS Software Easy Chat Server v2.2	windows	John Babio

<http://www.exploit-db.com/>

## What is it?

The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide. The framework is written in the Ruby programming language and includes components written in C and assembler.

Trinity brugte et exploit program ☺

Idag findes der samlinger af exploits som milw0rm

Udviklingsværktøjerne til exploits er idag meget raffinerede!

<http://www.metasploit.com/>

Bemærk: alle angreb har forudsætninger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

Kan du bryde kæden af forudsætninger har du vundet!

Stack protection er mere almindeligt  
- med i OpenBSD current fra 2. dec 2002

Buffer overflows er almindeligt kendte

- Selv OpenSSH har haft buffer overflows
- Stack protection prøver at modvirke/fjerne muligheden for buffer overflows. arbitrary code execution bliver til ude af drift for berørte services

Propolice

<http://www.openbsd.org>

<http://www.trl.ibm.com/projects/security/ssp/>

StackGuard

<http://www.immunix.org/stackguard.html>

Nyere versioner af Microsoft Windows, Mac OS X og Linux distributionerne inkluderer:

- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

OpenBSD er nok nået længst og et godt eksempel

<http://www.openbsd.org/papers/>

Hvorfor ikke bare bruge JAVA?

## JAVA karakteristik

- automatisk garbage collection
- bytecode verifikation på
- mulighed for signeret kode
- beskyldes for at være langsomt
- platformsuafhængigt

JAVA just in Time (JIT) er sammenligneligt med kompileret C

god sikkerhedsmodel - men problemer i implementationerne

JVM - den virtuelle maskine er utsat for hacking

## Diskussion:

I skal se/lære at mange protokoller i dag er *ASCII baserede* - dvs benytter kommandoer i klar tekst, GET, HEAD, QUIT osv. som gør det nemt at debugge.

Det gælder eksempelvis for:

- SMTP
- POP3
- FTP
- HTTP

man kan altså forbinde til den pågældende service og interagere



## Vi laver nu øvelsen

# Network scripting using netcat

som er øvelse **31** fra øvelseshæftet.



Vi laver nu øvelsen

## OpenSSL forbindelser

som er øvelse **32** fra øvelseshæftet.

Dan Farmer og Wietse Venema skrev i 1993 artiklen  
*Improving the Security of Your Site by Breaking Into it*

Senere i 1995 udgav de så en softwarepakke med navnet SATAN *Security Administrator Tool for Analyzing Networks* Pakken vagte en del furore, idet man jo gav alle på internet mulighed for at hacke

We realize that SATAN is a two-edged sword - like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

SATAN og ideerne med automatiseret scanning efter sårbarheder blev siden ført videre i programmer som Saint, SARA og idag findes mange hackerværktøjer og automatiserede scannere:

- OpenVAS, ISS scanner, Fyodor Nmap, Typhoon, ORAScan

Kilde: <http://www.fish.com/security/admin-guide-to-cracking.html>

Hackerværktøjer - bruger I dem? - efter dette kursus gør I portscannere kan afsløre huller i forsvaret  
webtestværktøjer som crawler igennem et website og finder alle forms kan hjælpe I vil kunne finde mange potentielle problemer proaktivt ved regelmæssig brug af disse værktøjer - også potentielle driftsproblemer  
husk dog penetrationstest er ikke en sølvkugle  
honeypots kan måske være med til at afsløre angreb og kompromitterede systemer hurtigere

Hvad skal manøre når man bliver hacket ?

Hvad koster et indbrud?

- Tid - antal personer der ikke kan arbejde
- Penge - oprydning, eksterne konsulenter
- Bøvl - sker altid på det værst mulige tidspunkt
- Besvær - ALT skal gennemrodes
- Tab af image/goodwill

Forensic challenge: I gennemsnit brugte deltagerne 34 timer pr person på at efterforske i rigtige data fra et indbrud! angriberen brugte ca. 30 min

Kilder: <http://project.honeynet.org/challenge/results/>  
<http://packetstorm.securify.com/docs/hack/i.only.replaced.index.html.txt>

## DU KAN IKKE HAVE TILLID TIL NOGET

På CERT website kan man finde mange gode ressourcer omkring sikkerhed og hvad man skal gøre med kompromiterede servere

Eksempelvis listen over dokumenter fra adressen:

<http://www.cert.org/nav/recovering.html>

- The Intruder Detection Checklist
- Windows NT Intruder Detection Checklist
- The UNIX Configuration Guidelines
- Windows NT Configuration Guidelines
- The List of Security Tools
- Windows NT Security and Configuration Resources



Vi laver nu øvelsen  
**OpenVAS scanning**  
som er øvelse **33** fra øvelseshæftet.

En firewall er noget som **blokerer** traffik på Internet

| En firewall er noget som **tillader** traffik på Internet

Myte: en firewall beskytter mod alt

Myten:

en firewall beskytter mod alt

Sandhed:

en firewall blokerer en masse, fint nok

en firewall tillader at du henter en masse ind

Beskytter mod direkte angreb fra netværket

Beskytter ikke mod fysiske angreb

Beskytter ikke mod malware gennem websider og e-mail

Firewall anbefales altid, specielt på bærbare

Basalt set et netværksfilter - det yderste fæstningsværk

Indholder typisk:

- Grafisk brugergrænseflade til konfiguration - er det en fordel?
- TCP/IP filtermuligheder - pakernes afsender, modtager, retning ind/ud, porte, protokol, ...
- kun IPv4 for de kommercielle firewalls
- både IPv4 og IPv6 for Open Source firewalls: IPF, OpenBSD PF, Linux firewalls, ...
- foruddefinerede regler/eksempler - er det godt hvis det er nemt at tilføje/åbne en usikker protokol?
- typisk NAT funktionalitet indbygget
- typisk mulighed for nogle serverfunktioner: kan agere DHCP-server, DNS caching server og lignende

En router med Access Control Lists - ACL kaldes ofte netværksfilter, mens en dedikeret maskine kaldes firewall - funktionen er reelt den samme - der filtreres trafik

```
# hosts
router="217.157.20.129"
webserver="217.157.20.131"
# Networks
homenet=" 192.168.1.0/24, 1.2.3.4/24 "
wlan="10.0.42.0/24"
wireless=wi0

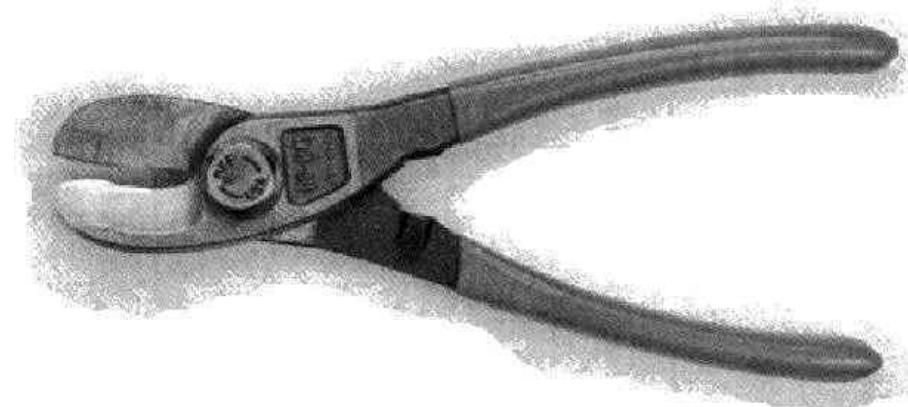
# things not used
spoofed=" 127.0.0.0/8, 172.16.0.0/12, 10.0.0.0/16, 255.255.255.255/32 "

block in all # default block anything
# loopback and other interface rules
pass out quick on lo0 all
pass in quick on lo0 all

# egress and ingress filtering - disallow spoofing, and drop spoofed
block in quick from $spoofed to any
block out quick from any to $spoofed

pass in on $wireless proto tcp from $wlan to any port = 22
pass in on $wireless proto tcp from $homenet to any port = 22
pass in on $wireless proto tcp from any to $webserver port = 80

pass out quick proto tcp from $homenet to any flags S/S keep state
pass out quick proto udp from $homenet to any keep state
pass out quick proto icmp from $homenet to any keep state
```



Hvor skal en firewall placeres for at gøre størst nytte?

