The Insider Threat

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 ……

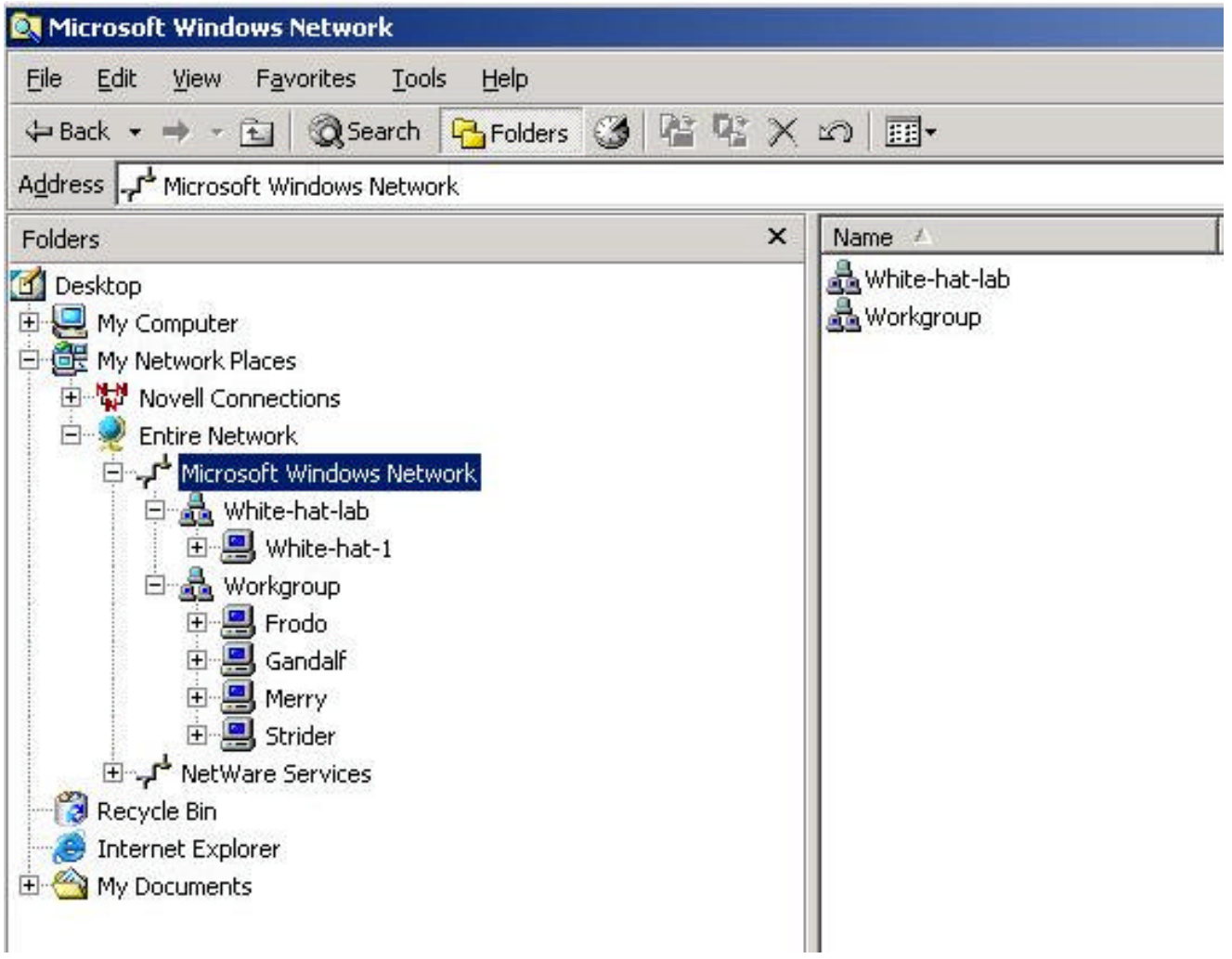
…. And you don’t need to be logged on

Get yourself an IP address

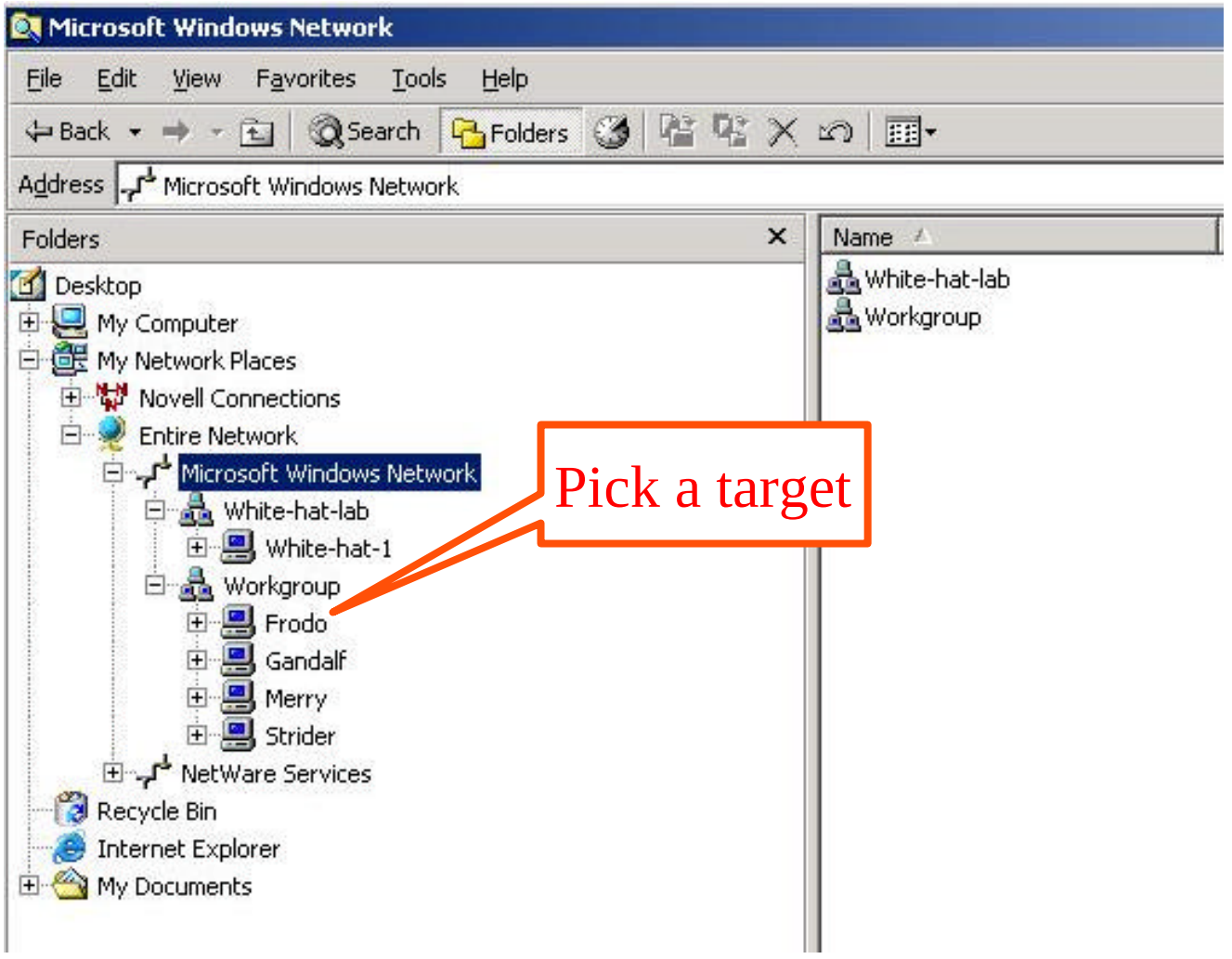
- Use DHCP since almost everyone does!
- Or … use a sniffer to see broadcast packets (even in a switched network) and try some suitable addresses

