Welcome to

# Krimihacking - fakta eller fiktion?

PROSA

Henrik Lund Kramshøj
mailto:hlk@security6.net hlk@security6.net

http://www.security6.net

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Formålet med foredraget

Lære om hacking

Almindelige myter om hacking

Sandheder indenfor hacking, hvad kan reelt lade sig gøre

Sjov ☺

# Hacker - cracker

**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 2009 Security6.net, Henrik Lund Kramshøj

# Definition af hacking, oprindeligt

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

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

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

Benyttes stadig i visse sammenhænge

Idag vil vi ikke diskutere etik men blot snakke teknik

# Aftale om test af netværk

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

Hacking kan betyde:

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

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Hackerværktøjer

Security6.net

Der benyttes en del værktøjer:

- BackTrack http://www.remote-exploit.org/backtrack.html
- nmap - http://nmap.org portscanner + Nmap bogen online og hardcopy!
- Metasploit Framework http://www.metasploit.com/ for creating security tools and exploits
- Wireshark - http://http://wireshark.org/ avanceret netværkssniffer
- OpenBSD - http://openbsd.org operativsystem med fokus på sikkerhed
- OpenSSH - http://openssh.org sikker terminaladgang og filoverførsel, FTP DØ!
- Putty - http://www.chiark.greenend.org.uk/ sgtatham/putty/download.html terminal emulator med indbygget SSH primært til Windows

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# BackTrack - all in one hackerdistribution

Apropos insane downloads - there have been 2,482,000+ downloads of BT3 iso and 1,575,000+ downloads of the BT3 VM since they came out. Yes, thats ”millions”. Ph33r.

BackTrack er en LiveCD med +300 tools som er vokset til en Linux distribution

BT4 er pt. i beta, men udleveres aligevel, få en kopi via HTTP lokalt eller via USB stick

BackTrack hjemmeside http://www.remote-exploit.org/backtrack.html

BackTrack blog http://backtrack4.blogspot.com/

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Hacking er magi

Hacking ligner indimellem magi

# Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

© copyright 2009 Security6.net, 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 2009 Security6.net, Henrik Lund Kramshøj

# Myten om MAC filtrering

Eksemplet med MAC filtrering er en af de mange myter

Hvorfor sker det?

Marketing - producenterne sætter store mærkater på æskerne

Manglende indsigt - forbrugerne kender reelt ikke koncepterne

Hvad *er* en MAC adresse egentlig

Relativt få har forudsætningerne for at gennemskue dårlig sikkerhed

Løsninger?

Udbrede viden om usikre metoder til at sikre data og computere

Udbrede viden om sikre metoder til at sikre data og computere

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# MAC filtrering

# Hvad skal der ske?

Tænk som en hacker

Rekognoscering

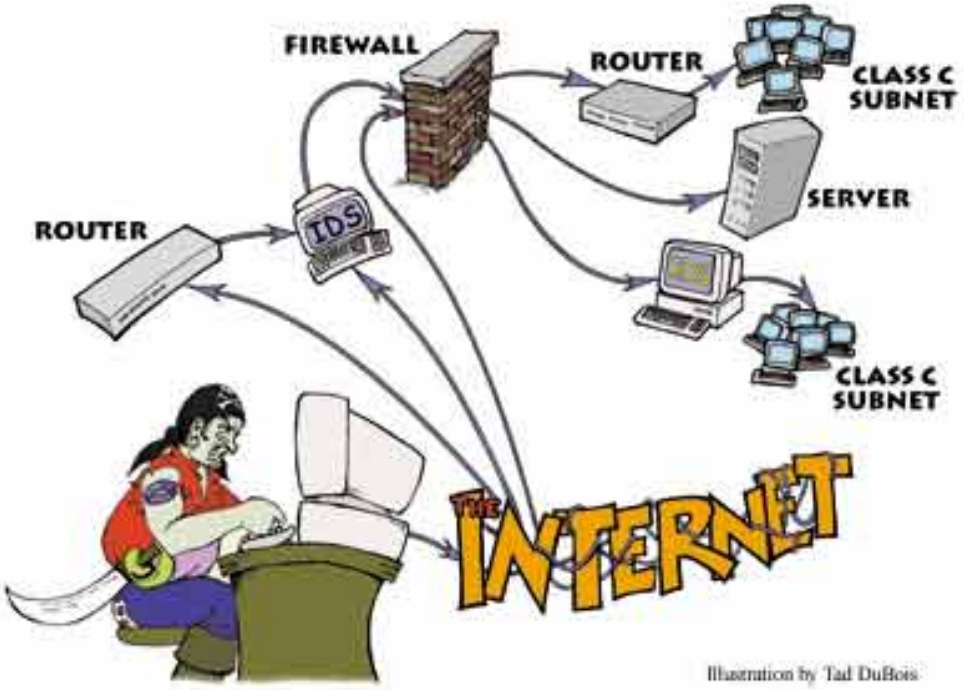
- ping sweep, port scan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

Udnyttelse/afprøvning: exploit programs

Jeg bruger lige BackTrack

- lytte efter trådløse netværk, se http://aircrack-ng.org
- opsnappe traffik, se http://www.wireshark.org

