Velkommen til

Security Tools in Software Development

FOSS Aalborg

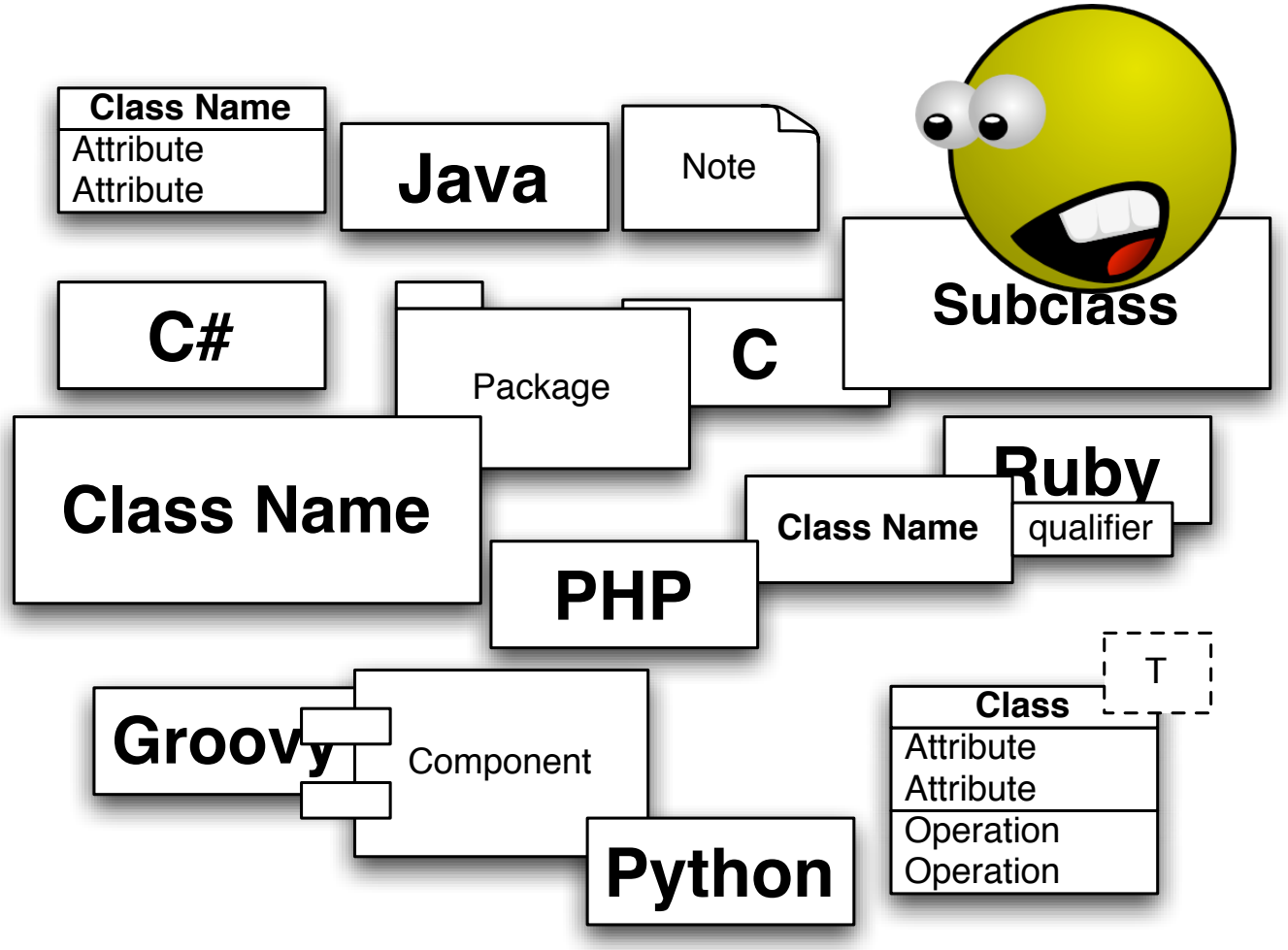
Henrik Lund Kramshøj
hlk@security6.net

http://www.security6.net

Slides are available as PDF and are in Danish only, sorry

© copyright 2009 Security6.net, Henrik Lund Kramshøj

