

Welcome to

UNF hacking - black/white hat

Henrik Lund Kramshøj
hlk@solido.net

<http://www.solidonetworks.com>



Don't Panic!

Skabe en 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

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

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

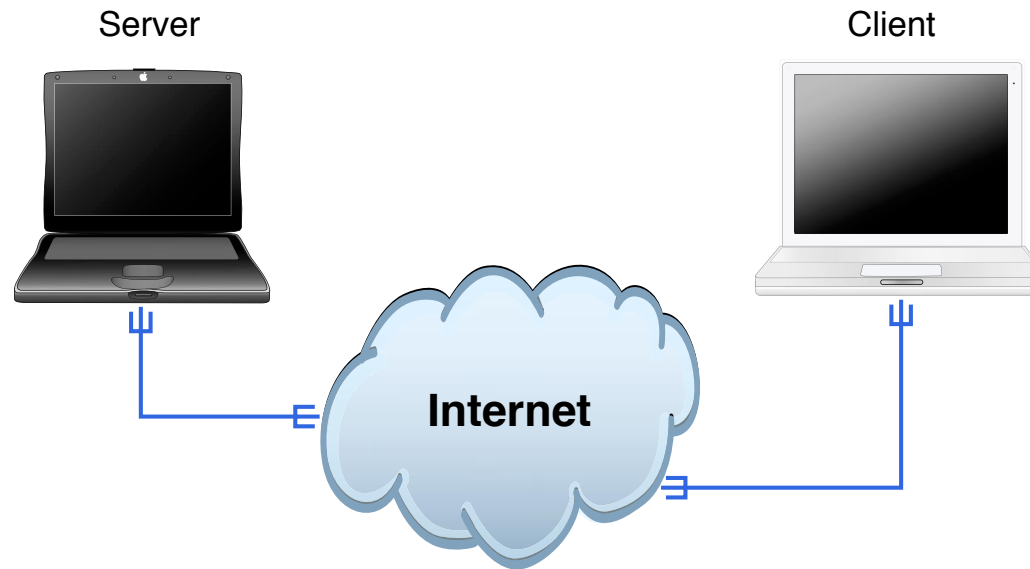
Kilde: Peter Makholm, <http://hacking.dk>

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

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!




