Identity Theft in the Corporate Environment

Peter Wood
Chief of Operations
First•Base Technologies
Who am I?

• Started in electronics in 1969
• Worked in networked computers since 1976
• Second microcomputer reseller in UK (1980)
• First local area networks in business (1985)
• Founded First•Base Technologies in 1989
• Designed secure LANs for major corporates
• Presented BS 7799 throughout UK for BSI
• First ethical hacking firm in UK
Social Engineering
The Undiscovered Threat

- Not every hacker is sitting alone with their computer, hacking into a corporate VPN or running a program to crack executives’ passwords.
- Sometimes all they have to do is call up and ask!
Human-based SE

• “Any medium that provides one-to-one communications between people can be exploited, including face-to-face, telephone and electronic mail. All it takes is to be a good liar.”

- Dorothy E. Denning
  Information Warfare and Security
Background Research

- A good social engineer will do background research on the target:
  - reading web sites
  - visiting & exploring premises
  - watching staff movements & dress code
  - watching cleaners, deliveries, etc.
  - dumpster diving
  - Friends Reunited!
No picnic for me, I'm afraid, as I have Visitor visitors this weekend. Also (guess what?) I will have to do a few hours work. I hope you all have fun, natural fun.

Stevie, what kind of bung do you require to sort me out with that cheeky CD mentioned in Another Place earlier this week? It's not going to be brown envelopes at Newport Pagnell Services, is it? That was bad enough the last time.

Cheerio team,

tx

This email has been sent from KPMG LLP, a UK limited liability partnership, or from Kingdom Plc and KPMG UK Limited). The information in this email is confidential and anyone else is unauthorised. If you are not the intended recipient, any disclosure may be unlawful. When addressed to our clients any opinions or advice contained in this email is for their information only.
Google groups search

**COM+ Enterprise services behaving differently on Win 2000 AND Win 2003 server**

Only 1 message in topic - [view as tree](#)

<table>
<thead>
<tr>
<th>From:</th>
<th>Not yet rated</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:sample@example.com">Email</a></td>
<td>hide options</td>
</tr>
<tr>
<td>Date:</td>
<td>Wed, Feb 22 2006 5:04 pm</td>
</tr>
<tr>
<td>Email:</td>
<td>'<a href="mailto:sample@example.com">sample@example.com</a>'</td>
</tr>
<tr>
<td>Groups:</td>
<td>microsoft.public.platformsdk.complus_mts</td>
</tr>
<tr>
<td>Reply</td>
<td>Reply to Author</td>
</tr>
</tbody>
</table>

Dear All,

I had referred to some of your tech forums on the net.
I had a problem that I wanted to discuss with you.
Basically I am working on a 3 tiered application in VB.Net/Oracle with middle tier hosted on IIS-remoting with COM+ serviced components.
The hosting of middle tier remoting assemblies is on Windows 2000 server.
There is a package for a middle tier assembly that works fine on setting as both Library OR Server activated.
Now we are shifting to Windows 2003 server. On this, the same assembly that works fine as both Library OR server activation on Windows 2000 does not work for both activation settings.
I.e. On Windows 2003 server, the assembly package works only when set to Server activation AND does not work when set as Library.
Any suggestions from you would be of great help and appreciated.

Thanks & Regards

[Reply](#)
Using 192.com

ANDREW R WILSON
37F CROMWELL ROAD
HOVE EAST SUSSEX
BN3 8EE

PROPERTY PRICE

<table>
<thead>
<tr>
<th>Property Type</th>
<th>Type Of Building</th>
<th>Date Sold</th>
<th>NIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flats/Maisonettes</td>
<td></td>
<td>February 25, 2003</td>
<td></td>
</tr>
</tbody>
</table>

© Crown copyright material reproduced with the permission of Land Registry. This material was last updated in December 2005. It covers the period from April 1st 2003 to December 2005.

UK maps powered by: Geographic Macsim

Search Telephones Numbers

Click here to order this aerial photo as a digital print or in 3D.
Using 1837online.com

Births from period Apr-May-Jun 1964
NORTHCOTE, Karen - NOTTAGE, Wendy E A
Remaining Units: 49
If you do not see an image below please click here.