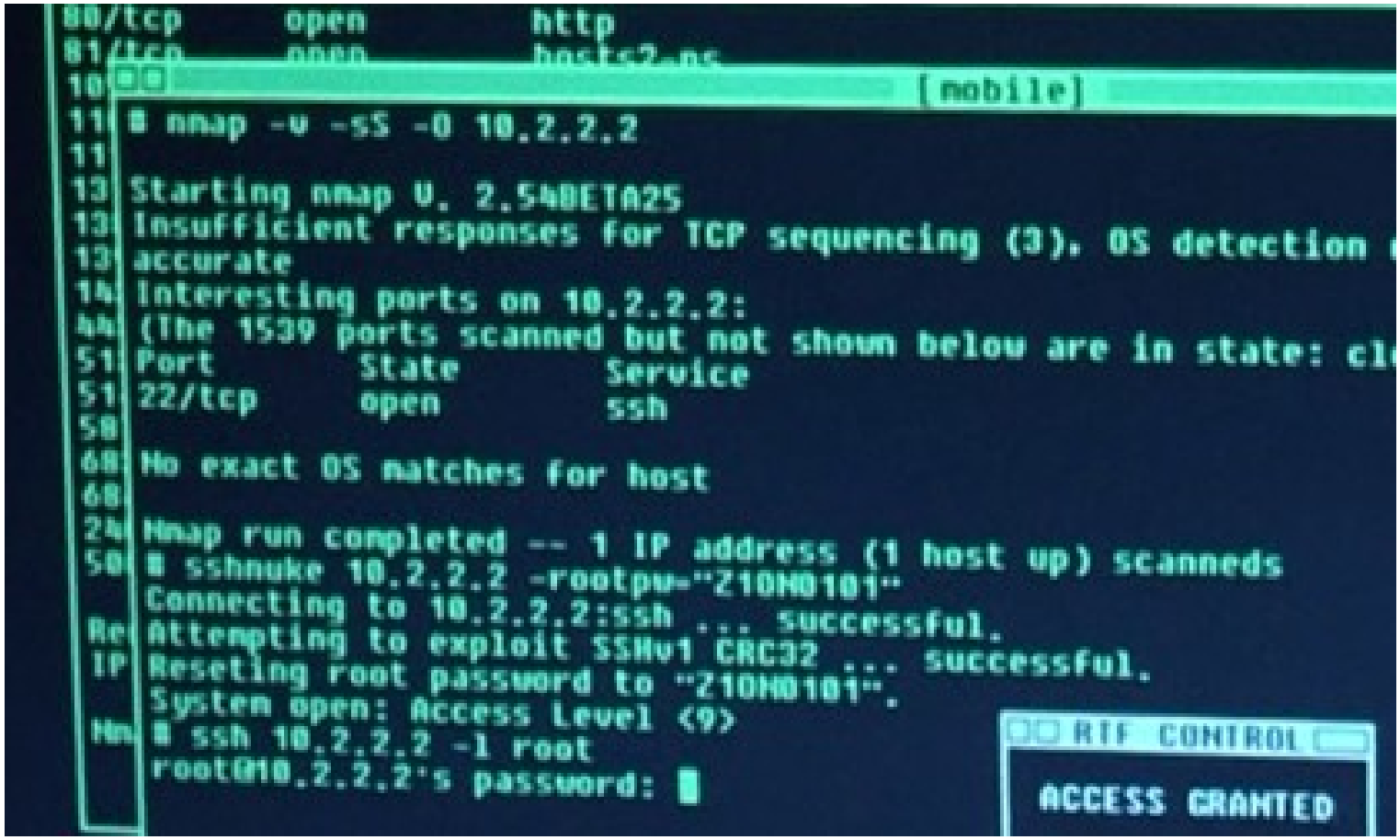
Formål



Lære om værktøjer der kan forbedre sikkerhed for produktionssystemer

Matrix style hacking anno 2003

Trinity breaking in



http://nmap.org/movies.html

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

