Welcome to

Paranoia and government hacking

IT-Universitetet 2013

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

Agenda and goal - workshop

Kl 16:00-18:00

Paranoia defined

Hacker tools

Attacks tools

Key words: crypto, back doors, hacker attacks, and hacker tools, what are 0-days - and how to protect yourself

Bjarne Jess Hansen - Vi voksne kan også være bange

https://www.youtube.com/watch?v=ApRPz9FzkQM

Kilde: teksten fundet på
http://www.fredsakademiet.dk/abase/sange/sang29.htm

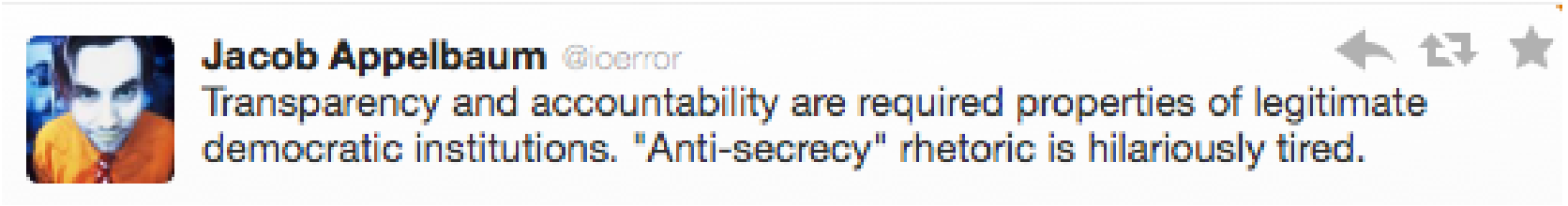
Syria: Protest singer Ibrahim Kashoush had his throat cut

> Four days later, his body was found dumped in the Assi River (also spelled: Isa River), with a big, open and bloody wound in his neck where his adam's apple and voice chord had been removed. A clear message to those who dare to raise their voice against the Syrian President Bashar al-Assad.

'Yalla Erhal Ya Bashar' (It's time to leave, Bashar), demanding an end to President Bashar al-Assads regime.

`https://www.youtube.com/watch?v=nox6sVyhBYk`
`http://freemuse.org/archives/5054`

Formål: Hvorfor gør vi det her?



Et demokrati fordrer borgere med frihed som har evnen til at tage beslutninger uden konstant at være overvåget.

Et demokrati fordrer borgere som aktivt vælger hvornår de afgiver personlige data om deres liv og færden og **kryptografi er en fredelig protest mod indsamling at data.**

Indsamlede data vil altid blive misbrugt

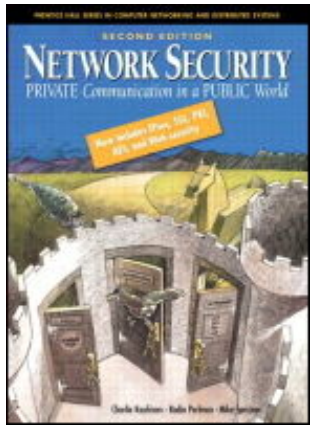
Data som indsamles **bliver misbrugt** enten til kriminelle formål, kommercielle formål uanset oprindelige formål med indsamlingen - under dække af beskyttelse mod terror, ekstremisme, nazisme, misbrug af børn, ... Le mal du jour / dagens onde.

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

Du bestemmer - det er demokrati

Rejsen starter

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.

Vi troede krypto kunne hjælpe os med næsten alle problemer ...

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`

Security is not magic

.

Think security, it may seem like magic - but it is not

Follow news about security

Support communities, join and learn

Part I: Paranoia defined

SOLIDO NETWORKS

par·a·noi·a

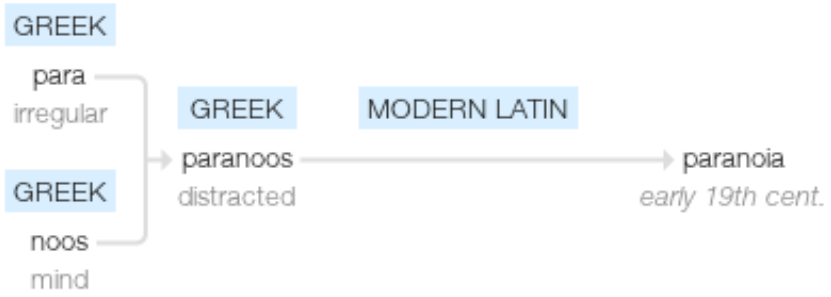
/ˌparəˈnoiə/

noun

noun: **paranoia**

1. a mental condition characterized by delusions of persecution, unwarranted jealousy, or exaggerated self-importance, typically elaborated into an organized system. It may be an aspect of chronic personality disorder, of drug abuse, or of a serious condition such as schizophrenia in which the person loses touch with reality.
   synonyms: persecution complex, delusions, obsession, psychosis More
- suspicion and mistrust of people or their actions without evidence or justification.
  "the global paranoia about hackers and viruses"

Origin



More

Source: google paranoia definition

Face reality

From the definition:

> suspicion and mistrust of people or their actions **without evidence or justification**. ”**the global paranoia about hackers and viruses**”

It is not paranoia when:

- Criminals sell your credit card information and identity theft
- Trade infected computers like a commodity
- Governments write laws that allows them to introduce back-doors - and use these
- Governments do blanket surveillance of their population
- Governments implement censorship, threaten citizens and journalist

You are not paranoid when there are people actively attacking you!

Government back-doors

SOLIDO NETWORKS

What if I told you:

Governments will introduce back-doors

Intercepting encrypted communications with fake certificates - check

May 5, 2011 A Syrian Man-In-The-Middle Attack against Facebook
”Yesterday we learned of reports that the Syrian Telecom Ministry had launched a man-in-the-middle attack against the HTTPS version of the Facebook site.”
Source:
`https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook`

Mapping out social media and finding connections - check

Creating fake certificates and intercepting social media sites - check

Checking porno preferences, for later intimidation - check

Too many things to list them here! `http://cryptome.org/`

Infecting activist machines

Infecting activist machines - check

Tibet activists are repeatedly being targeted with virus and malware, such as malicious apps for Android like KakaoTalk

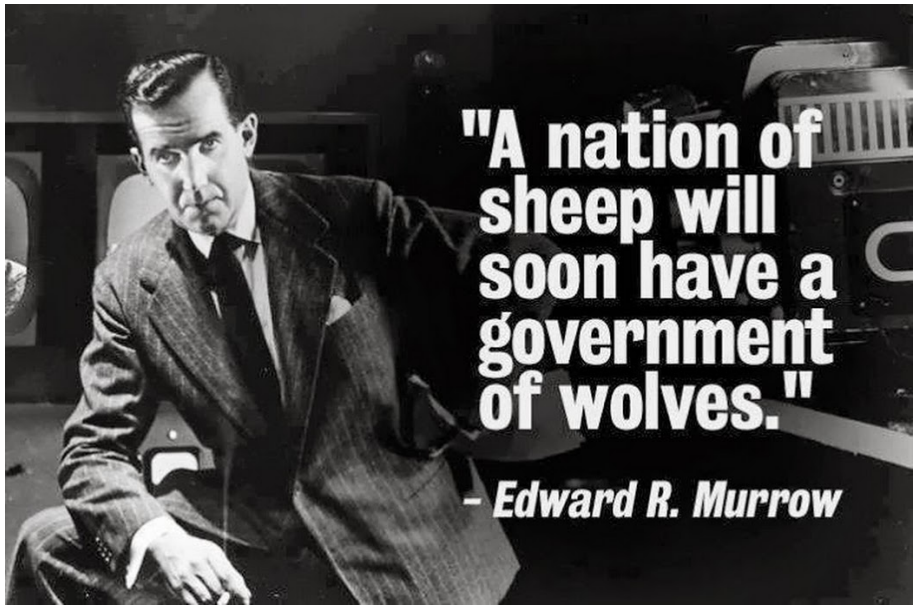
Tor-users infected with malicious code to reveal their real IPs

`https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting`

Copying journalist data in airports - check

Do you believe in democracy - you are the enemy of the state

Government backdoors is not news



Nothing new really, see for example D.I.R.T and Magic Lantern

D.I.R.T - Data Interception by Remote Transmission since the late 1990s
`http://cryptome.org/fbi-dirt.htm`
`http://cryptome.org/dirty-secrets2.htm`

They will always use *Le mal du jour* to increase monitoring

Government monitoring is not news

FBI Carnivore
"... that was designed to monitor email and electronic communications. It used a customizable packet sniffer that can monitor all of a target user's Internet traffic." `http://en.wikipedia.org/wiki/Carnivore_(software)`

NarusInsight "Narus provided Egypt Telecom with Deep Packet Inspection equipment, a content-filtering technology that allows network managers to inspect, track and target content from users of the Internet and mobile phones, as it passes through routers on the information superhighway. Other Narus global customers include the national telecommunications authorities in Pakistan and Saudi Arabia, ..."
`http://en.wikipedia.org/wiki/NarusInsight`

Denmark

Even Denmark which is considered a peaceful democracy has allowed this to go TO FAR

Danish police and TAX authorities have the legals means, even for small tax-avoidance cases, see *Rockerloven*

Danish TAX authorities have legal means to go into your property to catch builders working for cash and not reporting tax income

In both criminal and piracy cases we see a lot of extraneous equipment seized

Danish prime minister Helle Thorning-Schmidt does NOT criticize the USA

In fact the party Social Democrats are often pushing further surveillance

Use protection - always

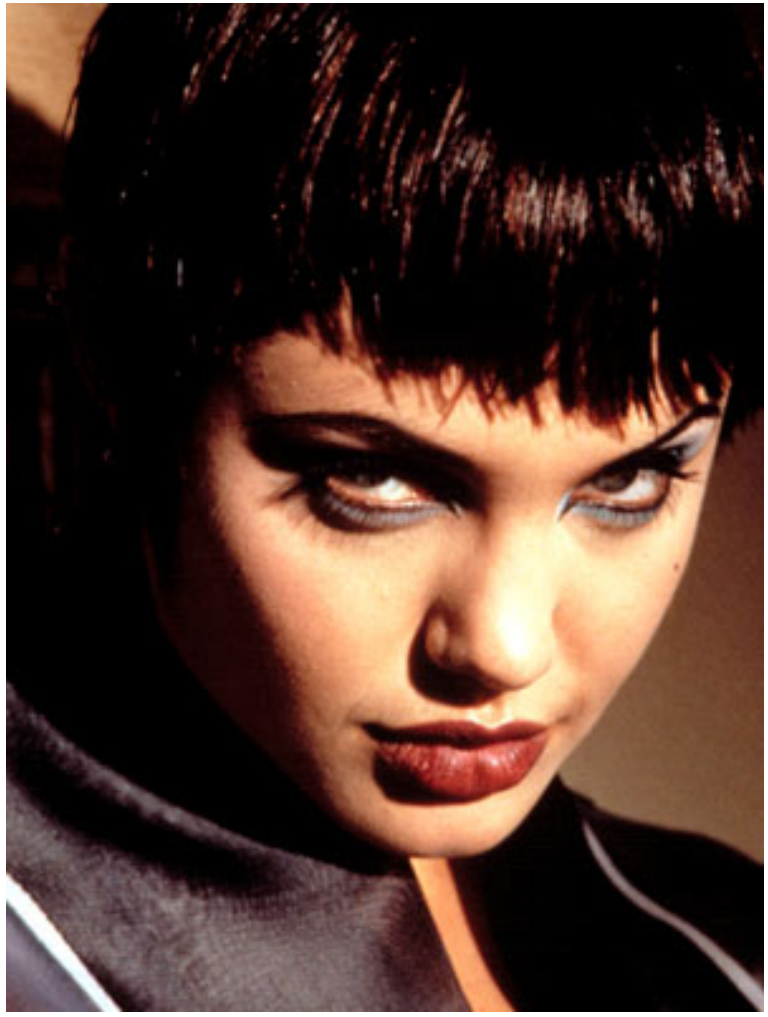
A vulnerability can and will be abused

What if I told you:

Criminals will be happy to leverage backdoors created by government

It does not matter if the crypto product has a weakness to allow investigations or the software has a backdoor to help law enforcement. Data and vulnerabilities WILL be abused and exploited.

Hacker types anno 1995



Lets go back to hacking

Hacker types anno 2008

Lisbeth Salander from the Stieg Larsson's award-winning Millennium series does research about people using hacking as a method to gain access

How can you find information about people?

From search patterns to persons

SOLIDO NETWORKS

First identify some basic information

Use search patterns like from email to full name

Some will give direct information about target

Others will point to intermediary information, domain names

Pivot and redo searching when new information bits are found

What information is public? (googledorks!)

Example patterns - for a Dane

Name, fullname, aliases

IDs and membership information, CPR (kind a like social security number)

Computerrelated information: IP, Whois, Handles, IRC nicks

Nick names

Writing style, specific use of words, common speling mistakes

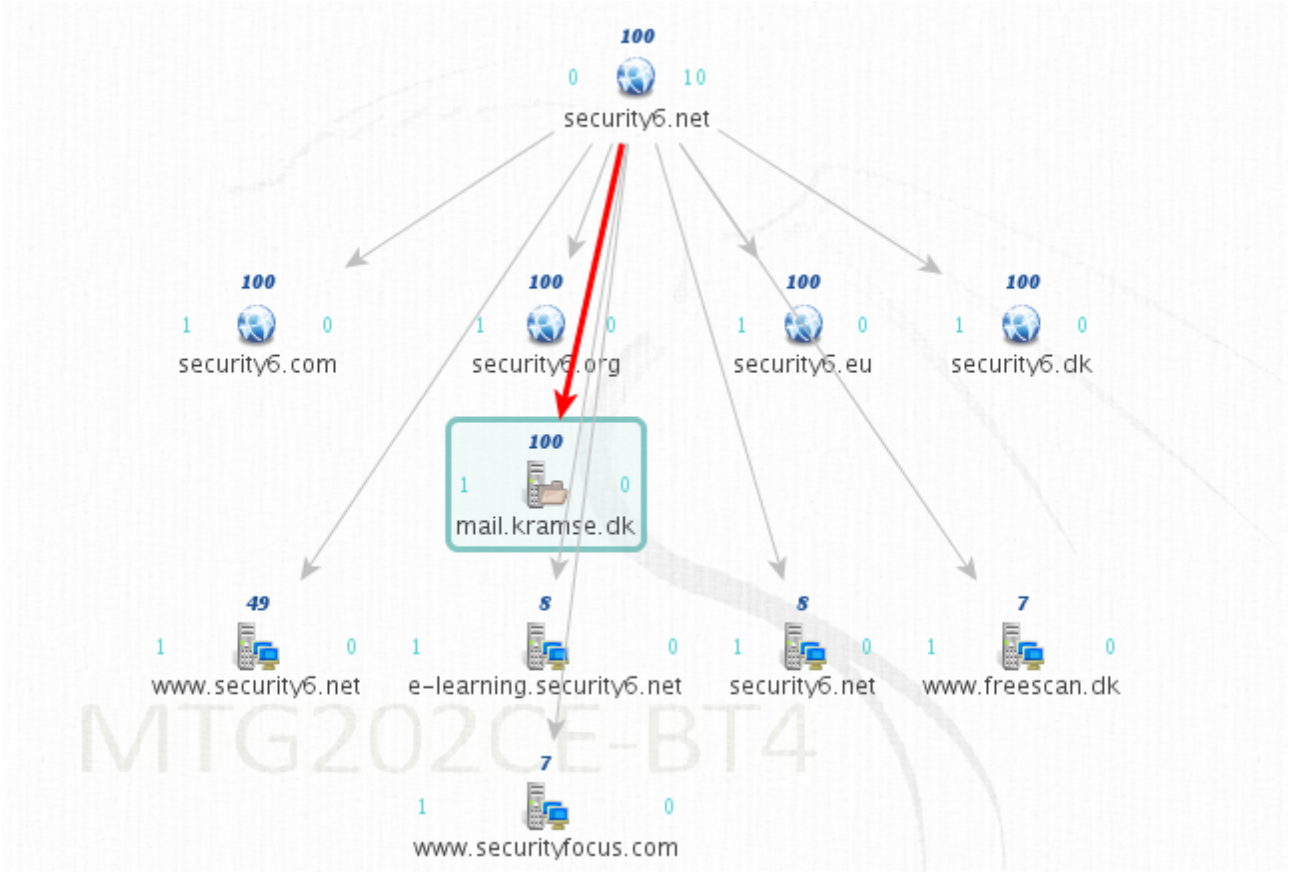
Be creative

Google for it

Google as a hacker tools?

Concept named googledorks when google indexes information not supposed to be public `http://johnny.ihackstuff.com/`

Lisbeth in a box?



Maltego can automate the mining and gathering of information uses the concept of transformations

`http://www.paterva.com/maltego/`

Hvordan bliver du sikker

Lad være med at bruge computere

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

Brug en sikker konfiguration, minimumskonfiguration

Brug sikre protokoller, kryptering: SSH, IMAPS, POP3S, OpenPGP, HTTPS, Tor

Opsætning af netværk, hvordan? Security Configuration Guides + paranoia

- `http://csrc.nist.gov/publications/PubsSPs.html`
- `http://www.nsa.gov/research/publications/index.shtml`
- `http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml`

Ånden til at hacke

Don’t Panic!

