Velkommen til

Krimihacking - fakta eller fiktion?

PROSA

Henrik Lund Kramshj
hlk@security6.net

© copyright 2010 Security6.net, Henrik Lund Kramshj

Formlet med foredraget

Lre om hacking

Almindelige myter om hacking

Sandheder indenfor hacking, hvad kan reelt lade sig gre

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 2010 Security6.net, Henrik Lund Kramshj

Definition af hacking, oprindeligt

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

- En person, der nyder at undersge detaljer i programmerbare systemer og hvordan man udvider deres anvendelsesmuligheder i modstning til de fleste brugere, der bare lrer det mest ndvendige
- En som programmerer lidenskabligt (eller enddog fanatisk) eller en der foretrkker at programmere fremfor at teoretiserer om det
- En ekspert i et bestemt program eller en der ofter arbejder med eller p det; som i ”en Unix-hacker”.

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

Benyttes stadig i visse sammenhnge

Idag vil vi ikke diskutere etik men blot snakke teknik

Aftale om test af netvrk

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

Hacking kan betyde:

- At man skal betale erstatning til personer eller virksomheder
- At man fr konfiskeret sit udstyr af politiet
- At man, hvis man er over 15 r og bliver dmt for hacking, kan f en bde - eller fngselsstraf i alvorlige tilflde
- At man, hvis man er over 15 r og bliver dmt for hacking, fr 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 Kriminalprventive Rd
- Frygten for terror har forstrket ovenstende - s lad vre!

© copyright 2010 Security6.net, Henrik Lund Kramshj

Hackervrktjer

Security .net

Der benyttes en del vrktjer:

- 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 netvrkssniffer
- OpenBSD - http://openbsd.org operativsystem med fokus p sikkerhed
- OpenSSH - http://openssh.org sikker terminaladgang og filoverfrsel, FTP D!
- Putty - http://www.chiark.greenend.org.uk/ sgtatham/putty/download.html terminal emulator med indbygget SSH primrt til Windows

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, f 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 2010 Security6.net, Henrik Lund Kramshj

Hacking er magi

Hacking ligner indimellem magi

Hacking er ikke magi

Hacking krver blot lidt ninja-trning

© copyright 2010 Security6.net, Henrik Lund Kramshj

Hacking eksempel - det er ikke magi

MAC filtrering p trdlse netvrk

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

Mange trdlse Access Points kan filtrere MAC adresser

Kun kort som er p listen over godkendte adresser tillades adgang til netvrket

Det virker dog ikke ☺

De fleste netkort tillader at man overskriver denne adresse midlertidigt

Derudover har der ofte vret fejl i implementeringen af MAC filtrering

© copyright 2010 Security6.net, Henrik Lund Kramshj

Myten om MAC filtrering

Eksemplet med MAC filtrering er en af de mange myter

Hvorfor sker det?

Marketing - producenterne stter store mrkater p skerne

Manglende indsigt - forbrugerne kender reelt ikke koncepterne

Hvad *er* en MAC adresse egentlig

Relativt f har forudstningerne for at gennemskue drlig sikkerhed

Lsninger?

Udbrede viden om usikre metoder til at sikre data og computere

Udbrede viden om sikre metoder til at sikre data og computere

© copyright 2010 Security6.net, Henrik Lund Kramshj

MAC filtrering

Hvad skal der ske?

Tnk som en hacker

Rekognoscering

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

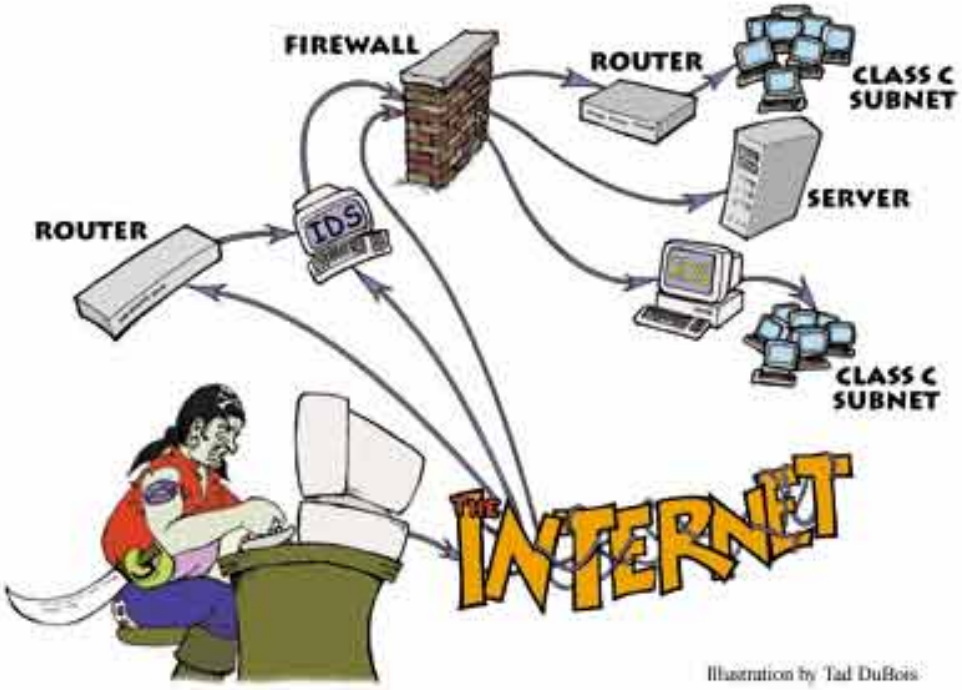
Udnyttelse/afprvning: exploit programs

Jeg bruger lige BackTrack

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

© copyright 2010 Security6.net, Henrik Lund Kramshj

Er sikkerhed interessant?