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

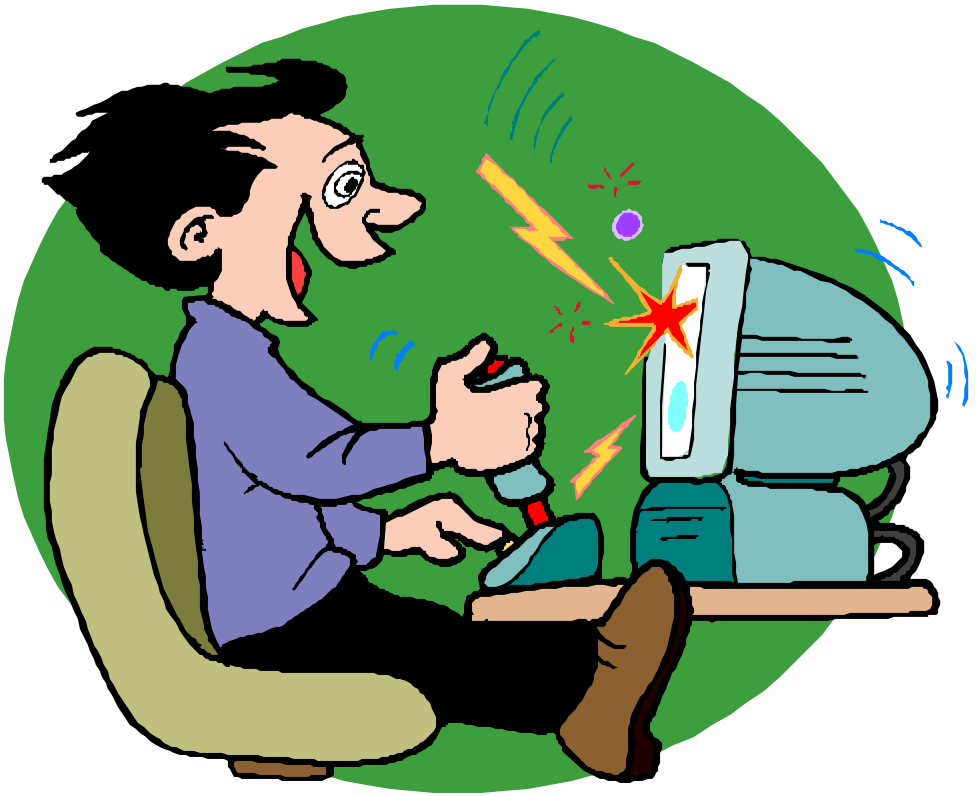
Group	MemberType	GroupMember
Administrators	User	Administrator
Administrators	User	keiron
Administrators	User	pete
Backup Operators		
Guests	User	Guest
Power Users		
Replicator		
Users	User	pete

Found 6 groups 00001

Typical passwords

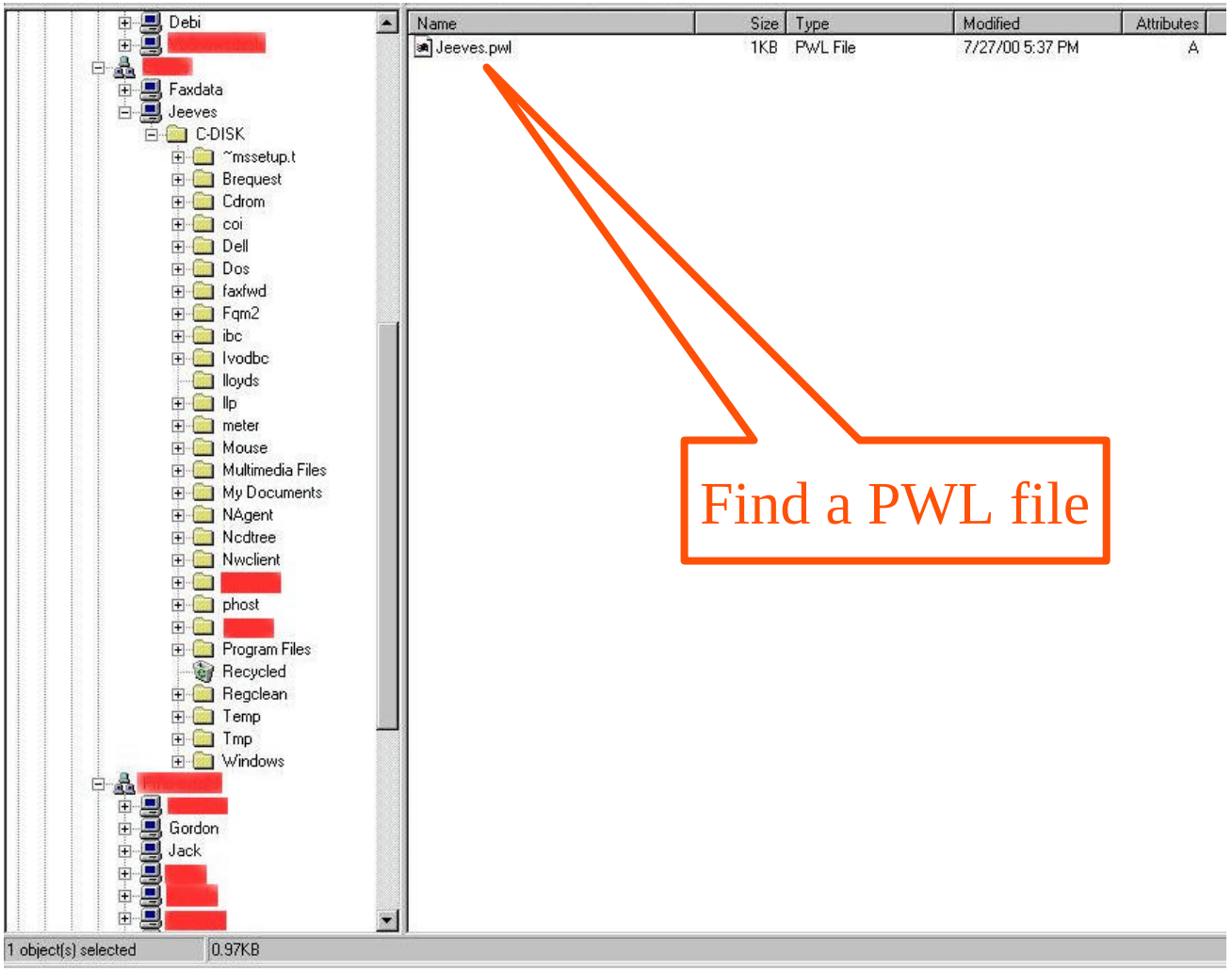
• administrator	null, password, administrator
• arcserve	arcserve, backup
• test	test, password
• username	username, company
• backup	backup
• tivoli	tivoli
• backupexec	backup

Game over!



