

The Insider Threat



FIRST • BASE
technologies

Peter Wood
First • Base
Technologies



Insiders - the Facts

- 70% - 80% of hacking comes from within the organisation
- 50% of job applicants misrepresent their credentials, of which:
 - 53% falsify length of employment
 - 51% inflate past salaries
 - 45% lie about their criminal records
 - 44% misrepresent their former job title
 - 35% falsely identify former employers

Information Systems Control Journal, Volume 3, 2002





Where to start?



Plug and go

Ethernet ports are never disabled

... or just steal a connection from a desktop

NetBIOS tells you lots and lots

.... And you don't need to be logged on



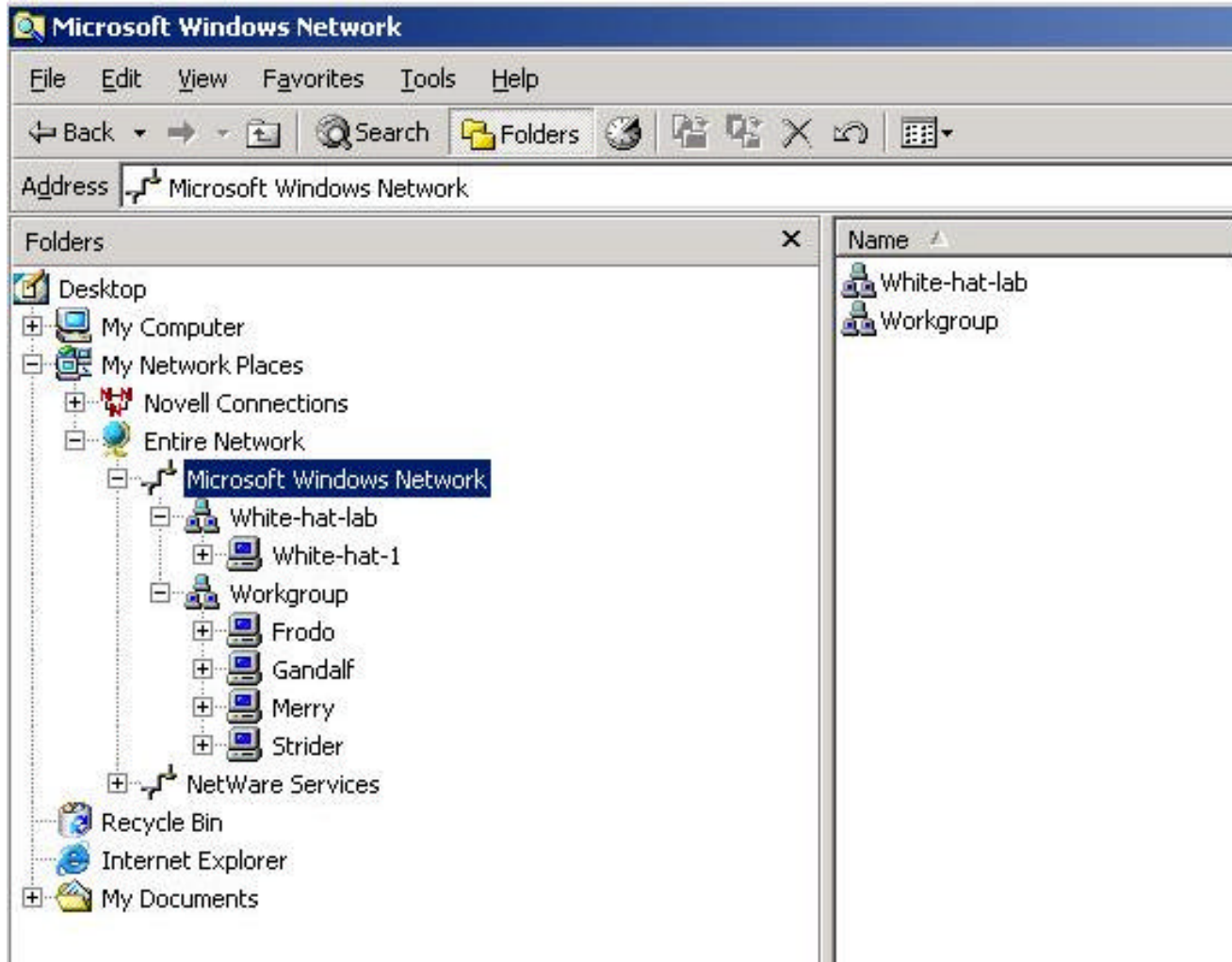
Get yourself an IP address

- Use DHCP since almost everyone does!
- Or ... use a sniffer to see broadcast packets (even in a switched network) and try some suitable addresses

