

Welcome to

# Penetration testing I basale pentest metoder

Henrik Lund Kramshøj  
hlk@solido.net

<http://www.solidonetworks.com>



## Don't Panic!

Introducere basale penetrationstestmetoder

Introducere basale værktøjer indenfor genren af hackerværktøjer

At forklare de problemer man støder på under udførelse af sikkerhedstest

Give inblick i processen omkring sikkerhedstest

Skabe en grundig forståelse for hackerværktøjer samt penetrationstest metoder

## 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 lidenskabligt (eller enddog fanatisk) eller en der foretrækker at programmere fremfor at teoretiserer om det
- En ekspert i et bestemt program eller en der ofter arbejder med eller på det; som i "en Unixhacker".

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

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

**Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.**

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
- Frygten for terror har forstærket ovenstående - så lad være!

## **Code of Ethics Preamble:**

- Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

## **Code of Ethics Canons:**

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

The following additional guidance is given regarding pursuit of these goals.

<https://www.isc2.org/ethics/default.aspx>

Sikkerhedsproblemer i netværk er mange

Kan være et krav fra eksterne - eksempelvis VISA PCI krav

Chefen: skal vi ikke have en sikkerhedstest udført?

IT-chefen: hmm, det kan vi da godt

IT-medarbejderen: \*gisp\* - jeg ved sikkerheden halter flere steder!

Husk at det ikke er jeres systemer - tag ikke kritik personligt, men som hjælp til at forbedre

[IT-NYHEDER](#)[BLOGS](#)[IT-JOB](#)[IT-FIRMAER](#)[WHITEPAPERS](#)

EMNER [Hacking](#), [It-sikkerhed](#)

 [Se kommentarer \(7\)](#)

## Hackerkursus satte Dong på sporet af sårbare servere

En uges kursus i at tænke som en hacker gav flere aha-oplevelser for sikkerhedskonsulent hos Dong Energy. For eksempel fandt han efterfølgende server-software, der kørte med standard-password.

*Af Jesper Kildebogaard Mandag, 19. marts 2012 - 6:59*

Det kræver kun én lille sprække i forsvarsværkerne, før en hacker kan snige sig ind. Men hvordan opdager man som sikkerhedsansvarlig sprækken før hackeren?

Hos energikoncernen Dong Energy har et af svarene været at lære at tænke som hackerne. Og det gør det muligt at se på systemerne med helt andre øjne, fortæller en af de Dong-folk, der har været på hackerkursus.

»Kurset var et wakeup-call om, hvor nemt det er for hackere, som går systematisk til værks, og som ved, hvad de gør,« siger Keld Hjortskov, der er sikkerhedskonsulent hos Dong.

- Introduktion - begreber og teknologierne
- Hvad er sikkerhedstest
- Fordele ved at få udført planlagt sikkerhedstest
- Planlægning af sikkerhedstest
- Før testen - forberedelse
- Udvælgelse af systemer til test
- Godkendelse og tilladelse fra systemejere m.fl.
- Oprydning og afrapportering - resultater
- Konsulentens udstyr - vil du være sikkerhedskonsulent
- Selve testens udførelse

Sikkerhedstest / penetrationstest

Afprøvning af sikkerhedsforanstaltninger og evaluering af sikkerhedsniveau ved hjælp af IT systemer og *hackerværktøjer*

Kaldes tillige sårbarhedstest, sårbarhedsanalyse m.v.

Ekstern - udføres fra internet typisk over WAN

Intern, inside, on-site - udføres hos kunden typisk over LAN og bag firewall

<http://www.google.com/search?q=sikkerhedstest>

## Forudsætninger og forudgående kendskab til miljøet

Afhængig af de informationer der er tilgængelige om opbygningen af det scannede netværk forud for NetSikkerhedsanalySEN taler man om henholdsvis White, Grey og Black Box testning.

- Black Box testen involverer en sikkerhedstestning af et netværk uden nogen form for insider viden om systemet udover den IP-adresse, der ønskes testet. Dette svarer til den situation en fjendtlig hacker vil stå i og giver derfor det mest realistiske billede af netværkets sårbarhed overfor angreb udefra. Men er dårlig ressourceudnyttelse.
- I den anden ende af skalaen har vi White Box testen. I dette tilfælde har sikkerhedsspecialisten både før og under testen fuld adgang til alle informationer om det scannede netværk. Analysen vil derfor kunne afsløre sårbarheder, der ikke umiddelbart er synlige for en almindelig angriber. En White Box test er typisk mere omfattende end en Black Box test og forudsætter en højere grad af deltagelse fra kundens side, men giver en meget detaljeret og tilbundsgående undersøgelse.
- En Grey Box test er som navnet siger et kompromis mellem en White Box og en Black Box test. Typisk vil sikkerhedsspecialisten udover en IP-adresse være i besiddelse af de mest grundlæggende systemoplysninger: Hvilken type af server der er tale om (mail-, webserver eller andet), operativsystemet og eventuelt om der er opstillet en firewall foran serveren.

Formålet med en sikkerhedstest er at nedbringe risici for systemerne og sikre organisationen mod uventede tab af data, tab af omdømme, forøgede omkostninger. Formålet er ikke at udpege en syndebuk eller identificere dårlige medarbejdere.

Giver gavnlig information

undgår nedbrud på uheldige tidspunkter

Målgrupper:

- IT-afdeling og teknisk personale
- Ledelse, koncernledelse

Afleveringer:

- Rapport med tekniske anbefalinger og opsummering/checklister
- Executive summary

## Alle bruger nogenlunde de samme værktøjer

- 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, ...

- Sikkerhedskonsulent - den konsulent der kommer ud til kunden
- Kontaktperson - kundens ansatte som kan hjælpe med praktiske spørgsmål og skabe kontakt til de rette personer i kundens organisation
- Systemejer - den ansvarlige for et bestemt system
- Netværksejer - den ansvarlige for netværk hos kunden
- Driftorganisation - dem der driver systemerne
- Sikkerhedsansvarlig - den ansvarlige for sikkerheden hos kunden

## Sårbarhedsanalysens omfang

- Scope - hvad skal testes
- Hvornår skal testes - indenfor et aftalt tidsrum
- Hvor testes fra - logfilerne vil afsløre IP-adresser
- Skal være aftalt på forhånd
- Kan overskrides delvist - eksempelvis ved port 80 scan på samme subnet eller tilsvarende
- Skal der forsøges ude af drift angreb - DoS
- Se endvidere slide om Rules of engagement senere

## SårbarhedsanalySEN omfatter (targets):

- 192.168.1.1 - firewall/router
- 192.168.1.2 - mailserver
- 192.168.1.3 - webserver
- Testen udføres i tidsrummet mandag 1. til fredag 5. fra 91.102.91.16/28

Testplan med oversigt over targets og IP-adresser

Netværkstegninger og anden information som er aftalt oplyst

Hvor skal sikkerhedskonsulenten placeres på insidetest - ikke i serverrum tak :-)

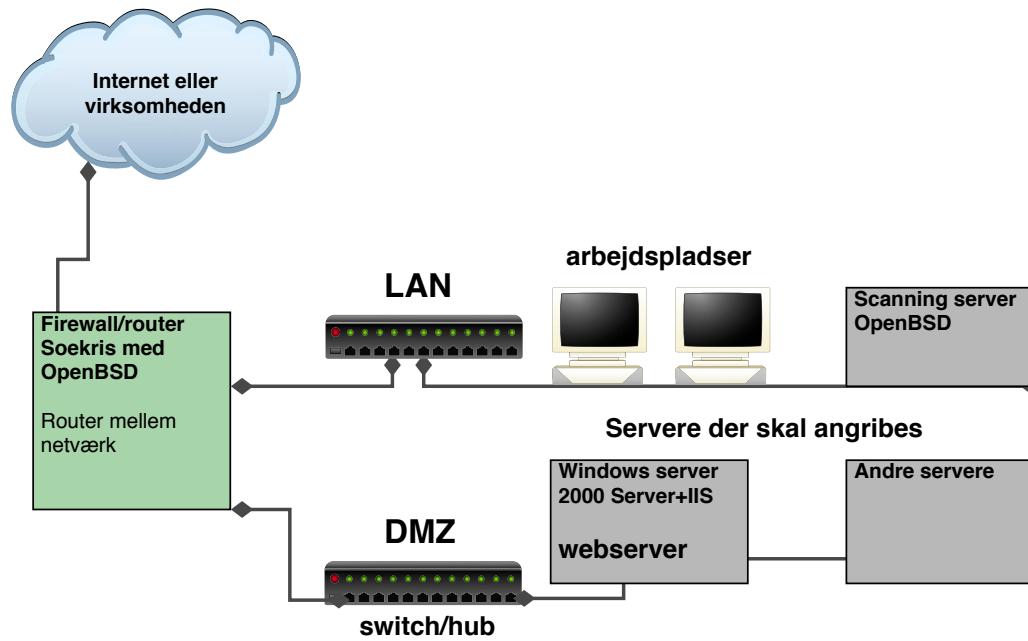
Kabling af netværksstik

Gæstekort - til test over flere dage

kantine, toiletter osv.

Betrugt det som en ny kollega - med tidsbegrænset kontrakt

# Udvælgelse af systemer til test



## Typiske interessante mål og årsager

- Routere på netværksvejen til kritiske systemer og netværk - tilgængelighed
- Firewall - begrænses trafikken tilstrækkeligt
- Mailservere - tillades relaying udefra
- Webservere - kan der afvikles kode på systemet, downloades data

Udførelse af test kan have negativ indflydelse på driften

Inden en test kan udføres skal der indhentes tilladelser fra:

- systemejere
- netværksejer
- driftorganisationer

At belyse problemerne er formålet

- at få dem belyst indenfor et aftalt tidsrum er en fordel!

Scannersystemer, hardware og software kræver en del ekspertise og opsætning. Det er tidskrævende at foretage denne opsætning og konsulenten har på forhånd udvalgt og konfigureret udstyr til testen. Det skal derfor accepteres at konsulenten tilslutter eget udstyr til de pågældende netværk og dette sker naturligvis under strenge krav til konsulentens udstyr.