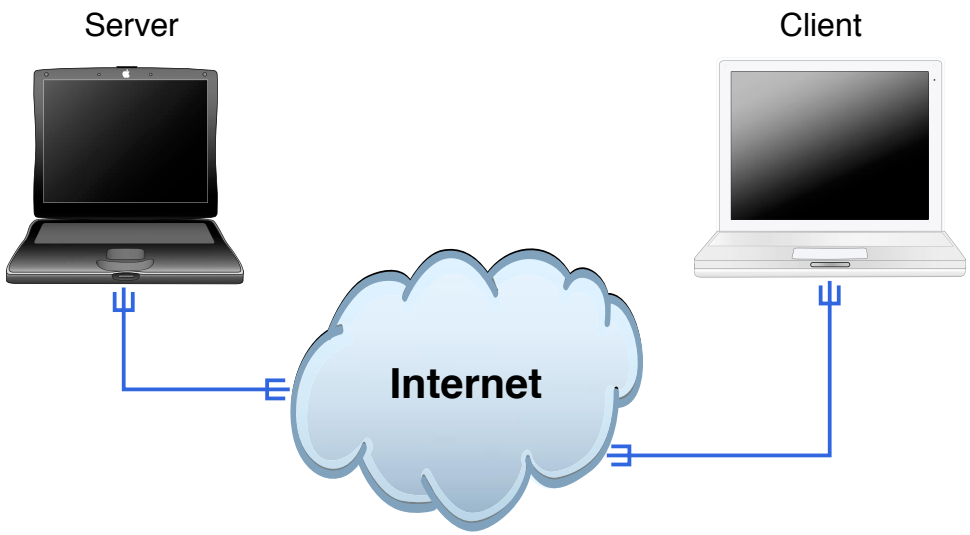


Sikkerhedsproblemerne i netvrk er mange

Mange services - mange srbare services

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

Internet og computere idag



Klienter og servere idag, enkeltstende computere tidligere

Centrale og stationre, brbare og hndholdte idag

Rdder i akademiske miljer, 20 r gamle protokoller

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

Alt er forbundet, ok ikke helt sandt men desvrre tt p

© copyright 2010 Security6.net, Henrik Lund Kramshj

POP3 - e-mail i Danmark

POP3 sender brugernavn og kodeord i klartekst - ligesom FTP

bruges dagligt af nsten alle privatkunder

alle internetudbydere og postudbydere tilbyder POP3

der findes en variant, POP3 over SSL/TLS

© copyright 2010 Security6.net, Henrik Lund Kramshj

dsniff

en sniffer til mange usikre protokoller

inkluderer **arpspoof**

Lavet af Dug Song, dugsong@monkey.org

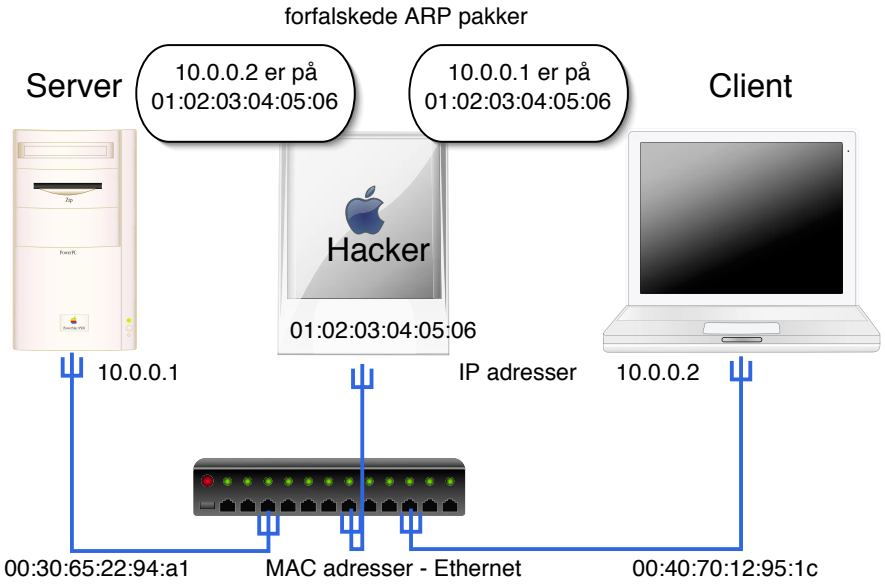
```
dsniff is a password sniffer which handles FTP, Telnet,
SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin,
RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11,
CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker,
Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft
SMB, Oracle SQL*Net,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

© copyright 2010 Security6.net, Henrik Lund Kramshj

dsniff forudstninger

Der er visse forudstninger der skal vre opfyldt

- Man skal have trafikken
- Det kan gres gennem arp spoofing eller ved at hacke ind i et system/router p netvrksvejen



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 netvrksdump kan man lse det med chaosreader

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

http://chaosreader.sourceforge.net/

Hvad er en firewall

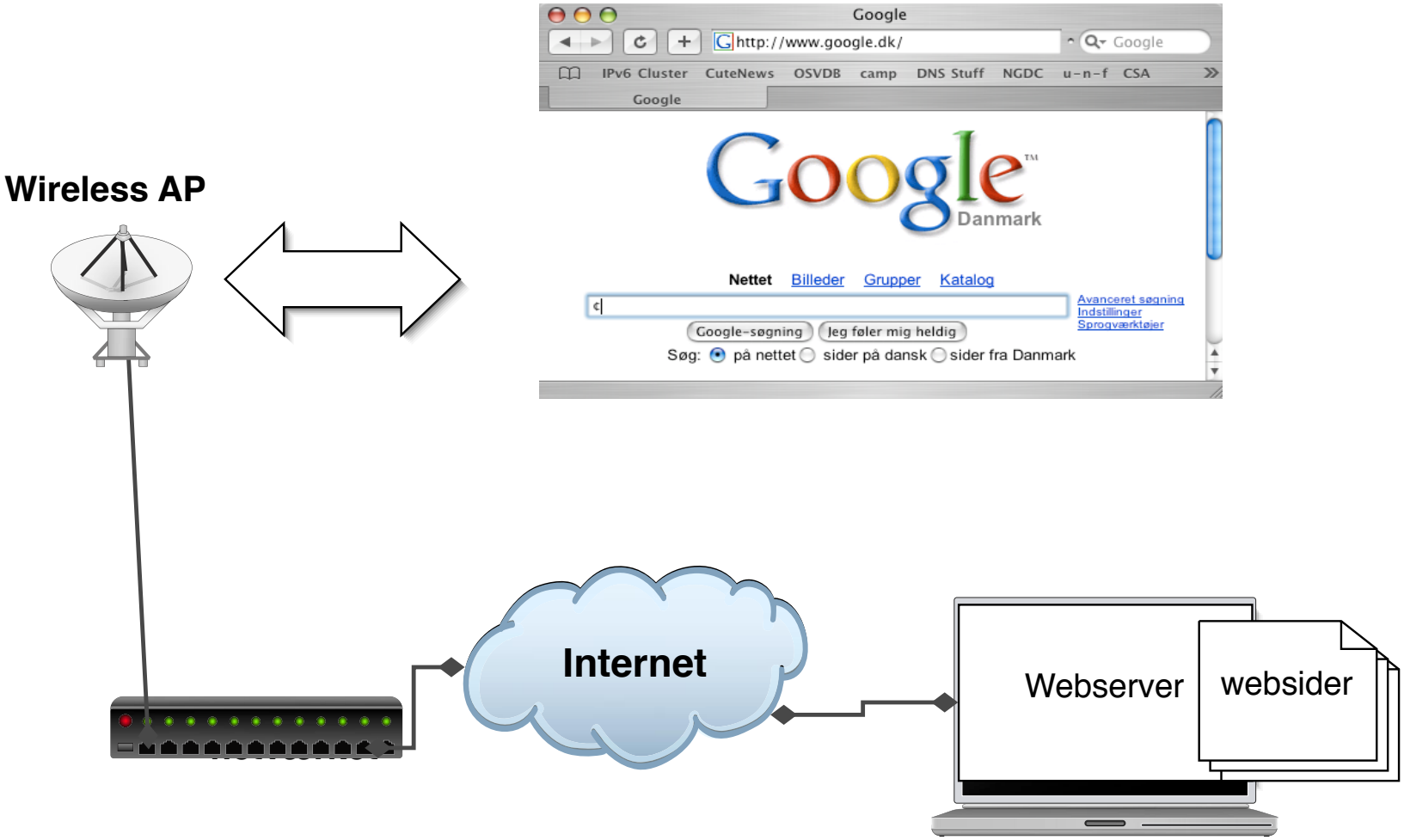
Lad os starte med noget alle kender

En firewall er noget som blokerer traffik p Internet

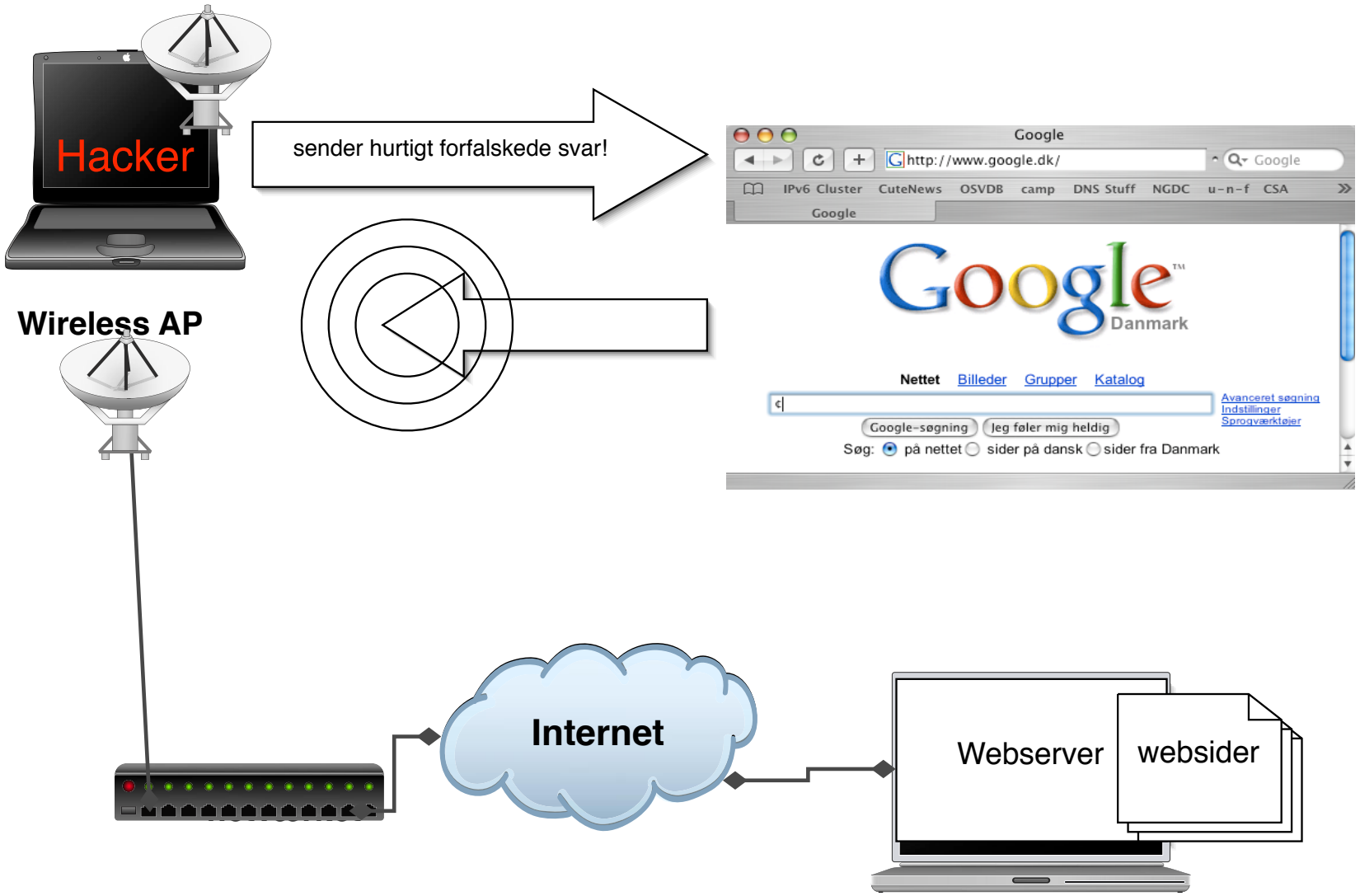
- En firewall er noget som tillader traffik p Internet

Myte: en firewall beskytter mod alt

Normal WLAN brug



Packet injection - airpwn



Airpwn teknikker

Klienten sender foresprgsel

Hackerens program airpwn lytter og sender s falske pakker

Hvordan kan det lade sig gre?

- Normal foresprgsel og svar p Internet tager 50ms
- Airpwn kan svare p omkring 1ms angives det
- Airpwn har alle informationer til rdighed

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

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

Det vil vre trivielt at introducere skadelig kode ad denne vej

© copyright 2010 Security6.net, Henrik Lund Kramshj

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 netvrket

Beskytter ikke mod fysiske angreb

Beskytter ikke mod malware gennem websider og e-mail

Firewall anbefales altid, specielt p brbare

© copyright 2010 Security6.net, Henrik Lund Kramshj

Hvorfor virkede airpwn?

Airpwn programmet virkede ved at sniffe og indstte falske beskeder

Sniffere findes i mange versioner:

- Dsniff - proof of concept program afkodning af drlige protokoller
  Sjovt nok benyttes mange af disse idag, og nye protokoller er ofte uden kryptering, why, why, **WHY!**