# Er sikkerhed interessant?

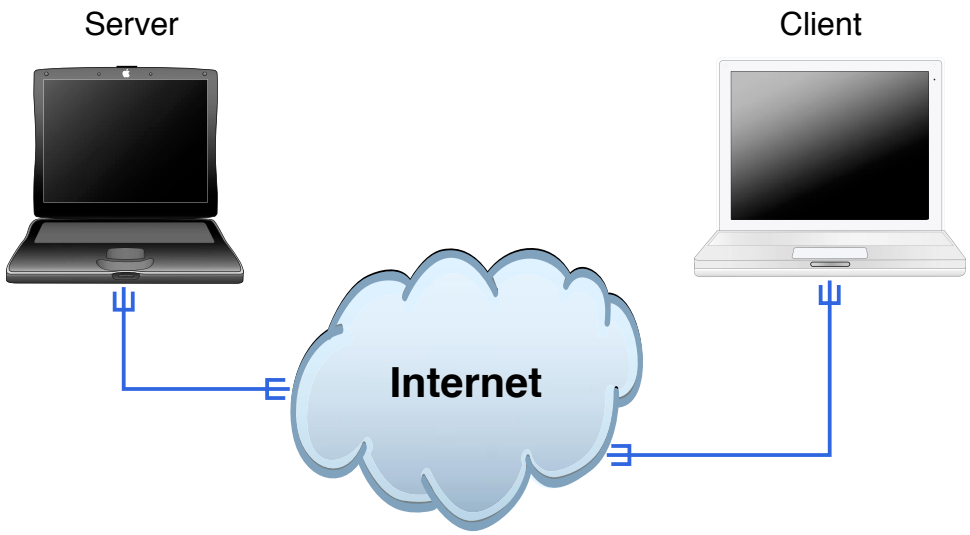



Sikkerhedsproblemerne i netværk er mange

Mange services - mange sårbare services

Alle er et mål - du har ressourcer maskine, IP og diskplads

# Internet og computere idag




Klienter og servere idag, enkeltstående computere tidligere

Centrale og stationære, bærbare og håndholdte idag

Rødder i akademiske miljøer, 20 år gamle protokoller

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

*Alt er forbundet*, ok ikke helt sandt men desværre tæt på

# 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 2009 Security6.net, Henrik Lund Kramshøj

# dsniff

en sniffer til mange usikre protokoller

inkluderer **arpspoof**

Lavet af Dug Song, dugsong@monkey.org

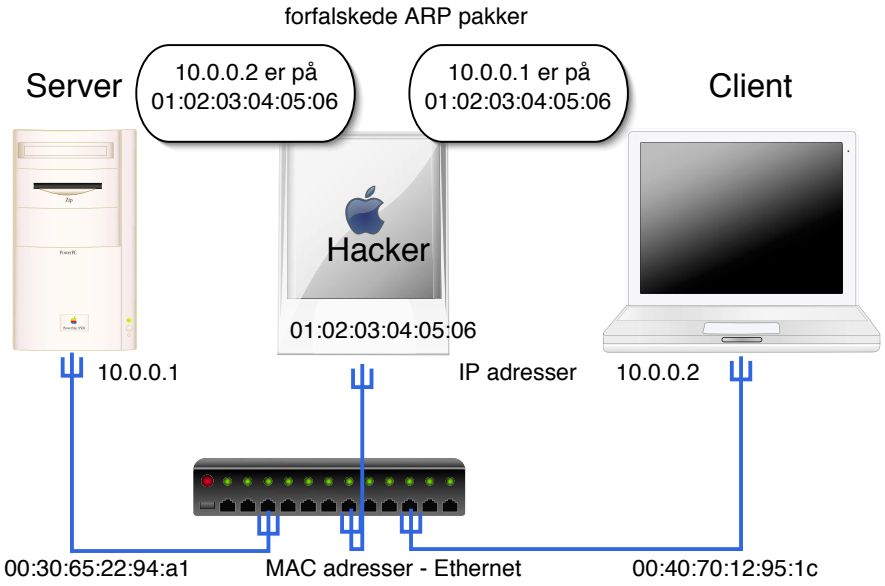
```
dsniff is a password sniffer which handles FTP, Telnet,
SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin,
RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11,
CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker,
Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft
SMB, Oracle SQL*Net,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

© copyright 2009 Security6.net, 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



# 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

# 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/

# Hvad er en firewall

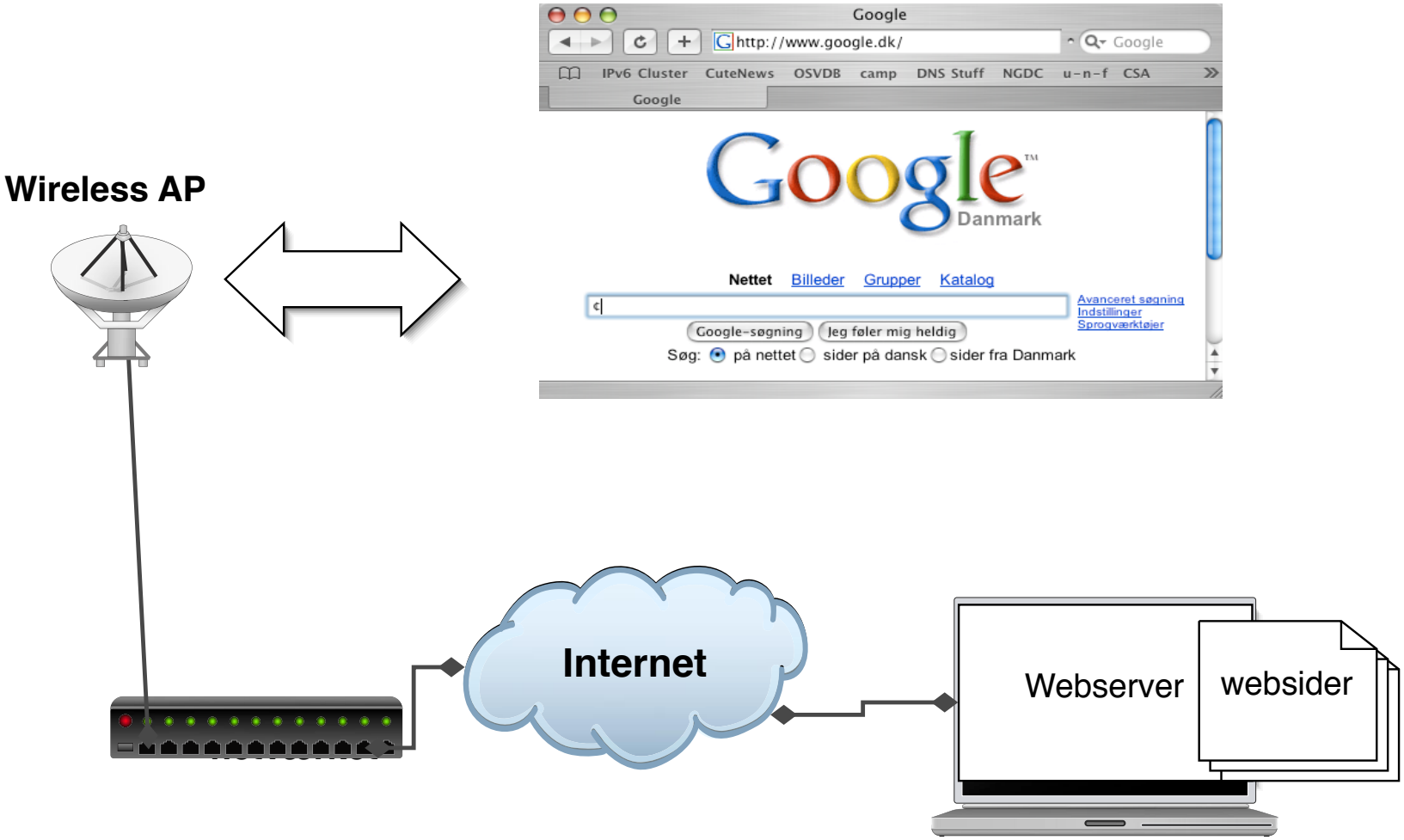
Lad os starte med noget alle kender

En firewall er noget som blokerer traffik på Internet

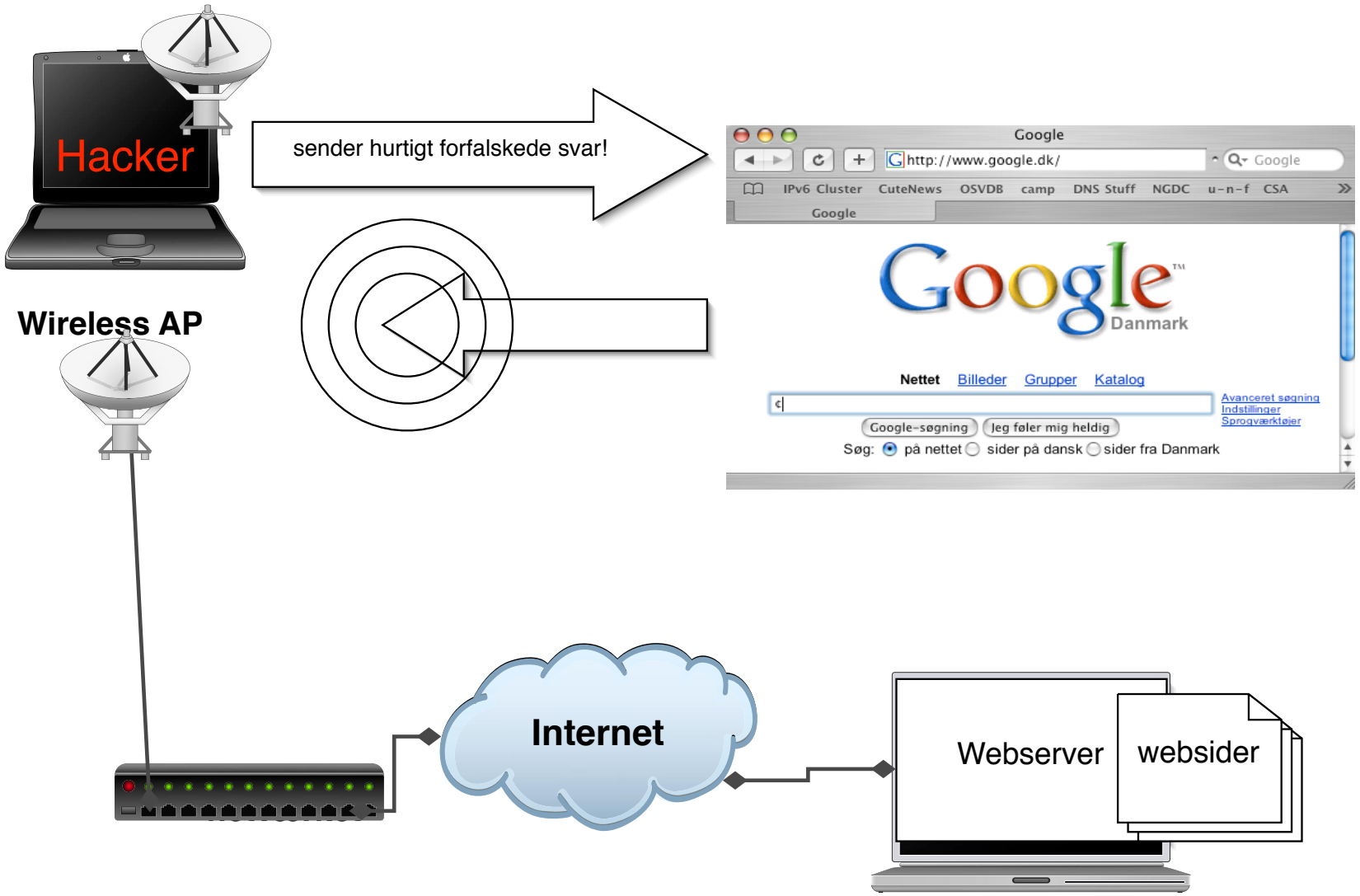
- En firewall er noget som tillader traffik på Internet

Myte: en firewall beskytter mod alt

# Normal WLAN brug



# Packet injection - airpwn



# Airpwn teknikker

Klienten sender forespørgsel

Hackerens program airpwn lytter og sender så falske pakker

Hvordan kan det lade sig gøre?

- Normal forespørgsel og svar på Internet tager 50ms
- Airpwn kan svare på omkring 1ms angives det
- Airpwn har alle informationer til rådighed

Airpwn på Defcon 2004 - findes på Sourceforge
http://airpwn.sourceforge.net/

NB: Airpwn som demonstreret er begrænset til TCP og ukrypterede forbindelser

Det vil være trivielt at introducere skadelig kode ad denne vej

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Myten om firewalls

Security .net

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 2009 Security6.net, Henrik Lund Kramshøj

# Hvorfor virkede airpwn?

Airpwn programmet virkede ved at sniffe og indsætte falske beskeder

Sniffere findes i mange versioner:

- Dsniff - proof of concept program afkodning af dårlige protokoller
  Sjovt nok benyttes mange af disse idag, og nye protokoller er ofte uden kryptering, why, why, **WHY!**
- Ettercap menustyret aflytning på netværk, Ethernet LAN - jeps, **switchede netværk er sårbare**
- Wireshark - afkodning af alle gængse protokoller

Packetstorm wireless tools http://packetstormsecurity.org/wireless/

*Beginner's Guide to Wireless Auditing* David Maynor
http://www.securityfocus.com/infocus/1877?ref=rss

# Mulige løsninger

Krypter trafikken
Hvad skal krypteres og hvordan?

Du kan kryptere netværket
WLAN delen, eksempelvis med WPA

Du kan kryptere dele eller al din traffik
VPN hvor alle dine data sendes hjem og derfra videre til internet

Du kan kryptere bestemte forbindelser
Websider med følsomme data, netbanken med HTTPS
Posten med dine e-mails, POP3 over SSL, IMAP over SSL

Du kan kryptere bestemte beskeder
Post med PGP Pretty Good Privacy

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Kryptering

Lisbeth Salander bruger PGP, men er det sikkert?

Jeg bruger PGP ☺

Politiet bruger det vist ikke liiiige, FTP er godt nok ...

# Formålet med kryptering

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