**Det er ikke en mulighed at bruge kundens udstyr!**

testen udføres ved samarbejde mellem konsulent og virksomhed

Først og fremmest skal testen startes

- Når konsulenten ankommer kontaktes kontaktpersonen
- Konsulenten vises til rette og pakker ud/stiller op
- Såfremt det ønskes inspiceres og godkendes udstyret
- Konsulenten tilslutter sig netværket og test er officielt igang
- Konsulenten verificerer adgangen til netværk og melder klar, begynder test

... tiden går ... testen udføres ...

kontaktpersonen er hele tiden til rådighed på mobiltelefon

Testen afsluttes og der pakkes ned i modsat rækkefølge

Der kan være årsager der medfører at testen skal indstilles

Sikkerhedskonsulenten afbryder testen

- Det anses for uforsvarligt at fortsætte, der er fundet kompromitterede systemer eller beviser der kan ødelægges
- Netværket er dårligt, mulighederne for udførelse er forringet

Kunden ønsker at afbryde testen

- Der opleves for store problemer under udførelsen
- Systemnedbrud på forretningskritiske systemer
- Andre kriser der gør det valgte tidspunkt uegnet

NB: eksempler! - man afbryder altid når kunden ønsker det!

Sikkerhedskonsulenten er ansvarlig for:

- Fjerne data fra systemerne
- Fjerne brugerkonti, få fjernet brugeroplysninger og loginmuligheder
- Fjerne software som ikke skal benyttes mere

Driftsorganisationen er ansvarlig for:

- Undersøgelse af systemerne
- Eventuel genstart af systemer, der kan være nedsat effektivitet
- Fjerne patchkabler for stik der er kablet speciet til konsulenten

Hvad indeholder en sikkerhedstest rapport:

- titel, indholdsfortegnelse, firmanavne - ca. 15-30 sider for 5 hosts
- fortrolighedserklæring - det er fortrolige oplysninger
- Executive summary - ofte i større virksomheder
- Information om den udførte scanning
- Omfang/scope
- Gennemgang af targets - detaljeret information og med anbefalinger
- Konklusion - ofte mere teknisk
- Bilag - detaljerede oplysninger og oversigter, checklister

Det er organisationen der selv vælger hvilke anbefalinger der følges

- NB: stor forskel på Danmark og udlandet!
- Sikkerhedskonsulenten må ikke give anledning til nye sårbarheder som følge af testen
- Sikkerhedskonsulenten må ikke installere ny software på systemer uden forudgående aftale
- Sikkerhedskonsulenten efterlader ikke usikre systemadministratorkonti eller tilsvarende efter testen
- Sikkerhedskonsulenten tager altid kontakt til kunden ved høj-risiko sårbarheder
- Er man hyret til netværkssikkerhed kan man godt *snuse* lidt rundt om systemerne under test - der kan være et sårbart testsystem lige ved siden af
- Solido.net vil ved opdagelse af åbenlyse sikkerhedsrisici dokumentere disse i rapporten, uanset scope for opgaven ellers

Det er en balancegang

## Bøger:

- *Metasploit The Penetration Tester's Guide* by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni <http://nostarch.com/metasploit>
- *Gray Hat Hacking: The Ethical Hacker's Handbook*, 3rd Edition, Shon Harris et al, Osborne
- *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses* (2nd Edition), Ed Skoudis, Prentice Hall PTR

## Internetressourcer:

- BackTrack <http://www.backtrack-linux.org/>
- OSSTMM - *Open Source Security Testing Methodology Manual*  
<http://www.isecom.org/>
- CCCure website <http://www.professionalsecuritytester.com/>
- Web sites for diverse værktøjer - inkluderer ofte en step-by-step guide

Sikkerhedskonsulenterne bruger typisk Open Source værktøjer på UNIX og enkelte systemer med Windows - jeg bruger helst Windows 7 i dag

Jeg anbefaler kraftigt at Windows systemerne ikke benyttes som arbejdsstation i hverdagen

I Solido.net bruges Windows hackersystemerne aldrig til håndtering af email, Windows systemerne benytter opdateret systemsoftware og oftest antivirus

Dette er et teknisk foredrag og fuldt udbytte kræver at deltagerne har mindst 2 års praktisk erfaring som teknikker og/eller systemadministrator

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

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

Der benyttes en del værktøjer:

- Nmap, Nping - tester porte, godt til firewall admins <http://nmap.org>
- Metasploit Framework gratis på <http://www.metasploit.com/>
- Wireshark avanceret netværkssniffer - <http://www.wireshark.org/>
- Burpsuite <http://portswigger.net/burp/>
- Skipfish <http://code.google.com/p/skipfish/>
- Apache Tomcat J2EE servlet container <http://tomcat.apache.org>
- OpenBSD operativsystem med fokus på sikkerhed <http://www.openbsd.org>

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: Metasploit, Nikto, exploit programs

Oprydning/hærdning vises måske ikke, men I bør i praksis:

- Lav en rapport
- Ændre, forbedre og hærde systemer
- Gennemgå rapporten, registrer ændringer
- Opdater programmer, konfigurationer, arkitektur, osv.

I skal jo også VISE andre at I gør noget ved sikkerheden.

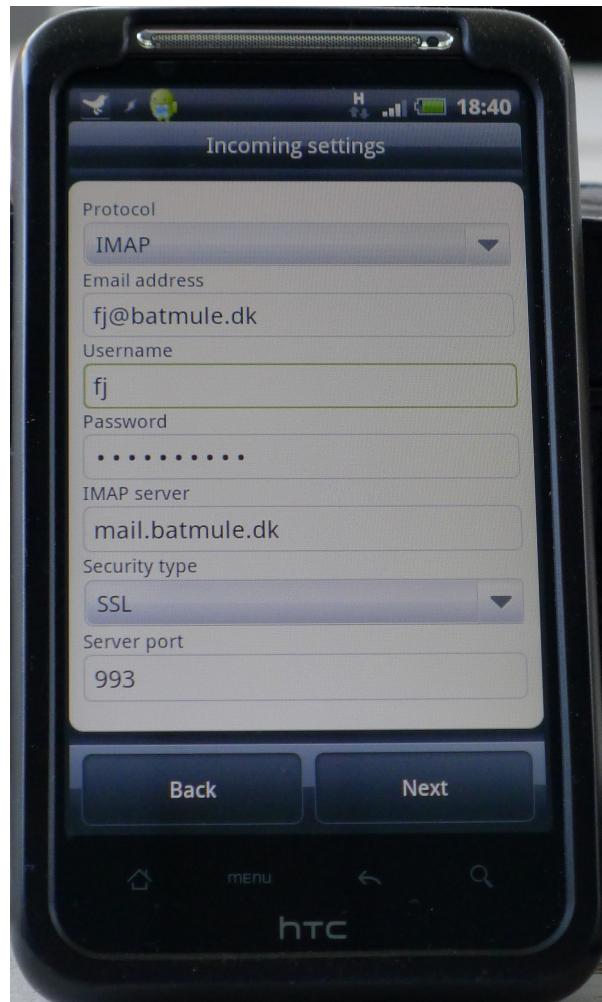
Brug teknologien

Lær teknologien at kende - læs manualen!

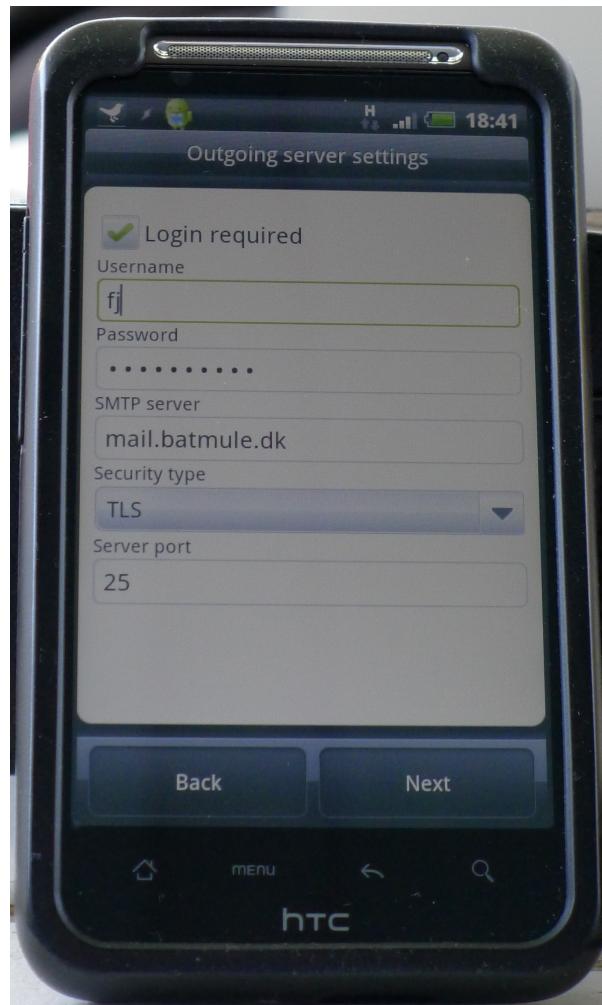
Tænk på følsomheden af data I gemmer og overfører

- Slå ting fra som I ikke bruger
- Slå bluetooth fra når I ikke bruger den
- Opdater softwaren på enheden
- Slå kryptering til hvor I kan: IMAPS, POP3S, HTTPS og over bluetooth
- Brug låsekode fremfor tastaturlås uden kode på mobiltelefonen
- Stol ikke for meget på fingertryksaflæsere