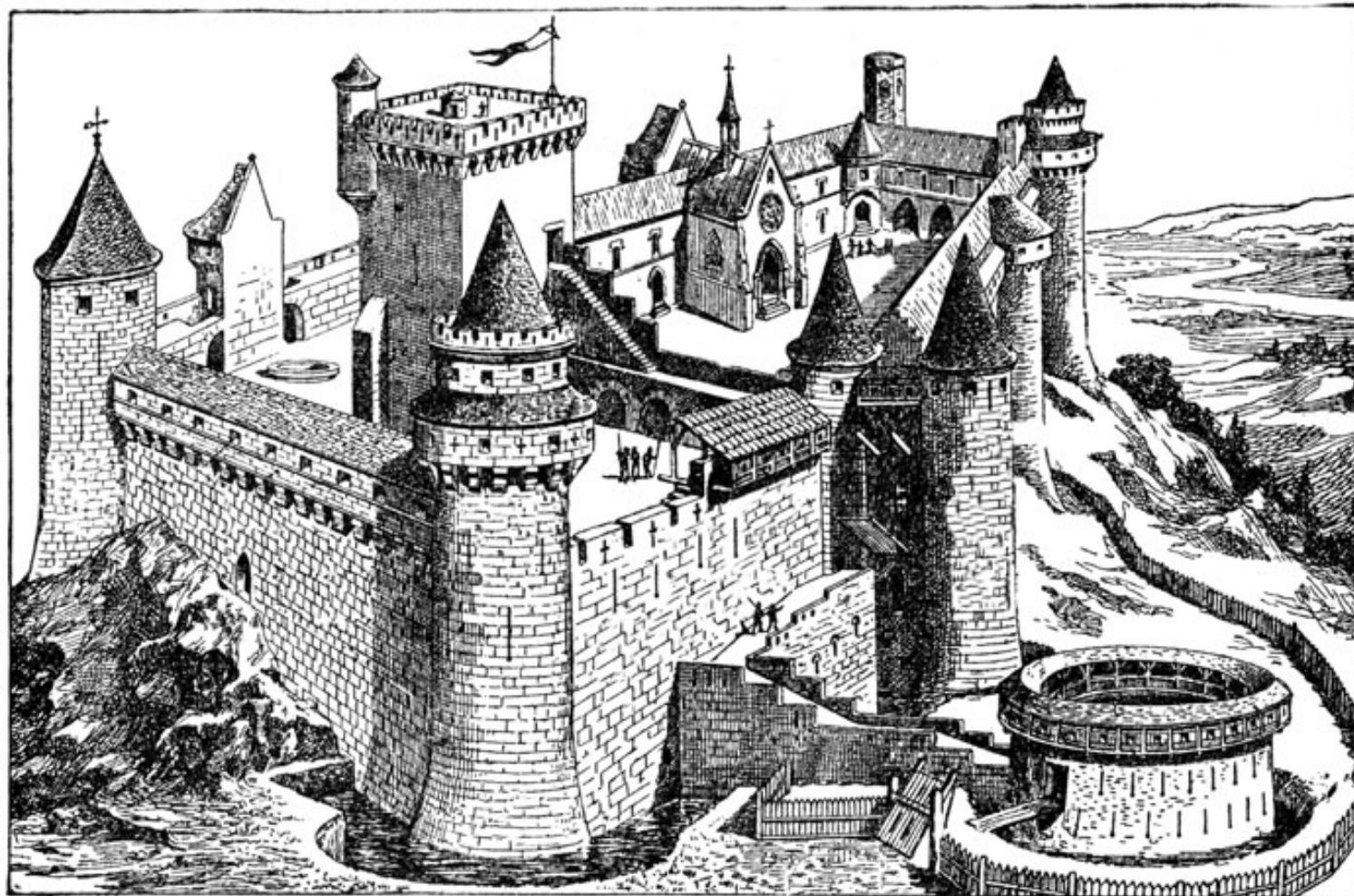
Hvad er forudsætningen for at en firewall virker?

At der er konfigureret et sæt fornuftige regler!

Hvor kommer reglerne fra? Sikkerhedspolitikken!

Kilde: Billedet er fra Marcus Ranum The ULTIMATELY Secure Firewall

# Enhance and secure runtime environment



Sidste chance er på afviklingstidspunktet

Nyere versioner af Microsoft Windows, Mac OS X og Linux distributionerne inkluderer:

- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

Vælg derfor hellere:

- Windows 7, end Windows Xp
- Mac OS X 10.7 fremfor 10.6
- Linux sikkerhedsopdateringer, sig ja når de kommer

Det samme gælder for serveroperativsystemer

NB: meget få embedded systemer har beskyttelse!

## **Adobe Flash problems, player security issues & exploits - 2011**

---

### **Google Chrome offers to help stop Flash security problems** - March 2011

Google have extended their flash security sandbox to allow Adobe flash to take advantage of it. Google have also enhanced plug-in security by notifying the user of out-of-date plug-ins that may cause vulnerabilities.

### **Flash security vulnerabilities affects Microsoft Excel** - March 2011

A flash security issue is currently being exploited by hackers by embedding malicious SWF files into Microsoft Excel spreadsheets. These are then emailed to unsuspecting users. All major OS's are affected by this flash security flaw.

### **USB flash security compromised by major design flaw** - February 2011

Secure flash drives manufactured by some of the big brand flash memory-makers can be sent an 'unlock' flag to the devices which makes them unlock without requiring the password. The system is inherently insecure because when the secure flash drive software authenticates the supplied password it sends an 'unlock' flag to the drive (a common 'conditional jump'), which can be patched to unlock the device.

### **Adobe flash security sandbox bypassed** - January 2011

Adobe flash player security has been bypassed by a security researcher who used a file request to a network machine. Adobe flash problems were meant to be minimized by use of the sandbox but the security researcher detailed how this could be easily bypassed by a malicious person.

Kilde: <http://www.locklizard.com/adobe-flash-security.htm>

## Drive-by download

---

From Wikipedia, the free encyclopedia

**Drive-by download** means three things, each concerning the unintended [download of computer software from the Internet](#):

1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit [executable program](#), [ActiveX component](#), or [Java applet](#)). This is usually caused by poor security design [clarification needed]. The user should not be frequently asked to accept security-critical decisions, often with very limited knowledge and within limited time.
2. Any [download](#) that happens without a person's knowledge.
3. Download of [spyware](#), a [computer virus](#) or any kind of [malware](#) that happens without a person's knowledge.

Kan vi undvære Flash og PDF?