- Ettercap menustyret aflytning p netvrk, Ethernet LAN - jeps, **switchede netvrk er srbare**
- Wireshark - afkodning af alle gngse 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 Isninger

Krypter trafikken
Hvad skal krypteres og hvordan?

Du kan kryptere netvrket
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 flsomme 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 2010 Security6.net, Henrik Lund Kramshj

Kryptering

Lisbeth Salander bruger PGP, men er det sikkert?

Jeg bruger PGP ☺

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

Formlet med kryptering

kryptering er den eneste mde 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 netvrkstrafik - Virtual Private Networks VPN

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

© copyright 2010 Security6.net, Henrik Lund Kramshj

DES, Triple DES og AES/Rijndael

DES kryptering baseret p den IBM udviklede Lucifer algoritme har vret benyttet gennem mange r.

Der er vedtaget en ny standard algoritme Advanced Encryption Standard (AES) som aflser 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

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 p papir og scannet igen - det var lovligt
- I dag kan en masse information om PGP findes gennem: http://www.pgpi.org

© copyright 2010 Security6.net, Henrik Lund Kramshj

Basale tools - GPG

Gnu Privacy Guard, forkortes GnuPG eller GPG

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

Open Source med GPL licens.

Kan bruges p alle de gngse operativsystemer

Sammen med Thunderbird Email programmet bruger man Enigmail plugin

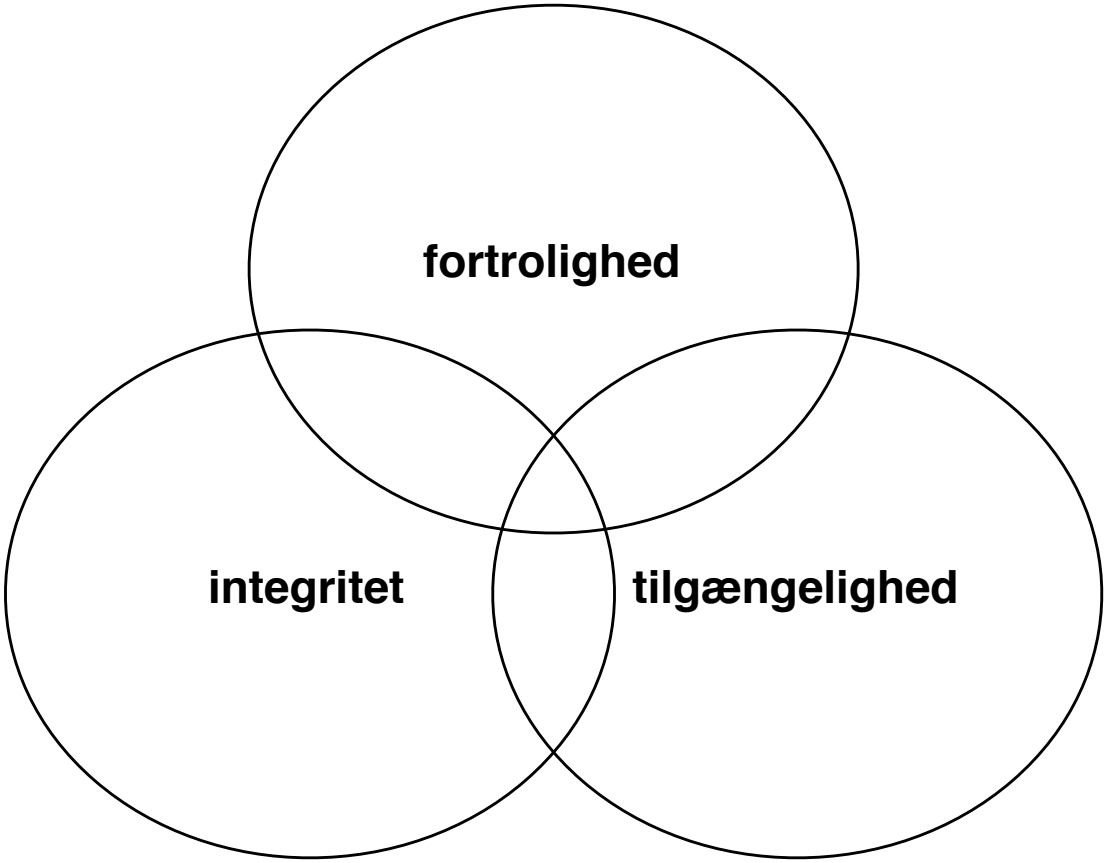
© copyright 2010 Security6.net, Henrik Lund Kramshj

Problemet med kryptering

ingen garantier

- Vi hber at vores antagelser om at de matematiske problemer der skal lses er rigtige

Confidentiality Integrity Availability



Husk altid de fundamentale principper indenfor sikkerhed

Hvad skal du beskytte mod **hvem**

© copyright 2010 Security6.net, Henrik Lund Kramshj

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 $400	Scavenged computer time FPGA	1 week 5 hours ($.08)	Not feasible 38 years ($5,000)
Small Business	$10,000	FPGA [1]	12 min.($.08)	556 days ($5,000)
Corporate Department	$300,000	FPGA ASIC [2]	24 sec. ($.08) 0.18 sec. ($.001)	19 days ($5,000) 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 prve at knkke noget kryptering

WEP cracking - airodump og aircrack

airodump - opsamling af krypterede pakker

aircrack - statistisk analyse og forsg p at finde WEP nglen

Med disse vrktjer er det muligt at knkke *128-bit ngler*!

Blandt andet fordi det reelt er 104-bit ngler ☺

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 2010 Security6.net, Henrik Lund Kramshj

airodump afvikling

Nr airodump krer 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 p 100% opdateret Mac udstyr

© copyright 2010 Security6.net, Henrik Lund Kramshj

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 2010 Security6.net, Henrik Lund Kramshj

Hvor lang tid tager det?

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

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

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