Istedet for POP3 brug POP3s, Istedet for IMAP brug IMAPs

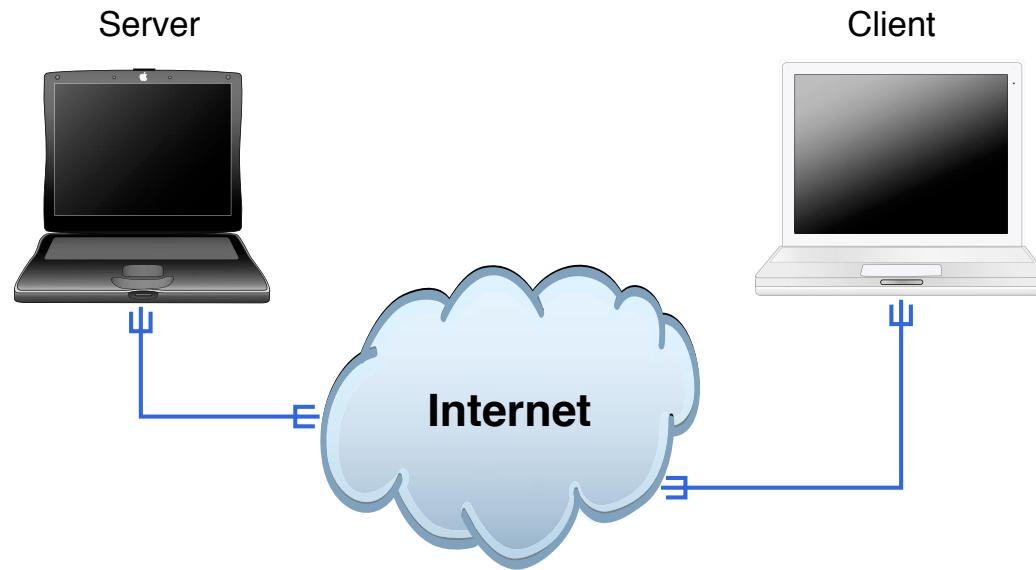


SMTP kan erstattes med SMTP+TLS



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





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

# Trinity breaking in

```
80/tcp      open     http  
81/tcp      open     hostx2_anc  
10  [ ]  
11  $ nmap -v -sS -O 10.2.2.2  
11  
13 Starting nmap 0. 2.54BETA25  
13 Insufficient responses for TCP sequencing (3). OS detection is  
13 inaccurate  
14 Interesting ports on 10.2.2.2:  
14 (The 1539 ports scanned but not shown below are in state: cle  
51 Port      State       Service  
51 22/tcp    open        ssh  
58  
68 No exact OS matches for host  
68  
24 Nmap run completed -- 1 IP address (1 host up) scanned  
50 $ sshngke 10.2.2.2 -rootpw="Z10H0101"  
Connecting to 10.2.2.2:ssh ... successful.  
Re  
IP Attempting to exploit SSHv1 CRC32 ... successful.  
Reseting root password to "Z10H0101".  
System open: Access Level <9>  
Hn $ ssh 10.2.2.2 -l root  
root@10.2.2.2's password: [REDACTED]  
[REDACTED] RIF CONTROL [REDACTED]  
[REDACTED] ACCESS GRANTED [REDACTED]
```

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

Meget realistisk [http://www.youtube.com/watch?v=511GCTgqE\\_w](http://www.youtube.com/watch?v=511GCTgqE_w)



Hacking ligner indimellem magi



Hacking kræver blot lidt ninja-træning

MAC filtrering på trådløse netværk

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

Mange trådløse Access Points kan filtrere MAC adresser

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

Det virker dog ikke ☺

De fleste netkort tillader at man overskriver denne adresse midlertidigt

Derudover har der ofte været fejl i implementeringen af MAC filtrering

Eksemplet med MAC filtrering er en af de mange myter

Hvorfor sker det?

Marketing - producenterne sætter store mærkater på æskerne

Manglende indsigt - forbrugerne kender reelt ikke koncepterne

Hvad *er* en MAC adresse egentlig

Relativt få har forudsætningerne for at gennemskue dårlig sikkerhed

Løsninger? ■

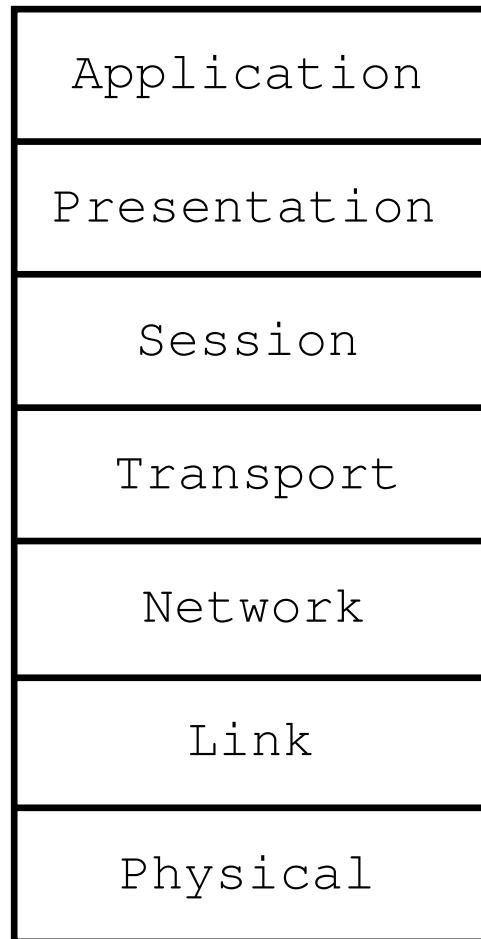
Udbrede viden om usikre metoder til at sikre data og computere

Udbrede viden om sikre metoder til at sikre data og computere

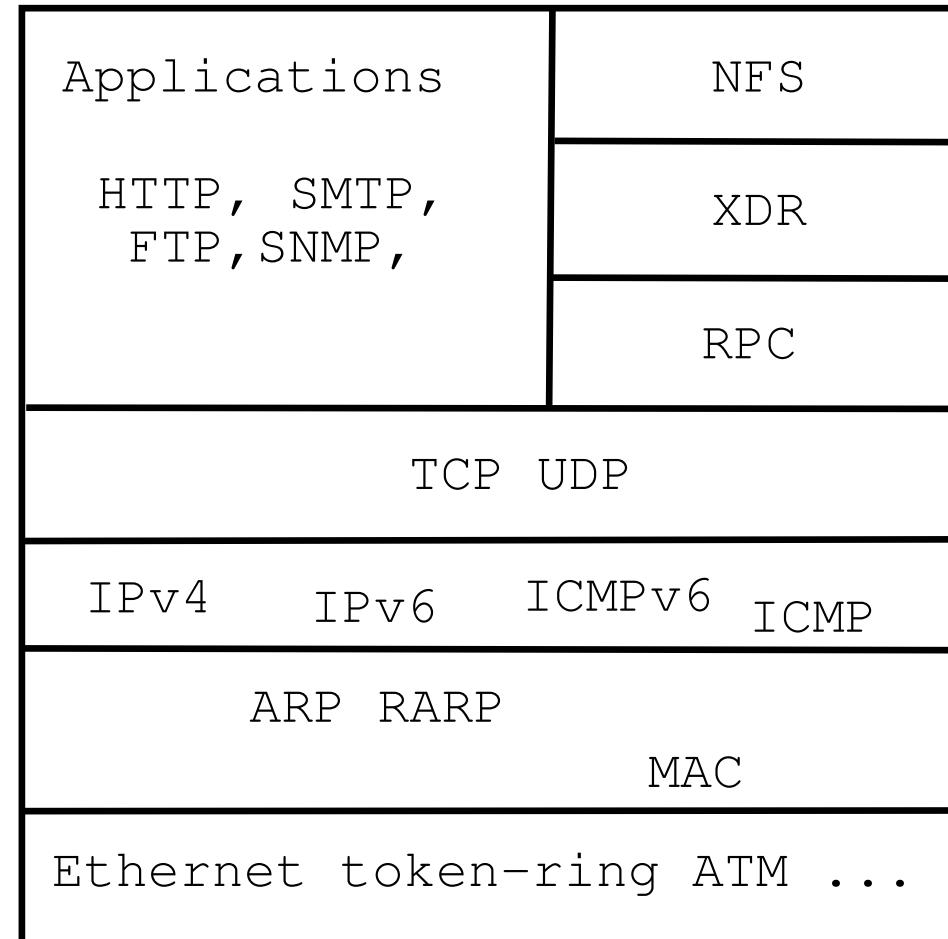
# MAC filtrering



OSI Reference Model



Internet protocol suite

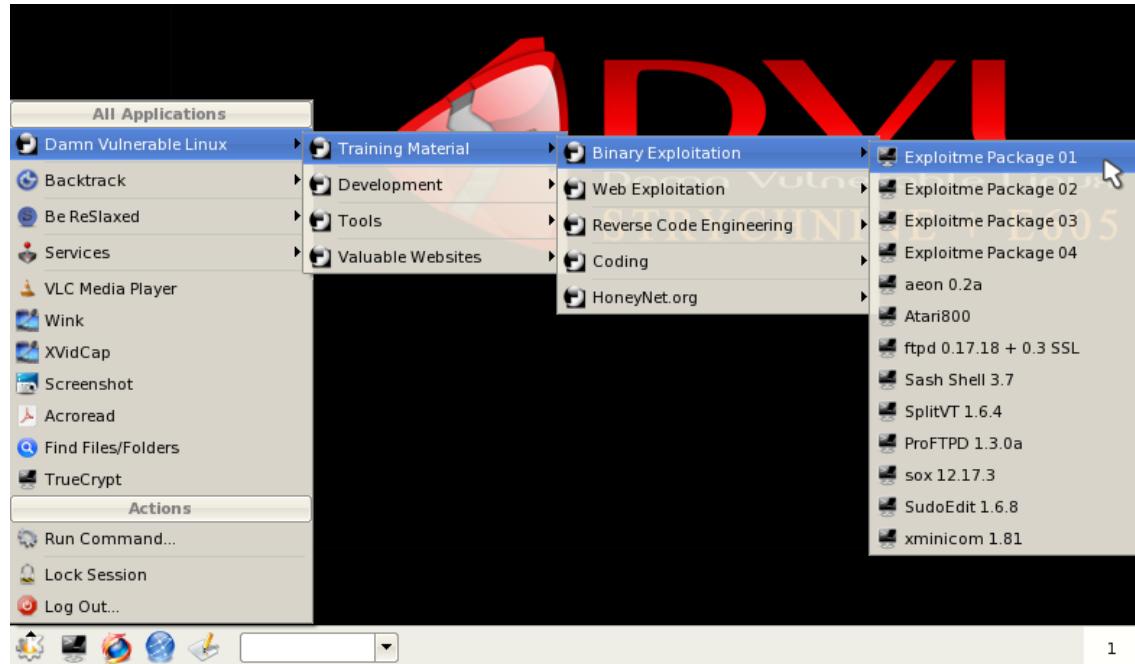




Wireshark - <http://www.wireshark.org> avanceret netværkssniffer  
bruger vi til at sniffe, vi bruger Wireshark til primære demo, nævner Ettercap osv.