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



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

```
80/tcp    open      http
81/tcp    open      hosts2.nc
10.0.0.1  [nobile]
11 # nmap -v -ss -O 10.2.2.2
11
13 Starting nmap V. 2.540E1A25
13 Insufficient responses for TCP sequencing (3). OS detection
13 accurate
14 Interesting ports on 10.2.2.2:
44 (The 1539 ports scanned but not shown below are in state: cl
51 Port      State      Service
51 22/tcp    open      ssh
58
68 No exact OS matches for host
68
24 Nmap run completed -- 1 IP address (1 host up) scanned
50 # sshnuke 10.2.2.2 -rootpw-"210N0101"
Connecting to 10.2.2.2:ssh ... successful.
Re Attempting to exploit SSHv1 CRC32 ... successful.
IP Resetting root password to "210N0101".
System open: Access Level (9)
H # ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```

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

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



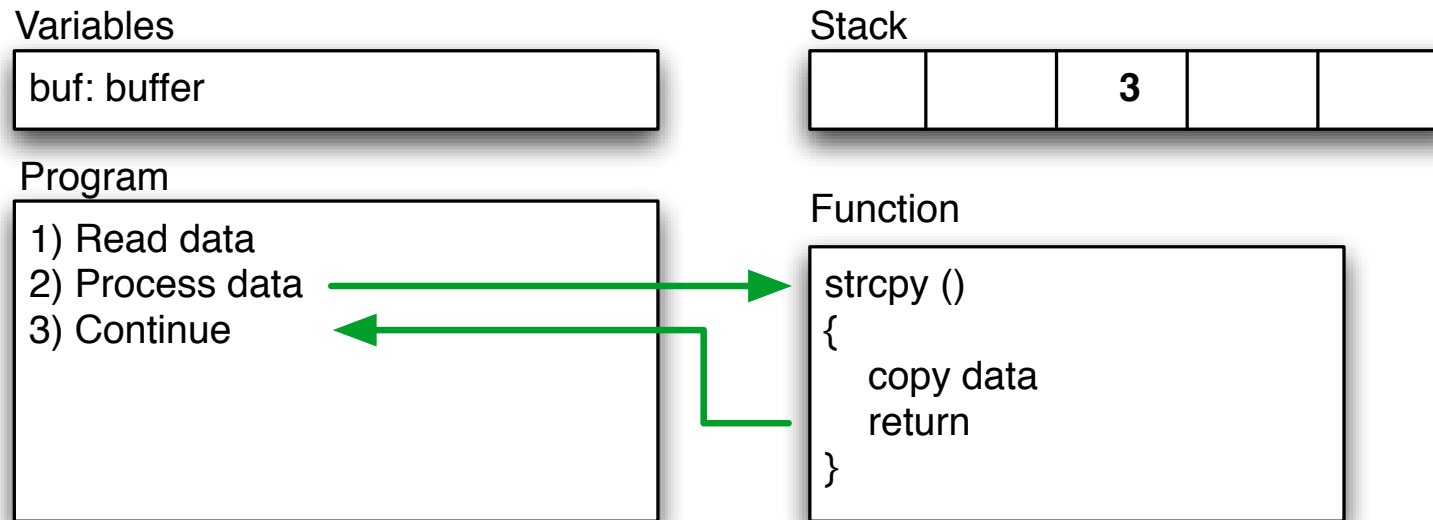
Hacking ligner indimellem magi



Hacking kræver blot lidt ninja-træning

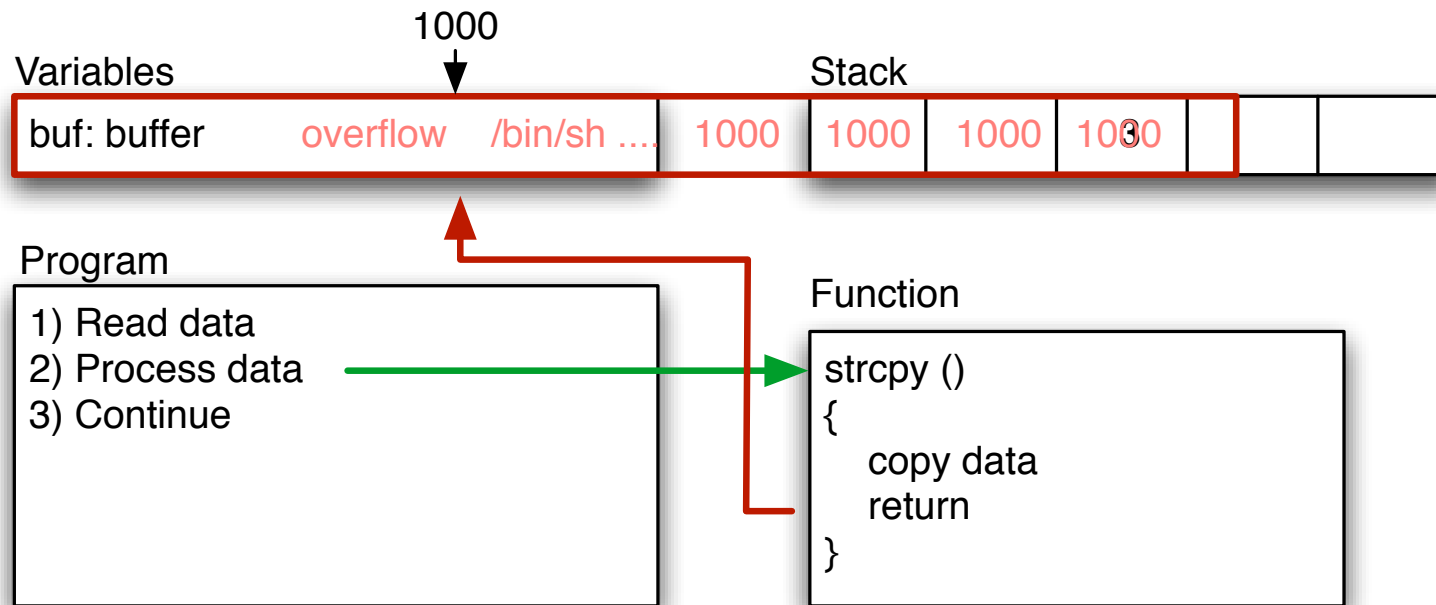
Et buffer overflow er det der sker når man skriver flere data end der er afsat plads til i en buffer, et dataområde. Typisk vil programmet gå ned, men i visse tilfælde kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

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



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

Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

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