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

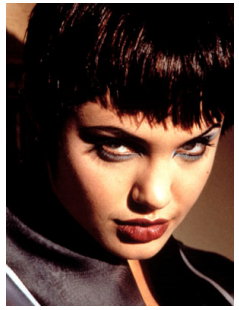
Oprindeligt betød hacking at man udforskede, undersøgte, involverede sig

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 ☺

Hackerværktøjer



- Nmap, Nping - tester porte, godt til firewall admins `http://nmap.org`
- Metasploit Framework gratis på `http://www.metasploit.com/`
- Wireshark avanceret netværkssniffer - `http://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`

Kilde: Angelina Jolie fra Hackers 1995

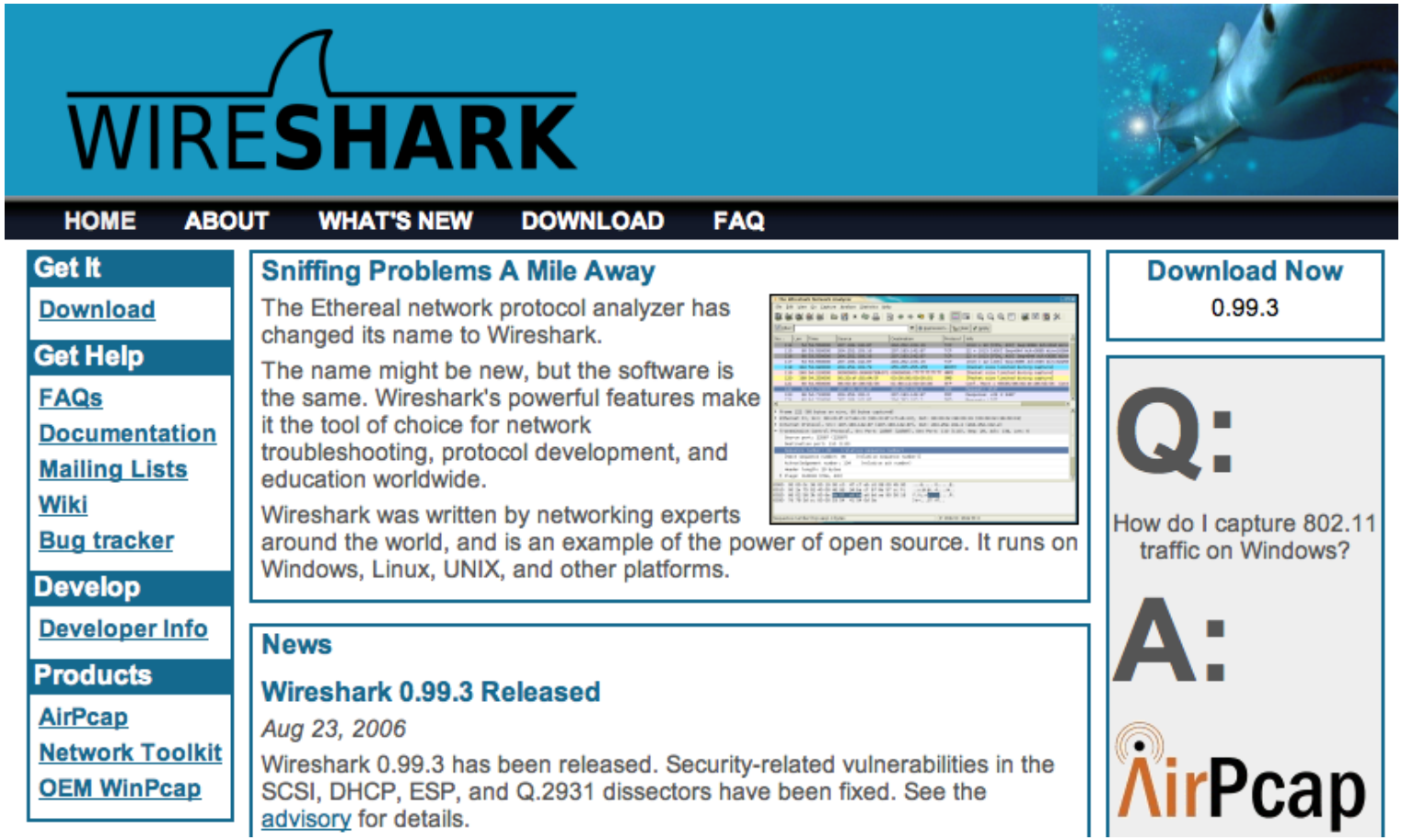
Kali Linux the new backtrack

BackTrack `http://www.backtrack-linux.org`

Kali `http://www.kali.org/`

Wireshark - `http://www.wireshark.org` avanceret netværkssniffer

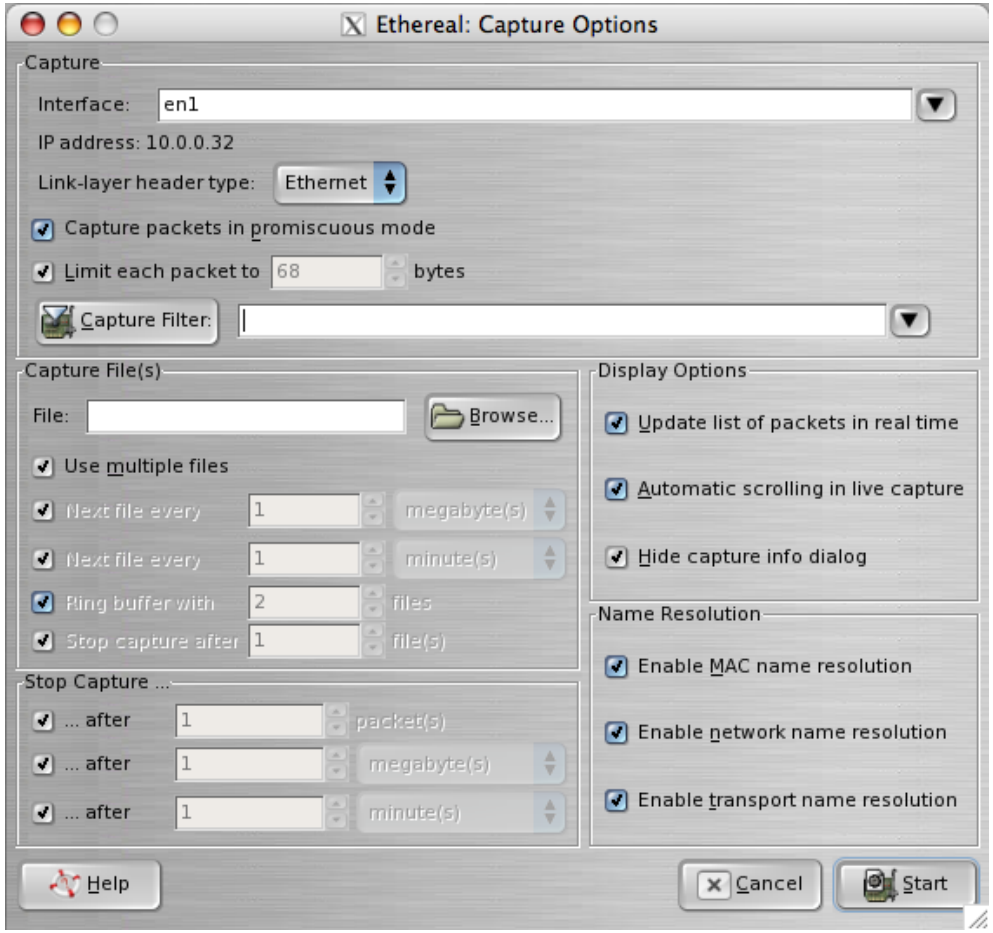
Wireshark - grafisk pakkesniffer



`http://www.wireshark.org`

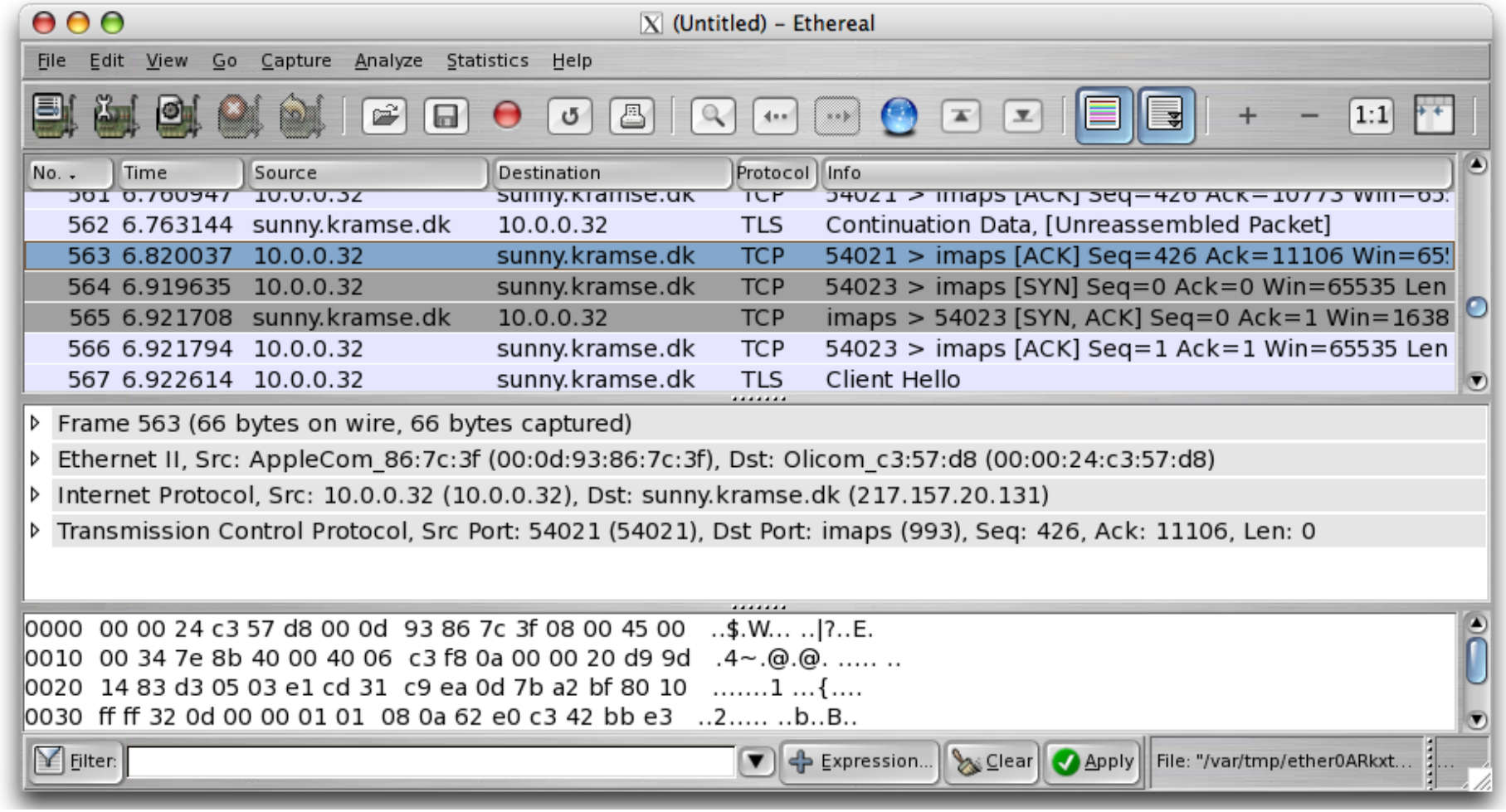
både til Windows og UNIX, tidligere kendt som Ethereal

Brug af Wireshark



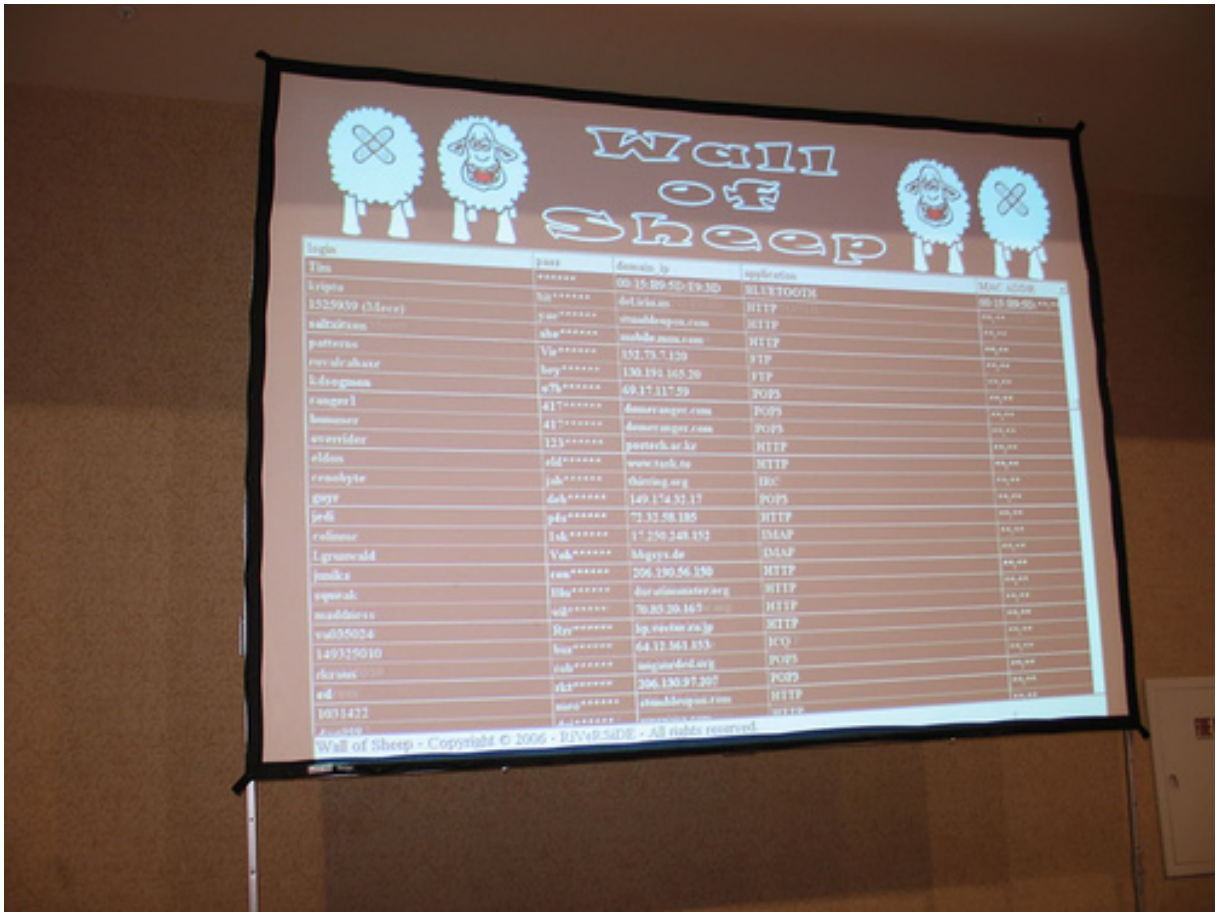
Man starter med Capture - Options

Brug af Wireshark



Læg mærke til filtermulighederne

Wall of sheep



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

Vi laver nu øvelsen

Wireshark installation

som er øvelse 1 fra øvelseshæftet.

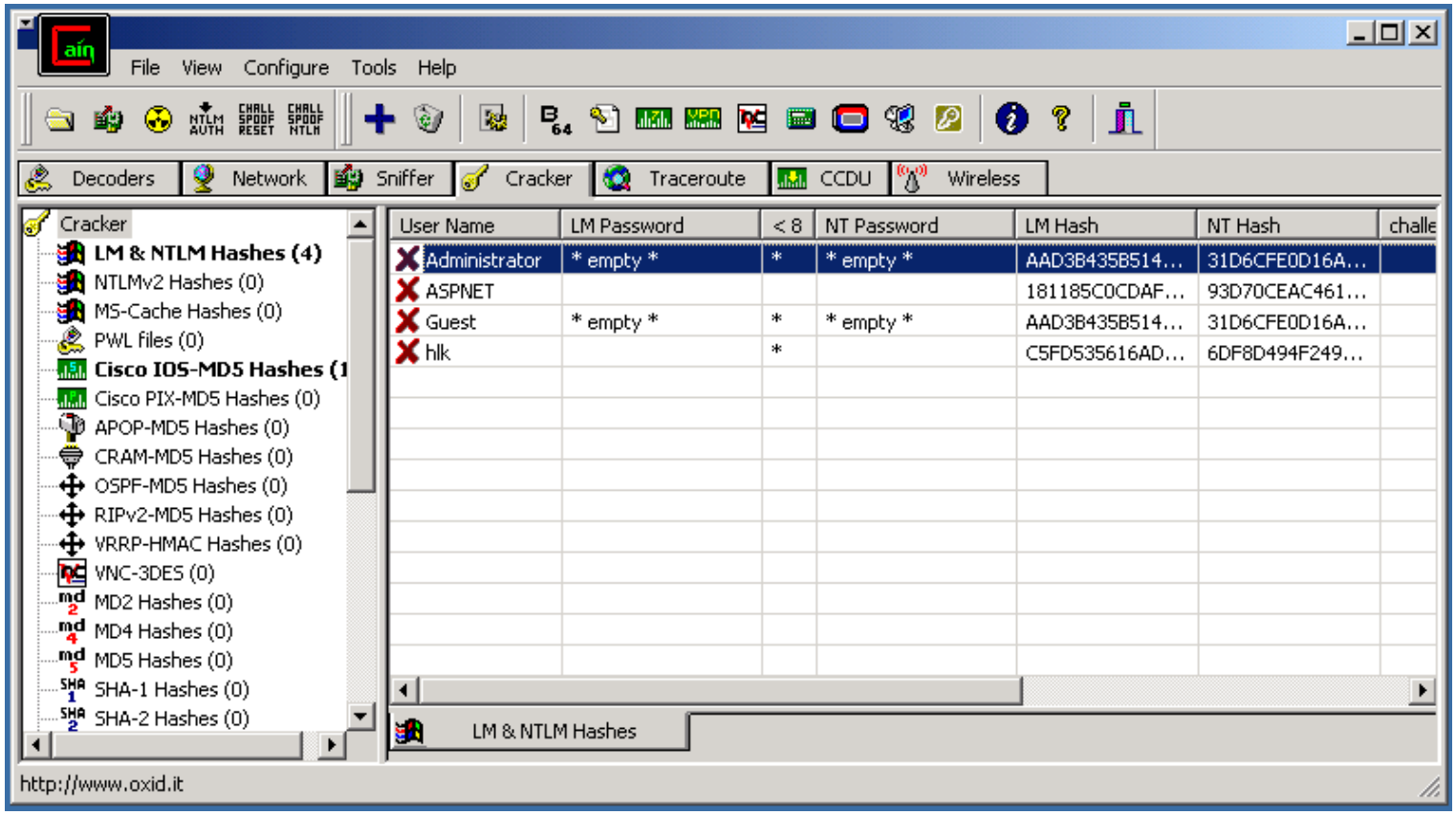
SOLIDO NETWORKS

Vi laver nu øvelsen

Sniffing network packets

som er øvelse 2 fra øvelseshæftet.