Kilde: [http://en.wikipedia.org/wiki/Drive-by\\_download](http://en.wikipedia.org/wiki/Drive-by_download)



Safari <http://clicktoflash.com/>

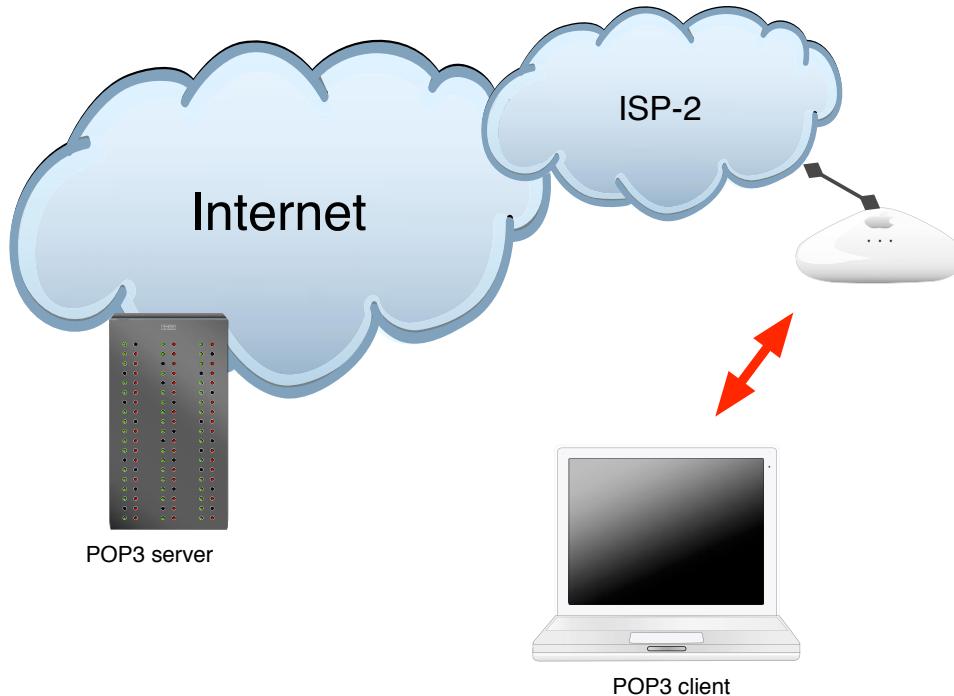
Firefox Extension Flashblock

Chrome extension called FlashBlock

Internet Explorer 8: IE has the Flash block functionality built-in so you don't need to install any additional plugins to be able to block flash on IE 8.

FlashBlock for Opera 9 - bruger nogen Opera mere?

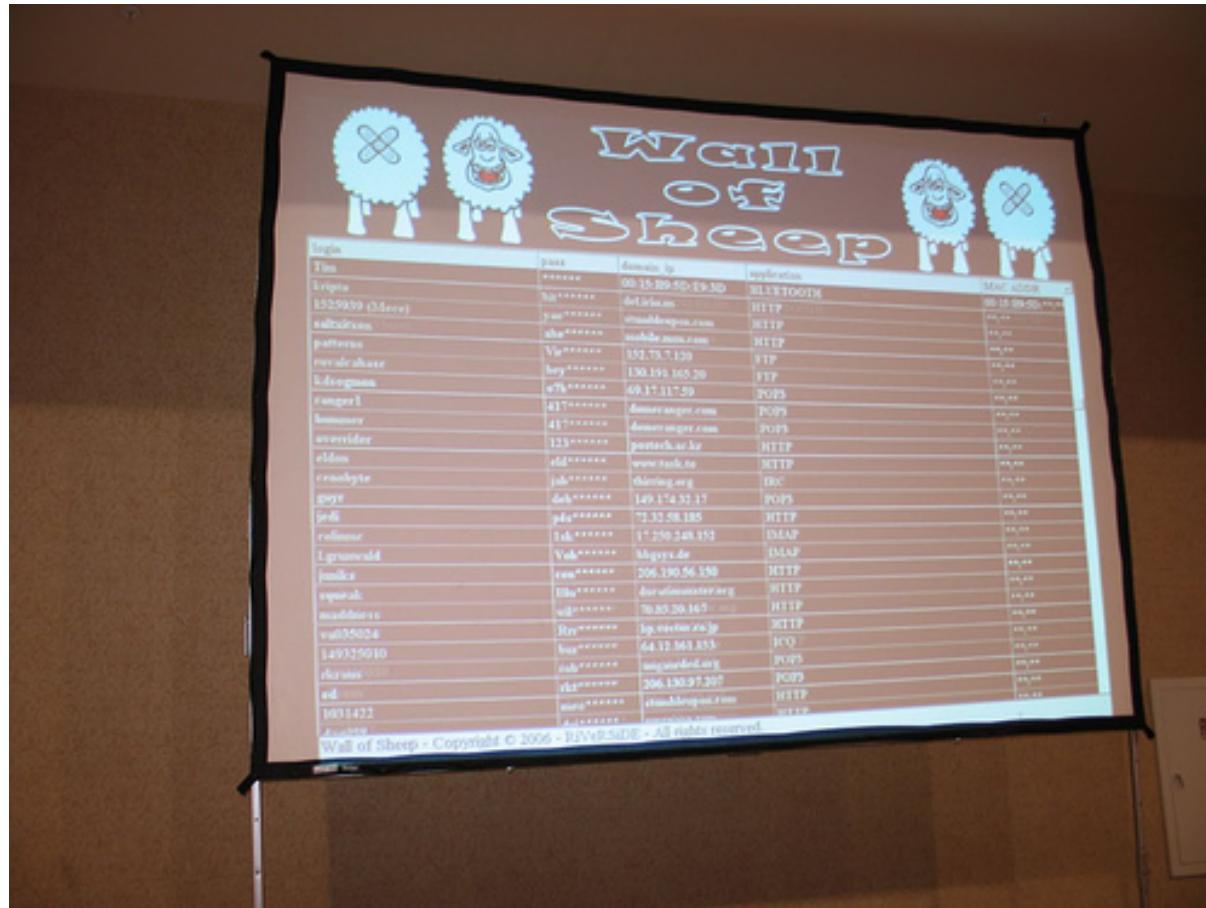
FlashBlockere til iPad? iPhone? Android? - hvorfor er det ikke default?



Har man tillid til andre ISP'er? Alle ISP'er?

Deler man et netværksmedium med andre?

Brug de rigtige protokoller!



Defcon Wall of Sheep  
Husk nu at vi er venner her! - idag er det kun teknikken



The screenshot shows the Twitter profile for the account @safety, which is associated with Twitter HQ. The profile includes a blue Twitter bird icon, the handle '@safety', the name 'Safety', and a verified checkmark. Below the profile is a bio: 'Twitter's Trust and Safety Updates!' and a link: 'http://help.twitter.com/forums/10711/entries/76036'. The interface shows a green 'Following' button, a message icon, and a user icon. A text input field says 'Tweet to @safety'. Below this is a navigation bar with tabs: 'Tweets' (selected), 'Favorites', 'Following', 'Followers', and 'Lists'. Three tweets from the account are listed:

- safety Safety**  
Also, we will never send you an email saying that you've been suspended for "tweeting too much." Those emails are fake & not from us.  
26 Sep
- safety Safety**  
We will never send you emails requiring you to "complete offers" in order to unsuspend your account. That's spam, not us.  
26 Sep
- safety Safety**  
Warn your friends if they sent you a DM saying "When I found this about you" with a link - they've been phished. [bit.ly/accountamiss](http://bit.ly/accountamiss)  
21 Sep

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

Unix systemer tillader ofte boot i singleuser mode  
hold command-s nede under boot af Mac OS X

Bærbare tillader typisk boot fra CD-ROM  
hold c nede på en Mac

Mac computere kan i nogle tilfælde være firewire diske  
hold t nede under boot

Harddisken kan typisk nemt fjernes fra en bærbar



Fysisk adgang til systemet - **game over**



Firewire target mode: Macbook disken kan tilgås fra en anden Mac

Press t to enter ☺

<http://support.apple.com/kb/ht1661>

# Hackertyper anno 1995



Lad os lige gå tilbage til hackerne



Lisbeth laver PU, personundersøgelser ved hjælp af hacking

Hvordan finder man information om andre

Først vil vi finde nogle mønstre

Derefter vil vi søge med de mønstre

Nogle giver direkte information

Andre giver baggrundsinformation

Hvad er offentligt og hvad er privat? (googledorks!)