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

Demo exploit in Perl

Hvordan finder man buffer overflow, og andre fejl

Black box testing

Closed source reverse engineering

White box testing

Open source betyder man kan læse og analysere koden

Source code review - automatisk eller manuelt

Fejl kan findes ved at prøve sig frem - fuzzing

Exploits virker typisk mod specifikke versioner af software

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 ...	

Alle bruger nogenlunde de samme værktøjer, måske forskellige mærker

- Portscanner - Fyodor Nmap
- Generel sårbarhedsscanner - OpenVAS/Nessus
- Speciel web sårbarhedsscanner - eksempelvis Nikto
- Speciel database sårbarhedsscanner
- Specielle scannere - wifi Aircrack-ng, m.fl.
- ...
- Rapportværktøj - manuel eller automatisk, helst så automatiseret som muligt
- Meget ofte er sikkerhedstest automatiseret på de indledende skridt og manuel derefter

og scripting, powershell, unix shell, perl, python, ruby, ...

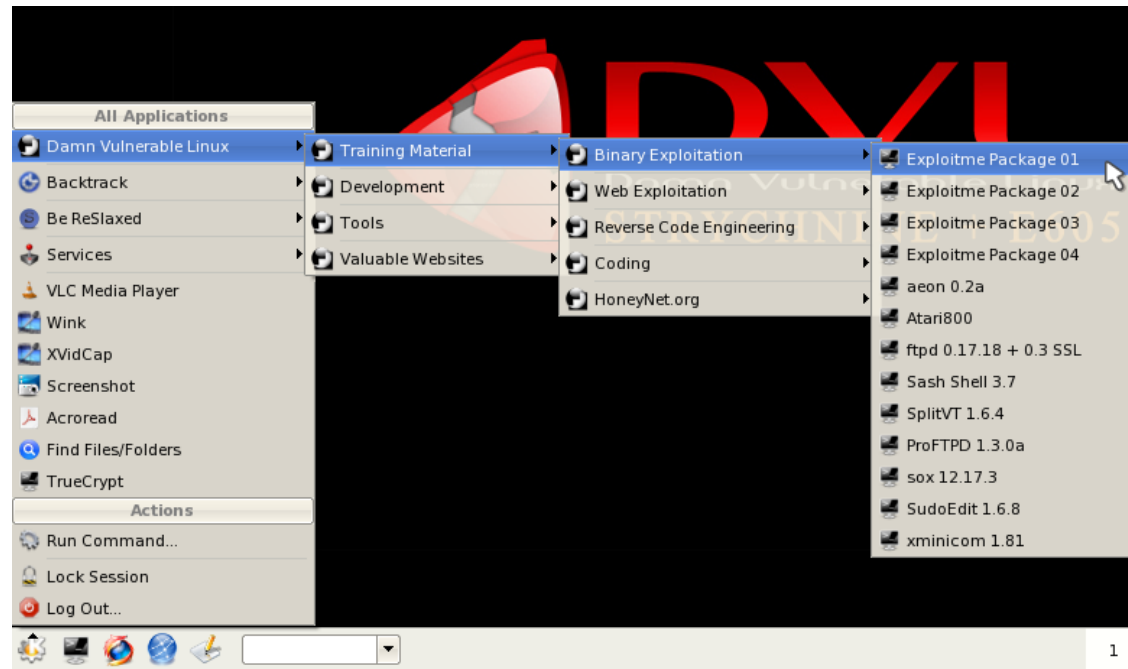


Wireshark - <http://www.wireshark.org> avanceret netværkssniffer
bruger vi til at sniffe, vi bruger Wireshark til primære demo, nævner Ettercap osv.

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

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

Damn Vulnerable Linux boot CD'er



Damn Vulnerable Linux <http://www.damnulnerablelinux.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.

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>

OSI Reference
Model

Application
Presentation
Session
Transport