Cain & Abel



sniff, crack and hack `http://www.oxid.it`

John the ripper

> 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

Suricata IDS/IPS/NSM

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF and its supporting vendors.

- `http://suricata-ids.org/`
- `http://openinfosecfoundation.org`

Netflow

Netflow is getting more important, more data share the same links

Accounting is important

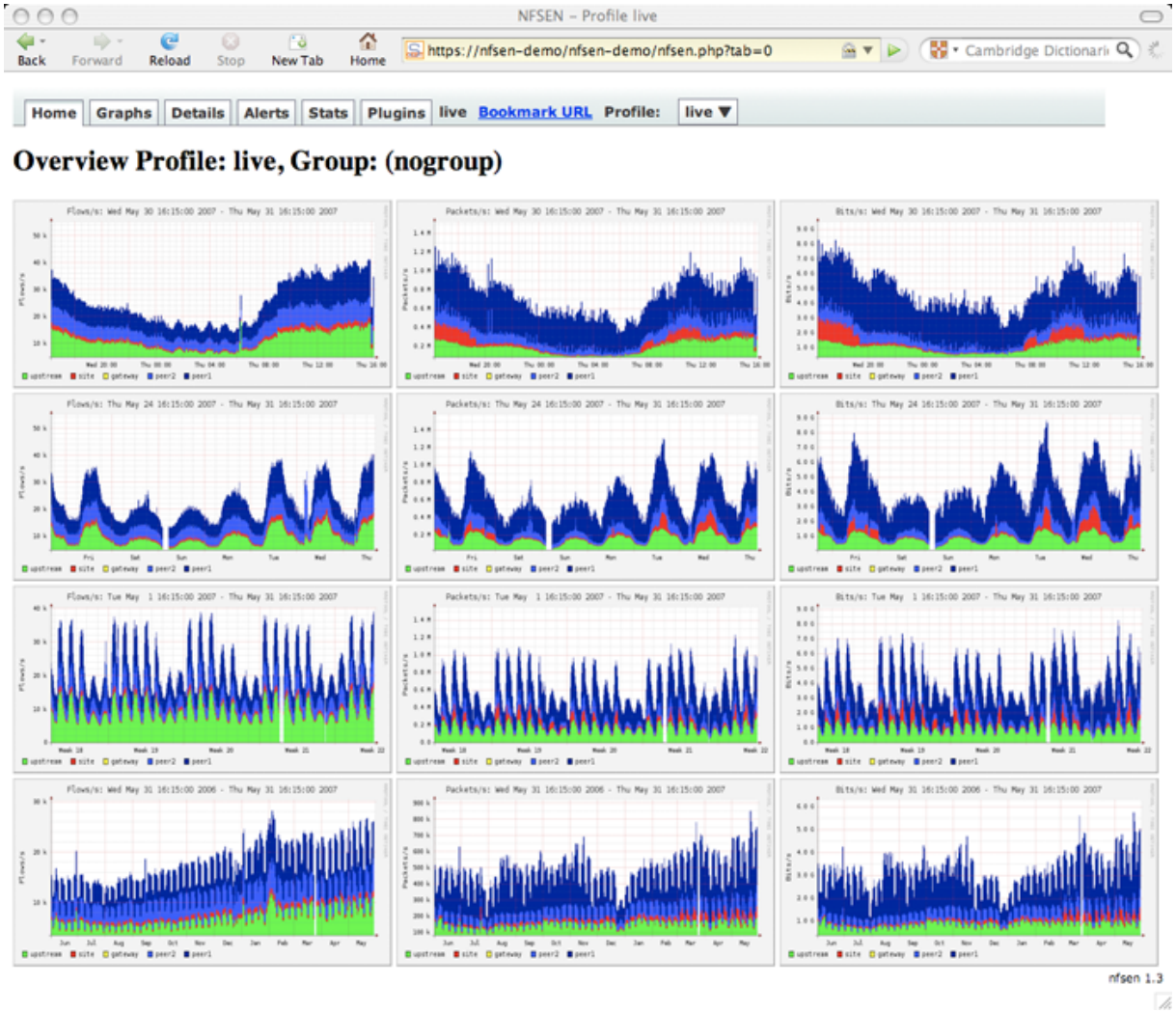
Detecting DoS/DDoS and problems is essential

Netflow sampling is vital information - 123Mbit, but what kind of traffic

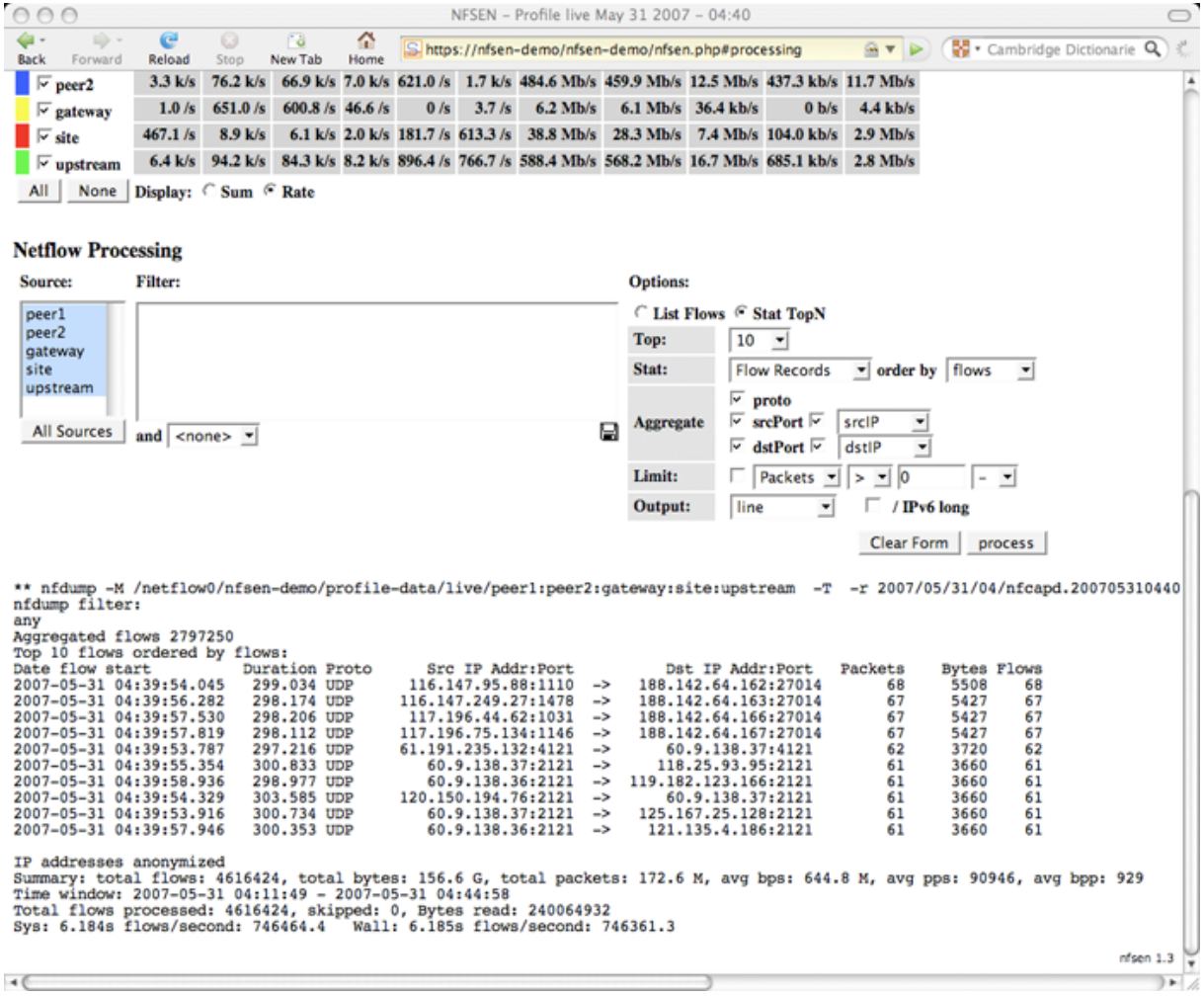
We use mostly NFSen, but are looking at various software packages
`http://nfsen.sourceforge.net/`

Currently also investigating sFlow - hopefully more fine grained

Netflow using NFSen



Netflow processing from the web interface



Bringing the power of the command line forward

Hackers do not discriminate

We have seen lots of hacker stories, and we learn:

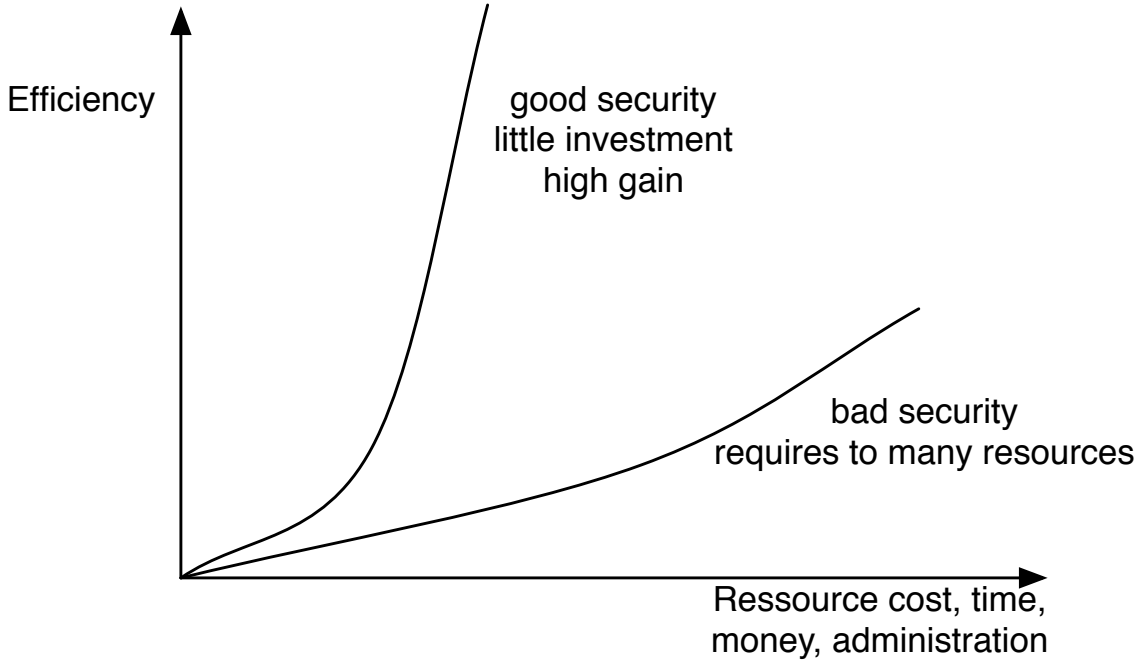
We are all targets of hacking

Social Engineering rockz! Phishing works.

Anyone can be hacked - resources used to protect vs attackers resources

Hacking is not cool

Good security



You always have limited resources for protection - use them as best as possible

First advice

Use technology

Learn the technology - read the freaking manual

Think about the data you have, upload, facebook license?! WTF!

Think about the data you create - nude pictures taken, where will they show up?

- Turn off features you don't use
- Turn off network connections when not in use
- Update software and applications
- Turn on encryption: IMAP**S**, POP3**S**, HTTP**S** also for data at rest, full disk encryption, tablet encryption
- Lock devices automatically when not used for 10 minutes
- Dont trust fancy logins like fingerprint scanner or face recognition on cheap devices

First advice use the modern operating systems

Newer versions of Microsoft Windows, Mac OS X and Linux

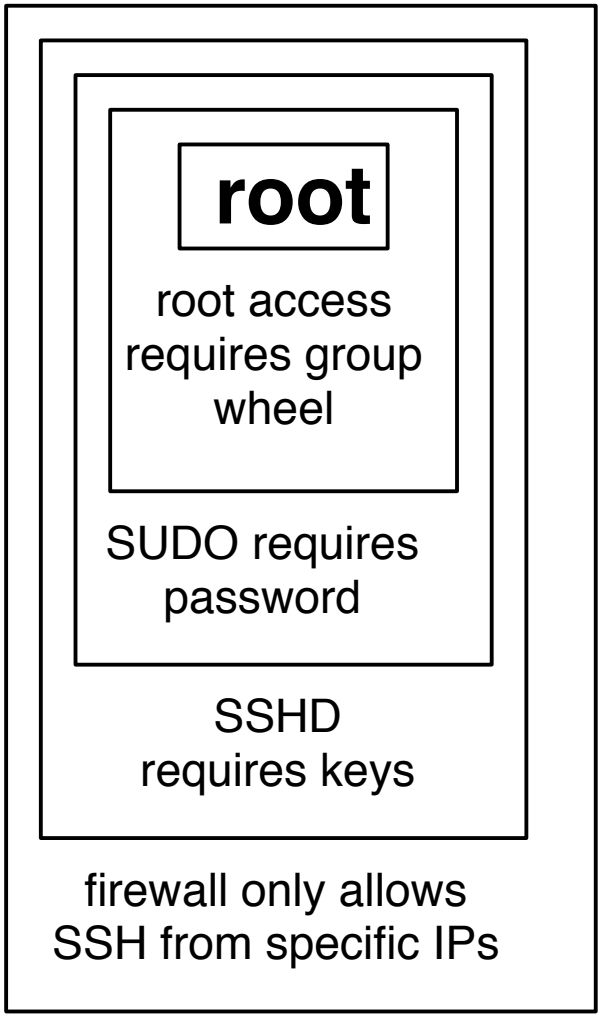
- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

Note: these still have errors and bugs, but are better than older versions

OpenBSD has shown the way in many cases
`http://www.openbsd.org/papers/`

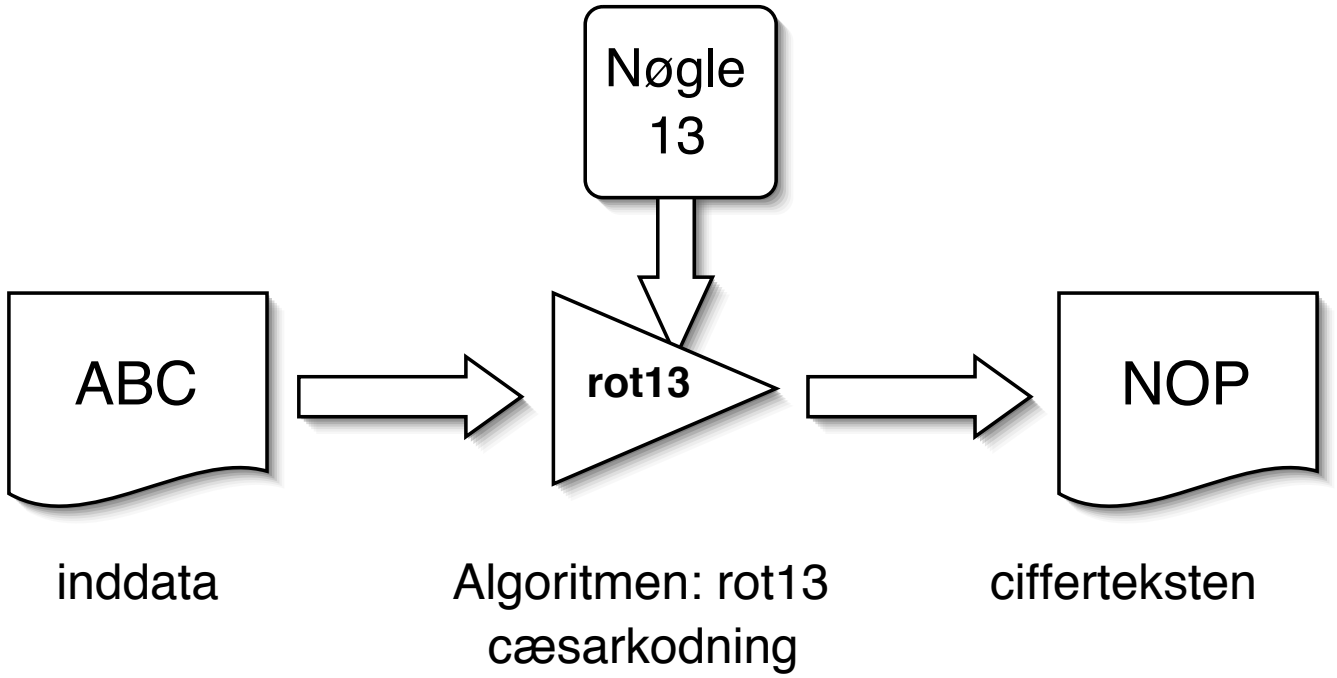
Always try to make life worse and more costly for attackers

Defense in depth



Defense using multiple layers is stronger!