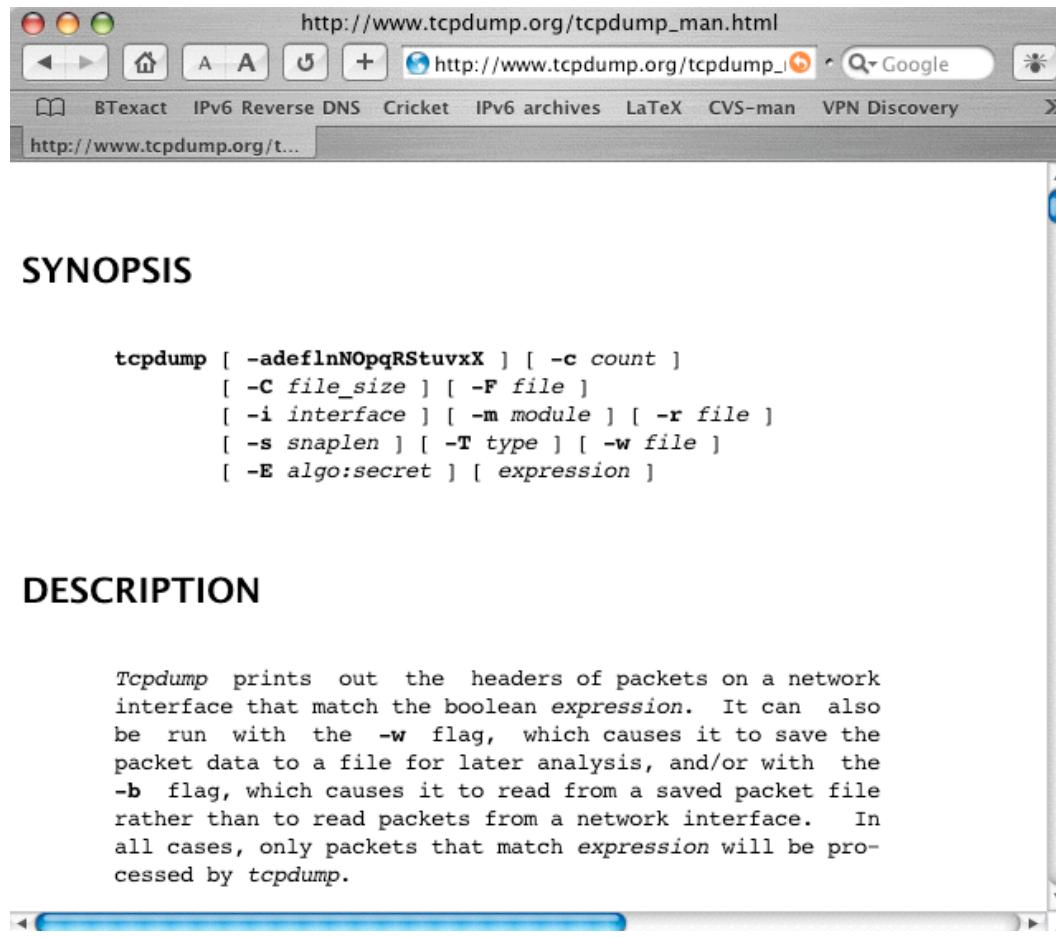
BackTrack <http://www.backtrack-linux.org/> BackTrack er baseret på Linux  
og må kopieres frit :-)

# Damn Vulnerable Linux boot CD'er



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

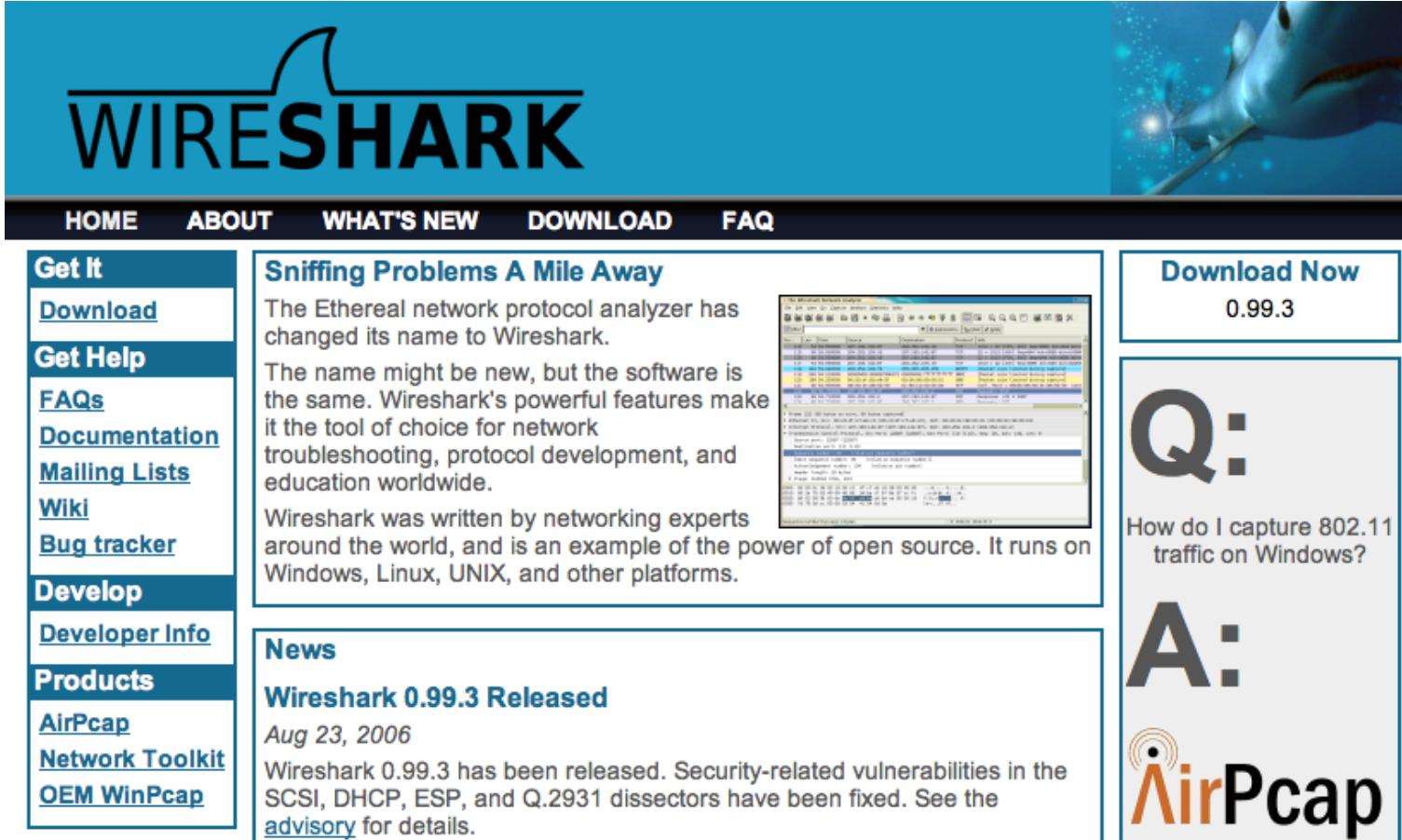
Brug CD'en eller VMware player til den



## DESCRIPTION

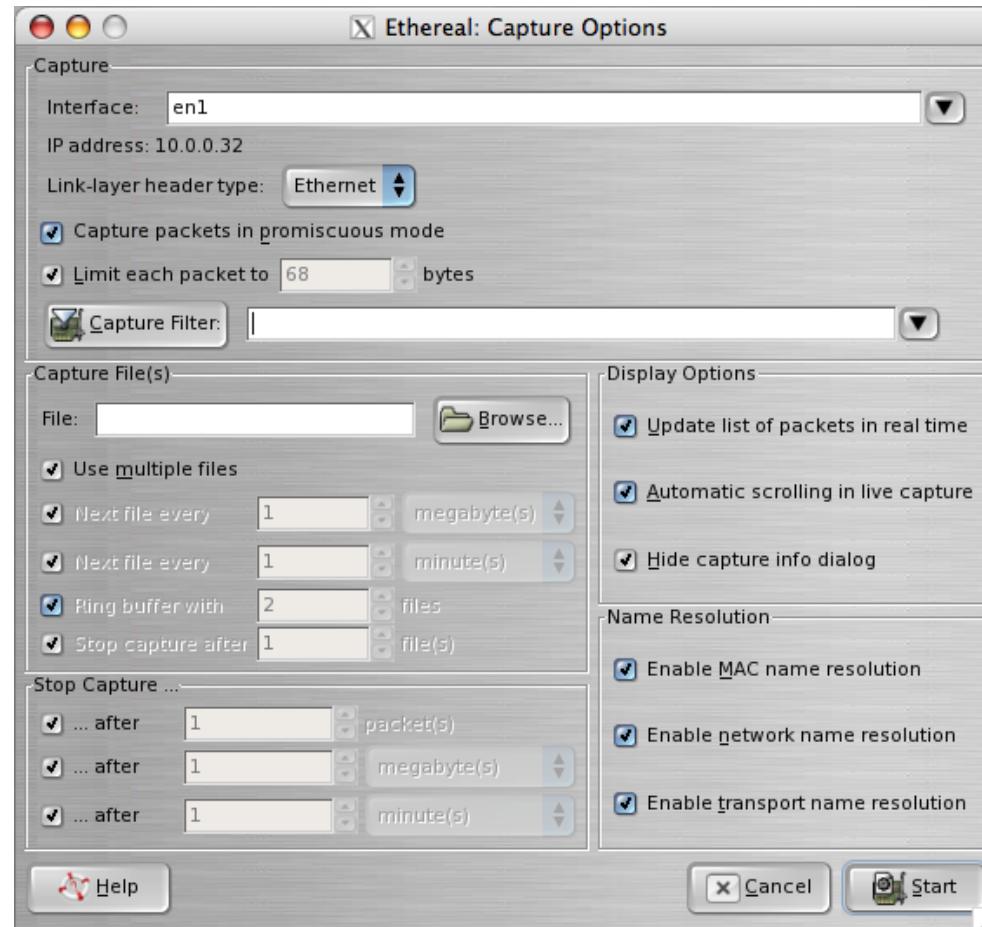
*Tcpdump* prints out the headers of packets on a network interface that match the boolean *expression*. It can also be run with the *-w* flag, which causes it to save the packet data to a file for later analysis, and/or with the *-b* flag, which causes it to read from a saved packet file rather than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



