

---

Velkommen til

# Basic firewall

Juli 2008

Henrik Lund Kramshøj  
hlk@security6.net

<http://www.security6.net>

# Formålet med foredraget

At introducere Firewall begrebet

At vise de sikkerhedsmæssige aspekter af firewalls og netsikkerhed

Kendskab til kendte sårbarheder i almindelige netværk og hvorfor en firewall ikke beskytter mod alt

Minimering af risici 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

# Aftale om test af netværk

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

Hacking kan betyde:

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

# Referencer

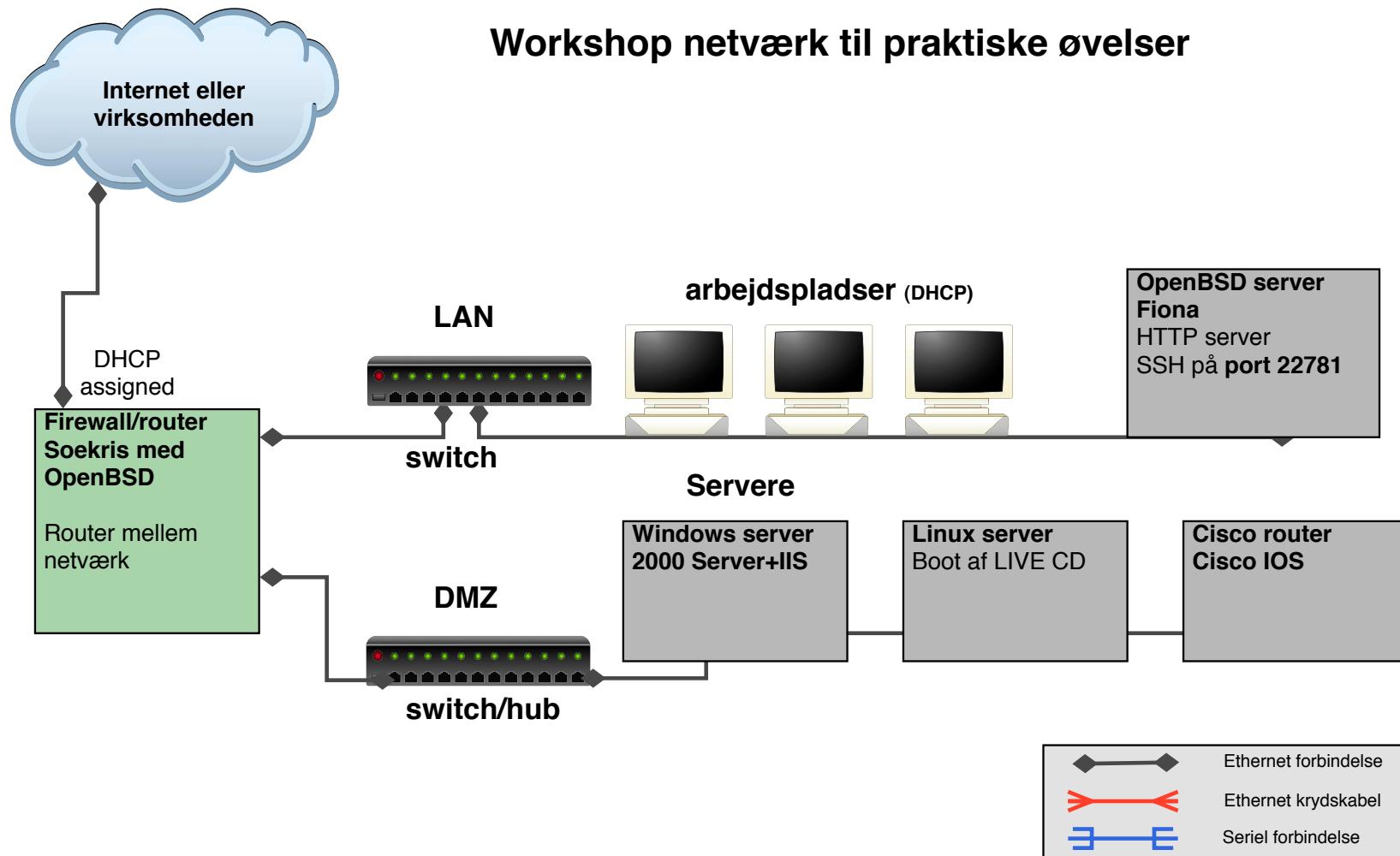
Det meste jeg siger kan genfindes i referencer på internet, eksempelvis:

- OpenBSD PF User's Guide <http://www.openbsd.org/faq/index.html>
- Firewalling with OpenBSD's PF packet filter <http://home.nuug.no/~peter/pf/>

eller i bøger som:

*Firewalls and Internet Security: Repelling the Wily Hacker* 2nd ed. William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin <http://www.wilyhacker.com/>

## Workshop netværk til praktiske øvelser



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 tekstfiler
- more - less - viser tekstfiler 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 en del værktøjer:

- nmap - <http://www.insecure.org> portscanner
- Wireshark - <http://www.wireshark.org/> avanceret netværkssniffer
- OpenBSD - <http://www.openbsd.org> operativsystem med fokus på sikkerhed
- BackTrack <http://www.remote-exploit.org/backtrack.html>
- Putty - <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> terminal emulator med indbygget SSH
- m0n0wall - <http://www.m0n0.ch> gratis firewall baseret på FreeBSD

# Hvad skal der ske?

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: Nessus, 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.

# Er Firewalls og netsikkerhed interessant?

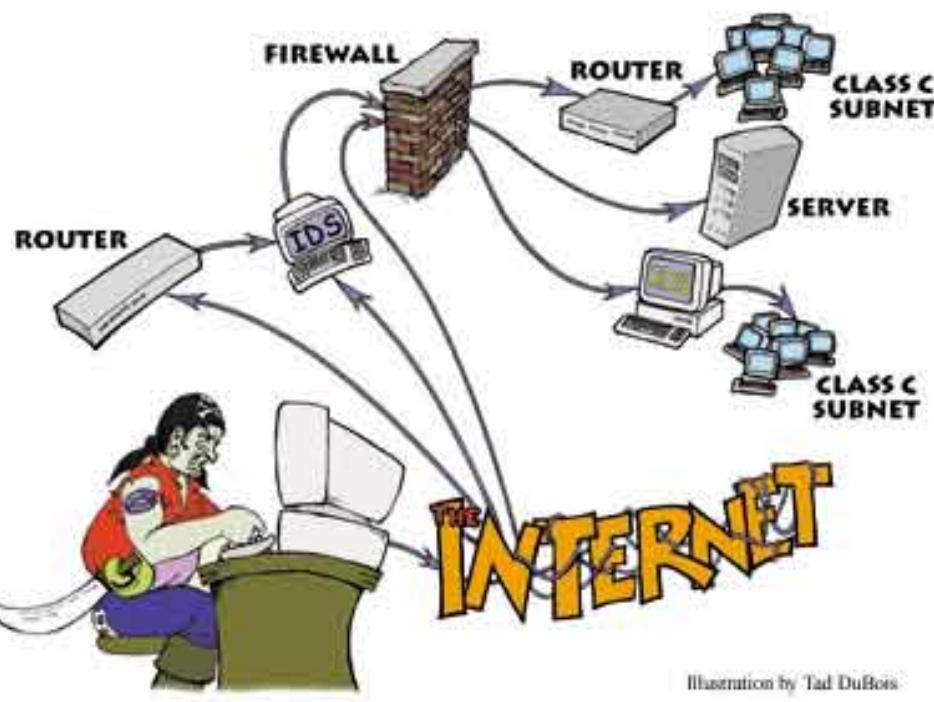


Illustration by Tad DuBois

Sikkerhedsproblemerne i netværk er mange

Mange services - mange sårbare services

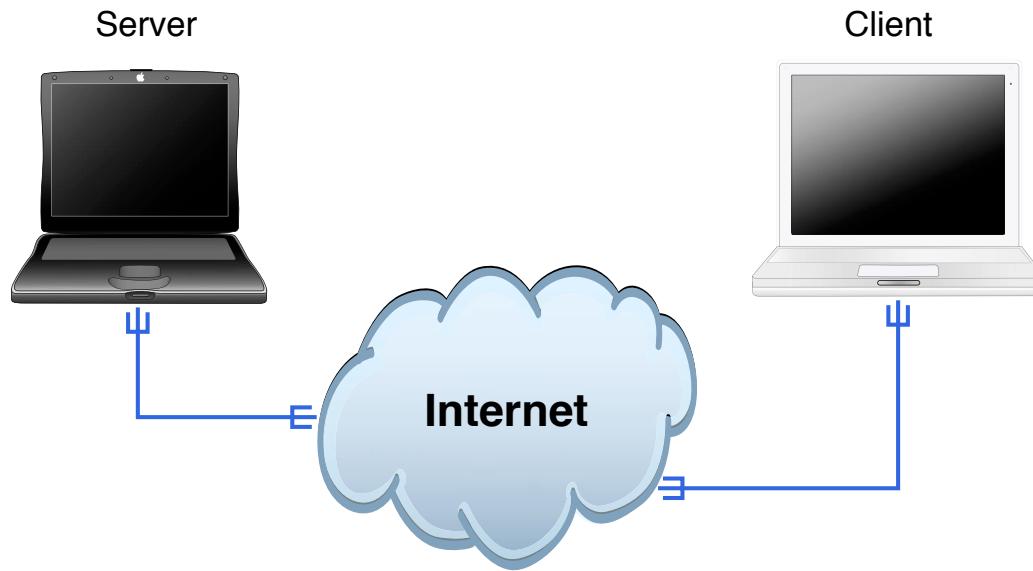
# Jeres kendskab til firewalls



Hvad kender I til firewalls?

# Emner

- Internet som en landsby
- Firewall historik
- An evening with Berferd
- Moderne firewalls
- Specielle features
- personlige firewalls
- Unicode angreb - hjælper firewall?
- Firewall konfiguration
- Bloker indefra og ud
- tips og tricks - samt diverse firewall relaterede emner



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

# Internet er åbne standarder!

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 tilbage fra 1969

Et RFC dokument ændres ikke, men får status Obsoleted

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

betratget som de seriøse - og konservative

informerer om sårbarheder og trusler

koordinerer aktiviteter - mellem leverandører

opsamler statistik for hacker aktivitet

# Firewallrollen idag

Idag skal en firewall være med til at:

- Forhindre angribere i at komme ind
- Forhindre angribere i at sende traffik ud
- Forhindre virus og orme i at sprede sig i netværk
- Indgå i en samlet løsning med ISP, routere, firewalls, switchede strukturer, intrusion detectionsystemer samt andre dele af infrastrukturen

Det kræver overblik!

## Praktiske øvelser!

Planen er at vi arbejder os gennem emnet - opbygger en riktig firewallløsning og afprøver lidt hackerprogrammer mod systemerne

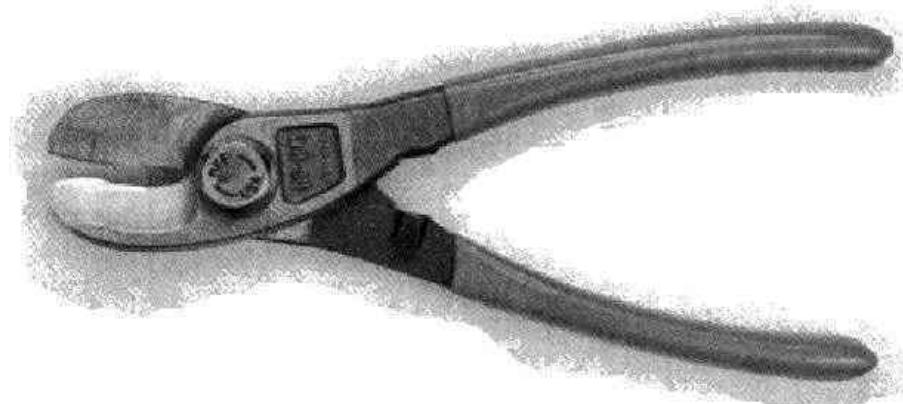
En firewall er noget som **blokerer** traffik på Internet

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

Indeholder typisk:

- Grafisk brugergrænseflade til konfiguration
- TCP/IP filtermuligheder - pakkernes 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
- typisk NAT funktionalitet indbygget - NAT is BAD
- typisk mulighed for nogle serverfunktioner:  
DHCP-server, DNS caching server og lignende

En router med Access Control Lists - kaldes ofte netværksfilter, mens en dedikeret maskine kaldes firewall



Hvor skal en firewall placeres for at gøre størst nytte?

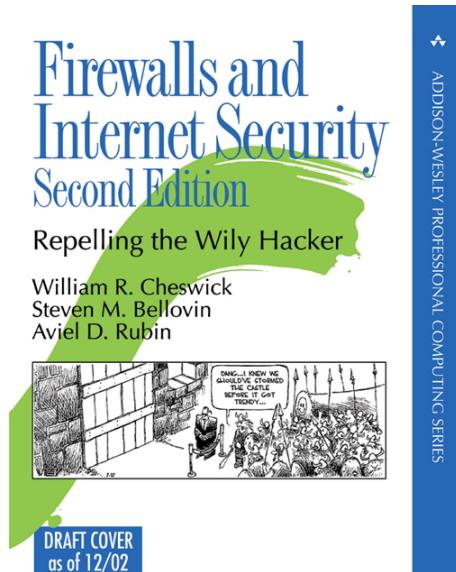
Hvad er forudsætningen for at en firewall virker?

At der er konfigureret et sæt fornuftige regler!

Hvor kommer reglerne fra? Sikkerhedspolitikken!

Kilde: Billedet er fra Marcus Ranum The ULTIMATELY Secure Firewall

# Firewall historik



Firewalls har været kendt siden starten af 90'erne

Den første bog *Firewalls and Internet Security* udkom i 1994 men der findes mange akademiske artikler om firewalls

Bogen *Firewalls and Internet Security* anbefales, William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, Addison-Wesley, 2nd edition, 2003

Artikel om en hacker der lokkes, vurderes, overvåges

Et tidligt eksempel på en honeypot

Idag anbefales The Honeynet Project hvis man vil vide mere

<http://www.honeynet.org>

# Kommercielle firewalls

- Checkpoint Firewall-1 <http://www.checkpoint.com>
- Nokia appliances - Nokia IPSO <http://www.nokia.com>
- Cisco PIX <http://www.cisco.com>
- Clavister firewalls <http://www.clavister.com>
- Netscreen - nu ejet af Juniper <http://www.juniper.net>

Ovenstående er dem som jeg oftest ser ude hos mine kunder

# Open source baserede firewalls

## Linux firewalls - fra begyndelsen til det nuværende netfilter til kerner version 2.4 og 2.6

<http://www.netfilter.org>

- Firewall GUIs ovenpå Linux - mange! IPcop, Guarddog, Watchguard nogle Linux firewalls er kommersielle produkter
- IP Filter (IPF) <http://coombs.anu.edu.au/~avalon/>
- OpenBSD PF - findes idag på andre operativsystemer <http://www.openbsd.org>
- FreeBSD IPFW og IPFW2 <http://www.freebsd.org>
- Mac OS X benytter IPFW
- FreeBSD inkluderer også OpenBSD PF
- NetBSD - bruger IPF og er ved at inkludere OpenBSD PF

NB: kun eksempler og dem jeg selv har brugt

# personlige firewalls

Personlige firewalls:

- Microsoft Windows XP
- ZoneAlarm <http://www.zonelabs.com>

Personlige firewalls til Microsoft Windows inkluderer ofte blokering af hvilket programmer der må tilgå netværk

Det anbefales at bruge en personlig firewall

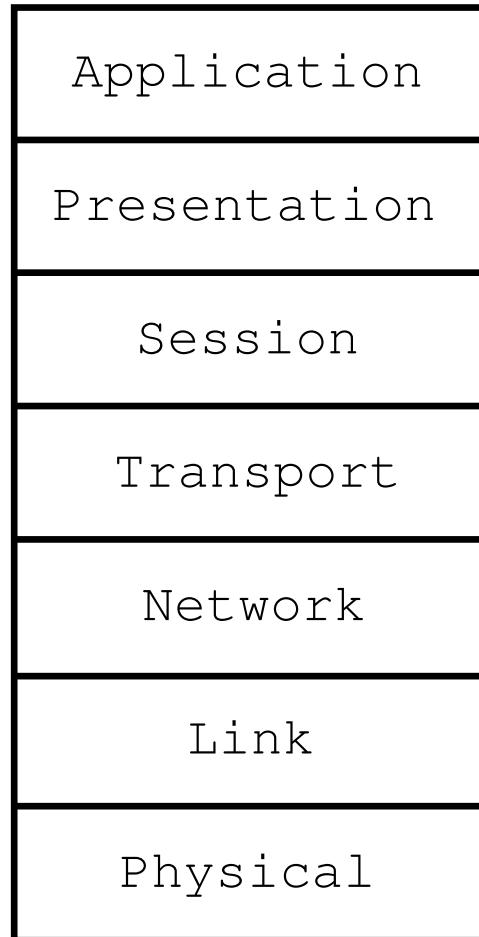
Note: Lad være med at stille spørgsmål om logfilen i diverse fora!

**Hvis du ikke forstår loggen så lad den ligge!**

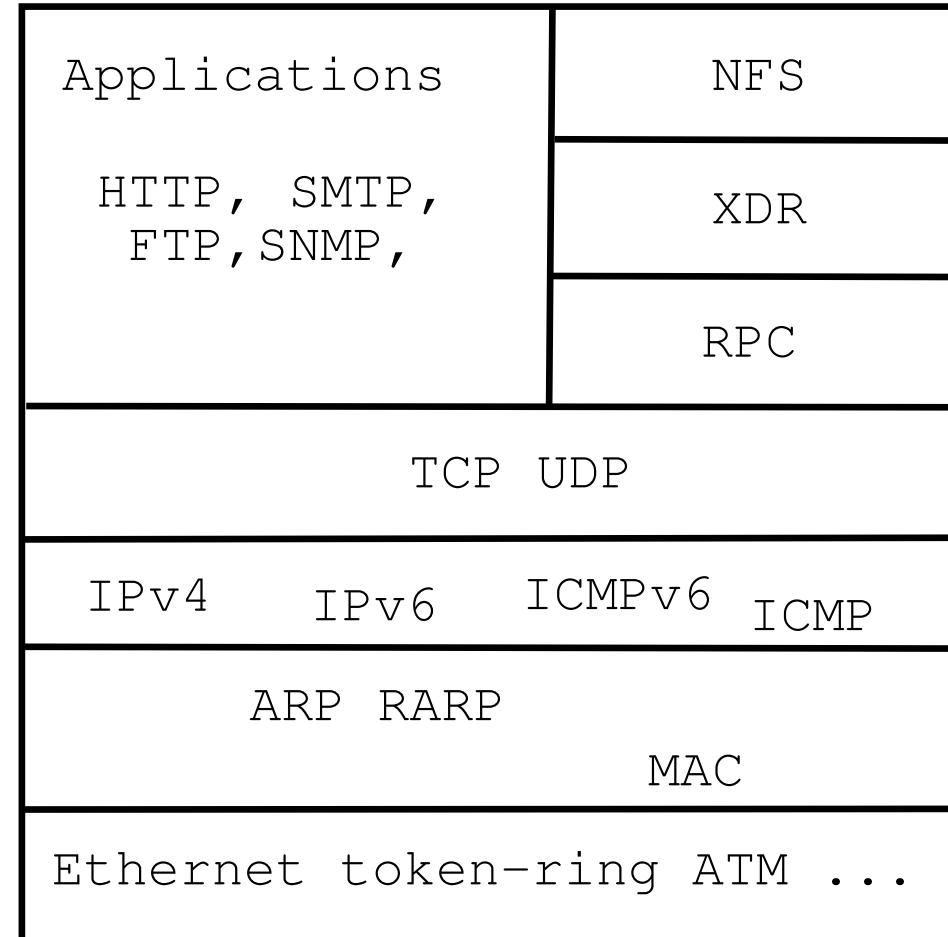
# OSI og Internet modellerne



OSI Reference Model



Internet protocol suite



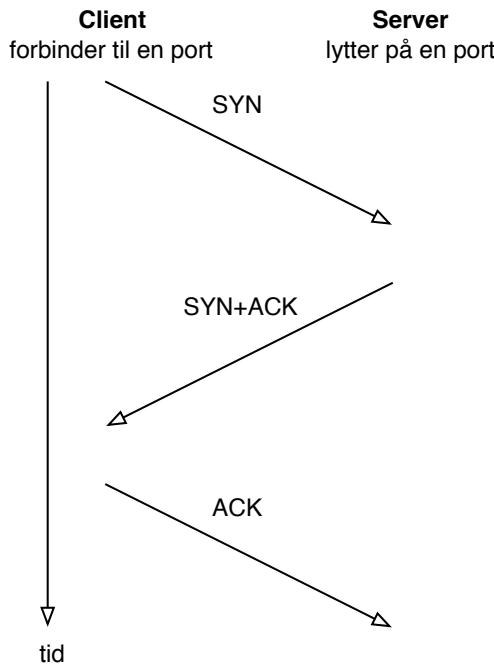
# Packet filtering

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

Packet filtering er firewalls der filtrerer på IP niveau

I dag inkluderer de fleste statefull inspection

# 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**

# Proxy servers

Filtrering på højere niveauer i OSI modellen er muligt

Idag findes proxy applikationer til de mest almindelige funktioner

Den typiske proxy er en caching webproxy der kan foretage HTTP request på vegne af arbejdsstationer og gemme resultatet

NB: nogle protokoller egner sig ikke til proxy servere - SSL forbindelser til *secure websites*

Se eksempelvis på Squid webcache <http://www.squid-cache.org/>  
eller Varnish reverse proxy <http://varnish.projects.linpro.no/>

## Hardware eller software

Man hører indimellem begrebet *hardware firewall*

Det er dog et faktum at en firewall består af:

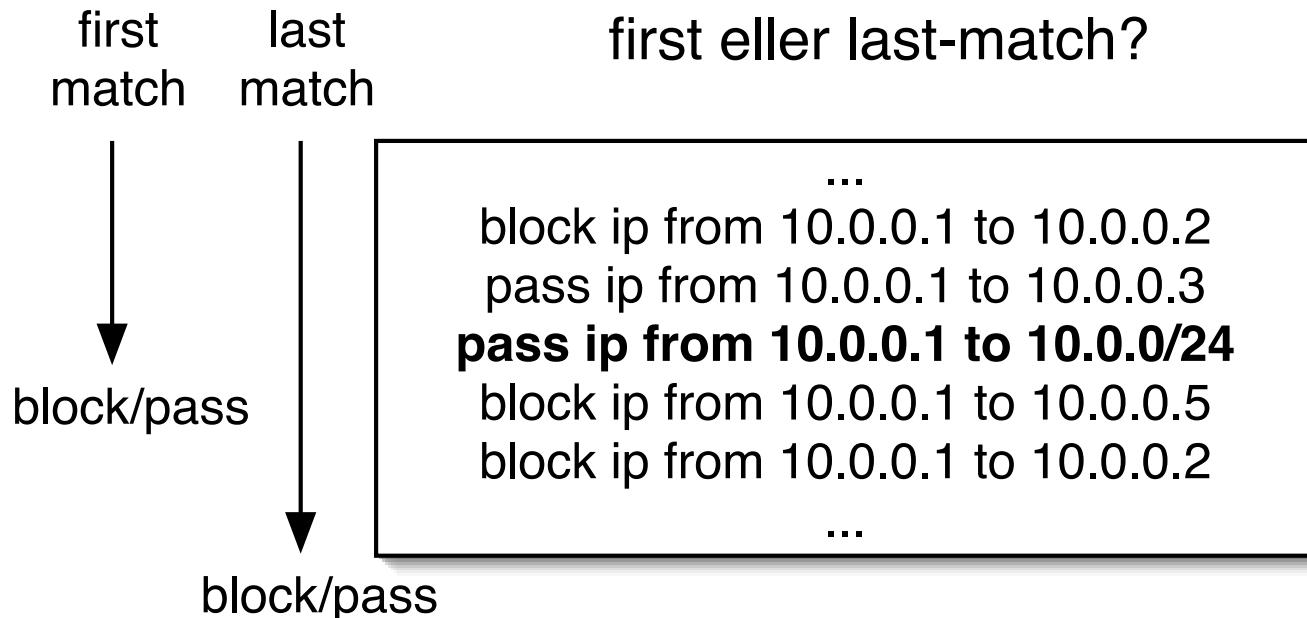
- Netværkskort - som er hardware
- Filtreringssoftware - som er *software!*

Det giver ikke mening at kalde en Zyxel 10 en hardware firewall og en Soekris med OpenBSD for en software firewall!