Navn, fulde navn, fornavne, efternavne, alias'es

Diverse idnumre, som CPR - tør du søge på dit CPR nr?

Computerrelaterede informationer: IP, Whois, Handles

Øgenavne, kendenavne

Skrivestil, ordbrug mv.

Tiden på din computer?

Tænk kreativt ☺

# Hvor finder du informationerne

Email

DNS

Gætter

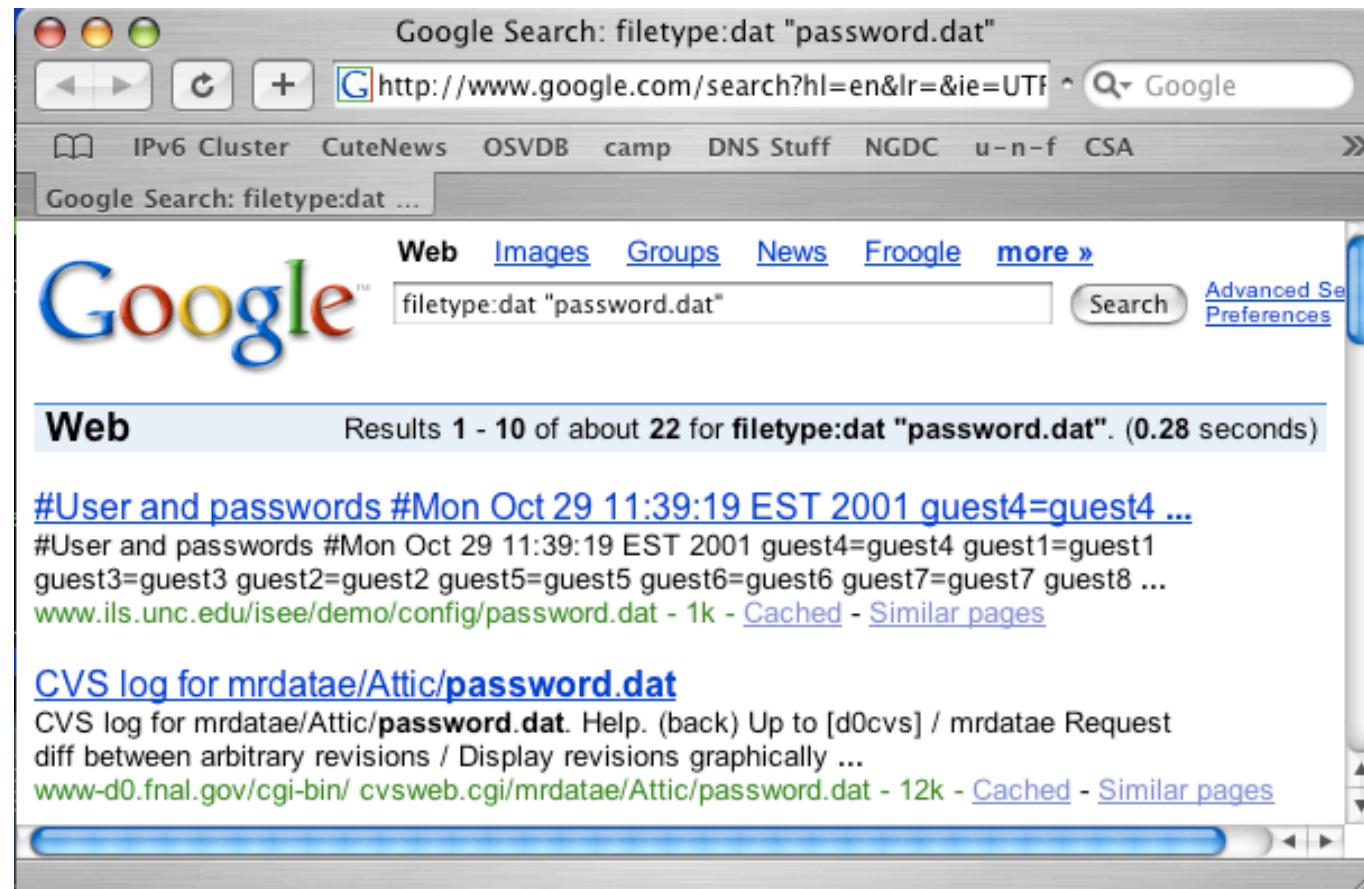
Google

Alt hvad du ellers har adgang til - eller som Lisbeth tilraner sig adgang til

IP adresserne administreres i dagligdagen af et antal Internet registries, hvor de største er:

- RIPE (Réseaux IP Européens) <http://ripe.net>
- ARIN American Registry for Internet Numbers <http://www.arin.net>
- Asia Pacific Network Information Center <http://www.apnic.net>
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands

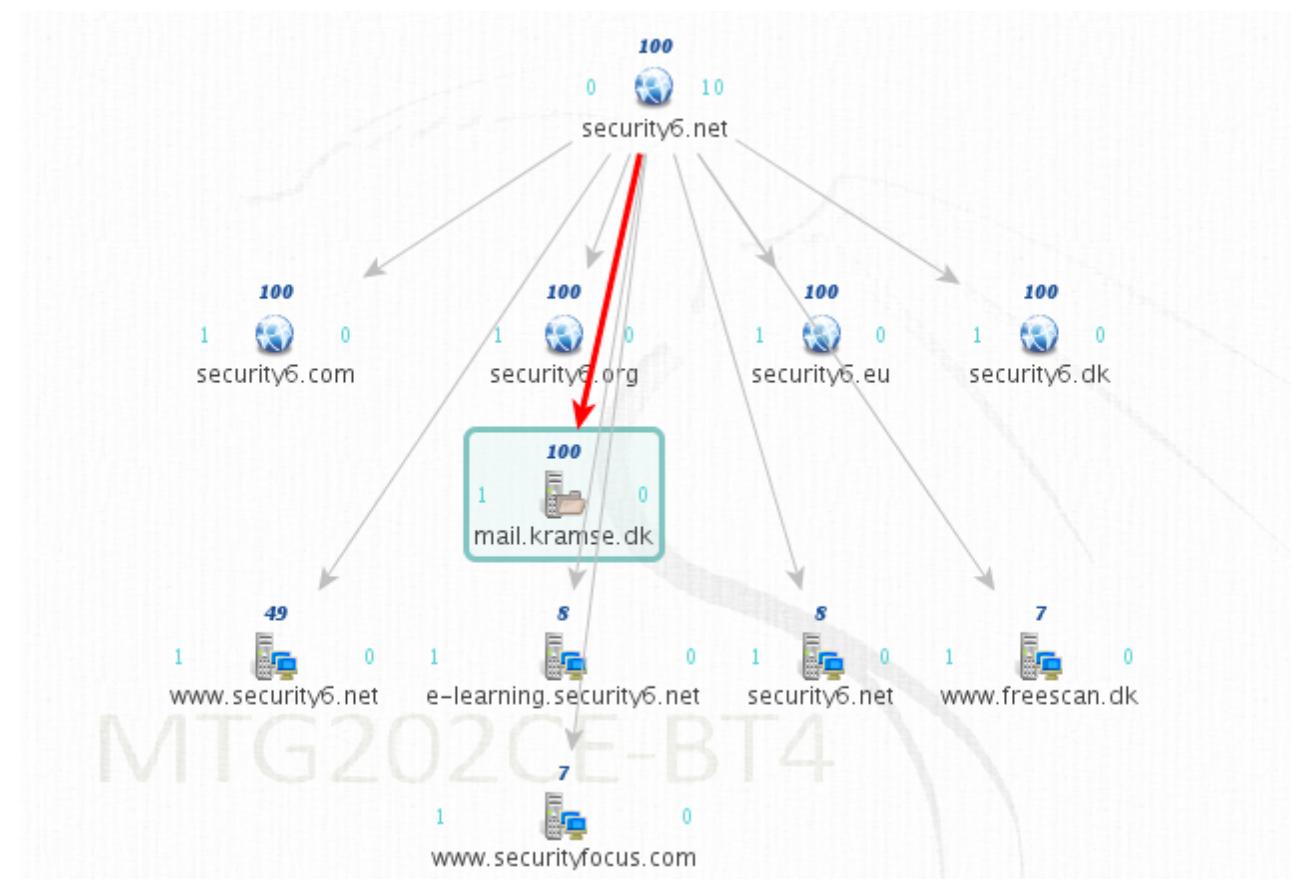
disse fire kaldes for Regional Internet Registries (RIRs) i modsætning til Local Internet Registries (LIRs) og National Internet Registry (NIR)