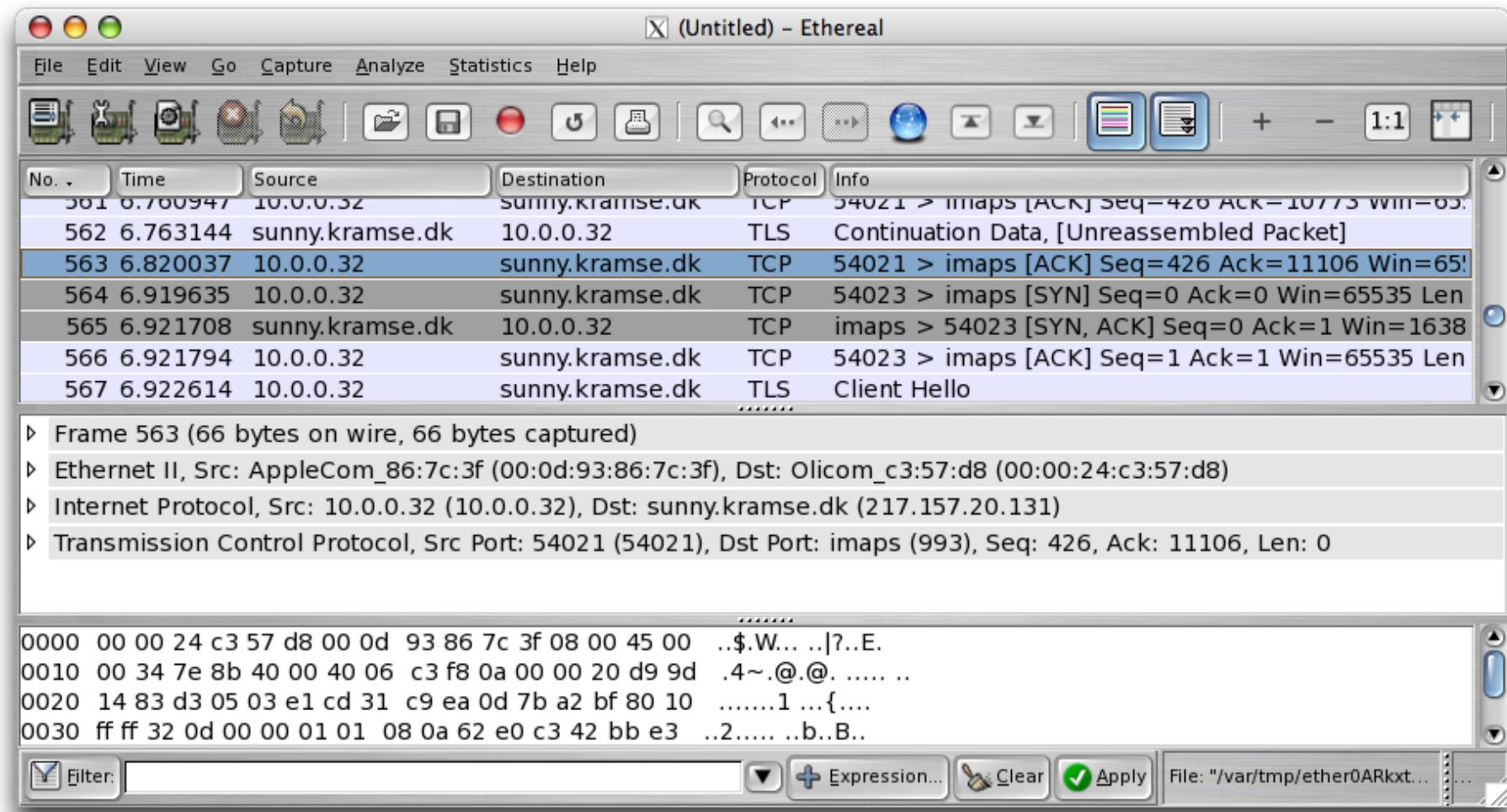
The screenshot shows the official Wireshark website. At the top, there's a navigation bar with links for HOME, ABOUT, WHAT'S NEW, DOWNLOAD, and FAQ. Below the navigation is a large blue header with the "WIRESHARK" logo and a shark swimming in water. On the left, there's a sidebar with sections for "Get It" (links to Download, Get Help, FAQs, Documentation, Mailing Lists, Wiki, Bug tracker, Develop, Developer Info, Products, AirPcap, Network Toolkit, OEM WinPcap), "Sniffing Problems A Mile Away" (text explaining the name change from Ethereal to Wireshark), and a screenshot of the Wireshark interface. In the center, there's a "News" section about the release of version 0.99.3, dated Aug 23, 2006, with a link to the advisory. To the right, there's a "Download Now" section for version 0.99.3, a Q&A section about capturing 802.11 traffic, and the AirPcap logo.

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



Man starter med Capture - Options

# Brug af Wireshark



Læg mærke til filtermulighederne

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
```

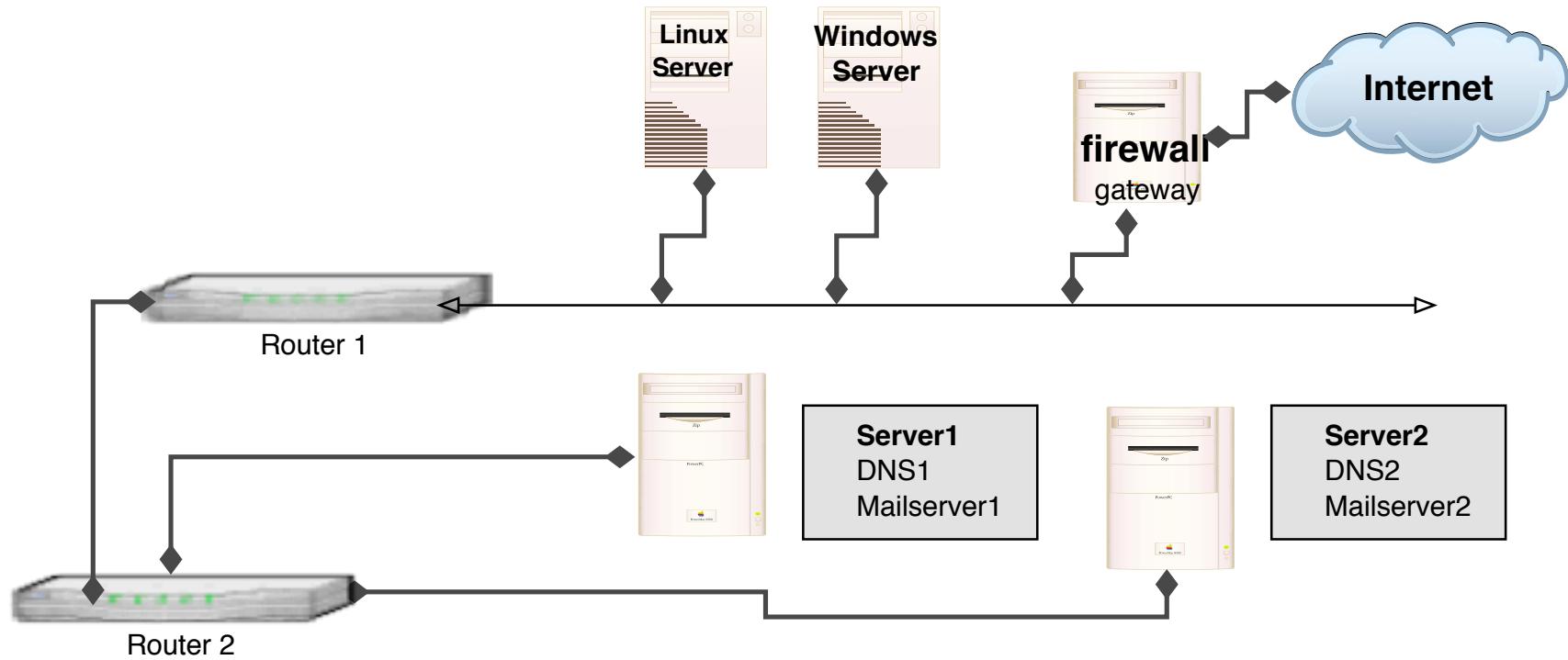
diagnosticering af netværksproblemer - formålet med traceroute

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

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.traceroute.org>

# Chaosreader

## Chaosreader Report

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

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

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

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

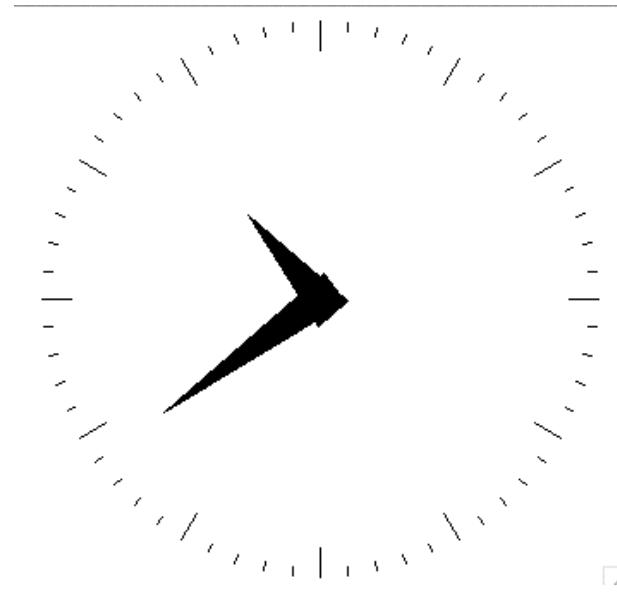
### TCP/UDP/... Sessions

1.	Sun Nov 16 20:38:22 2003	30 s	192.168.1.3:1368 <-> 192.77.84.99:80	web	383 bytes	• <a href="#">as html</a>
2.	Sun Nov 16 20:38:22 2003	29 s	192.168.1.3:1366 <-> 192.77.84.99:80	web	381 bytes	• <a href="#">as html</a>

Med adgang til et netværksdump kan man læse det med chaosreader

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

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



Hvad er klokken?

Hvad betydning har det for sikkerheden?

Brug NTP Network Time Protocol på produktionssystemer

ICMP timestamp option - request/reply

hvad er klokken på en server

Slayer icmpush - er installeret på server

viser tidstempel