Det er efter min mening et marketingtrick

Man kan til gengæld godt argumentere for at en dedikeret firewall som en separat enhed kan give bedre sikkerhed

# First or Last match firewall?



Med dette regelsæt vil en first-match firewall blokere pakker fra 10.0.0.1 til 10.0.0.2 - men tillade alt andet fra 10.0.0.1 til 10.0.0/24

Med dette regelsæt vil en last-match firewall blokere pakker fra 10.0.0.1 til 10.0.0.2, **10.0.0.1 til 10.0.0.5**, **10.0.0.1 til 10.0.0.2** - men ellers tillade alt andet fra 10.0.0.1 til 10.0.0/24

- To typer af firewalls: First match - eksempelvis IPFW, Last match - eksempelvis PF

## First match - IPFW

```
00100 16389 1551541 allow ip from any to any via lo0
00200      0      0 deny log ip from any to 127.0.0.0/8
00300      0      0 check-state
...
65435    36    5697 deny log ip from any to any
65535    865    54964 allow ip from any to any
```

Den sidste regel nås aldrig!

# Last match - OpenBSD PF

```
ext_if="ext0"
int_if="int0"

block in
pass out keep state

pass quick on { lo $int_if }

# Tillad forbindelser ind på port 80=http og port 53=domain
# på IP-adressen for eksterne netkort ($ext_if) syntaksen
pass in on $ext_if proto tcp to ($ext_if) port http keep state
pass in on $ext_if proto { tcp, udp } to ($ext_if) port domain keep state
```

Pakkerne markeres med block eller pass indtil sidste regel  
nøgleordet *quick* afslutter match - god til store regelsæt

# Linux iptables/netfilter eksempel

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

NB: husk at aktivere IP forwarding

# Firewall GUI

A screenshot of a Firewall GUI application. The interface includes a menu bar with File, Edit, View, Insert, Rules, Tools, and Help. A toolbar with icons for New, Open, Save, Print, and Exit is located above the main window. On the left is a tree view labeled 'User Standard' showing a hierarchy: Name, Objects, Services, Firewalls, fw (selected), fw, eth1, eth0, lo, Policy, NAT, and Time. The main area contains a table of firewall rules with columns: Num, Source, Destination, Service, Action, Time, Options, and Comment. The rules listed are:

Num	Source	Destination	Service	Action	Time	Options	Comment
00		Any		<input checked="" type="checkbox"/> Accept	Any		firewall uses DNS server on Inet
01	Any			<input checked="" type="checkbox"/> Accept	Any		firewall serves as DNS server for LAN
02	Any			<input checked="" type="checkbox"/> Accept	Any		firewall serves as DHCP server for LAN
03		Any		<input checked="" type="checkbox"/> Accept	Any		firewall serves as DHCP server for LAN
04	Any		 	<input checked="" type="checkbox"/> Accept	Any		mail and ftp server behind the firewall
05		Any		<input checked="" type="checkbox"/> Accept	Any		
06				<input checked="" type="checkbox"/> Accept	Any		ssh access to firewall from internal LAN
07	Any	Any	Any	<input type="radio"/> Deny	Any		'catch all' rule

At the bottom right are 'Apply' and 'Undo' buttons.

Der findes mange GUI programmer til Open Source firewalls

Kilde: billede fra <http://www.fwbuilder.org>

# Firewalls og ICMP

```
ipfw add allow icmp from any to any icmp types 3,4,11,12
```

Ovenstående er IPFW syntaks for at tillade de interessant ICMP beskeder igennem

Tillad ICMP types:

- 3 Destination Unreachable
- 4 Source Quench Message
- 11 Time Exceeded
- 12 Parameter Problem Message

# Specielle features

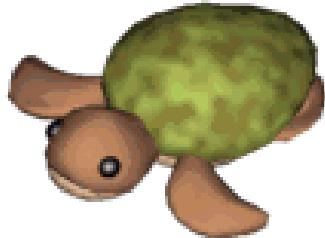
- Network Address Translation - NAT
- IPv6 funktionalitet
- IPsec og Andre VPN features
- Båndbredde håndtering
- VLAN funktionalitet - mere udbredt i forbindelse med VoIP
- Redundante firewalls - pfsync og CARP

## Network Address Translation

En quick and dirty fix der vil forfølge os for resten af vores liv

Ødelægger en del protokoller :-(

Lægger state i netværket - ødelægger fate sharing

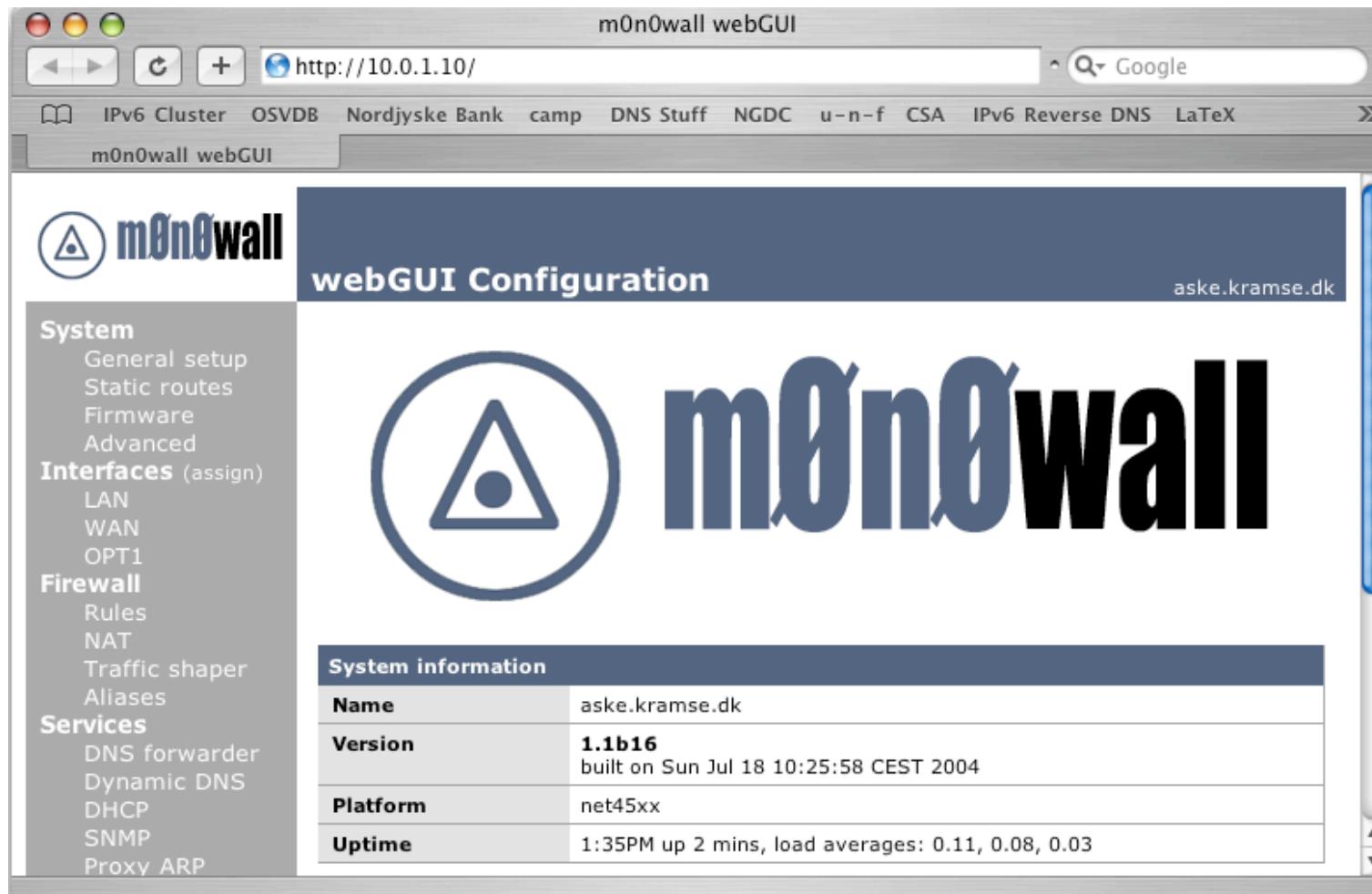


IPv6 understøttes i næsten alle Open Source firewalls

IPv6 understøttes i næsten ingen kommercielle firewalls

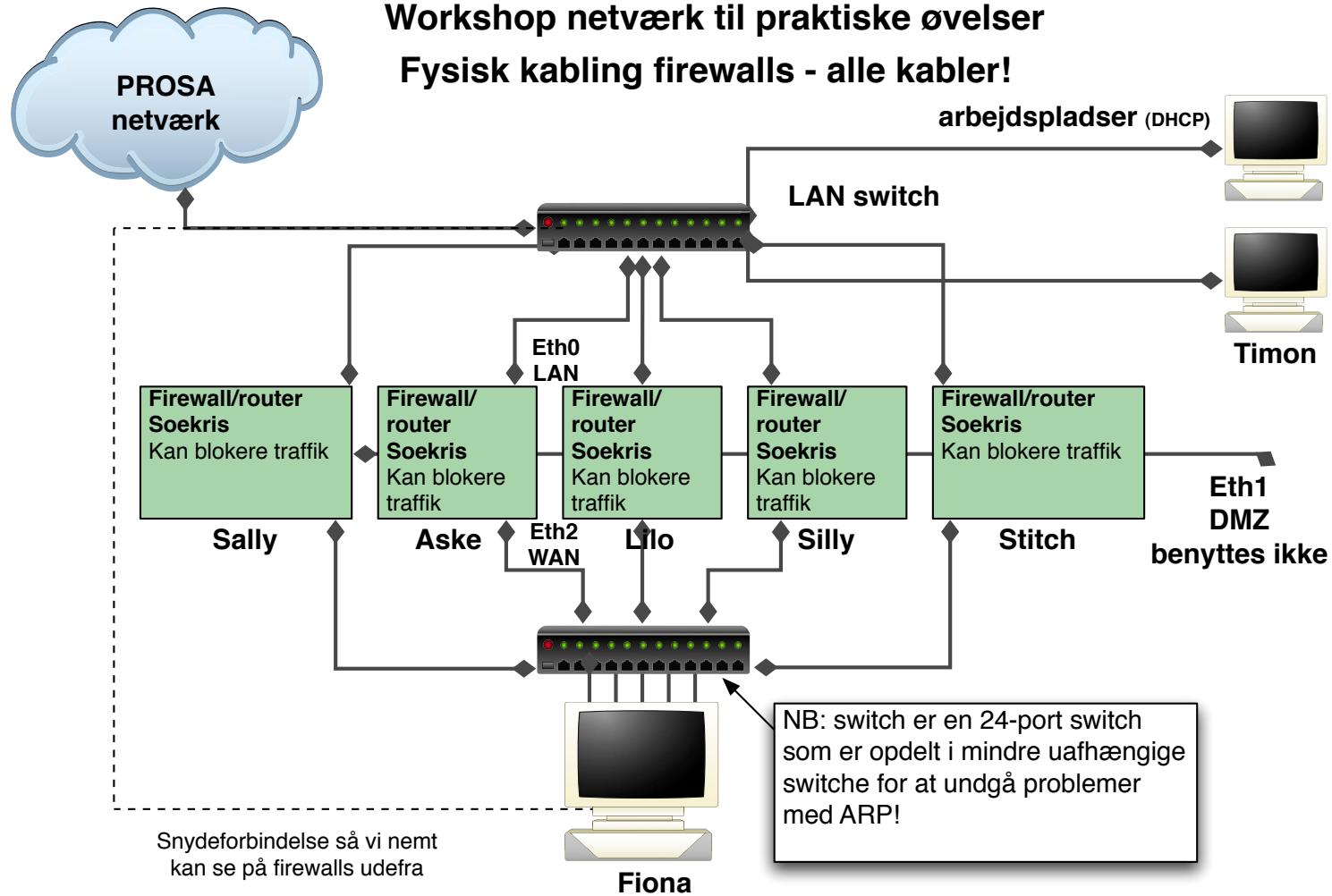
Cisco PIX IPv6 support er udskudt flere gange

Der mangler erfaring med IPv6 firewalls



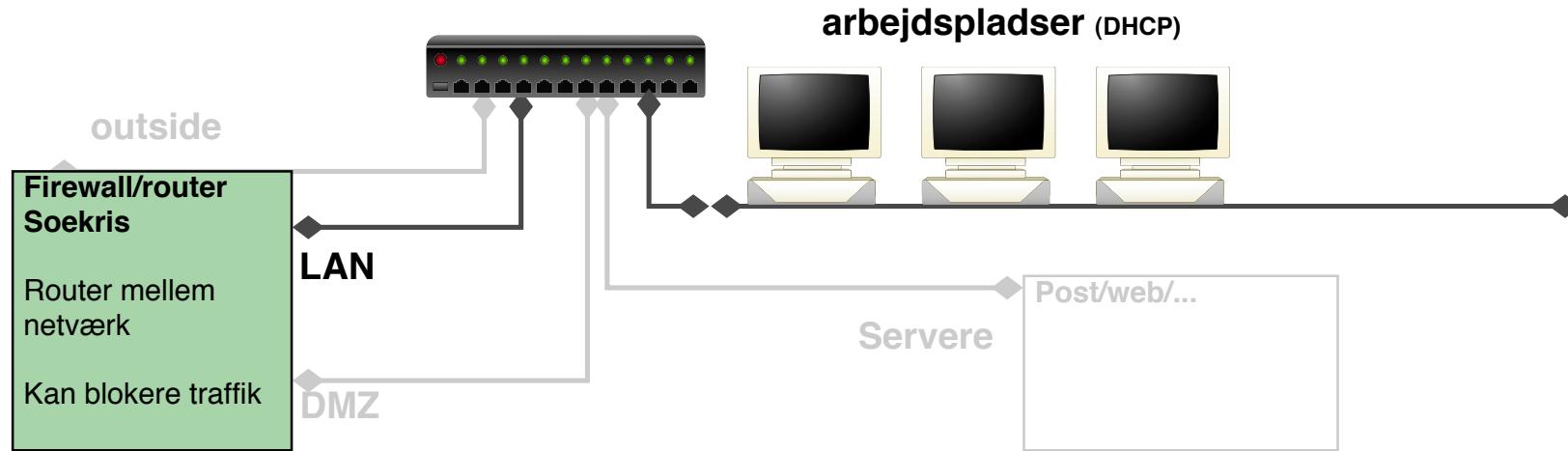
Kilde: billede fra <http://m0n0.ch/wall/>

## Workshop netværk til praktiske øvelser Fysisk kabling firewalls - alle kabler!



- PROSA kursusnetværk er inside LAN på firewalls
- I København benyttes 192.168.100/24, i Århus benyttes 10.0.0/24
- WAN netværk er 5 netværk: 192.168.200/24, 192.168.201/24, 192.168.202/24, 192.168.203/24, 192.168.204/24
- DMZ netværk benyttes ikke som udgangspunkt
- Det forventes at kursisterne arbejder i hold og der er en firewall til hvert hold - i alt max 5 hold
- Allesammen deler det fysiske inderside netværk, dog er der flere logiske switchede netværk - portbaserert VLAN

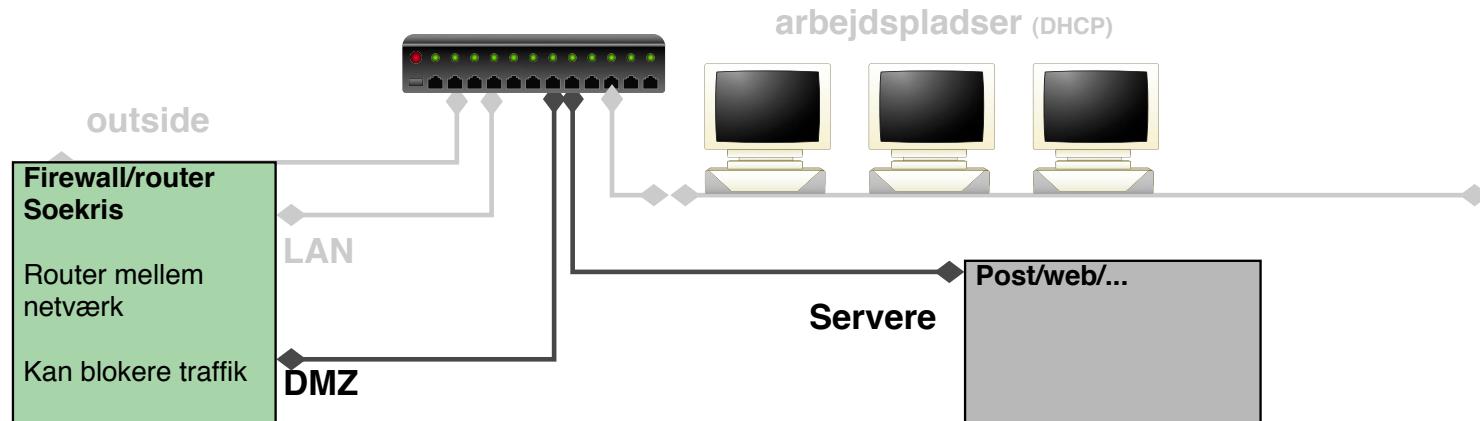
## Workshop netværk til praktiske øvelser Logisk brug af netværket her!



- Sådan er jeres systemer konfigureret i udgangspunktet og kablet
- vi skal tilføje adresser og routes til "WAN netværk" til arbejdspladsen!
- Prøv kun at tænke på jeres lille del af netværket - som er vist på tegningen

## Workshop netværk til praktiske øvelser

### Logisk brug af netværket her!



"servere" og DMZ interface ligger i samme IP-range og kan kommunikere

- I vores netværk er der kun en fysisk server - Fiona med HTTP webserver
- Fiona er en server med flere adresser på hvert sit fysiske netkort
- For at undgå at skulle splitte LAN benyttes NAT, og derfor WAN interface!
- Tegningen viser hvor I bør placere internetservere i et rigtigt netværk

# Netværkskonfiguration - Windows

## Windows

- Brug kontrolpanelet
- Ret adresserne og husk routing information

## UNIX

- ifconfig -a viser alle netkort og adresserne
- netstat -rn viser routing informationerne
- ifconfig eth0 10.1.2.3 netmask 255.255.255.0 sætter adressen 10.1.2.3 på netkortet med navnet eth0
- route add default 10.1.1.1 sæt default route til at være 10.1.1.1
- Kommandoen `route` kan bruges med `change` istedet for `add`

Der udleveres tilpasset routing.bat og routing.sh scripts til dette!

## Portscan demo

Hvad er forskellen med og uden firewall, kan man se det?

Brug kursusserver, Linux boot-CD eller Windows portscanner

Formålet er senere at kunne afgøre om firewall virker og er konfigureret korrekt

En gylden regel er at en firewall ikke svarer på blokerede porte, sender ikke RESET pakker

# Vores firewall giver optimal sikkerhed

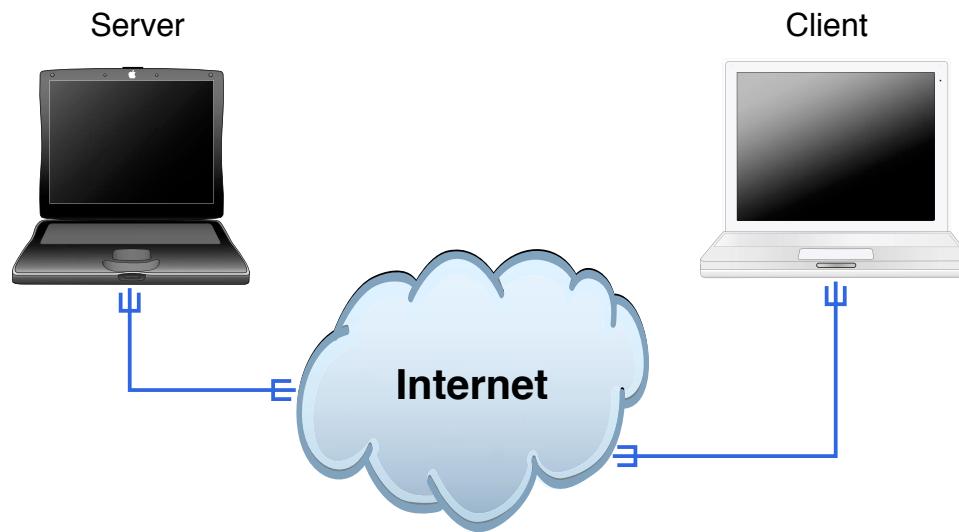


Vi har en server og har sat den bagved firewalls!

Den er sikker!

Desværre ikke!

# Start på demo: DCOM sårbarhed



- To almindelige computere - en switch erstatter Internet
- VMware player benyttes til det sårbare Windows 2000 system
- Windows er installeret på et system og ikke opdateret
- dcom.c exploit er hentet fra Internet og bruges næsten uændret

# Hvad sker der?

```
[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  
exit
```

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

- Read failure
- ```
[hlk@fiona hlk]$
```

# Unicode - det klassiske port 80 problem

A screenshot of a Mac OS X desktop showing a web browser window. The address bar shows 'http://10.0.1.2/scripts/..%c0%af..winnt/system32/cmd.exe?/c+dir+c:\'. The page content is a directory listing for 'c:\'.