Unprotected Shares

Browse for shared c-drives



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\Dictionaries\ — Browse

Hybrid brute

0:0:0:1

???? p/sec

CPU | About

SearchPasswordFast | SearchPassword

CheckPassFast | Client/Server

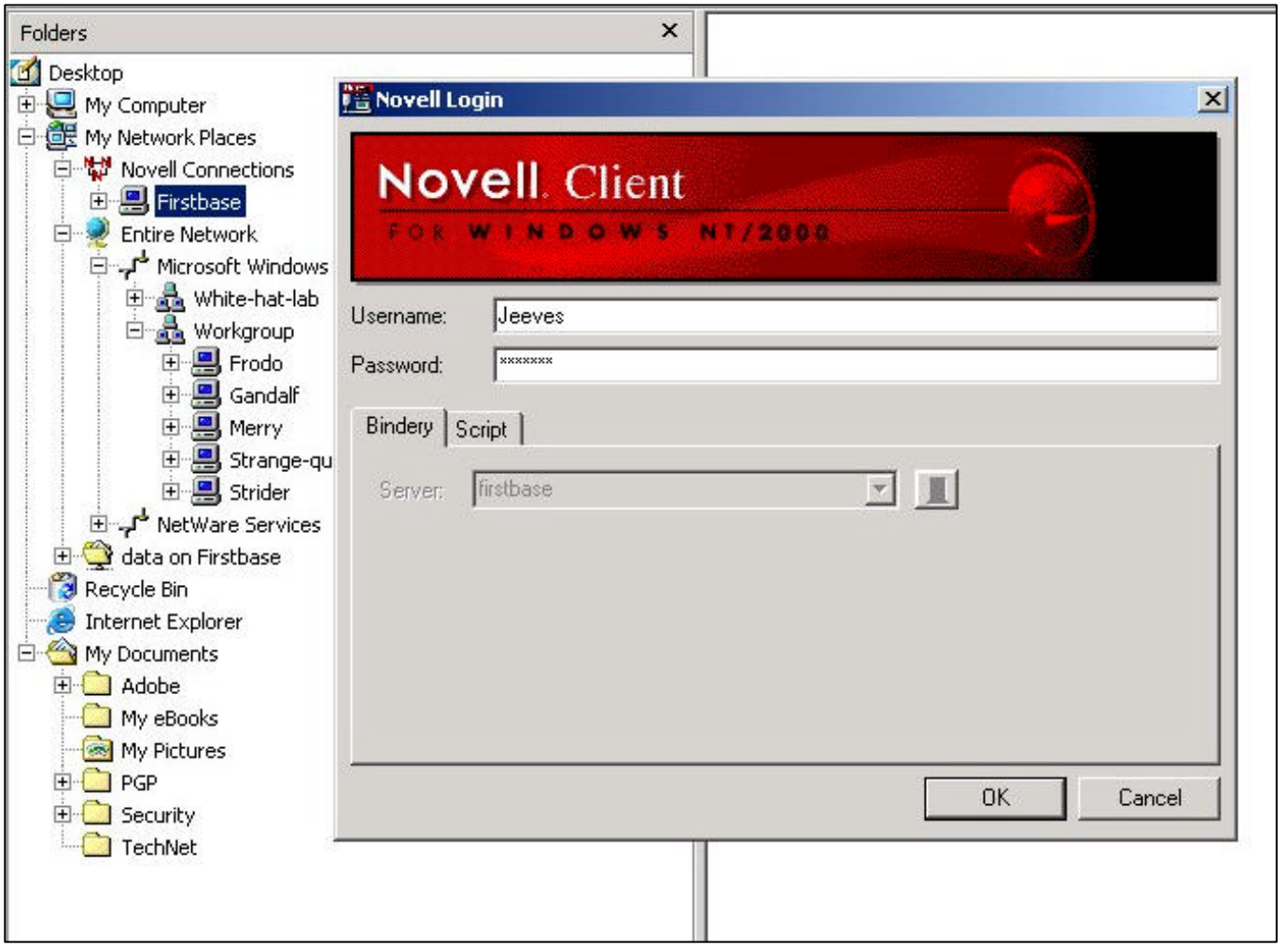
Zombie mode | Help | Adv

Cached passwords

File: [redacted]\Network
review\Jeeves\JEEVES.PWL
User name: 'JEEVES'
Password: ''

Mail:'[illegible]'
Password:'wooster'
Mail:'[illegible]'
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



Game over!

Plain Text Passwords

Netlogon

In the unprotected netlogon share on a server:

logon scripts can contain:

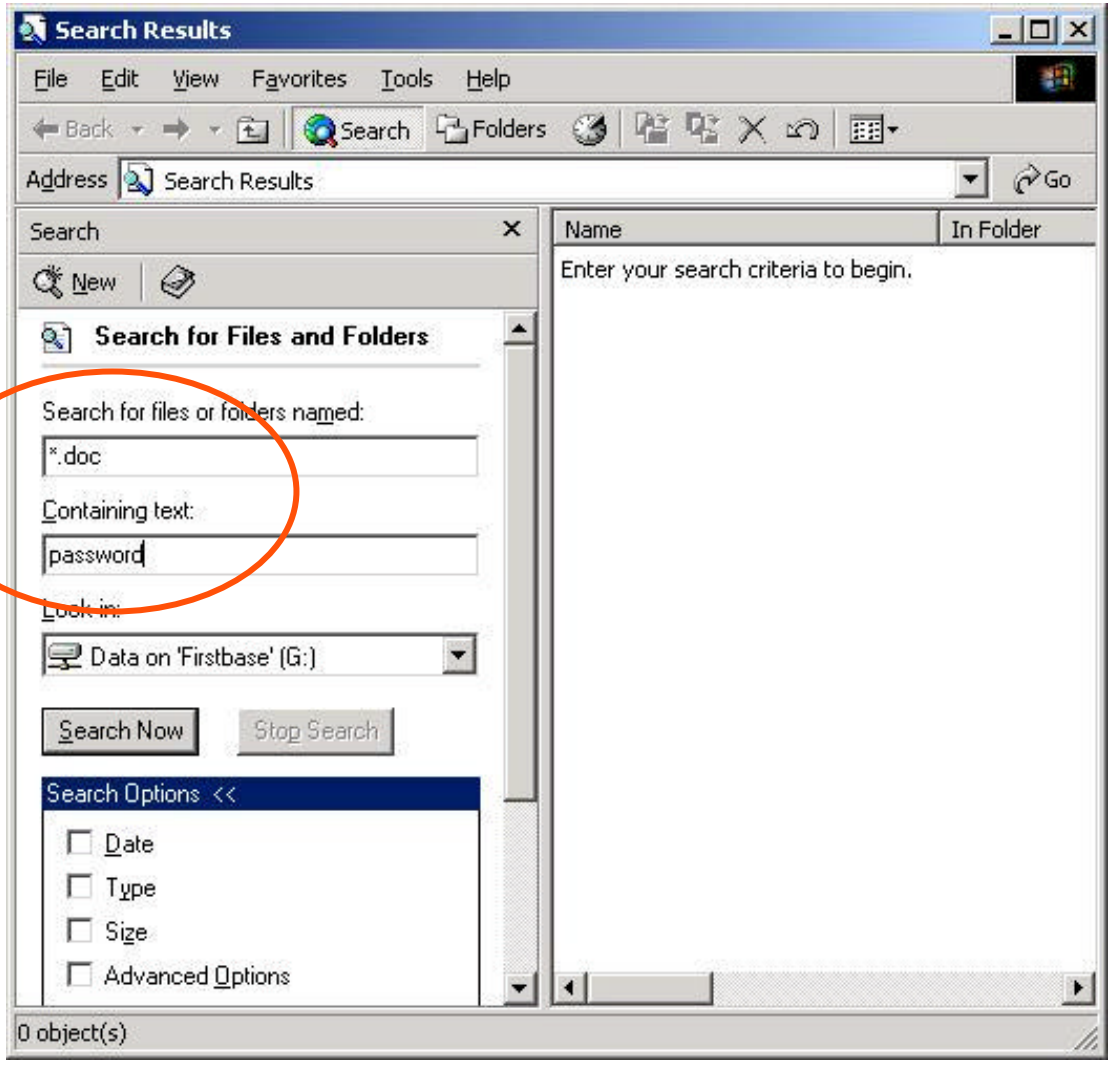
net use \\server\share “password” /u:“user”