Network
Link
Physical

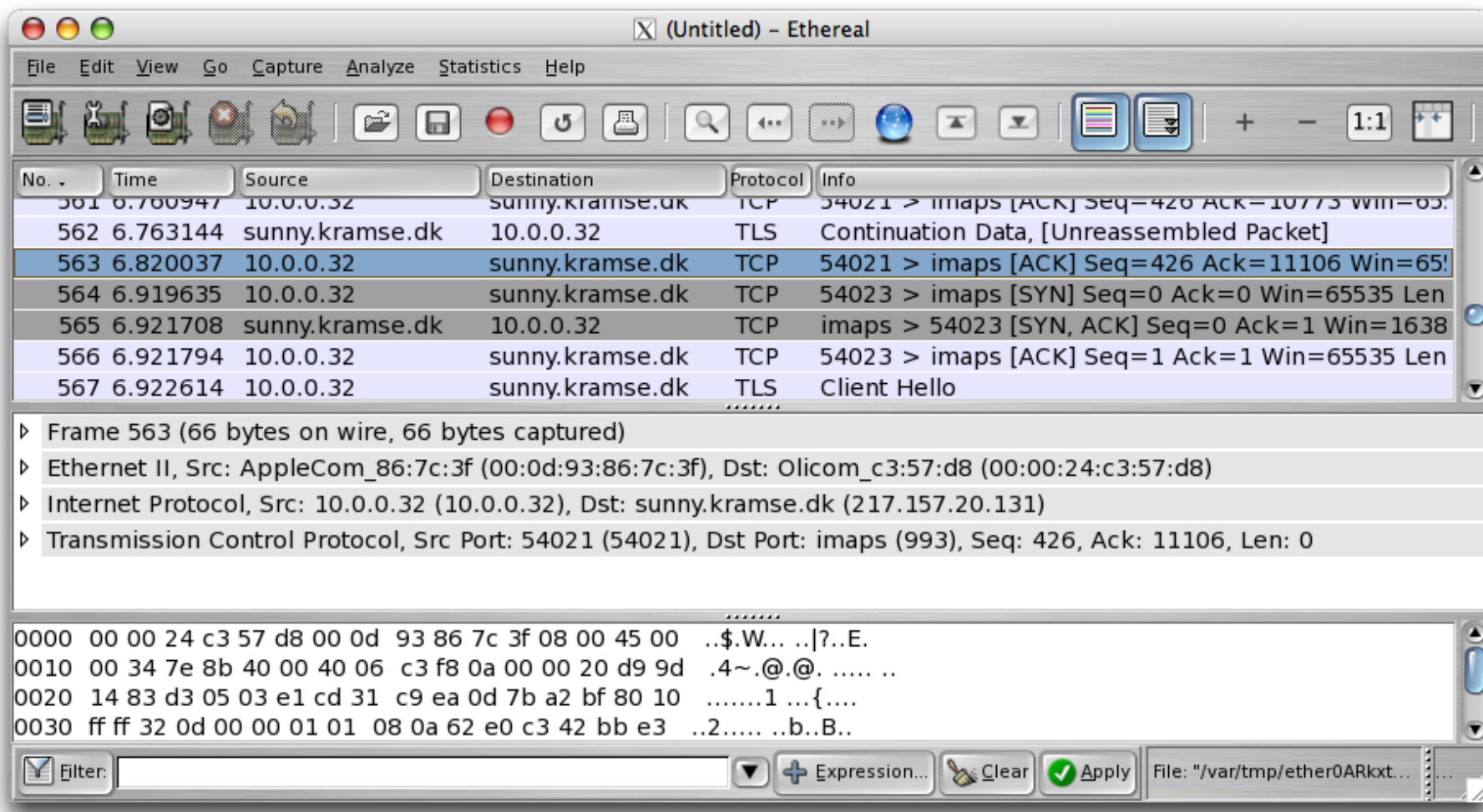
Internet protocol suite

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



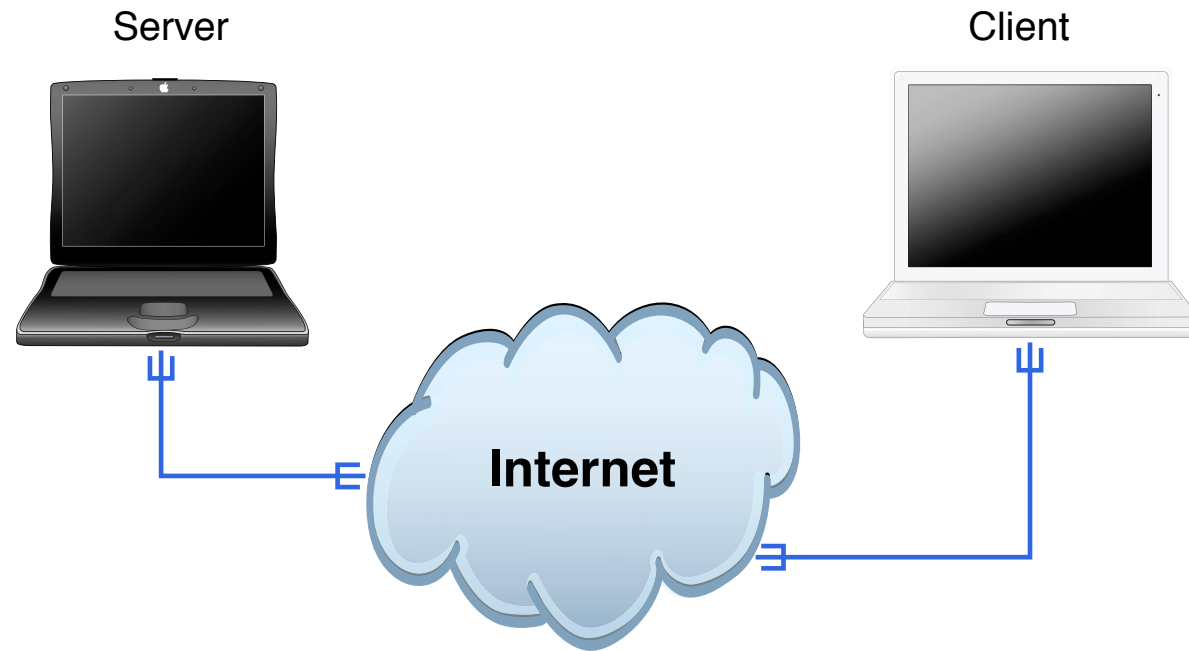
The screenshot shows the Wireshark website homepage. At the top is a blue banner with the 'WIRESHARK' logo and a shark illustration. Below the banner is a navigation bar with links: HOME, ABOUT, WHAT'S NEW, DOWNLOAD, and FAQ. The main content area is divided into several sections. On the left is a sidebar with links under categories: 'Get It' (Download), 'Get Help' (FAQs, Documentation, Mailing Lists, Wiki, Bug tracker), 'Develop' (Developer Info), and 'Products' (AirPcap, Network Toolkit, OEM WinPcap). The central part features an article titled 'Sniffing Problems A Mile Away' with text about the name change from Ethernet to Wireshark and a screenshot of the Wireshark interface. Below this is a 'News' section titled 'Wireshark 0.99.3 Released' dated Aug 23, 2006, mentioning security fixes. On the right side, there is a 'Download Now' box showing version 0.99.3, and a Q&A section with a question about capturing 802.11 traffic and an answer, with the AirPcap logo at the bottom.

`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/>

tracert programmet virker ved hjælp af TTL

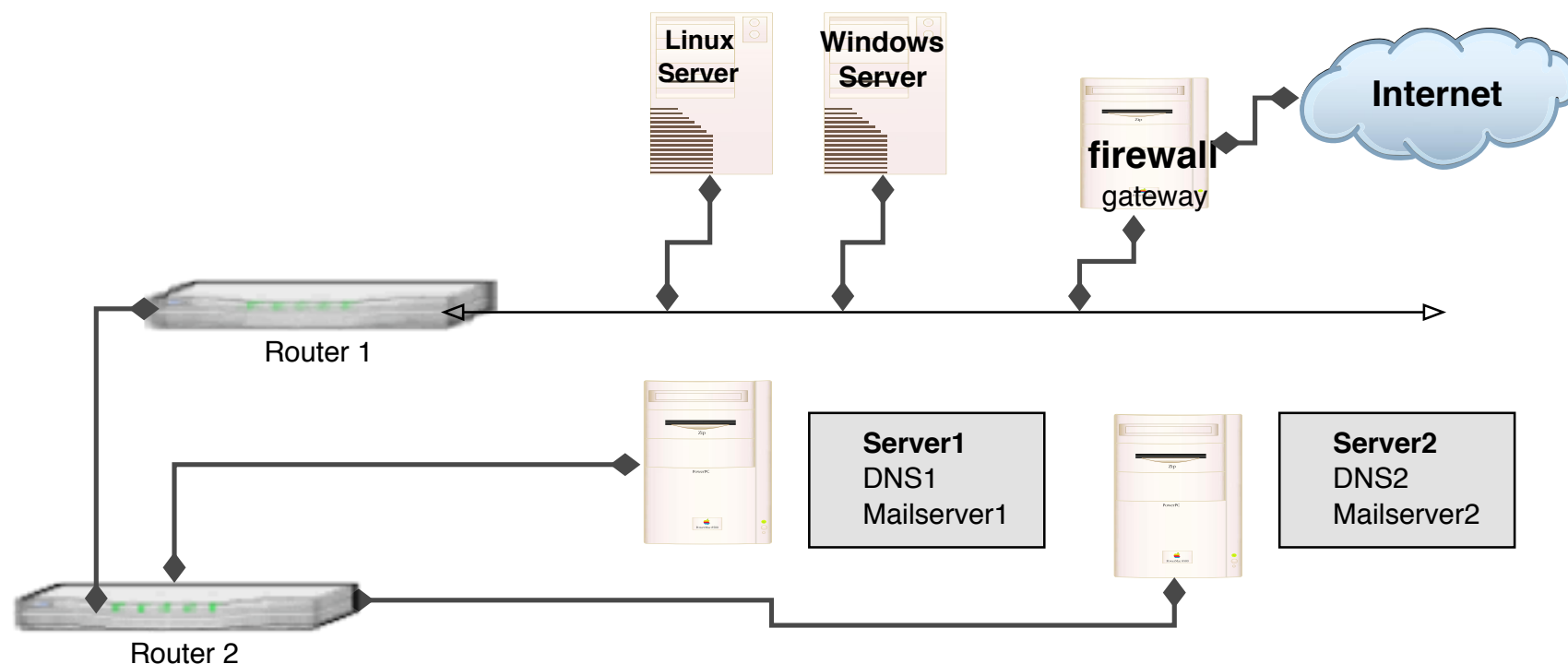
levetiden for en pakke tælles ned i hver router på vejen og ved at sætte denne lavt opnår man at pakken *timer ud* - besked fra hver router på vejen

default er UDP pakker, men på UNIX systemer er der ofte mulighed for at bruge ICMP