File	Last Modified	Size	Name
26-08-2004	13:08	1.024	.rnd
05-06-2004	15:32	105.973	audit.txt
24-04-2004	14:06	3.157	cisco-803.txt
07-12-1999	14:00	236.304	cmd.exe
09-04-2004	21:25	125.767	comreads.dbg
09-04-2004	21:25	121.706	comused.dbg
23-03-2004	21:34	<DIR>	Documents and Settings
11-04-2004	15:15	1.356.075	drwtsn32.log
22-05-2004	11:47	<DIR>	dwl-650
22-05-2004	12:08	232	fake_htpasswd.txt
30-05-2004	11:04	18.434	form-1.html

Hvorfor går det galt? gennemgang på tavlen

Traffikken går via de godkendte porte - normal port 80 webtraffik

Så går man igang med de almindelige værktøjer

Fyodor Top 100 Network Security Tools

<http://sectools.org/>

**Forsvaret er som altid - flere lag af sikkerhed!**

(engelsk: Security in depth)

# Firewall er ikke alene

## Firewalls er ikke alene

- anti-virus på klienter og postsystemer
- IDS systemer
- Backupsystemer
- Adgangskontrol
- ... mange andre ting er mindst ligeså vigtige

# Firewall konfiguration

Den bedste firewall konfiguration starter med:

- Papir og blyant
- En fornuftig adressestruktur

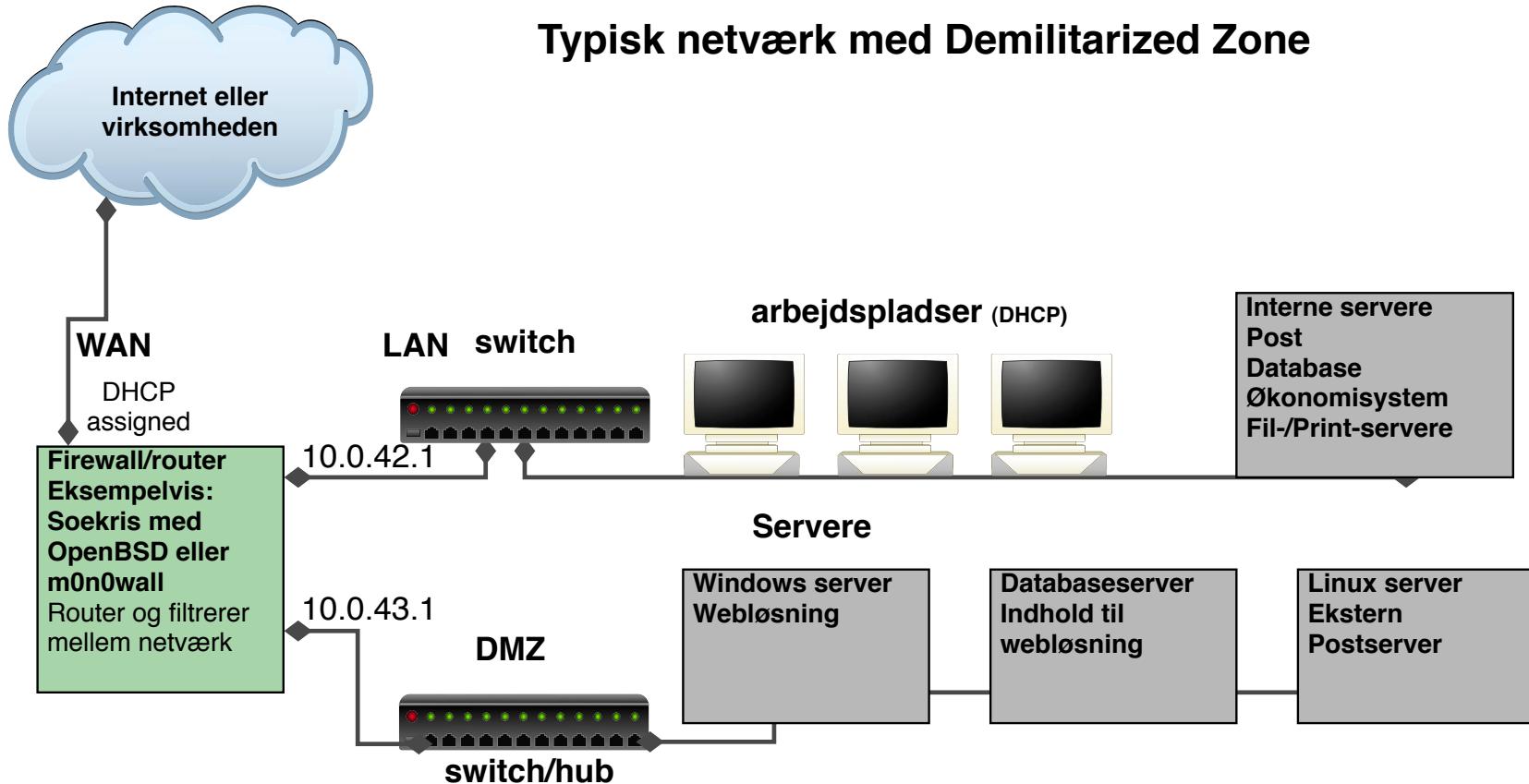
Brug dernæst en firewall med GUI første gang!

Husk dernæst:

- En firewall skal passes
- En firewall skal opdateres
- Systemerne bagved skal hærdes!

# En typisk firewall konfiguration

Typisk netværk med Demilitarized Zone



Opdeling i separate netværkssegmenter!

# Blokér indefra og ud

Der er porte og services som altid bør blokeres

Det kan være kendte sårbare services

- Windows SMB filesharing - ikke til brug på Internet!
- UNIX NFS - ikke til brug på Internet!

Kendte problemer:

- KaZaA og andre P2P programmer - hvis muligt!
- Portmapper - port 111

# IPsec og Andre VPN features

De fleste firewalls giver mulighed for at lave krypterede tunneler

Nyttigt til fjernkontorer der skal have usikker traffik henover usikre netværk som Internet

Konceptet kaldes Virtual Private Network VPN

IPsec er de facto standarden for VPN og beskrevet i RFC'er

Giver sikkerhed i netværket på lavt niveau - IP-niveau

- 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

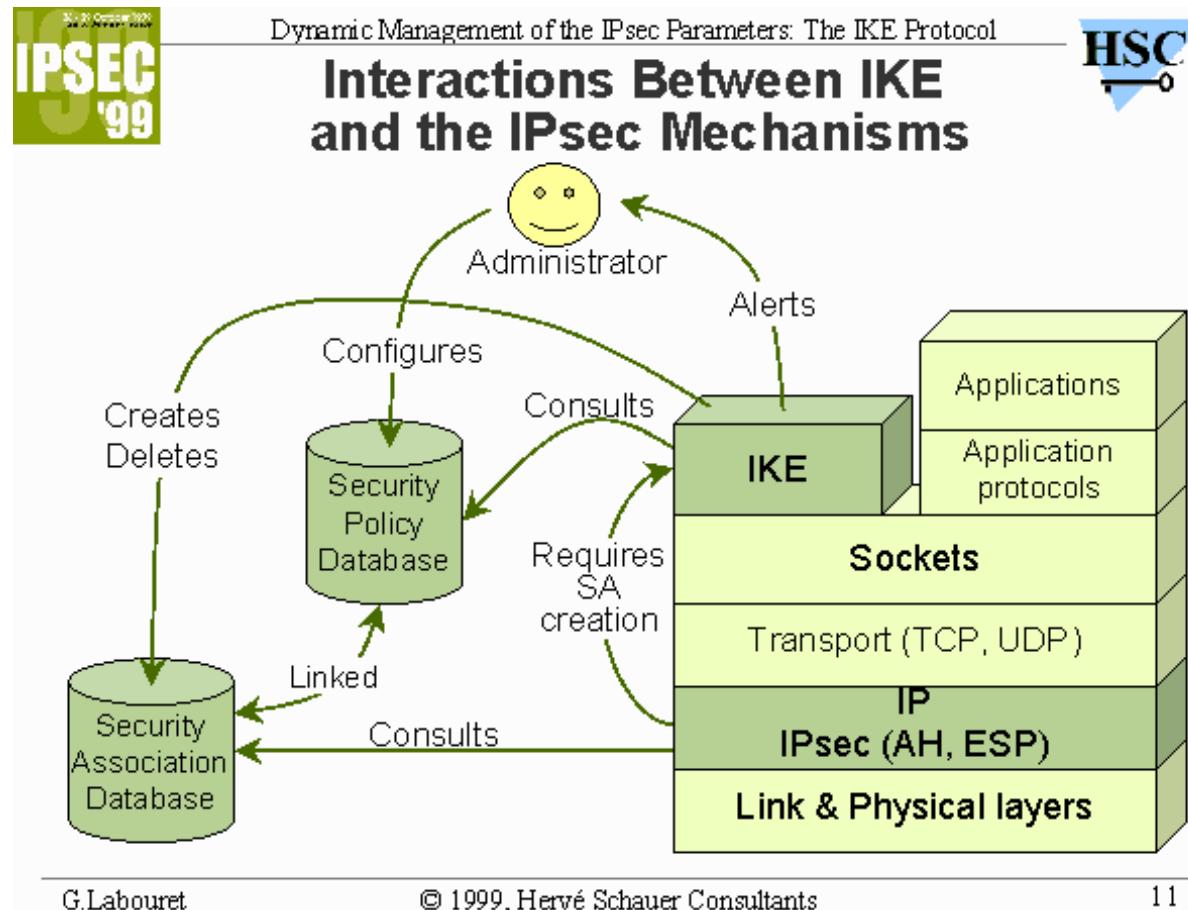
Både til IPv4 og IPv6

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

god præsentation på

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

# IPsec er ikke simpelt!



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

# RFC-2402 IP AH



The diagram illustrates the structure of the IPsec AH header. It consists of several fields arranged horizontally:

- Version**: A single byte (0x05) at the top left.
- Next Header**: A single byte (e.g., 0x0A for TCP).
- Payload Len**: A single byte representing the length of the payload.
- RESERVED**: A single byte reserved for future use.
- Security Parameters Index (SPI)**: A single byte used to identify the security association.
- Sequence Number Field**: A single byte used for sequence numbering.
- Authentication Data (variable)**: A variable-length field containing authentication data.

Below the header structure, there are two sets of vertical lines on the left and right sides, indicating padding or alignment.

# RFC-2402 IP AH

Indpakning - pakkerne før og efter Authentication Header:

BEFORE APPLYING AH

IPv4	orig IP hdr			
	(any options)	TCP	Data	

AFTER APPLYING AH

IPv4	orig IP hdr				
	(any options)	AH	TCP	Data	

-----

|<----- authenticated ----->|  
except for mutable fields

# RFC-2406 IP ESP

Pakkerne før og efter:

BEFORE APPLYING ESP

IPv6		ext	hdrs			
	orig	IP	hdr	if present	TCP	Data

AFTER APPLYING ESP

IPv6	orig	hop-by-hop,	dest*,	dest			ESP		ESP
	IP	hdr  routing,	fragment.	ESP  opt*	TCP  Data	Trailer	Auth		

| <---- encrypted ----> |  
| <---- authenticated ----> |

OpenVPN is a full-featured SSL VPN solution which can accomodate a wide range of configurations, including remote access, site-to-site VPNs, WiFi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls (articles) (examples) (security overview) (non-english languages).

Et andet populært VPN produkt er OpenVPN

Kilde: <http://openvpn.net/>

# OpenSSH portforward

OpenSSH kan bruges både til login og til filoverførsel

Men den kan også forwarde porte over usikre netværk

```
ssh -L2500:127.0.0.1:25 mail.kramse.dk
```

De senere versioner kan oprette tun interface til VPN brug

Secure Shell kan bruges som "fattigmandsVPN"

## Videregående firewalls

Mange firewalls tilbyder idag mere avancerede funktioner

Båndbreddestyring

Firewallcluster redundante firewalls

Virtuelle firewalls, firewall blades, men også i produkter som VMware

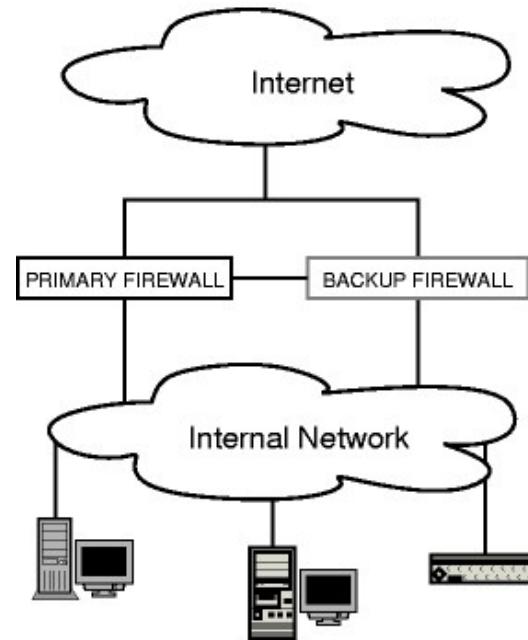
# Båndbreddestyring

Mange firewalls idag kan lave båndbredde allokering til protokoller, porte og derved bestemte services

Mest kendte er i Open Source:

- ALTQ bruges på OpenBSD - integreret i PF
- FreeBSD har dummynet
- Linux har tilsvarende  
ADSL-Bandwidth-Management-HOWTO, ADSL Bandwidth Management HOWTO  
Adv-Routing-HOWTO, Linux Advanced Routing & Traffic Control HOWTO  
<http://www.knowplace.org/shaper/resources.html> Linux resources

# Redundante firewalls - pfsync og CARP



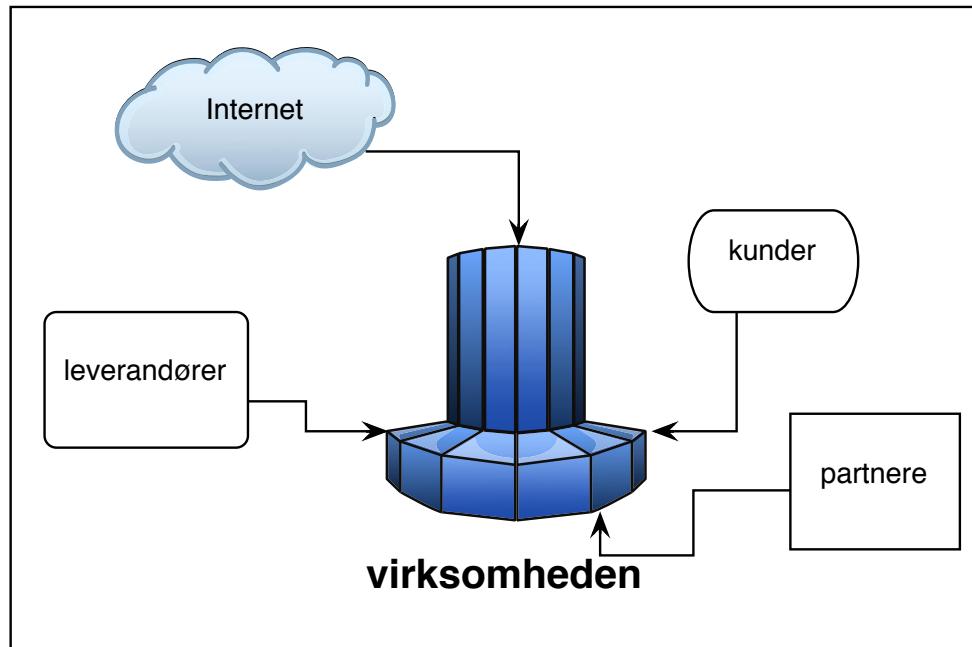
OpenBSD 3.5 har fået funktionalitet til at bygge redundante firewalls:

- Common Address Redundancy Protocol CARP - overtakelse af adresse både IPv4 og IPv6
- pfsync - sender opdateringer om firewall states mellem de to systemer
- Kilde: <http://www.countersiege.com/doc/pfsync-carp/>

# Design af en firewall platform

Hvordan ser den perfekte firewall ud?

Start med papir og blyant!



- Du VIL komme ud for hændelser, man kan ikke regne med at sikkerhedsforanstaltninger altid virker
- Der ER sket en hændelse - håndterer I den optimalt? - hvad er forøvrigt optimalt?
- Lav en plan over håndtering af hændelser

# Hændelseshåndtering - en metode

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

# Spørgsmål?



Dette afslutter det basale firewall foredrag, pause - derefter fortsætter vi med mere avancerede ting som pentestværktøjer, VLANs, WLANs osv.

**Henrik Lund Kramshøj**  
**hlk@security6.net**

<http://www.security6.net>

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

## Oversigt over anbefalinger

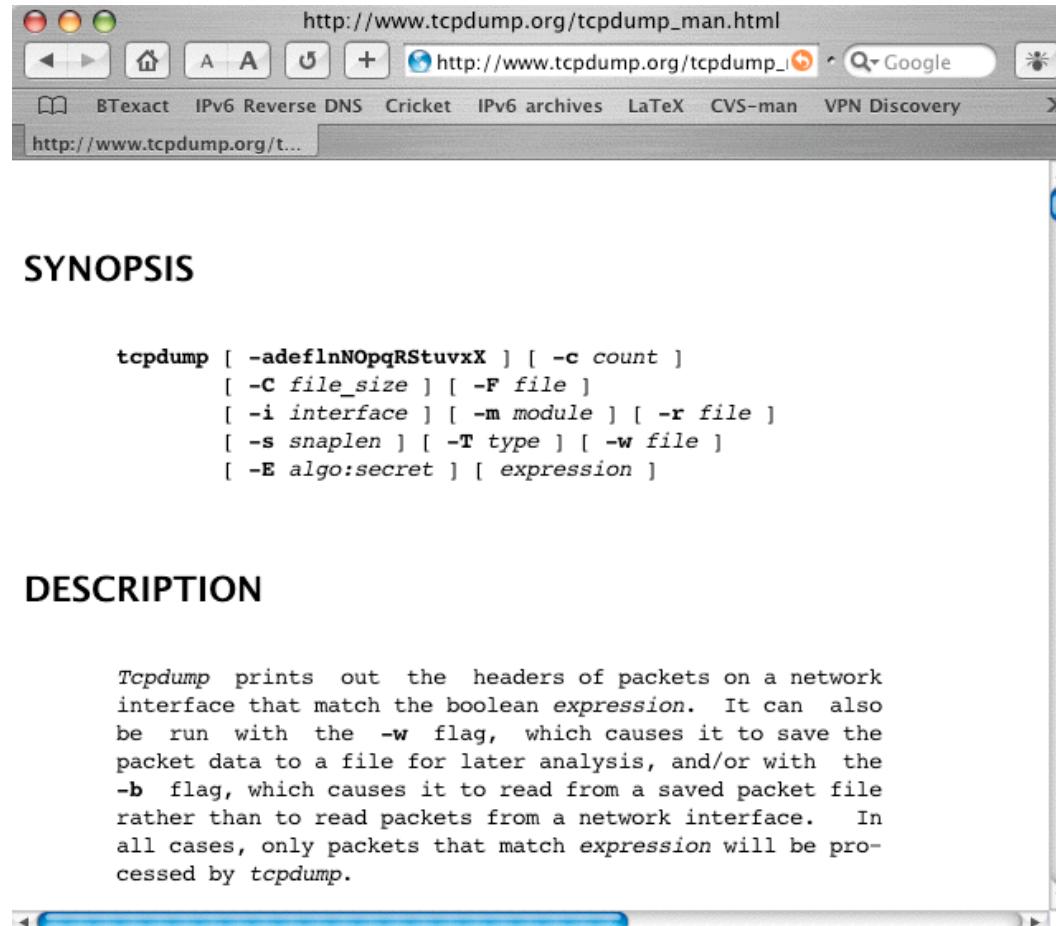
**Følg med!** - læs websites, bøger, artikler, mailinglister, ...

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

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

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

# TCPDUMP - protokolanalyse pakkesniffer



## SYNOPSIS

```
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 ]
```

## DESCRIPTION

*Tcpdump* prints out the headers of packets on a network interface that match the boolean expression. It can also be run with the **-w** flag, which causes it to save the packet data to a file for later analysis, and/or with the **-b** flag, which causes it to read from a saved packet file rather than to read packets from a network interface. In all cases, only packets that match expression will be processed by *tcpdump*.