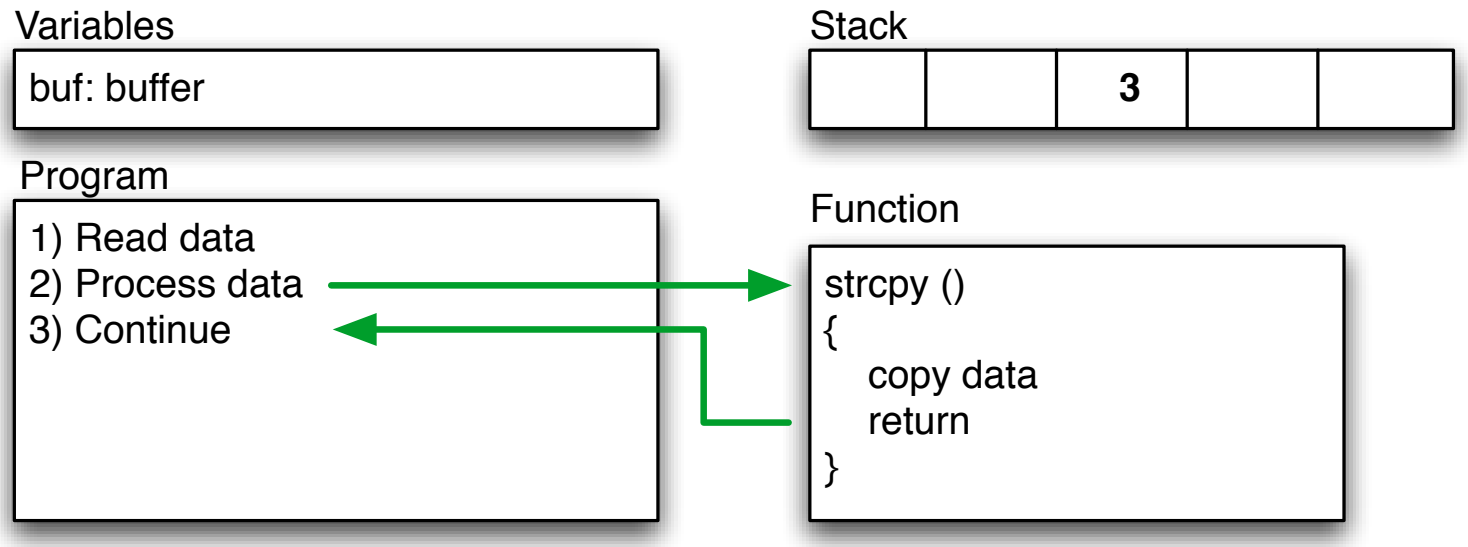
buffer overflows et C problem

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

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

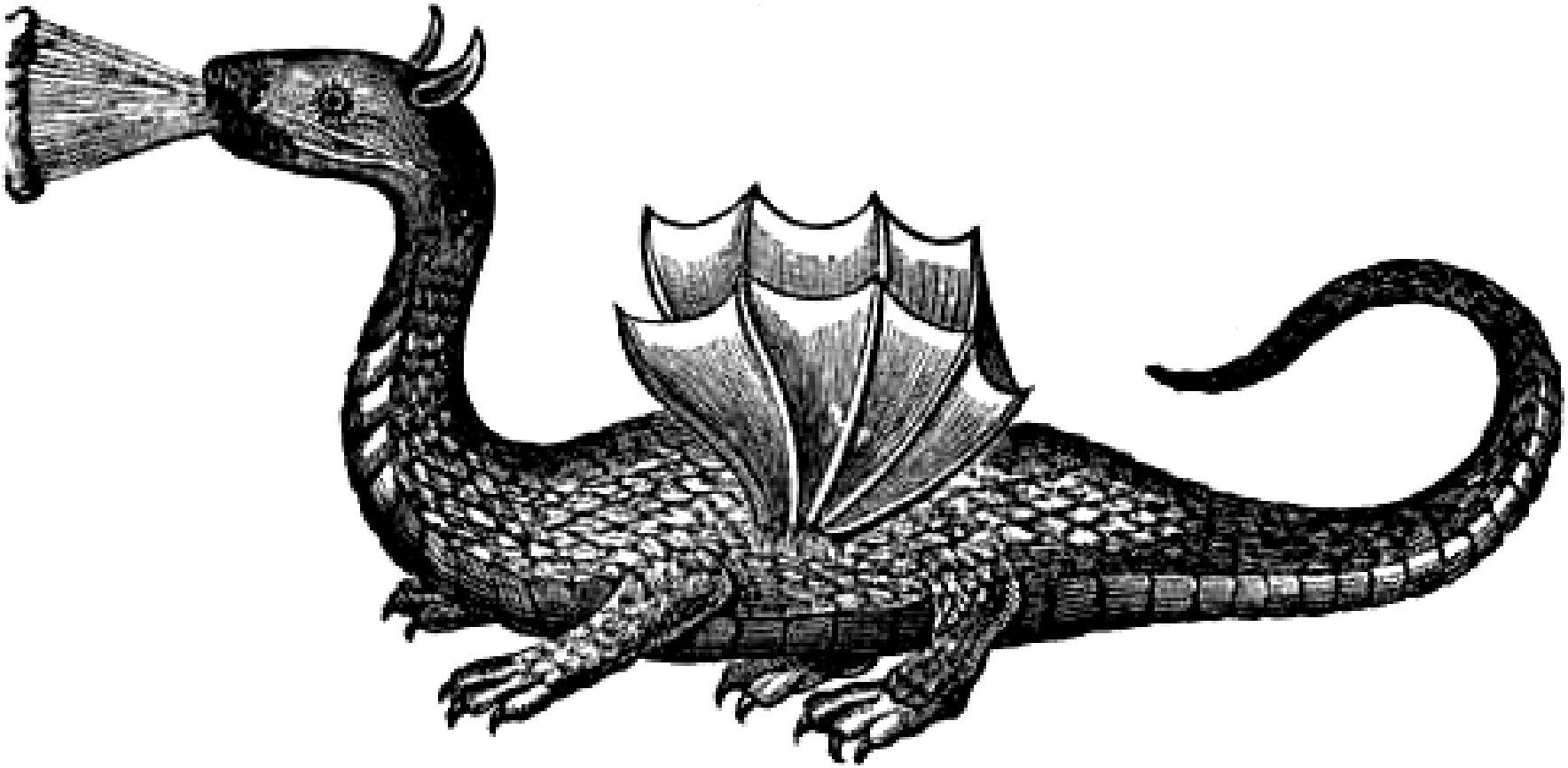
© copyright 2009 Security6.net, Henrik Lund Kramshøj