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



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:

carol1zz

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.
```

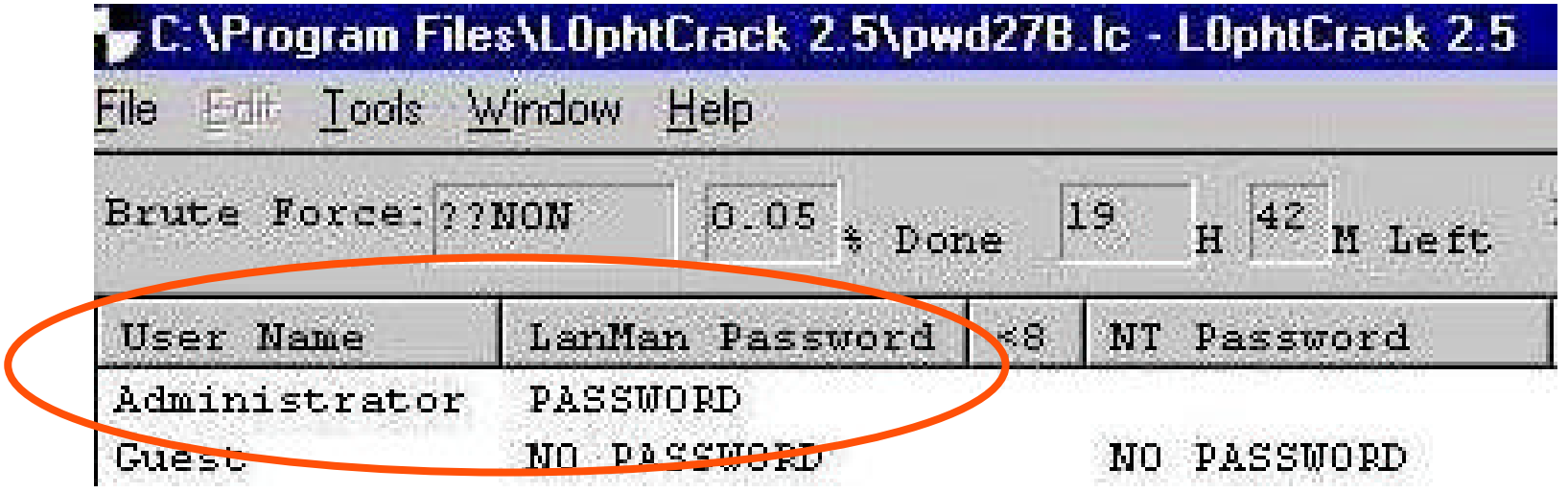
Game over!

Password Cracking

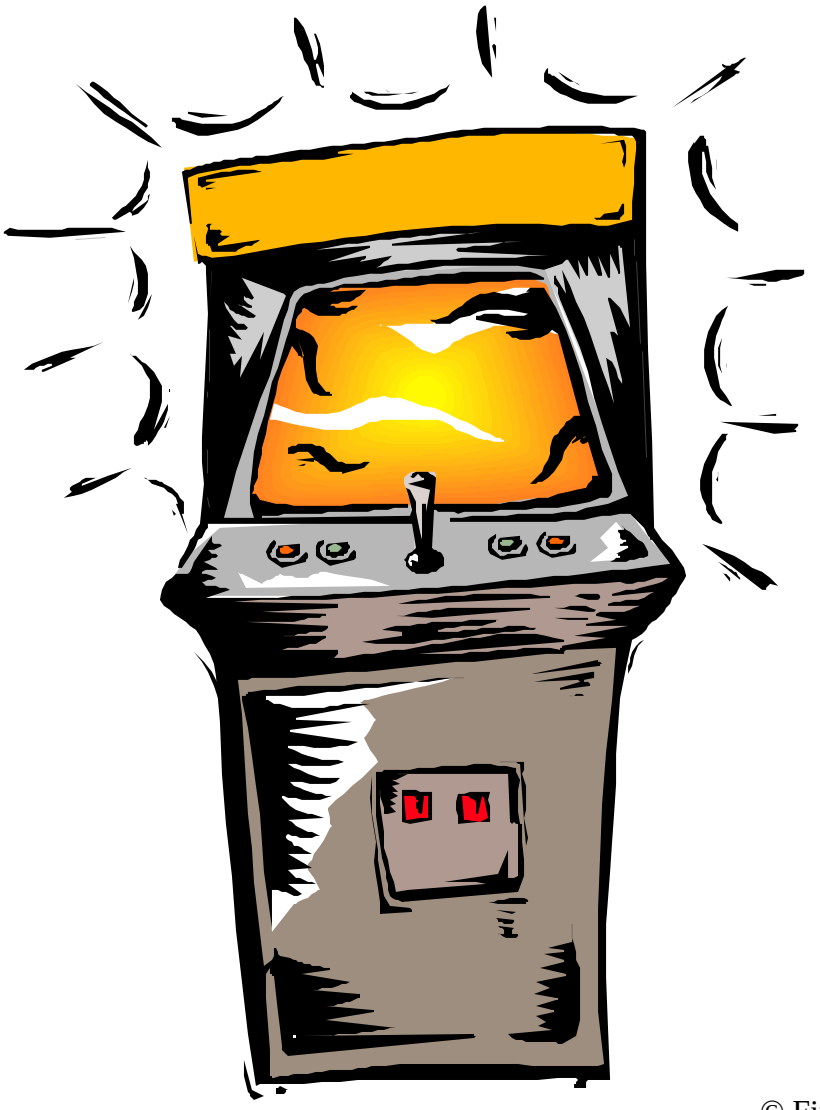
How to get the SAM

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

Cracking - L0phtcrack



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**

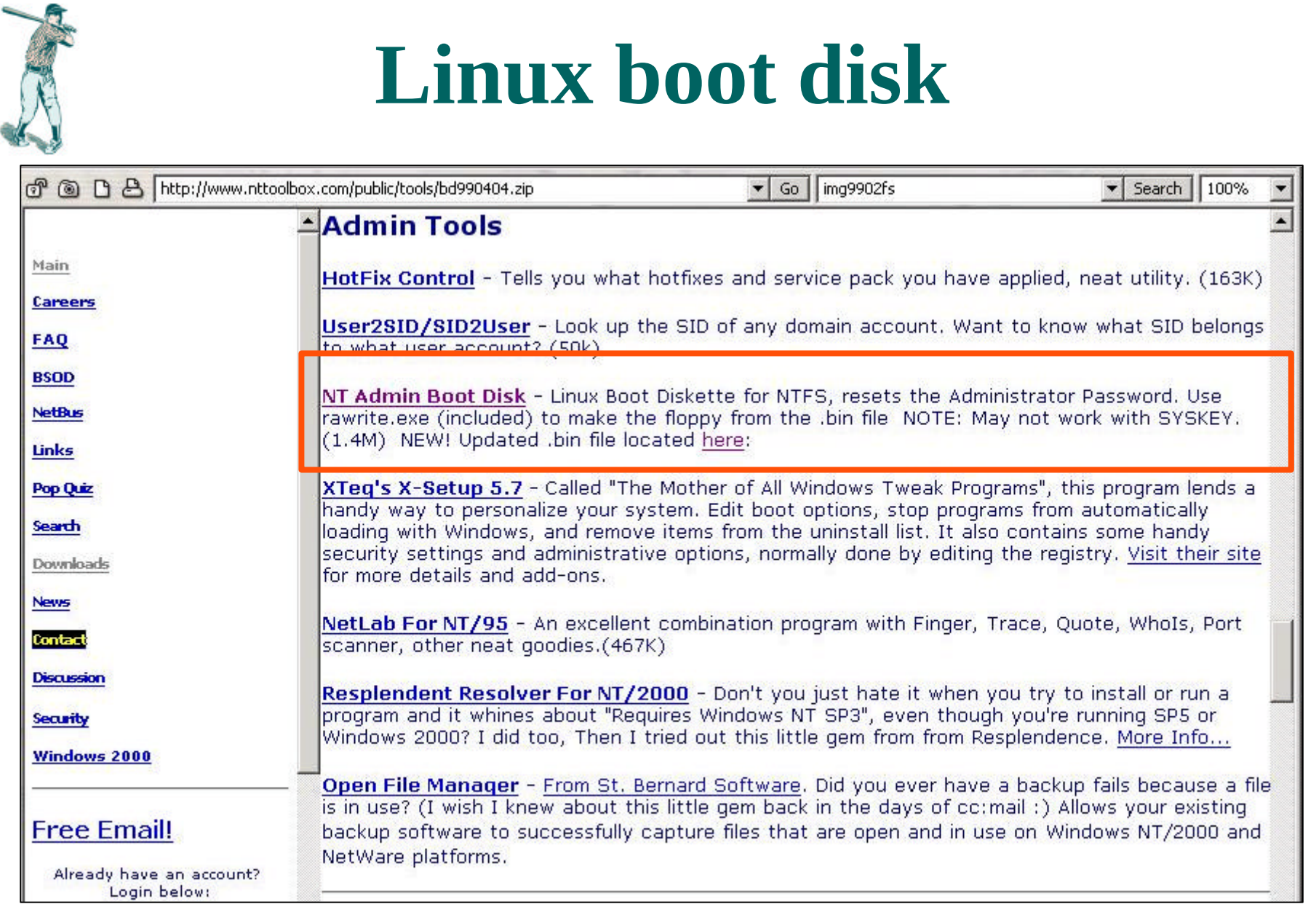
For security reasons, the photo (above right) is only a representation of what the KeyGhost looks like. The actual KeyGhost II is injection molded to look exactly like an EMC Balun.