```
# icmpush -v -tstamp 10.0.0.12
```

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

Receiving ICMP replies ...

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

```
icmpush: Program finished OK
```

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

```
[h1k@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.solido.net.
IN	MX	20	mail2.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>

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

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

TCP sequence number kan måske gættes

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

Hvad er portscanning

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

målet er at identificere åbne porte - sårbare services

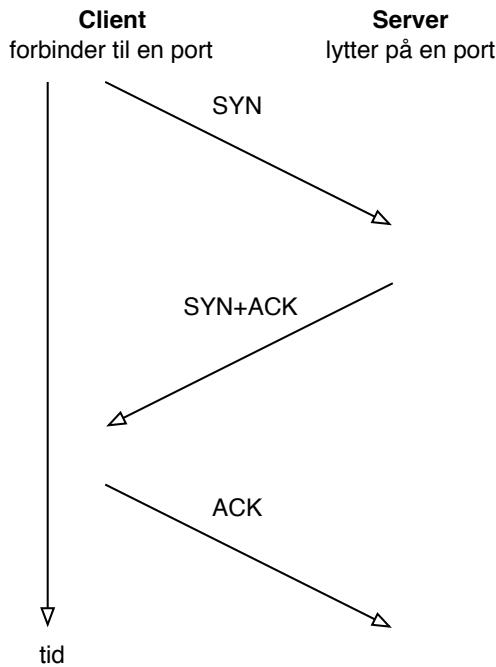
typisk TCP og UDP scanning

TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

# TCP three way handshake



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

scanninger på tværs af netværk kaldes for sweeps

Scan et netværk efter aktive systemer med PING

Scan et netværk efter systemer med en bestemt port åben

Er som regel nemt at opdage:

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

# nmap port sweep efter port 80/TCP

Port 80 TCP er webservere

```
# nmap -p 80 217.157.20.130/28
```

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on router.kramse.dk (217.157.20.129):

```

Port	State	Service
80/tcp	filtered	http

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

```

Port	State	Service
80/tcp	open	http

```
Interesting ports on (217.157.20.139):

```

Port	State	Service
80/tcp	open	http

# nmap port sweep after port 161/UDP

Port 161 UDP er SNMP

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

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on router.kramse.dk (217.157.20.129):
Port      State       Service
161/udp   open        snmp
```

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

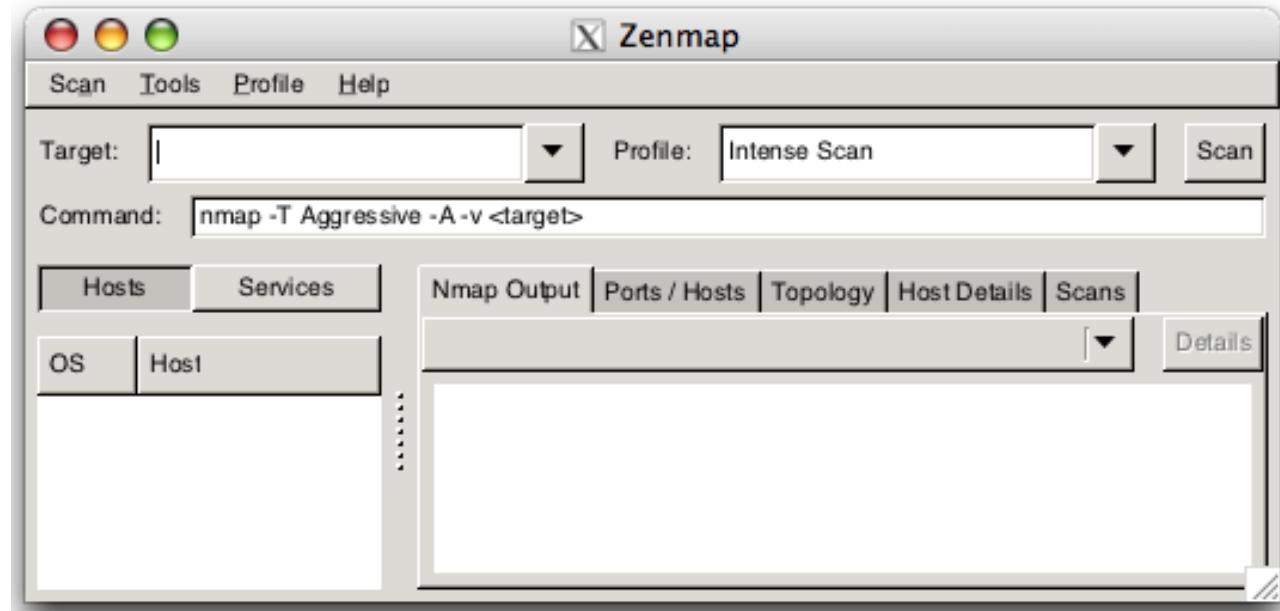
```
Interesting ports on www.kramse.dk (217.157.20.131):
Port      State       Service
161/udp   open        snmp
```

The 1 scanned port on (217.157.20.132) is: closed

```
# nmap -O ip.adresse.slet.tet scan af en gateway
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-03 11:31 CET
Interesting ports on gw-int.solido.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, prøv også nmap -A
- 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



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

Pentesting er ikke kun til test af produktionsnetværk

man skal ofte vurdere nye produkter - sikkerhedsmæssigt og funktionalitetsmæssigt -  
yder det beskyttelse, forbedrer det sikkerheden m.v.

hvor og hvordan kan I bruge penetrationstest

hvis man vil have et andet indblik i netværket, TCP, UDP, ICMP, portscanning og samle puslespil udfra få informationer

Netværksadministratorer kan bruge pentesting til at sikre egne netværk ved brug af samme teknikker som hackere

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

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

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

hosts - skal slås til men følger som regel med

SNMP bruges til:

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

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

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

## hvad betyder bruteforcing? afprøvning af alle mulighederne

Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>

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

Options:

- S connect via SSL
- s PORT if the service is on a different default port, define it here
- l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
- p PASS or -P FILE try password PASS, or load several passwords from FILE
- e ns additional checks, "n" for null password, "s" try login as pass
- C FILE colon seperated "login:pass" format, instead of -L/-P option
- M FILE file containing server list (parallizes attacks, see -T)
- o FILE write found login/password pairs to FILE instead of stdout

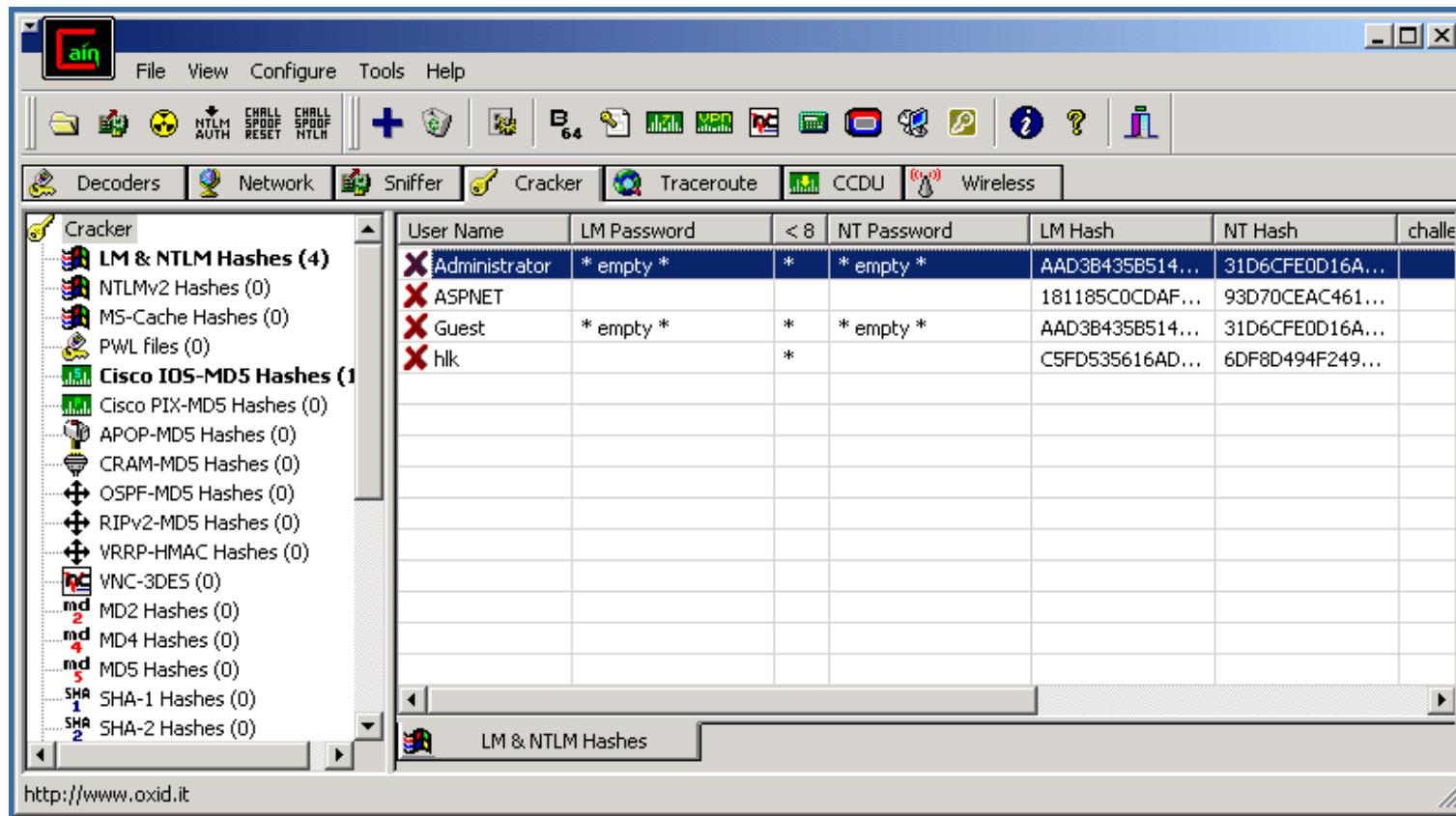
...