<table>
<thead>
<tr>
<th>NORTHCOTE, Karen</th>
<th>NOTTAGE, Wendy E A</th>
</tr>
</thead>
<tbody>
<tr>
<td>CARL H.</td>
<td>WILLIAMSON</td>
</tr>
<tr>
<td>LAURA H.</td>
<td>MORRISON</td>
</tr>
<tr>
<td>MARTIN A.</td>
<td>WHITELEY</td>
</tr>
<tr>
<td>NORTHCOTES, LYNAL</td>
<td></td>
</tr>
<tr>
<td>NORTMOR, JANET A.</td>
<td></td>
</tr>
<tr>
<td>KERLY G.</td>
<td>MAY</td>
</tr>
<tr>
<td>NORTHGREN, IAN</td>
<td>MURRELL</td>
</tr>
<tr>
<td>SUSAN T.</td>
<td>TAYLOR</td>
</tr>
<tr>
<td>NORTHOVER, ASHLEY</td>
<td>ROCKETT</td>
</tr>
<tr>
<td>AUDLEY</td>
<td>NORTHOVER</td>
</tr>
<tr>
<td>NORTHOVER,</td>
<td>POOLE</td>
</tr>
<tr>
<td>SOUTHGREN, IAN</td>
<td>HACKNEY</td>
</tr>
<tr>
<td></td>
<td>BEDFORD</td>
</tr>
</tbody>
</table>

© First Base Technologies 2006
order a certificate

Order a certificate

A certified copy of a birth, marriage, or death certificate may be ordered online from the General Register Office (GRO) - simply click here and follow the instructions. This service is now available to visitors based in the UK or overseas for both English and Welsh and Overseas births, marriages and deaths.

Please note: when ordering certificates through the GRO you will need to register a username and password different to those you use for 1837online.com.

You can also order certificates from the GRO by post, email, telephone or fax.

General Register Office
PO Box 2
Southport
Merseyside
PR8 2JD

certificate.services@ons.gov.uk

Tel 0845 603 7788 or (international) +44 845 603 7788
Fax 01704 550013 or (international) +44 1704 550013

Opening hours
Monday to Friday - 8 a.m. to 8 p.m. GMT
Saturday - 9 a.m. to 4 p.m. GMT

The GRO operates a graduated fee structure for obtaining a copy of a certificate based upon how much information you can provide to identify the certificate you require. By using the results from our site you can obtain the full GRO reference and may benefit from the lowest charges offered by the GRO.

Click the following link for more information on ordering a certificate from the GRO. Their site will give further details on certificate fees.

You may also download the application forms below.

Birth Marriage Death
Impersonation

- Social engineering usually impersonation:
  - Service or repair engineer
  - IT support
  - Fellow employee
  - Irate manager
  - Trusted third party
Andy’s Remote Worker Hack

1. Buy a pay-as-you-go mobile phone
2. Call the target firm’s switchboard and ask for IT staff names and phone numbers
3. Overcome their security question: *Are you a recruiter?*
4. Call each number until voicemail tells you they are out
5. Call the help desk claiming to be working from home
6. Say you have forgotten your password and need it reset now, as you are going to pick up your kids from school
7. Receive the username and password as a text to your mobile
8. Game over!
Pete’s IT Support Hack

1. Get staff contact names and numbers from reception
2. Call a target user who is unlikely to be technical
3. Say you are Peter Wood from IT working on upgrading their servers over the weekend
4. Say you need their username and password to test their account so that all will work smoothly on Monday morning
5. Game over!
In Person

• Be an employee, visitor or maintenance staff
• Look for information lying on desks and overhear conversations
• Find modems and note the numbers (written on the sockets)
• Plug in a sniffer or Keyghost
• Simply use a vacant desk & PC
Would you let this man into your building?
Things Found “Lying Around”

- Customer account details
- Payroll data disks
- Voicemail guide with default passwords
- Advertising spend
- Bank statements
- Company staff directory
- Notes on white-boards
Dumpster Diving

• Looking through rubbish for valuable information:
  - “For shredding”
  - “For recycling”
  - Individual’s rubbish bins
  - Corporate rubbish (outside)
Shoulder Surfing

- Looking over someone’s shoulder to try to see:
  - Their password
  - Door entry codes
  - Information on their screen
  - What they are writing
Pop-up Windows

Your connection to the network has been lost.