KeyGhost - keystroke capture

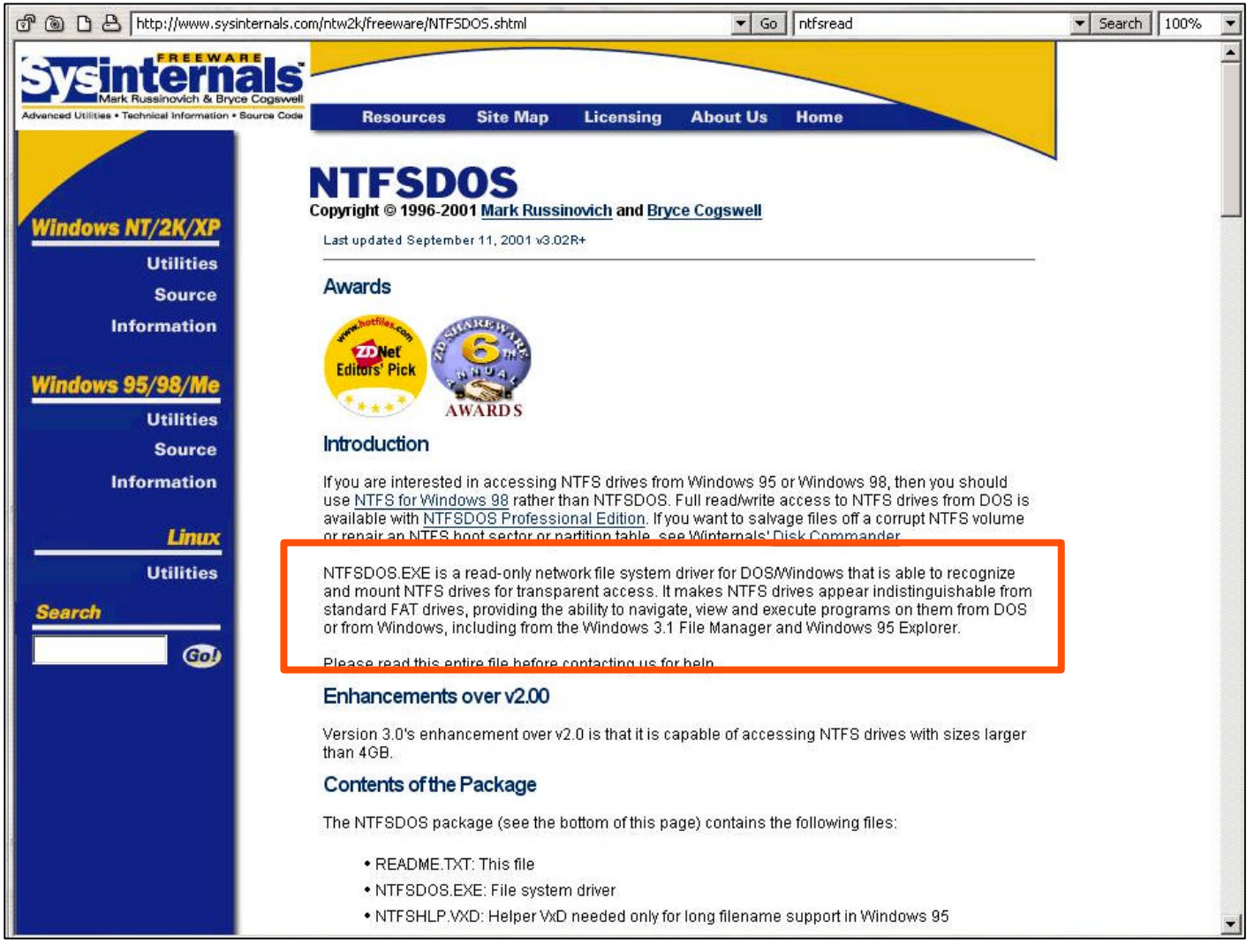
Keystrokes recorded so far is 2706 out of 107250 ...

<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

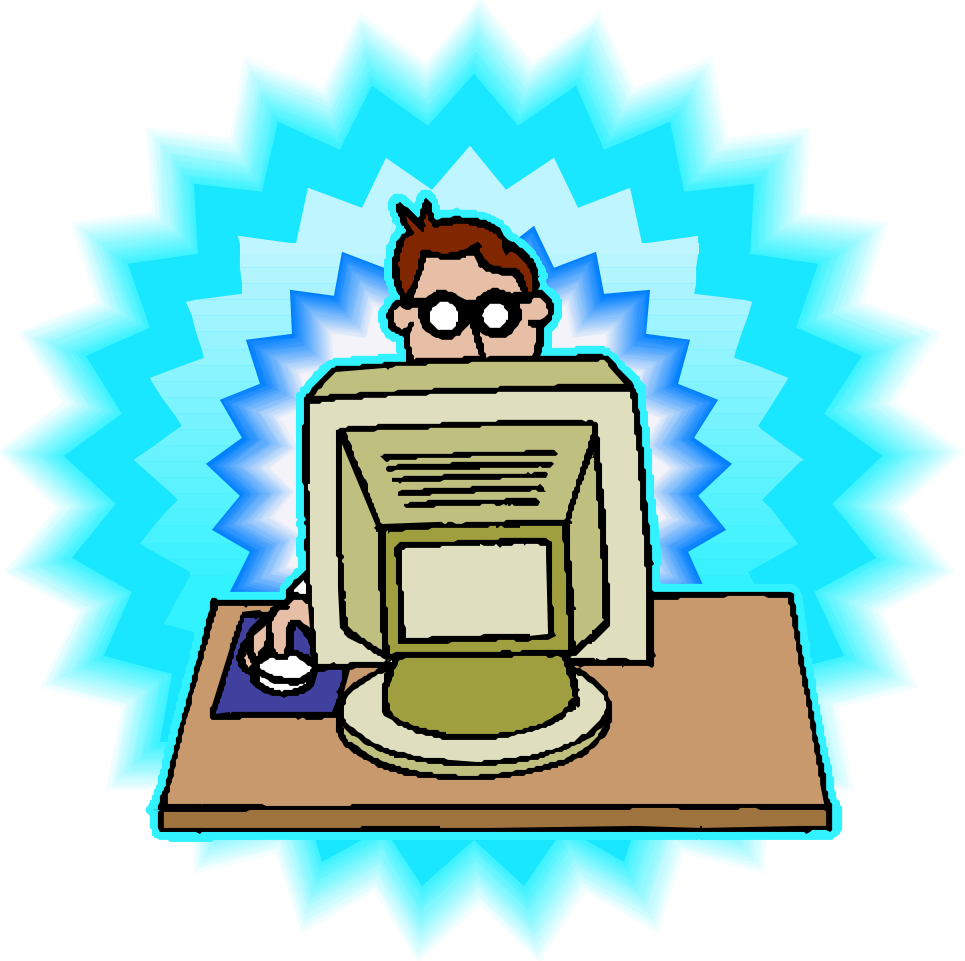
Linux boot disk



NTFSDOS



Game over!



Scanning & Dictionary Attacks

Port scan

NetScanTools Pro 2000 (TM)

Quote | Character Generator Client | Echo | Time Sync | IDENT Server | Database Tests | Launcher | WinSock Info | Preferences | About