```
$ tracert 91.102.91.18
```

```
tracert 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
```



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 netværkspakker og portscanne

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`

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	zfront01.solido.net.
	IN	MX	20	zfront02.solido.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;

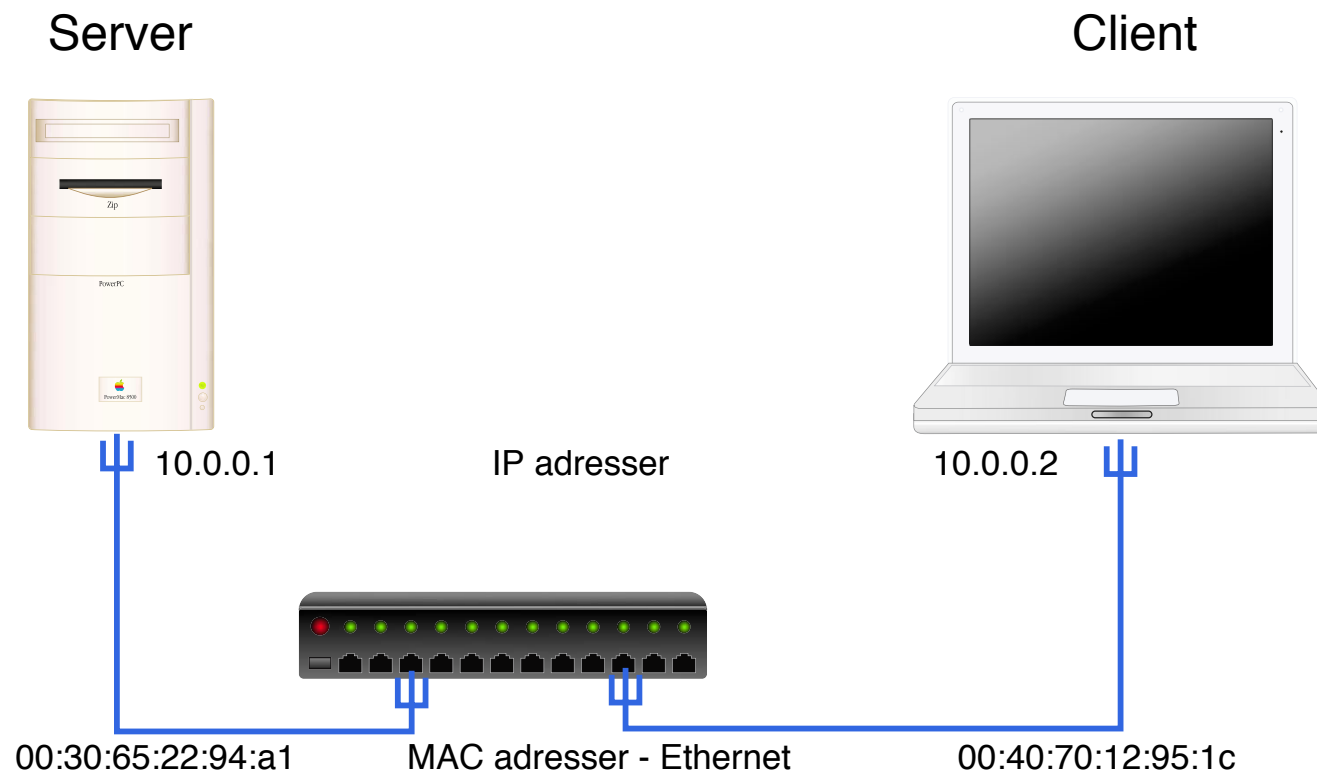
my $resolver = Net::DNS::Resolver->new;
$resolver->nameservers($ARGV[0]);

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

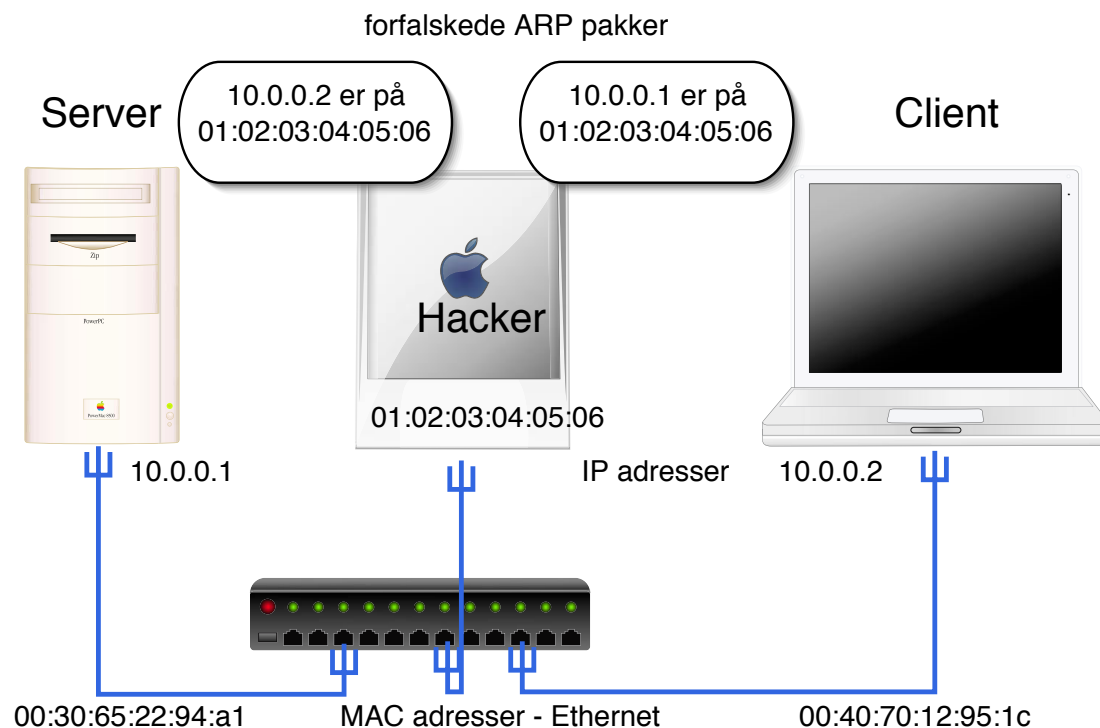
IP ICMP request/reply:

- 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

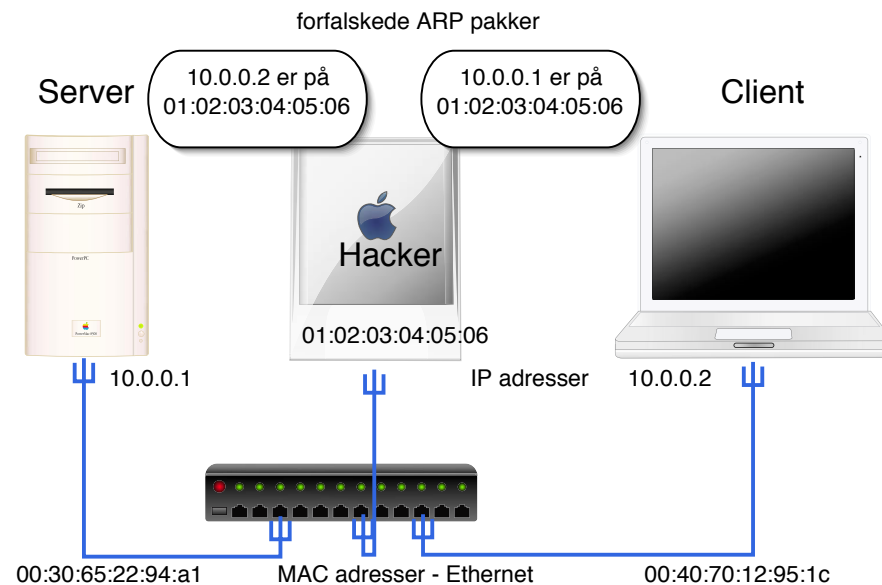
inkluderer **arpspoof**

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?

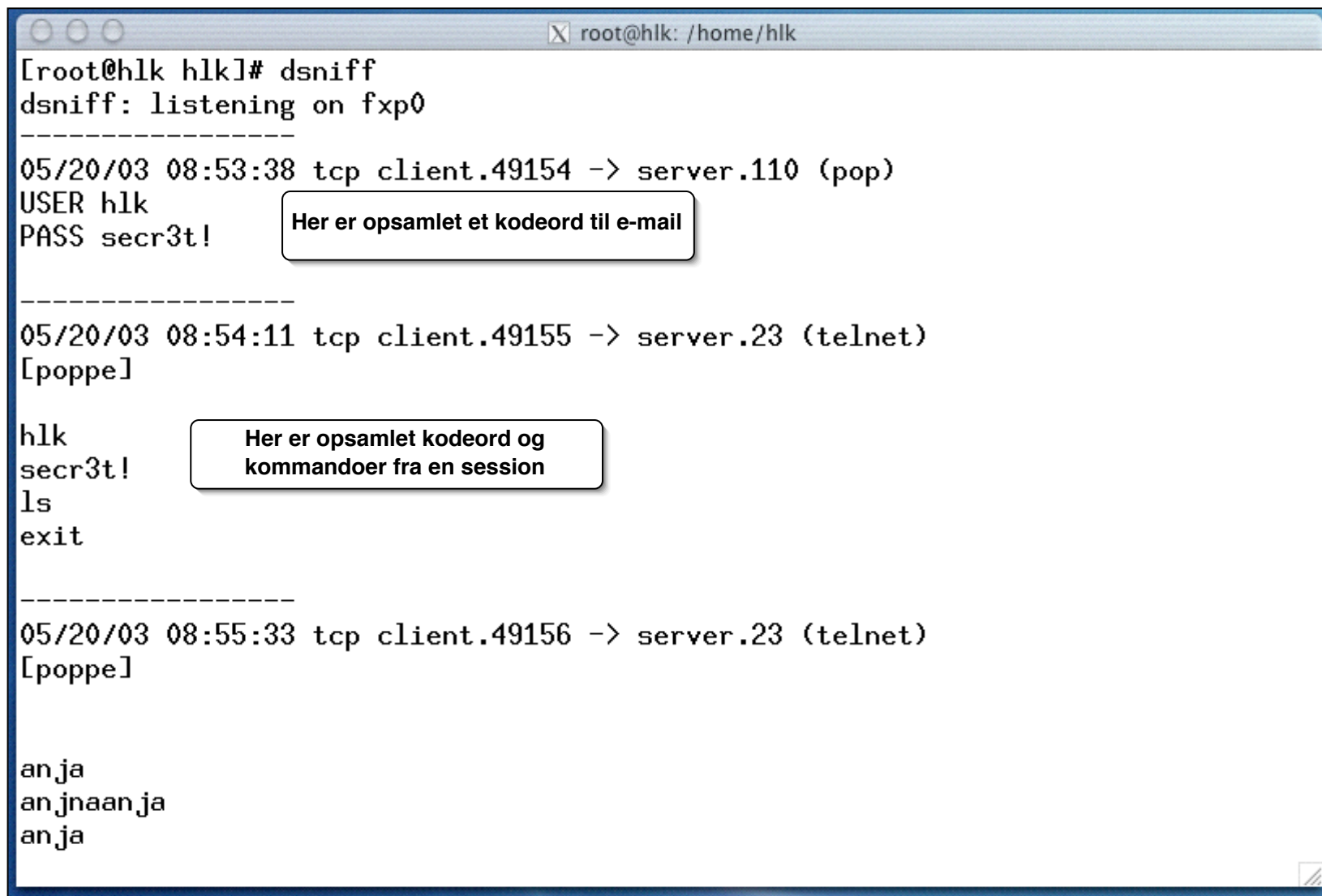
låse MAC adresser til porte på switche

låse MAC adresser til bestemte IP adresser

Efterfølgende administration!

arpwatch er et godt bud - overvåger ARP

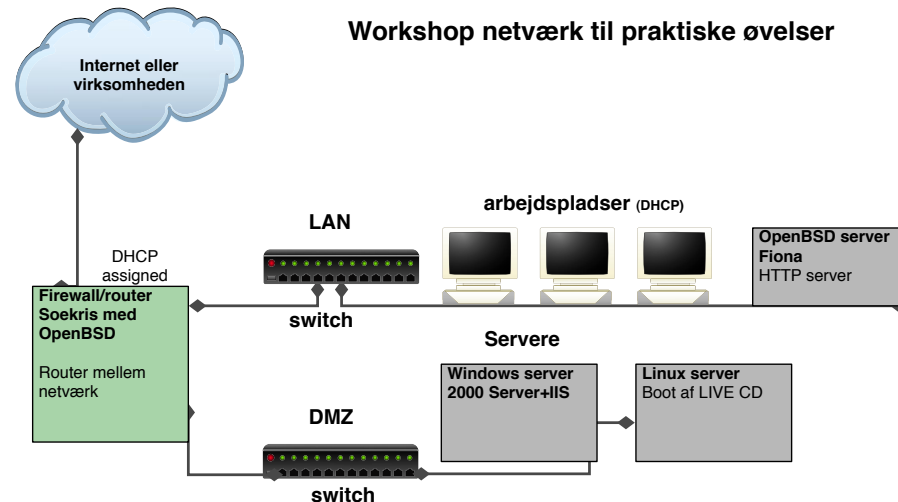
bruge protokoller som ikke er sårbare overfor opsamling