# Kryptering i praksis

## Kryptering af e-mail

- Pretty Good Privacy - Phil Zimmermann
- GNU Privacy Guard - Open Source implementation af OpenPGP
- OpenPGP = mail sikkerhed, OpenPGP RFC-2440, PGP/MIME RFC 3156)

## Kryptering af sessioner SSL/TLS

- Secure Sockets Layer SSL / Transport Layer Services TLS
- krypterer data der sendes mellem webservere og klienter
- SSL kan bruges generelt til mange typer sessioner, eksempelvis POP3S, IMAPS, SSH m.fl.

## Kryptering af netværkstrafik - Virtual Private Networks VPN

- IPsec IP Security Framework, se også L2TP
- PPTP Point to Point Tunneling Protocol - dårlig og usikker, brug den ikke mere!
- OpenVPN m.fl.

© copyright 2009 Security6.net, 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

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Basale tools - PGP

- Pretty Good Privacy - PGP
- Oprindeligt udviklet af Phil Zimmermann
- nu kommercielt, men der findes altid en freeware version http://www.pgp.com
- Eksporteret fra USA på papir og scannet igen - det var lovligt
- I dag kan en masse information om PGP findes gennem: http://www.pgpi.org

# Basale tools - GPG

Gnu Privacy Guard, forkortes GnuPG eller GPG

brug linket: http://www.gnupg.org/

Open Source med GPL licens.

Kan bruges på alle de gængse operativsystemer

Sammen med Thunderbird Email programmet bruger man Enigmail plugin

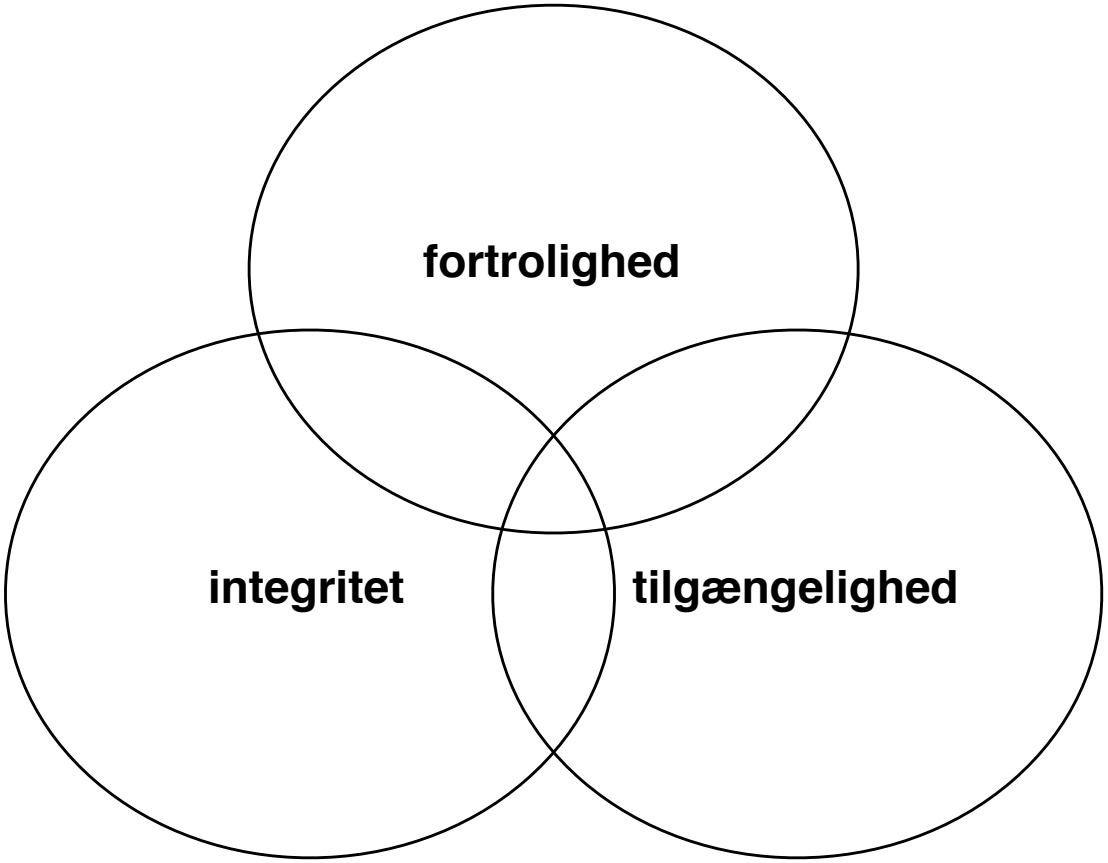
© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Problemet med kryptering

ingen garantier

- Vi håber at vores antagelser om at de matematiske problemer der skal løses er rigtige

# Confidentiality Integrity Availability




Husk altid de fundamentale principper indenfor sikkerhed

**Hvad** skal du beskytte mod **hvem**

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Encryption key length

**Encryption key lengths & hacking feasibility**

| *Type of Attacker* | *Budget* | Tool | *Time & Cost/Key 40 bit* | *Time & Cost/Key 56 bit* |
|---|---|---|---|---|
| Regular User | Minimal<br><br>$400 | Scavenged computer time<br><br>FPGA | 1 week<br><br>5 hours ($.08) | Not feasible<br><br>38 years ($5,000) |
| Small Business | $10,000 | FPGA [1] | 12 min.($.08) | 556 days ($5,000) |
| Corporate Department | $300,000 | FPGA<br><br>ASIC [2] | 24 sec. ($.08)<br><br>0.18 sec. ($.001) | 19 days ($5,000)<br><br>3 hours ($38) |
| Large Corporation | $10M | ASIC | 0.005 sec.($0.001) | 6 min. ($38) |
| Intelligence Agency | $300M | ASIC | 0.0002 sec.($0.001) | 12 sec. ($38) |

Kilde: http://www.mycrypto.net/encryption/encryption$_crack.html$

# Movie OS - cracking

Supercomputer!

Oh nooooes, he has encrypted the disk!

Let me just try this with my PDA!

It worxs! I am the haxx0r saving the w0rld!

Lad os lige prøve at knække noget kryptering

# WEP cracking - airodump og aircrack

airodump - opsamling af krypterede pakker

aircrack - statistisk analyse og forsøg på at finde WEP nøglen

Med disse værktøjer er det muligt at knække *128-bit nøgler*!

Blandt andet fordi det reelt er 104-bit nøgler ☺

tommelfingerregel - der skal vel opsamles ca. 50.000 pakker, mere er godt

Links:
http://www.cr0.net:8040/code/network/aircrack/ aircrack
http://www.securityfocus.com/infocus/1814 WEP: Dead Again

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# airodump afvikling

Når airodump kører opsamles pakkerne

samtidig vises antal initialisationsvektorer IV's:

| BSSID | CH | MB | ENC | PWR | Packets | LAN IP / # IVs | ESSID |
|---|---|---|---|---|---|---|---|
| 00:03:93:ED:DD:8D | 6 | 11 | | 209 | **801963** | **540180** | wanlan |

NB: dataopsamlingen er foretaget på 100% opdateret Mac udstyr

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# aircrack - WEP cracker