Google som hacker værktøj?

Googledorks <http://johnny.ihackstuff.com/>

# Listbeth in a box?



BT4 udgaven, kommercial udgave på <http://www.paterva.com/maltego/>

# Demo Maltego



# Er du passende paranoid?



Vær på vagt

Lad være med at bruge computere

Lad være med at bruge en computer til alt - en privat bærbar ER mere privat end en firmacomputer

Forskellige computere til forskellige formål, en server er mail-server en anden er web-server

Brug en sikker konfiguration, minimumskonfiguration

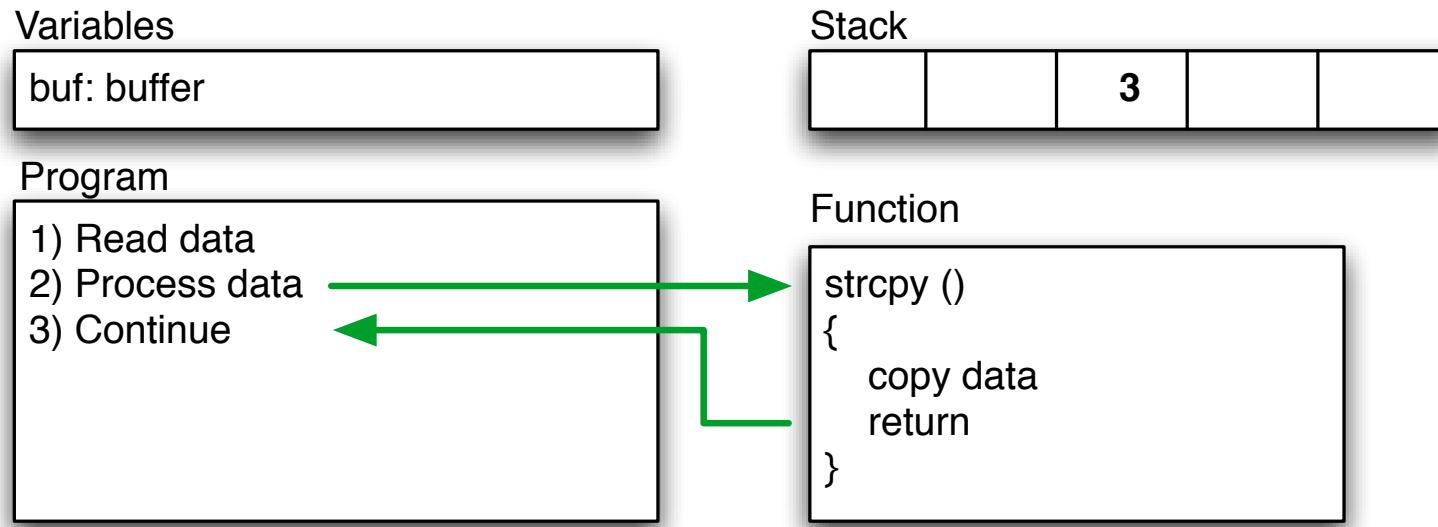
Brug sikre protokoller, kryptering, evt. TOR

Opsætning af netværk, hvordan? Security Configuration Guides + paranoia

- <http://csrc.nist.gov/publications/PubsSSPs.html>
- <http://www.nsa.gov/research/publications/index.shtml>
- [http://www.nsa.gov/ia/guidance/security\\_configuration\\_guides/index.shtml](http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml)

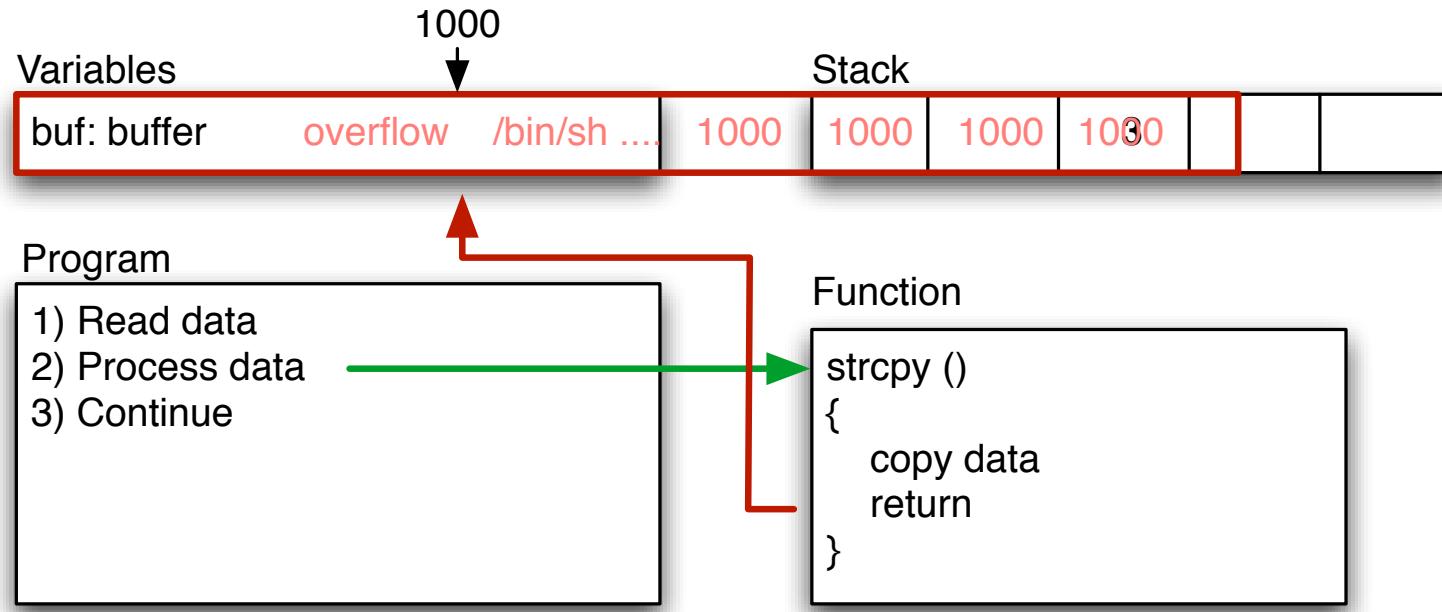
**Et buffer overflow** er det der sker når man skriver flere data end der er afsat plads til i en buffer, et dataområde. Typisk vil programmet gå ned, men i visse tilfælde kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