1535	IP/UDP	00:02:E3:17:9E:A3 <=> Broadcast	192.168.254.88 <=> 192.168.254.255	137 <=> 137
1564	IP/UDP	00:02:E3:17:9E:A3 <=> Broadcast	192.168.254.88 <=> 192.168.254.255	137 <=> 137
1630	IP/UDP	00:02:E3:17:9E:A3 <=> Broadcast	192.168.254.88 <=> 192.168.254.255	137 <=> 137
2403	IP/UDP	00:02:E3:17:9E:A3 <=> Broadcast	192.168.254.88 <=> 192.168.254.255	137 <=> 137
2433	IP/UDP	00:02:E3:17:9E:A3 <=> Broadcast	192.168.254.88 <=> 192.168.254.255	137 <=> 137
2491	IP/UDP	00:02:E3:17:9E:A3 <=> Broadcast	192.168.254.88 <=> 192.168.254.255	137 <=> 137
3174	IP/UDP	00:02:E3:17:9E:A3 <=> Broadcast	192.168.254.88 <=> 192.168.254.255	138 <=> 138
4811	IP/UDP	00:01:E6:3F:A2:D7 <=> Broadcast	0.0.0.0 <=> 255.255.255.255	68 <=> 67
5069	IP/UDP	00:02:E3:17:9E:A3 <=> Broadcast	192.168.254.88 <=> 192.168.254.255	137 <=> 137
5098	IP/UDP	00:02:E3:17:9E:A3 <=> Broadcast	192.168.254.88 <=> 192.168.254.255	137 <=> 137
5127	IP/UDP	00:02:E3:17:9E:A3 <=> Broadcast	192.168.254.88 <=> 192.168.254.255	137 <=> 137