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

# tcpdump - normal brug

- 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
...
```

# Wireshark - grafisk pakkesniffer



The screenshot shows the official Wireshark website homepage. At the top, there's a large blue header with the "WIRESHARK" logo and a shark silhouette. Below the header is a navigation bar with links: HOME, ABOUT, WHAT'S NEW, DOWNLOAD, and FAQ. To the right of the navigation is a photograph of a shark swimming in the ocean. On the left side, there's a sidebar with a dark blue background containing links under categories like "Get It", "Get Help", "Develop", and "Products". The main content area has several sections: "Sniffing Problems A Mile Away" which explains the name change from Ethereal to Wireshark; a screenshot of the Wireshark interface showing network traffic; a "News" section about the release of version 0.99.3; and a "FAQs" section with a question and answer about capturing 802.11 traffic using AirPcap.

**Sniffing Problems A Mile Away**

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

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

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

**News**

**Wireshark 0.99.3 Released**

Aug 23, 2006

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

**Download Now**

0.99.3

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

**A:**  
**AirPcap**

<http://www.wireshark.org>

både til Windows og UNIX, tidligere kendt som Ethereal

# Programhygiejne!

Download, installer - kør! - farligt!

Sådan gøres det:

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

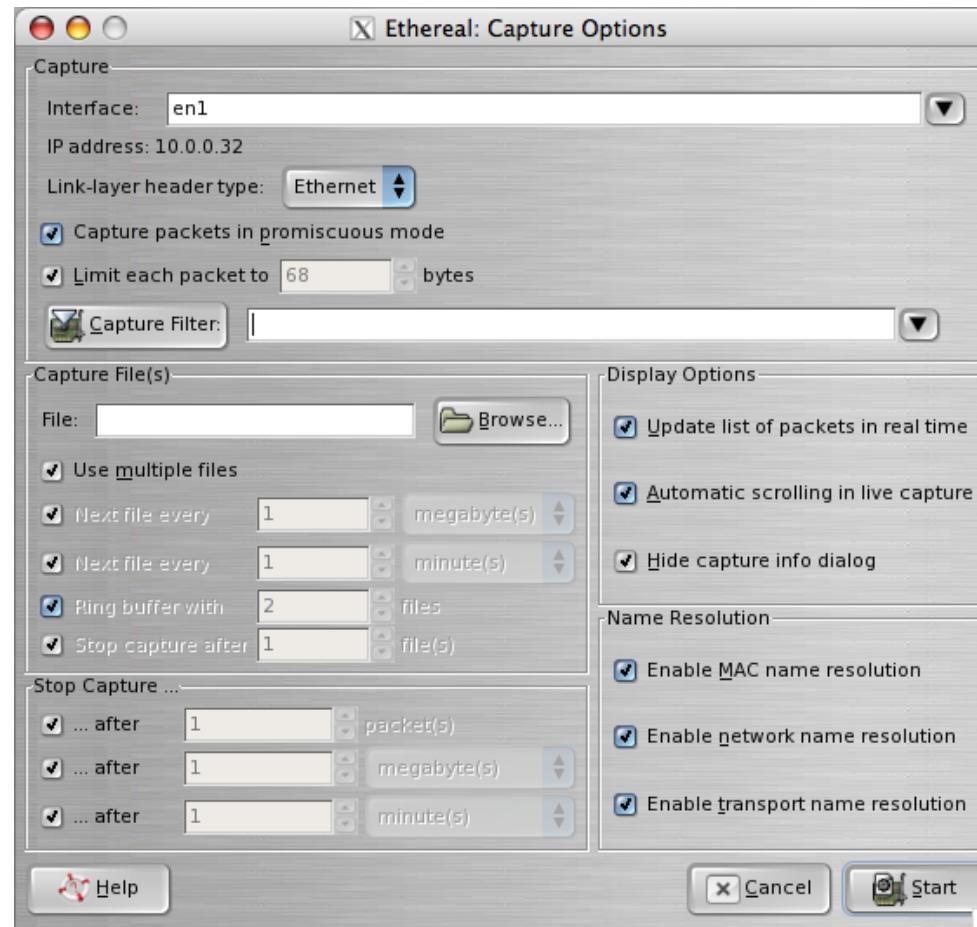
Se eksempelvis teksten på hjemmesiden:

*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

# Brug af Wireshark



Man starter med Capture - Options

# Brug af Wireshark



The screenshot shows the Wireshark interface with the title bar "X (Untitled) - Ethereal". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains various icons for file operations, search, and analysis. The main pane displays a list of network frames. Frame 563 is selected, showing details: Source 10.0.0.32, Destination sunny.kramse.dk, Protocol TCP, and Info 54021 > imaps [ACK] Seq=426 Ack=11106 Win=65!. Below this, a detailed description of the frame is provided. The bottom pane shows the raw hex and ASCII data of the selected frame.

No.	Time	Source	Destination	Protocol	Info
561	0.700947	10.0.0.32	sunny.kramse.dk	TCP	54021 > imaps [ACK] Seq=426 Ack=11106 Win=65!
562	6.763144	sunny.kramse.dk	10.0.0.32	TLS	Continuation Data, [Unreassembled Packet]
563	6.820037	10.0.0.32	sunny.kramse.dk	TCP	54021 > imaps [ACK] Seq=426 Ack=11106 Win=65!
564	6.919635	10.0.0.32	sunny.kramse.dk	TCP	54023 > imaps [SYN] Seq=0 Ack=0 Win=65535 Len
565	6.921708	sunny.kramse.dk	10.0.0.32	TCP	imaps > 54023 [SYN, ACK] Seq=0 Ack=1 Win=1638
566	6.921794	10.0.0.32	sunny.kramse.dk	TCP	54023 > imaps [ACK] Seq=1 Ack=1 Win=65535 Len
567	6.922614	10.0.0.32	sunny.kramse.dk	TLS	Client Hello

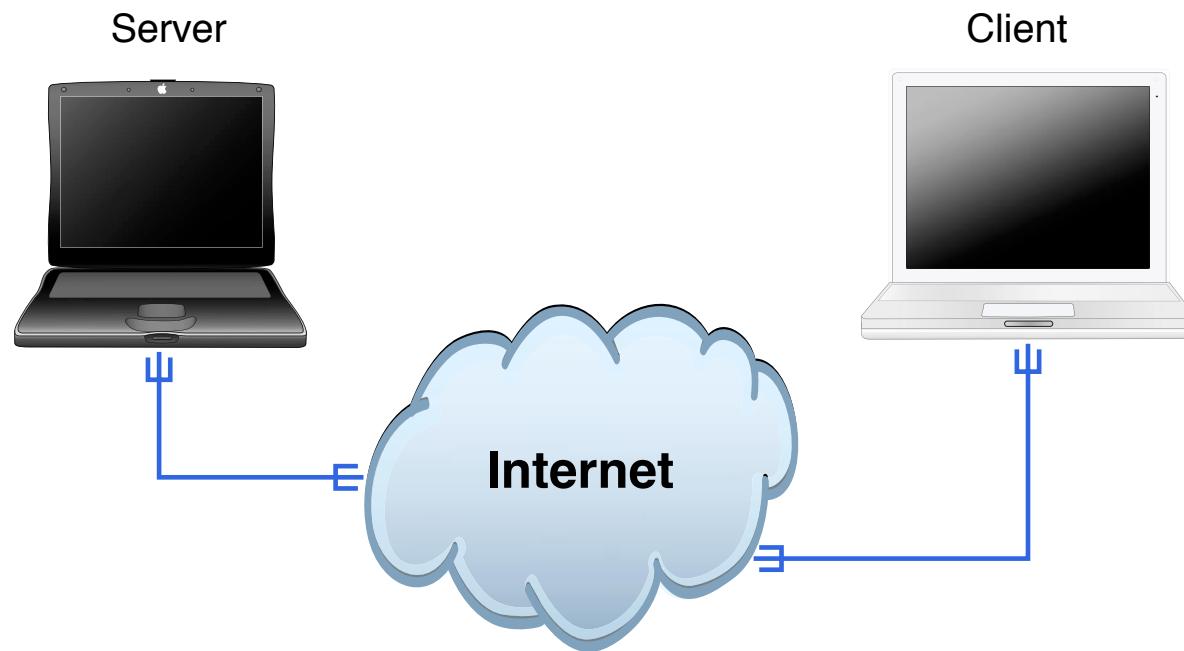
Frame 563 (66 bytes on wire, 66 bytes captured)  
Ethernet II, Src: AppleCom\_86:7c:3f (00:0d:93:86:7c:3f), Dst: Olicom\_c3:57:d8 (00:00:24:c3:57:d8)  
Internet Protocol, Src: 10.0.0.32 (10.0.0.32), Dst: sunny.kramse.dk (217.157.20.131)  
Transmission Control Protocol, Src Port: 54021 (54021), Dst Port: imaps (993), Seq: 426, Ack: 11106, Len: 0

0000 00 00 24 c3 57 d8 00 0d 93 86 7c 3f 08 00 45 00 ..\$.W...|?.E.  
0010 00 34 7e 8b 40 00 40 06 c3 f8 0a 00 00 20 d9 9d .4~.@@. .... ..  
0020 14 83 d3 05 03 e1 cd 31 c9 ea 0d 7b a2 bf 80 10 .....1 ...{....  
0030 ff ff 32 0d 00 00 01 01 08 0a 62 e0 c3 42 bb e3 ..2.....b..B..

Filter: Expression... Clear Apply File: "/var/tmp/ether0ARkxt..."

Læg mærke til filtermulighederne

# Demo: Wireshark



## Wireshark



SSH afløser en række protokoller som er usikre:

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

# SSH - de nye kommandoer er

kommandoerne er:

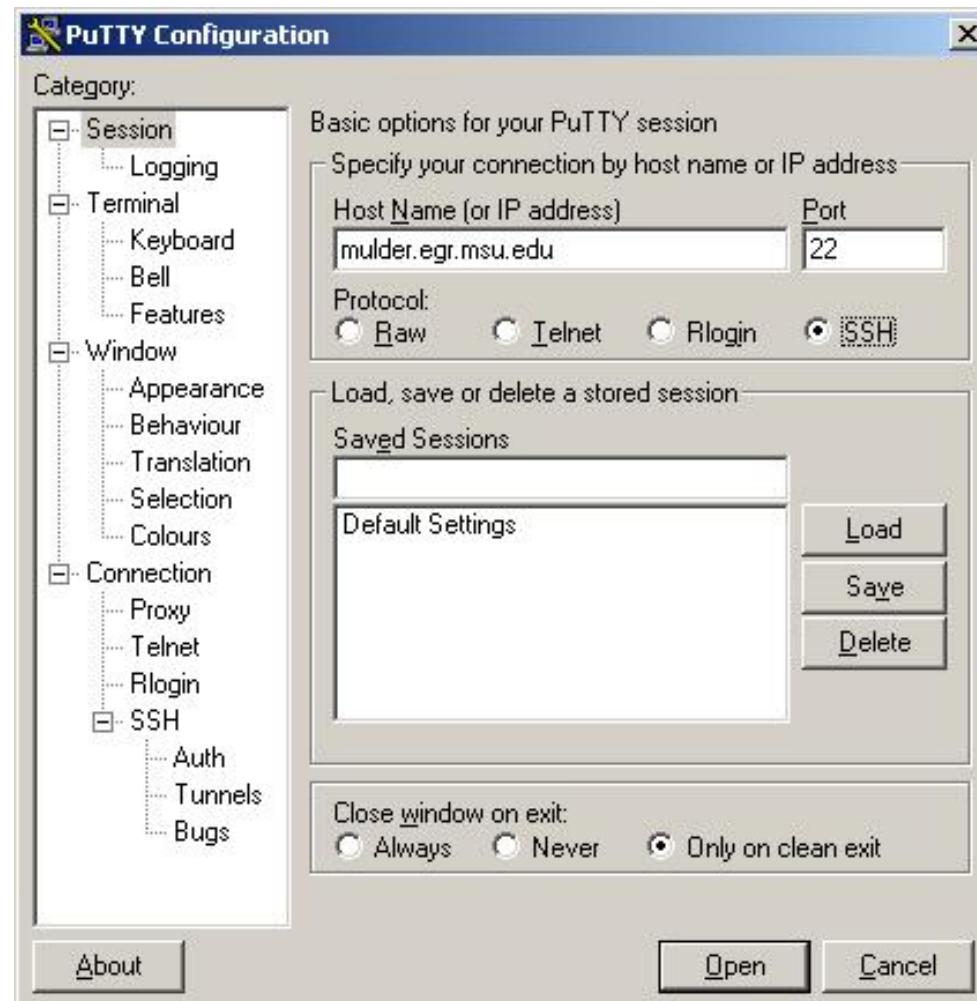
- ssh - Secure Shell
- scp - Secure Copy
- sftp - secure FTP

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

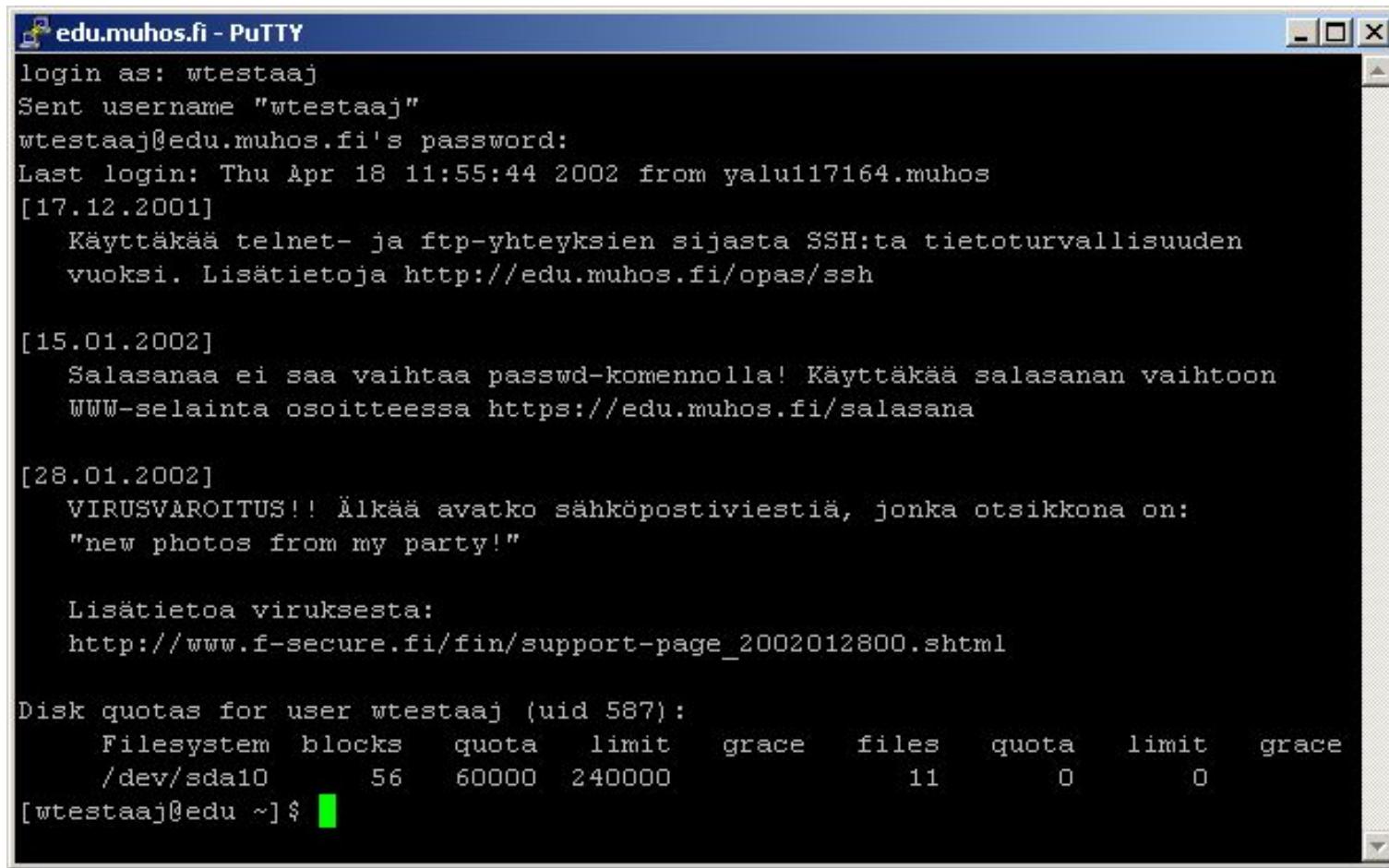
**NB: Man bør idag bruge SSH protokol version 2!**

# 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 log 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 yalu117164.muhos
[17.12.2001]
    Käyttää telnet- ja ftp-yhteyksien sijasta SSH:ta tietoturvallisuuden
    vuoksi. Lisätietoja http://edu.muhos.fi/opas/ssh

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

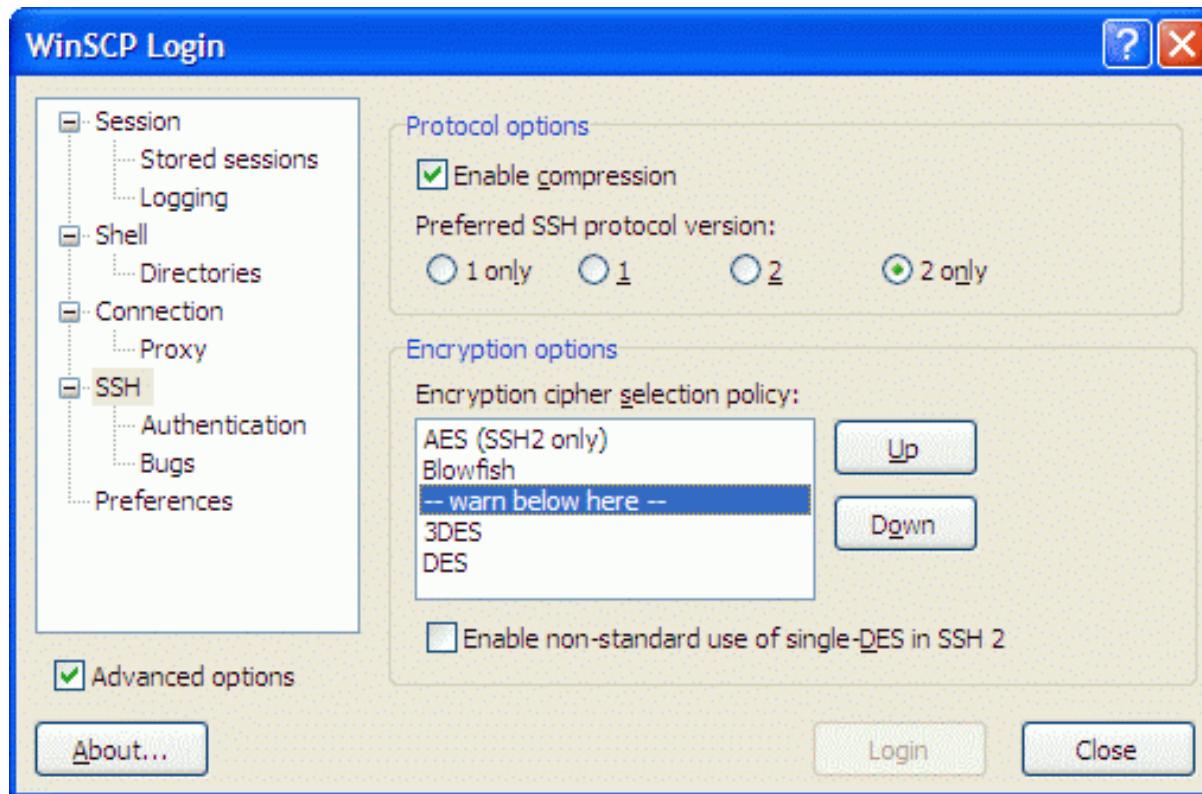
[28.01.2002]
    VIRUSVAROITUS!! Älkää avatko sähköpostiviestiä, jonka otsikkona on:
    "new photos from my party!"

    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>

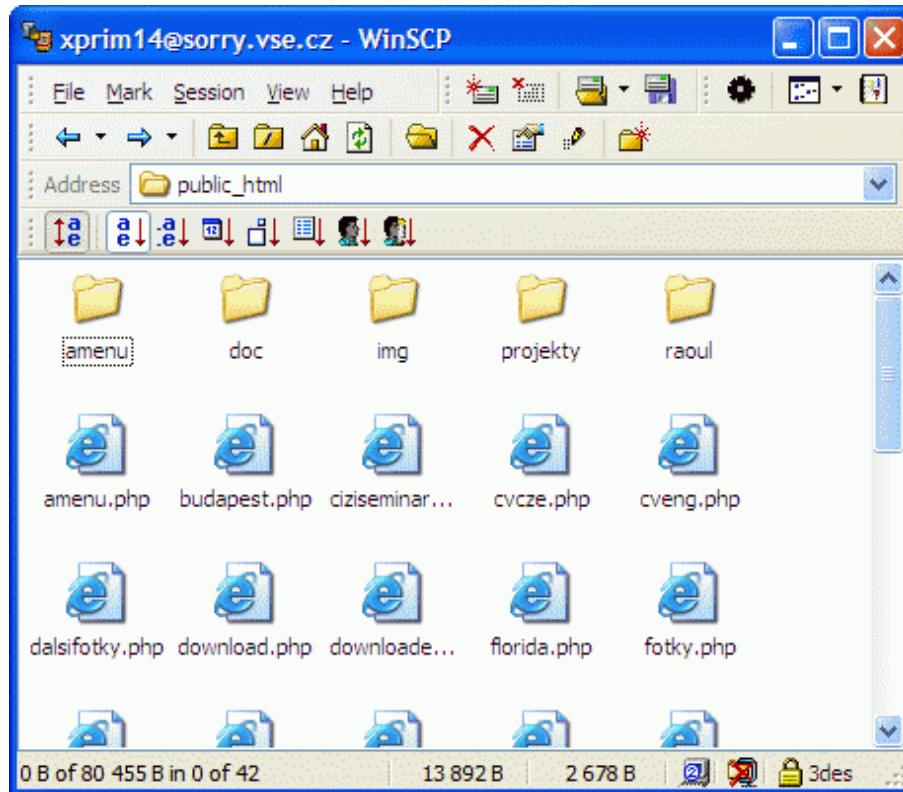
# Grafisk Secure Copy - WinSCP



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>

## traceroute

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
```

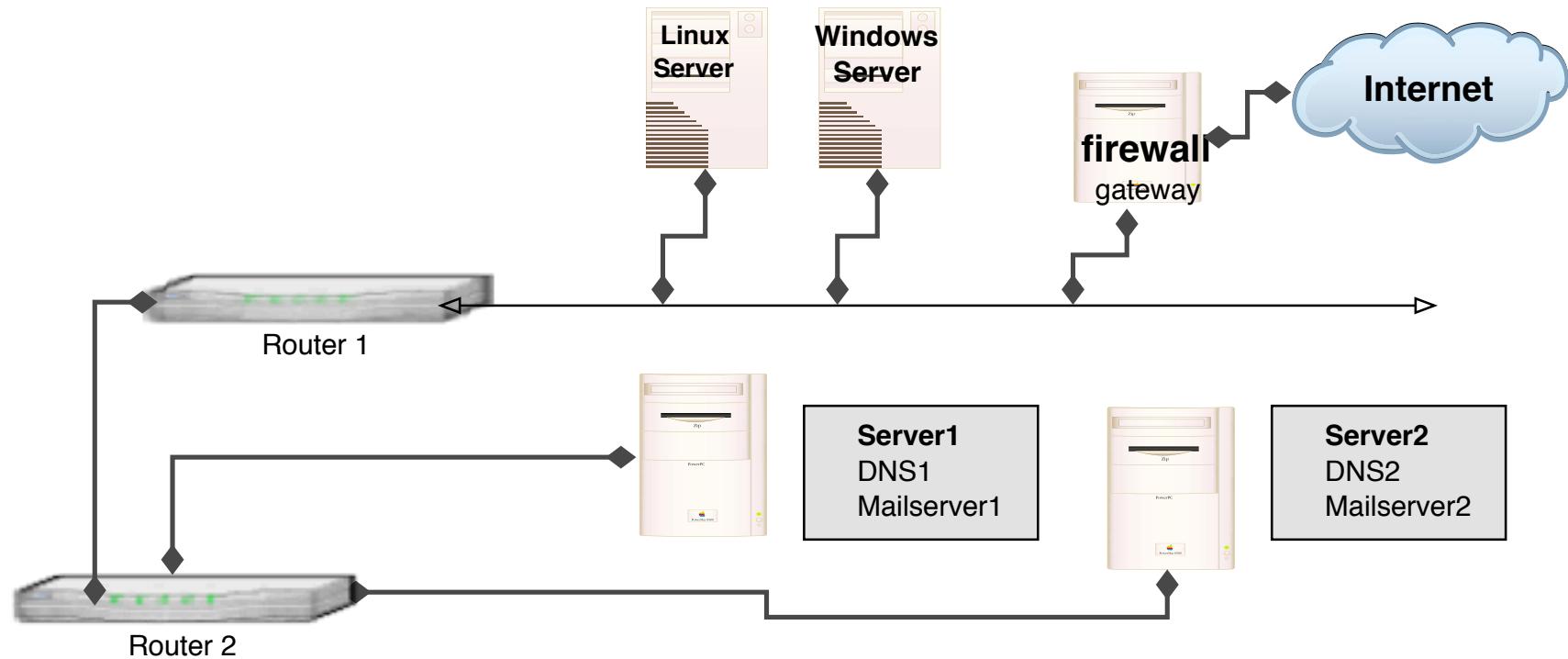
diagnosticering af netværksproblemer - formålet med traceroute

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

## Flere traceprogrammer

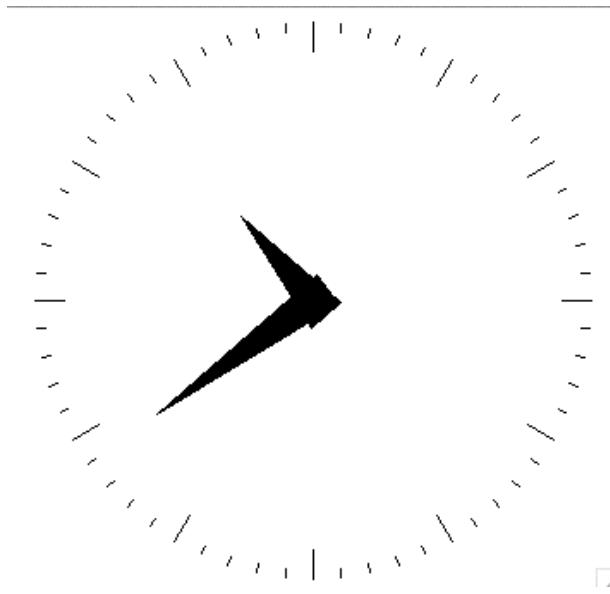
mtr My traceroute - grafisk <http://www.bitwizard.nl/mtr/>