**Stack protection** er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.



```
main(int argc, char **argv)  
{  
    char buf[200];  
    strcpy(buf, argv[1]);  
    printf("%s\n", buf);  
}
```

# Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

```
$buffer = "";
$null = "\x00"; █
$nop = "\x90";
$nopsize = 1; █
$len = 201; // what is needed to overflow, maybe 201, maybe more!
$the_shell_pointer = 0xdeadbeef; // address where shellcode is
# Fill buffer
for ($i = 1; $i < $len;$i += $nopsize) {
    $buffer .= $nop;
}█
$address = pack('l', $the_shell_pointer);
$buffer .= $address;█
exec "$program", "$buffer";
```

## Demo exploit in Perl

Black box testing

Closed source reverse engineering

White box testing

Open source betyder man kan læse og analysere koden

Source code review - automatisk eller manuelt

Fejl kan findes ved at prøve sig frem - fuzzing

Exploits virker typisk mod specifikke versioner af software

# The Exploit Database - dagens buffer overflow



The screenshot shows the homepage of The Exploit Database. At the top, there's a banner with the word "EXPLOIT" in large letters, "D a t a b a s e" below it, and a silhouette of a person holding a briefcase. To the right, it says "Currently Archiving 10343 Exploits". Below the banner is a navigation menu with links like [ home ], [ news ], [ remote ], [ local ], [ web ], [ dos ], [ shellcode ], [ papers ], [ search ], [ D ], [ submit ], and [ rss ]. The main content area has a dark background with floral patterns on the sides. It features a section titled "The Exploit Database" with a sub-section "Remote Exploits". Below this is a table listing seven remote exploits:

Date	D	A	V	Description	Plat.	Author
2010-01-27	D	A	✓	CamShot v1.2 SEH Overwrite Exploit	windows	technik
2010-01-25	D	-	✓	AOL 9.5 Phobos.Playlist 'Import()' Buffer Overflow Exploit (Meta)	windows	Trancer
2010-01-22	D	A	✓	IntelliTamper 2.07/2.08 (SEH) Remote Buffer Overflow	windows	loneferret
2010-01-21	D	-	✓	EFS Easy Chat server Universal BOF-SEH (Meta)	windows	FB1H2S
2010-01-20	D	-	✓	AOL 9.5 ActiveX 0day Exploit (heap spray)	windows	Dz_attacker
2010-01-19	D	-	✓	Pidgin MSN <= 2.6.4 File Download Vulnerability	multiple	Mathieu GASPARD
2010-01-18	D	A	✓	Exploit EFS Software Easy Chat Server v2.2	windows	John Babio

<http://www.exploit-db.com/>

## What is it?

The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide. The framework is written in the Ruby programming language and includes components written in C and assemblers.

Idag findes der samlinger af exploits som exploit-db eller exploit packs

Udviklingsværktøjerne til exploits er idag meget raffinerede!

<http://www.metasploit.com/>

<http://www.fastandeasyhacking.com/> Armitage GUI til Metasploit

<http://www.offensive-security.com/metasploit-unleashed/>

Bemærk: alle angreb har forudsætninger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

Kan du bryde kæden af forudsætninger har du vundet!

Computeren skal være tændt

Funktionen der misbruges skal være slået til

Executable stack

Executable heap

Fejl i programmet

|

**alle programmer har fejl**

Nyere versioner af Microsoft Windows, Mac OS X og Linux distributionerne inkluderer:

- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

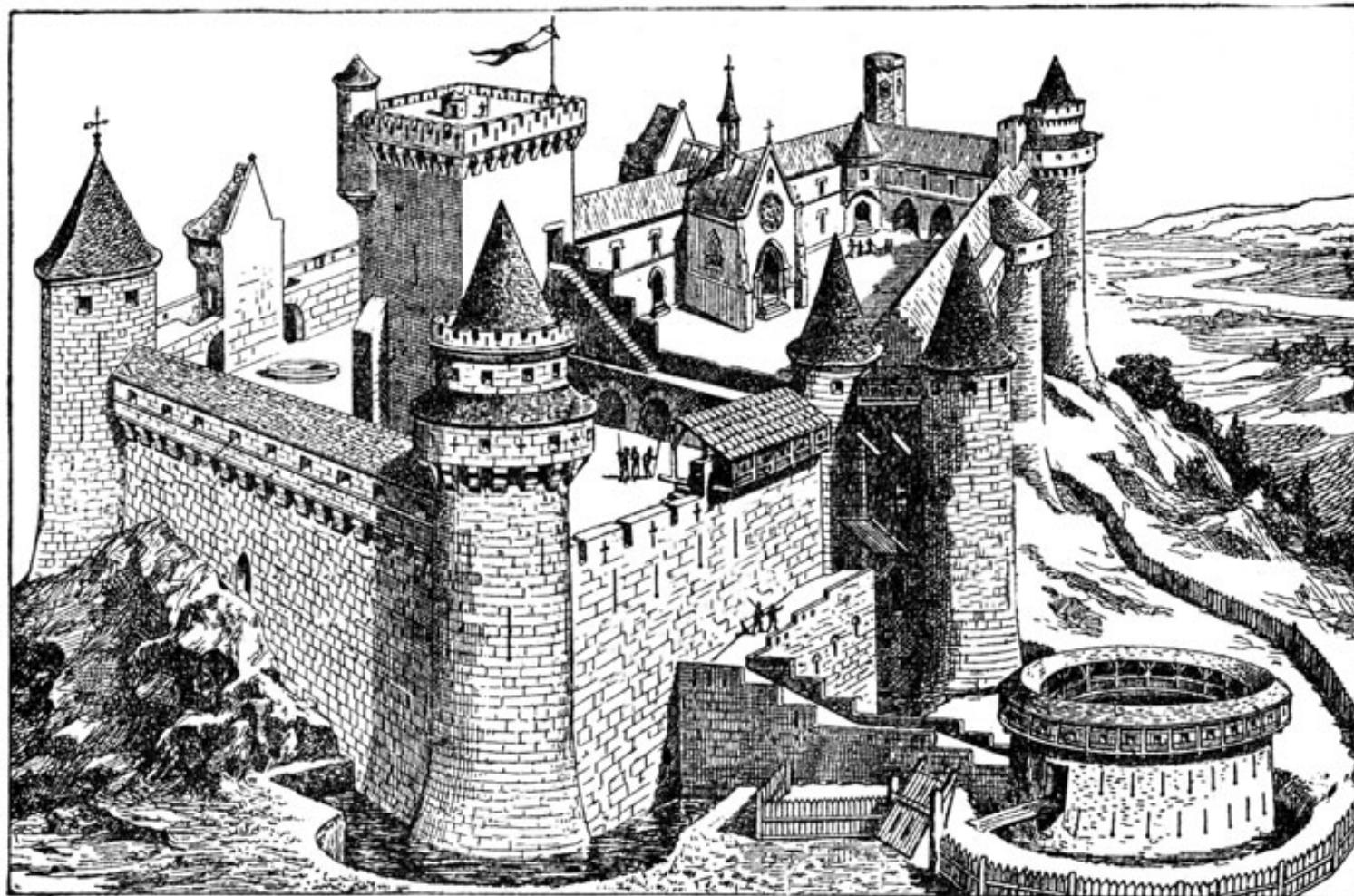
Vælg derfor hellere:

- Windows 7, end Windows Xp
- Mac OS X 10.7 fremfor 10.6
- Linux sikkerhedsopdateringer, sig ja når de kommer