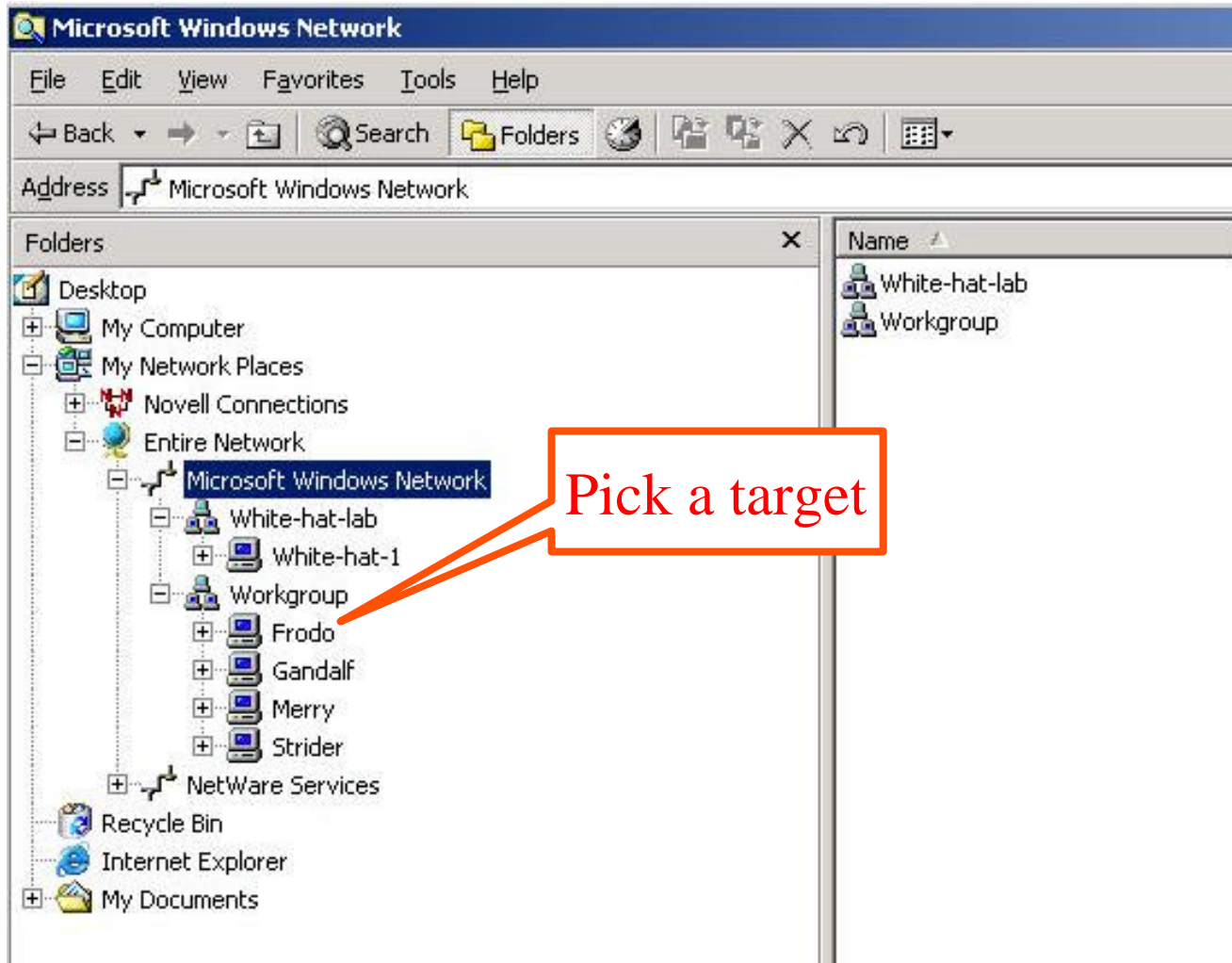


Browse the network





Pick a target machine





Try null sessions ...

```
C:\>nbtstat -a frodo

Local Area Connection:
Node IpAddress: [192.168.254.48] Scope Id: []

          NetBIOS Remote Machine Name Table

   Name                Type               Status
-----
   FRODO                <00>              UNIQUE            Registered
   FRODO                <20>              UNIQUE            Registered
   WORKGROUP            <00>              GROUP             Registered
   FRODO                <03>              UNIQUE            Registered
   WORKGROUP            <1E>              GROUP             Registered
   KEIRON               <03>              UNIQUE            Registered
   WORKGROUP            <1D>              UNIQUE            Registered
   .._MSBROWSE_..      <01>              GROUP             Registered

MAC Address = 00-02-E3-17-9E-A3

C:\>net use \\frodo\ipc$ "" /u:""
The command completed successfully.

C:\>_
```



... and list administrators!

Somarsoft DumpSec (formerly DumpAcl) - \\frodo

File Edit Search Report View Help

Group	MemberType	GroupMember
Administrators	User	Administrator
Administrators	User	keiron
Administrators	User	pete
Backup Operators		
Guests	User	Guest
Power Users		
Replicator		
Users	User	pete

