## **The Future of Hacking**

### An Ethical Hacker's View



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
- Conceived network security best practice (1991)
- Presented BS 7799 throughout UK for BSI (1997)
- First independent ethical hacking firm in UK
- Founded white-hats.co.uk in 2002
- Times 1000 / FTSE 100 and CNI clients



## What is a hacker?

- Someone who plays golf poorly
- A programmer who breaks into computer systems in order to steal or change or destroy information
- A programmer for whom computing is its own reward; may enjoy the challenge of breaking into other computers but does no harm
- One who works hard at boring tasks

[WordWeb.info]

### Is that all?



## What is hacking?

• Hacking is a way of thinking

A hacker is someone who thinks outside the box. It's someone who discards conventional wisdom, and does something else instead. It's someone who looks at the edge and wonders what's beyond. It's someone who sees a set of rules and wonders what happens if you don't follow them. [Bruce Schneier]

- Hacking applies to all aspects of life and not just computers
- Increasingly, hacking is used to perpetrate crimes theft, blackmail, terrorism ...

## **Criminal hacking techniques**

- Internet intrusion attacks (against web applications, remote access portals)
- Trojans, rootkits, keyloggers et al. (via phishing, cross-site scripting, web sites)
- Botnets and denial of service attacks (primarily for blackmail or political attacks)
- Social engineering & physical attacks (insider attacks, wireless, bluetooth, laptop theft)



#### For web application attacks



#### For remote access attacks



This becomes an arms race criminals will seek an easier route ...



## The blended attack

## Social engineering plus technology



#### Currently:

- Phishing
- Trojans & rootkits
- Laptop theft
- In person intrusion

# X

## Why social engineering?



- 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.



## **Social engineering**

- 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



## **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!



## 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 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
- Do some shoulder surfing
- Plug in a sniffer or keylogger
- Simply use a vacant desk & workstation







Would you let this man into your building?













#### Time to get admin password = 10 minutes



## **Keystroke capture**

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

cisco



## A typical response



## **Preventing blended attacks**

All the money spent on software patches, security hardware, and audits could be wasted without prevention of social engineering attacks

That means investing in staff awareness backed up by policies



## Countermeasures

#### Physical aspect:

- in the workplace
- over the phone
- dumpster diving
- on-line

#### Psychological aspect:

- persuasion
- impersonation
- conformity
- friendliness

Combat strategies require action on **both** the physical and psychological levels



## **Staff Awareness**

- Train <u>all</u> 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



## **Workplace Security Policy**



- 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



## **End Point Security Policy**

- 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



## **Help Desk Policy**

- 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 ....."



## **Staff 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



## 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



## **End of Part One**



## **Need more information?**

### Peter Wood Chief of Operations First•Base Technologies

peterw@firstbase.co.uk

http://fbtechies.co.uk http://white-hats.co.uk http://peterwood.com



## The Real Risks of Stolen Laptops

### An Ethical Hacker's View



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
- Conceived network security best practice (1991)
- Presented BS 7799 throughout UK for BSI (1997)
- First independent ethical hacking firm in UK
- Founded white-hats.co.uk in 2002
- Times 1000 / FTSE 100 and CNI clients



## **This Presentation**

- All organisations now have laptop users
- Laptops are vulnerable to theft
- This info may help reduce your exposure!

## The target - a "corporate" laptop

- What sensitive information can we steal?
- What credentials can we steal?
- Can we connect to the corporate network?
- Can we introduce a Trojan?





## Some example objectives

- Company-confidential documents & spreadsheets
- User's logon
- The local admin logon
- User's personal data
- User's VPN logon
- The contents of the corporate network!





Slide 33



## If we can boot from CD ...





© First Base Technologies 2008



## We have the passwords!

	USERNAME/LMHASH	LMpasswd1	LMpasswd2	NTpasswd
00	Administrator	WINDOW5		
01	Guest	/EMPTY/		/EMPTY/
1002	SUPPORT_388945a0	/EMPTY/		
1003	XPADMIN	LONGHOR	N	L0ngh0rn
1004	ASPNET	01ZIANA		-
1011	HelpAssistant		ZYTC56G	
1014	LMAdmin	YA6PT3P	J1	yA6pT3pl1



## ... or just read the disk

=E SOFTWARE ]

Active@ UNERASER

Active@ KILLDISK [FREE]

Active@ Partition Recovery

Active@ Password Changer

Active@ NTFS Reader [FREE]