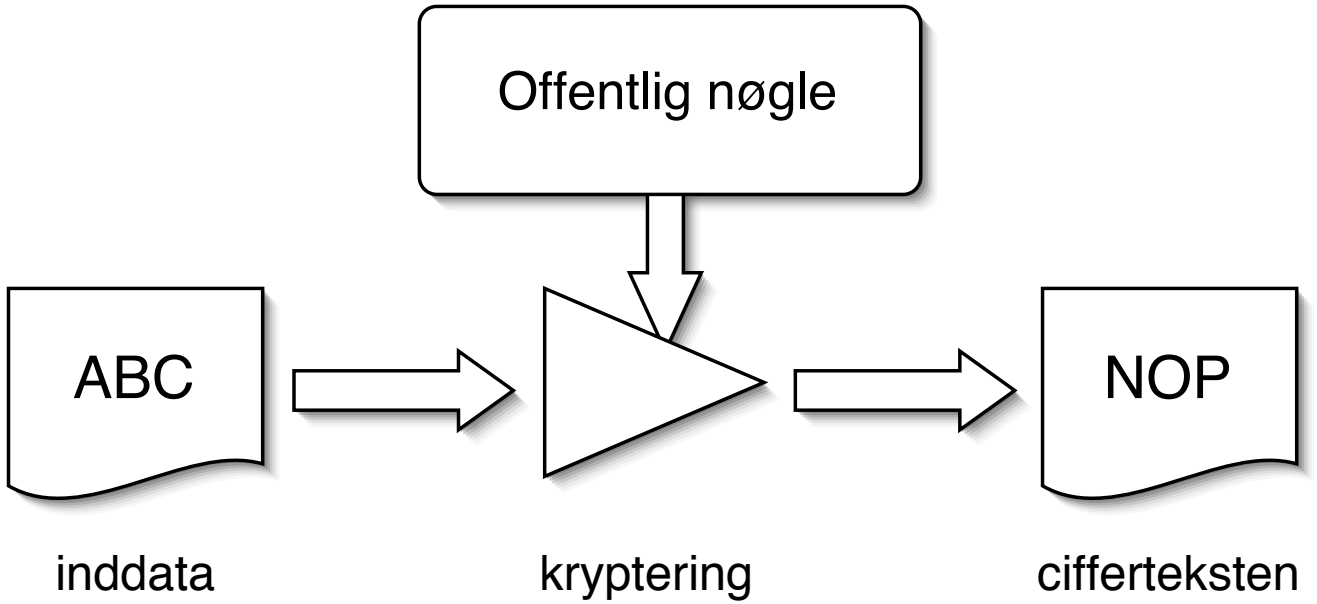
Kryptografi



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

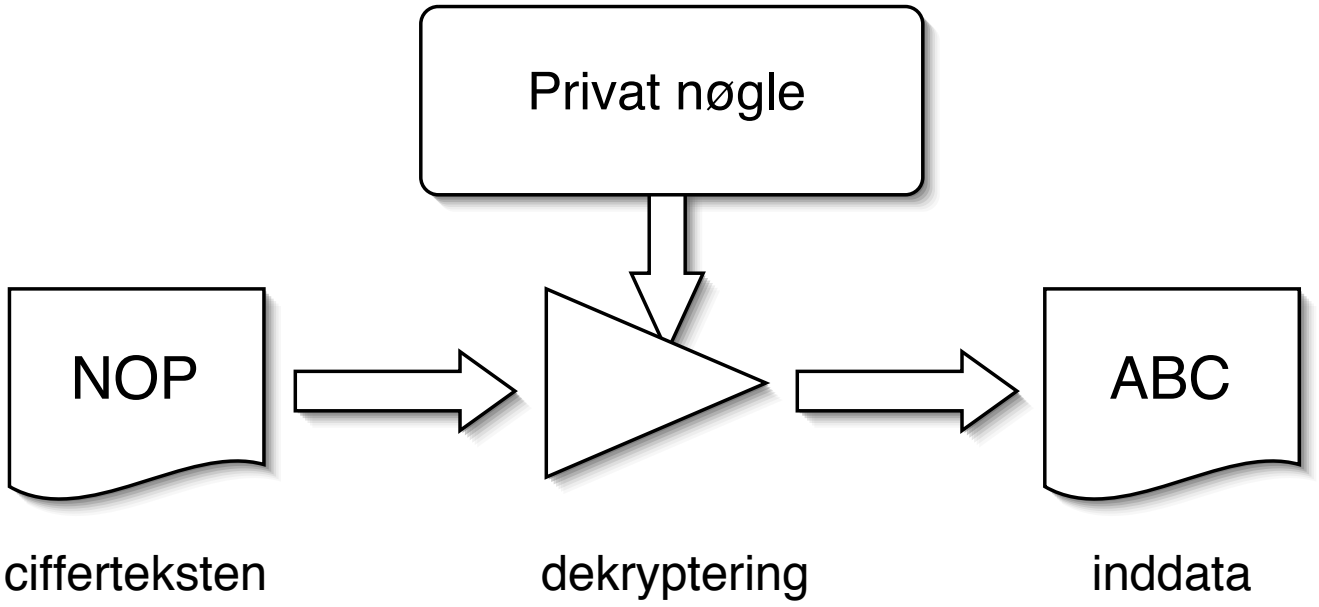
Public key kryptografi - 1



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

Public key kryptografi - 2



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

Kryptografiske principper

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

Et successfuldt 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

DES, Triple DES og AES

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://www.cs.bc.edu/~straubin/cs381-05/blockciphers/rijndael_ingl`
`swf?utm_content=bufferfabef&utm_source=buffer&utm_medium=twitter&u`
`campaign=Buffer`

hashing algoritmer

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.

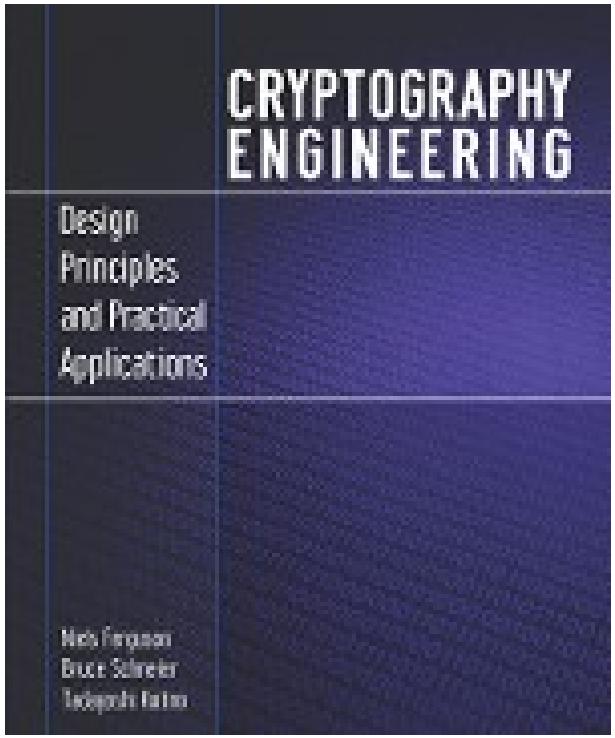
...

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`

Cryptography Engineering

SOLIDO NETWORKS



Cryptography Engineering by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno

`https://www.schneier.com/book-ce.html`

Sikre protokoller som bruger crypto

SOLIDO NETWORKS

Kryptering af e-mail

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

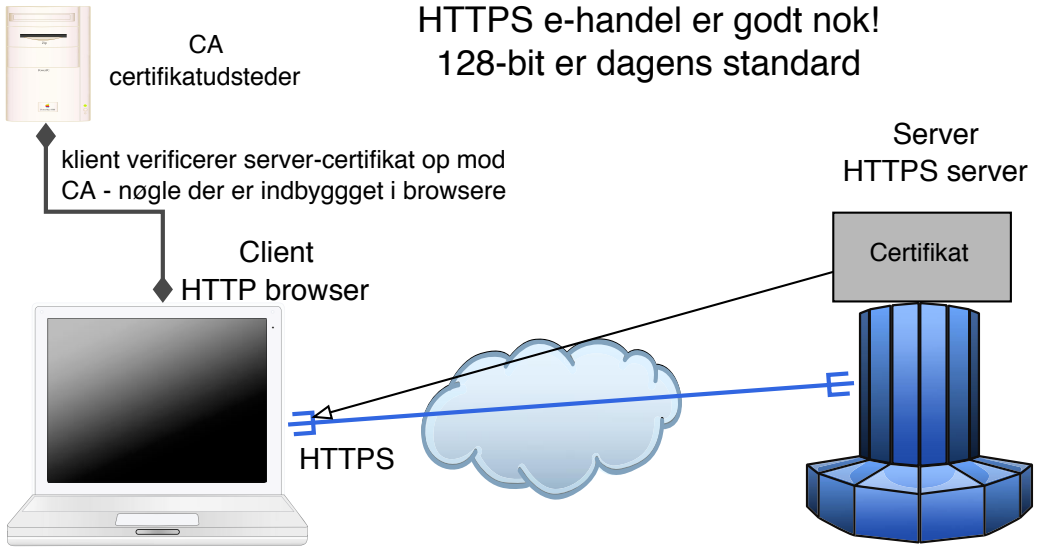
Kryptering af sessioner SSL/TLS

- 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.

SSL og TLS

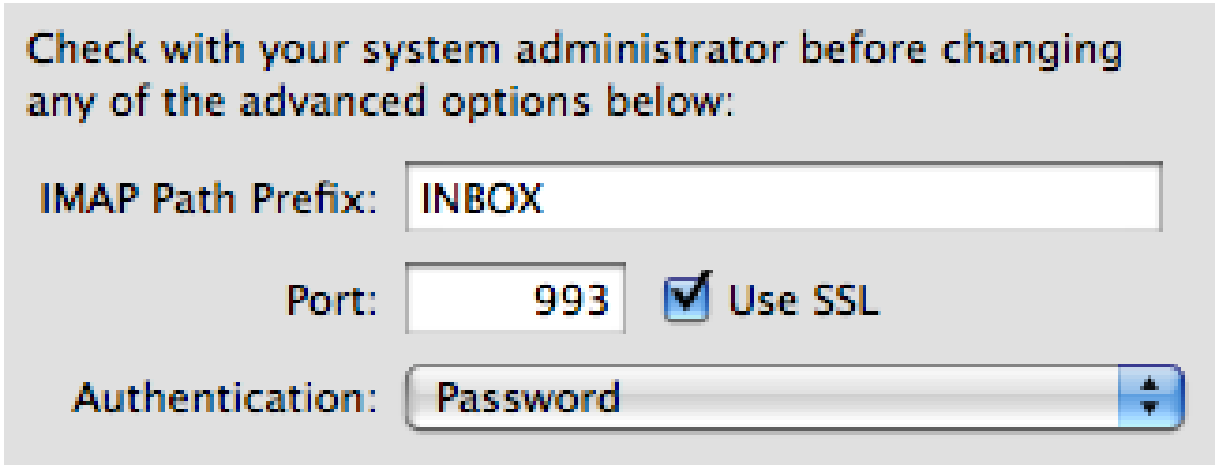


Oprindeligt udviklet af Netscape Communications Inc.

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

SSL/TLS udgaver af protokoller



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

Secure Shell - SSH og SCP

Hvad er Secure Shell SSH?

Oprindeligt udviklet af Tatu YlÃ¶nen 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

Do NOT USE FTP

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

FileZilla - understøtter SFTP

FileZilla Features

Overview

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

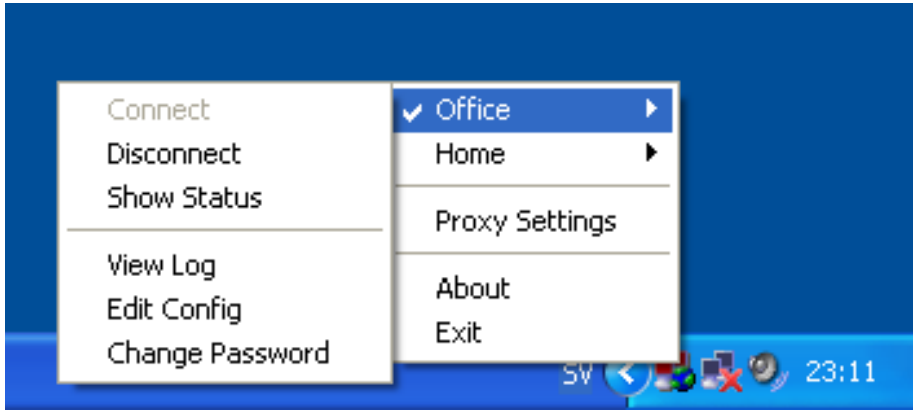
Features

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/

VPN



Virtual Private Networks are useful - or even required when travelling

VPN `http://en.wikipedia.org/wiki/Virtual_private_network`

SSL/TLS VPN - Multiple incompatible vendors: OpenVPN, Cisco, Juniper, F5 Big IP

IETF IPsec does work cross-vendors - sometimes, and is also increasingly becoming blocked or unusable due to NAT :-(

Internet sniffing by government

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

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.

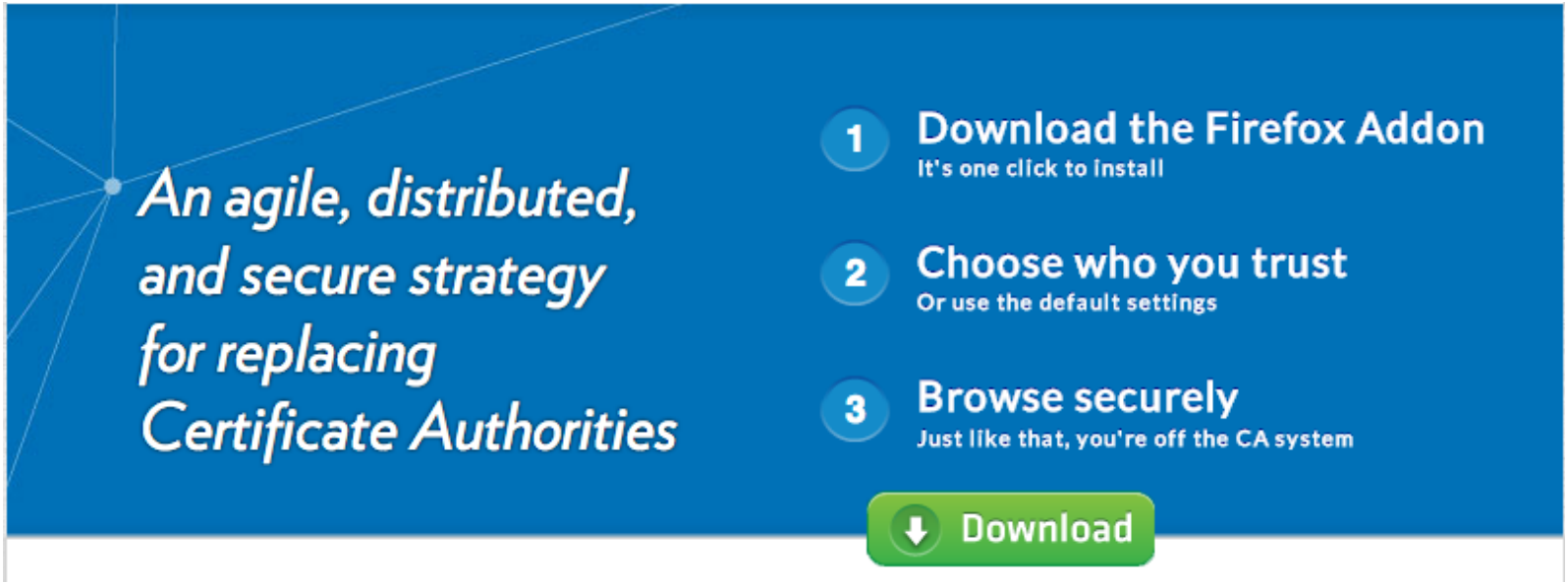
`http://www.eff.org/https-everywhere`

CertPatrol - which site uses which certificate

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/`

Convergence - who do you trust



http://convergence.io/

Warning: radical change to how certificates work

SOLIDO NETWORKS

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)