```
$ aircrack -n 128 -f 2 aftendump-128.cap
                                aircrack 2.1
* Got  540196! unique IVs | fudge factor = 2
* Elapsed time [00:00:22] | tried 12 keys at 32 k/m
KB    depth   votes
 0    0/  1   CE(  45) A1(  20) 7E(  15) 98(  15) 72(  12) 82(  12)
 1    0/  2   62(  43) 1D(  24) 29(  15) 67(  13) 94(  13) F7(  13)
 2    0/  1   B6( 499) E7(  18) 8F(  15) 14(  13) 1D(  12) E5(  10)
 3    0/  1   4E( 157) EE(  40) 29(  39) 15(  30) 7D(  28) 61(  20)
 4    0/  1   93( 136) B1(  28) 0C(  15) 28(  15) 76(  15) D6(  15)
 5    0/  2   E1(  75) CC(  45) 39(  31) 3B(  30) 4F(  16) 49(  13)
 6    0/  2   3B(  65) 51(  42) 2D(  24) 14(  21) 5E(  15) FC(  15)
 7    0/  2   6A( 144) 0C(  96) CF(  34) 14(  33) 16(  33) 18(  27)
 8    0/  1   3A( 152) 73(  41) 97(  35) 57(  28) 5A(  27) 9D(  27)
 9    0/  1   F1(  93) 2D(  45) 51(  29) 57(  27) 59(  27) 16(  26)
10    2/  3   5B(  40) 53(  30) 59(  24) 2D(  15) 67(  15) 71(  12)
11    0/  2   F5(  53) C6(  51) F0(  21) FB(  21) 17(  15) 77(  15)
12    0/  2   E6(  88) F7(  81) D3(  36) E2(  32) E1(  29) D8(  27)
```

**KEY FOUND! [ CE62B64E93E13B6A3AF15BF5E6 ]**

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Hvor lang tid tager det?

Opsamling a data - ca. en halv time på 802.11b ved optimale forhold

Tiden for kørsel af aircrack på en VIA CL-10000 1GHz CPU med almindelig disk OpenBSD:

```
25.12s real     0.63s user     2.14s system
```

Idag snakker vi få minutter med 802.11g og moderne algoritmer

# WPA cracking med Pyrit

*Pyrit* takes a step ahead in attacking WPA-PSK and WPA2-PSK, the protocol that today de-facto protects public WIFI-airspace. The project's goal is to estimate the real-world security provided by these protocols. Pyrit does not provide binary files or wordlists and does not encourage anyone to participate or engage in any harmful activity. **This is a research project, not a cracking tool.**

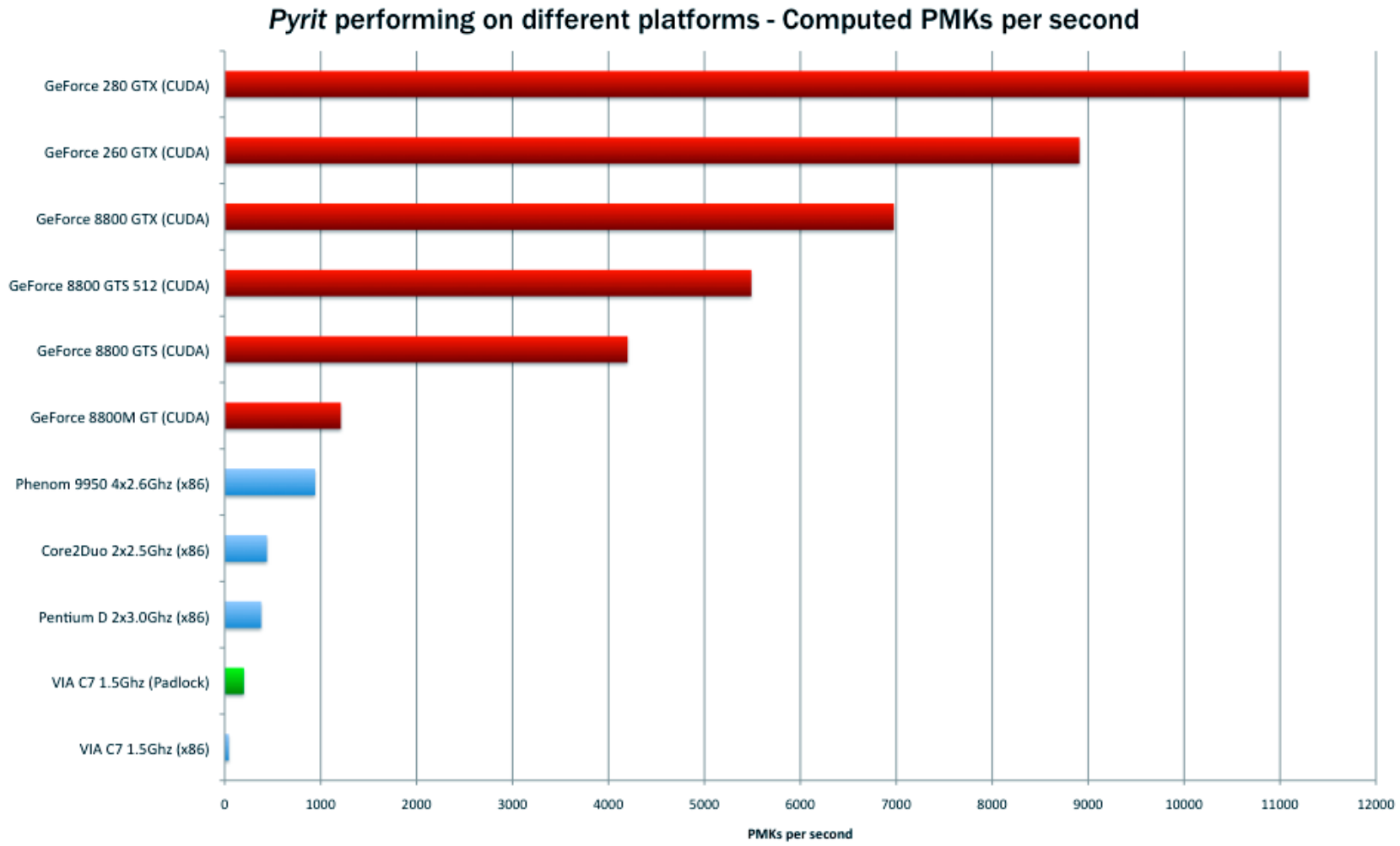
*Pyrit's* implementation allows to create massive databases, pre-computing part of the WPA/WPA2-PSK authentication phase in a space-time-tradeoff. The performance gain for real-world-attacks is in the range of three orders of magnitude which urges for re-consideration of the protocol's security. Exploiting the computational power of GPUs, *Pyrit* is currently by far the most powerful attack against one of the world's most used security-protocols.

sloooow, plejede det at være - 150 keys/s på min Thinkpad X31

Kryptering afhænger af SSID! Så check i tabellen er minutter.

http://pyrit.wordpress.com/about/

# Tired of WoW?




Kilde: http://code.google.com/p/pyrit/

# Kryptografiske principper

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

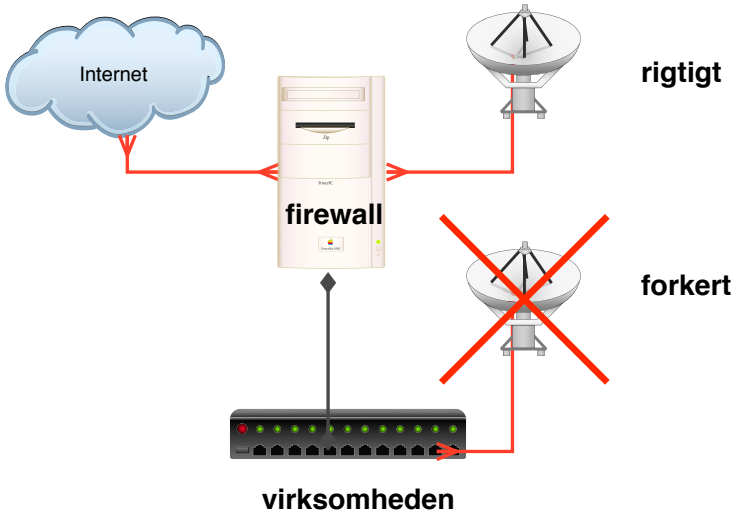
Et successfuldt angreb på en krypto-algoritme er enhver genvej som kræver mindre arbejde end en gennemgang af alle nøglerne

Nye algoritmer, programmer, protokoller m.v. skal gennemgås nøje!

Se evt. Snake Oil Warning Signs: Encryption Software to Avoid
http://www.interhack.net/people/cmcurtin/snake-oil-faq.html

© copyright 2009 Security6.net, Henrik Lund Kramshøj

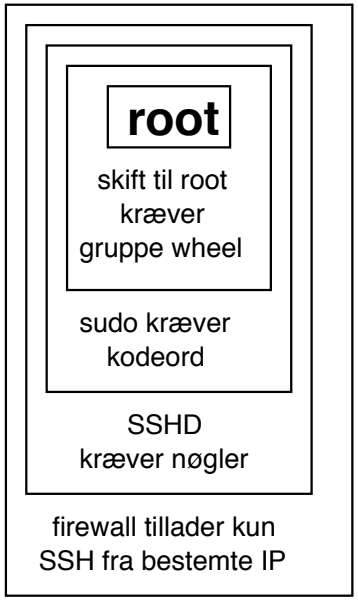
# Anbefalinger mht. trådløse netværk




- Brug noget tilfældigt som SSID - netnavnet
- Brug ikke WEP til virksomhedens netværk
  - men istedet en VPN løsning med individuel autentificering eller WPA
- NB: WPA Personal/PSK kræver passphrase på +40 tegn!
- Skift til WPA2 Personal, WPA Enterprise eller WPA2 Enterprise
- Placer de trådløse adgangspunkter hensigtsmæssigt i netværket - så de kan overvåges
- Lav et sæt regler for brugen af trådløse netværk - hvor må medarbejdere bruge det?
- Se eventuelt pjecerne *Beskyt dit trådløse Netværk* fra Ministeriet for Videnskab, Teknologi og Udvikling http://www.videnskabsministeriet.dk/

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Når adgangen er skabt




Så går man igang med de almindelige værktøjer

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

Forsvaret er som altid - flere lag af sikkerhed!

© copyright 2009 Security6.net, 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

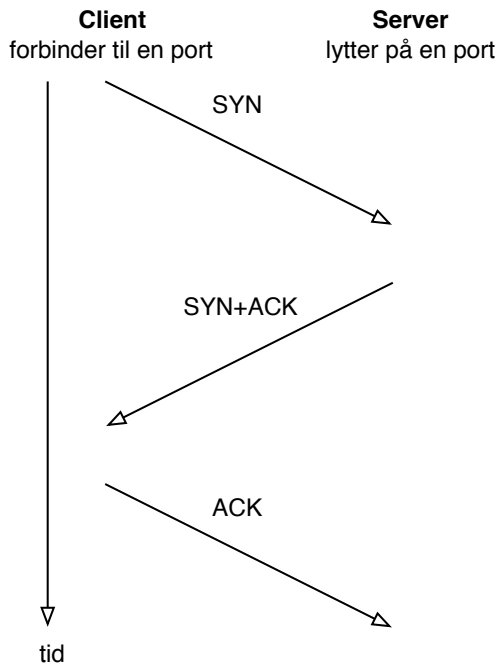
TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

© copyright 2009 Security6.net, 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 2009 Security6.net, Henrik Lund Kramshøj

# Ping og port sweep

scanninger på tværs af netværk kaldes for sweeps

Scan et netværk efter aktive systemer med PING

Scan et netværk efter systemer med en bestemt port åben

Er som regel nemt at opdage:

- 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 2009 Security6.net, 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
```