Buffer og stacks

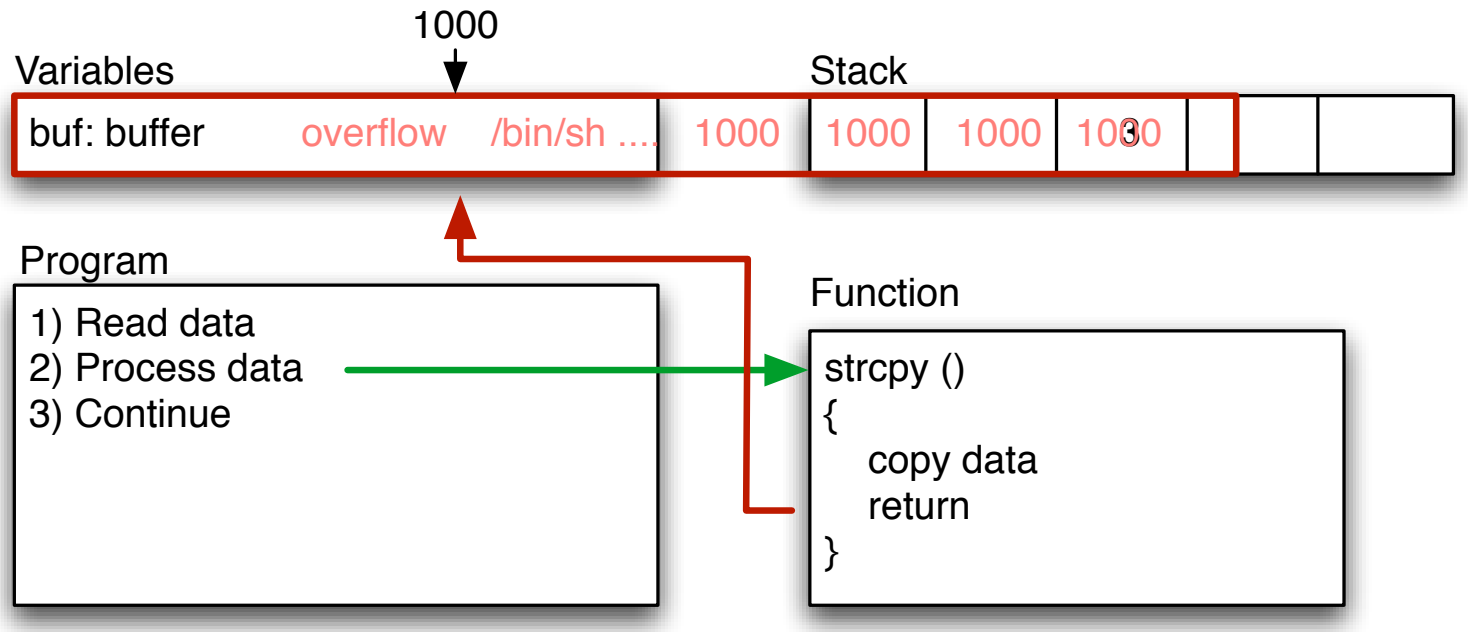



```
main(int argc, char **argv)
{       char buf[200];
         strcpy(buf, argv[1]);
         printf("%s\n",buf);
}
```

Internet - Here be dragons



Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

Exploits

```
$buffer = "";
$null = "\x00";
```

Exploits

```
$buffer = "";
$null = "\x00";
$nop = "\x90";
$nopsize = 1;
```

Exploits

```
$buffer = "";
$null = "\x00";
$nop = "\x90";
$nopsize = 1;
$len = 201; // what is needed to overflow, maybe 201, maybe more!
$the_shell_pointer = 0xdeadbeef; // address where shellcode is
# Fill buffer
for ($i = 1; $i < $len;$i += $nopsize) {
    $buffer .= $nop;
}
```

Exploits

```
$buffer = "";
$null = "\x00";
$nop = "\x90";
$nopsize = 1;
$len = 201; // what is needed to overflow, maybe 201, maybe more!
$the_shell_pointer = 0xdeadbeef; // address where shellcode is
# Fill buffer
for ($i = 1; $i < $len;$i += $nopsize) {
    $buffer .= $nop;
}
$address = pack('l', $the_shell_pointer);
$buffer .= $address;
```

Exploits

```
$buffer = "";
$null = "\x00";
$nop = "\x90";
$nopsize = 1;
$len = 201; // what is needed to overflow, maybe 201, maybe more!
$the_shell_pointer = 0xdeadbeef; // address where shellcode is
# Fill buffer
for ($i = 1; $i < $len;$i += $nopsize) {
    $buffer .= $nop;
}
$address = pack('l', $the_shell_pointer);
$buffer .= $address;
exec "$program", "$buffer";
```

Demo exploit in Perl

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Hvordan laves et buffer overflow?

Black box testing

Closed source reverse engineering

Findes ved at prøve sig frem - fuzzing

Open source betyder man kan læse og analysere koden

Exploits virker typisk mod specifikke versioner af software

Forudsætninger

Bemærk: alle angreb har forudsætninger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

Kan du bryde kæden af forudsætninger har du vundet!