Det samme gælder for serveroperativsystemer

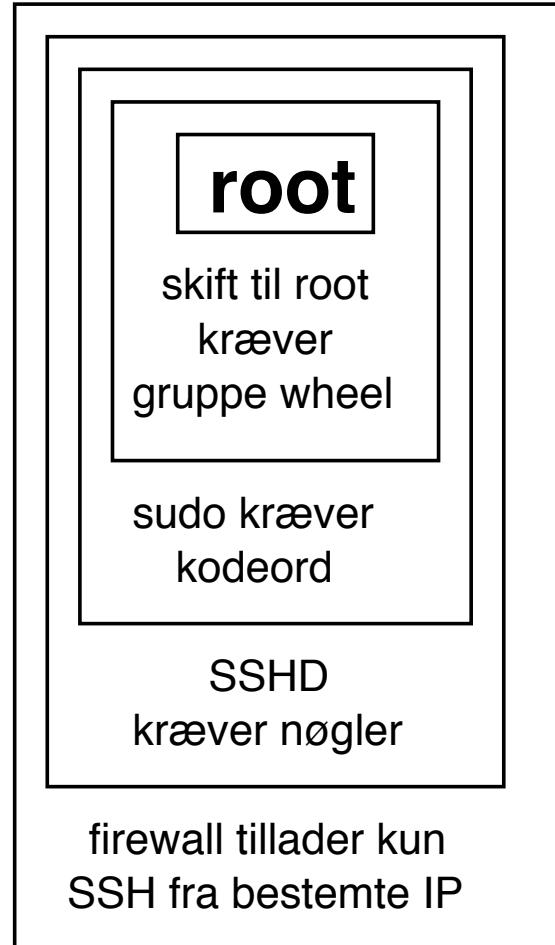
NB: meget få embedded systemer har beskyttelse!

# Enhance and secure runtime environment



Sidste chance er på afviklingstidspunktet

# Defense in depth - flere lag af sikkerhed



Forsvar dig selv med flere lag af sikkerhed!

Der findes mange typer *jails* på Unix

Ideer fra Unix chroot som ikke er en egentlig sikkerhedsfeature

- Unix chroot - bruges stadig, ofte i daemoner som OpenSSH
- FreeBSD Jails
- SELinux
- Solaris Containers og Zones - *jails på steroider*
- VMware virtuelle maskiner, er det et jail?

Hertil kommer et antal andre måder at adskille processer - sandkasser

Husk også de simple, database som `postgresql`, Tomcat som `tomcat`, Postfix postsystem som `postfix`, SSHD som `sshd` osv. - simple brugere, få rettigheder

## systrace - generate and enforce system call policies

### EXAMPLES

An excerpt from a sample ls(1) policy might look as follows:

```
Policy: /bin/ls, Emulation: native
[...]
    native-fsread: filename eq "$HOME" then permit
    native-fchdir: permit
[...]
    native-fsread: filename eq "/tmp" then permit
    native-stat: permit
    native-fsread: filename match "$HOME/*" then permit
    native-fsread: filename eq "/etc/pwd.db" then permit
[...]
    native-fsread: filename eq "/etc" then deny[eperm], if group != wheel
```

### SEE ALSO

systrace(4)

```
// ===== WEB APPLICATION PERMISSIONS =====
// These permissions are granted by default to all web applications
// In addition, a web application will be given a read FilePermission
// and JndiPermission for all files and directories in its document root.
grant {
    // Required for JNDI lookup of named JDBC DataSource's and
    // javamail named MimePart DataSource used to send mail
    permission java.util.PropertyPermission "java.home", "read";
    permission java.util.PropertyPermission "java.naming.*", "read";
    permission java.util.PropertyPermission "javax.sql.*", "read";
...
};
// The permission granted to your JDBC driver
// grant codeBase "jar:file:$catalina.home/webapps/examples/WEB-INF/lib	driver.jar!/-" {
//     permission java.net.SocketPermission "dbhost.mycompany.com:5432", "connect";
// };
```

Eksempel fra apache-tomcat-6.0.18/conf/catalina.policy

# Apple sandbox named generic rules

```
; ; named - sandbox profile
; ; Copyright (c) 2006-2007 Apple Inc. All Rights reserved.
; ;
; ; WARNING: The sandbox rules in this file currently constitute
; ; Apple System Private Interface and are subject to change at any time and
; ; without notice. The contents of this file are also auto-generated and not
; ; user editable; it may be overwritten at any time.
; ;
(version 1)
(debug deny)

(import "bsd.sb")

(deny default)
(allow process*)
(deny signal)
(allow sysctl-read)
(allow network*)
```

# Apple sandbox named specific rules

```
;; Allow named-specific files
(allow file-write* file-read-data file-read-metadata
  (regex "^(/private)?/var/run/named\\\.pid$"
        "^(/Library/Logs/named\\\.log$"))

(allow file-read-data file-read-metadata
  (regex "^(/private)?/etc/rndc\\\.key$"
        "^(/private)?/etc/resolv\\\.conf$"
        "^(/private)?/etc/named\\\.conf$"
        "^(/private)?/var/named/"))
```

Eksempel fra /usr/share/sandbox på Mac OS X

## **Adobe Flash problems, player security issues & exploits - 2011**

---

### **Google Chrome offers to help stop Flash security problems** - March 2011

Google have extended their flash security sandbox to allow Adobe flash to take advantage of it. Google have also enhanced plug-in security by notifying the user of out-of-date plug-ins that may cause vulnerabilities.

### **Flash security vulnerabilities affects Microsoft Excel** - March 2011

A flash security issue is currently being exploited by hackers by embedding malicious SWF files into Microsoft Excel spreadsheets. These are then emailed to unsuspecting users. All major OS's are affected by this flash security flaw.

### **USB flash security compromised by major design flaw** - February 2011

Secure flash drives manufactured by some of the big brand flash memory-makers can be sent an 'unlock' flag to the devices which makes them unlock without requiring the password. The system is inherently insecure because when the secure flash drive software authenticates the supplied password it sends an 'unlock' flag to the drive (a common 'conditional jump'), which can be patched to unlock the device.

### **Adobe flash security sandbox bypassed** - January 2011

Adobe flash player security has been bypassed by a security researcher who used a file request to a network machine. Adobe flash problems were meant to be minimized by use of the sandbox but the security researcher detailed how this could be easily bypassed by a malicious person.

Kilde: <http://www.locklizard.com/adobe-flash-security.htm>

## Drive-by download

---

From Wikipedia, the free encyclopedia

**Drive-by download** means three things, each concerning the unintended [download of computer software from the Internet](#):

1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit [executable program](#), [ActiveX component](#), or [Java applet](#)). This is usually caused by poor security design [clarification needed]. The user should not be frequently asked to accept security-critical decisions, often with very limited knowledge and within limited time.
2. Any [download](#) that happens without a person's knowledge.
3. Download of [spyware](#), a [computer virus](#) or any kind of [malware](#) that happens without a person's knowledge.

Kan vi undvære Java, Flash og PDF?

Kilde: [http://en.wikipedia.org/wiki/Drive-by\\_download](http://en.wikipedia.org/wiki/Drive-by_download)



Safari <http://clicktoflash.com/>

Firefox Extension Flashblock

Chrome extension called FlashBlock

Internet Explorer 8: IE has the Flash block functionality built-in so you don't need to install any additional plugins to be able to block flash on IE 8.

FlashBlock for Opera 9 - bruger nogen Opera mere?

FlashBlockere til iPad? iPhone? Android? - hvorfor er det ikke default?