Idag snakker vi f 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.**

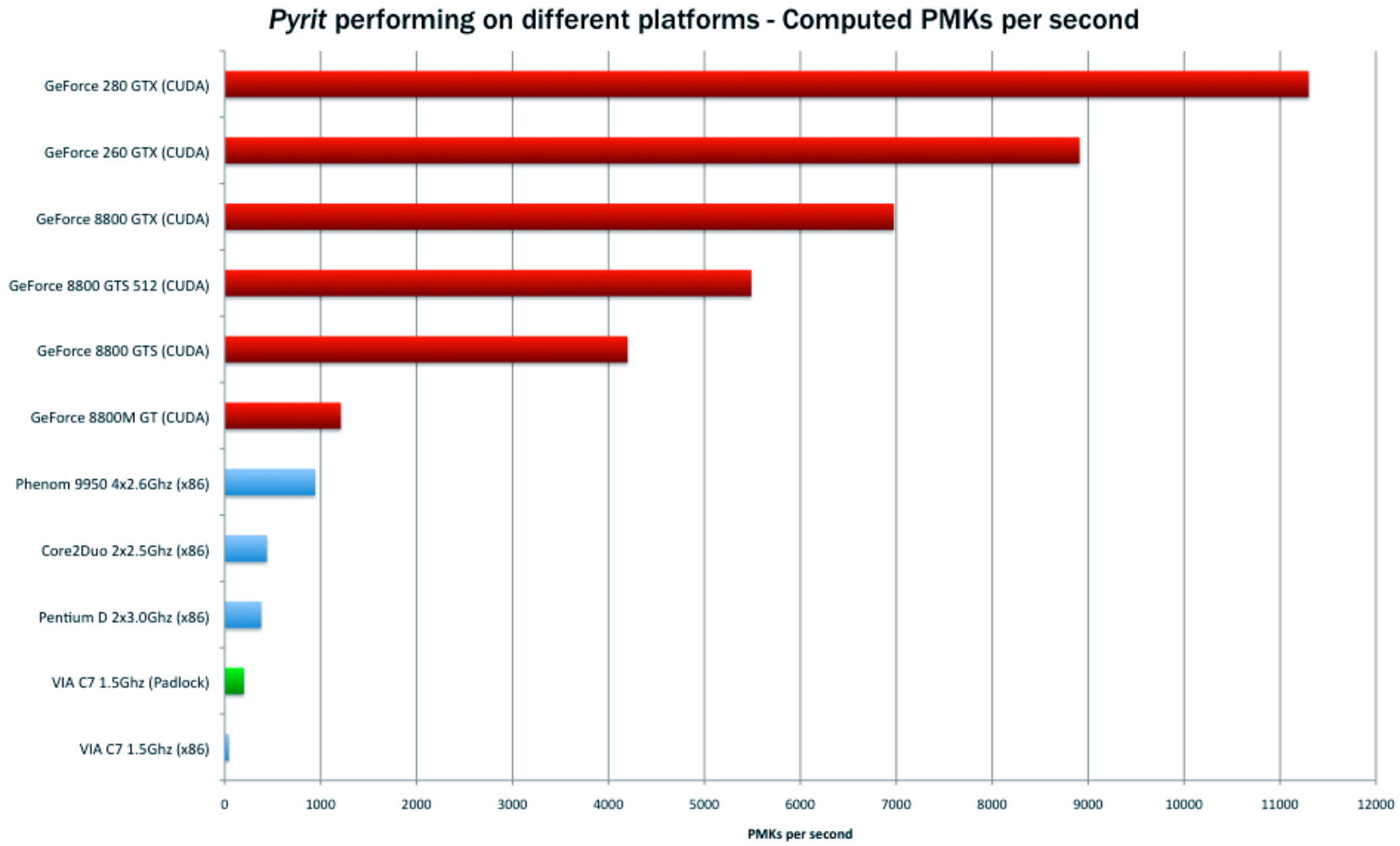
Pyrit's implementation allows to create massive databases, pre-computing part of the WPA/WPA2-PSK authentication phase in a space-time-tradeoff. The performance gain for real-world-attacks is in the range of three orders of magnitude which urges for re-consideration of the protocol's security. Exploiting 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 vre - 150 keys/s p min Thinkpad X31

Kryptering afhnger af SSID! S check i tabellen er minutter.

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

Tired of WoW?



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

© copyright 2010 Security6.net, Henrik Lund Kramshj

Kryptografiske principper

Algoritmerne er kendte

Nglerne er hemmelige

Ngler har en vis levetid - de skal skiftes ofte

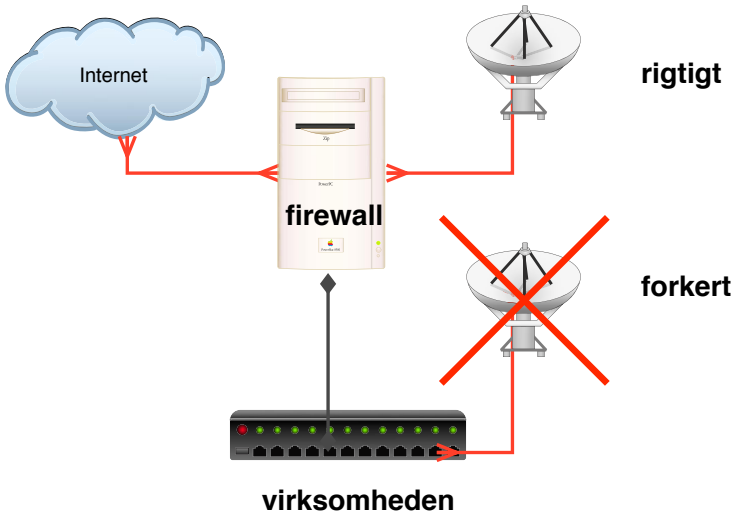
Et successfuldt angreb p en krypto-algoritme er enhver genvej som krver mindre arbejde end en gennemgang af alle nglerne

Nye algoritmer, programmer, protokoller m.v. skal gennemgs nje!

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

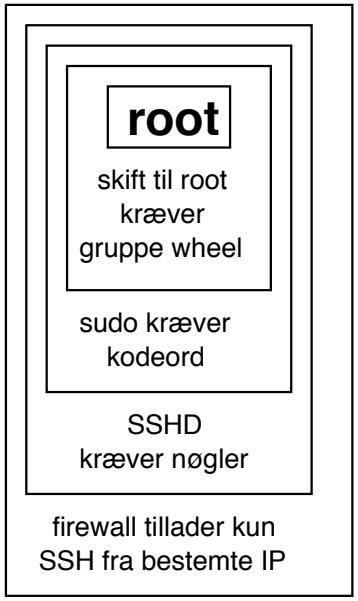
© copyright 2010 Security6.net, Henrik Lund Kramshj

Anbefalinger mht. trdlse netvrk



- Brug noget tilfldigt som SSID - netnavnet
- Brug ikke WEP til virksomhedens netvrk
  - men istedet en VPN lsning med individuel autentificering eller WPA
- NB: WPA Personal/PSK krver passphrase p +40 tegn!
- Skift til WPA2 Personal, WPA Enterprise eller WPA2 Enterprise
- Placer de trdlse adgangspunkter hensigtsmssigt i netvrket - s de kan overvges
- Lav et st regler for brugen af trdlse netvrk - hvor m medarbejdere bruge det?
- Se eventuelt pjecerne *Beskyt dit trdlse Netvrk* fra Ministeriet for Videnskab, Teknologi og Udvikling http://www.videnskabsministeriet.dk/

Nr adgangen er skabt



S gr man igang med de almindelige vrktjer

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

Forsvaret er som altid - flere lag af sikkerhed!

Basal Portscanning

Hvad er portscanning

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

mlet er at identificere bne porte - srbare services

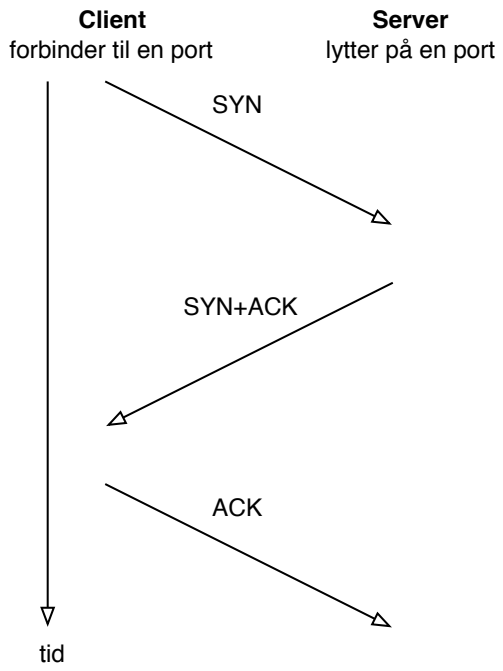
typisk TCP og UDP scanning

TCP scanning er ofte mere plidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

TCP three way handshake



- **TCP SYN half-open** scans
- Tidligere loggede systemer kun nr 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 Security6.net, Henrik Lund Kramshj

Ping og port sweep

scanninger p tvrs af netvrk kaldes for sweeps

Scan et netvrk efter aktive systemer med PING

Scan et netvrk efter systemer med en bestemt port ben

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 Security6.net, Henrik Lund Kramshj

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 mde at identificere operativsystemer p
- 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 drlige passwords!

Folk vlger drlige kodeord - inkl. mig.

Systemer skal krve komplekse kodeord

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

De gttede kodeord, brd ikke krypteringen

