

Welcome to

# Capture The Flag intro - basic hacking

Henrik Lund Kramshøj  
hlk@solidonetworks.com

`http://www.solidonetworks.com`

Slides are available as PDF

# Formålet med introduktionen

Beskrive setup

Svare på spørgsmål

## 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

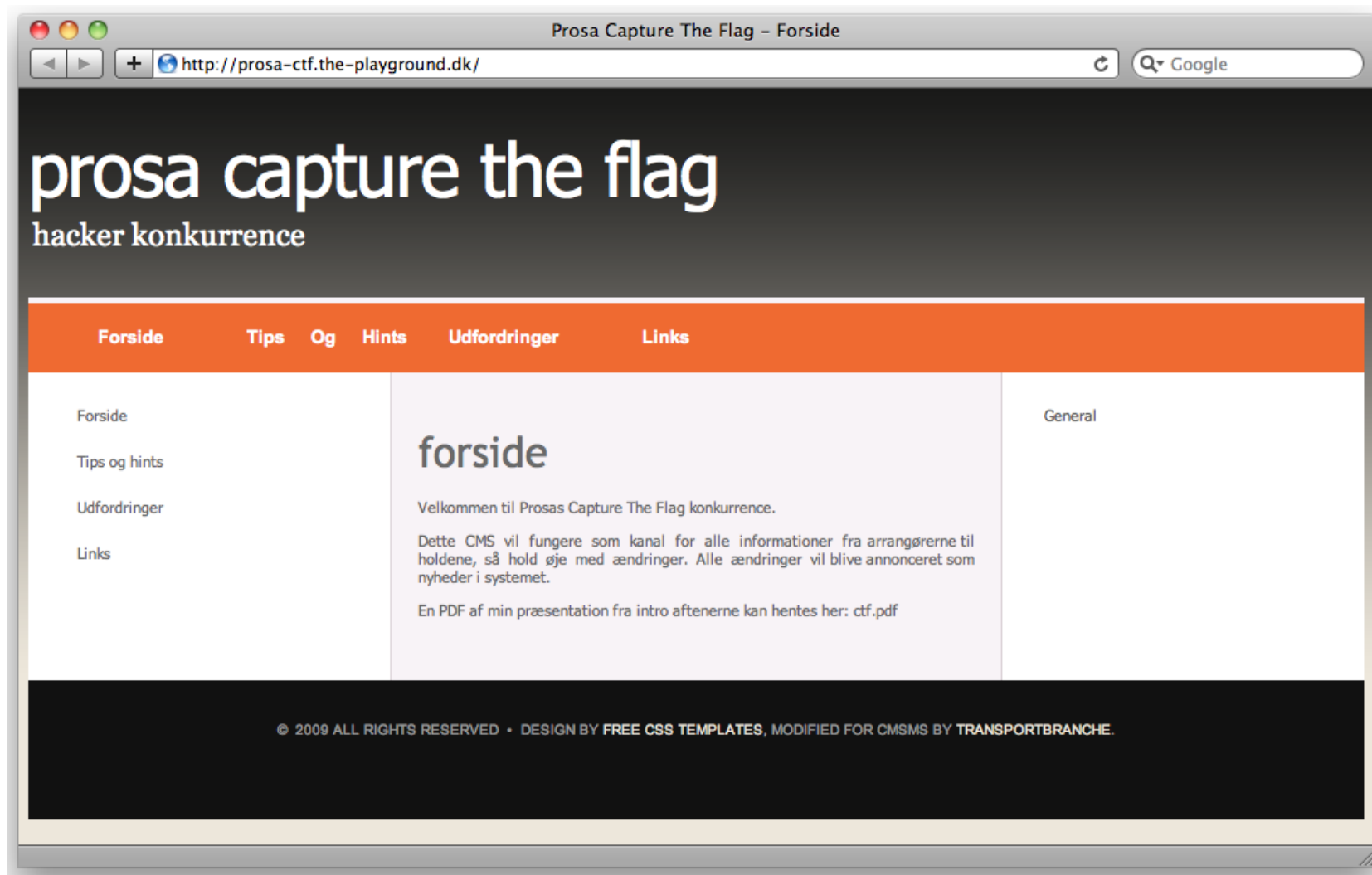
Hvis man vil vide mere kan man starte med:

- *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

**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!



<http://prosa-ctf.the-playground.dk/>

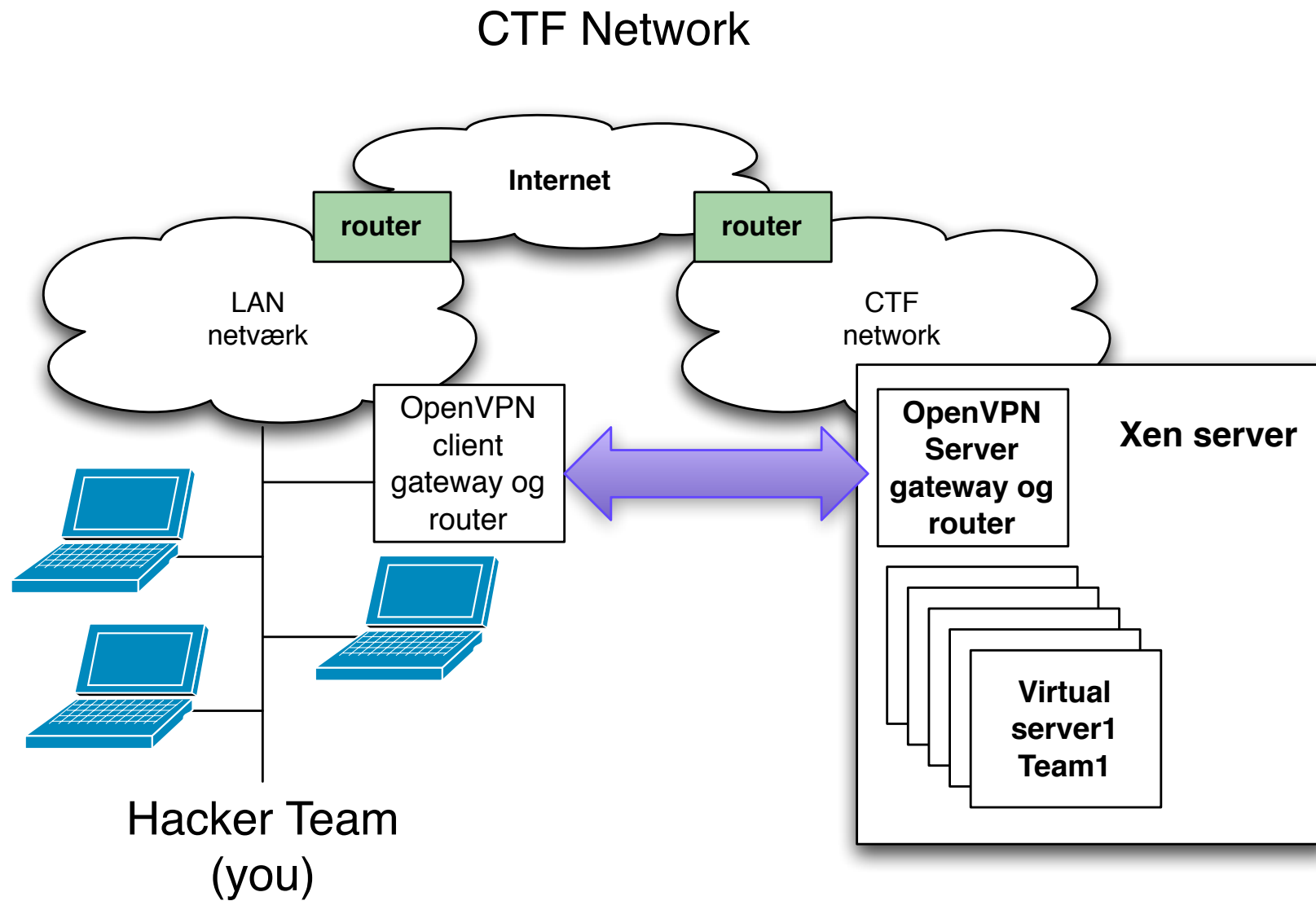
Man deltager som hold

Man får en virtuel maskine

Man får lov til at hacke de andres virtuelle maskiner

Play fair :-)

Admingruppen, Henrik og Robert er newbies i afholdelse af CTF



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`



Der benyttes en del værktøjer:

- **nmap** - <http://www.insecure.org/portscanner>
- **Wireshark** - <http://http://www.wireshark.org/> avanceret netværkssniffer
- **BackTrack** <http://www.remote-exploit.org/backtrack.html>
- **Putty** - <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> terminal emulator med indbygget SSH
- **OpenVPN** - <http://www.openvpn.org> VPN adgang til CTF systemerne
- **OpenBSD** - <http://www.openbsd.org> operativsystem med fokus på sikkerhed, kan bruges som OpenVPN router

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.