Found 6 groups

00001

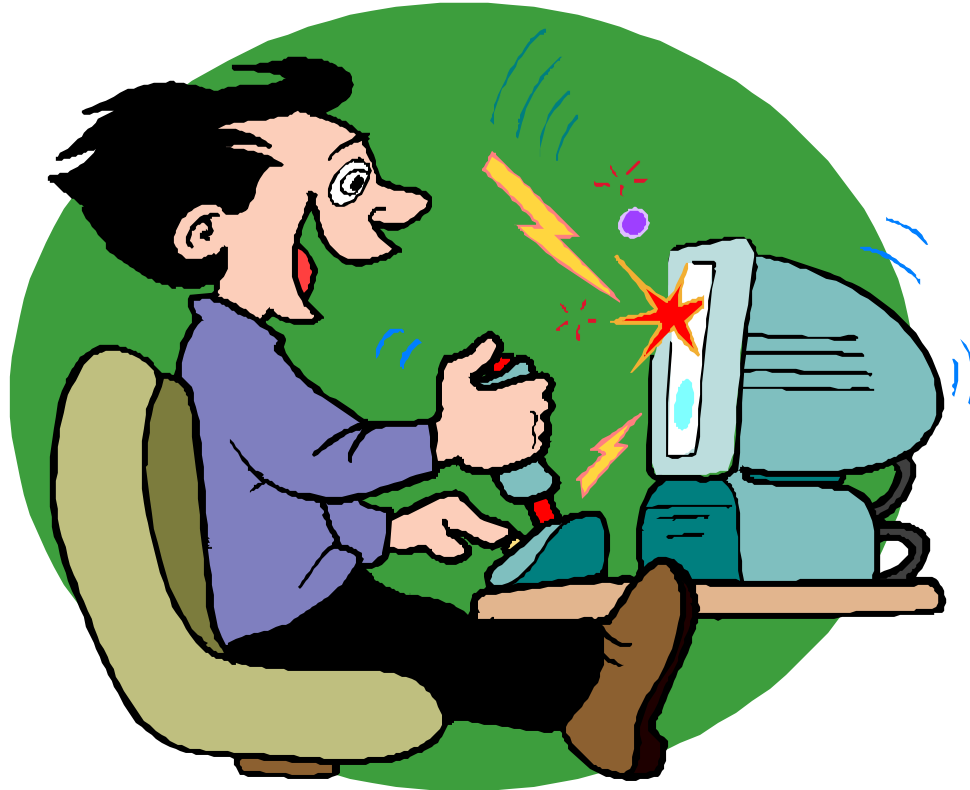


Typical passwords

- administrator null, password, administrator
- arcserve arcserve, backup
- test test, password
- username username, company
- backup backup
- tivoli tivoli
- backupexec backup



Game over!





Unprotected Shares



Browse for shared c-drives

The screenshot shows a Windows Explorer window with the following table of contents:

Name	Size	Type	Modified	Attributes
Jeeves.pwl	1KB	PWL File	7/27/00 5:37 PM	A

An orange callout box with the text "Find a PWL file" points to the selected file "Jeeves.pwl".

At the bottom of the window, the status bar indicates "1 object(s) selected" and "0.97KB".



Crack the PWL file

Repwl (version 6.5, commercial)

PWL file: H:\EXTERNAL\ [redacted] \Network Browse

User name: JEEVES Glide

Password: CheckPass

Brute force | SmartForce | Dictionary

Dictionary: G:\SOURCES\SECURITY\Dictionaryes\ Browse

Hybrid brute

0:0:0:1
???? p/sec

CPU About

SearchPasswordFast SearchPassword

CheckPassFast Client/Server

Zombie mode Help Adv

Cached passwords

File: [redacted] \Network

review\Jeeves\JEEVES.PWL
User name: 'JEEVES'
Password: "

Mail: 'jif{650}P'"
Password: 'wooster'

Mail: 'jif{650}P'"
Password: "

NW Server: 'ERIK'
Login: password: 'JEEVES:WOOSTER'
NW Server: 'FQM'
Login: password: 'JEEVES:WOOSTER'
NW Server: 'FRED'
Login: password: 'JEEVES:WOOSTER'
NW Server: 'FQM1'
Login: password: 'JEEVES:WOOSTER'



Use the logon

The screenshot displays a Windows XP desktop environment. In the background, a 'Folders' window shows a tree view of the file system, including 'My Computer', 'My Network Places', and 'Novell Connections'. The 'Novell Connections' folder is expanded, showing a 'Firstbase' connection. In the foreground, a 'Novell Login' dialog box is open. The dialog box has a red header with the text 'Novell. Client FOR WINDOWS NT/2000'. Below the header, there are two input fields: 'Username:' with the text 'Jeeves' and 'Password:' with masked characters '*****'. There are two tabs: 'Bindery' (selected) and 'Script'. Below the tabs, there is a 'Server:' dropdown menu with 'firstbase' selected. At the bottom of the dialog box are 'OK' and 'Cancel' buttons.



Game over!





Plain Text Passwords



Netlogon

In the unprotected netlogon share on a server:
logon scripts can contain:
`net use \\server\share "password" /u:"user"`