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



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

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

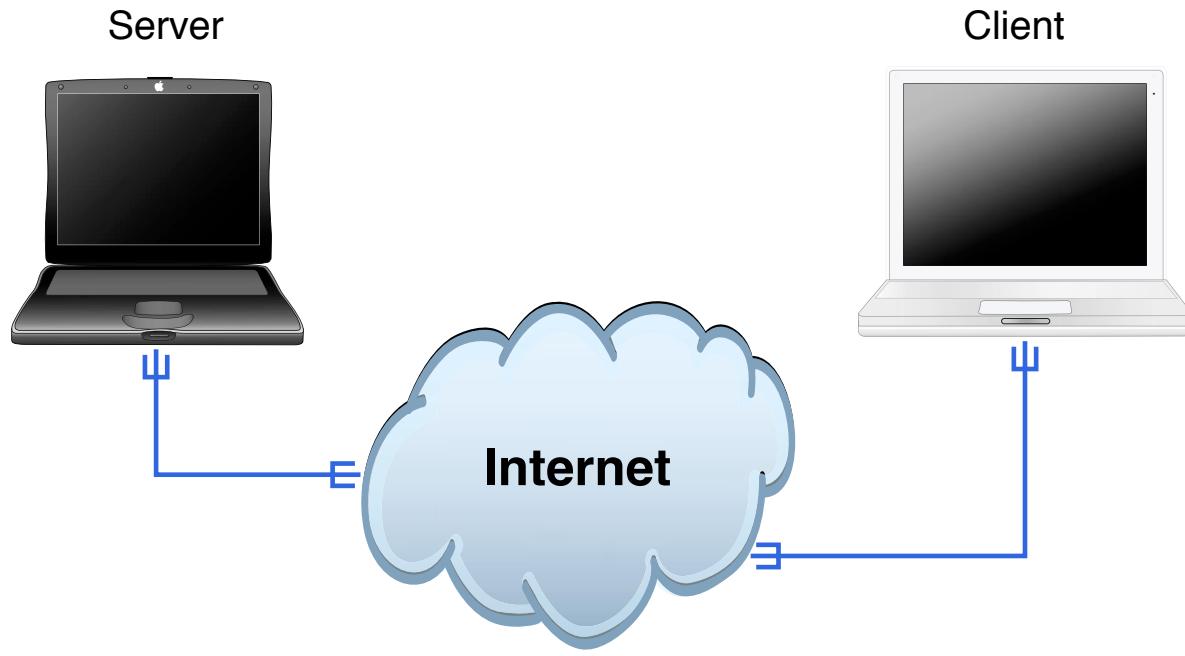


Cain og Abel anbefales <http://www.oxid.it>

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**

## The 5<sup>th</sup> Wave

By Rich Tennant

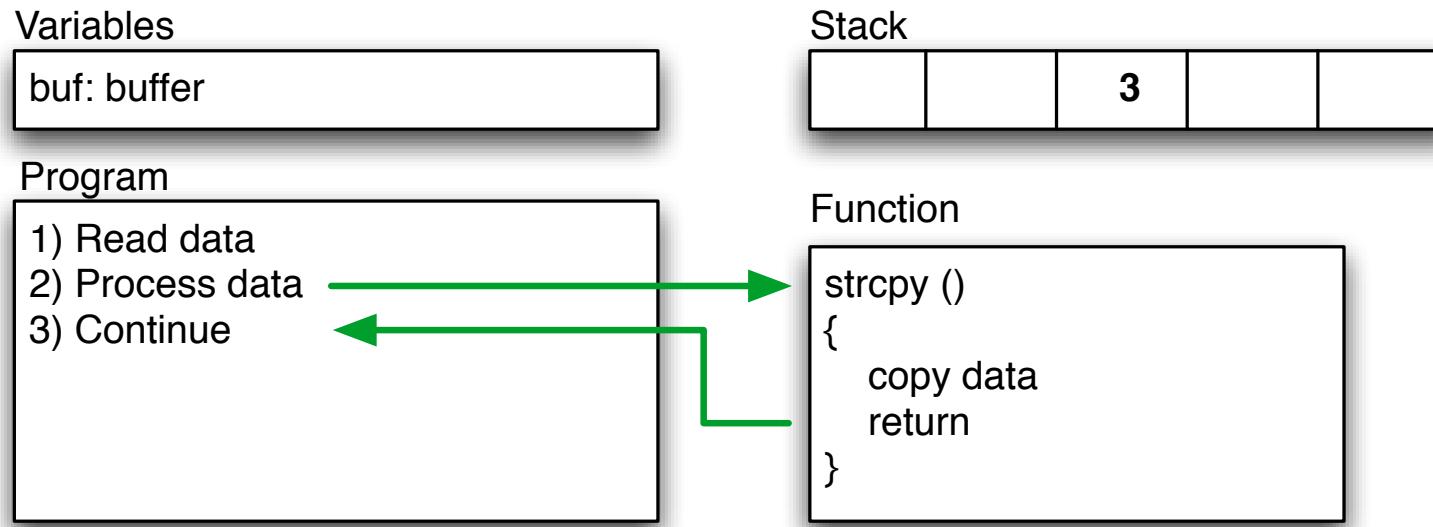


**"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."**

**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.

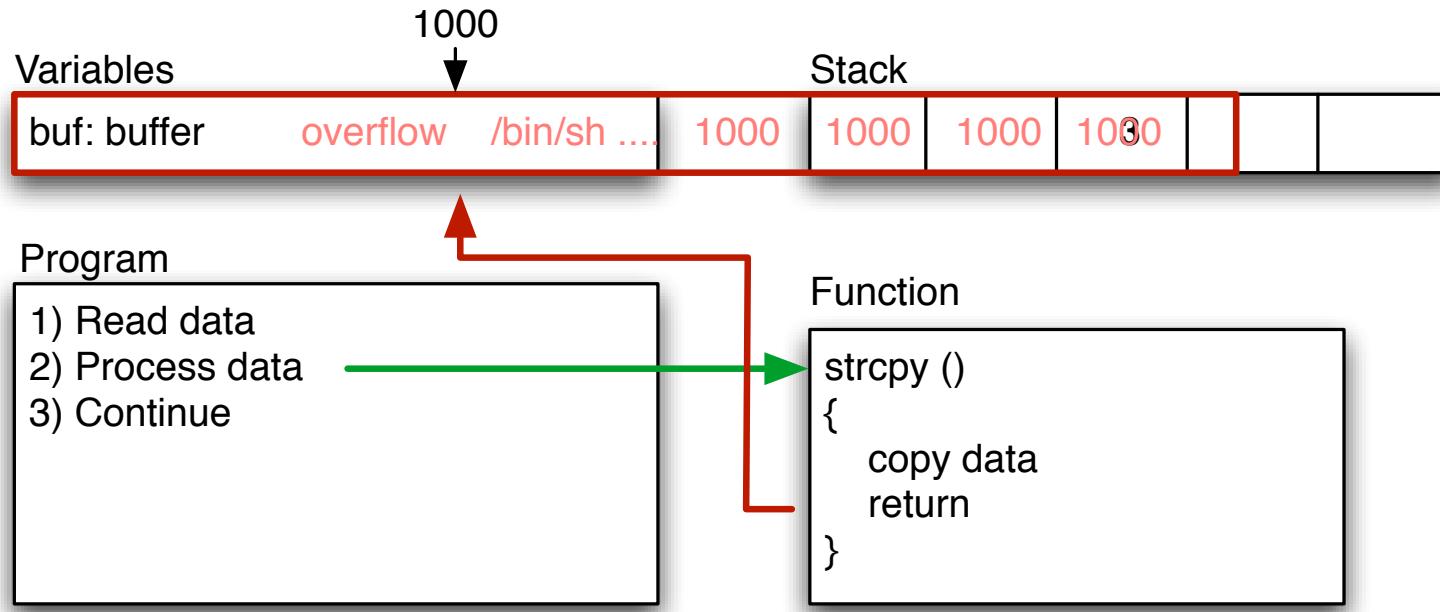
**Stack protection** er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

# Buffer og stacks



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

# Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

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

## Demo exploit in Perl

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

Common Vulnerabilities and Exposures (CVE) er:

- klassifikation
- unik navngivning af sårbarheder.

Sårbarheder tildeles

- initieret oprettes med status CANDIDATE

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

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



Læg mærke til at der er forskel på antallet af sårbarheder - nogle databaser opretter enkeltvis mens andre slår dem sammen

Demo sårbarhederne idag tæller eksempelvis i OSVDB 1 sårbarhed for hvert sårbart script

Kilde: <http://www.osvdb.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 afvike 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

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

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

**Opgave:** Lav et C program og oversæt det

**Forslag til fremgangsmåde:**

- Prøv at skrive dette program ind som `demo.c`
- Dernæst oversættes med kommandoen: `gcc -o demo demo.c`
- start programmet med kommandoen `./demo test` eller andre input

**Hjælp:**

```
main(int argc, char **argv)
{
    char buf[10];
    strcpy(buf, argv[1]);
    printf("%s\n", buf);
}
the_shell()
{   system("/bin/sh"); }
```

GNU compileren og debuggeren fungerer godt!

prøv `gdb ./demo` og kør derefter programmet fra *gdb prompten* med `run 1234`

når I således ved hvor lang strengen skal være kan I fortsætte med `nm` kommandoen - til at finde adressen på `the_shell`

skriv `nm demo | grep shell`

Kunsten er således at generere en streng der er præcist så lang at man får lagt denne adresse ind på det *rigtige sted*.