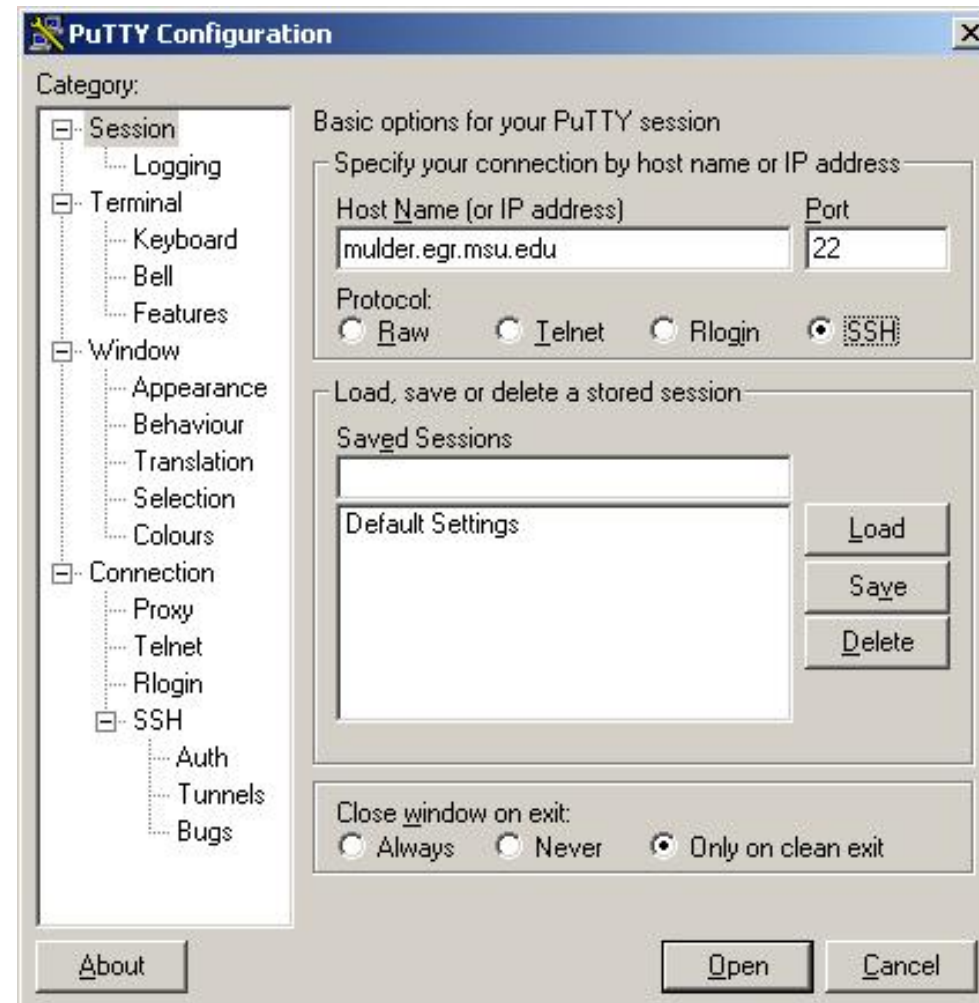
kommandoerne er:

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

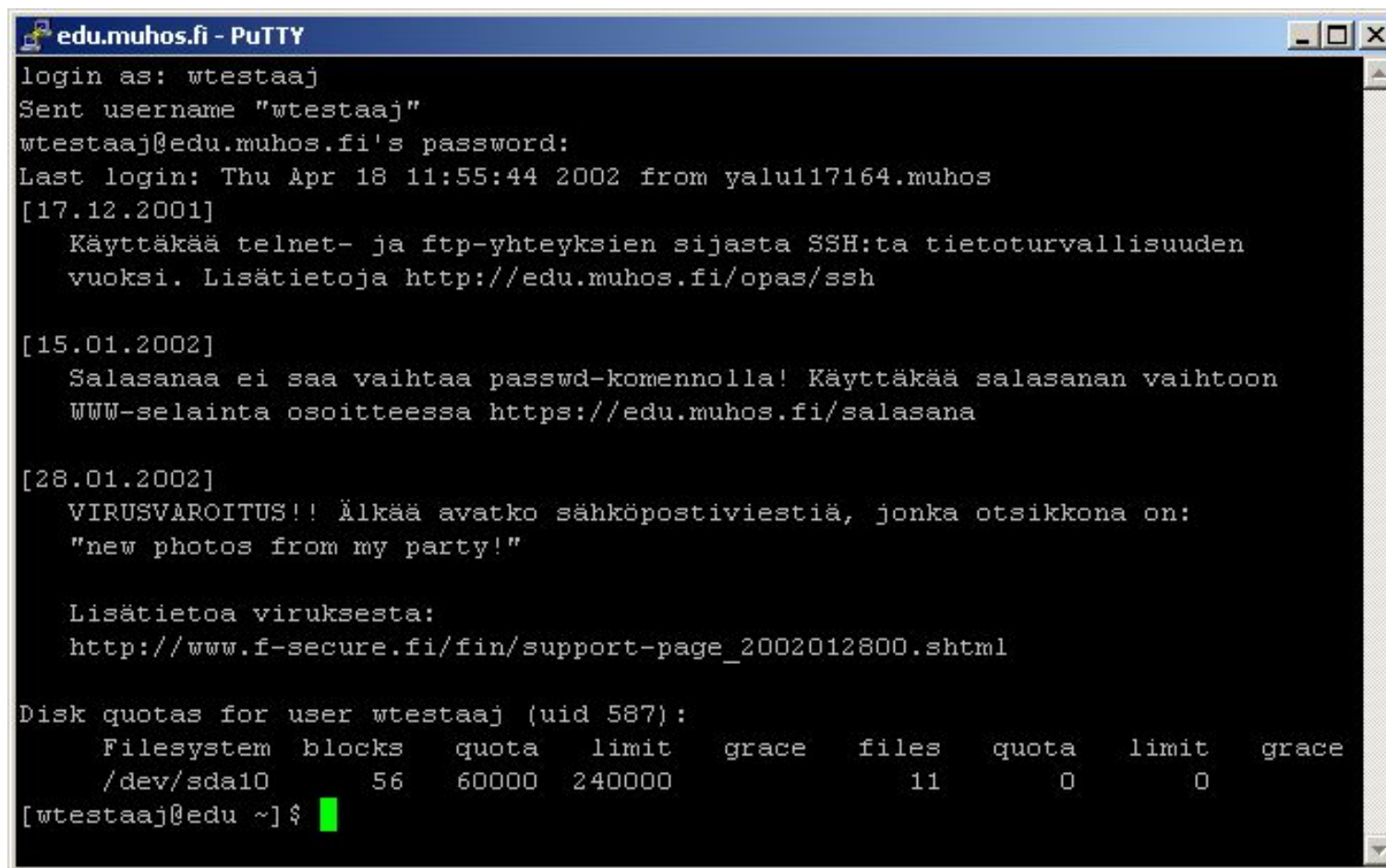
Husk: SSH er både navnet på protokollerne - version 1 og 2 samt programmet `ssh` til at logge ind på andre systemer