# Er du passende paranoid?



Vær på vagt

Lad være med at bruge computere :-)

Lad være med at bruge en computer til alt - en privat bærbar ER mere privat end en firmacomputer

Forskellige computere til forskellige formål, en server er mail-server en anden er web-server

Brug en sikker konfiguration, minimumskonfiguration

Brug sikre protokoller, kryptering, evt. TOR

Opsætning af netværk, hvordan? Security Configuration Guides + paranoia

- <http://csrc.nist.gov/publications/PubsSSPs.html>
- <http://www.nsa.gov/research/publications/index.shtml>
- [http://www.nsa.gov/ia/guidance/security\\_configuration\\_guides/index.shtml](http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml)

# Følg med Twitter news



The screenshot shows the Twitter profile for the account @safety, which is verified. The profile bio reads: "Twitter's Trust and Safety Updates! http://help.twitter.com/forums/10711/entries/76036". Below the bio, there is a green "Following" button, a reply icon, and a direct message icon. A text input field says "Tweet to @safety". Below these are navigation tabs for "Tweets", "Favorites", "Following", "Followers", and "Lists". Three tweets from the account are listed:

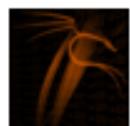
- safety Safety** Also, we will never send you an email saying that you've been suspended for "tweeting too much." Those emails are fake & not from us.  
26 Sep
- safety Safety** We will never send you emails requiring you to "complete offers" in order to unsuspend your account. That's spam, not us.  
26 Sep
- safety Safety** Warn your friends if they sent you a DM saying "When I found this about you" with a link - they've been phished. [bit.ly/accountamiss](http://bit.ly/accountamiss)  
21 Sep

Twitter has become an important new resource for lots of stuff

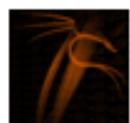
Twitter has replaced RSS for me



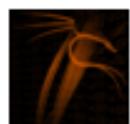
**exploitdb** [webapps] – BPAffiliate Affiliate Tracking  
Authentication Bypass Vulnerability: <http://bit.ly/9LOC3K>  
about 5 hours ago via twitterfeed



**exploitdb** [webapps] – BPDirectory Business Directory  
Authentication Bypass Vulnerability: <http://bit.ly/c4TeLz>  
about 5 hours ago via twitterfeed



**exploitdb** [webapps] – BPConferenceReporting Web Reporting  
Authentication Bypass Vulnerability: <http://bit.ly/cM61AK>  
about 5 hours ago via twitterfeed



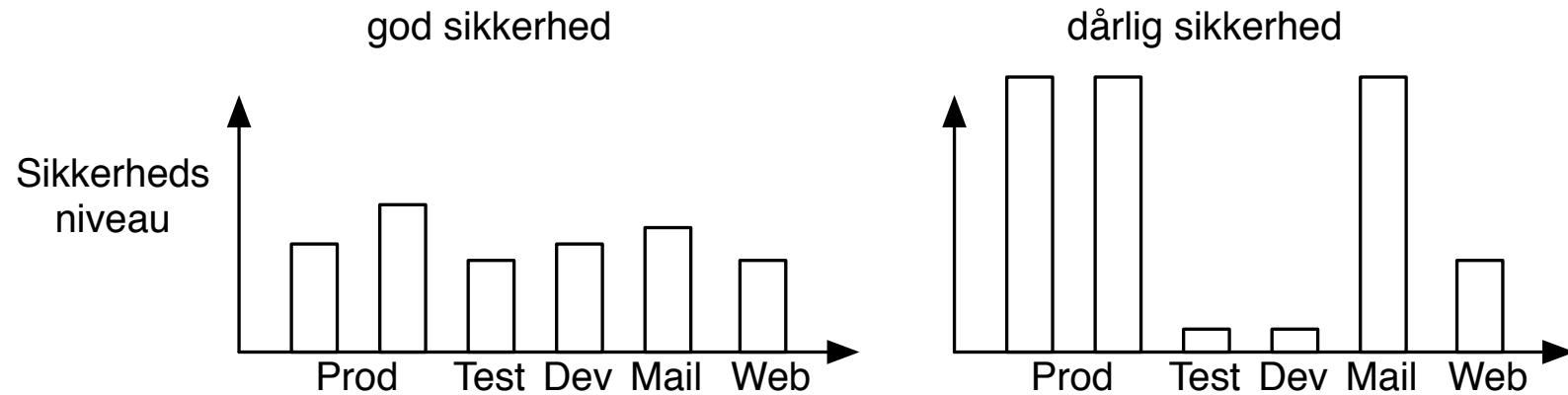
**exploitdb** [webapps] – BPRalestate Real Estate  
Authentication Bypass Vulnerability: <http://bit.ly/bYx2aY>  
about 5 hours ago via twitterfeed



**sans\_isc** [Diary] Mac OS X Server v10.6.5 (10H575) Security  
Update: <http://support.apple.com/kb/HT4452>, (Tue, Nov  
16th): .... <http://bit.ly/azBrso>  
about 7 hours ago via twitterfeed

## Exploits og nye sårbarheder

- BIOS kodeord, pin-kode til telefon
- Firewall - specielt på laptops
- Installer anti-virus og anti-spyware hvis det er på Windows
- Brug to browsere med forskellige indstillinger
- Brug evt. PGP til mailkryptering
- Brug Password Safe, Keychain Access (OSX) eller tilsvarende
- Overvej at bruge harddisk eller filkryptering
- Opdatere alle programmer jævnligt
- **Backup af vigtige data - harddiske i bærbare kan også dø**
- Husk: sikker sletning af harddiske, medier osv.



Det er bedre at have et ensartet niveau

Hvor rammer angreb hvis du har Fort Knox et sted og kaos andre steder

Hackere vælger ikke med vilje den sværreste vej ind



Team up!

Snak med din sidemand/dame - I har sikkert mange af de samme udfordringer.



PROSA afholdt fredag 17. september - til lørdag 18. september Capture the Flag

Distribueret CTF med 6 hold og arrangørerne i Aalborg

Sjovt og lærerigt - gentages helt sikkert

Kilde: <http://prosa-ctf.the-playground.dk/>

Get ready! Lær debuggere, perl, java at kende, start på at hacke

I 1993 skrev Dan Farmer og Wietse Venema artiklen  
*Improving the Security of Your Site by Breaking Into it*

I 1995 udgav de softwarepakken SATAN  
*Security Administrator Tool for Analyzing Networks*

We realize that SATAN is a two-edged sword - like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

Se <http://sectools.org> og <http://www.packetstormsecurity.org/>

Kilde: <http://www.fish2.com/security/admin-guide-to-cracking.html>

Henrik Lund Kramshøj, internet samurai  
[hlk@solido.net](mailto:hlk@solido.net)

<http://www.solidonetworks.com>

I er altid velkomne til at sende spørgsmål på e-mail

Welcome to VikingScan – miniscan

http://miniscan6.vikingscan.org/ Google

## VikingScan.org - free portscanning

Home Miniscan List

On this page you can configure and start a portscan of your IP-address from this server.  
Your IP-address is: 2001:16d8:dd0f:cf0f:223:6cff:fe9a:f52c

Configure and start a scan of the IP-address

Note that this service is currently software in development and you also need to make sure that you are allowed to scan the IP-address specified.

Do you need more? What about a basic webtest for DKK 8.000 ex VAT?

© 2009 VikingScan.org: Free portscanning  
<http://www.vikingscan.org>

WEB SCANNING WIRELESS SCANNING  
PENETRATION TESTING SECURITY TRAINING  
SECURE WEBSERVERS  
IMPLEMENTING IPV6  
FIREWALLS & VPN

Security is a process, not a tool, not a single portscan

  
Security .net

VikingScan.org is a service of Security6.net  
Security6.net provides this service for the community for free. If you need firewalls, penetration testing, security consulting please visit [Security6.net](#).