Censurfridns.dk uncensoredDNS

```
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!

PS nu også med DNS på port 5353

DNSSEC trigger

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

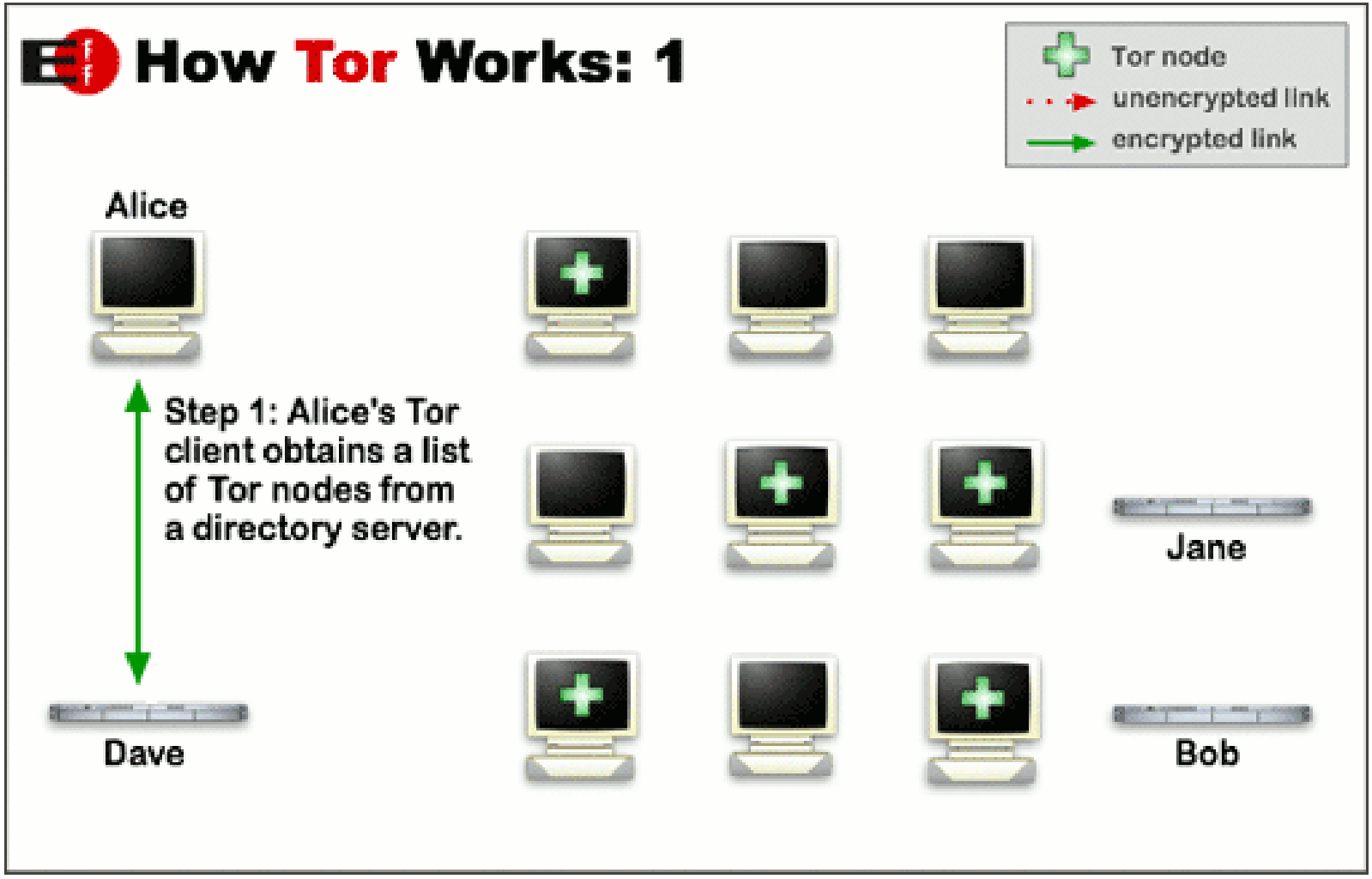
- DNSSEC Validator for firefox
  `https://addons.mozilla.org/en-us/firefox/addon/dnssec-validator/`
- OARC tools `https://www.dns-oarc.net/oarc/services/odvr`
- `http://www.nlnetlabs.nl/projects/dnssec-trigger/`

Tor project

`https://www.torproject.org/`

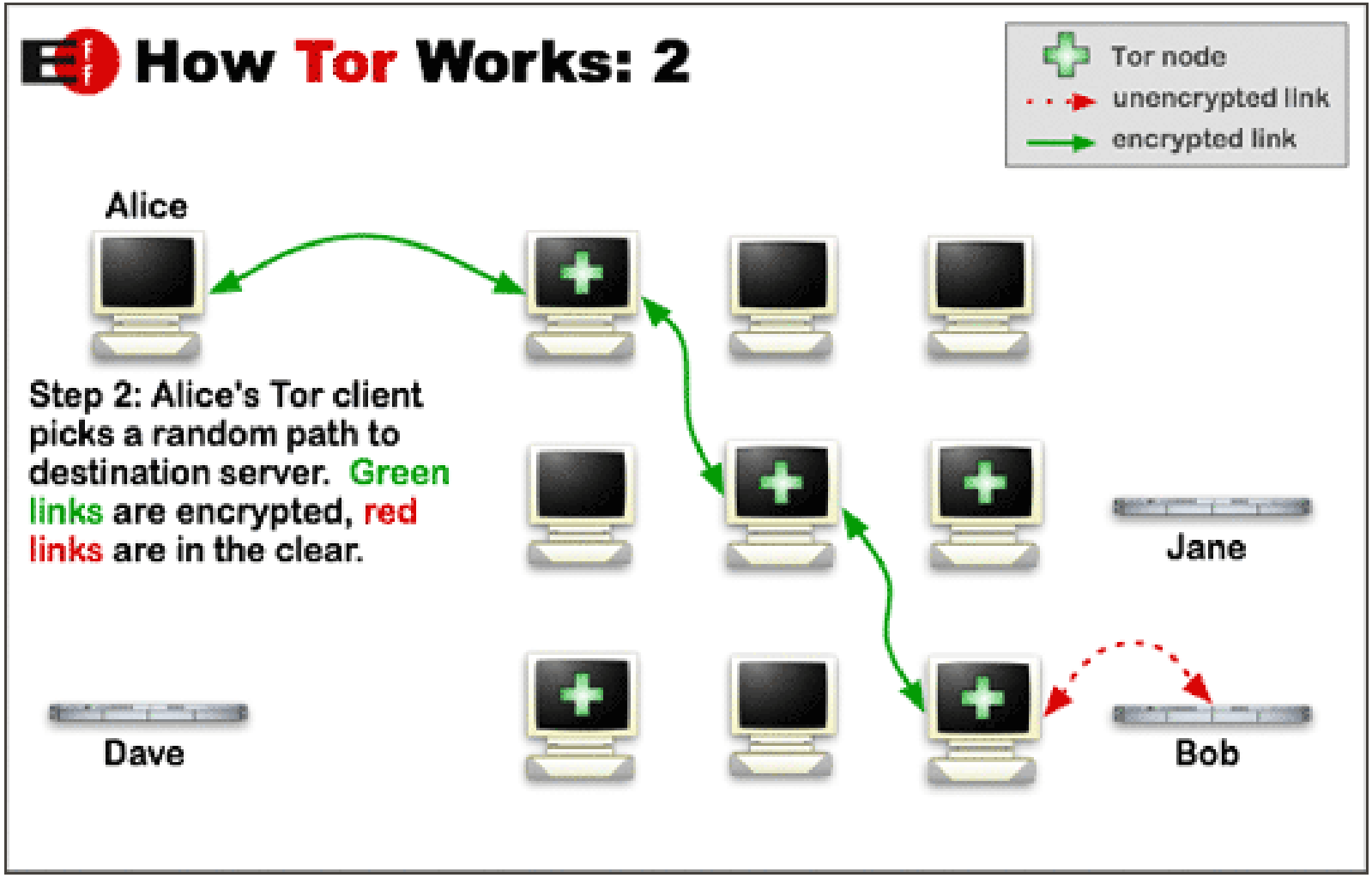
Der findes alternativer, men Tor er mest kendt

Tor project - how it works 1



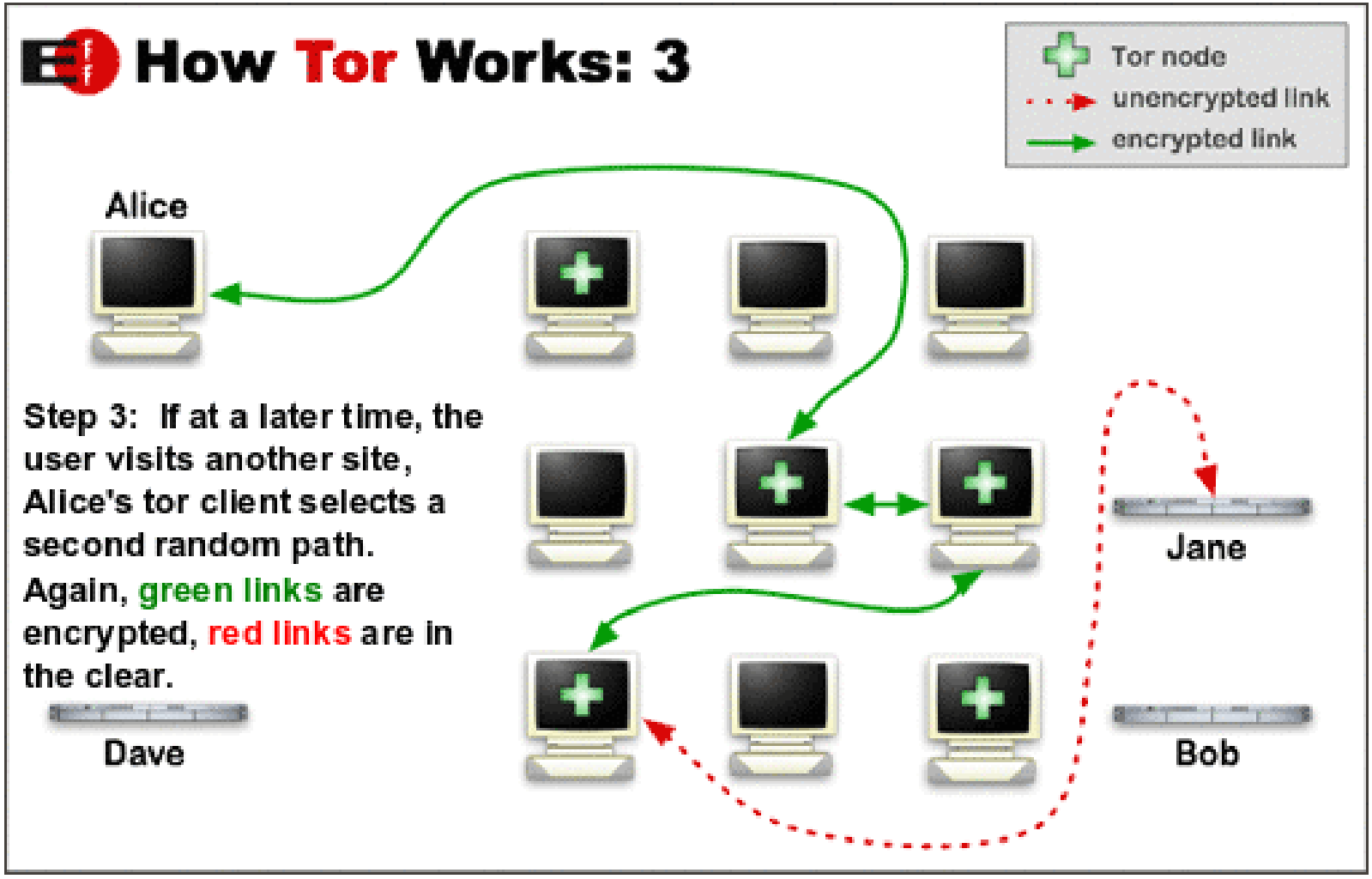
pictures from `https://www.torproject.org/about/overview.html.en`

Tor project - how it works 2



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

Tor project - how it works 3



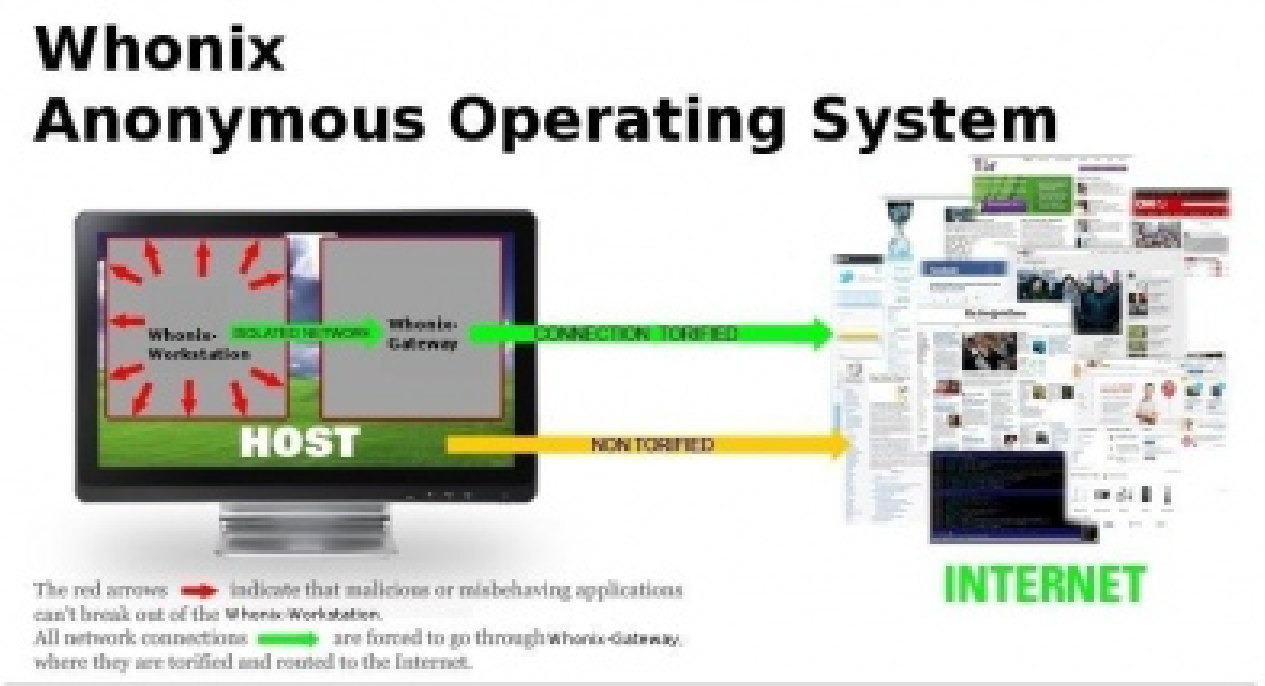
pictures from `https://www.torproject.org/about/overview.html.en`

Tor project install

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

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

Whonix



Whonix is an operating system focused on anonymity, privacy and security. It's based on the Tor anonymity network[5], Debian GNU/Linux[6] and security by isolation. DNS leaks are impossible, and not even malware with root privileges can find out the user's real IP.

`https://www.whonix.org/`

Bonus: brug Bitcoins?

Part III: Mere Hacking, Hackerværktøjer

Teknisk hvad er hacking - og værktøjer
Mere frit - vi undersøger diverse emner som hackere

Målet for denne del

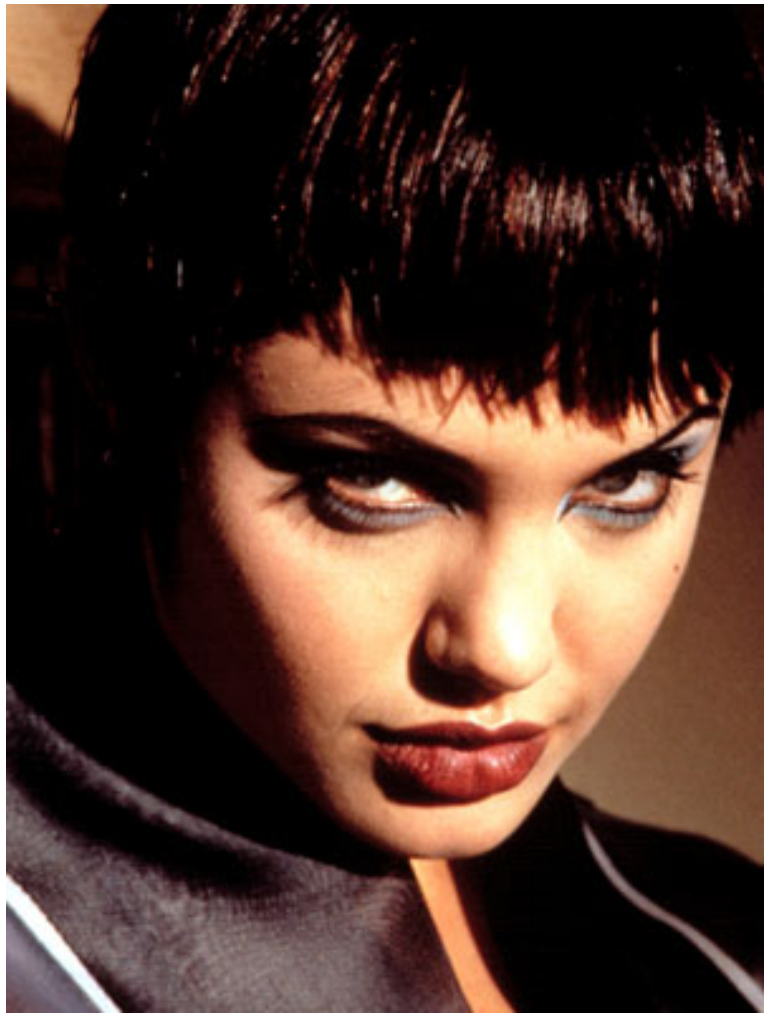
Don’t Panic!

Introduce hacking and a couple of hacker tools

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

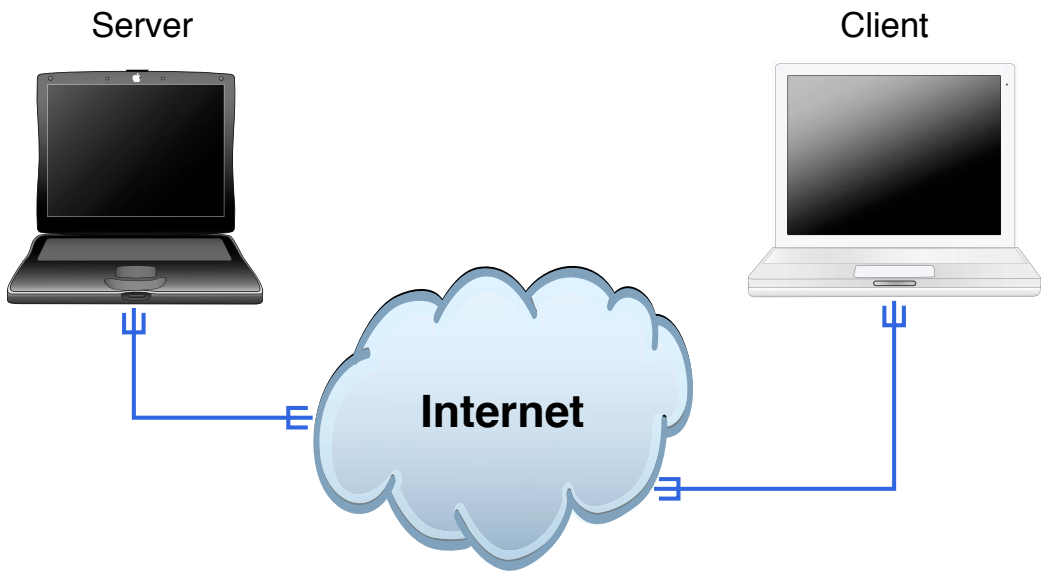
PS Sorry about the many TLAs ... og danglish

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



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

Internet today



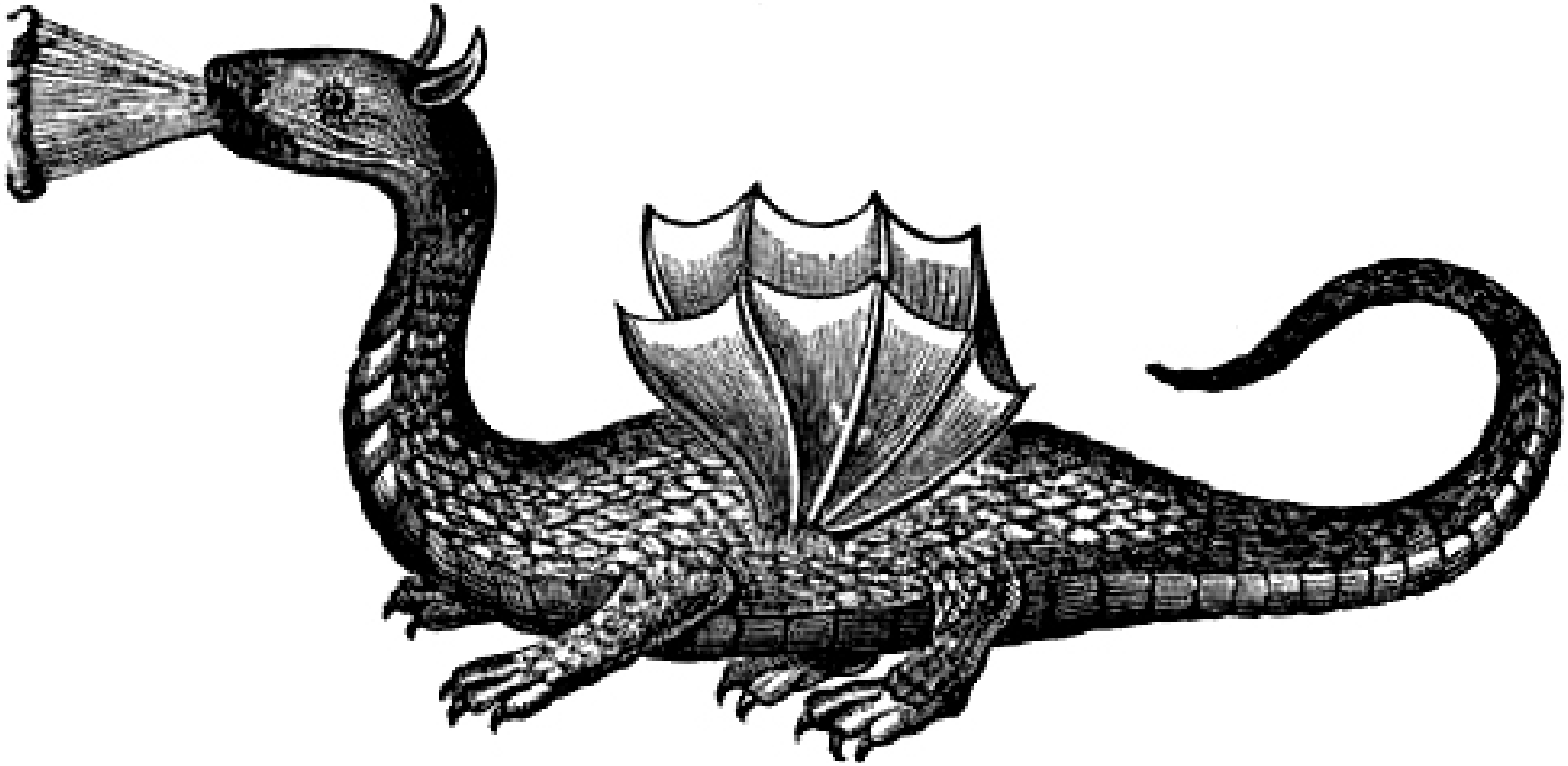
Clients and servers

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



Hacker - cracker

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

Definition af hacking, oprindeligt

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`

Internet er åbne standarder!

SOLIDO NETWORKS

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 $\rightarrow$ Draft Standard $\rightarrow$ Standard

Åbne standarder = åbenhed, ikke garanti for sikkerhed

The Internet Worm 2. nov 1988

SOLIDO NETWORKS

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`

Aftale om test af netværk

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!

Hacking er magi

Hacking ligner indimellem magi

Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

Hacking eksempel - det er ikke magi

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

Myten om MAC filtrering

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

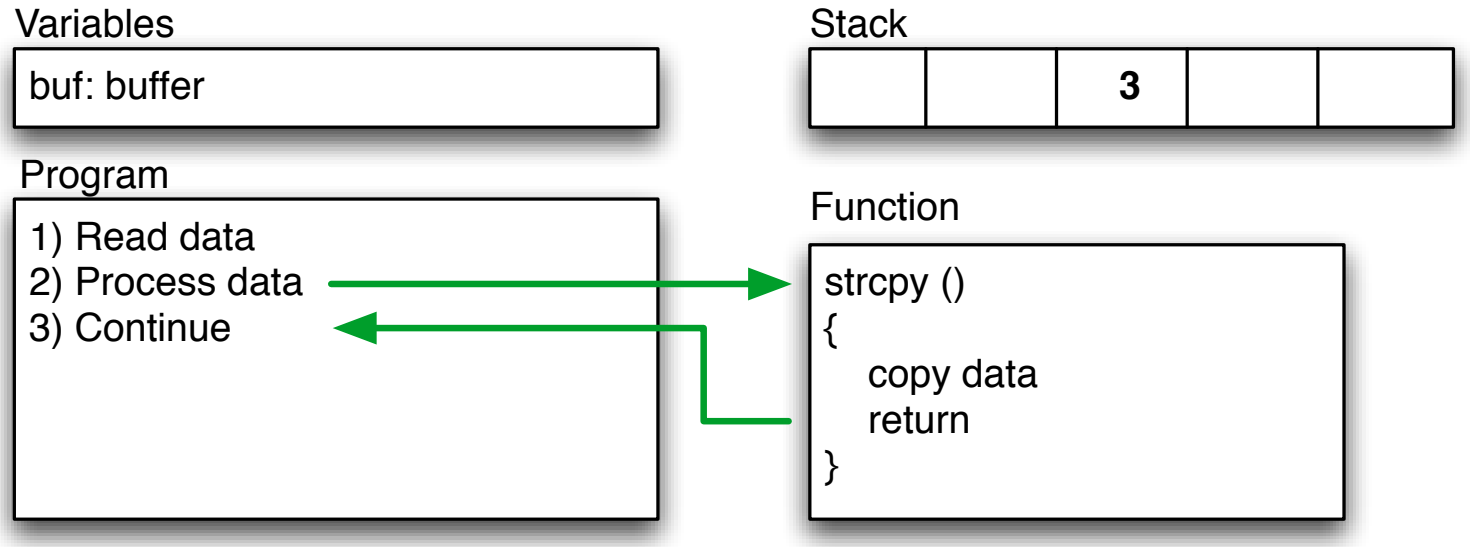
buffer overflows is a C problem

SOLIDO NETWORKS

Et buffer overflow is what happens if some internal structure in programs are modified by an attacker for the purpose of taking control of the application and system. Often a program will crash, but if the attacker can input specific data it might be possible to point to their own **shell code** containing instructions to be executed.

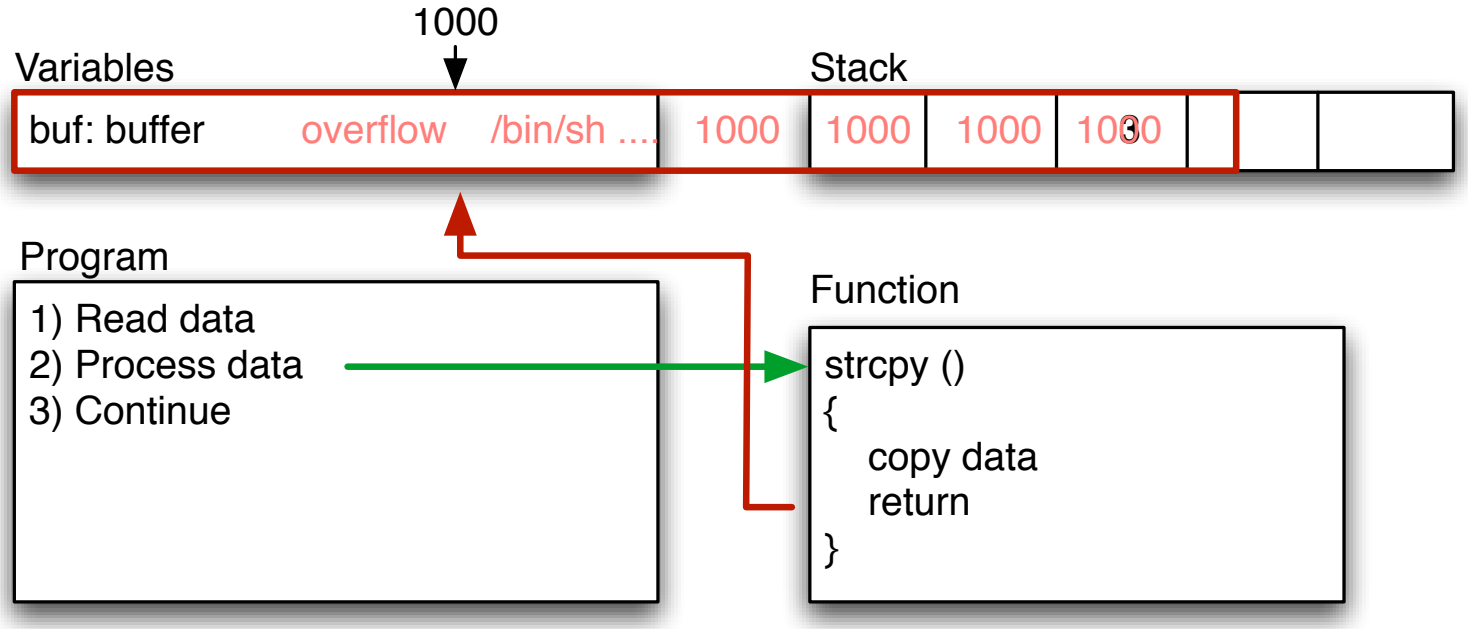
Stack protection today both a specific technique and generic term for adding protection to operating systems and programs to reduce the likelihood of buffer overflows succeeding. The main features are protecting areas in memory by making them non-writeable and non-executable. StackGuard and Propolice are some popular choices

Buffer og stacks