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

# What time is it? - spørg ICMP

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
```

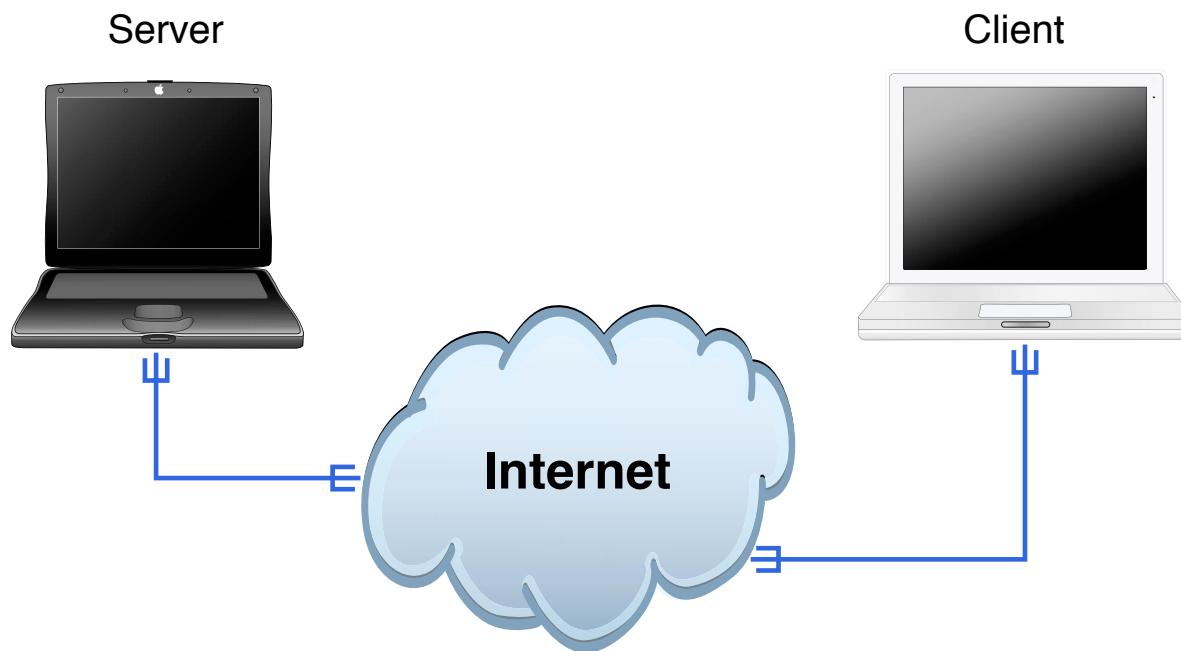
```
ICMP Timestamp Request packet sent to 10.0.0.12 (10.0.0.12)
```

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

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

```
icmpush: Program finished OK
```

# Demo: ICMPUSH og tracroute



## ICMPUSH og tracroute

# Informationsindsamling

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

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)

## whois systemet -2

ansvaret for Internet IP adresser ligger hos ICANN The Internet Corporation for Assigned Names and Numbers <http://www.icann.org>

NB: ICANN må ikke forveksles med IANA Internet Assigned Numbers Authority <http://www.iana.org/> som bestyrer portnumre og andre magiske konstanter m.v.

# DNS systemet

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

# Mere end navneopslag

består af resource records med en type:

- adresser A-records
- 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.

# 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;

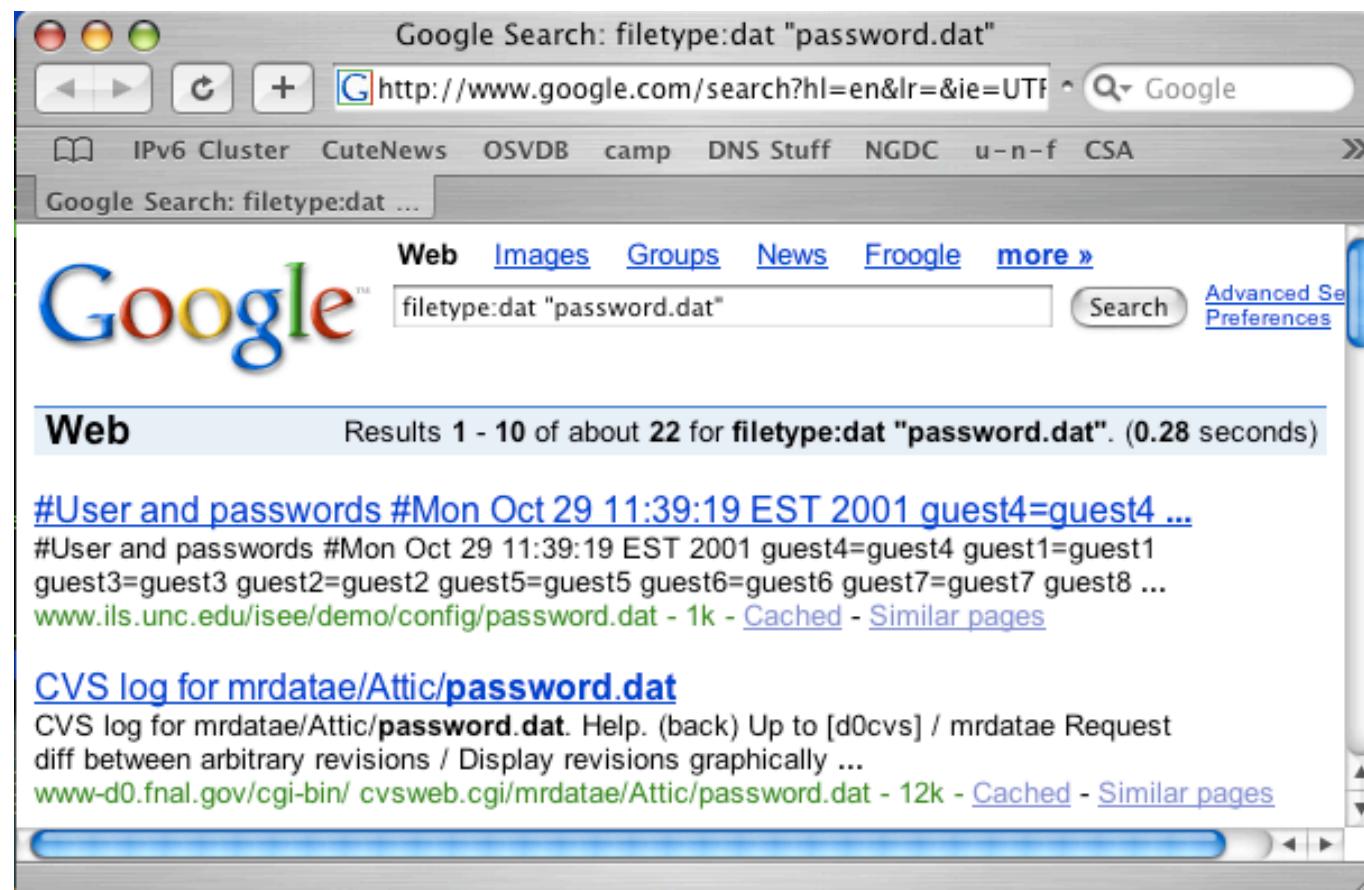
my $resolver = Net::DNS::Resolver->new;
$resolver->nameservers ($ARGV[0] );

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 for it



Google som hacker værktøj?

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

# Hvordan virker ARP?

Server



10.0.0.1

IP adresser

00:30:65:22:94:a1



MAC adresser - Ethernet

Client



10.0.0.2

10.0.0.1

## Hvordan virker ARP? - 2

**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

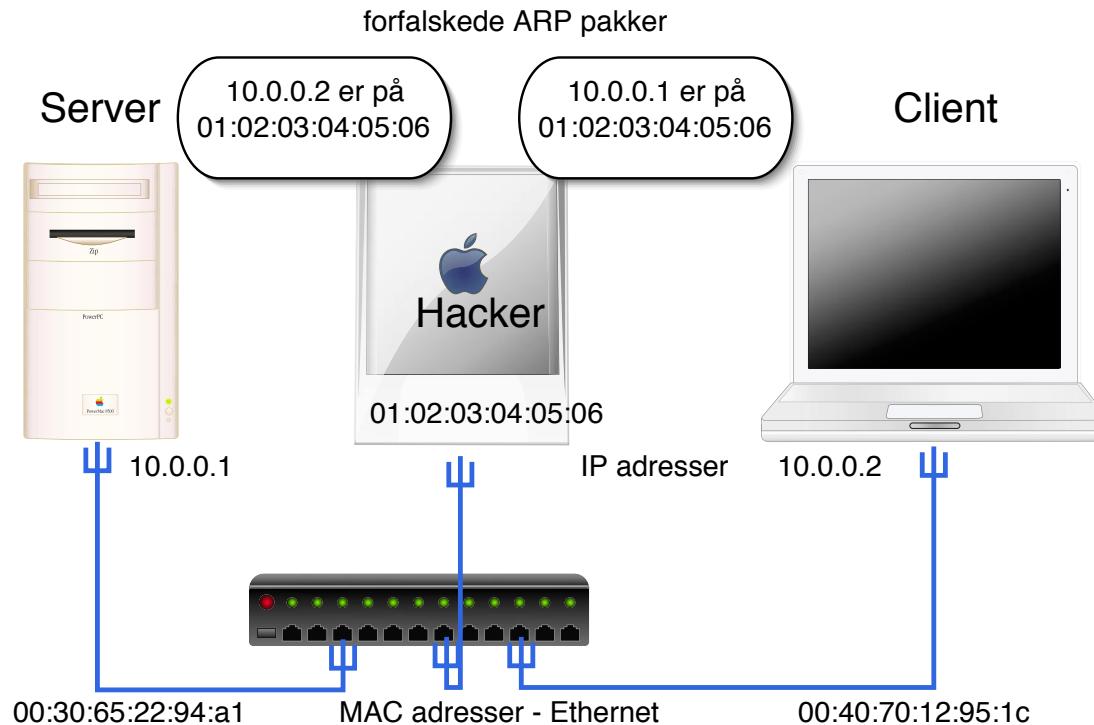
IP ICMP request/reply:

- 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

# dsniff

en sniffer til mange usikre protokoller

inkluderer **arpspoof**

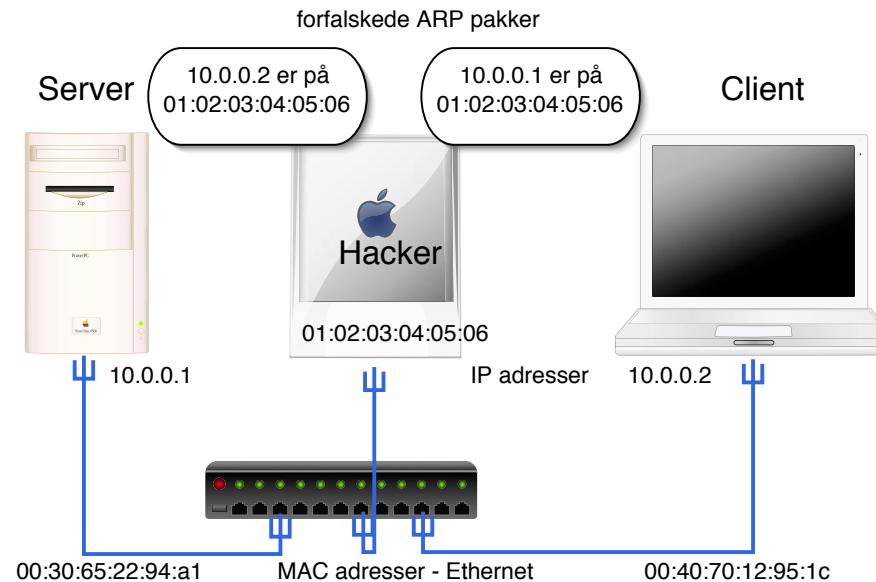
Lavet af Dug Song, [dugsong@monkey.org](mailto:dugsong@monkey.org)

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.

# dsniff forudsætninger

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



# Forsvar mod ARP spoofing

Hvad kan man gøre?

låse MAC adresser til porte på switcher

låse MAC adresser til bestemte IP adresser

Efterfølgende administration!

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

bruge protokoller som ikke er sårbare overfor opsamling

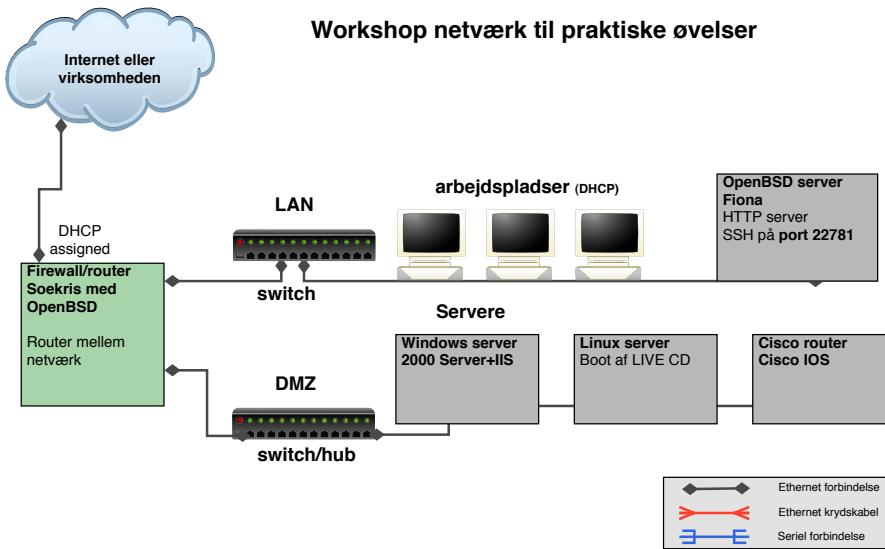
# Kommenteret dsniff

```
[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
```

## Workshop netværk til praktiske øvelser



## 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

# Intrusion Detection Systems - IDS

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

# Basal Portscanning

Hvad er portscanning

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

målet er at identificere åbne porte - sårbare services

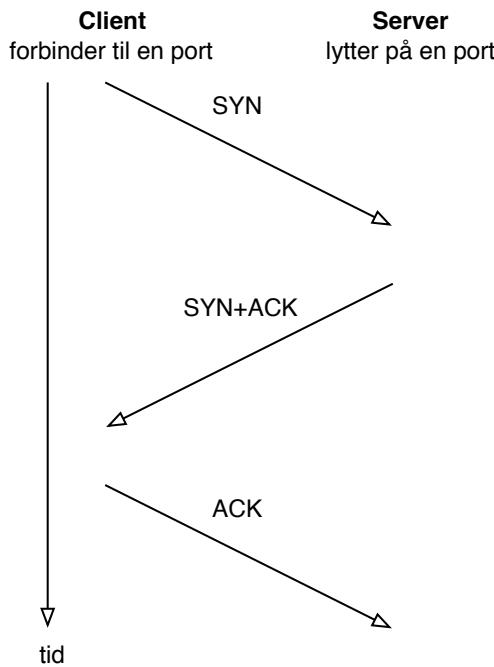
typisk TCP og UDP scanning

TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

# TCP three way handshake



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

# Ping og port sweep

scanninger på tværs af netværk kaldes for sweeps

Scan et netværk efter aktive systemer med PING

Scan et netværk efter systemer med en bestemt port åben

Er som regel nemt at opdage:

- 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 after 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
```

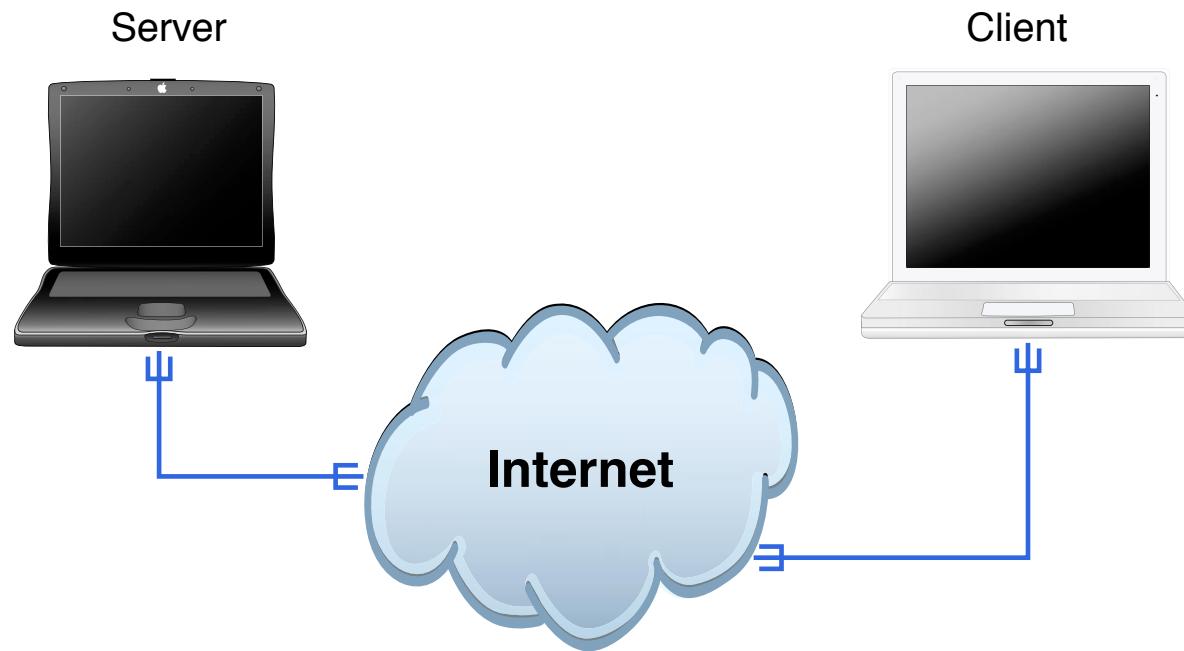
The 1 scanned port on (217.157.20.132) is: closed

# OS detection

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

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

# Demo: Portscans med Nmap Frontend program



## Portscans med Nmap Frontend program

## Erfaringer hidtil

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

# Simple Network Management Protocol



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>

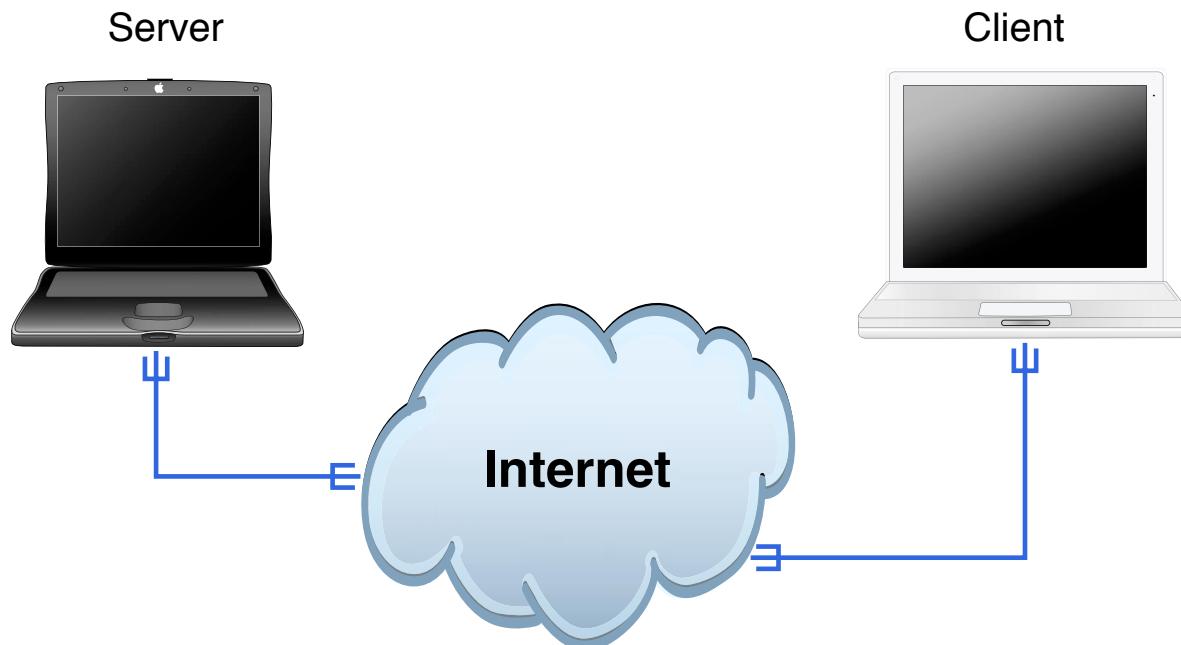
Syntax: hydra [[[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]  
[-o FILE] [-t TASKS] [-g TASKS] [-T SERVERS] [-M FILE] [-w TIME]  
[-f] [-e ns] [-s PORT] [-S] [-vV] server service [OPT]

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

...

# Demo: snmpwalk og Hydra



**snmpwalk og Hydra**

## NT hashes

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 l0phtcrack 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

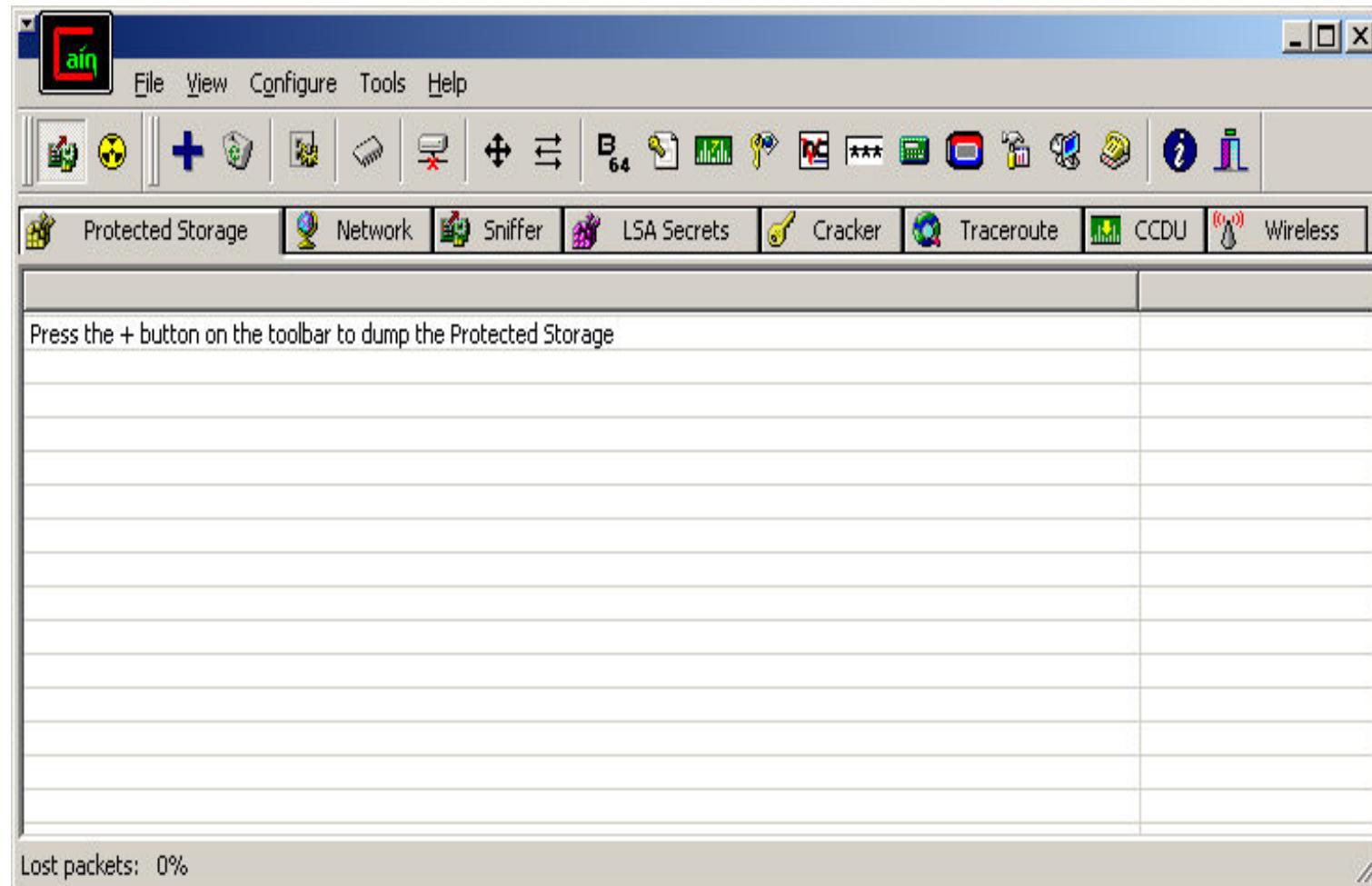
# I0phcrack LC4



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

L0ptCrack 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



Cain og Abel anbefales ofte istedet for l0phtcrack <http://www.oxid.it>

# John the ripper

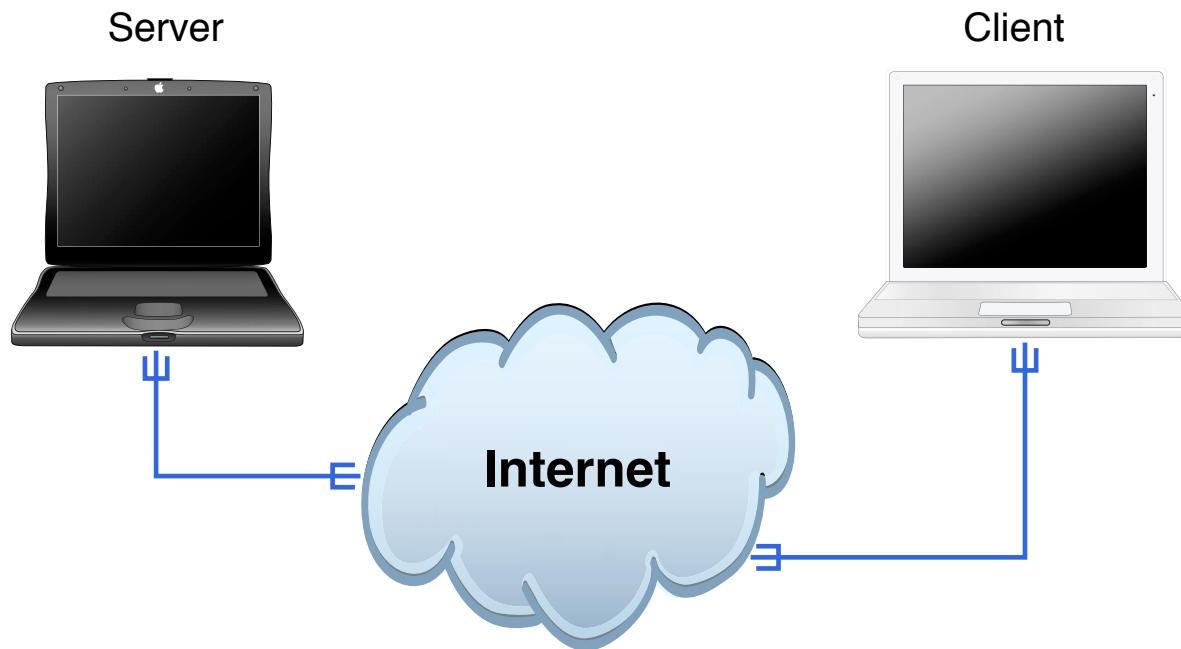


John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly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