Please reenter your username and password.

login: 

password: 

Login

Unsigned Java Applet Window
Mail Attachments

- Viruses, worms and trojan horses
- Names to entice the employee to click on them, such as “Fun Love” or “I Love You”
- Attempt to hide the file extension by giving the attachment a long file name
  - e.g. AnnaKournikova.jpg.vbs. If the name is truncated it will look like a jpg file and the user will not notice the .vbs extension
Websites & Intranets

- Offer something free or a chance to win on a Website
- The user must enter an email address and a password
- Many employees will use the same password that they use at work
Snail Mail

• While snail mail is the oldest and slowest methods of communication, it is often quite effective.
• The hacker can set up a PO Box easily. The equipment and overall cost of snail mail is relatively inexpensive. It is quite easy to hide and fake a business this way. It is important to remember that snail mail is not tapped.
• People are more likely to respond to a survey they receive in the mail. The survey could ask tons of information about you and your company. The survey will have a stamped envelope included so you will not pay to have it mailed back. The survey will even promise cash or other prizes for completed and returned surveys.
• By the time your company notices that this survey was a scam, the hacker has moved on to a different PO Box, under a different name, targeting a new company.
Summary

- Social engineering can be used to gain access to any system, irrespective of the platform.
- It’s the hardest form of attack to defend against because hardware and software alone can’t stop it.
The Inside-Out Hacker
Working on a laptop at home
... open an attachment or download something

Laptop

Internet

e-mail

Trojan software now silently installed
... take laptop to work
... trojan sees what you see
Information flows out of the organisation
Summary

• Laptops are the best backdoor
• (So are home PCs with wireless)
• Trojans have access to everything you do
• Internal hosts aren’t patched up to date
• If it’s on your PC or server - it’s stolen!
The Inside Hacker
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
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRODO</td>
<td>&lt;00&gt;</td>
<td>UNIQUE</td>
</tr>
<tr>
<td>FRODO</td>
<td>&lt;20&gt;</td>
<td>UNIQUE</td>
</tr>
<tr>
<td>WORKGROUP</td>
<td>&lt;00&gt;</td>
<td>GROUP</td>
</tr>
<tr>
<td>FRODO</td>
<td>&lt;03&gt;</td>
<td>UNIQUE</td>
</tr>
<tr>
<td>WORKGROUP</td>
<td>&lt;1E&gt;</td>
<td>GROUP</td>
</tr>
<tr>
<td>KEIRON</td>
<td>&lt;03&gt;</td>
<td>UNIQUE</td>
</tr>
<tr>
<td>WORKGROUP</td>
<td>&lt;1D&gt;</td>
<td>UNIQUE</td>
</tr>
<tr>
<td>MSBROWSE</td>
<td>&lt;01&gt;</td>
<td>GROUP</td>
</tr>
</tbody>
</table>