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!**



Login skærmen til Putty terminal programmet



```
edu.muhos.fi - PuTTY
login as: wtestaaaj
Sent username "wtestaaaj"
wtestaaaj@edu.muhos.fi's password:
Last login: Thu Apr 18 11:55:44 2002 from yalu117164.muhos
[17.12.2001]
    Käyttäkää telnet- ja ftp-yhteyksien sijasta SSH:ta tietoturvallisuuden
    vuoksi. Lisätietoja http://edu.muhos.fi/opas/ssh

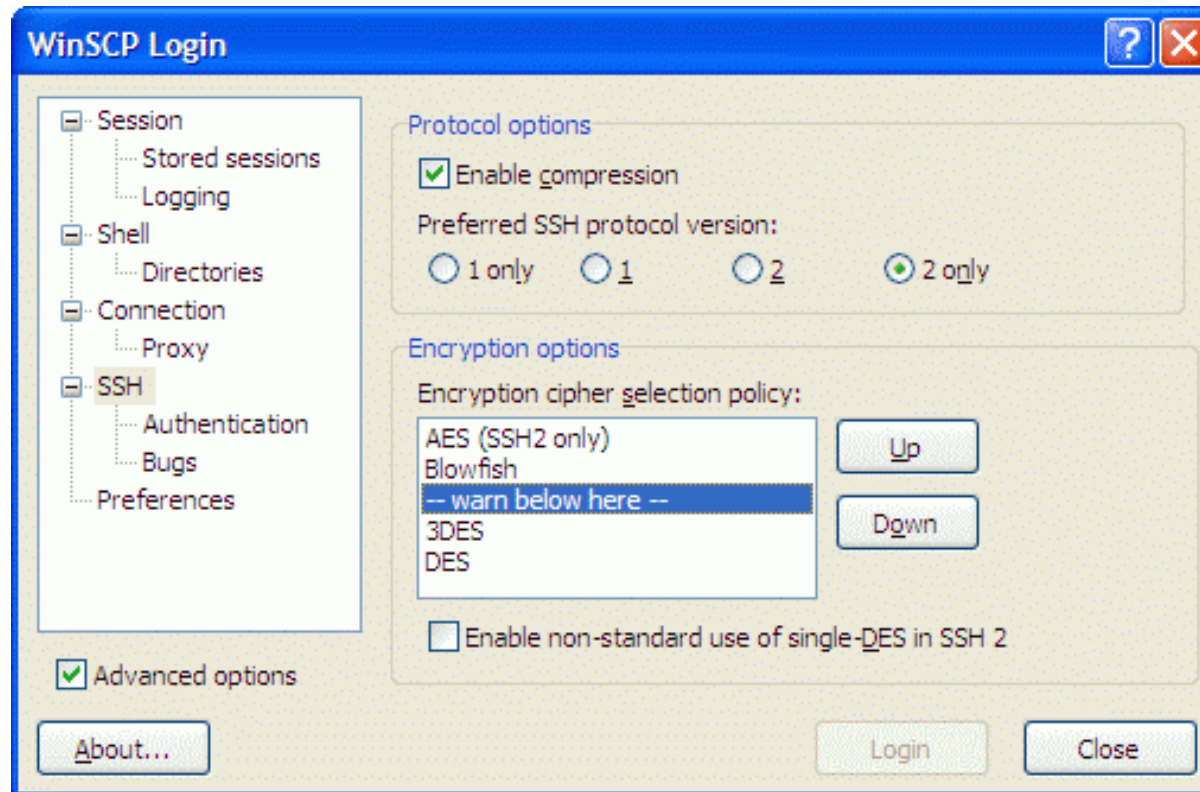
[15.01.2002]
    Salasanaa ei saa vaihtaa passwd-komennolla! Käyttäkää salasanan vaihtoon
    WWW-selainta osoitteessa https://edu.muhos.fi/salasana

[28.01.2002]
    VIRUSVAROITUS!! Älkää avatko sähköpostiviestiä, jonka otsikkona on:
    "new photos from my party!"

    Lisätietoa viruksesta:
    http://www.f-secure.fi/fin/support-page\_2002012800.shtml

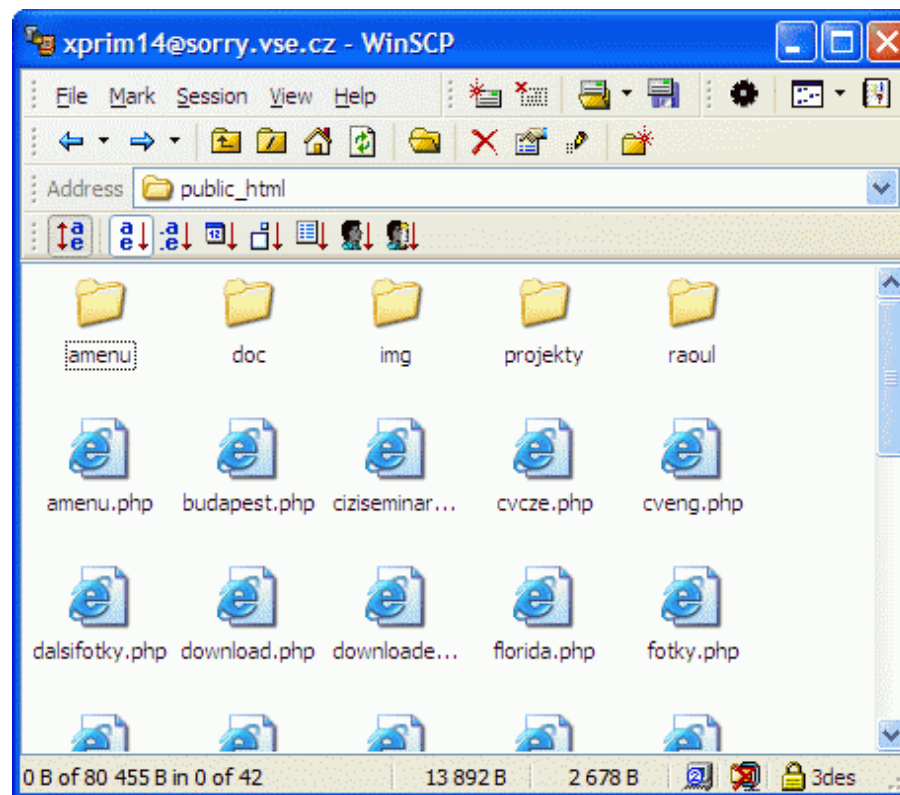
Disk quotas for user wtestaaaj (uid 587):
   Filesystem  blocks   quota  limit  grace  files   quota  limit  grace
   /dev/sda10     56  60000 240000      0     11      0      0      0
[wtestaaaj@edu ~]$
```