```
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

Exploits - exploiting vulnerabilities

an exploit is a program designed to abuse some weakness or vulnerability

- Usually the expliot will demonstrate the weakness found, proof-of-concept (PoC)
- Usually the exploit will only include one vulnerability and is targeted at specific versions of the vulnerable program
- Exploits can be a few lines of code or multiple pages
- Used to be written using Perl and C, but today popular choices include Ruby and Python
- Can often be plugged into the Metasploit framework for direct execution

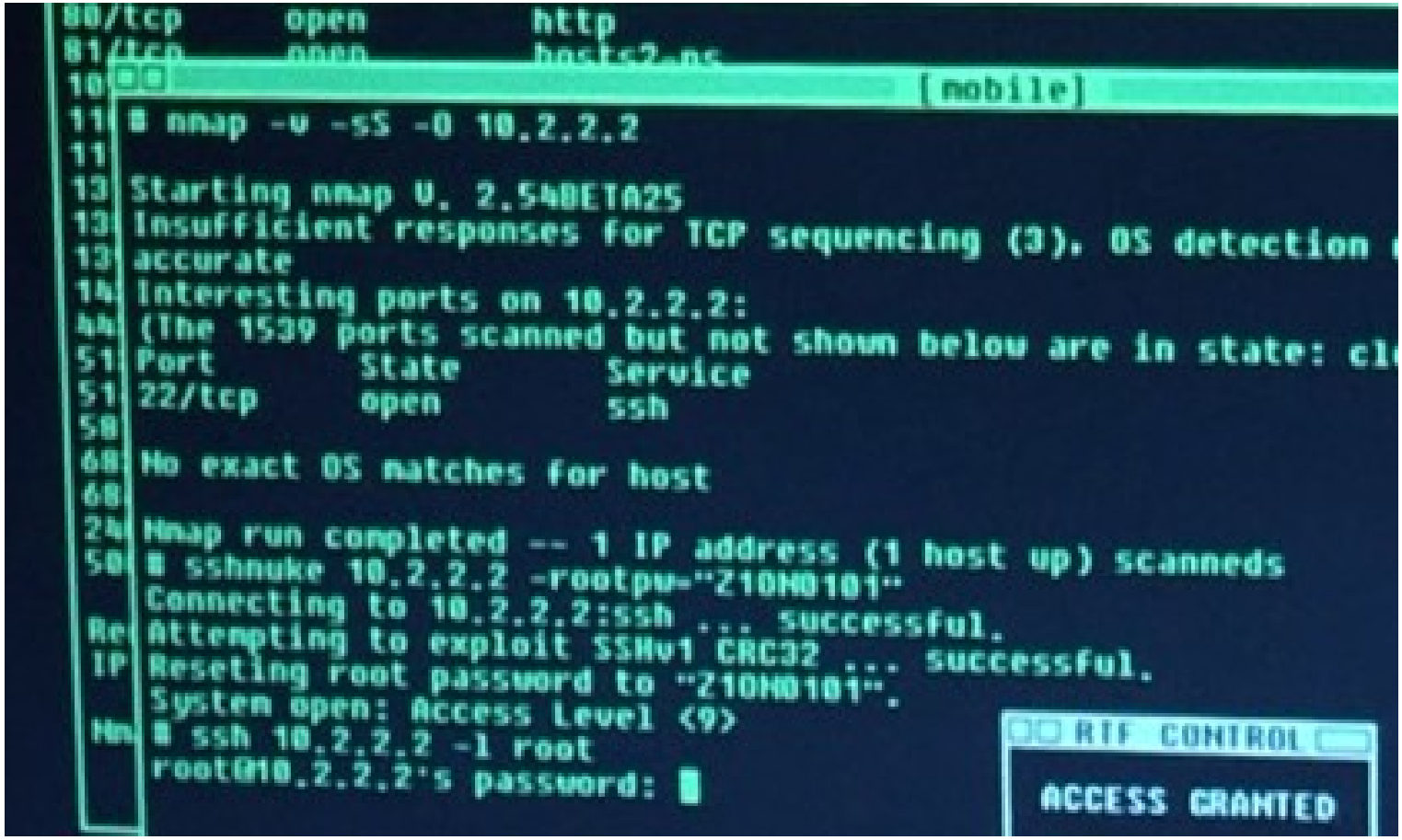
Exploit sample

```
$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

Matrix style hacking anno 2003

Trinity breaking in



http://nmap.org/movies.html

Meget realistisk http://www.youtube.com/watch?v=51lGCTgqE_w

Principle of least privilege

Why execute applications with administrative rights - if they only need to read from a database

principle of least privilege execute code only with the most restrictive set of permissions required to perform a task

Privilege escalation

privilege escalation is what an attacker aims to perform

Trying to get from an authenticated user to a higher privileged administrative user id

Some functions in operating systems require higher privileges, and they can sometimes be persuaded to fail in spectacular ways

When an attacker can execute commands they can often find a way to exploit software and escalate privileges

local vs. remote exploits

local vs. remote signifies if the specific attack exploited is done from the operating system using a local command/feature or if this is done remotely across some network connection

remote root exploit - feared because it would grant administrative rights across a network connection

More often an attacker will combine a remote exploit with a privilege escalation exploit

zero-day exploits 0-days are not made public, but kept in small groups and suddenly can be found in use on the internet, or in specific use for a targeted attack

Since nobody is aware of the problem, there is no fix readily available from the vendors/programmers

The Exploit Database - dagens buffer overflow

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

Create your own exploits and spearphishing?

SOLIDO NETWORKS

Metasploit Still rocking the internet
`http://www.metasploit.com/`

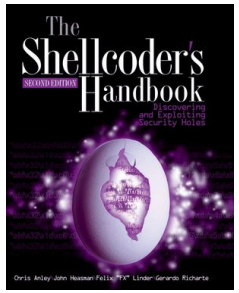
Armitage GUI fast and easy hacking for Metasploit
`http://www.fastandeasyhacking.com/`

Metasploit Unleashed
`http://www.offensive-security.com/metasploit-unleashed/Main_Page`

Social-Engineer Toolkit
`https://www.trustedsec.com/downloads/social-engineer-toolkit/`

You can get these easily on `http://www.kali.org`

Buffer overflows



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!

Code quality

SOLIDO NETWORKS

Why are programs still insecure?

Programs are complex!

Try implementing tools to improve quality

Hudson Extensible continuous integration server `http://hudson-ci.org/`

Sonar `http://www.sonarsource.org/`

Yasca can scan source code written in Java, C/C++, HTML, JavaScript, ASP, ColdFusion, PHP, COBOL, .NET, and other languages. Yasca can integrate easily with other tools
`http://www.scovetta.com/yasca.html`