```
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

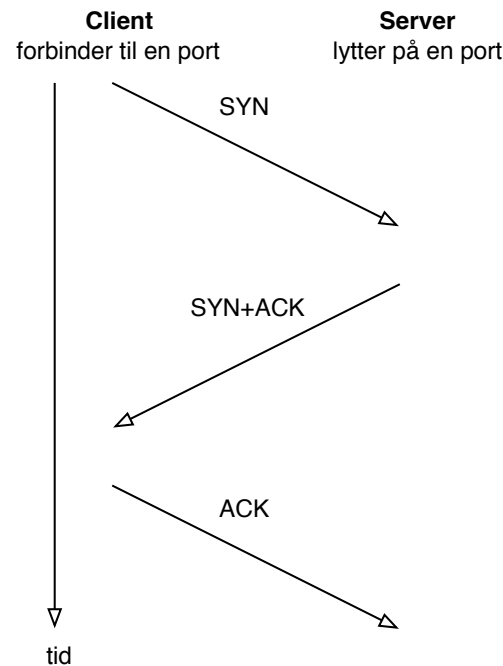
typisk TCP og UDP scanning

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

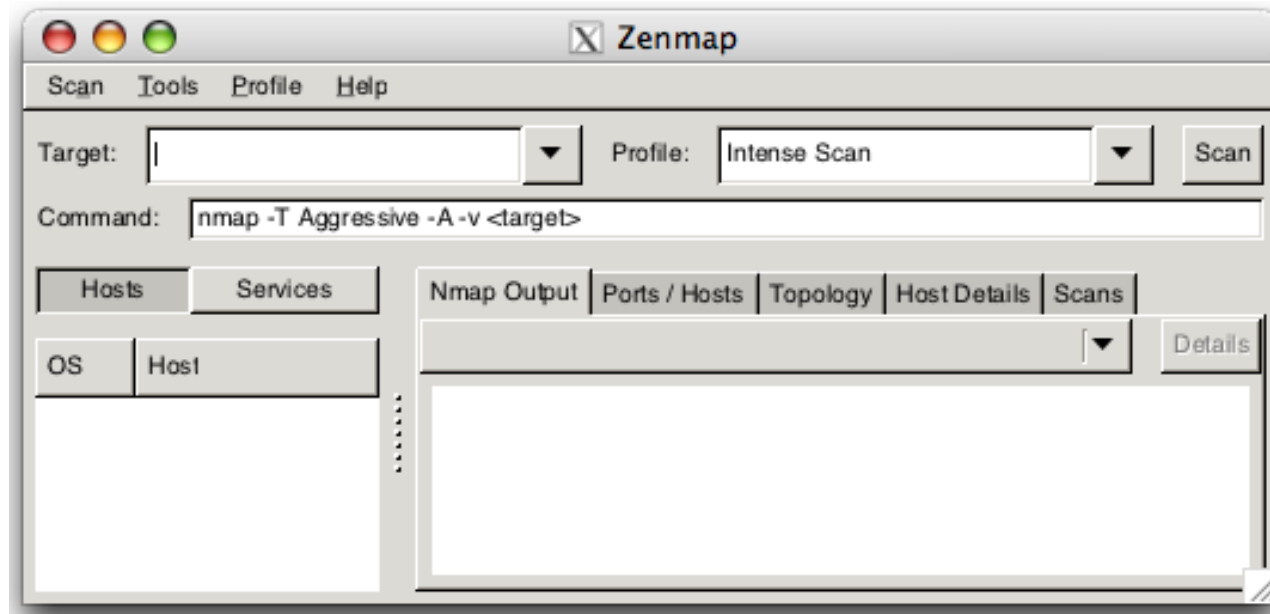
Scan et netværk efter aktive systemer med PING

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

Portscan med Zenmap GUI



Zenmap følger med i pakken når man henter Nmap <http://nmap.org>

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

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

...

<http://www.thc.org/thc-hydra/>
hvad betyder bruteforcing?

Why another one? Words are generated in a bruteforce fashion but, when a condition takes place, it skips forward to the next valid word! User can define charset, maximum number of uses for every char in charset, patterns/repetitions to exclude. User can trim down number of combinations generated excluding 'invalid' words by setting some criteria.

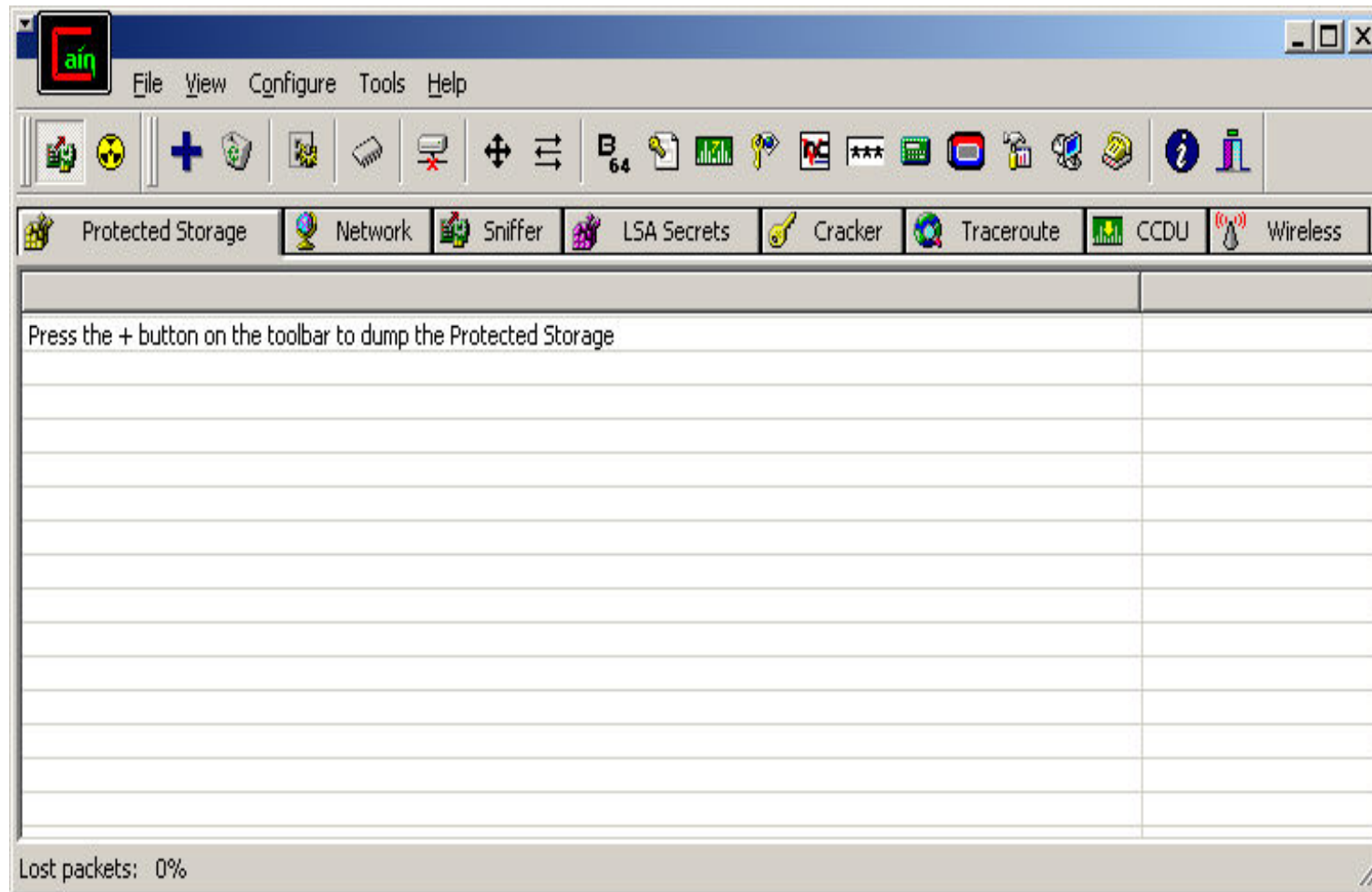
Hvordan laver man rigtigt bruteforce?