Registry Scripts

In shared directories you may find
.reg files like this:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon]  
"DefaultUserName"="username"  
"DefaultPassword"="password"  
"AutoAdminLogon"="1"
```



Simple Searches

The screenshot shows a Windows Search Results window with the following details:

- Search Criteria:** A red circle highlights the search criteria section, which includes:
 - Search for files or folders named: *.doc
 - Containing text: password
- Location:** Look in: Data on 'Firstbase' (G:)
- Buttons:** Search Now and Stop Search
- Search Options:** A list of checkboxes for Date, Type, Size, and Advanced Options, all of which are currently unchecked.
- Search Results:** The main pane on the right is empty, displaying the text "Enter your search criteria to begin."
- Status Bar:** Shows "0 object(s)" at the bottom left.



Packet Sniffing

- Leave the sniffer running
- Capture all packets to port 23 or 21
- Run the capture file through TCP.demux
- The result ...

Generated by : TCP.demux V1.02

Input File: carol.cap

Output File: TB000463.txt

Summary File: summary.txt

Date Generated: Thu Jan 27 08:43:08 2000

10.1.1.82 1036

10.1.2.205 23 (telnet)

UnixWare 2.1.3 (mikew) (pts/31).

login:

cl_Carol

Password:

carollzz

UnixWare 2.1.3.

mikew.

Copyright 1996 The Santa Cruz Operation, Inc. All Rights Reserved..

Copyright 1984-1995 Novell, Inc. All Rights Reserved..

Copyright 1987, 1988 Microsoft Corp. All Rights Reserved..

U.S. Pat. No. 5,349,642.



Game over!





Password Cracking



How to get the SAM

- Server memory (registry)
- `c:\winnt\repair\sam` (invoke `rdisk?`)
- Emergency Repair Disk
- Backup tapes
- L0phtcrack's sniffer



Cracking - L0phtcrack

C:\Program Files\L0phtCrack 2.5\pwd278.lc - L0phtCrack 2.5

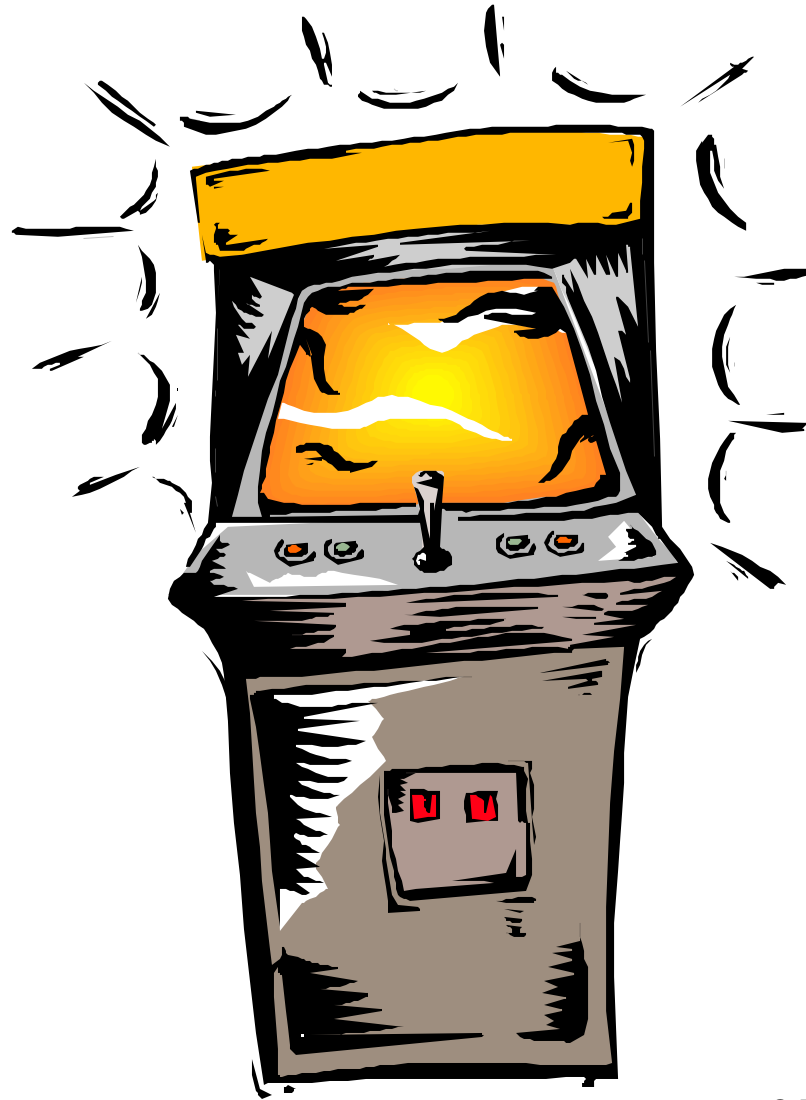
File Edit Tools Window Help

Brute Force: ??NON 0.05 % Done 19 H 42 M Left

User Name	LanMan Password	<8	NT Password
Administrator	PASSWORD		
Guest	NO PASSWORD		NO PASSWORD



Game over!





Direct Methods



KeyGhost

To install the KeyGhost you simply unplug the keyboard cable from the back of the PC, plug it into one end of the KeyGhost, then plug the other end back into the PC. No software installation is necessary!

BEFORE



AFTER



For security reasons, the photo (above right) is only a representation of what the KeyGhost looks like. The actual KeyGhost II is injection molded to look exactly like an EMC Balun.



KeyGhost - keystroke capture

Keystrokes recorded so far is 2706 out of 107250 ...