# 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
```

# 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

# Myte: den bedste teknologi kan redde dig

Ingen kryptering kan redde dig fra dårlige passwords!

Folk vælger dårlige kodeord - inkl. mig.

Systemer skal kræve komplekse kodeord

Klassisk eksempel er det danske politi der ”knækkede SafeGuard Easy”

De gættede kodeord, brød ikke krypteringen

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Myte: kodeord på bærbare beskytter data

Myten:

man tror at et kodeord på en bærbar beskytter data

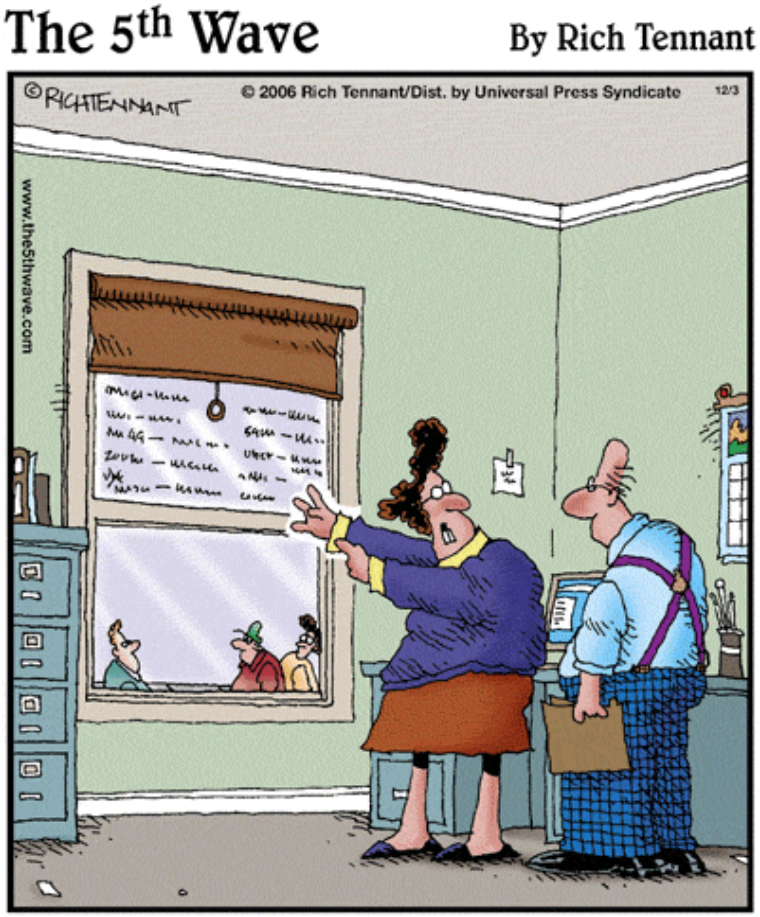
Sandhed:

I praksis er det kun en mindre gene

Windows password skjuler ikke data på harddisken

Ligeså på Unix

# Opbevaring af passwords




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

# Single user mode boot

Unix systemer tillader ofte boot i singleuser mode
hold command-s nede under boot af Mac OS X

Bærbare tillader typisk boot fra CD-ROM
hold c nede på en Mac

Mac computere kan i nogle tilfælde være firewire diske
hold t nede under boot

Harddisken kan typisk nemt fjernes fra en bærbar

Fysisk adgang til systemet - **game over**

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Harddisk kryptering

Et værn mod fysisk adgang er harddisk kryptering

Eksempler på software er:

- PGP disk encryption
- Utimaco SafeGuard Easy
- Mac OS X FileVault, kryptering af hjemmekatalog

Det er nemt at komme igang med, og ikke specielt dyrt - hverken i penge eller ressourcer

NB: husk at holde softwaren opdateret og husk backup

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# harddisk beskyttelse og data kryptering

Kryptering findes i alle de gængse klient operativsystemer

- Microsoft Windows 2000 EFS Encrypting Filesystem - kryptering af filer
- Apple Mac OS X - krypterer nemt hjemmekataloget for en bruger med FileVault
- FreeBSD GEOM og GBDE - giver mulighed for at kryptere enheder generelt
- PGP disk - Pretty Good Privacy - laver en virtuel krypteret disk
- Nogle producenter har kodeord på disken - IBM harddisk BIOS kodeord

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Pyha, så er vi vel sikre med harddisk kryptering

DMA adgang via FireWire
FireWire gav tidligere DMA adgang til at læse al memory, uden restriktioner

Ruxcon, Firewire, DMA & Windows, Winlockpwn
http://www.storm.net.nz/projects/16

Jeg prøvede at læse memory fra en iBook og vupti, på relativt få sekunder havde man et image!

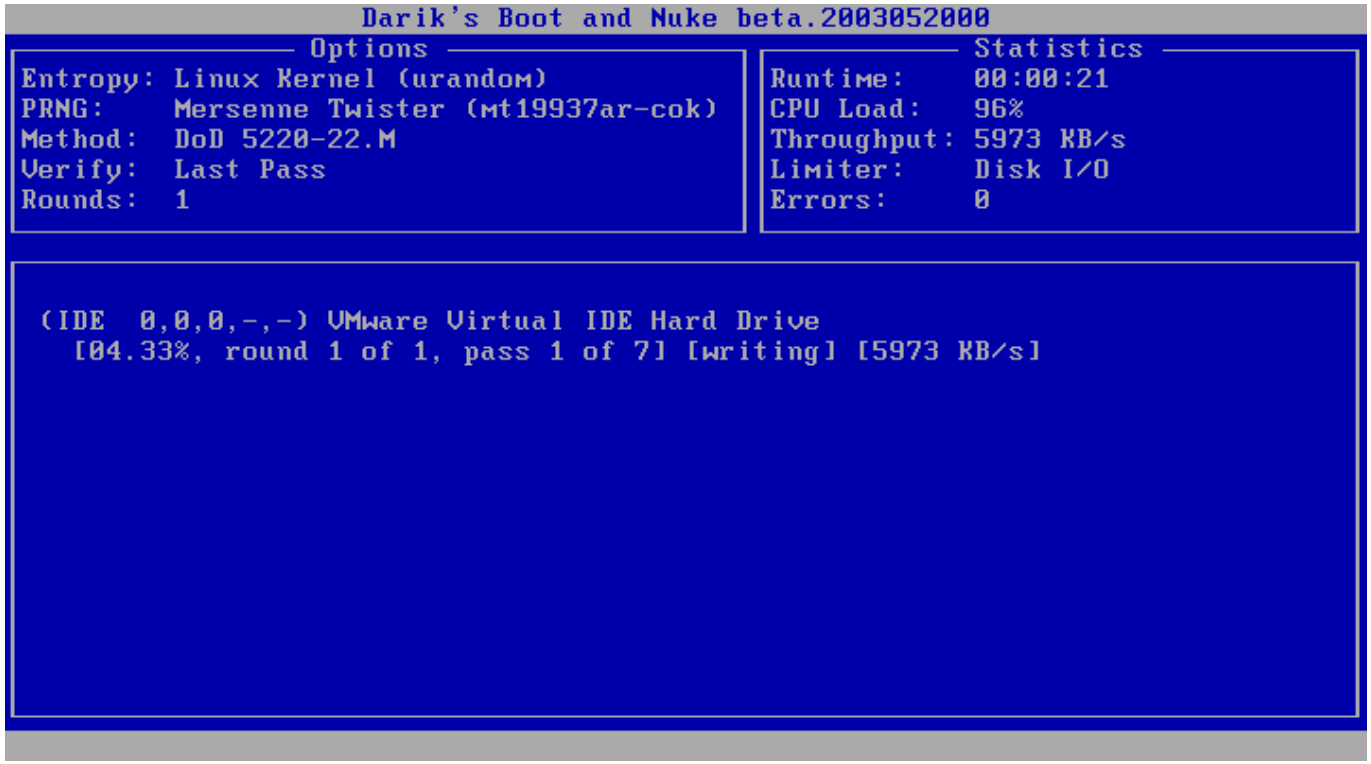
Fjernelse af memory - men data bevaret og kan aflæses
Lest We Remember: Cold Boot Attacks on Encryption Keys
http://citp.princeton.edu/memory/
- bliver det mere hollywood?

Så måske skal du bruge harddisk kryptering OG lukke ned efter brug?

pssst husk også VileFault!

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# ... og husk sletning




Bortskaffelse af data

Sletning med sletteprogrammer

Darik's Boot and Nuke ("DBAN") http://www.dban.org/

# Tid til en demo

Target: Macbook disken

Press t to enter ☺

# Definition

Computer Forensics involves the preservation, identification, extraction, documentation and interpretation of computer data.

*Computer Forensics: Incident Response Essentials*, Warren G. Kruse II og Jay G. Heiser, Addison-Wesley, 2002

# TASK og Autopsy

Inspireret af TCT har Brian Carrier fra Atstake lavet flere værktøjer til forensics analyse

Det officielle hjem for TASK og autopsy er nu: www.sleuthkit.org

TASK kan betragtes som en erstatning for TCT the coroners toolkit lavet af Dan Farmer og Wietse Venema

Autopsy er en Forensic Browser - et interface til TASK

# Myten: Bare du bruger harddisk kryptering så er du sikker

Myten:

man tror at blot fordi man har installeret harddisk kryptering er man sikker

Sandhed:

I praksis er det meget afhængigt af den valgte teknologi

Kodeordet til krypteringen bliver essentielt

Vælg gode kodeord!

Jeg bruger selv en Keychain.app applikation på Mac OS X til at gemme koder

Brug selvfølgelig ikke samme kodeord på hotmail og din PGP key ;-)

© copyright 2009 Security6.net, Henrik Lund Kramshøj

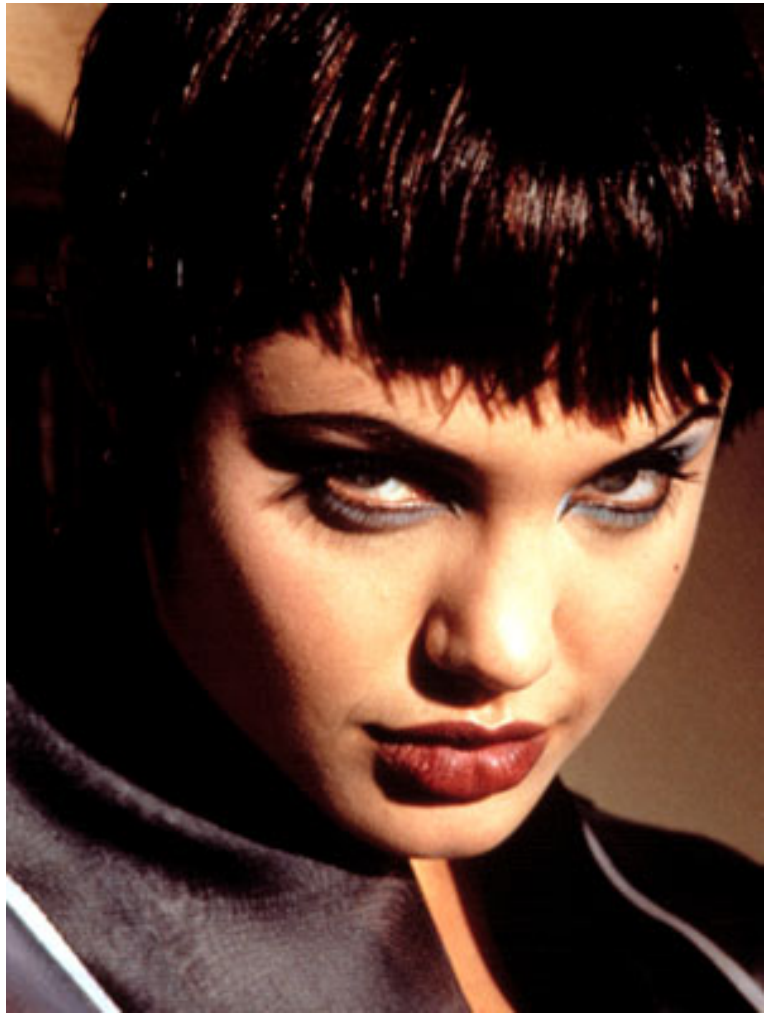
# Opsummering - hidtil

Firewalls er nødvendige, men pas på trojanere og virus aligevel

Brug kryptering og vælg algoritmer og produkter med omhu

og husk så at vælge gode passwords!

# Hackertyper anno 1995



# Hackertyper anno 2008

Lisbeth laver PU, personundersøgelser ved hjælp af hacking

Hvordan finder man information om andre

# Fra mønstre til person

Først vil vi finde nogle mønstre

Derefter vil vi søge med de mønstre

Nogle giver direkte information

Andre giver baggrundsinformation

Hvad er offentligt og hvad er privat? (googledorks!)

# Eksempler på mønstre

Navn, fulde navn, fornavne, efternavne, alias'es

Diverse idnumre, som CPR - tør du søge på dit CPR nr?

Computerrelaterede informationer: IP, Whois, Handles

Øgenavne, kendenavne

Skrivestil, ordbrug mv.

Tiden på din computer?

Tænk kreativt ☺

# Hvor finder du informationerne

Email

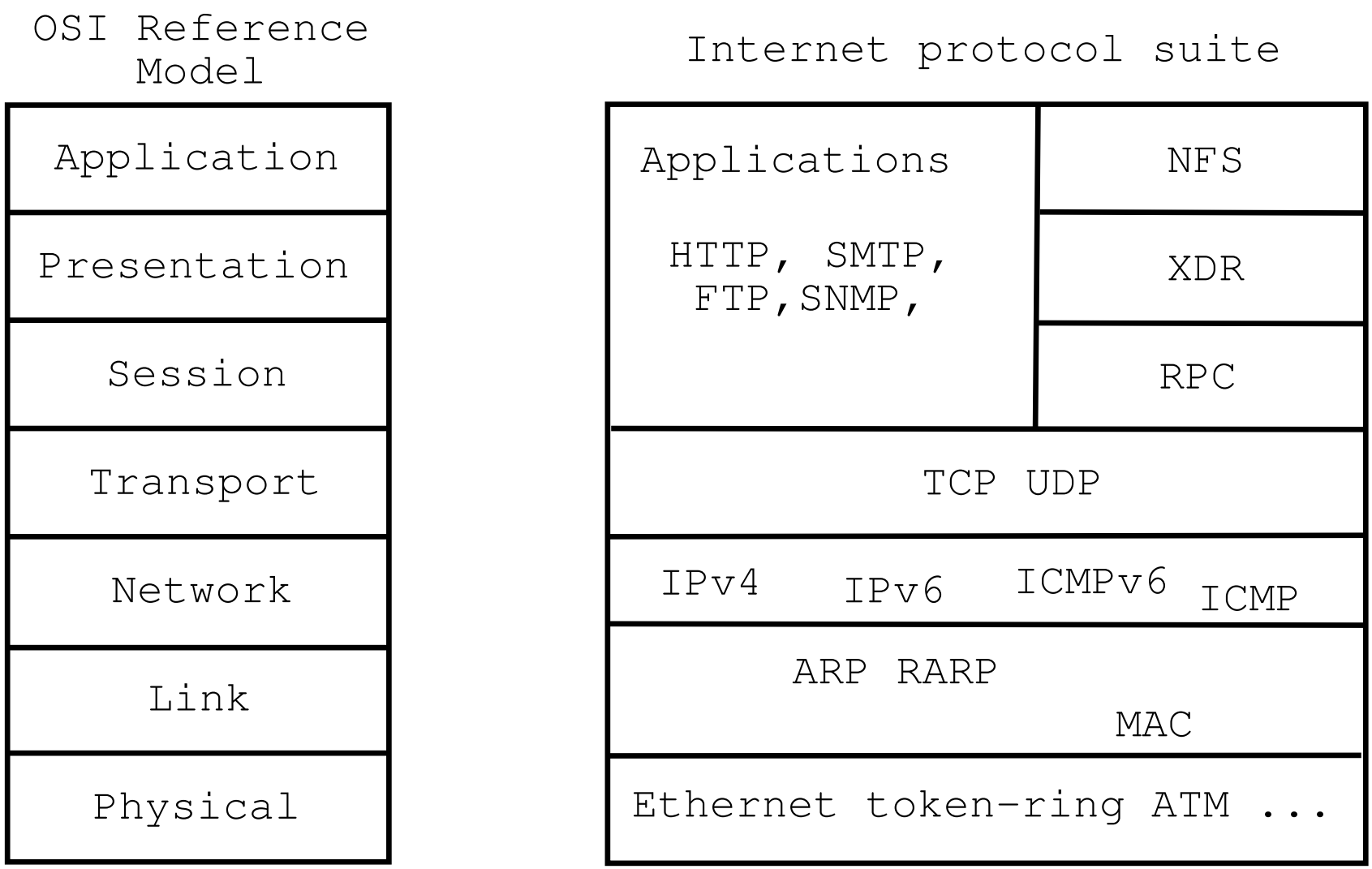
DNS

Gætter

Google

Alt hvad du ellers har adgang til - eller som Lisbeth tilraner sig adgang til

# OSI og Internet modellerne



# 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

# 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 2009 Security6.net, 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 2009 Security6.net, Henrik Lund Kramshøj

# traceroute

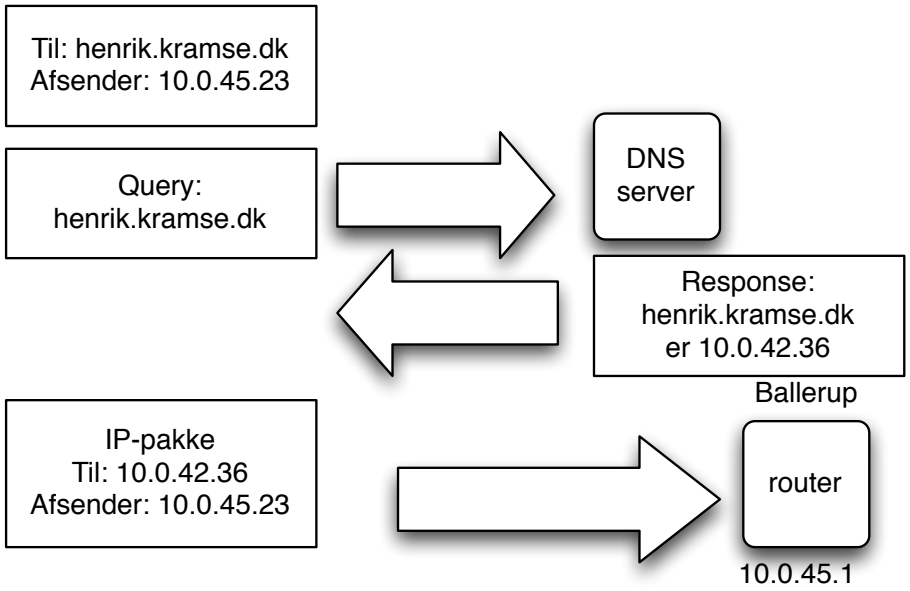
traceroute programmet virker ved hjælp af TTL

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
```