Name Server Lookup | HyperTrans | Finger | Ping | TraceRoute | Whois | SNMP | Detection | Email Validate | SMTP Email Generator
What's New at NWPSW | TCP Term | NetScanner | NetTopography | Arp | NetBios Info | Network Info and Stats | Port Probe | TTCP | Daytime

Probe Single Host
Probe IP Range
Autoclear
Show non-responding ports
TCP
UDP
TCP/UDP

Image Key
Images have tooltips.

Target Host Name or Start IP Address: 194.129.36.50 C
Start Port: 1
Connection Timeout (ms): 3000
End IP Address: 193.41.154.59 C
End Port: 256
Wait After Connect (ms): 3000

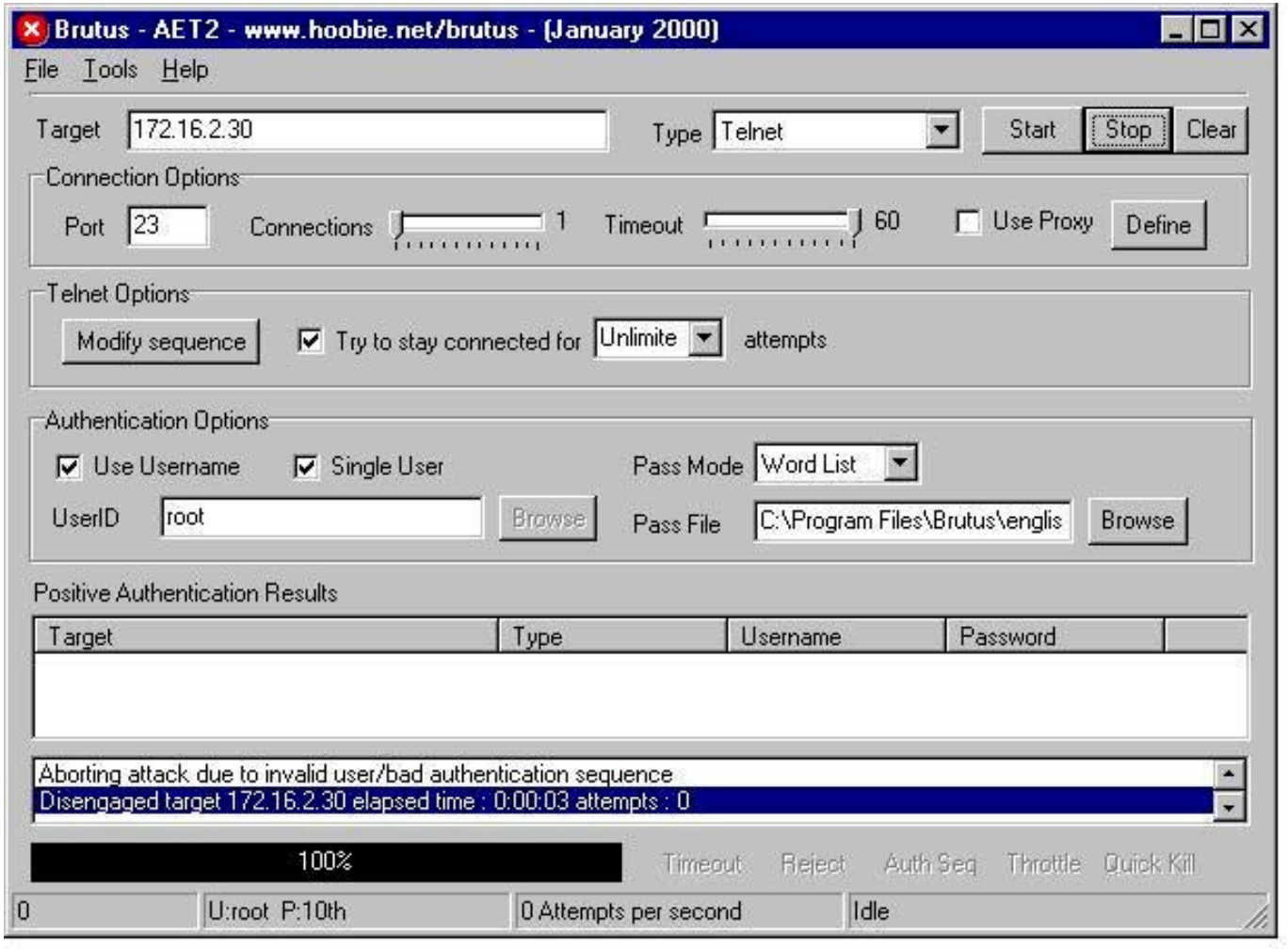
Seq Probe
Probe Port List