Skal man teste ALT - A, AA, AAA, AAAA, AAAAA, AAAAAAAAAA

<http://masterzorag.blogspot.com/>

Real life bruteforce? Found in Jan 2012

```
root:admin:87.x.202.63
admin:admin:91.x.104.207
admin:0767390145:x.72.110.84
admin:0767390145:89.xx.163.73
admin:0767390145:89.x.142.153
root:root:186.x.39.228
admin:admin:189.x.160.98
root:dumn3z3u:189.x.216.232
admin:0767390145:189.x.36.247
root:admin:169.x.34.145
root:default:66.x.33.138
root:default:66.x.33.138
root:111111:213.x.89.250
admin:admin:91.x.52.114
admin:0767390145:195.x.246.131
admin:0767390145:195.x.246.131
```

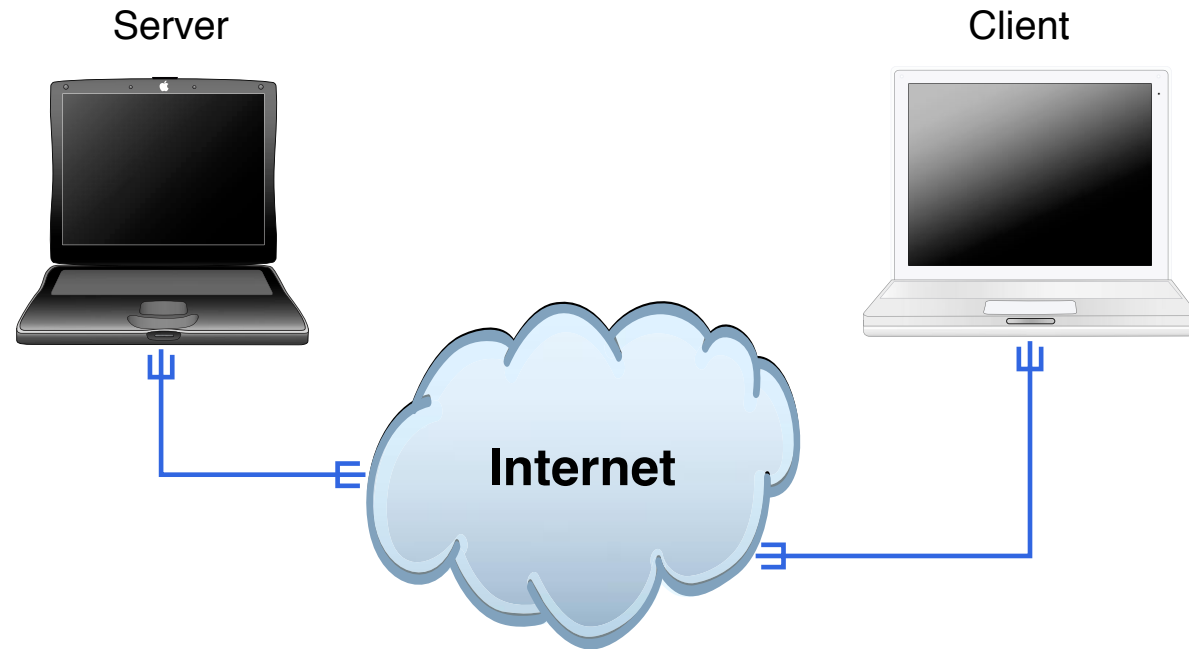


C&B er en generel cracker, der findes dog andre <http://www.oxid.it>

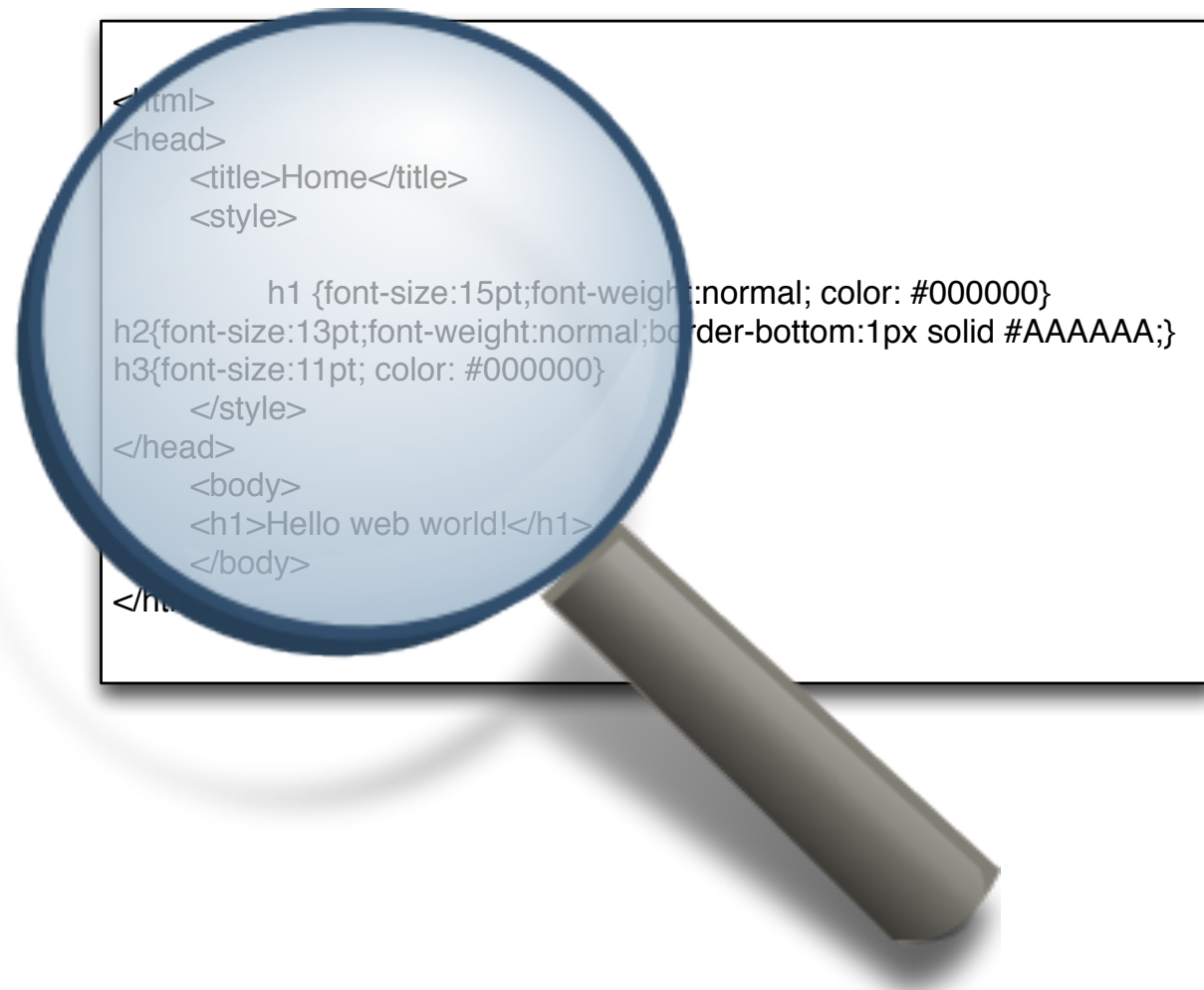
John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly 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

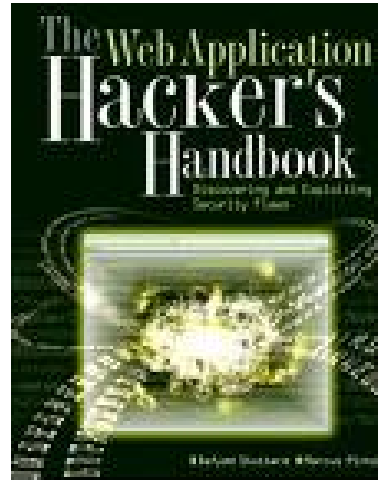
Pas på shell escapes!!!