# 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

# DNS systemet

navneopslag på Internet

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

UNIX: /etc/hosts

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

Eksempel: www.security6.net har adressen 217.157.20.131

skrives i database filer, zone filer

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

# Mere end navneopslag

Security .net

består af resource records med en type:

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

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

# 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

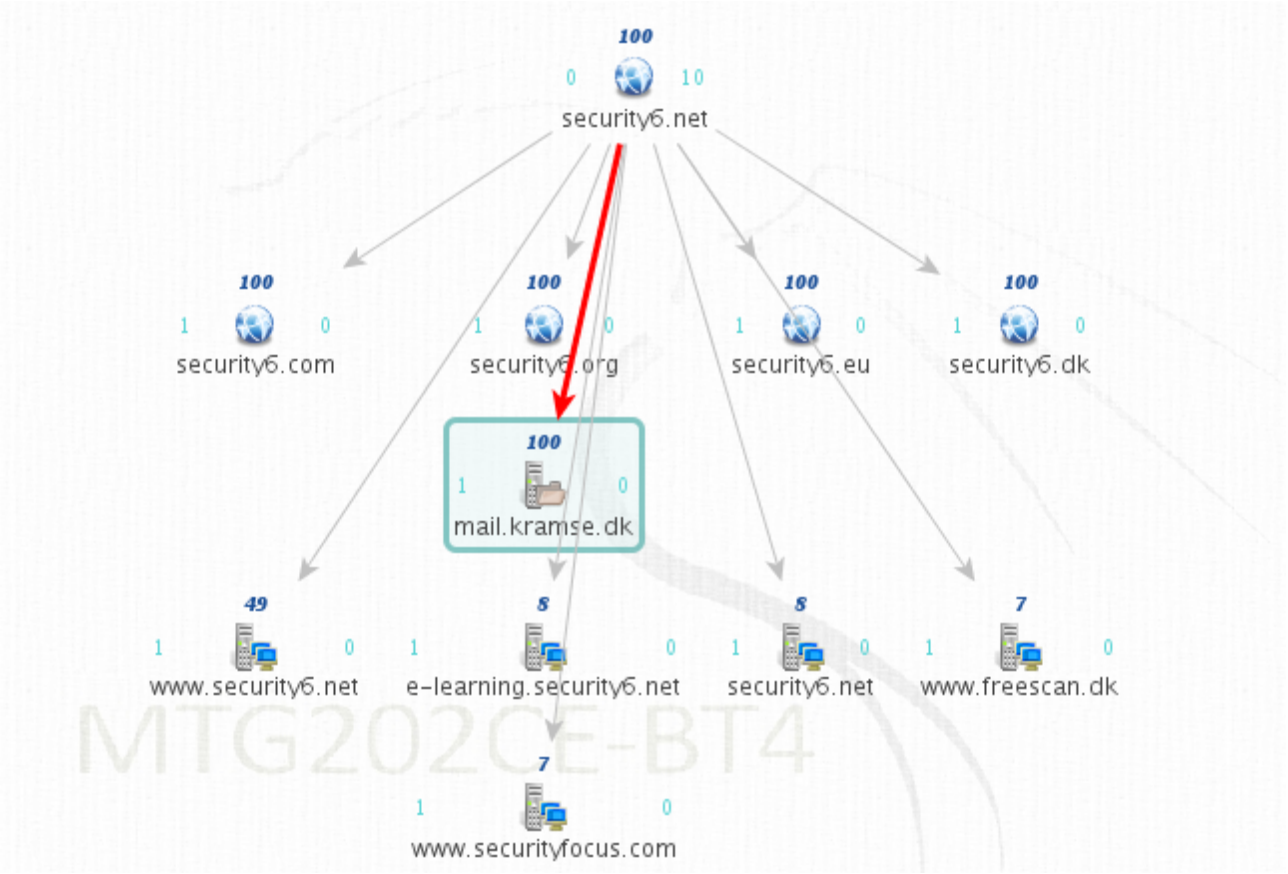
disse fire kaldes for Regional Internet Registries (RIRs) i modsætning til Local Internet Registries (LIRs) og National Internet Registry (NIR)

# Google for it

Google som hacker værktøj?

Googledorks http://johnny.ihackstuff.com/

# Listbeth in a box?




BT4 udgaven, kommerciel udgave på http://www.paterva.com/maltego/

# Er du passende paranoid?

Vær på vagt

# The bad stuff - breaking in

Hvordan bryder man ind?

Det kan ske på mange måder:

- e-mail trojaner/keylogger forklædt som spam
- drive-by-hacking, på websider - evt. a la airpwn
- introduktion af fysiske enheder, fysisk keylogger
- direkte fysiske angreb, *bag jobs*

Definitioner

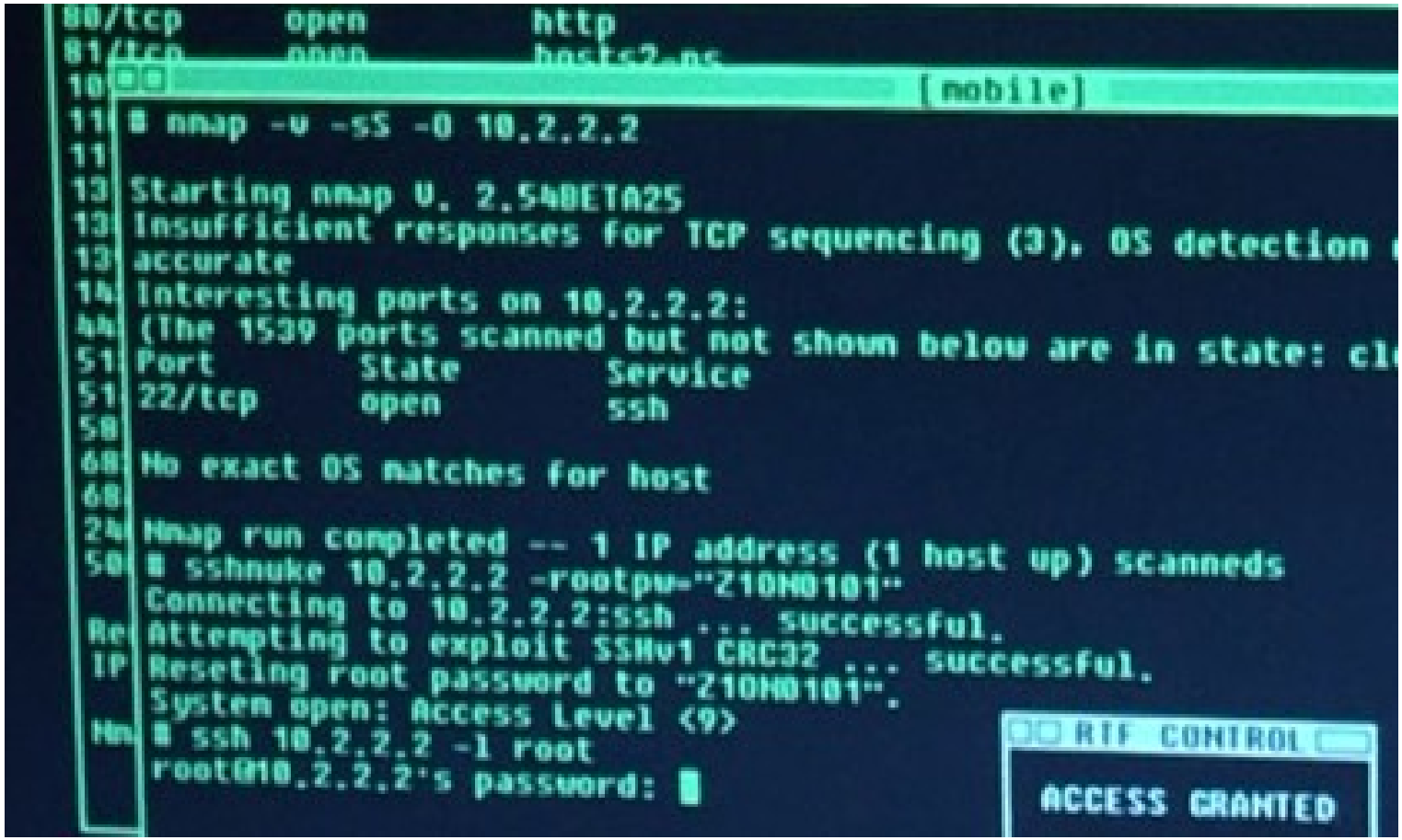
- trojaner program der udgiver sig for at være noget andet, eksempelvis et spil, men installerer en keylogger
- keylogger logger tastetryk, fysiske enheder eller software
- root kit, software der skjuler sig og ændrer systemet
- malware, skadelig software herunder ovenstående, virus og orme m.v.

Bonusspørgsmål: finder anti-virusprogrammerne en one-off custom virus/trojaner?

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Matrix style hacking anno 2003

# Trinity breaking in




http://nmap.org/movies.html
Meget realistisk http://www.youtube.com/watch?v=Zy5$_gYu_isg$

# buffer overflows et C problem

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

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

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Exploits - udnyttelse af sårbarheder

exploit/exploitprogram er

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

Eksempel:

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

# local vs. remote exploits

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

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

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

# Hvordan laves et buffer overflow?

Findes ved at prøve sig frem

- black box testing
- closed source
- reverse engineering

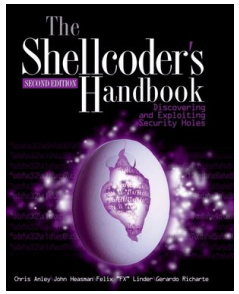
Ved Open source Findes de typisk ved at læse/analysere koden

- RATS
- flere andre

Virker typisk mod specifikke versioner

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

# Buffer overflows




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

*Smashing The Stack For Fun And Profit* Aleph One

*Writing Buffer Overflow Exploits with Perl - anno 2000*

Følgende bog kan ligeledes anbefales: *The Shellcoder's Handbook : Discovering and Exploiting Security Holes* af Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte 2nd Edition , John Wiley & Sons, august 2007

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/

# Metasploit

## 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!

# Gode operativsystemer

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/

# Diverse hackerværktøjer

Vi prøver et par af hackerværktøjerne, kunne være:

- Nikto, SSLScan, Nmap med scripts
- W3af
- Metasploit webudgaven
- OpenVAS
- Damn Vulnerable Linux - demo af en anden boot CD baseret på BackTrack