© copyright 2010 Security6.net, Henrik Lund Kramshj

Myte: kodeord p brbare beskytter data

Myten:

man tror at et kodeord p en brbar beskytter data

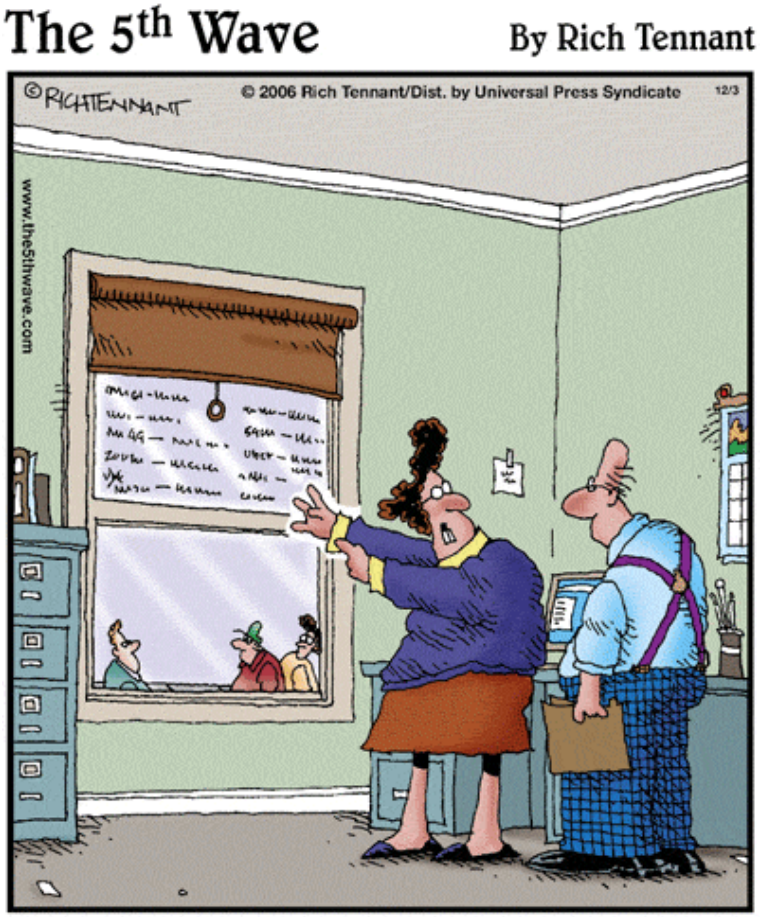
Sandhed:

I praksis er det kun en mindre gene

Windows password skjuler ikke data p harddisken

Liges p 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

Brbare tillader typisk boot fra CD-ROM
hold c nede p en Mac

Mac computere kan i nogle tilflde vre firewire diske
hold t nede under boot

Harddisken kan typisk nemt fjernes fra en brbar

Fysisk adgang til systemet - **game over**

© copyright 2010 Security6.net, Henrik Lund Kramshj

Harddisk kryptering

Et vrn mod fysisk adgang er harddisk kryptering

Eksempler p 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 2010 Security6.net, Henrik Lund Kramshj

harddisk beskyttelse og data kryptering

Kryptering findes i alle de gngse 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 p disken - IBM harddisk BIOS kodeord

Pyha, s er vi vel sikre med harddisk kryptering

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

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

Jeg prvede at lse memory fra en iBook og vupti, p relativt f sekunder havde man et image!

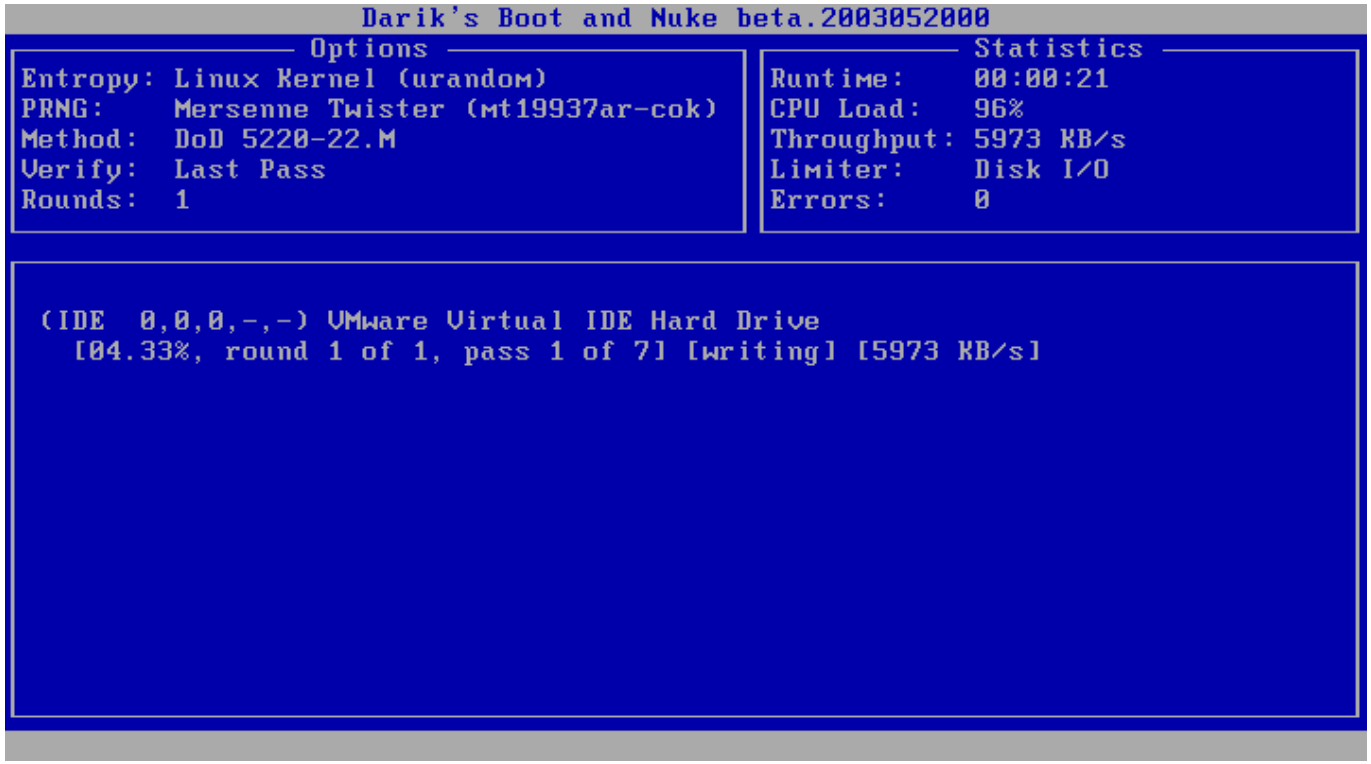
Fjernelse af memory - men data bevaret og kan aflses
Lest We Remember: Cold Boot Attacks on Encryption Keys
http://citp.princeton.edu/memory/
- bliver det mere hollywood?

S mske skal du bruge harddisk kryptering OG lukke ned efter brug?

pssst husk ogs VileFault!

© copyright 2010 Security6.net, Henrik Lund Kramshj

... 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 vrktjer 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

© copyright 2010 Security6.net, Henrik Lund Kramshj

Myten: Bare du bruger harddisk kryptering s er du sikker

Myten:

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

Sandhed:

I praksis er det meget afhngigt af den valgte teknologi

Kodeordet til krypteringen bliver essentielt

Vlg gode kodeord!

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

Brug selvflgelig ikke samme kodeord p hotmail og din PGP key ;-)

© copyright 2010 Security6.net, Henrik Lund Kramshj

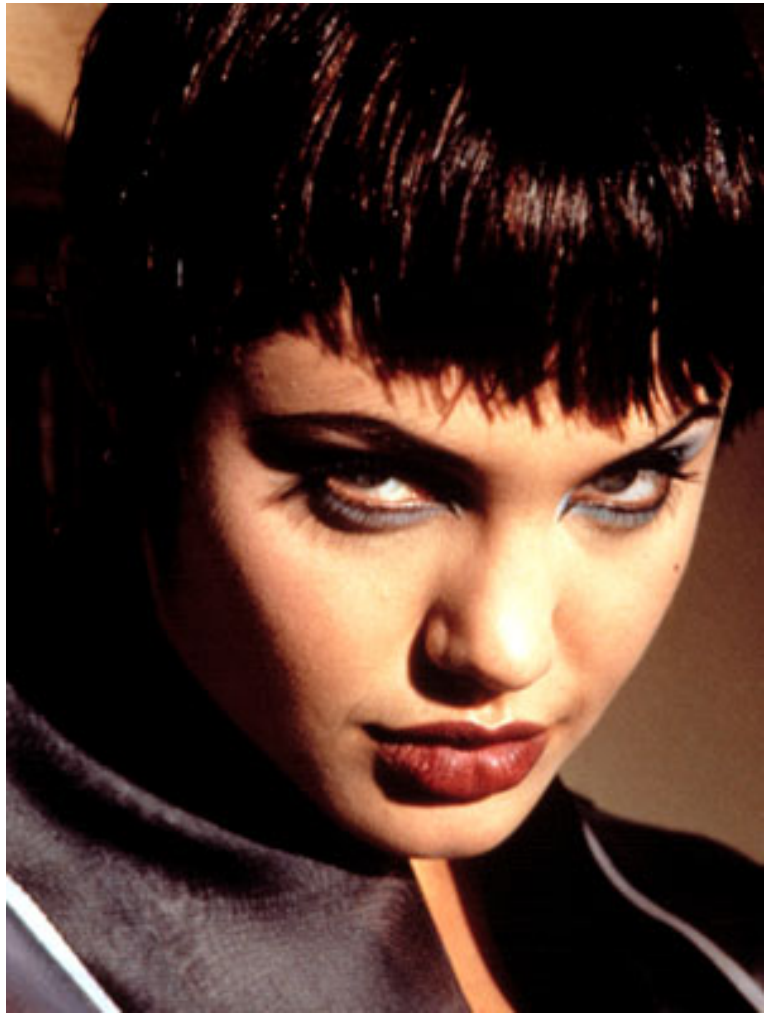
Opsummering - hidtil

Firewalls er ndvendige, men pas p trojanere og virus aligevel

Brug kryptering og vlg algoritmer og produkter med omhu

og husk s at vlge gode passwords!

Hackertyper anno 1995



Hackertyper anno 2008

Lisbeth laver PU, personundersgelser ved hjlp af hacking

Hvordan finder man information om andre

Fra mnstre til person

Frst vil vi finde nogle mnstre

Derefter vil vi sge med de mnstre

Nogle giver direkte information

Andre giver baggrundsinformation

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

Eksempler p mnstre

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

Diverse idnumre, som CPR - tr du sge p dit CPR nr?

Computerrelaterede informationer: IP, Whois, Handles

genavne, kendenavne

Skrivestil, ordbrug mv.

Tiden p din computer?

Tnk kreativt ☺

Hvor finder du informationerne

Email

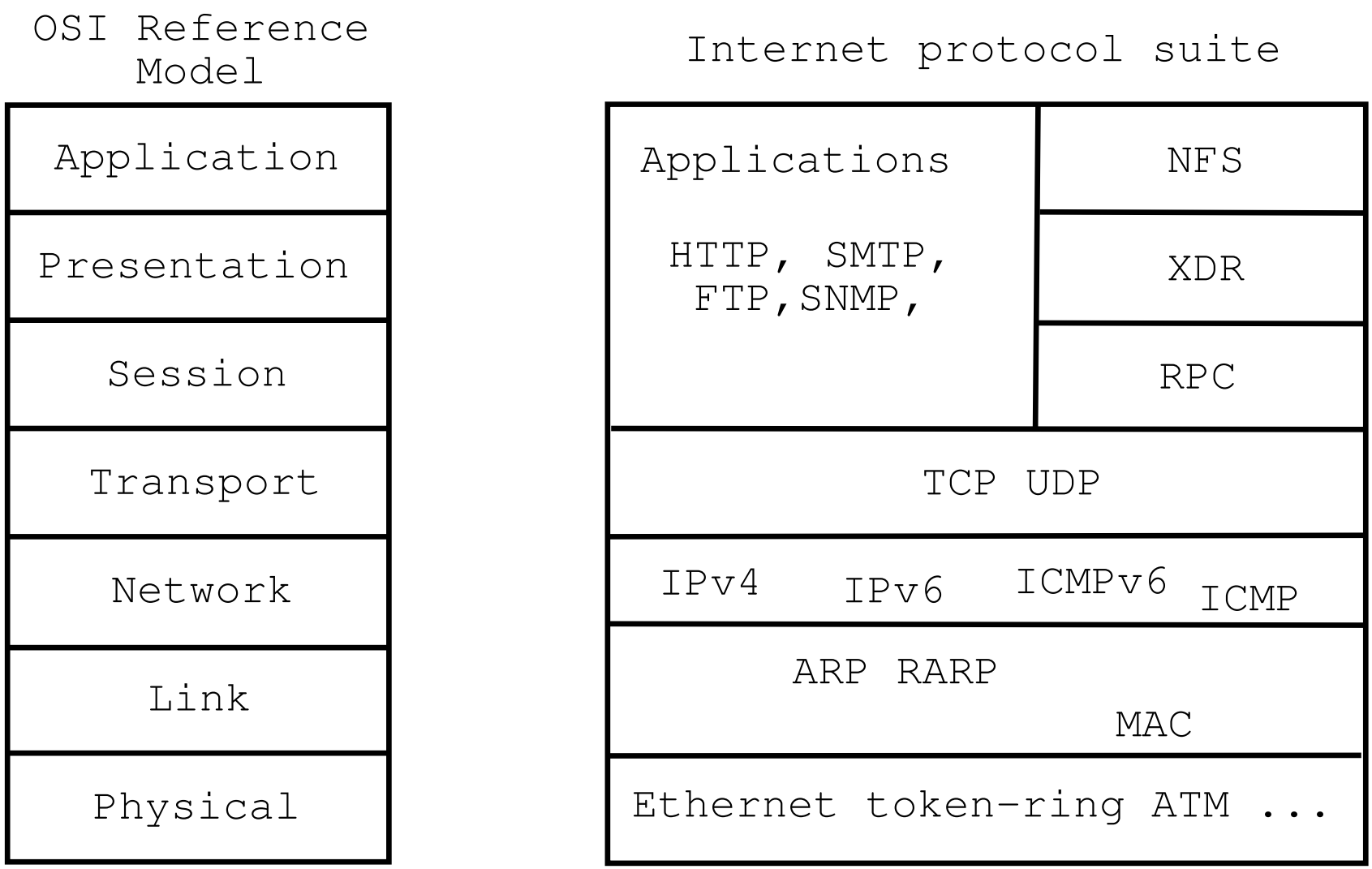
DNS

Gtter

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
```