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



screenshot fra

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



screenshot fra

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

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
```



Hvad er portscanning

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

målet er at identificere åbne porte - sårbare services

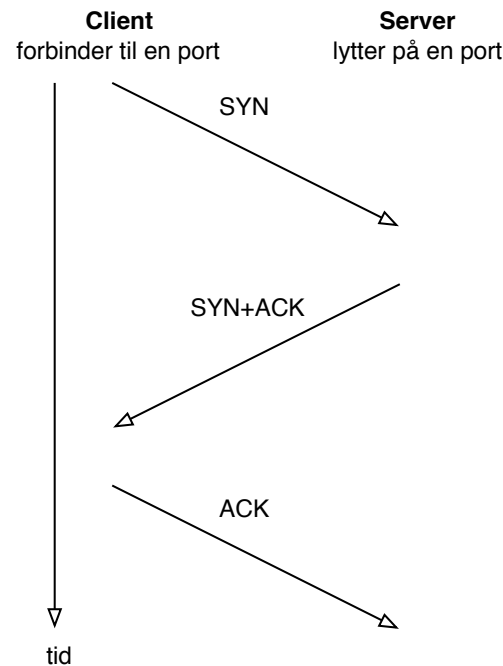
typisk TCP og UDP scanning

TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

# TCP three way handshake



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

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

## 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

## 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
```

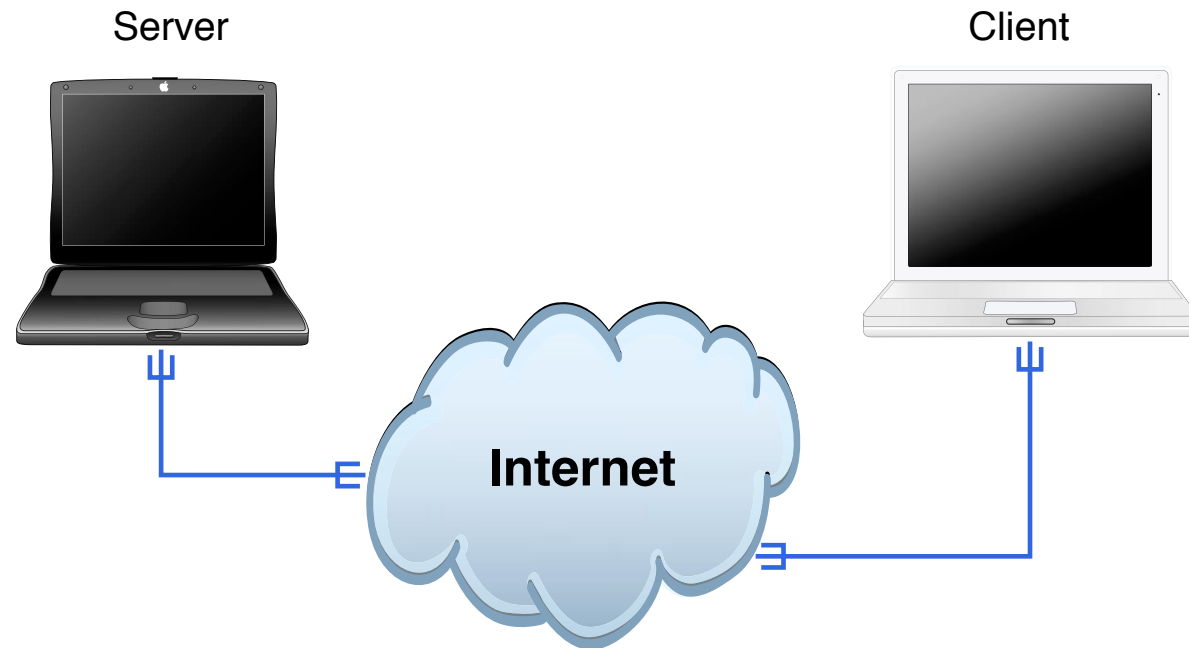
```
Interesting ports on www.kramse.dk (217.157.20.131):
```