# 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

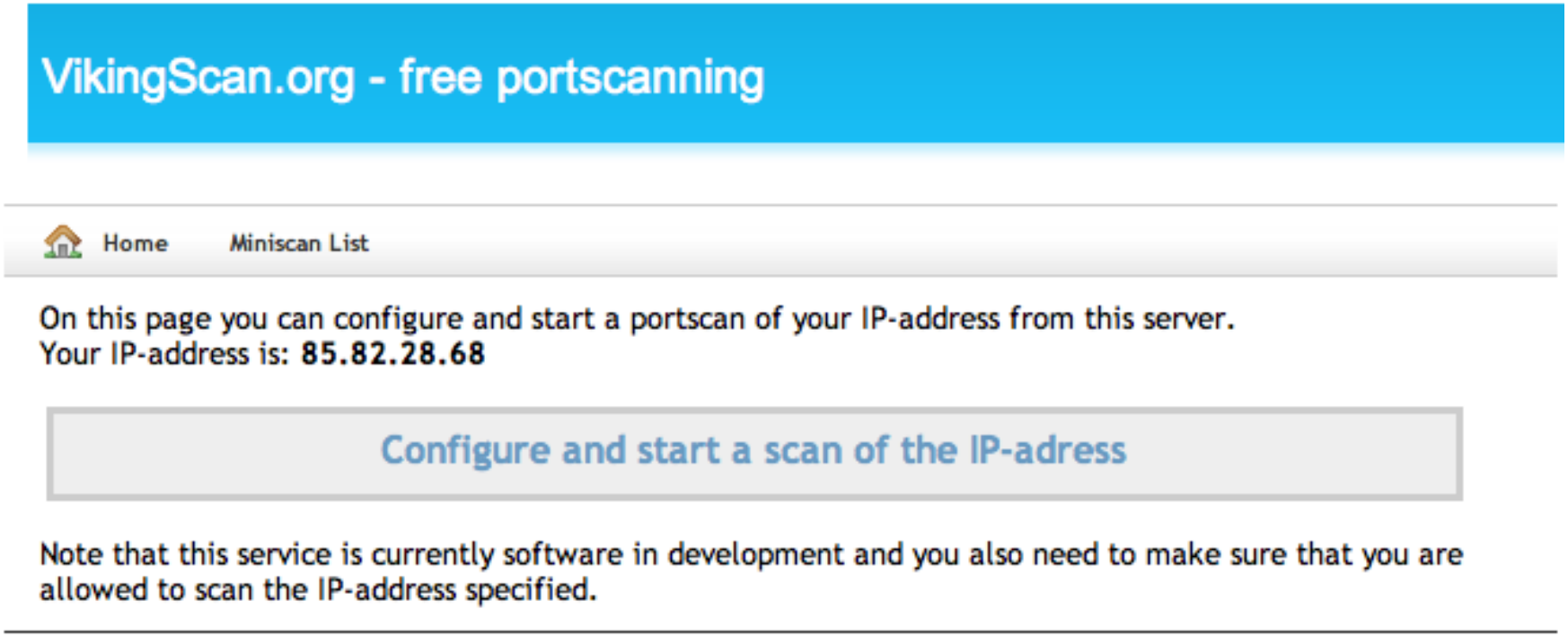
> We realize that SATAN is a two-edged sword - like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

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:

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

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

# VikingScan.org - gratis portscanning




http://www.vikingscan.org

# Diverse, som vi måske ikke når

Hvad med fysisk sikkerhed og telefonhacking, krokodillenæb rulez!!

VoIP sikkerhed, aflytning af telefonsamtaler i VoIP, helt sikkert interessant
http://www.voipsa.org/

Bluetooth sikkerhed, bluesniper, car whisperer

Lockpicking

Fast flux netværk

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Hvordan bliver du sikker

Lad være med at bruge computere

Lad være med at bruge een computer til alt - en privat bærbar ER mere privat end en firmacomputer

Forskellige computere til forskellige formål, en server er mail-server en anden er web-server

Brug en sikker konfiguration, minimumskonfiguration

Brug sikre protokoller, kryptering, evt. TOR

Opsætning af netværk, hvordan? Security Configuration Guides + paranoia

- http://csrc.nist.gov/publications/PubsSPs.html
- http://www.nsa.gov/research/publications/index.shtml
- http://www.nsa.gov/ia/guidance/security$_configurationguides/index.shtml$

# Informationssikkerhed

Husk følgende:

Sikkerhed kommer fra langsigtede intiativer

Hvad er informationssikkerhed?

Data på elektronisk form

Data på fysisk form

Social engineering - *The Art of Deception: Controlling the Human Element of Security* af Kevin D. Mitnick, William L. Simon, Steve Wozniak

## Informationssikkerhed er en proces

# Spørgsmål?

Henrik Lund Kramshøj
mailto:hlk@security6.net hlk@security6.net

http://www.security6.net

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

© copyright 2009 Security6.net, Henrik Lund Kramshøj

# Reklamer: kursusafholdelse

Security6.net

Følgende kurser afholdes med mig som underviser

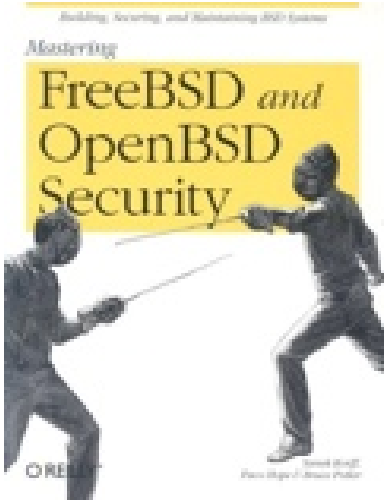
- IPv6 workshop - 1 dag
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop - 2 dage
  En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk, samt integration med hjemmepc og wirksomhedsnetværk.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

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

© copyright 2009 Security6.net, Henrik Lund Kramshøj

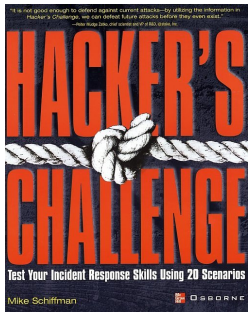
# Network Security Tools

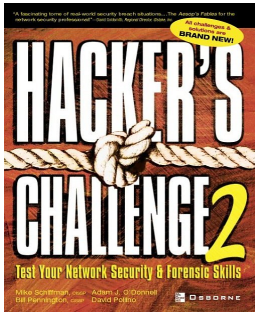
*Network Security Tools : Writing, Hacking, and Modifying Security Tools* Nitesh Dhanjani, Justin Clarke, O'Reilly 2005, ISBN: 0596007949

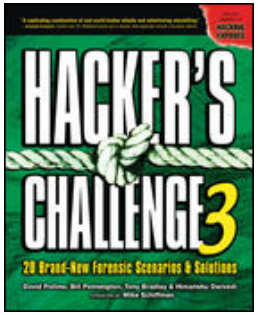



*Mastering FreeBSD and OpenBSD Security* Yanek Korff, Paco Hope, Bruce Potter, O'Reilly, 2005, ISBN: 0596006268

# Hackers Challenge







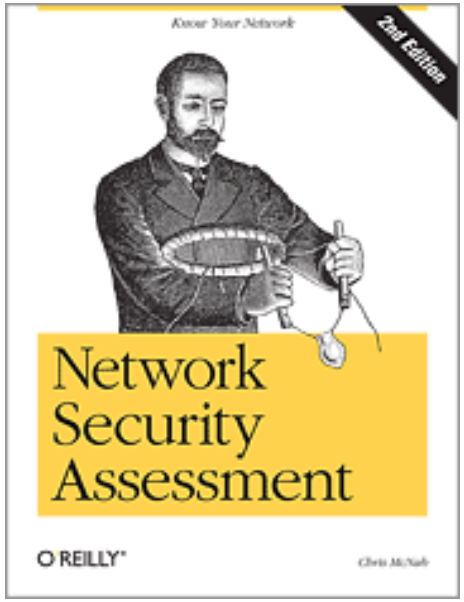

*Hacker's Challenge : Test Your Incident Response Skills Using 20 Scenarios* af Mike Schiffman McGraw-Hill Osborne Media; (October 18, 2001) ISBN: 0072193840

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

*Hacker's Challenge 3: 20 Brand New Forensic Scenarios And Solutions* David Pollino et al ISBN-10: 0072263040 McGraw-Hill Osborne Media; 3 edition (April 25, 2006)

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

# Network Security Assessment

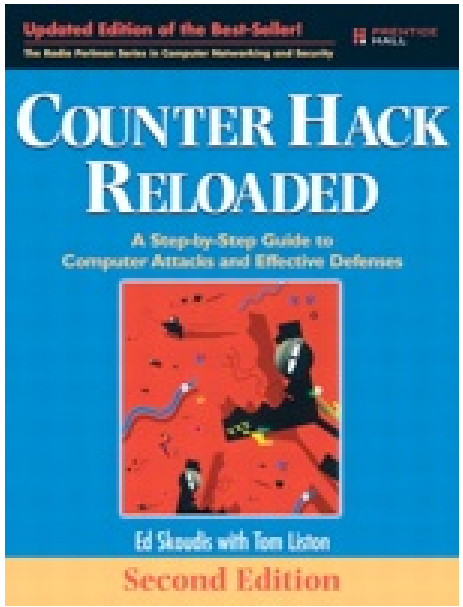



*Network Security Assessment Know Your Network* af Chris McNab, O'Reilly Marts 2004 ISBN: 0-596-00611-X

Bogen er anbefalelsesværdig

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

# Counter Hack




*Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses (2nd Edition)*, Ed Skoudis, Prentice Hall PTR, 2nd ed. 2006

Bogen er anbefalelsesværdig og er kommet i anden udgave

Minder mig om et universitetskursus i opbygningen

http://www.counterhack.net

# 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

## Internet

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

## Mailinglists

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

## Papers - der findes MANGE dokumenter på Internet

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

# Packet factory projects

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

# CISSP fra ISC2

Security6.net

(ISC)2SM (CISSP)® (SSCP)CM

Approved marks of the International Information Systems Security Certification Consortium, Inc.

Primære website: http://www.isc2.org

Vigtigt link http://www.cccure.org/

Den kræver mindst 3 års erfaring indenfor et relevant fagområde

Multiple choice 6 timer 250 spørgsmål - kan tages i Danmark

# GIAC GSEC krav

Security Essentials - basal sikkerhed

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

multiple choice eksamen

Primære website: http://www.giac.org

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

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