Seq Target List
Port/Target List
Stop
Edit Target List
Edit Port List
Clear Results
Merge Drilldown
Probe Delay (ms): 0

Ready.

Target Computer List
194.129.36.50
00020 - TCP - ftp data
00021 - TCP - ftp
00025 - TCP - smtp
00080 - TCP - http
00135 - TCP - unknown
00139 - TCP - nbsession

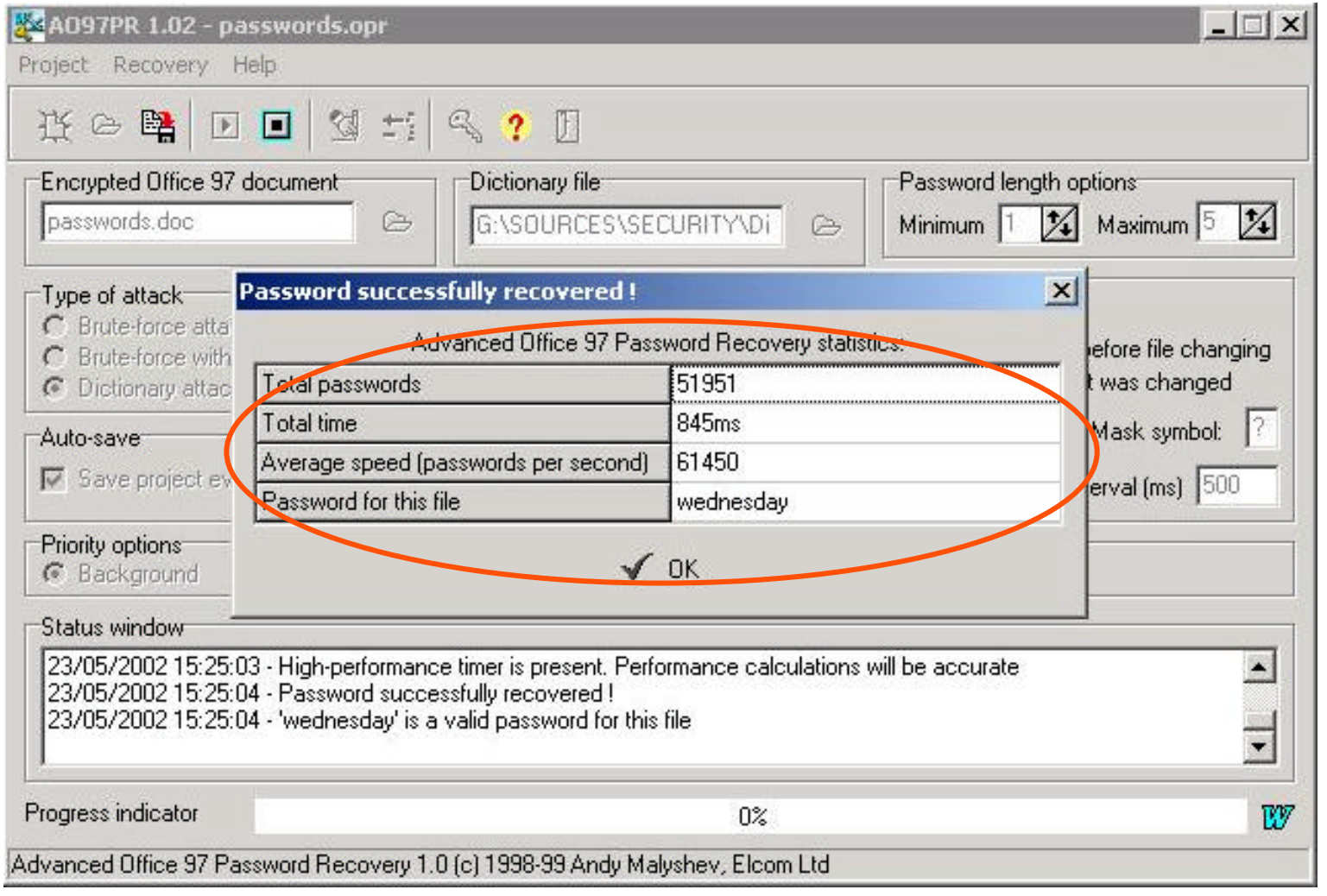
Print | Save To File | Find | Copy | <-> | Email Results | RFCs | Exit | Help

Dictionary Attack

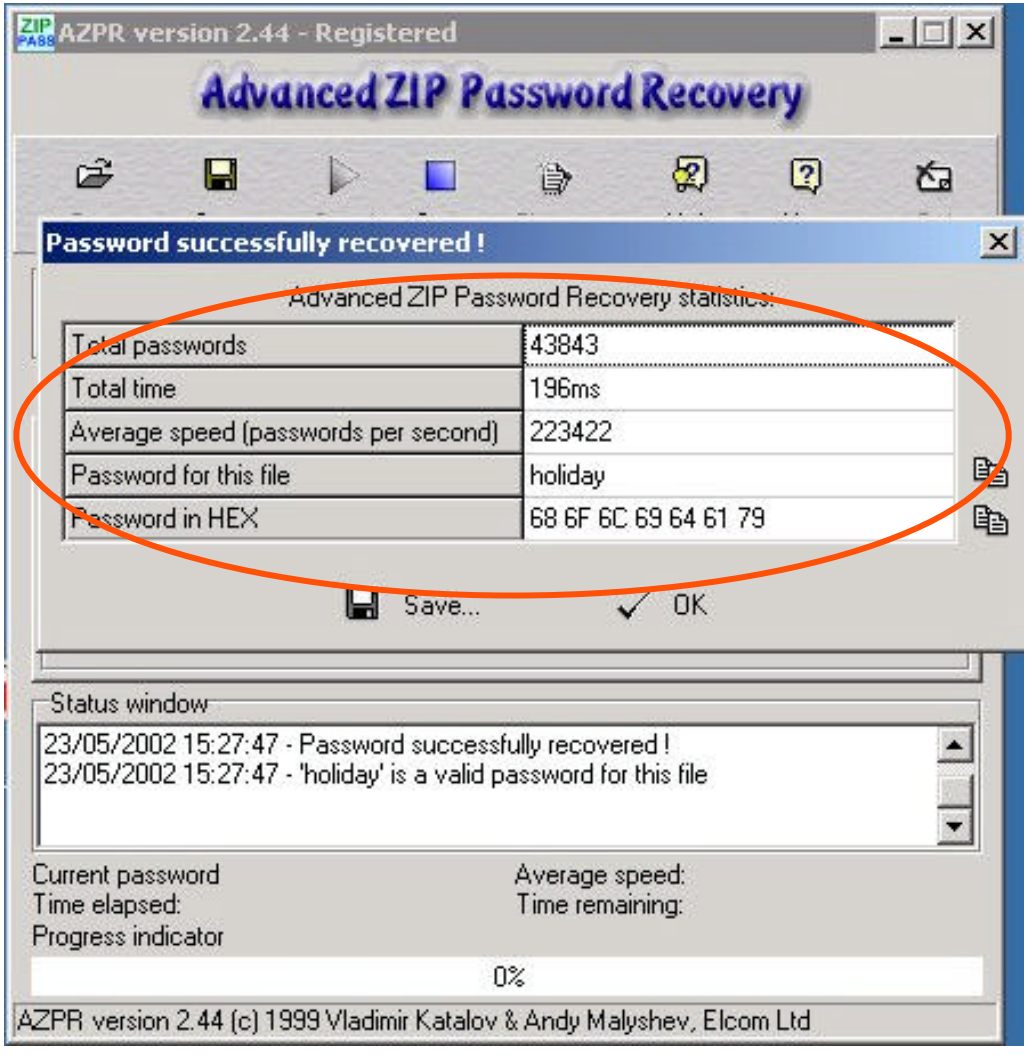


Indirect Password Cracking

Office Documents



Zip Files



And how to prevent it!

Peter Wood

First•Base Technologies