Software analysis can help
`http://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html`

NB: you still have to think ☺

Stack protection

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`

We must allow open hacker tools

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`

OWASP top ten

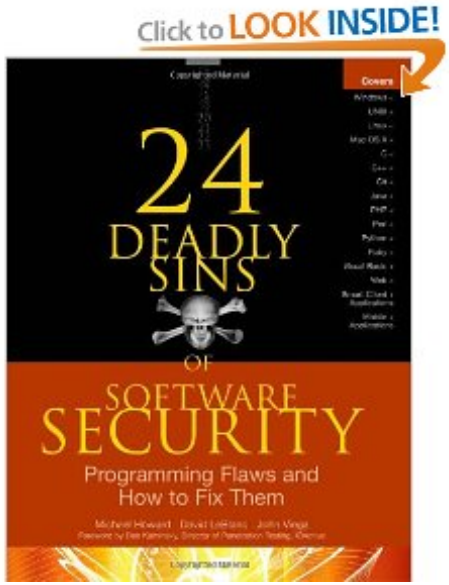
> The OWASP Top Ten provides a minimum standard for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

The Open Web Application Security Project (OWASP)

OWASP har gennem flere år udgivet en liste over de 10 vigtigste sikkerhedsproblemer for webapplikationer

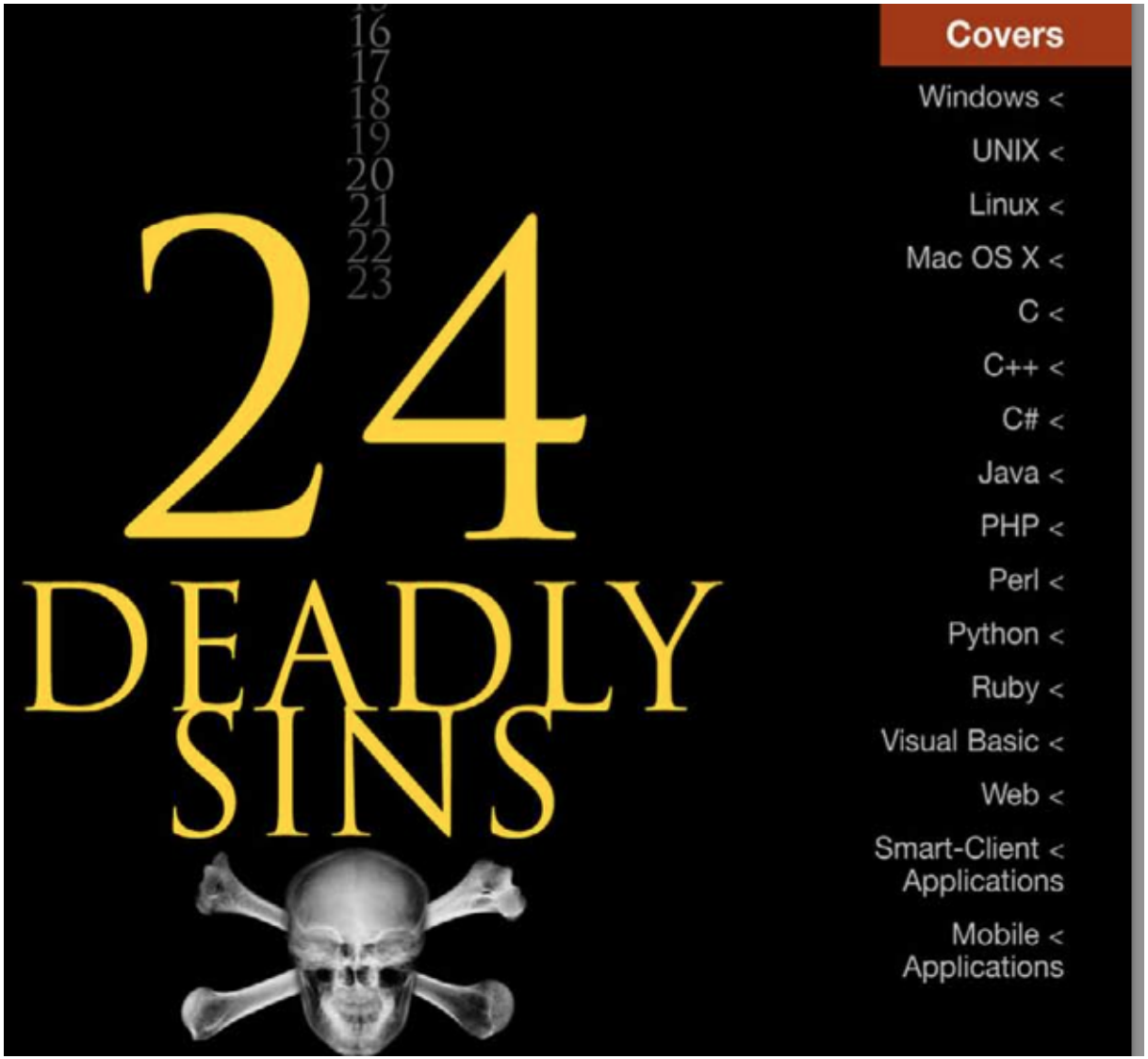
`http://www.owasp.org`

Deadly sins bogen



24 Deadly Sins of Software Security Michael Howard, David LeBlanc, John Viega 2. udgave, første hed 19 Deadly Sins

Deadly sins bogen - close up



Deadly Sins 1/2

SOLIDO NETWORKS

Part I Web Application Sins 1-4

- 1) SQL Injection
- 2) Web Server-Related Vulnerabilities
- 3) Web Client-Related Vulnerabilities (XSS)
- 4) Use of Magic URLs, Predictable Cookies, and Hidden Form Fields

Part II Implementation Sins 5-18
5) Buffer Overruns, 6) Format String, 7) Integer Overflows, 8) C++ Catastrophes, 9) Catching Exceptions, 10) Command Injection 11) Failure to Handle Errors Correctly 12) Information Leakage 13) Race Conditions 14) Poor Usability 15) Not Updating Easily 16) Executing Code with Too Much Privilege 17) Failure to Protect Stored Data 18) The Sins of Mobile Code

Still want to program in C?

Deadly Sins 2/2

SOLIDO NETWORKS

Part III Cryptographic Sins 19-21

- 19) Use of Weak Password-Based System
- 20) Weak Random Numbers
- 21) Using Cryptography Incorrectly

Part IV Networking Sins 22-24

- 22) Failing to Protect Network Traffic,
- 23) Improper use of PKI, Especially SSL,
- 24) Trusting Network Name Resolution

Use cases for BackTrack and Kali

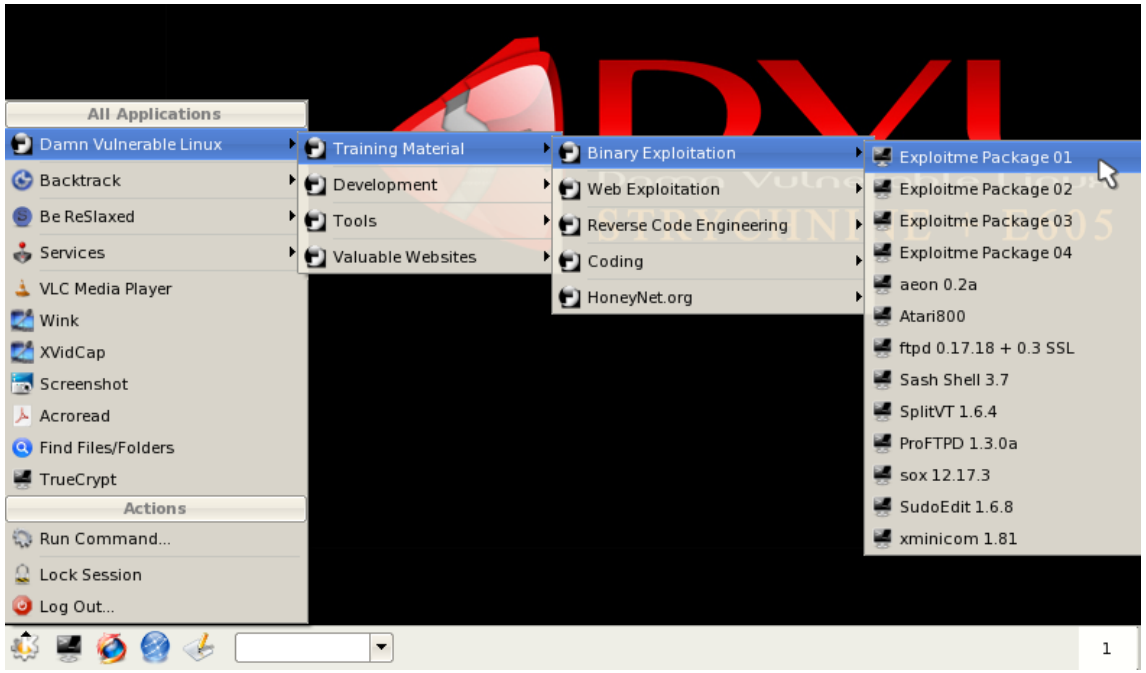
Det anbefales at afvikle BackTrack i en virtuel maskine, på klient med VMware Player, Virtualbox eller tilsvarende

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

BackTrack Linux `http://www.backtrack-linux.org/`

Kali Linux `http://www.kali.org/`

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

OWASP WebGoat

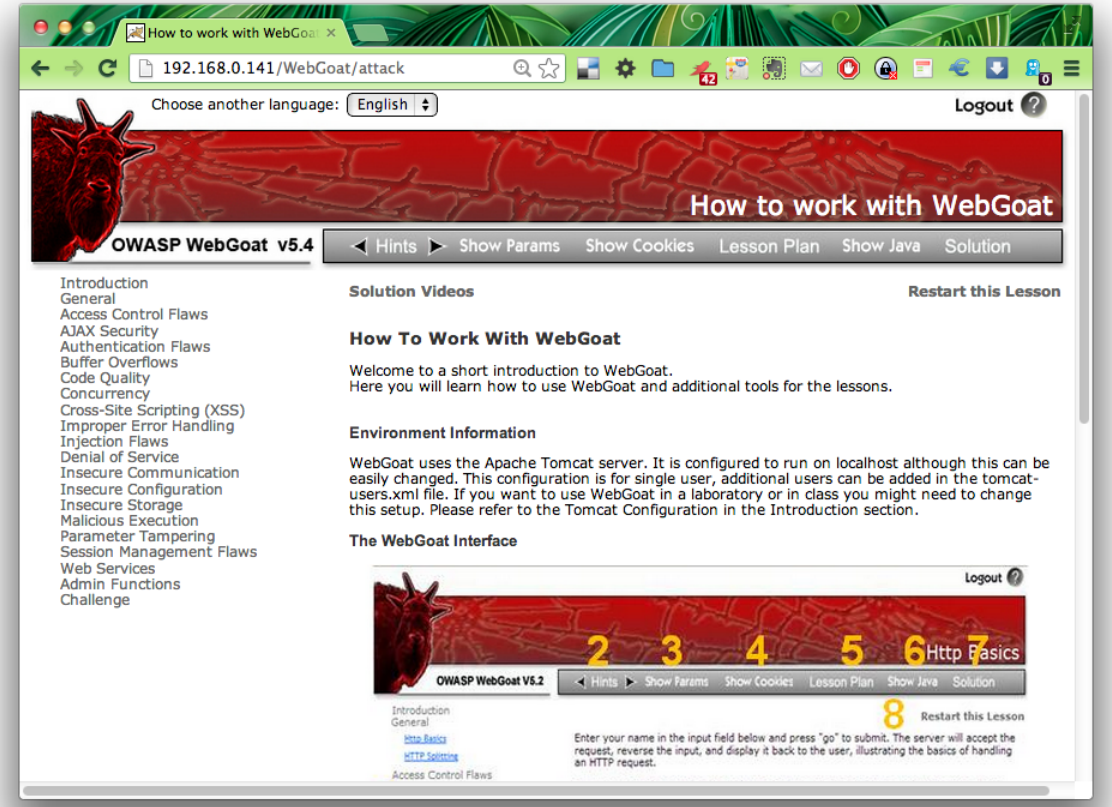
WebGoat fra OWASP, `http://www.owasp.org`

Træningsmiljø til webhacking

Downloades som Zipfil og kan afvikles direkte på en Windows laptop

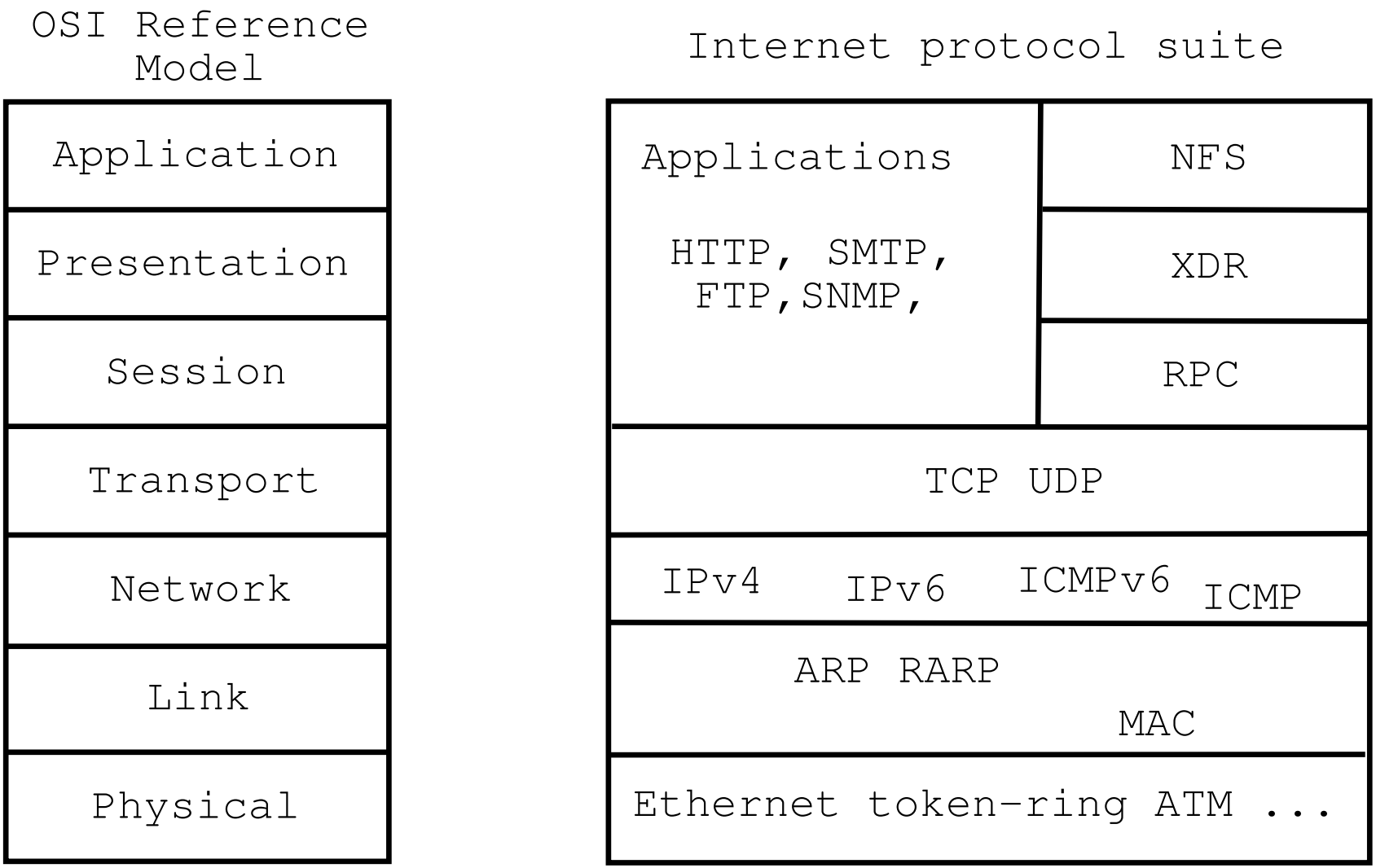
`https://www.owasp.org`

WebGoat og Kali

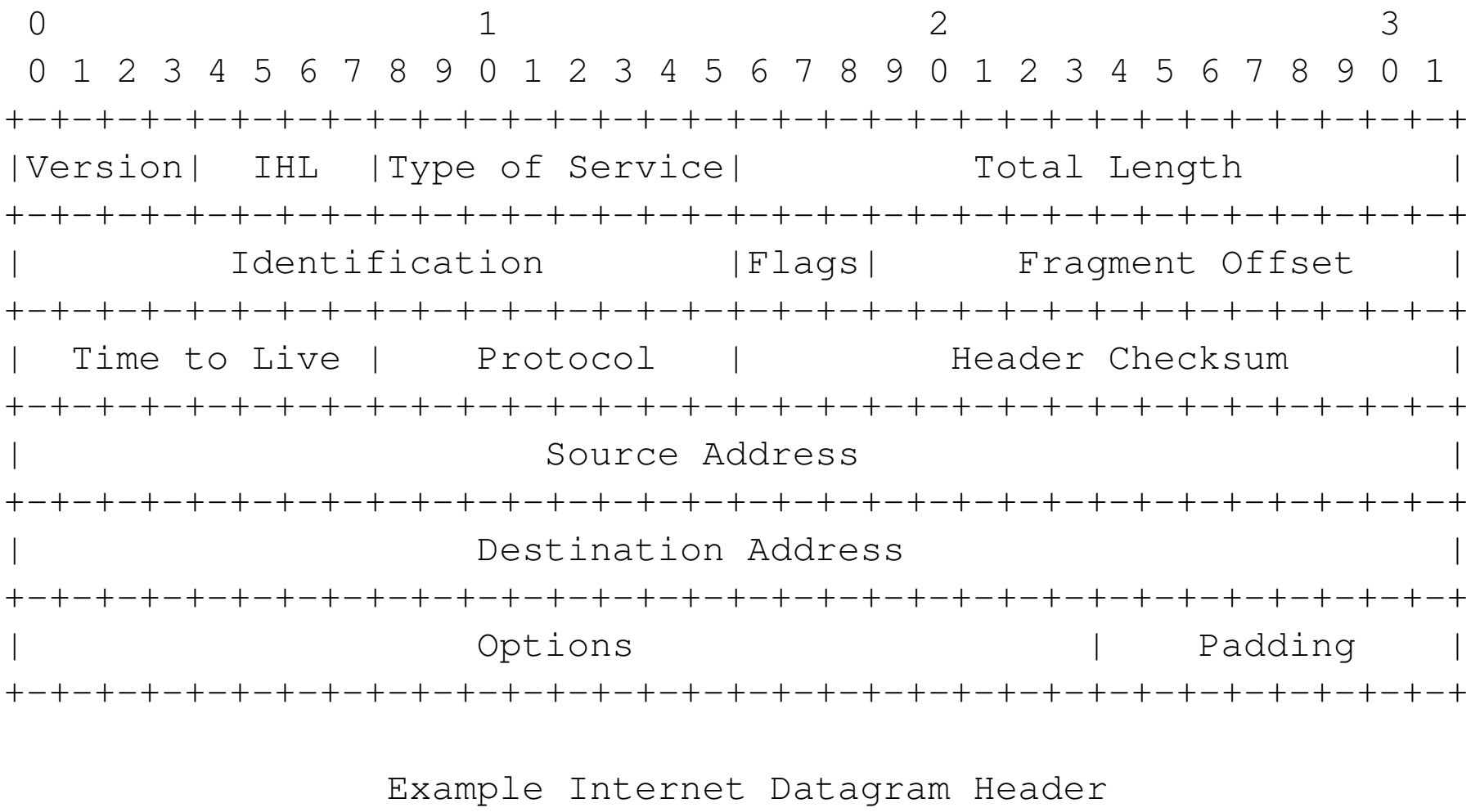


Hvor er den der ged?

OSI og Internet modellerne



IPv4 pakken - header - RFC-791



Example Internet Datagram Header

Basal Portscanning

Hvad er portscanning

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

målet er at identificere åbne porte - sårbare services

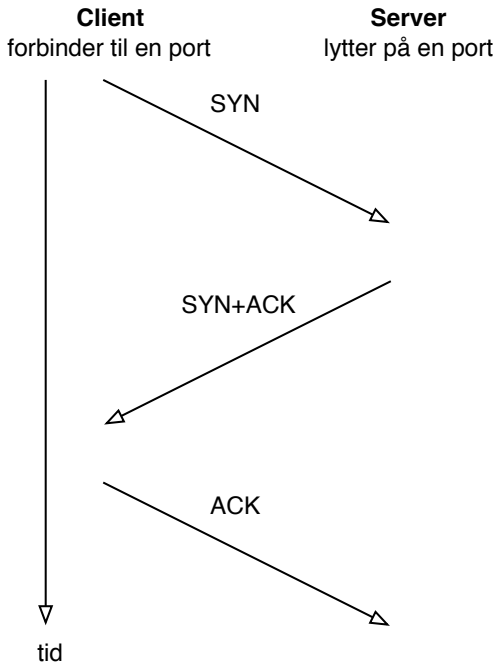
typisk TCP og UDP scanning

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**

Ping og port sweep

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:

- konfigurer 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

nmap port sweep efter port 80/TCP

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 efter port 161/UDP

SOLIDO NETWORKS

Port 161 UDP er SNMP

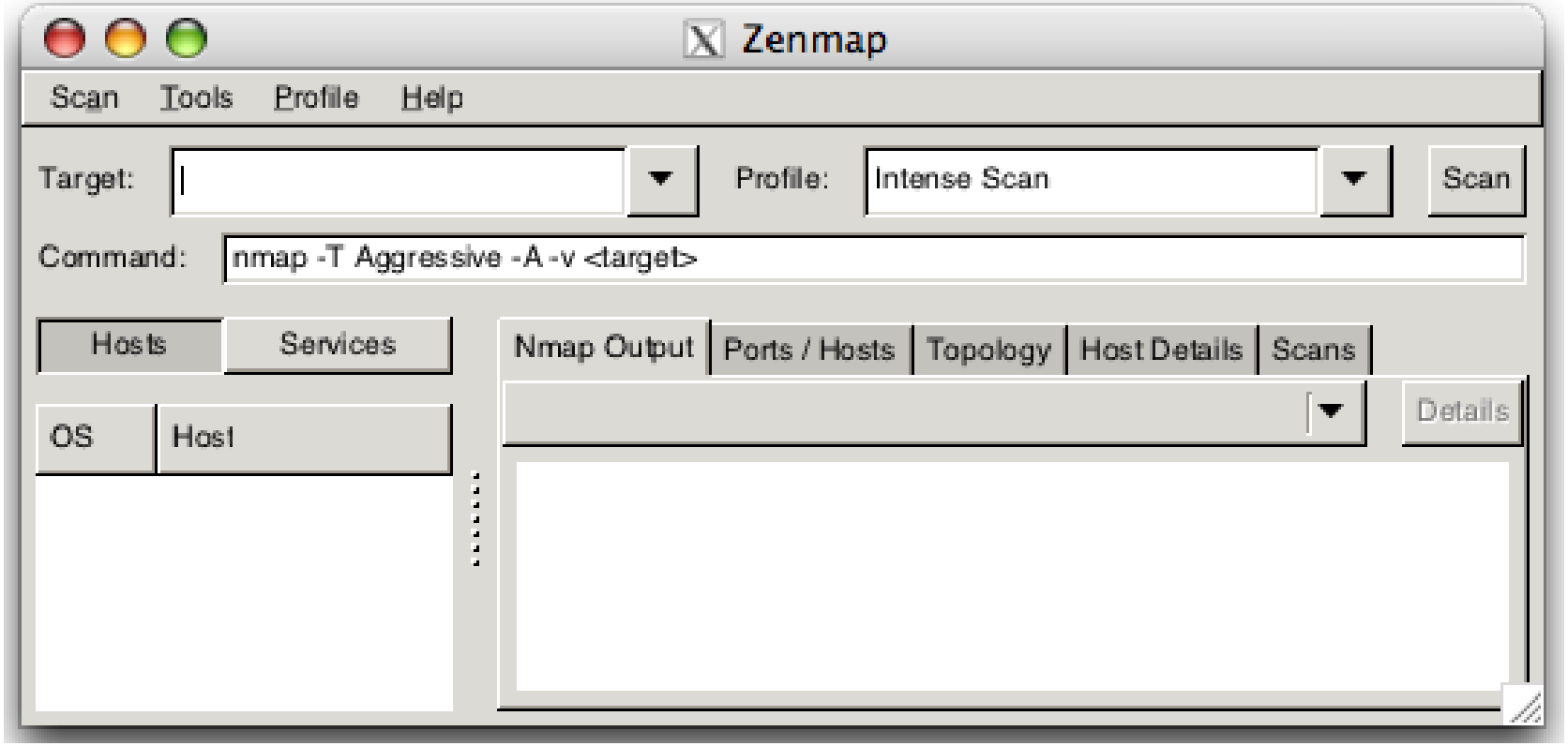
```
 #  nmap -sU -p 161 217.157.20.130/28