```
<PWR><CAD>fsmith<tab><tab>arabella  
xxxxxxx <tab><tab>None<tab><tab>None<tab><tab>None<tab><tab>  
<CAD> arabella  
<CAD>  
<CAD> arabella  
<CAD>  
<CAD> arabella  
exit  
tracert 192.168.137.240  
telnet 192.168.137.240  
cisco
```



Linux boot disk

http://www.nttoolbox.com/public/tools/bd990404.zip Go img9902fs Search 100%

Admin Tools

[HotFix Control](#) - Tells you what hotfixes and service pack you have applied, neat utility. (163K)

[User2SID/SID2User](#) - Look up the SID of any domain account. Want to know what SID belongs to what user account? (50k)

[NT Admin Boot Disk](#) - Linux Boot Diskette for NTFS, resets the Administrator Password. Use rawrite.exe (included) to make the floppy from the .bin file NOTE: May not work with SYSKEY. (1.4M) NEW! Updated .bin file located [here](#):

[XTeg's X-Setup 5.7](#) - Called "The Mother of All Windows Tweak Programs", this program lends a handy way to personalize your system. Edit boot options, stop programs from automatically loading with Windows, and remove items from the uninstall list. It also contains some handy security settings and administrative options, normally done by editing the registry. [Visit their site](#) for more details and add-ons.

[NetLab For NT/95](#) - An excellent combination program with Finger, Trace, Quote, WhoIs, Port scanner, other neat goodies.(467K)

[Resplendent Resolver For NT/2000](#) - Don't you just hate it when you try to install or run a program and it whines about "Requires Windows NT SP3", even though you're running SP5 or Windows 2000? I did too, Then I tried out this little gem from from Resplendence. [More Info...](#)

[Open File Manager](#) - From St. Bernard Software. Did you ever have a backup fails because a file is in use? (I wish I knew about this little gem back in the days of cc:mail :) Allows your existing backup software to successfully capture files that are open and in use on Windows NT/2000 and NetWare platforms.

[Main](#)
[Careers](#)
[FAQ](#)
[BSOD](#)
[NetBus](#)
[Links](#)
[Pop Quiz](#)
[Search](#)
[Downloads](#)
[News](#)
[Contact](#)
[Discussion](#)
[Security](#)
[Windows 2000](#)

Free Email!

Already have an account?
Login below:



NTFSDOS

http://www.sysinternals.com/ntw2k/freeware/NTFSDOS.shtml

Sysinternals
Mark Russinovich & Bryce Cogswell
Advanced Utilities • Technical Information • Source Code



Resources Site Map Licensing About Us Home

NTFSDOS

Copyright © 1996-2001 Mark Russinovich and Bryce Cogswell

Last updated September 11, 2001 v3.02R+

Awards



Introduction

If you are interested in accessing NTFS drives from Windows 95 or Windows 98, then you should use [NTFS for Windows 98](#) rather than NTFSDOS. Full read/write access to NTFS drives from DOS is available with [NTFSDOS Professional Edition](#). If you want to salvage files off a corrupt NTFS volume or repair an NTFS boot sector or partition table, see [Winternals' Disk Commander](#).

NTFSDOS.EXE is a read-only network file system driver for DOS/Windows that is able to recognize and mount NTFS drives for transparent access. It makes NTFS drives appear indistinguishable from standard FAT drives, providing the ability to navigate, view and execute programs on them from DOS or from Windows, including from the Windows 3.1 File Manager and Windows 95 Explorer.

Please read this entire file before contacting us for help.

Enhancements over v2.00

Version 3.0's enhancement over v2.0 is that it is capable of accessing NTFS drives with sizes larger than 4GB.

Contents of the Package

The NTFSDOS package (see the bottom of this page) contains the following files:

- README.TXT: This file
- NTFSDOS.EXE: File system driver
- NTFSHLP.VXD: Helper VxD needed only for long filename support in Windows 95



Game over!





Scanning & Dictionary Attacks



Port scan

The screenshot shows the NetScanTools Pro 2000 (TM) interface. The main window displays the results of a port scan for the target host 194.129.36.50. The scan was performed using TCP probes. The results are listed in a tree view under 'Target Computer List'.

Target Computer List

- 194.129.36.50
 - 00020 - TCP - tcp_data
 - 00021 - TCP - ftp**
 - 00025 - TCP - smtp
 - 00080 - TCP - http
 - 00135 - TCP - unknown
 - 00139 - TCP - nbssession

The port 00021 (FTP) is circled in red in the original image. The interface also shows various settings for the scan, such as 'Probe Single Host', 'Autoclear', and 'TCP' selected as the probe type. The status bar at the bottom includes buttons for 'Print', 'Save To File', 'Find', 'Copy', '<>', 'Email Results', 'RFCs', 'Exit', and 'Help'.



Dictionary Attack

Brutus - AET2 - www.hoobie.net/brutus - (January 2000)

File Tools Help

Target: Type: [Start] [Stop] [Clear]

Connection Options

Port: Connections: Timeout: Use Proxy [Define]

Telnet Options

[Modify sequence] Try to stay connected for attempts

Authentication Options

Use Username Single User Pass Mode:

UserID: [Browse] Pass File: [Browse]

Positive Authentication Results

Target	Type	Username	Password
Aborting attack due to invalid user/bad authentication sequence			
Disengaged target 172.16.2.30 elapsed time : 0:00:03 attempts : 0			

100% [Progress Bar]

Timeout Reject Auth Seq Throttle Quick Kill

0 U:root P:10th 0 Attempts per second Idle



Indirect Password Cracking



Office Documents

The screenshot shows the 'A097PR 1.02 - passwords.opr' application window. The main interface includes a menu bar (Project, Recovery, Help), a toolbar with various icons, and several configuration panels. The 'Encrypted Office 97 document' field contains 'passwords.doc'. The 'Dictionary file' field contains 'G:\SOURCES\SECURITY\Di'. The 'Password length options' panel shows 'Minimum' set to 1 and 'Maximum' set to 5. The 'Type of attack' panel has 'Dictionary attack' selected. The 'Auto-save' panel has 'Save project every' checked. The 'Priority options' panel has 'Background' selected. The 'Status window' at the bottom displays the following log entries:

```
23/05/2002 15:25:03 - High-performance timer is present. Performance calculations will be accurate
23/05/2002 15:25:04 - Password successfully recovered !
23/05/2002 15:25:04 - 'wednesday' is a valid password for this file
```

A modal dialog box titled 'Password successfully recovered !' is overlaid on the main window. It contains a table of 'Advanced Office 97 Password Recovery statistics' and an 'OK' button. The table data is as follows:

Advanced Office 97 Password Recovery statistics:	
Total passwords	51951
Total time	845ms
Average speed (passwords per second)	61450
Password for this file	wednesday

The dialog box also features a progress indicator at the bottom showing 0% completion.



Zip Files

Advanced ZIP Password Recovery statistics:

Total passwords	43843
Total time	196ms
Average speed (passwords per second)	223422
Password for this file	holiday
Password in HEX	68 6F 6C 69 64 61 79

23/05/2002 15:27:47 - Password successfully recovered!
23/05/2002 15:27:47 - 'holiday' is a valid password for this file

Current password: _____ Average speed: _____
Time elapsed: _____ Time remaining: _____
Progress indicator: _____ 0%

AZPR version 2.44 (c) 1999 Vladimir Katalov & Andy Malyshev, Elcom Ltd

And how to prevent it!



FIRST • BASE
technologies

Peter Wood
First • Base
Technologies



Prevention is better ...

- Harden the servers
- Monitor alerts (e.g. www.sans.org)
- Scan, test and apply patches
- Monitor logs
- Good physical security
- Intrusion detection systems
- Train the technical staff on security
- Serious policy and procedures!



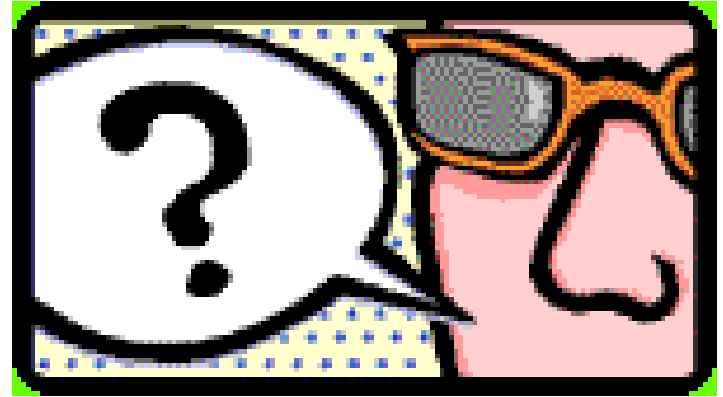
Server hardening

- www.fbtechies.co.uk/resources.htm
- FAQ for How to Secure Windows NT (www.sans.org)
- Fundamental Steps to Harden Windows NT 4_0 (www.sans.org)
- ISF NT Checklist v2 (www.securityforum.org)
- <http://www.microsoft.com/technet/security/bestprac/default.asp>
- Lockdown.pdf (www.iss.net)
- Windows NT Security Guidelines (nsa1.www.conxion.com)
- NTBugtraq FAQs (<http://ntbugtraq.ntadvice.com/default.asp?pid=37&sid=1>)
- Securing Windows 2000 (www.sans.org)
- Securing Windows 2000 Server (www.sans.org)
- Windows 2000 Known Vulnerabilities and Their Fixes (www.sans.org)
- SANS step-by-step guides



Alerts

- www.sans.org
- www.cert.org
- www.microsoft.com/security
- www.ntbugtraq.com
- www.winnetmag.com
- razor.bindview.com
- eeye.com
- Security Pro News (ientrymail.com)





Scan and apply patches

Machine / IP: WHITE-HAT-1 IP: 192.168.0.77 OS: Windows 2000 Workstation