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

Jeg bruger selv John The Ripper

# Demo: Cain og Abel



## Cain og Abel

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, Triple DES og AES/Rijndael

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

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>

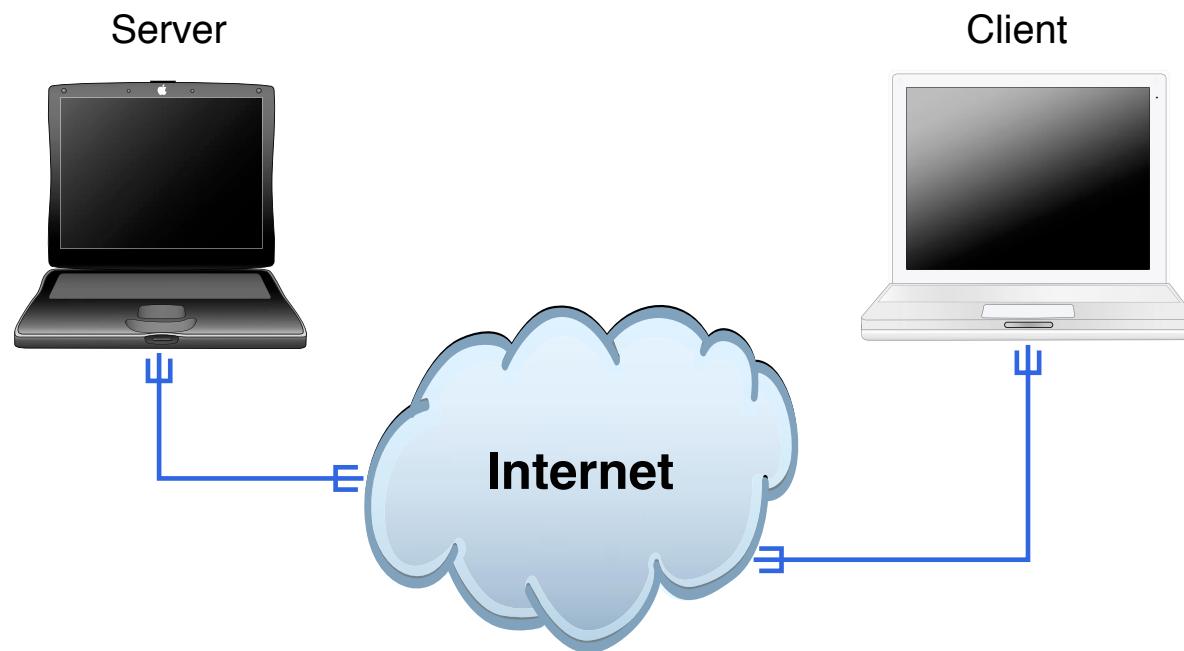
## Kilder:

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

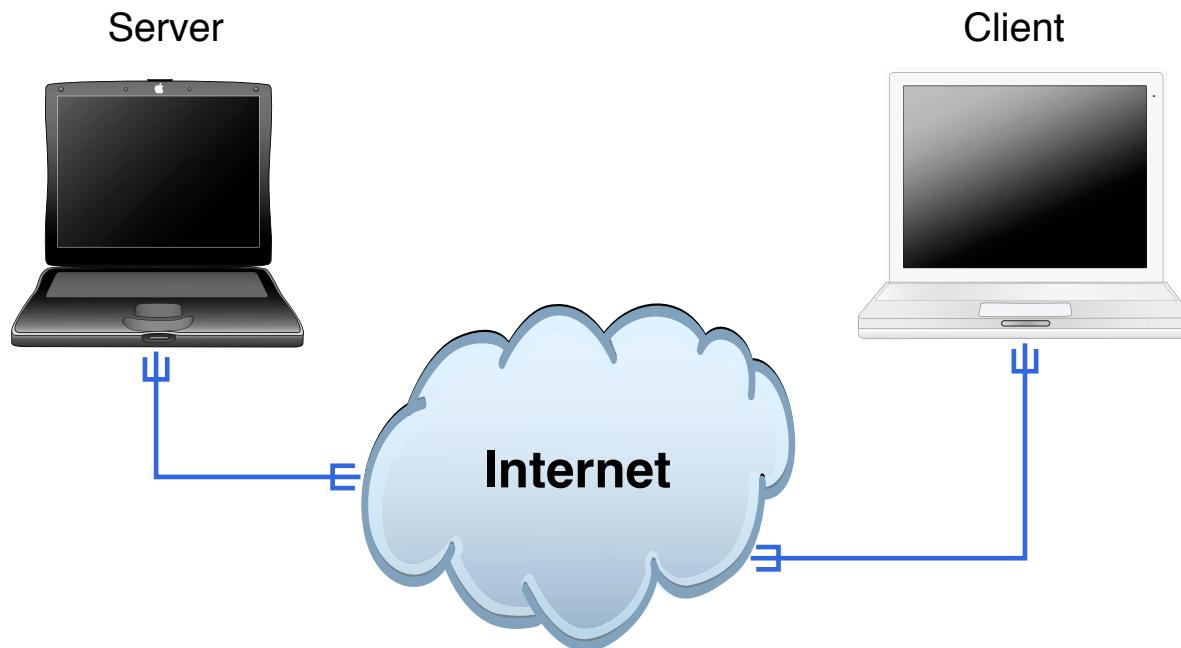
<http://www.cert.org/advisories/CA-2003-16.html>

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

# Demo: Exploit dcom.c



## Exploit dcom.c



- 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
- Husk at selom dcom er gammel er der mange tilsvarende idag!

# Hvad sker der?

```
[hlk@fiona hlk]$ ./dcom 1 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]$
```

Common Vulnerabilities and Exposures (CVE) er:

- klassifikation
- unik navngivning af sårbarheder.

Sårbarheder tildes

- 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>

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>

## 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

- Websvoren 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 familien

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)*

# konfigurationsfejl - ofte overset

Security

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

# Insecure programming

Problem:

Ønsker et simpelt CGI program, en web udgave af finger

Formål:

Vise oplysningerne om brugere på systemet

# review af nogle muligheder

## 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!!!

# Hello world of insecure web CGI

Demo af et sårbart system - badfinger

Løsning:

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

# De vitale - og usikre dele

```
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";
}
}
```

# Almindelige problemer

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

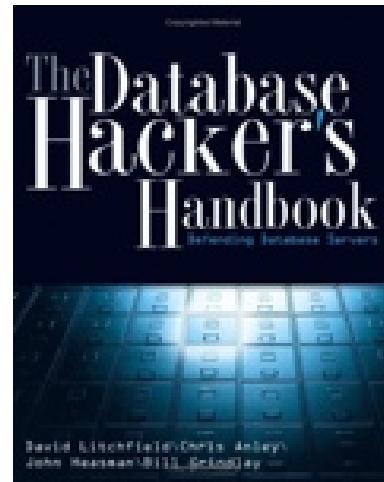
SQL Injection FAQ <http://www.sqlsecurity.com>:

```
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

# Mere SQL injection / SQL server

## 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

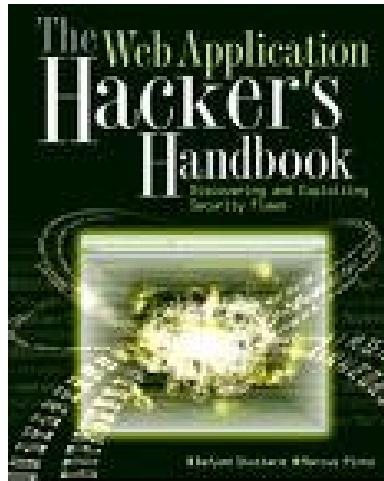
[http://www.nextgenss.com/papers/advanced\\_sql\\_injection.pdf](http://www.nextgenss.com/papers/advanced_sql_injection.pdf)

(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]

# Mere Web application hacking



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

# Hvordan udnyttes forms nemmest?

Manuelt download form:

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

fjern kald til validering:

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

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

# Hvordan udnyttes forms nemmest?

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

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

Kald form i en browser og indtast værdier

# WebScarab eller Firefox plugins

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

# Historik indenfor websikkerhed

## 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

# Opsummering websikkerhed

Security

.net

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 listen fra <http://www.owasp.org>

## Privilegier least privilege

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

# Privilegier privilege escalation

**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

# Hærdning af Microsoft IIS

Internet Information Services kan hærdes ...  
det kræver blot at man følger den guide som Microsoft har lavet  
- og at man jævnligt følger med i opdateringer til denne guide  
det anbefales at bruge de tilgængelige værktøjer som eksempelvis urlscan

IIS version 6 er mere sikker i default opsætningen - næsten alt er slået fra

# Undgå standard indstillinger

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

# buffer overflows et C problem

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.

# Exploits - udnyttelse af sårbarheder

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 exploits

**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

# Hvordan laves et buffer overflow?

Findes ved at prøve sig frem

- black box testing
- closed source
- reverse engineering

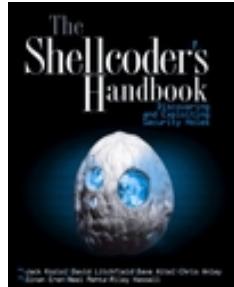
Ved Open source Findes de typisk ved at læse/analysere koden

- RATS
- flere andre

Virker typisk mod specifikke versioner

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

# Buffer overflows



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

*Smashing The Stack For Fun And Profit* Aleph One

*Writing Buffer Overflow Exploits with Perl - anno 2000*

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!

# Stack protection

Security

.net

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>

# Hackerværktøjer

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

Senere i 1995 udgav de så en softwarepakke med navnet SATAN *Security Administrator Tool for Analyzing Networks*. Pakken vagte en del furore, idet man jo gav alle på internet mulighed for at 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 i dag findes mange hackerværktøjer og automatiserede scannere:

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

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

# Brug hackerværktøjer!

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

## What is it?

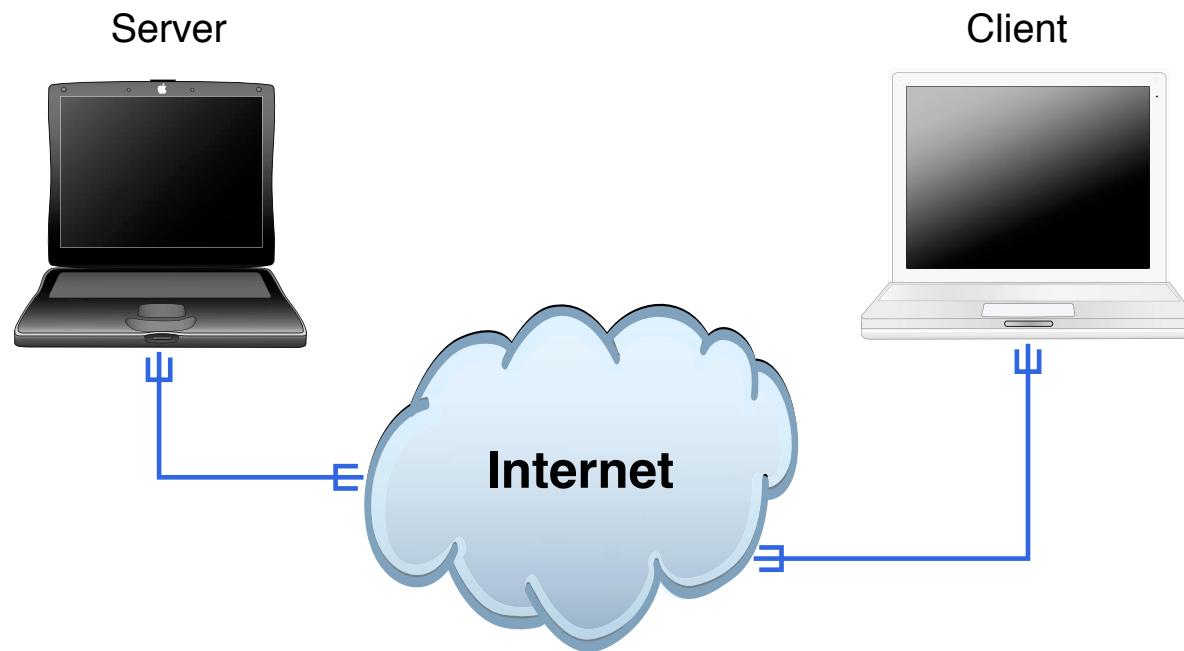
The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers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

Metasploit er modulært og nemt at bruge

Det er skræmmende enkelt at udvikle og udføre exploits

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

# Demo: Metasploit med dcom



## Metasploit med dcom

802.11 er arbejdsgruppen under IEEE

De mest kendte standarder idag indenfor trådløse teknologier:

- 802.11b 11Mbps versionen
- 802.11g 54Mbps versionen

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>

# 802.11 modes og frekvenser



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

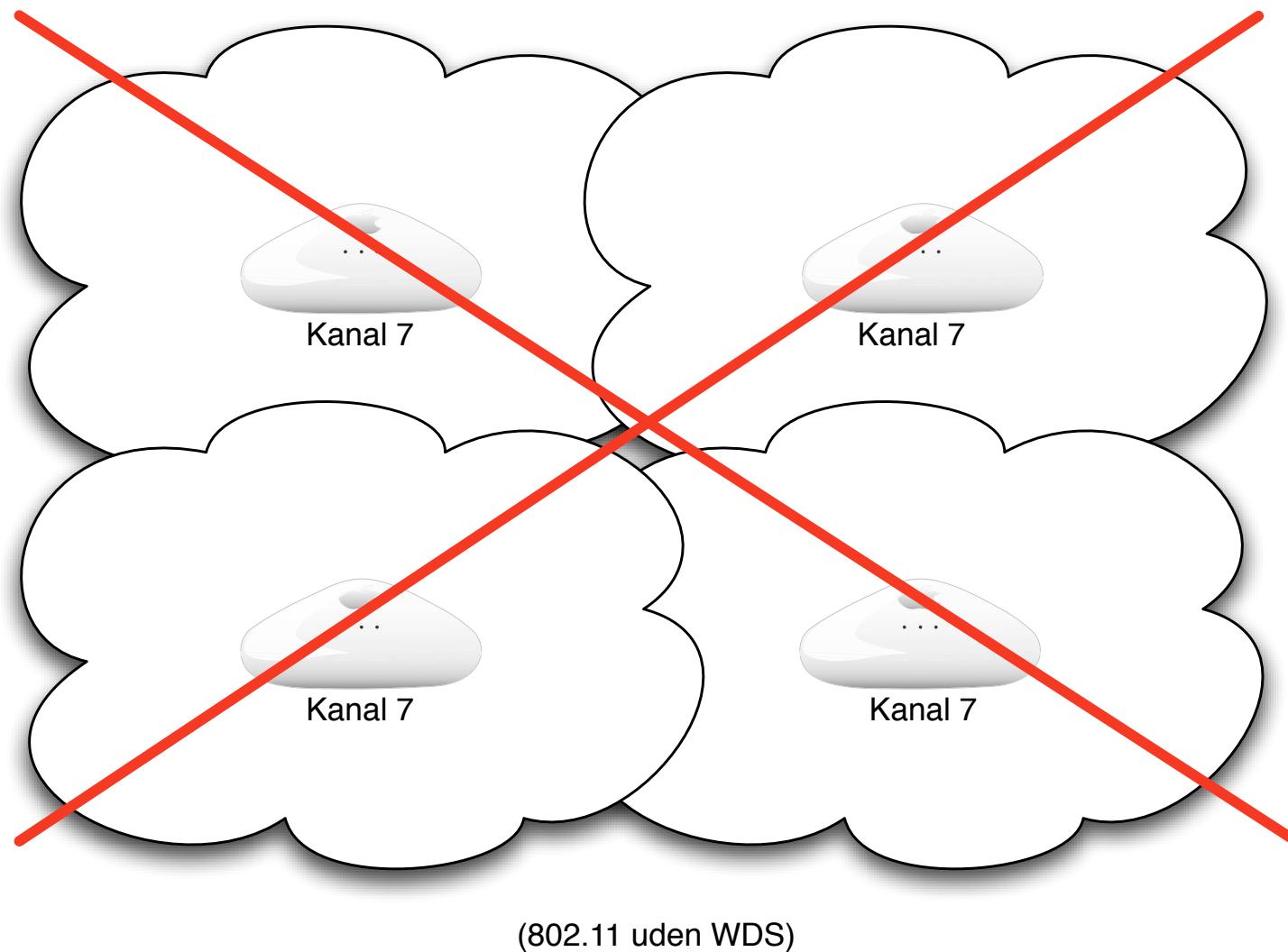
Alternativt kan wireless kort oprette ad-hoc netværk - hvor trafikken går direkte mellem netkort

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

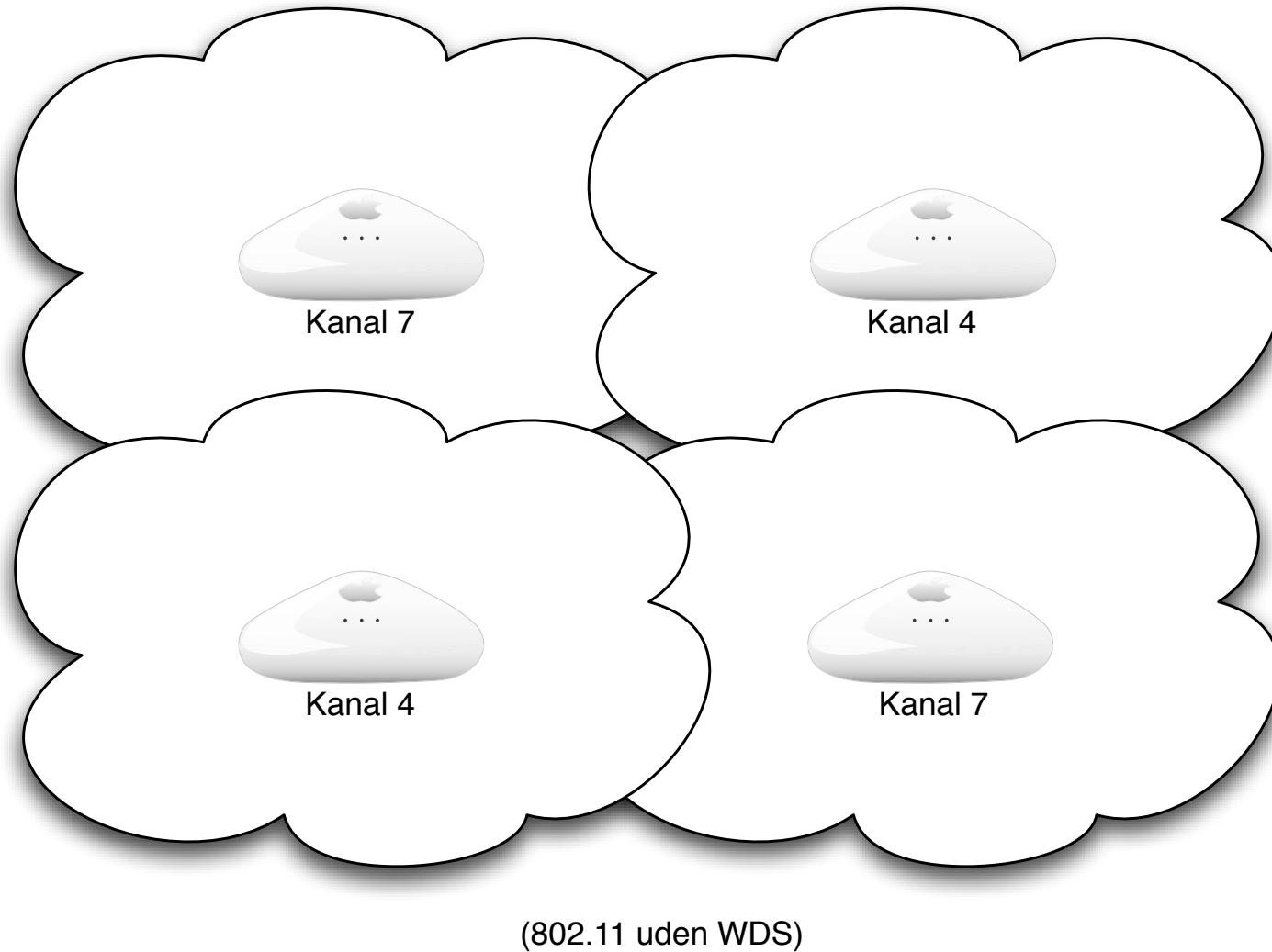
Helst 2 kanaler spring for 802.11b AP der placeres indenfor rækkevidde

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

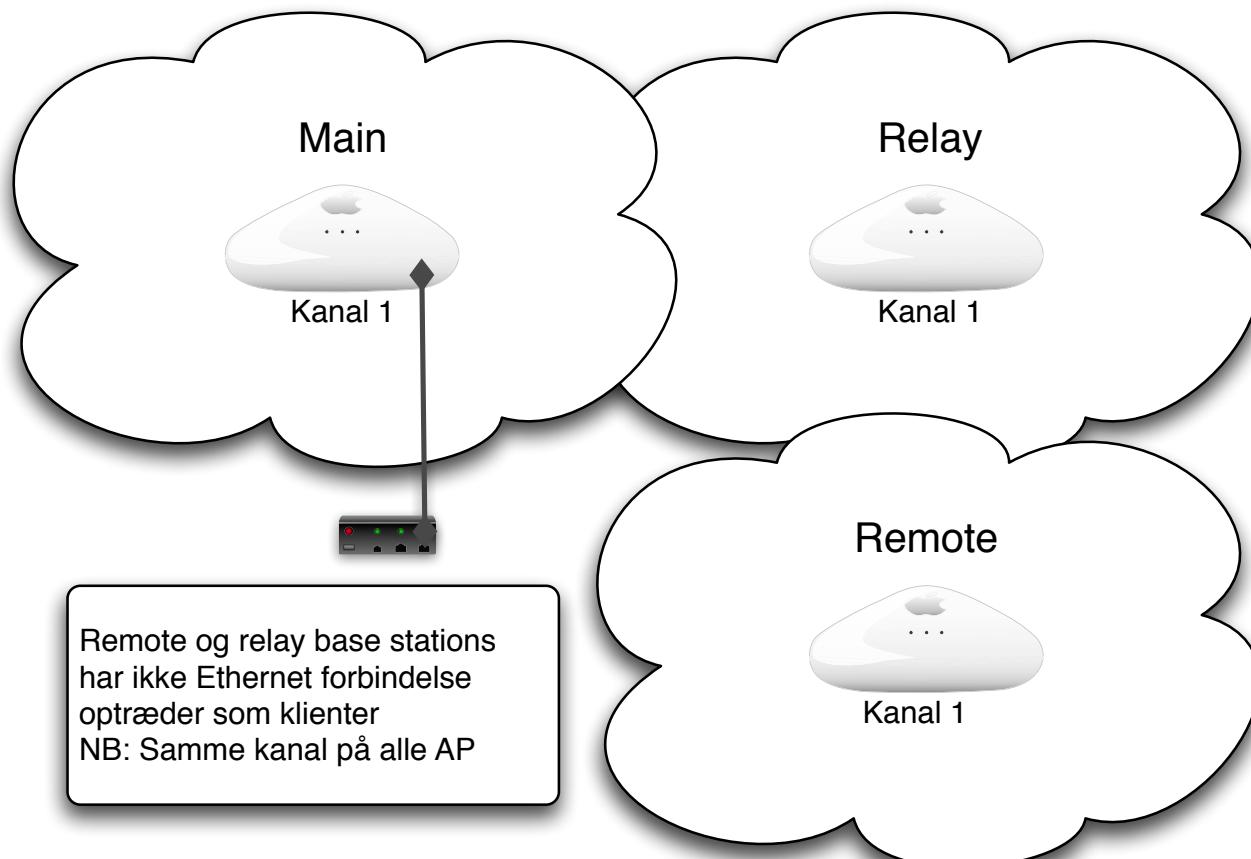
# Eksempel på netværk med flere AP'er



# 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)

# Er trådløse netværk interessante?

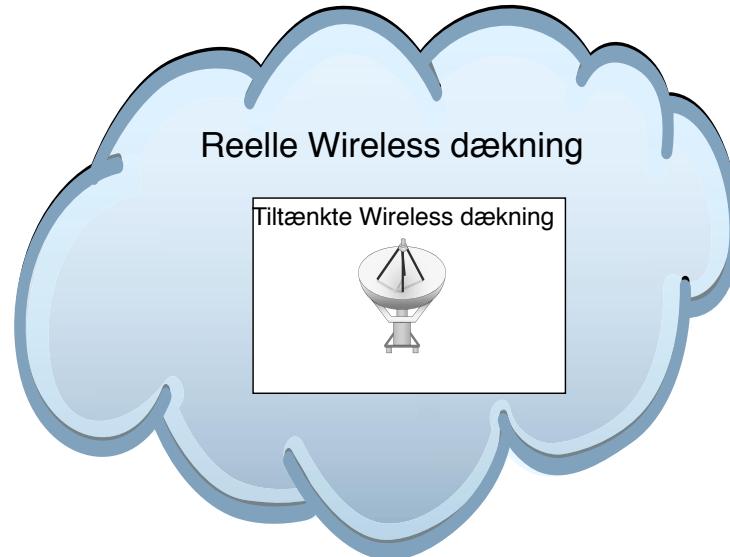


Sikkerhedsproblemer i de trådløse netværk er mange

- 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!

# Værktøjer

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

# Konsulentens udstyr wireless

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:

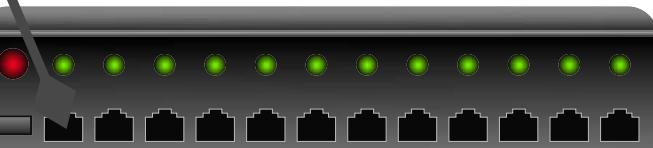
- *Real 802.11 security*
- Se oversigter over bøger og værktøjer igennem præsentationen:

Internetressourcer:

- Auditor Security Collection - 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>



## Wireless Access Point

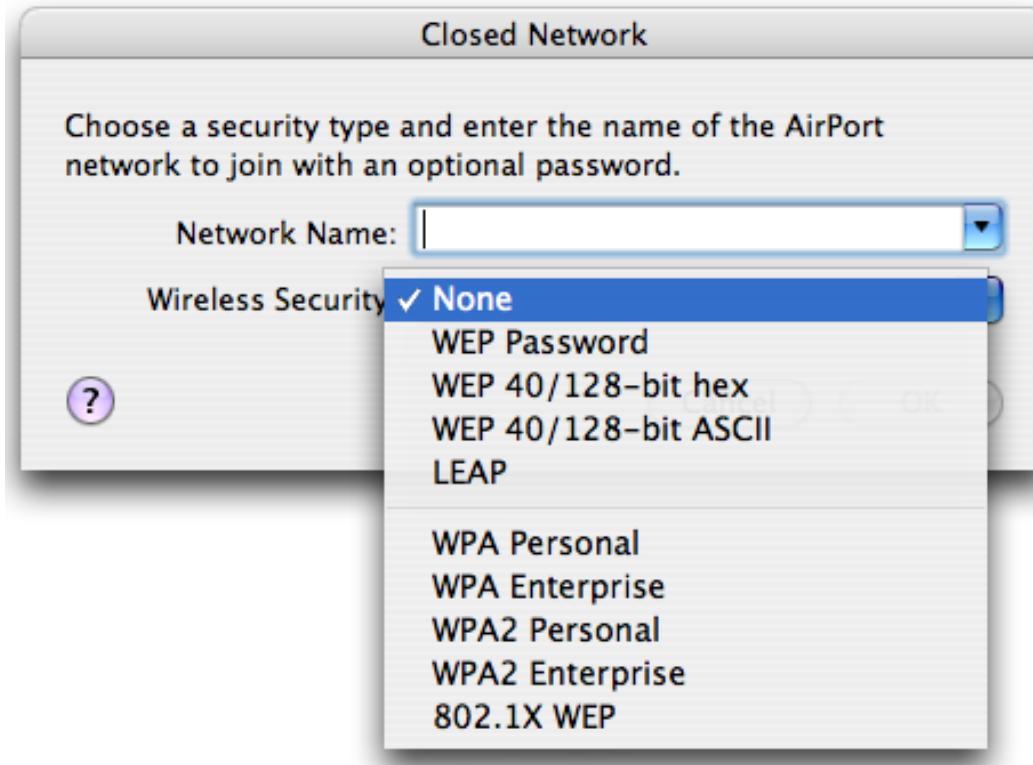


## netværket - typisk Ethernet

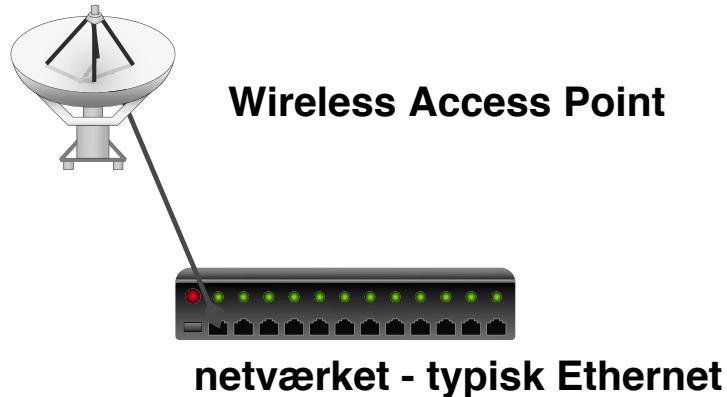
et access point - forbindes til netværket

# Basal konfiguration

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

# Forudsætninger

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

## SSID - netnavnet

Service Set Identifier (SSID) - netnavnet

32 ASCII tegn eller 64 hexadecimale cifre

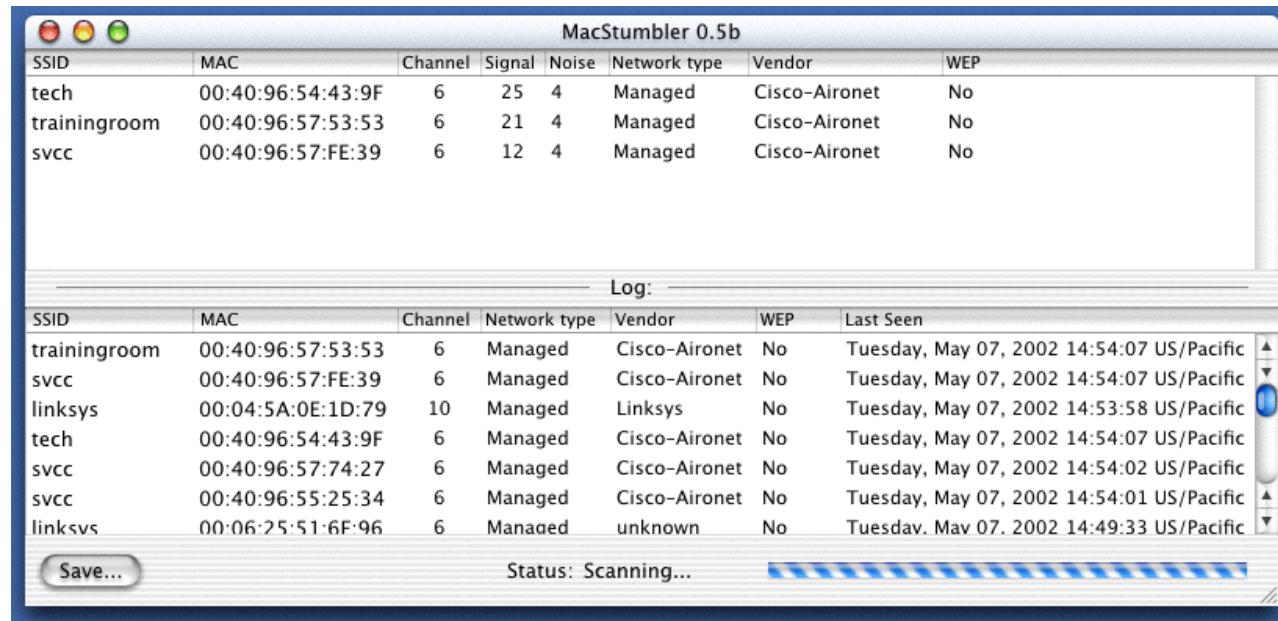
Udstyr leveres typisk med et standard netnavn

- 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

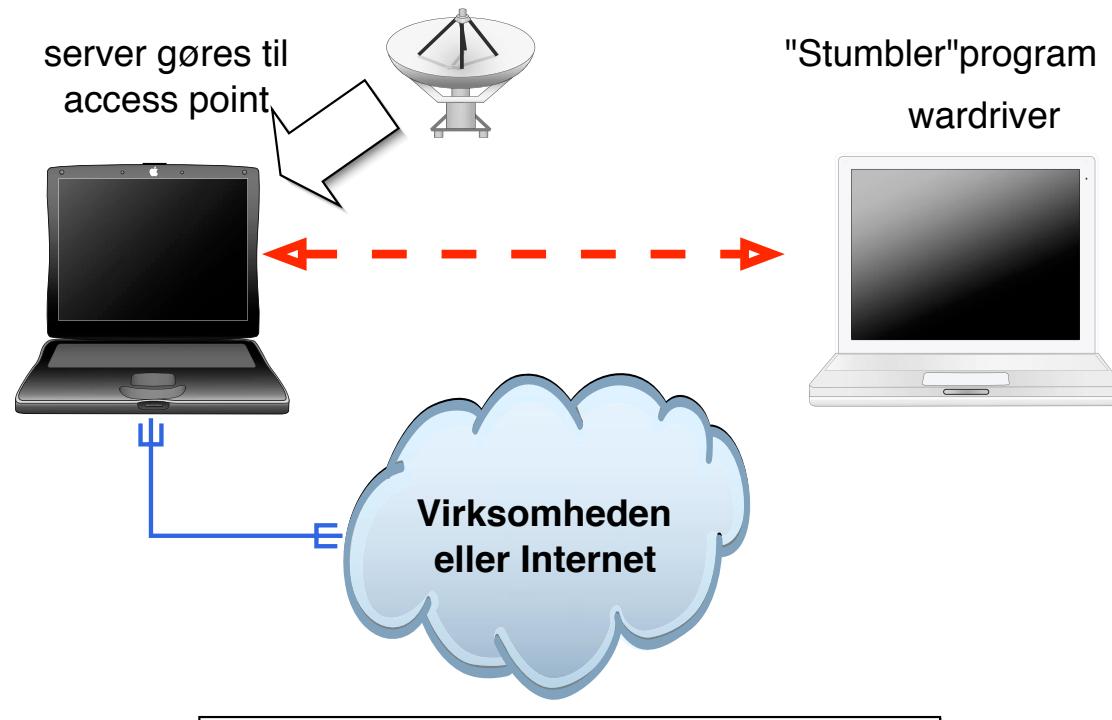
# Demo: wardriving med stumbler programmer



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*

## MAC filtrering

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 ...

# Resultater af wardriving

## 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

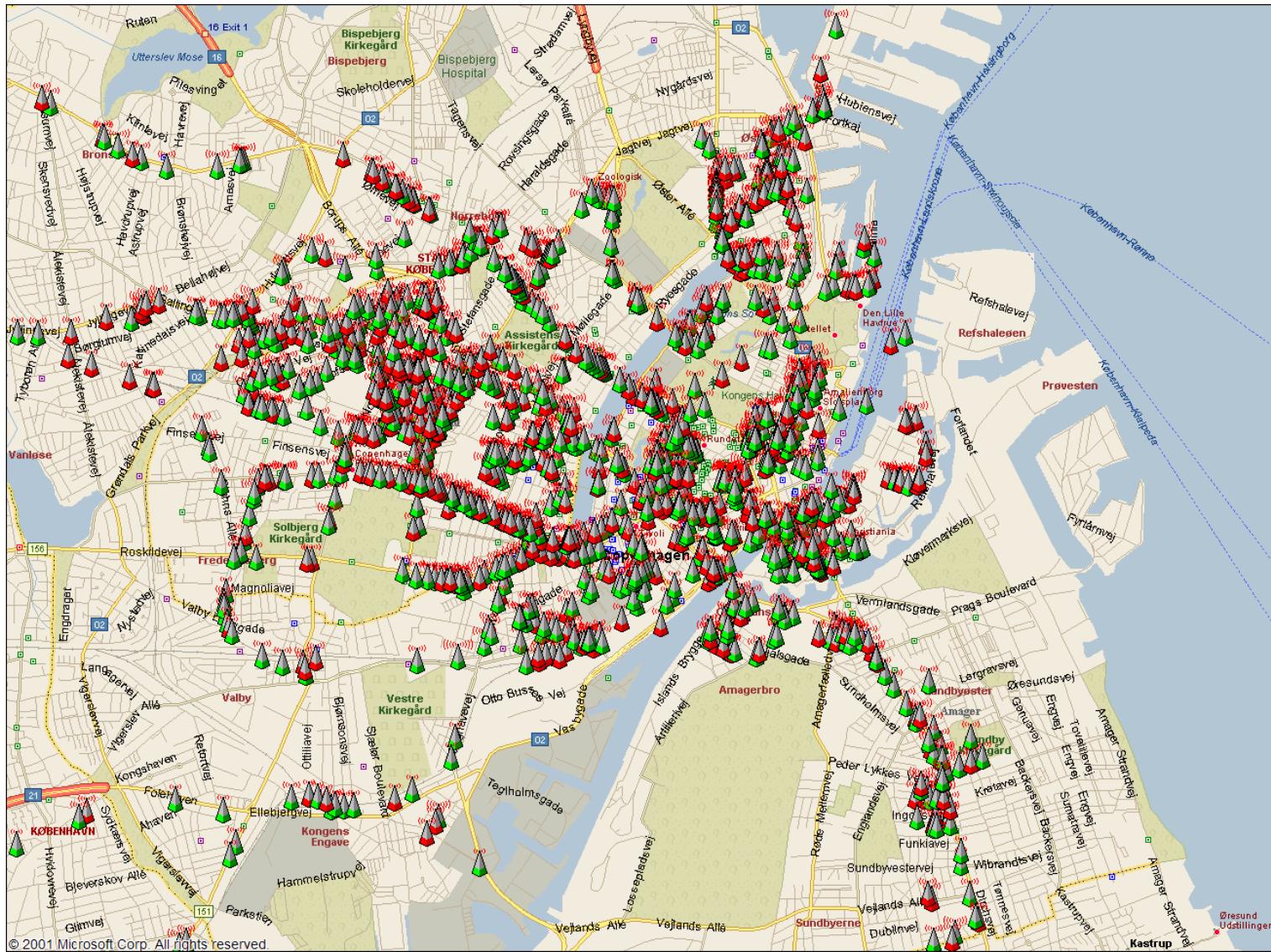
Man kan altså lytte med på et netværk med WEP, genbruge en anden maskines MAC adresse - og måske endda bryde WEP krypteringen.

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

# Storkøbenhavn



- Security



# Informationsindsamling

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

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

## De første fejl ved WEP

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/>

## major cryptographic errors

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 intergritetscheck 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**

# WEP cracking - airodump og aircrack



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. 500.000 er godt

Links:

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

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

# airodump afvikling

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 - WEP cracker



```
$ 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 ]**

## Hvor lang tid tager det?

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

## Erstatning for WEP- WPA

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

## Erstatninger for WEP

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)

# WPA eller WPA2?

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

# WPA Personal eller Enterprise

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

## WPA cracking

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

Desværre ikke!

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

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

# WPA cracking demo

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

# Tools man bør kende

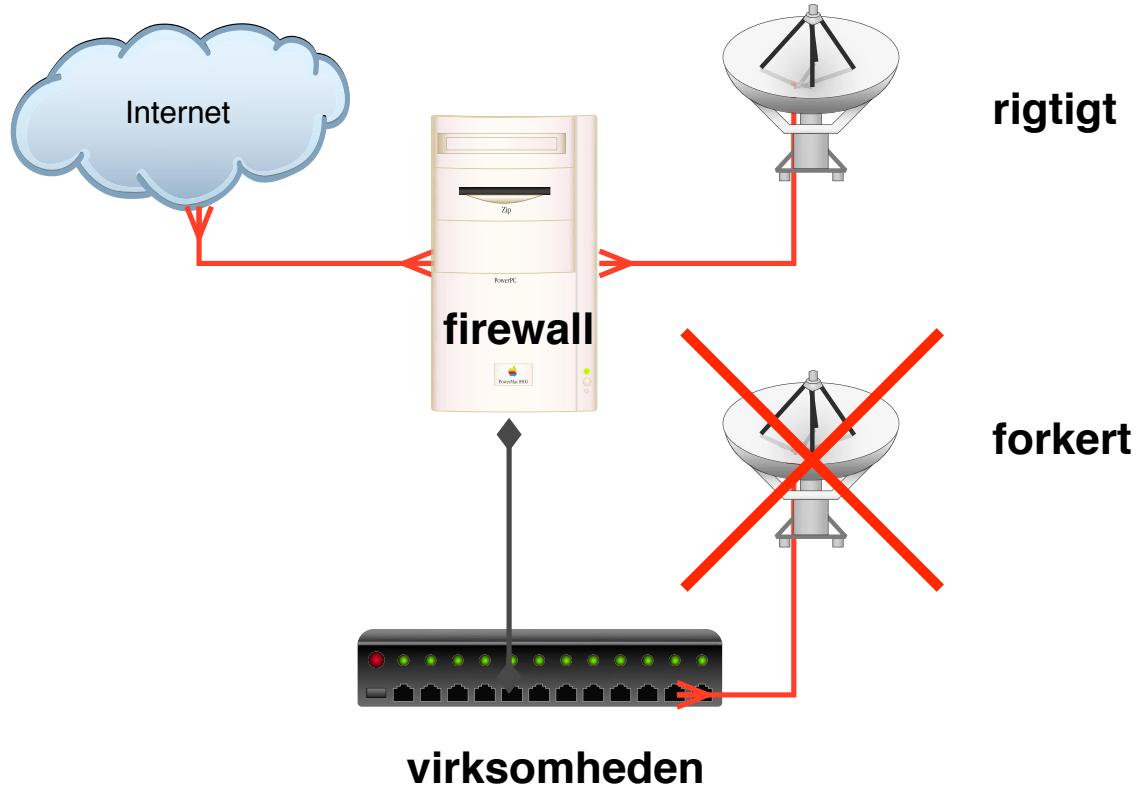


- **BSD Airtools** <http://www.dachb0den.com/projects/bsd-airtools.html>
- **Kismet** <http://www.kismetwireless.net/>
- **Airsnort** <http://airsnort.shmoo.com/> læs pakkerne med WEP kryptering
- **wepcrack** <http://wepcrack.sourceforge.net/> - knæk krypteringen i WEP
- **Airsnarf** <http://airsnarf.shmoo.com/> - lav dit eget AP parallelt med det rigtige og snif hemmeligheder
- **Wireless Scanner** <http://www.iss.net/> - kommersielt
- Dette er et lille uddrag af programmer  
Se også <http://packetstormsecurity.org/wireless/>

Så går man igang med de almindelige værktøjer

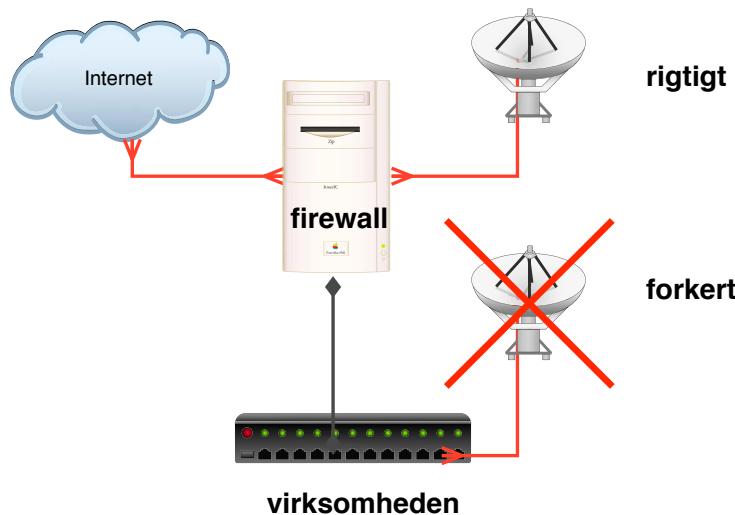
Fyodor Top 100 Network Security Tools <http://www.sectools.org>

Forsvaret er som altid - flere lag af sikkerhed!