Port	State	Service
161/udp	open	snmp

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

```
# 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>



## Portscans med Nmap Frontend program

**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

Eksempel:

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

**local vs. remote** 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

Findes ved at prøve sig frem

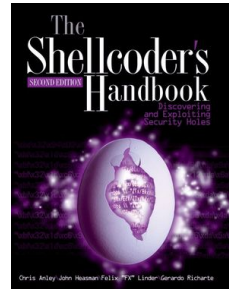
- black box testing
- closed source
- reverse engineering

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



*Smashing The Stack For Fun And Profit* Aleph One

*Writing Buffer Overflow Exploits with Perl* - anno 2000

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

NB: bogen er avanceret og således IKKE for begyndere!

Stack protection 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>

Jeg kan ikke vente til fredag!!!!111111

Jeg kan ikke vente til fredag!!!!111111

Se på Damn Vulnerable Linux :-)

<http://www.damnulnerablelinux.org/>

Henrik Lund Kramshøj  
hlk@solidonetworks.com

`http://www.solidonetworks.com`

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



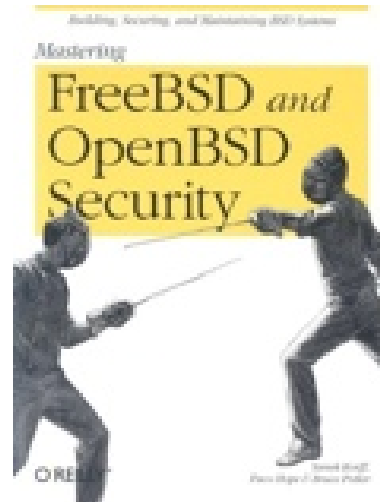
Følgende kurser afholdes med mig som underviser

- 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.

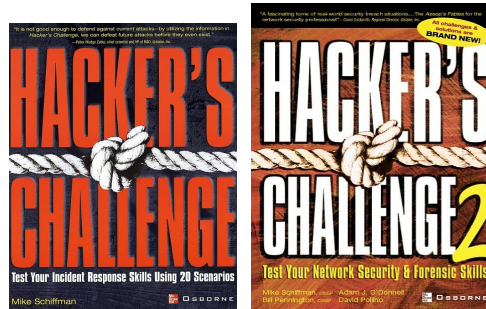
Se mere på <http://www.security6.net/courses.html>



*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



*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

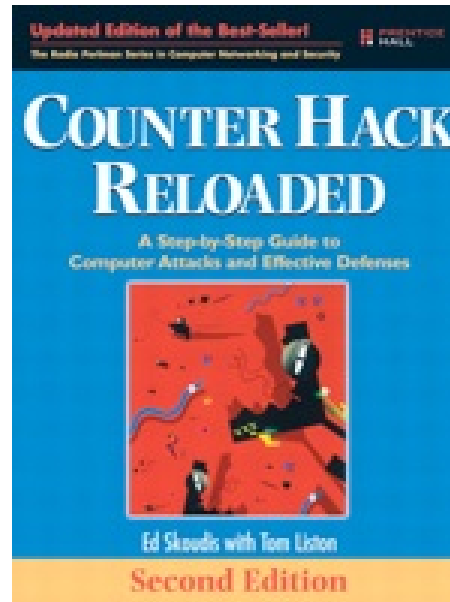
Hackers challenge nr 3 udkommer i 2006



*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: 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

- **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 hacker-værktøjer

## 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



## 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 værktøjer har mailinglister tilknyttet

## Papers - der findes MANGE dokumenter på Internet

- *Security Problems in the TCP/IP Protocol Suite*, S.M. Bellovin, 1989 og fremefter



- 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>

(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



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>