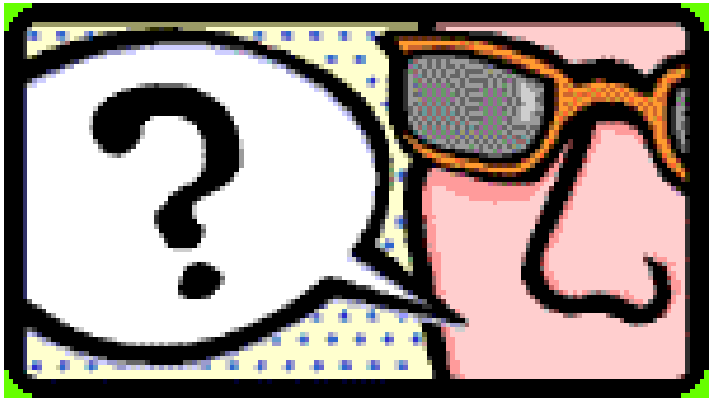
Prevention is better ...

- 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

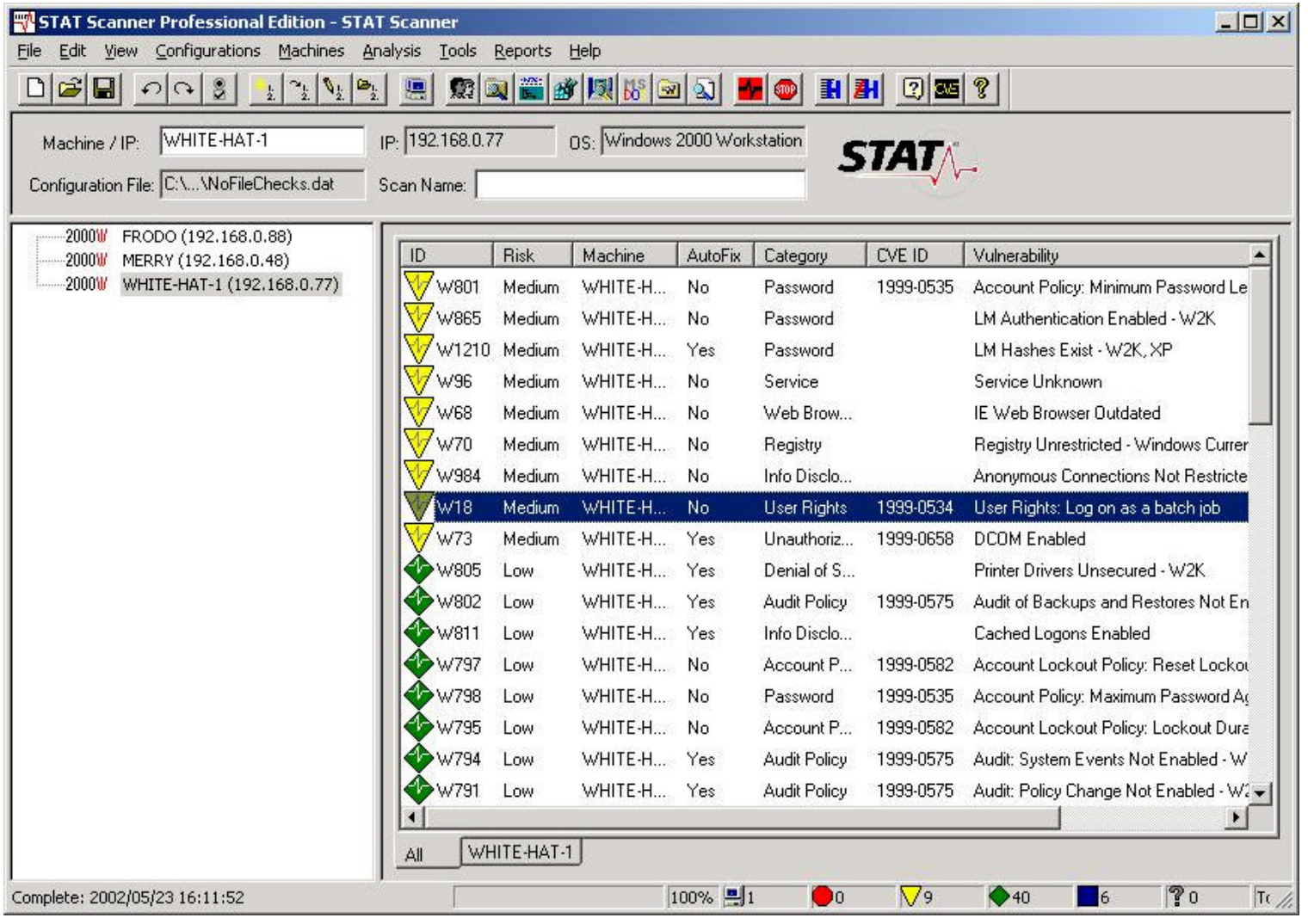
- www.fbtechies.co.uk/resources.htm
- FAQ for How to Secure Windows NT (www.sans.org)
- Fundamental Steps to Harden Windows NT 4_0 (www.sans.org)
- ISF NT Checklist v2 (www.securityforum.org)
- http://www.microsoft.com/technet/security/bestprac/default.asp
- Lockdown.pdf (www.iss.net)
- Windows NT Security 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



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