Demo af et sårbart system - badfinger

Løsning:

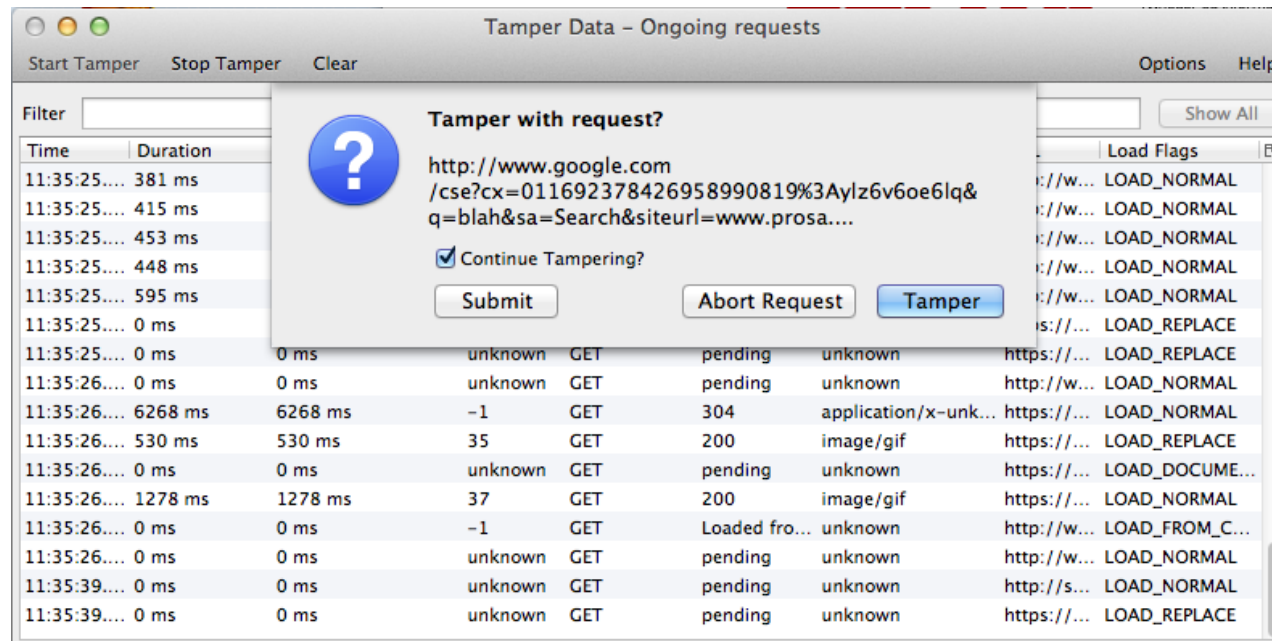
- Kalde finger kommandoen
- et Perl script
- afvikles som CGI
- standard Apache HTTPD 1.3 server

```
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";
}
```



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



<https://addons.mozilla.org/en-US/firefox/addon/tamper-data/>

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

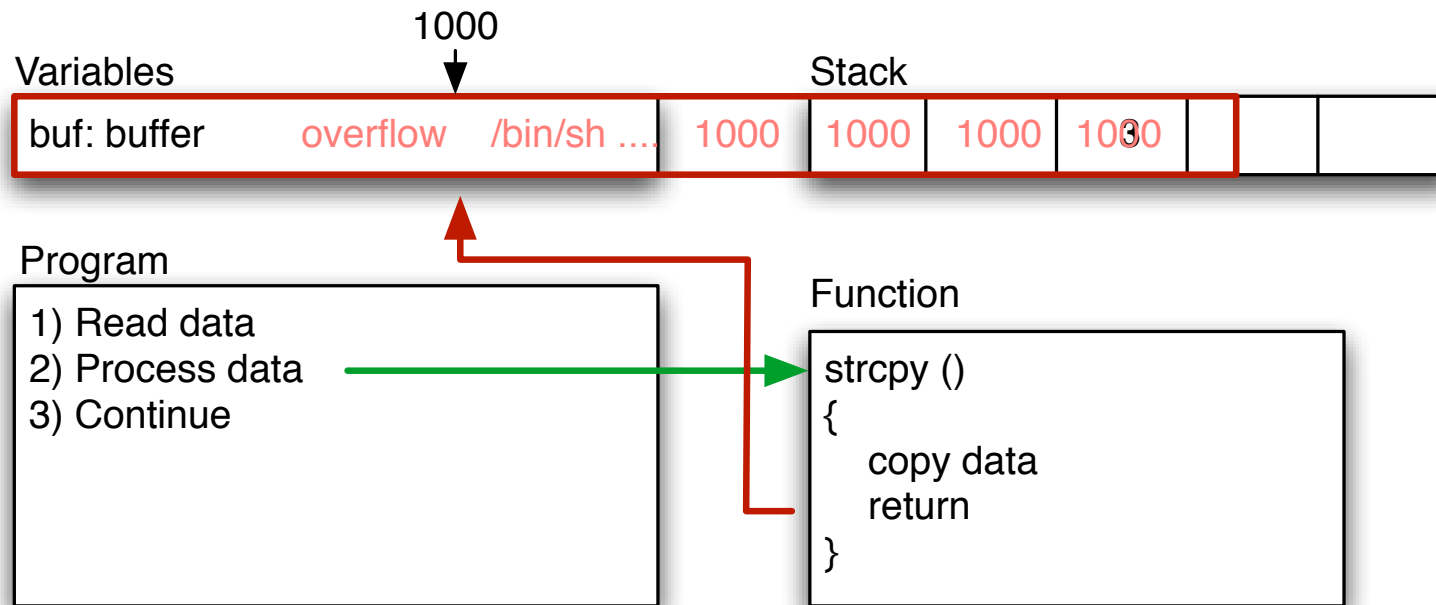
privilege escalation er når man på en eller anden vis opnår højere privileger på et system, eksempelvis som følge af fejl i programmer der afvikles med højere privilegier. Derfor HTTPD servere på UNIX afvikles som nobody - ingen specielle rettigheder. En angriber der kan afvikle vilkårlige kommandoer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

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

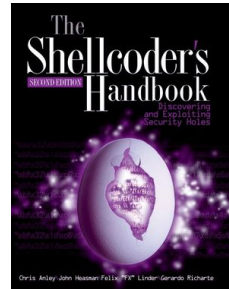
Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place



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



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 exploit-db og Metasploit

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 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



PROSA afholder en åben hackerkonkurrence for hold Capture the Flag
Distribueret CTF med omkring 10 hold
Hovedformål Sjovt og lærerigt - for alle!

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

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

Henrik Lund Kramshøj
hlk@solido.net

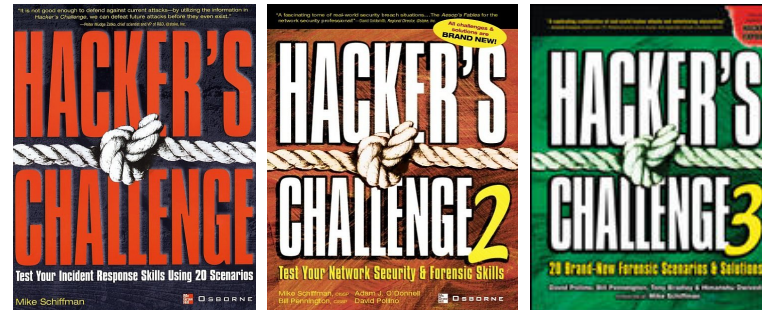
`http://www.solidonetworks.com`

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>



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

(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