Sådan bør et access point forbides 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

# firewalls

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

# firewall regelsæt eksempel

```
# 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

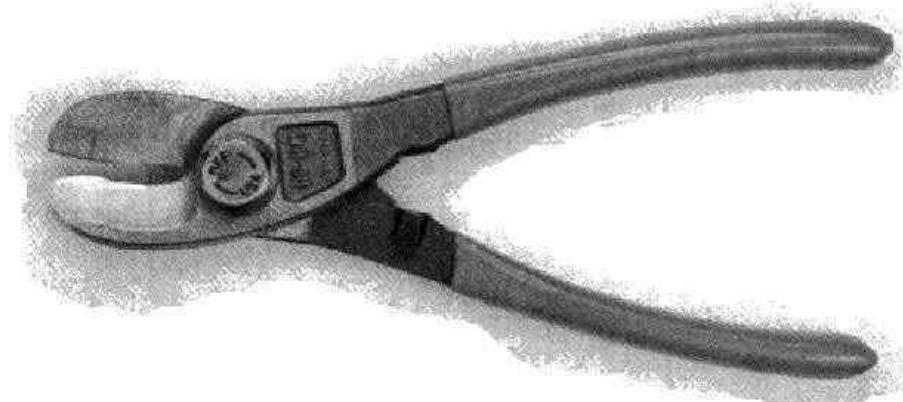
# things not used
spoofed=" 127.0.0.0/8, 172.16.0.0/12, 10.0.0.0/16, 255.255.255.255/32 "

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?

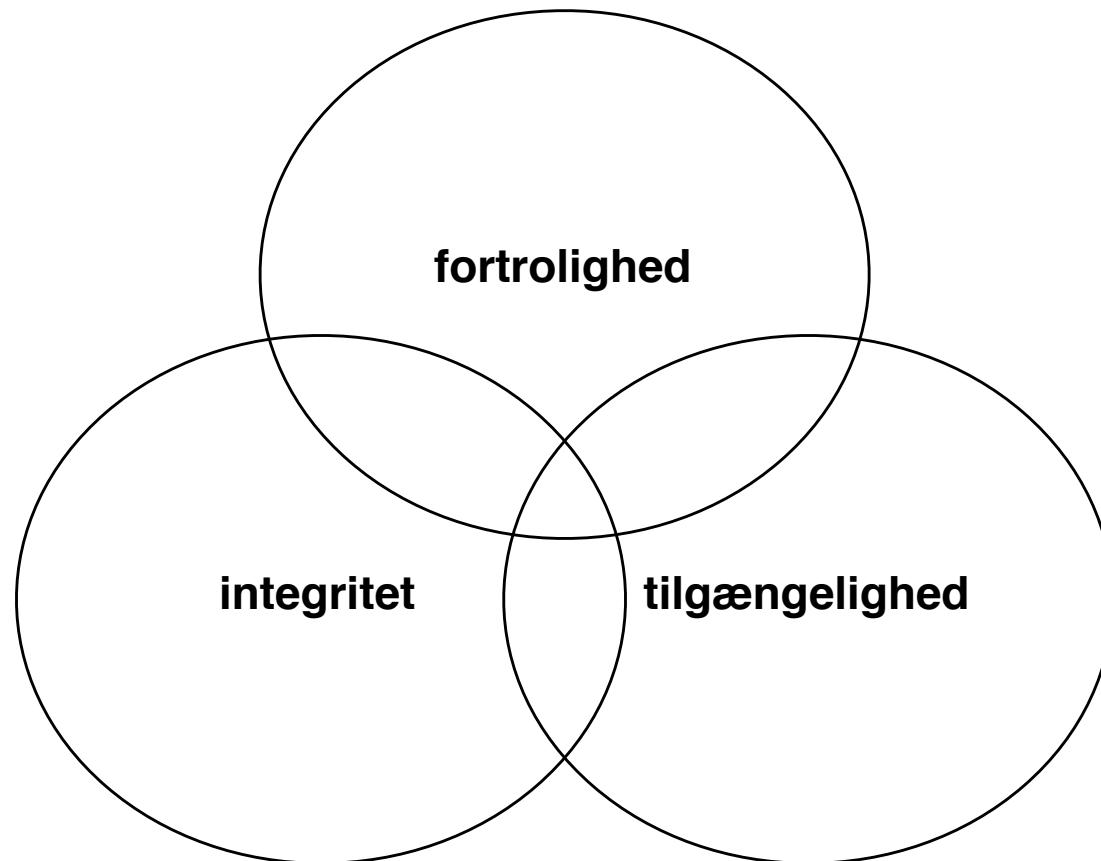
Hvad er forudsætningen for at en firewall virker?

At der er konfigureret et sæt fornuftige regler!

Hvor kommer reglerne fra? Sikkerhedspolitikken!

Kilde: Billedet er fra Marcus Ranum The ULTIMATELY Secure Firewall

Husk altid de fundamentale principper indenfor sikkerhed



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

## Tip ACK prioritering

Daniel Hartemeier som oprindeligt skrev PF har en god hjemmeside

<http://www.benzedrine.cx/dhartmei.html>

Et eksempel er prioritering af ACK pakker, som blot sender acknowledgement - men ellers er tomme

Ved at prioritere disse kan man både downloade og uploade med fuld hastighed

# PF konfigurationen

```
ext_if="kue0"

altq on $ext_if priq bandwidth 100Kb queue { q_pri, q_def }
queue q_pri priority 7
queue q_def priority 1 priq(default)

pass out on $ext_if proto tcp from $ext_if to any flags S/SA
keep state queue (q_def, q_pri)

pass in  on $ext_if proto tcp from any to $ext_if flags S/SA
keep state queue (q_def, q_pri)
```

# Relayd

```
www1="10.0.0.1"
www2="10.0.0.2"
table <webhosts> {
    $www1
    $www2
}
```

relayd - OpenBSD 4.1 og fremefter, tidlige hostated

**DESCRIPTION** relayd is a daemon to relay and dynamically redirect incoming connections to a target host. Its main purposes are to run as a load-balancer, application layer gateway, or transparent proxy. The daemon is able to monitor groups of hosts for availability, which is determined by checking for a specific service common to a host group. When availability is confirmed, Layer 3 and/or layer 7 forwarding services are set up by relayd.

## relayd eksempel

```
table <service> { 192.168.1.1, 192.168.1.2, 192.168.2.3 }
    table <backup> disable { 10.1.5.1 retry 2 }

    redirect "www" {
        listen on www.example.com port 80
        forward to <service> check http "/" code 200
        forward to <backup> check http "/" code 200
    }
```

Den kan checke med HTTP eller ICMP  
relayd kan forwarde med HTTP/HTTPS

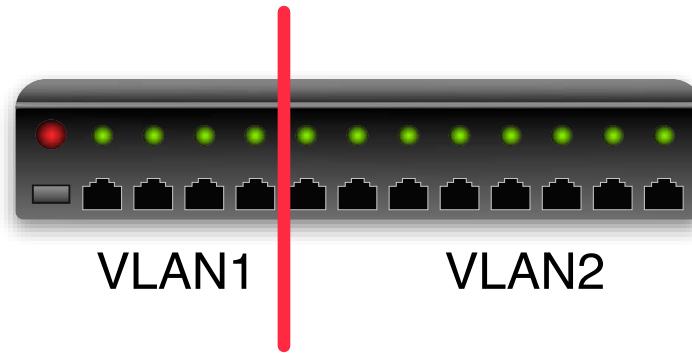
OpenBSD integrerer en masse daemoner og services

DHCPD er eksempelvis integreret så man kunne blokere for alle, undtagen dem som har fået en adresse fra DHCPD

Login authpf ved ssh login tilføjes regler for en bruger

Mange andre steder, for mange til at jeg kan huske dem :-)

## Portbased VLAN



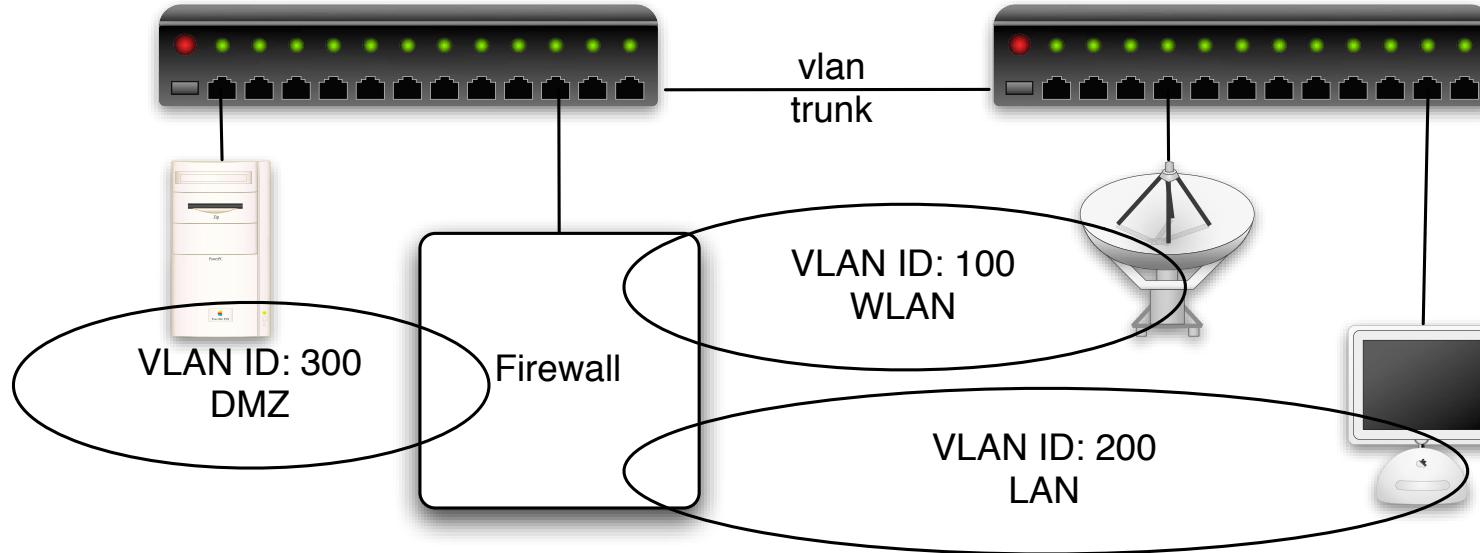
Nogle switcher tillader at man opdeler portene

Denne opdeling kaldes VLAN og portbaseret er det mest simple

Port 1-4 er et LAN

De resterende er et andet LAN

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2



Nogle switcher tillader at man opdeler portene, men tillige benytter 802.1q

Med 802.1q tillades VLAN tagging på Ethernet niveau

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

VLAN trunking giver mulighed for at dele VLANs ud på flere switches

Der findes administrationsværktøjer der letter dette arbejde: OpenNAC FreeNAC, Cisco VMPS

# OpenBSD VLAN

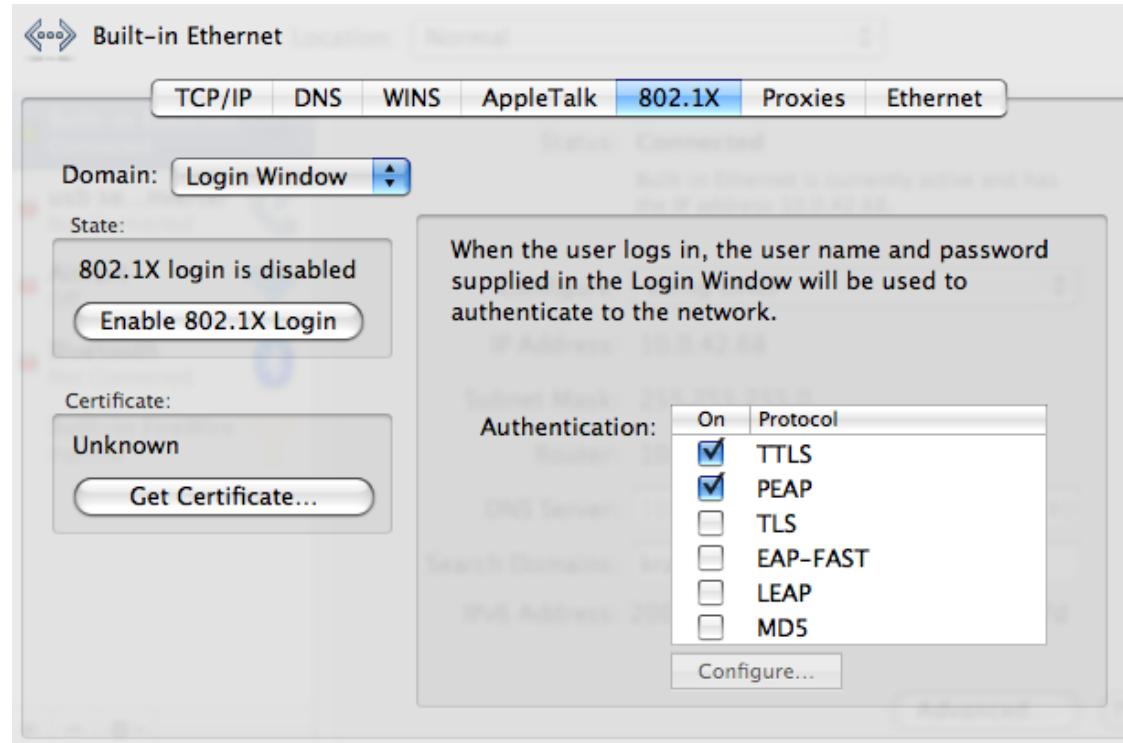
Normal konfiguration af fast IP på en OpenBSD med hostname.if fil:

```
hlk@luffe:hlk$ cat /etc/hostname.vr0
inet 10.0.45.2 255.255.255.0 NONE
inet6 2001:7b8:3e4:0045::2
```

VLAN konfiguration af fast IP på en OpenBSD med hostname.if fil:

```
hlk@luffe:hlk$ cat /etc/hostname.vlan2
inet 10.0.72.2 255.255.255.0 NONE vlan 2 vlandev vr0
inet6 2001:7b8:3e4:0072::2
```

# IEEE 802.1x Port Based Network Access Control



Nogle switcher tillader at man benytter 802.1x

Denne protokol sikrer at man valideres før der gives adgang til porten

Når systemet skal have adgang til porten afleveres brugernavn og kodeord/certifikat

Denne protokol indgår også i WPA Enterprise

## 802.1x og andre teknologier

802.1x i forhold til MAC filtrering giver væsentlige fordele

MAC filtrering kan spoofes, hvor 802.1x kræver det rigtige kodeord

Typisk benyttes RADIUS og 802.1x integrerer således mod både LDAP og Active Directory

# IPv6 firewalls

```
# remember to allow icmpv6 for neighbour discovery
pass in inet6 proto ipv6-icmp all icmp6-type neighbradv keep state
pass in inet6 proto ipv6-icmp all icmp6-type routeradv keep state
pass in inet6 all
pass out inet6 all
pass in net6 proto tcp from any to 2001:7b8:3e4:72::20 port = www flags S/SA ke
```

IPv6 minder meget om IPv4, men ARP er udskiftet med NDP

Mit råd er at bruge aliases så een regel i PF.conf rammer flere hosts

# IPv6 neighbor discovery protocol (NDP)

OSI	IPv4	IPv6
Network	IP / ICMP	IPv6 / ICMPv6
Link	ARP	
Physical	Physical	Physical

ARP er væk

NDP erstatter og udvider ARP, Sammenlign arp -an med ndp -an

Til dels erstatter ICMPv6 således DHCP i IPv6, DHCPv6 findes dog

**NB: bemærk at dette har stor betydning for firewallregler!**

# ARP vs NDP



```
h1k@bigfoot:basic-ipv6-new$ arp -an
? (10.0.42.1) at 0:0:24:c8:b2:4c on en1 [ethernet]
? (10.0.42.2) at 0:c0:b7:6c:19:b on en1 [ethernet]
h1k@bigfoot:basic-ipv6-new$ ndp -an
Neighbor                               Linklayer Address  Netif Expire   St Flgs Prbs
::1                                     (incomplete)        lo0 permanent R
2001:16d8:fffd2:cf0f:21c:b3ff:fec4:e1b6 0:1c:b3:c4:e1:b6 en1 permanent R
fe80::1%lo0                            (incomplete)        lo0 permanent R
fe80::200:24ff:fec8:b24c%en1  0:0:24:c8:b2:4c       en1 8h54m51s S R
fe80::21c:b3ff:fec4:e1b6%en1  0:1c:b3:c4:e1:b6        en1 permanent R
```

# IPv4 + IPv6 serviceeksempel

Først tilføjes aliases i /etc/hosts (kan være DNS) og simpel regel til PF konfigurationsfilen

/etc/hosts:

```
2001:7b8:3e4:72::20    webserver
```

```
10.0.72.20  webserver
```

/etc/pf.conf:

```
pass in on $ext_if proto tcp to webserver port http
```

giver så endeligt reglerne:

```
pass in on vr3 inet6 proto tcp from any to 2001:7b8:3e4:72::20 port = www flags S/SA keep state
pass in on vr3 inet proto tcp from any to 10.0.72.20 port = www flags S/SA keep state
```

# IPv4 + IPv6 serviceeksempel, med tables

Istedet for DNS aliases og /etc/hosts kan tilføjes table og simpel regel til PF konfigurationsfilen

```
table <webservers> 2001:7b8:3e4:72::20 10.0.72.20  
...  
pass in on $ext_if proto tcp to <webserver> port http
```

giver så endeligt reglen:

```
pass in on vr3 proto tcp from any to <webserver> port = www flags S/SA keep state
```

# Opsummering afslutning

Husk følgende:

- Husk: IT-sikkerhed er ikke kun netværkssikkerhed!
- Sikkerhed kommer fra langsigtede intiativer  
**Vi håber I kan genkende de problemer vi har talt om, og finde information om nye problemer i netværk som bliver kendt eksempelvis nye metoder til scanning eller omgåelse af firewalls**
- 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**

# Anbefalinger generelt

Security

.net

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

## Anbefalinger til jer

### 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 ca. 100 nye sårbarheder i produkter - software/hardware**

## Følg med! - mange kilder

**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>

# Spørgsmål?



Henrik Lund Kramshøj  
hlk@security6.net

<http://www.security6.net>

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

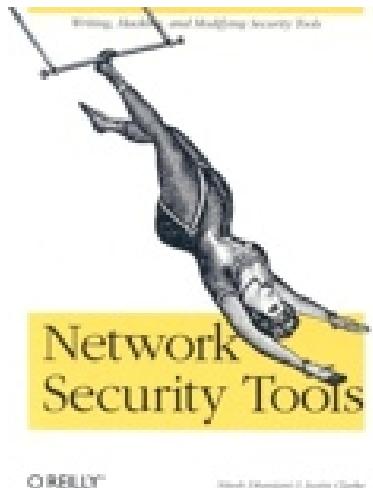
# Reklamer: kursusafholdelse

Følgende kurser afholdes med mig som underviser

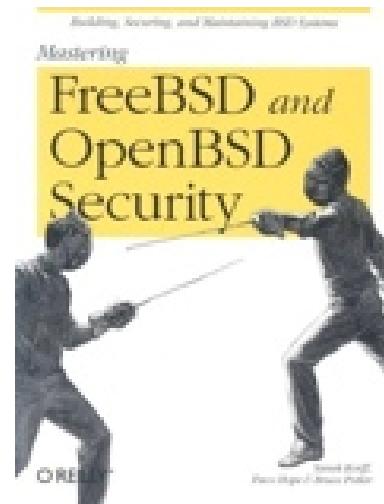
- IPv6 workshop - 1 dag  
Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop - 1-2 dage  
En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk, samt integration med hjemmepc og virksomhedsnetværk.
- Hacker workshop 2 dage  
Workshop med detaljeret gennemgang af hackermetoderne angreb over netværk, exploitprogrammer, portscanning, Nessus 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>

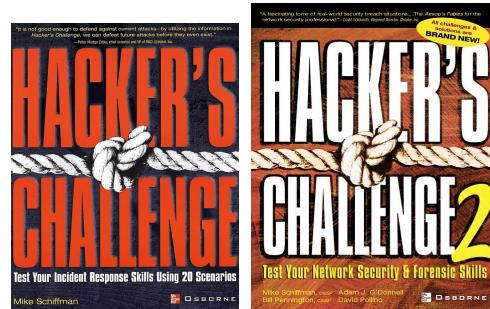
# Network Security Tools



*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



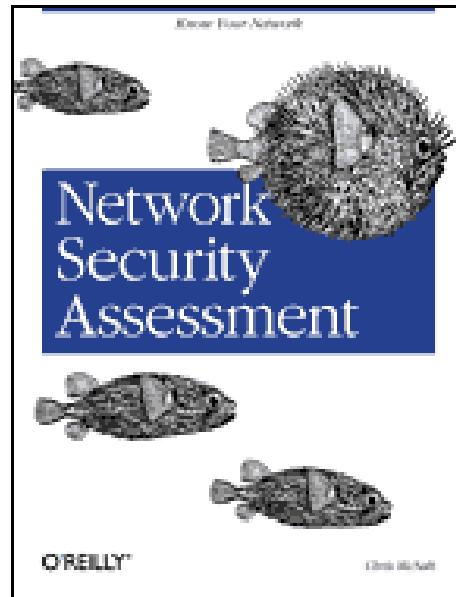
*Hacker's Challenge : Test Your Incident Response Skills Using 20 Scenarios* af Mike Schiffman McGraw-Hill Osborne Media; (October 18, 2001) ISBN: 0072193840

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

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

Hackers challenge nr 3 udkommer i 2006

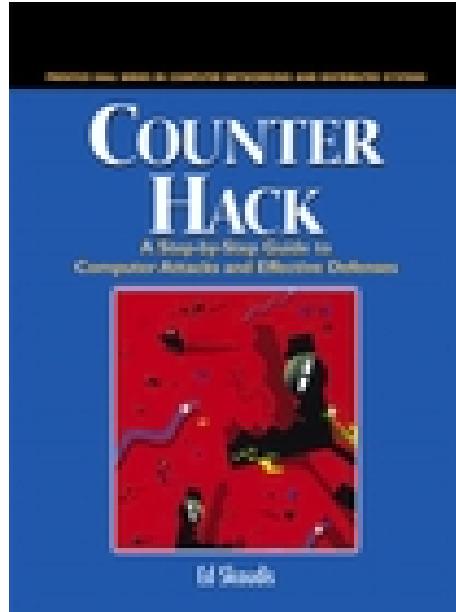
# Network Security Assessment



*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, 1st edition July 2001

Bogen er anbefalelsesværdig og er kommet i anden udgave

Minder mig om et universitetskursus i opbygningen

# Hackerværktøjer

- nmap - <http://www.insecure.org> portscanner
- Nessus - <http://www.nessus.org> automatiseret testværktøj
- l0phtcrack - <http://www.atstake.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

# Referencer

## 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

# Packet factory projects



- 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<sub>SM</sub></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



Security Essentials - basal sikkerhed

Krav om en *Practical assignment* - mindst 8 sider, 15 sider i gennemsnit  
multiple choice eksamen

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

Reading room: <http://www.sans.org/rr/>

Der findes en god oversigt i filen *GIAC Certification: Objectives and Curriculum*  
<http://www.giac.org/overview/brief.pdf>