Configuration File: C:\...\NoFileChecks.dat Scan Name:

ID	Risk	Machine	AutoFix	Category	CVE ID	Vulnerability
W801	Medium	WHITE-H...	No	Password	1999-0535	Account Policy: Minimum Password Le
W865	Medium	WHITE-H...	No	Password		LM Authentication Enabled - W2K
W1210	Medium	WHITE-H...	Yes	Password		LM Hashes Exist - W2K, XP
W96	Medium	WHITE-H...	No	Service		Service Unknown
W68	Medium	WHITE-H...	No	Web Brow...		IE Web Browser Outdated
W70	Medium	WHITE-H...	No	Registry		Registry Unrestricted - Windows Curr
W984	Medium	WHITE-H...	No	Info Disclo...		Anonymous Connections Not Restrict
W18	Medium	WHITE-H...	No	User Rights	1999-0534	User Rights: Log on as a batch job
W73	Medium	WHITE-H...	Yes	Unauthoriz...	1999-0658	DCOM Enabled
W805	Low	WHITE-H...	Yes	Denial of S...		Printer Drivers Unsecured - W2K
W802	Low	WHITE-H...	Yes	Audit Policy	1999-0575	Audit of Backups and Restores Not En
W811	Low	WHITE-H...	Yes	Info Disclo...		Cached Logons Enabled
W797	Low	WHITE-H...	No	Account P...	1999-0582	Account Lockout Policy: Reset Lockou
W798	Low	WHITE-H...	No	Password	1999-0535	Account Policy: Maximum Password Ac
W795	Low	WHITE-H...	No	Account P...	1999-0582	Account Lockout Policy: Lockout Dura
W794	Low	WHITE-H...	Yes	Audit Policy	1999-0575	Audit: System Events Not Enabled - W
W791	Low	WHITE-H...	Yes	Audit Policy	1999-0575	Audit: Policy Change Not Enabled - W

Complete: 2002/05/23 16:11:52

100% 1 0 9 40 6 0 Tr



Log Reporting Products

- **DumpEvt** (freeware)
(www.systemtools.com/free_frame.htm)
- **NTLast** (freeware) & **VisualLast**
(www.foundstone.com/knowledge/free_tools.html)
- **InTrust** (previously EventAdmin)
(www.aelita.net/products/intrust.htm)
- **Event Log Monitor**
(www.tntsoftware.com/products/ELM3/ELM30/)
- **BindView** (part of bv-Control suite)
(www.bindview.com)



Good Physical Security

- Perimeter security
- Computer room security
- Desktop security
- Close monitoring of admin's work areas
- No floppy drives?
- No bootable CDs?



IDS

- RealSecure
- Tripwire
- Dragon
- Snort
- *www.networkintrusion.co.uk/ids.htm*
for impartial guidance



Security Awareness

- Sharing admin accounts
- Service accounts
- Account naming conventions
- Server naming conventions
- Hardening
- Passwords (understand NT passwords!)
- Two-factor authentication?



Serious Policy & Procedures

- Top-down commitment
- Investment
- Designed-in security
- Regular audits
- Regular penetration testing
- Education & awareness



Need more information?

Peter Wood

peterw@firstbase.co.uk

www.fbtechies.co.uk