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

C:\>net use \\frodo\ipc$ "" /u:"" The command completed successfully.
```
List privileged users
Typical passwords

- administrator
- arcserv
- test
- username
- backup
- tivoli
- backupexec
- smsservice
- ... any service account
- null, password, administrator
- arcserv, backup
- test, password
- password, monday, football
- backup
- tivoli
- backup
- smsservice
- ... same as account name
Summary

• Any user, contractor, cleaner, visitor ...
• (Wireless is the same as being there)
• A service account is an administrator
• An administrator has access to *everything*
• If it’s on your PC or server - it’s stolen!
Physical Attacks
What NT password?

Offline NT Password & Registry Editor, Bootdisk

I've put together a single floppy or CD which contains things needed to edit the passwords on most systems.

The bootdisk supports standard (dual)IDE controllers, and most SCSI-controllers with the drivers supplied in a separate archive below. It does not need any other special hardware, it will run on 486 or higher, with at least 32MB (I think) ram or more. Unsupported hardware: MCA and EISA not supported, Io may not work. USB keyboard may not work. Quite a few IDE and SCSI raid-controllers may not work either.

DANGER WILL ROBINSON!
If used on users that have EFS encrypted files, and the system is XP or later service packs on win2k, all encrypted files for that user will be UNREADABLE! and cannot be recovered unless you remember the old password again.

Please see the Frequently Asked Questions before emailing questions to me. Thanks!

Also take a look at Grenier's DOS port

How to fix it if you lost your admin password for your ActiveDirectory. Thanks to John Simpson.

Other ways to recover lost password etc at MCSE World
NTFSDOS

Introduction

If you are interested in accessing NTFS drives from Windows 95 or Windows 98, then you should use NTFSDOS 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, use Windows 95 Repair Disk Command.

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 2.0'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
- NTFSDOS.H: Header file needed only for long filename support in Windows 95
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!

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

Time to get admin password = 10 minutes
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
Summary

• Physical security on PCs doesn’t exist
• You can’t detect hardware key loggers
• Admin PCs are as important as servers
• Trust no-one!
• If it’s on your PC or server - it’s stolen!
Countermeasures
Policy

- Management must understand that all of the money they spend on software patches, security hardware, and audits will be a waste without adequate prevention of social engineering and reverse social engineering attacks.

- One of the advantages of policies is that they remove the responsibility of employees to make judgement calls regarding a hacker's requests. If the requested action is prohibited by policy, the employee has no choice but to deny the hacker's request.
Building Security

• Install cameras so you can see who is coming and going
• Use biometrics or electronic security badges to limit access to the building
• No one should hold the door open for anyone not showing proper ID
Desktop Security

• Shred phone lists, email lists and other important documents before throwing away
• Some documents will need to be locked away
• Basic best practice - clear desk policy
IT Security

- Use screen savers with password controls
- Encrypt information on desktops, laptops and PDAs
- Secure mobiles and PDAs (infrared, bluetooth)
- Secure wireless (strong encryption, short range)
- Physically destroy unused hard disks, CDs and other media
User Guidance

• What can be discussed over the telephone
• What can be discussed outside the building
• What can be written in an e-mail
• Don’t use e-mail notification or voicemails when away from the office. It sets up the replacement as a target.
• How to report an incident and to whom
Help Desk

- Password resets only with call-back and PIN authentication
- Incident reporting and response procedures
- Clear escalation procedures
- Help desk staff should be encouraged to withhold support when a call does not feel right. In other words “just say no…..”
Training, training, training

- Train all employees - everyone has a role in protecting the organisation and thereby their own jobs
- If someone tries to threaten them or confuse them, it should raise a red flag
- Train new employees as they start
- Give extra security training to security guards, help desk staff, receptionists, telephone operators
- Keep the training up to date and relevant
How to Spot an SE Attack

• Refusal to give contact information
• Rushing
• Name-dropping
• Intimidation
• Small mistakes (misnomers, odd questions)
• Requesting forbidden information
• Look for things that don’t quite add up
Compliance

• Have a security assessment test performed and heed the recommendations
  - Test the company's ability to protect its environment, its ability to detect the attack and its ability to react and repel the attack
  - Have the first test performed when the company is expecting it
  - Do a blind test the second time around
Resources

- Social Engineering Fundamentals Sarah Granger (securityfocus.com)
- Cracking a Social Engineer Al Berg
- Social Engineering: Policies and Education a Must Rick Tims (sans.org)
- Social Engineering: A Backdoor to the Vault Chris Orr (sans.org)
- The Cyber Con Game – Social Engineering Christopher Paradowski (sans.org)
- How To Thwart The 'Social Engineers’ Sharon Gaudin
- Corporate Espionage 101 Shane W. Robinson (sans.org)
- A Proactive Defence to Social Engineering Wendy Arthurs (sans.org)
- People Hacking: The Psychology of Social Engineering Harl’s Talk at Access All Areas III
Need more information?

Peter Wood
Chief of Operations
First•Base Technologies

peterw@firstbase.co.uk
www.fbtechies.co.uk
www.white-hats.co.uk