Netvrksteknologierne benytter adresser p lag 2

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

Frste halvdel af adresserne er Organizationally Unique Identifier (OUI)

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

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

© copyright 2010 Security6.net, Henrik Lund Kramshj

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 p http://www.iana.org

© copyright 2010 Security6.net, Henrik Lund Kramshj

traceroute

traceroute programmet virker ved hjlp af TTL

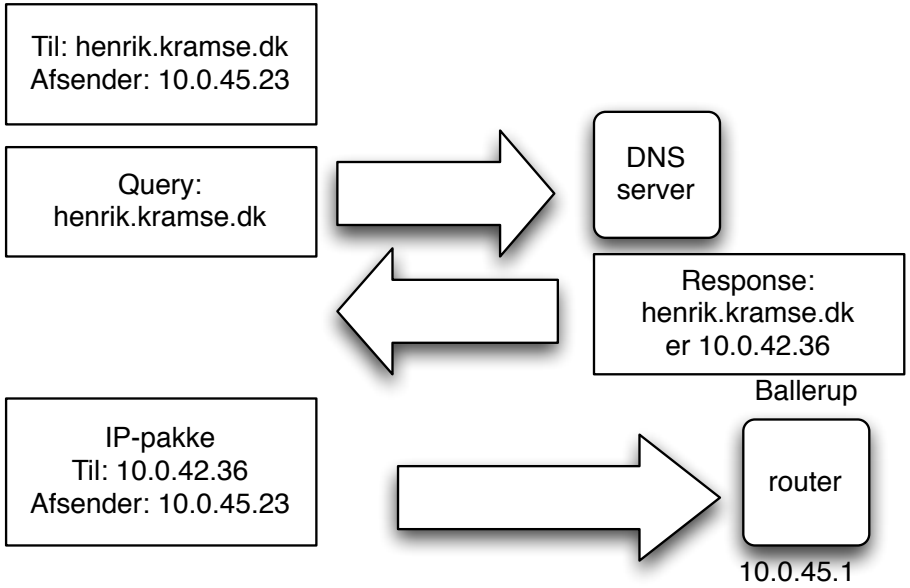
levetiden for en pakke tlles ned i hver router p vejen og ved at stte denne lavt opnr man at pakken *timer ud* - besked fra hver router p vejen

default er UDP pakker, men p 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 Security6.net, Henrik Lund Kramshj

Domain Name System



Gennem DHCP fr man typisk ogs information om DNS servere

En DNS server kan sl navne, domner og adresser op

Foregr via query og response med datatyper kaldet resource records

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

DNS systemet

navneopslag p 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

bestr 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 strste er:

- RIPE (Rseaux IP Europens) 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 modstning til Local Internet Registries (LIRs) og National Internet Registry (NIR)

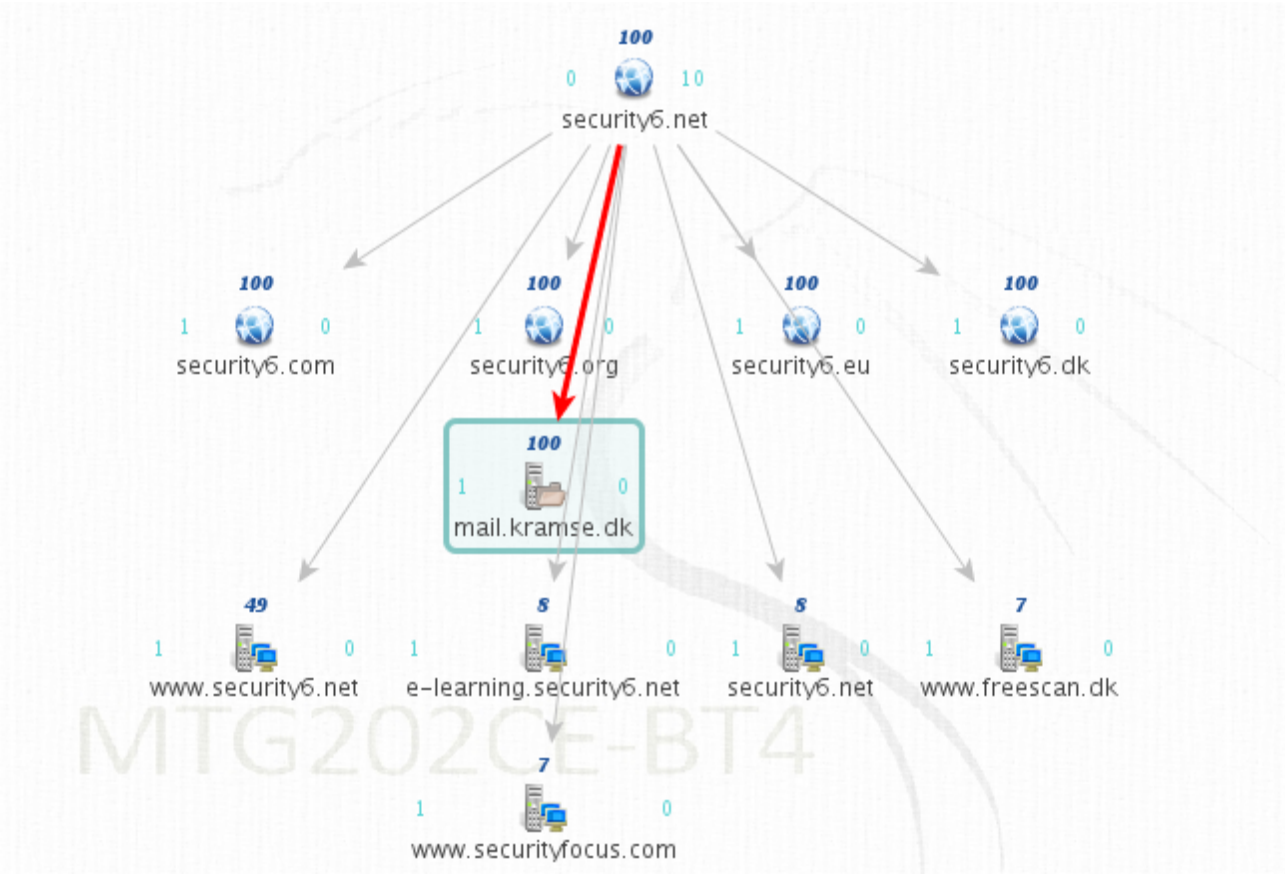
© copyright 2010 Security6.net, Henrik Lund Kramshj