alle programmer har fejl

Computeren skal være tændt

Funktionen der misbruges skal være slået til

Executable stack

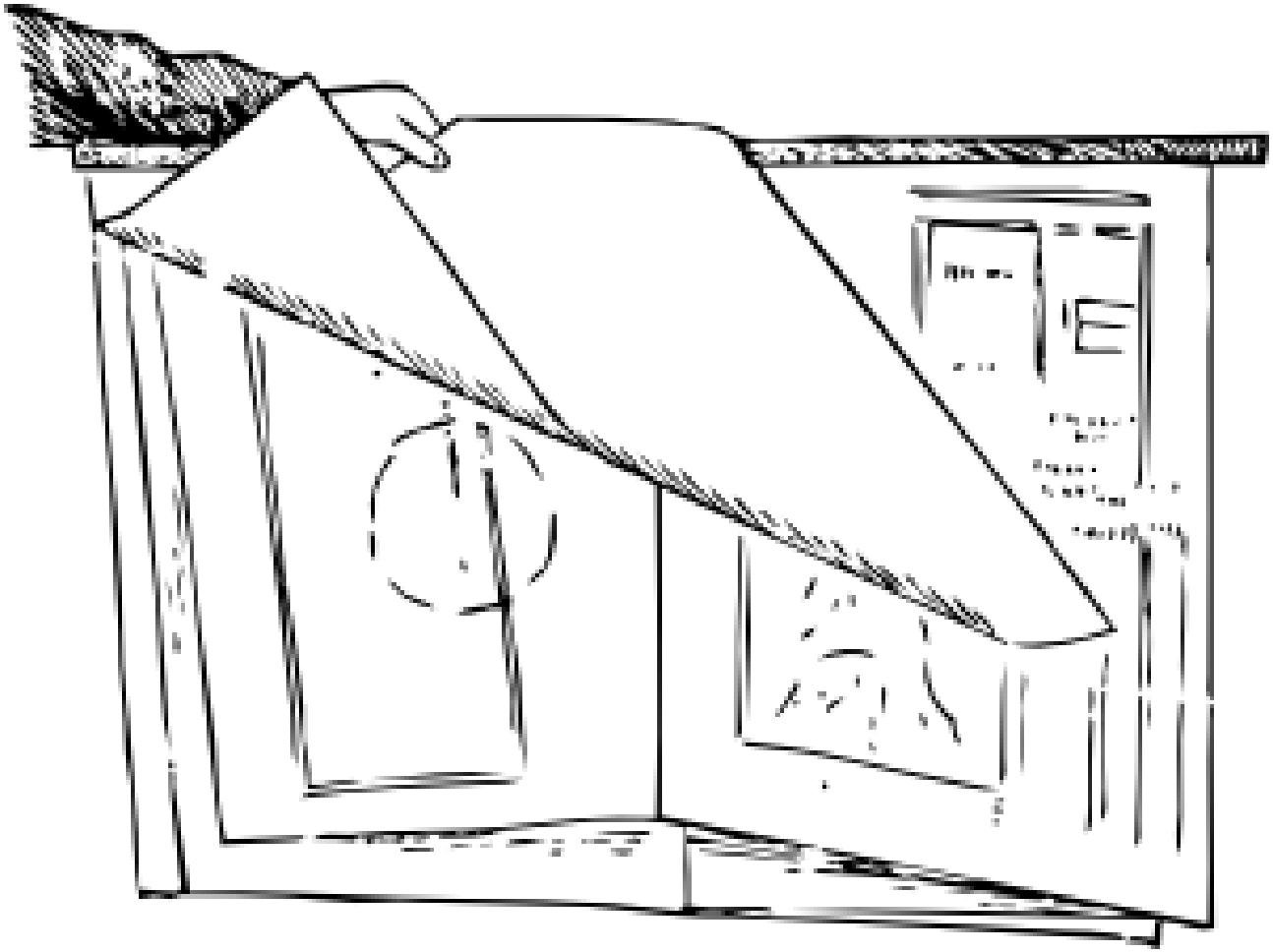
Executable heap

Fejl i programmet

© copyright 2009 Security6.net, Henrik Lund Kramshøj

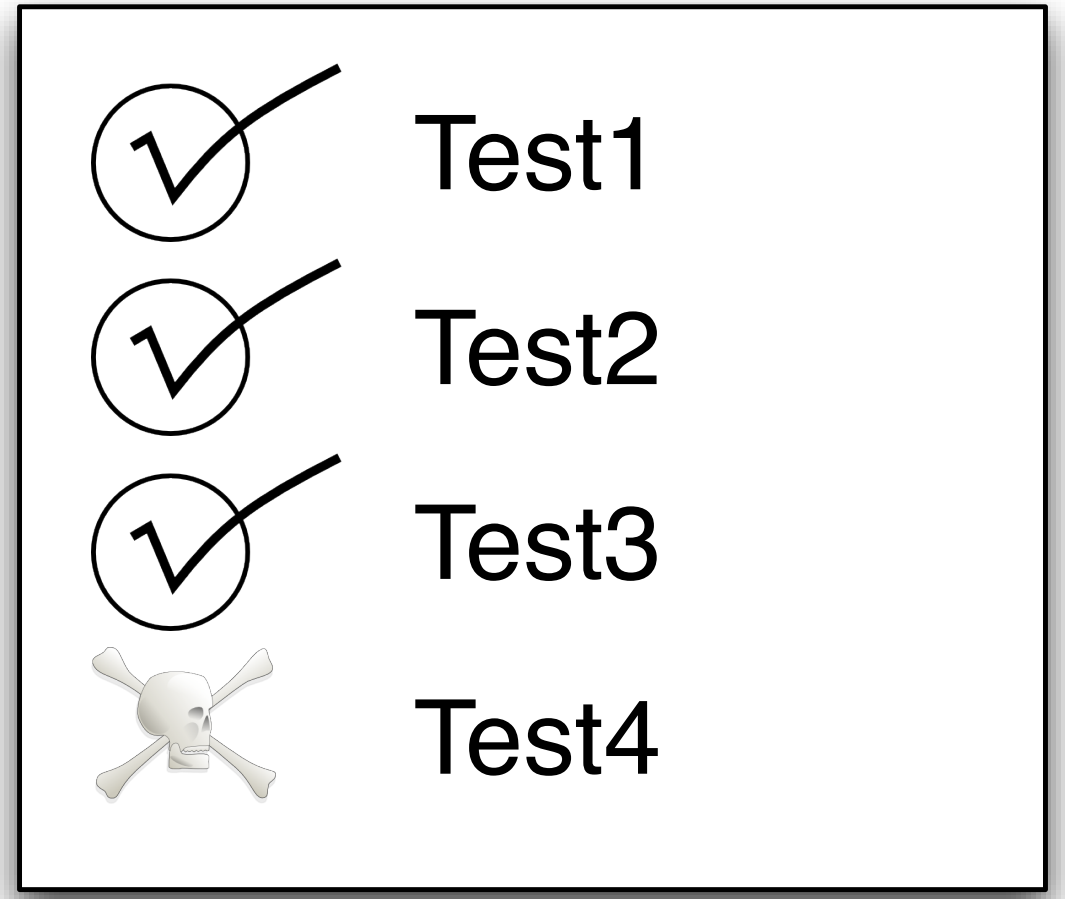
Part 1 Low hanging fruits - easy

Part 2 More work Design for security



Sikkerhed er mere effektivt hvis det tænkes ind i design

Part 3 Testing



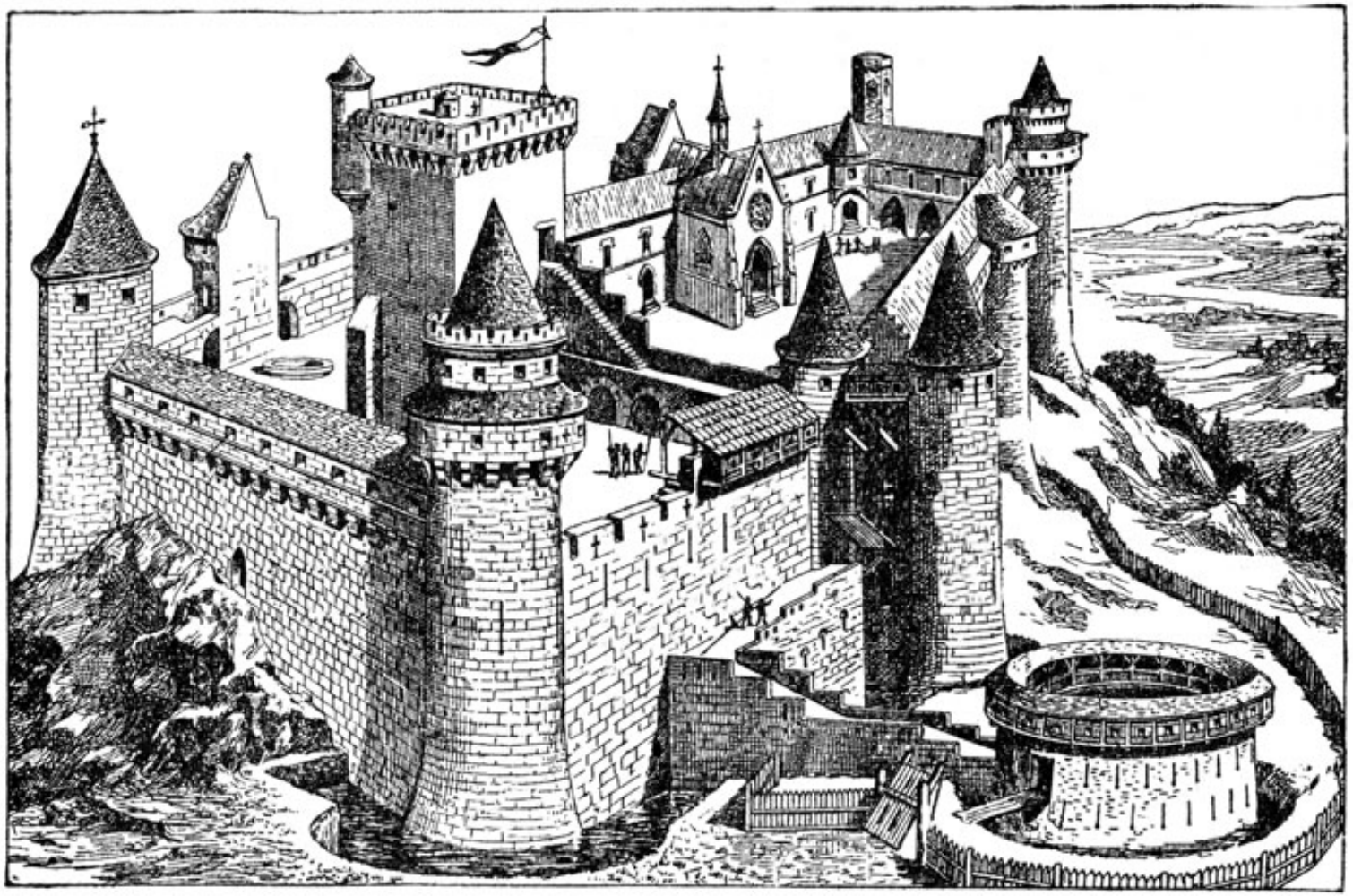
continous building and testing

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Part 4 Analysis

PMD RATS Flawfinder ...

Part 5 Enhance and secure environment



Gode operativsystemer

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

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

OpenBSD er nok nået længst og et godt eksempel
http://www.openbsd.org/papers/

Part 6 Break it

Use fuzzer, hackertools, improve security by breaking it

Hackerværktøjer

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

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

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

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

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

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

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Informationssikkerhed

Husk følgende:

Sikkerhed kommer fra langsigtede intiativer

Hvad er informationssikkerhed?