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
```

OS detection

```
# 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`

Zenmap



Vi bruger Zenmap til at scanne med, GUI til Nmap

Vi laver nu øvelsen

Discover active systems ping sweep

som er øvelse 3 fra øvelseshæftet.

Vi laver nu øvelsen

Execute nmap TCP and UDP port scan

som er øvelse 4 fra øvelseshæftet.

Vi laver nu øvelsen

Perform nmap OS detection

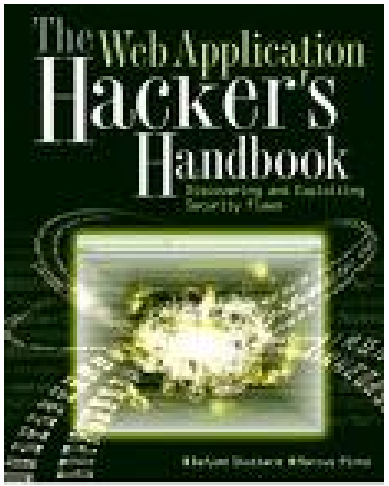
som er øvelse **5** fra øvelseshæftet.

Vi laver nu øvelsen

Perform nmap service scan

som er øvelse 6 fra øvelseshæftet.

Mere Web application hacking



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

WebScarab eller Firefox plugins

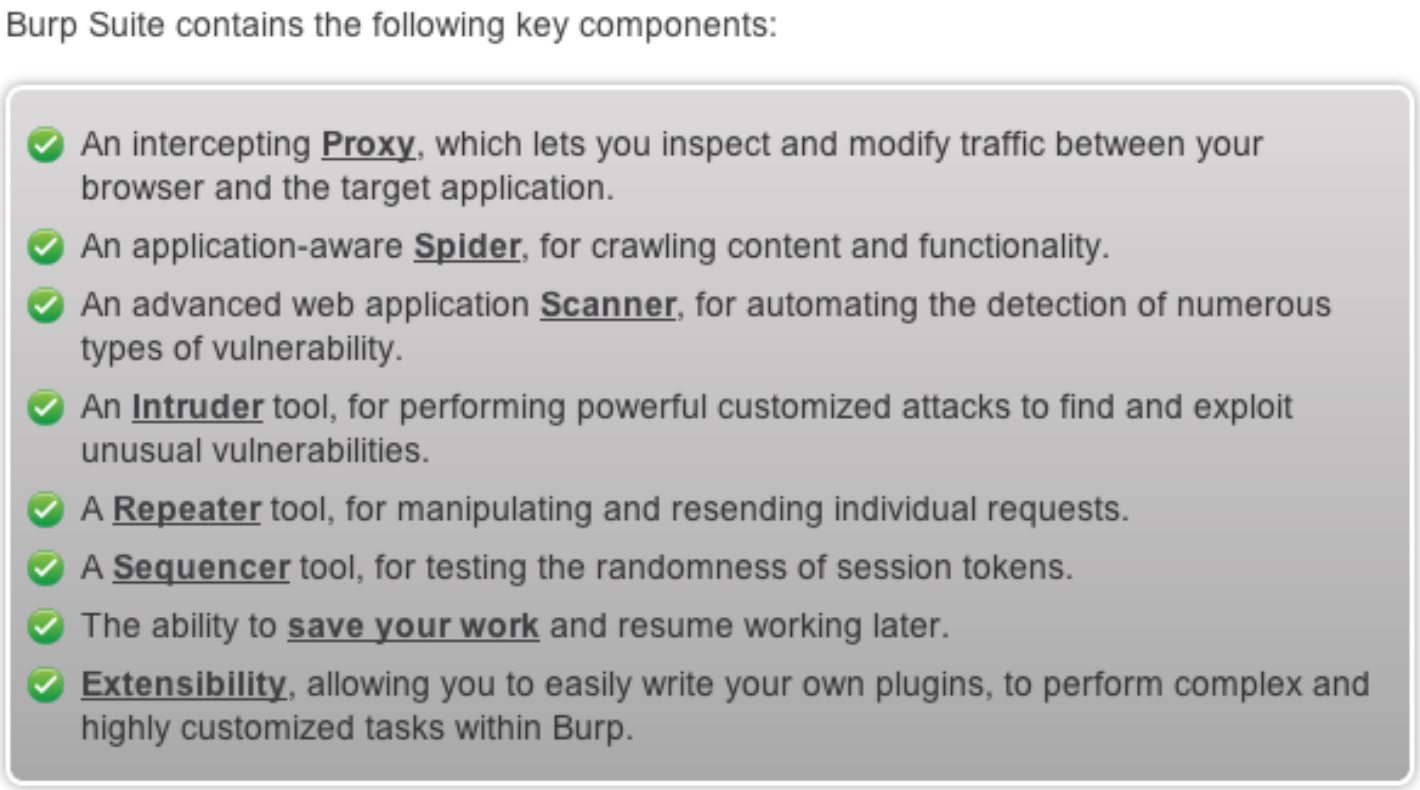
Form validation kan omgås med proxyprogrammer

Nogle af de mest kendte er:

- Burp proxy
- Tamper Data plugin til Firefox
- OWASP WebScarab

Burp Suite

SOLIDO NETWORKS



Burp Suite af Dafydd Stuttard `http://portswigger.net/burp/`

Twitter @PortSwigger

Burpsuite

SOLIDO NETWORKS

> Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
>
> Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Burp suite indeholder både proxy, spider, scanner og andre værktøjer i samme pakke - NB: EUR 249 per user per year.

`http://portswigger.net/burp/`

Nikto og W3af

Nikto web server scanner `http://cirt.net/nikto2`

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

Begge findes på BackTrack/Kali

Skipfish

Skipfish fully automated, active web application security reconnaissance tool.

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

Simple Network Management Protocol

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

brute force

SOLIDO NETWORKS

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
...
```

Vi laver nu øvelsen

Find systems with SNMP

som er øvelse 7 fra øvelseshæftet.

Vi laver nu øvelsen

Try Hydra brute force

som er øvelse 8 fra øvelseshæftet.

SOLIDO NETWORKS

Vi laver nu øvelsen

Try Cain brute force

som er øvelse 9 fra øvelseshæftet.

Følg med Twitter news

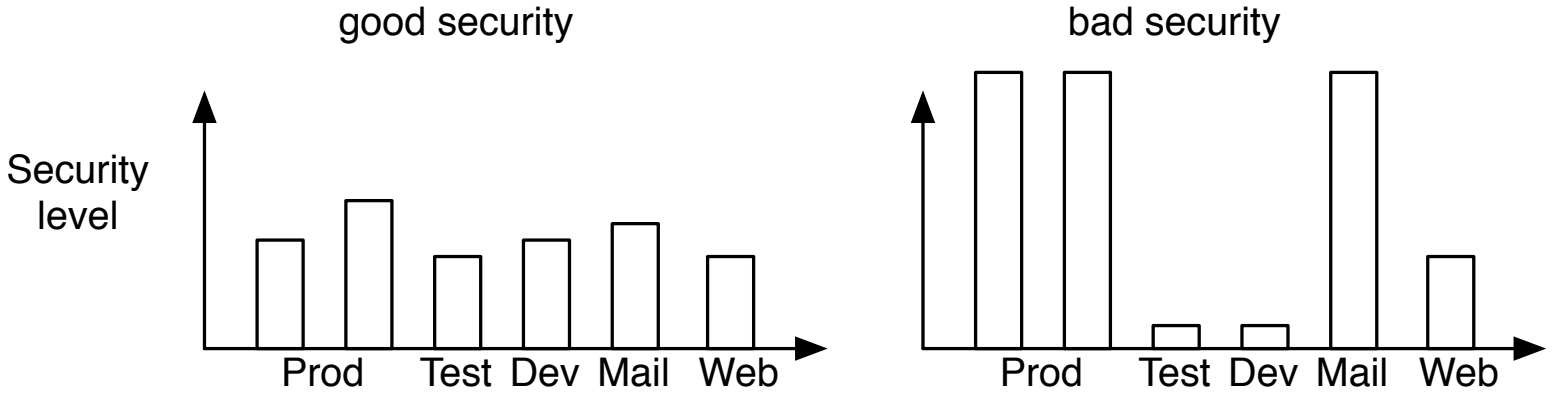
Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

Checklisten

- 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.

Balanced security



Better to have the same level of security

If you have bad security in some part - guess where attackers will end up

Hackers are not required to take the hardest path into the network

Realize there is no such thing as 100% security

Work together

Team up!

We need to share security information freely

We often face the same threats, so we can work on solving these together

PROSA CTF

PROSA afholdte CTF konkurrence 2013 29. - 30. november

Capture the Flag er en mulighed for at afprøve sine hackerskillz

Distribueret CTF med hold Sjovt og lærerigt

Kilde: `http://ctf2013.the-playground.dk/`

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

Fri adgang til hackerværktøjer

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

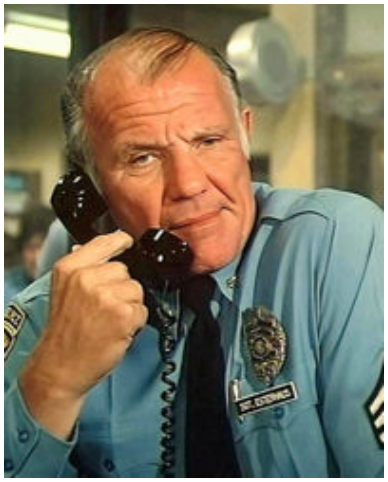
I 1995 udgav de softwarepakken SATAN
Security Administrator Tool for Analyzing Networks

> 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`

Be careful - questions?



Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

Source: Michael Conrad `http://www.hillstreetblues.tv/`

VikingScan.org - free portscanning