Google for it

Google som hacker vrktj?

Googledorks http://johnny.ihackstuff.com/

Listbeth in a box?



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

Er du passende paranoid?

Vr p vagt

The bad stuff - breaking in

Hvordan bryder man ind?

Det kan ske p mange mder:

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

Definitioner

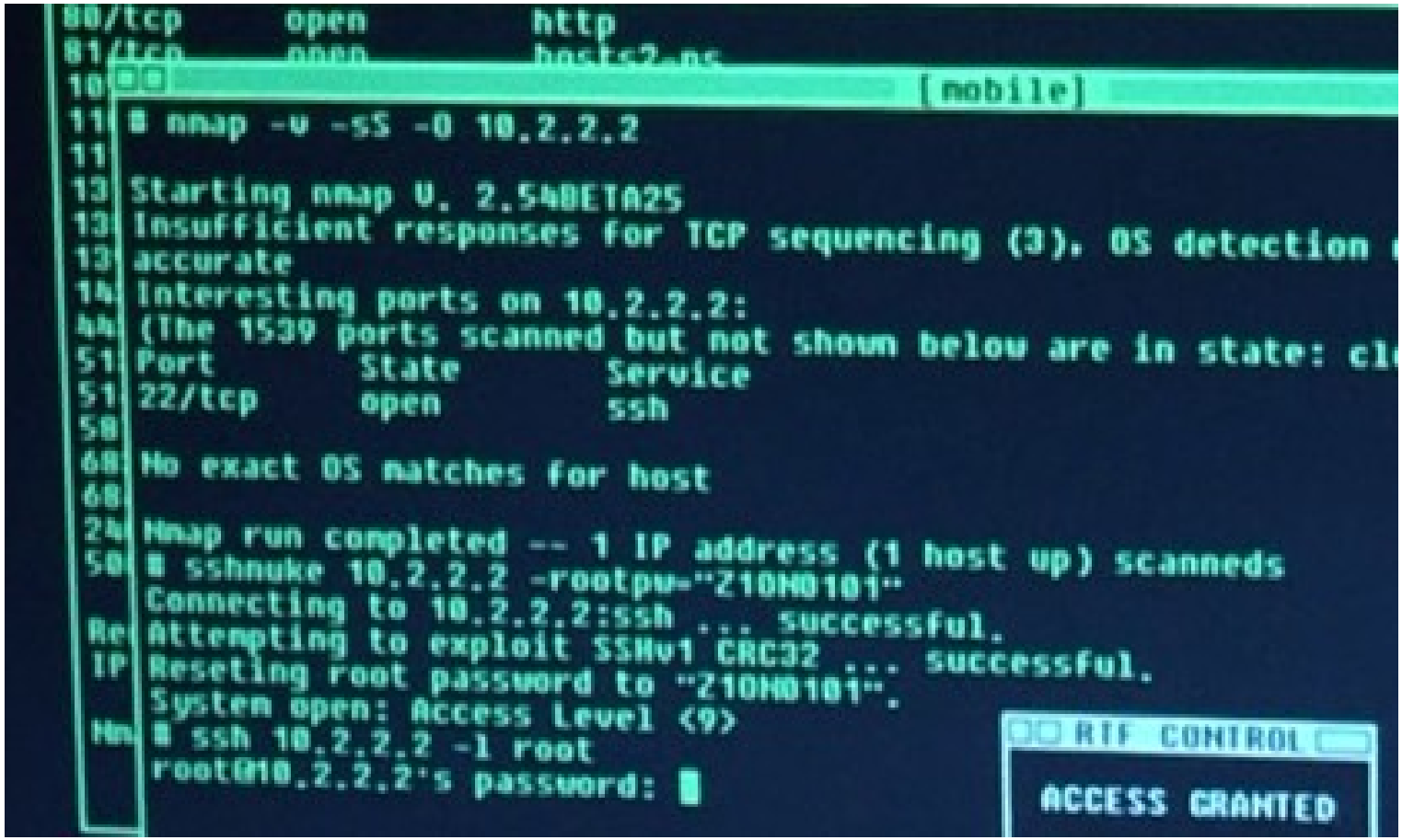
- trojaner program der udgiver sig for at vre noget andet, eksempelvis et spil, men installerer en keylogger
- keylogger logger tastetryk, fysiske enheder eller software
- root kit, software der skjuler sig og ndrer systemet
- malware, skadelig software herunder ovenstende, virus og orme m.v.

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

© copyright 2010 Security6.net, Henrik Lund Kramshj

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 nr man skriver flere data end der er afsat plads til i en buffer, et dataomrde. Typisk vil programmet g ned, men i visse tilflde kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

Stack protection er et udtryk for de systemer der ved hjlp 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 Security6.net, Henrik Lund Kramshj

Exploits - udnyttelse af srbarheder

exploit/exploitprogram er

- udnytter eller demonstrerer en srbarhed
- rettet mod et specifikt system.
- kan vre 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 srbarhed lokalt p maskinen, eksempelvis opn hjere privilegier, eller beregnet til at udnytter srbarheder over netvrk

remote root exploit - den type man frygter mest, idet det er et exploit program der nr det afvikles giver angriberen fuld kontrol, root user er administrator p UNIX, over netvrket.

zero-day exploits dem som ikke offentliggres - dem som hackere holder for sig selv. Dag 0 henviser til at ingen kender til dem fr de offentliggres og ofte er der umiddelbart ingen rettelser til de srbarheder

© copyright 2010 Security6.net, Henrik Lund Kramshj

Hvordan laves et buffer overflow?

Findes ved at prve sig frem

- black box testing
- closed source
- reverse engineering

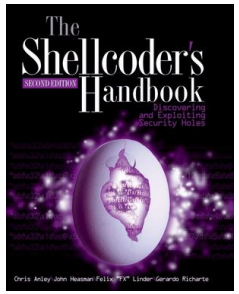
Ved Open source Findes de typisk ved at lse/analysere koden

- 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 lre at lave buffer overflows og exploit programmer er flgende dokumenter et godt sted at starte

Smashing The Stack For Fun And Profit Aleph One

Writing Buffer Overflow Exploits with Perl - anno 2000

Flgende 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 sledes 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

Udviklingsvrktjerne til exploits er idag meget raffinerede!

http://www.metasploit.com/

Forudstninger

Bemrk: alle angreb har forudstninger 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 kden af forudstninger 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 net lngst og et godt eksempel
http://www.openbsd.org/papers/

Diverse hackervrktjer

Vi prver et par af hackervrktjerne, kunne vre:

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

Hackervrktjer

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

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

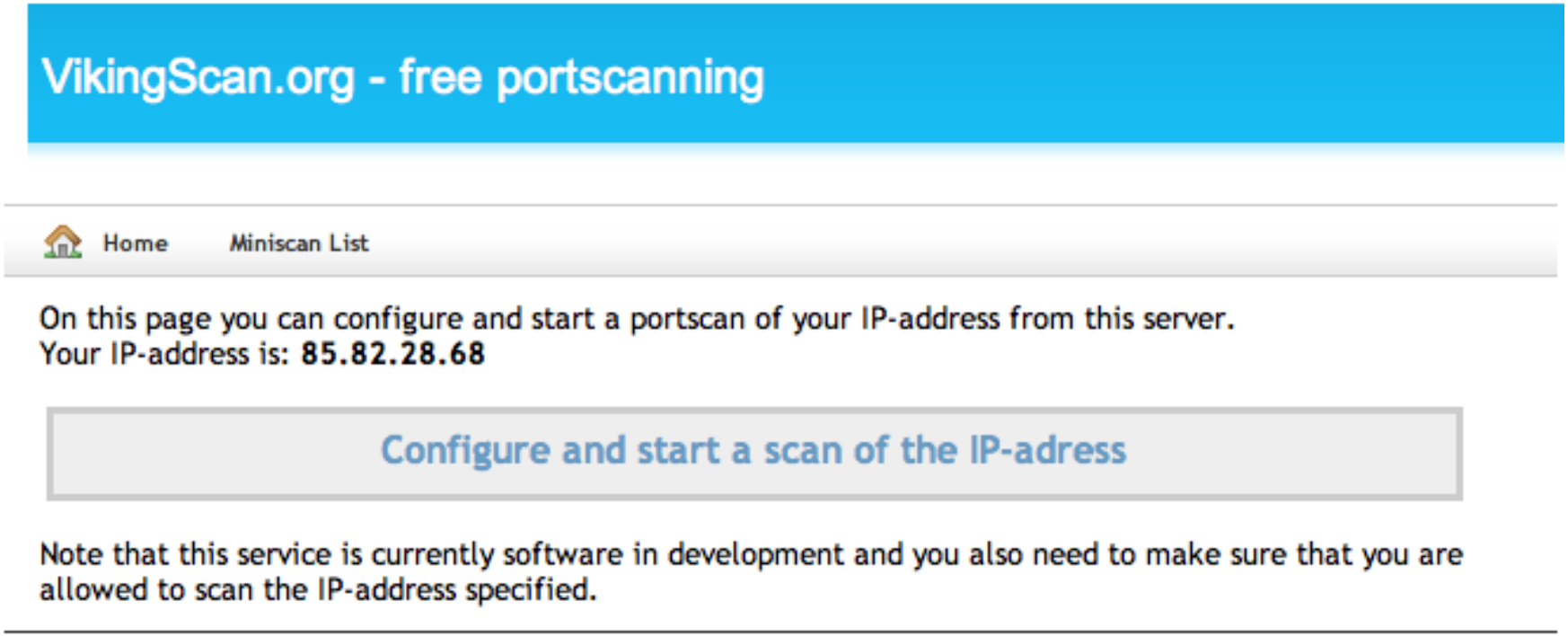
> We realize that SATAN is a two-edged sword - like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

SATAN og ideerne med automatiseret scanning efter srbarheder blev siden frt videre i programmer som Saint, SARA og idag findes mange hackervrktjer 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 mske ikke nr

Hvad med fysisk sikkerhed og telefonhacking, krokodillenb rulez!!

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

Bluetooth sikkerhed, bluesniper, car whisperer

Lockpicking

Fast flux netvrk

Hvordan bliver du sikker

Lad vre med at bruge computere

Lad vre med at bruge een computer til alt - en privat brbar ER mere privat end en firmacomputer

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

Brug en sikker konfiguration, minimumskonfiguration

Brug sikre protokoller, kryptering, evt. TOR

Opstning af netvrk, 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 flgende:

Sikkerhed kommer fra langsigtede intiativer

Hvad er informationssikkerhed?

Data p elektronisk form

Data p 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

Sprgsml?

Henrik Lund Kramshj
hlk@security6.net

http://www.security6.net

I er altid velkomne til at sende sprgsml p e-mail

Reklamer: kursusafholdelse

Flgende kurser afholdes med mig som underviser

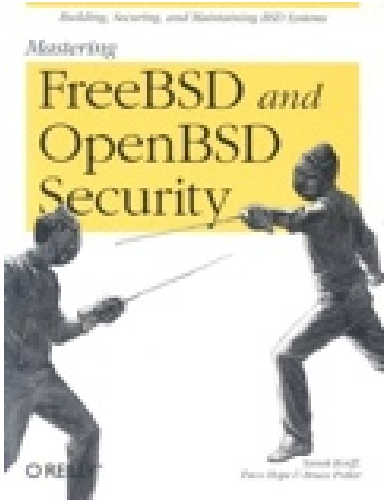
- IPv6 workshop - 1 dag
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netvrk.
- Wireless teknologier og sikkerhed workshop - 2 dage
  En dag med fokus p netvrksdesign og fornuftig implementation af trdlse netvrk, samt integration med hjemmepc og wirksomhedsnetvrk.
- Hacker workshop 2 dage
  Workshop med detaljeret gennemgang af hackermetoderne angreb over netvrk, exploitprogrammer, portscanning, Nessus m.fl.
- Forensics workshop 2 dage
  Med fokus p tilgngelige open source vrktjer gennemgs metoder og praksis af undersgelse af diskimages og spor p computer systemer
- Moderne Firewalls og Internetsikkerhed 2 dage
  Informere om trusler og aktivitet p Internet, samt give et bud p hvorledes en avanceret moderne firewall idag kunne konfigureres.

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

© copyright 2010 Security6.net, Henrik Lund Kramshj

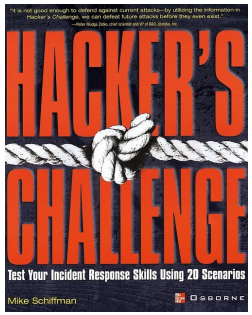
Network Security Tools

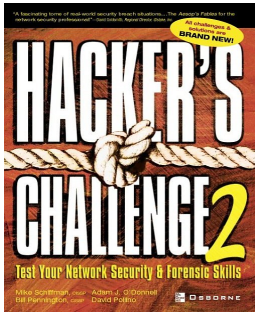
Network Security Tools : Writing, Hacking, and Modifying Security Tools Nitesh Dhanjani, Justin Clarke, O'Reilly 2005, ISBN: 0596007949

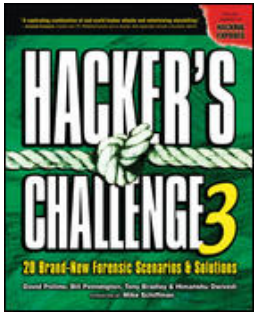


Mastering FreeBSD and OpenBSD Security Yanek Korff, Paco Hope, Bruce Potter, O'Reilly, 2005, ISBN: 0596006268

Hackers Challenge







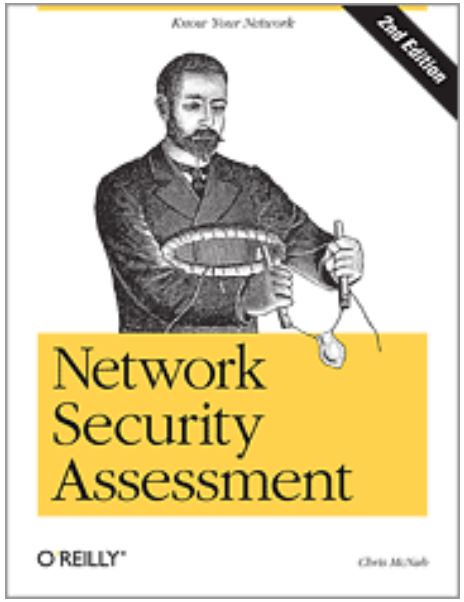
Hacker's Challenge : Test Your Incident Response Skills Using 20 Scenarios af Mike Schiffman McGraw-Hill Osborne Media; (October 18, 2001) ISBN: 0072193840

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)

Bgerne indeholder scenarier i frste halvdel, og lsninger i anden halvdel - med fokus p relevante logfiler og srbarheder

Network Security Assessment

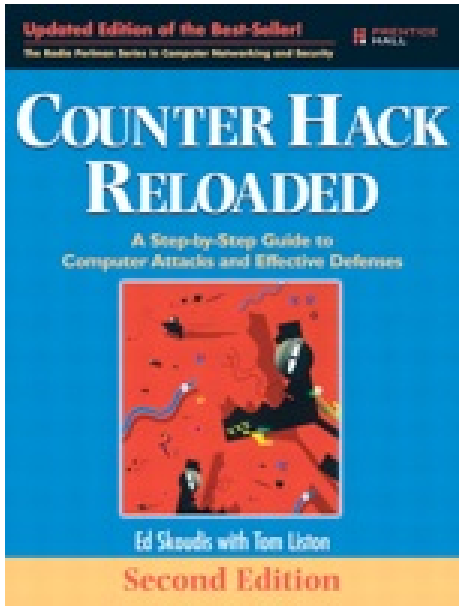


Network Security Assessment Know Your Network af Chris McNab, O'Reilly Marts 2004 ISBN: 0-596-00611-X

Bogen er anbefalelsesvrdig

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 anbefalelsesvrdig og er kommet i anden udgave

Minder mig om et universitetskursus i opbygningen

http://www.counterhack.net

Referencer

Anbefalede bger:

- *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 netvrk. 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 netvrk 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 vktjer har mailinglister tilknyttet

Papers - der findes MANGE dokumenter p 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.

Primre website: http://www.isc2.org

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

Den krver mindst 3 rs erfaring indenfor et relevant fagomrde

Multiple choice 6 timer 250 sprgsml - 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

Primre 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