Perl kan erstatte AAAAA således '`perl -e "print 'A'x10"`'

Vi laver sammen en session med GDB

Afprøvning med diverse input

- ./demo langstrengs om giver problemer for programmet hvorførm'en
- gdb demo efterfulgt af run med parametre  
run AAAAAAAAAAAAAAAAAAAAAA

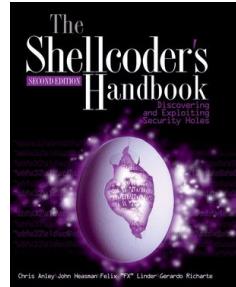
## Hjælp:

Kompiler programmet og kald det fra kommandolinien med ./demo 123456...7689  
indtil det dør ... derefter prøver I det samme i GDB

Hvad sker der? Avancerede brugere kan ændre strcpy til strncpy

# GDB output

```
h1k@bigfoot:demo$ gdb demo
GNU gdb 5.3-20030128 (Apple version gdb-330.1) (Fri Jul 16 21:42:28 GMT 2004)
Copyright 2003 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB. Type "show warranty" for details.
This GDB was configured as "powerpc-apple-darwin".
Reading symbols for shared libraries .. done
(gdb) run AAAAAAAAAAAAAAAAAAAAAA
Starting program: /Volumes/userdata/projects/security/exploit/demo/demo AAAAAAA
Reading symbols for shared libraries . done
AAAAAAAAAAAAAAAAAAAAA
Program received signal EXC_BAD_ACCESS, Could not access memory.
0x41414140 in ?? ()
(gdb)
```



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

*Smashing The Stack For Fun And Profit* Aleph One

*Writing Buffer Overflow Exploits with Perl - anno 2000*

Følgende bog kan ligeledes anbefales: *The Shellcoder's Handbook : Discovering and Exploiting Security Holes* af Jack Koziol, David Litchfield, Dave Aitel, Chris Anley, Sinan "noir" Eren, Neel Mehta, Riley Hassell, John Wiley & Sons, 2004

NB: bogen er avanceret og således IKKE for begyndere!

Bemærk: alle angreb har forudsætninger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

Kan du bryde kæden af forudsætninger har du vundet!

Computeren skal være tændt

Funktionen der misbruges skal være slået til

Executable stack

Executable heap

Fejl i programmet

|

**alle programmer har fejl**

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.

Vælg derfor hellere:

- Windows 7, end Windows Xp
- Mac OS X 10.7 fremfor 10.6
- Linux sikkerhedsopdateringer, sig ja når de kommer

Det samme gælder for serveroperativsystemer

NB: meget få embedded systemer har beskyttelse!

## Drive-by download

---

From Wikipedia, the free encyclopedia

**Drive-by download** means three things, each concerning the unintended [download of computer software from the Internet](#):

1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit [executable program](#), [ActiveX component](#), or [Java applet](#)). This is usually caused by poor security design [clarification needed]. The user should not be frequently asked to accept security-critical decisions, often with very limited knowledge and within limited time.
2. Any [download](#) that happens without a person's knowledge.
3. Download of [spyware](#), a [computer virus](#) or any kind of [malware](#) that happens without a person's knowledge.

Kan vi undvære Flash og PDF?

Kilde: [http://en.wikipedia.org/wiki/Drive-by\\_download](http://en.wikipedia.org/wiki/Drive-by_download)



Safari <http://clicktoflash.com/>

Firefox Extension Flashblock

Chrome extension called FlashBlock

Internet Explorer 8: IE has the Flash block functionality built-in so you don't need to install any additional plugins to be able to block flash on IE 8.

FlashBlock for Opera 9 - bruger nogen Opera mere?

FlashBlockere til iPad? iPhone? Android? - hvorfor er det ikke default?

# Er du passende paranoid?



Vær på vagt

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>:

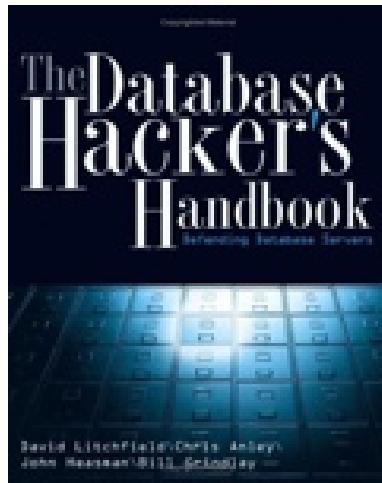
```
Set myRecordset = myConnection.execute  
("SELECT * FROM myTable  
WHERE someText ='" & request.form("inputdata") & "'")  
med input: ' exec master..xp_cmdshell 'net user test testpass /ADD' --  
modtager og udfører serveren:  
SELECT * FROM myTable  
WHERE someText ='' exec master..xp_cmdshell 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

– er kommentar i SQL

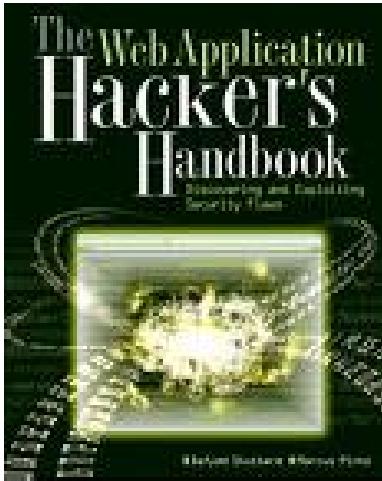
# Er SQL injection almindeligt?

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>

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

De udgav i 1995 så en softwarepakke med navnet SATAN *Security Administrator Tool for Analyzing Networks*

De forårsagede en del panik og furore, alle kan hacke, verden bryder sammen

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.

Kilde: <http://www.fish2.com/security/admin-guide-to-cracking.html>

SATAN og ideerne med automatiseret scanning efter sårbarheder blev siden ført videre i programmer som Saint, SARA

idag findes mange hackerværktøjer og automatiserede scannere

- Oprindeligt var det Unix scripts og tiger tools i 1990'erne
- idag har vi større pakker som Fyodor Nmap og Metasploit idag med god dokumentation

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	-::R	-::D	-::AUTHOR
2009-03-05	Winamp <= 5.541 Skin Universal Buffer Overflow Exploit	3128	R	D	SkD
2009-02-26	Coppermine Photo Gallery <= 1.4.20 (BBCode IMG) Privilege Escalation	7338	R	D	StAkeR
2009-02-25	Apple MACOS X xnu <= 1228.x Local Kernel Memory Disclosure Exploit	4111	R	D	mu-b
2009-02-23	Adobe Acrobat Reader JBIG2 Local Buffer Overflow PoC #2 0day	17652	R	D	Guido Landi
2009-02-23	MLdonkey <= 2.9.7 HTTP DOUBLE SLASH Arbitrary File Disclosure Vuln	4225	R	D	Michael Peselnik
2009-02-23	Multiple PDF Readers JBIG2 Local Buffer Overflow PoC	7781	R	D	webDEVIL
[ remote ]					
-::DATE	-::DESCRIPTION	-::HITS	-::R	-::D	-::AUTHOR
2009-03-05	SupportSoft DNA Editor Module (dnaedit.dll) Code Execution Exploit	1093	R	D	X Nine:Situations:Group
2009-03-04	Easy File Sharing Web Server 4.8 File Disclosure Vulnerability	1424	R	D	Stack
2009-03-04	EFS Easy Chat Server Authentication Request Buffer Overflow Exploit (pl)	969	R	D	Dr4sH
2009-03-04	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (fast)	3965	R	D	Ahmed Obied
2009-03-03	EFS Easy Chat Server (XSRF) Change Admin Pass Vulnerability	1215	R	D	Stack
2009-03-03	Imera ImeraIEPlugin ActiveX Control Remote Code Execution Exploit	1020	R	D	Elazar
[ local ]					
-::DATE	-::DESCRIPTION	-::HITS	-::R	-::D	-::AUTHOR
2009-03-05	Media Commands (.m3u File) Universal SEH Overwrite Exploit	669	R	D	His0k4
2009-03-05	Media Commands .m3l File Local Buffer Overflow Exploit	621	R	D	Stack

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



The screenshot shows the homepage of The Exploit Database. At the top, there's a banner with the word "EXPLOIT" in large letters, where each letter has a different background color. Below the banner, it says "D a t a b a s e". To the right, there's a counter that says "Currently Archiving 10343 Exploits". A navigation bar below the banner includes links for home, news, remote, local, web, dos, shellcode, papers, search, D, submit, and rss.

**The Exploit Database**

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.

We are running a general cleanup on the DB and have changed our submission policy - please [check it out](#) before submitting exploits to us.

Due to recent DOS attacks, our application downloads are now captcha protected.

## Remote Exploits

Date	D	A	V	Description	Plat.	Author
2010-01-27	D	A	✓	CamShot v1.2 SEH Overwrite Exploit	windows	technik
2010-01-25	D	-	✓	AOL 9.5 Phobos.Playlist 'Import()' Buffer Overflow Exploit (Meta)	windows	Trancer
2010-01-22	D	A	✓	IntelliTamper 2.07/2.08 (SEH) Remote Buffer Overflow	windows	loneferret
2010-01-21	D	-	✓	EFS Easy Chat server Universal BOF-SEH (Meta)	windows	FB1H2S
2010-01-20	D	-	✓	AOL 9.5 ActiveX 0day Exploit (heap spray)	windows	Dz_attacker
2010-01-19	D	-	✓	Pidgin MSN <= 2.6.4 File Download Vulnerability	multiple	Mathieu GASPARD
2010-01-18	D	A	✓	Exploit EFS Software Easy Chat Server v2.2	windows	John Babio

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

## 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/>

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!
- Sikkerhed kommer fra langsigtede intiativer
- Hvad er informationssikkerhed?
- Data på elektronisk form
- Data på fysisk form
- Drop legacy kompatibilitet

**Informationssikkerhed er en proces**

## 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



PROSA afholdt fredag 17. september - til lørdag 18. september Capture the Flag  
Distribueret CTF med 6 hold og arrangørerne i Aalborg  
Sjovt og lærerigt - gentages helt sikkert

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

Get ready! Lær debuggere og scripting sprog at kende, start på at hacke

Henrik Lund Kramshøj  
[hlk@solido.net](mailto:hlk@solido.net)

<http://www.solidonetworks.com>

You are always welcome to send me questions later via email

## 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.