Data på elektronisk form

Data på fysisk form

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

Informationssikkerhed er en proces

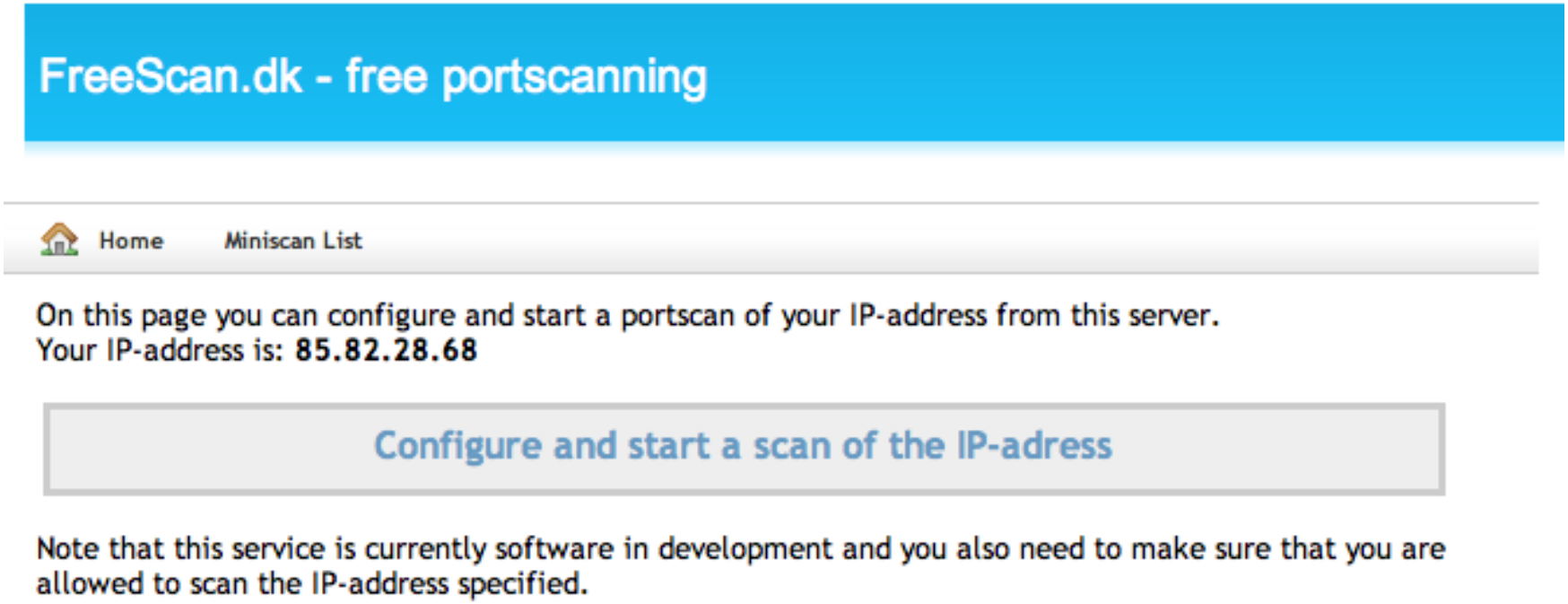
Spørgsmål?

Henrik Lund Kramshøj
hlk@security6.net

http://www.security6.net

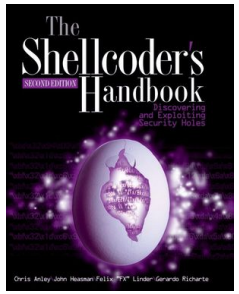
I er altid velkomne til at sende spørgsmål på e-mail

FreeScan.dk - gratis portscanning



http://www.freescan.dk

Buffer overflows



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

Smashing The Stack For Fun And Profit Aleph One

Writing Buffer Overflow Exploits with Perl - anno 2000

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

NB: bogen er avanceret og således IKKE for begyndere!

milw0rm - dagens buffer overflow

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

MILW0RM

[highlighted]

-::DATE	-::DESCRIPTION	-::HITS					-::AUTHOR
2009-03-05	Winamp <= 5.541 Skin Universal Buffer Overflow Exploit	3128	R		D		SkD
2009-02-26	Coppermine Photo Gallery <= 1.4.20 (BBCode IMG) Privilege Escalation	7338	R		D		StAkeR
2009-02-25	Apple MACOS X xnu <= 1228.x Local Kernel Memory Disclosure Exploit	4111	R		D		mu-b
2009-02-23	Adobe Acrobat Reader JBIG2 Local Buffer Overflow PoC #2 0day	17652	R		D		Guido Landi
2009-02-23	MLdonkey <= 2.9.7 HTTP DOUBLE SLASH Arbitrary File Disclosure Vuln	4225	R		D		Michael Peselnik
2009-02-23	Multiple PDF Readers JBIG2 Local Buffer Overflow PoC	7781	R		D		webDEVIL

[remote]

-::DATE	-::DESCRIPTION	-::HITS					-::AUTHOR
2009-03-05	SupportSoft DNA Editor Module (dnaedit.dll) Code Execution Exploit	1093	R		D	X	Nine:Situations:Group
2009-03-04	Easy File Sharing Web Server 4.8 File Disclosure Vulnerability	1424	R		D		Stack
2009-03-04	EFS Easy Chat Server Authentication Request Buffer Overflow Exploit (pl)	969	R		D		Dr4sH
2009-03-04	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (fast)	3965	R		D		Ahmed Obied
2009-03-03	EFS Easy Chat Server (XSRF) Change Admin Pass Vulnerability	1215	R		D		Stack
2009-03-03	Imera ImeraIEPlugin ActiveX Control Remote Code Execution Exploit	1020	R		D		Elazar

[local]

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

http://milw0rm.com/

Metasploit

What is it?

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

Trinity brugte et exploit program ☺

Idag findes der samlinger af exploits som milw0rm

Udviklingsværktøjerne til exploits er idag meget raffinerede!

http://www.metasploit.com/

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Reklamer: kursusafholdelse

Security6.net

Følgende kurser afholdes med mig som underviser

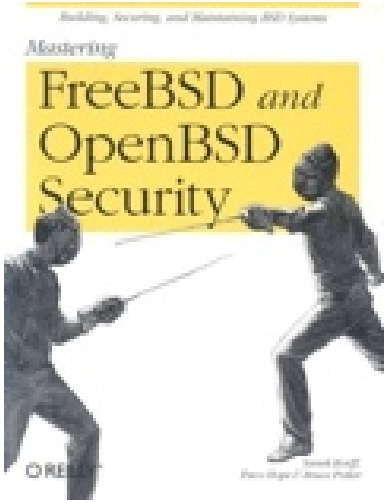
- IPv6 workshop - 1 dag
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop - 2 dage
  En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk, samt integration med hjemmepc og wirksomhedsnetværk.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

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

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Network Security Tools

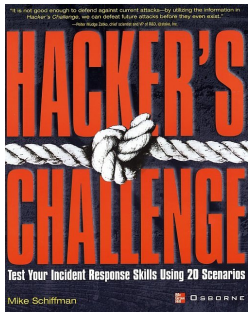
Network Security Tools : Writing, Hacking, and Modifying Security Tools Nitesh Dhanjani, Justin Clarke, O'Reilly 2005, ISBN: 0596007949

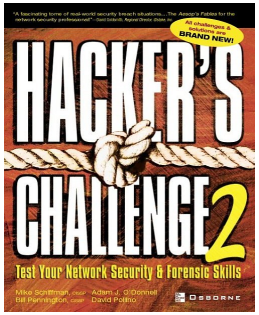


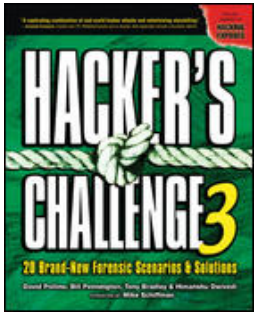
Mastering FreeBSD and OpenBSD Security Yanek Korff, Paco Hope, Bruce Potter, O'Reilly, 2005, ISBN: 0596006268

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Hackers Challenge







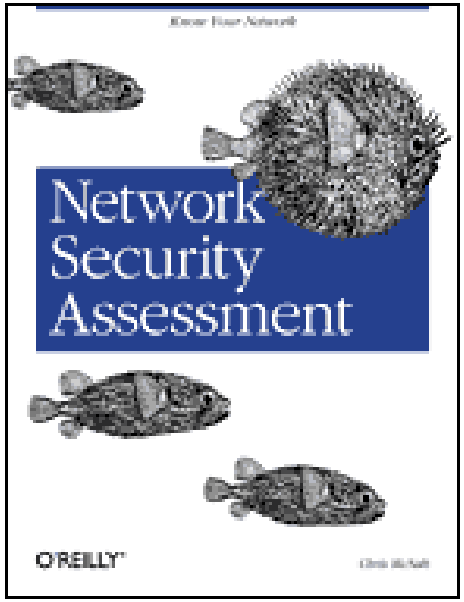
Hacker's Challenge : Test Your Incident Response Skills Using 20 Scenarios af Mike Schiffman McGraw-Hill Osborne Media; (October 18, 2001) ISBN: 0072193840

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

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

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

Network Security Assessment

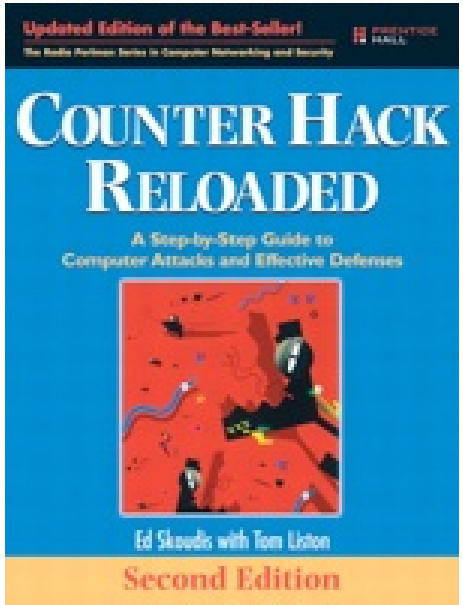


Network Security Assessment Know Your Network af Chris McNab, O'Reilly Marts 2004 ISBN: 0-596-00611-X

Bogen er anbefalelsesværdig

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

Counter Hack



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

Bogen er anbefalelsesværdig og er kommet i anden udgave

Minder mig om et universitetskursus i opbygningen

http://www.counterhack.net

Referencer

Anbefalede bøger:

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

© copyright 2009 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

Packet factory projects

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

CISSP fra ISC2

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

Primære website: http://www.isc2.org

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

Den kræver mindst 3 års erfaring indenfor et relevant fagområde

Multiple choice 6 timer 250 spørgsmål - kan tages i Danmark

CEH

Certified Ethical Hacker

Certified Ethical Hacker exam 312-50

Bogen *CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50* af Kimberly Graves kan anbefales

Primære website: `http://eccouncil.org/ceh.htm`

GIAC GSEC

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/`