Active@ Disk Image

E DESCRIP that provi from a MS. NTES Reade provides r a MS DOS e supports fragmented NTFS and co

or network

© First Base Technologies 2008



## Find the password hashes

HDD 80h	C:\WINDOWS\system32\config\		
HDD 81h	Long file name	Size	
Unallocated	SAM	262144	
└→ Logical D:	SAM.LOG	1824	
🛏 Unallocated	SECURITY	262144	
HDD 82h	SECURITY.LOG	1924	
HDD 83h	SecEvent.Evt	262144	
	SysEvent.Evt	131972	
	TempKey.LOC	1924	
	Windows .evt	65536	
	WindowsPowerShell.evt	65536	
	default	524288	
	default.LOG	1824	
	default.sav	94208	
	netlogon ftl	256	
	software	25427968	
	software LOG	1824	
	software sau	659456	
	sustem	5767168	
	sustem LOG	1024	
F1-Help	Tab-DOS names ENTER-Preview Ctr	+С-Сору	
ctive@ NIFS Reader for DO	S v 1.0.2 http://	//www.NTFS.com	
FREEMARE>	1000 2002 (C) Octivo Data Por	woru Software	



## **Copy hashes to USB key**



© First Base Technologies 2008

## Copy hashes to your cracking PC and plug in the rainbow tables





## ... a few minutes later







### No CD boot possible, but we have access to CMOS

•	0	• •
Page 1 of 7	Dell Computer Corporatio Dell Latitude D800 Se	n (www.dell.com) ries Setup BIOS Version: A07
Time: 103:28 Pentium M Current CPU Speed Level 2 Cache System Memory Video Controlles Video Memory Panel Type Audio Controlles Modem Controlles Primary Hard Drive Modular Bay System D-Bay	Date: Fri Sep 1, 2006 1.30 GHz/600 MHz 1.30 GHz/600 MHz 1.024KB 1.30 GHz/600 MHz 1.024KB	Resets the time on the computer's internal clock. Time is kept in a 24-hour format (hrs:mins:secs). Enter new values or press the left- or right-arrow key to decrease or increase the value.
C Copyright 1990-20 T,4 ch	opyright 1985-1988 Phoeni 04 Dell Computer Corporat ange fields +,+ change va	x Technologies Ltd. ion and others, All Rights Reserved lues Alt-P page Esc exit
	C DELL	0

© First Base Technologies 2008

## Only the hard disk is enabled

Dell Latitude D600 Series Setup

CD/DVD/CD-RW Drive Internal HDD Diskette Drive USB Storage Device Modular Bay HDD Cardbus NIC D/Dock PCI slot NIC Omboard NIC

Page 2 of

This category co system file sear CAUTION: DISK DRIVE LETTE THIS SETTING IS

The System searc system files on list. If the fi bootable, not pr enabled, the sys the second devic until the system list is exhausted



## Config is password protected, but the hard disk is not

#### Page 7 of 7 Dell Computer Corporation Dell Latitude D600 Ser

\*\*\*\*\*\*\*\*\* System Security \*\*\*\*\*\*\*\*\*
Primary Password: Disabled
Admin Password: Enabled
Configure Setup: Disabled
Configure Passwords: Enabled
\*\*\*\*\* Hard-disk drive password(s) \*\*\*\*
System Primary: Disabled









## .. And read it in our laptop!



		Server and a		
		<dir></dir>	04-14-2004	8:43
		(DIR)	84-14-2884	8:43
APPEVENT E	VT	524,288	09-03-2006	1:51
DEFAULT		196,608	09-01-2006	5:51
DEFAULT S	AV	81,920	07-10-2003	1:47
SAM		28,672	09-03-2006	1:51
ECEVENT E	VT	65,536	64-14-2664	9:03
ECURITY		40,960	09-03-2006	2:47
OFTWARE	27	,942,912	09-03-2006	2:47
OFTWARE S	AU	536.576	07-10-2003	1:47
YSEVENT E	UT	524.288	89-83-2886	1:51
YSTEM	5	.149.489	09-03-2005	2:47
YSTEN AL	LT 5	.149.489	89-83-2886	2:47
YSTEM SI	AU	352.256	87-18-2883	1:47
SERDIFF		139.264	87-18-2883	1.47
13	file(s)	40.7	14.240 hutes	1.411
2	dir(s)	13.25	4 Mega hutes	free





## So what now?

- What sensitive information can we steal?
- What credentials can we steal?
- Can we connect to the corporate network?
- Can we introduce a Trojan?





# What sensitive information can we steal?

- Almost anything on the hard disk!
  - MS Office passwords are no protection
  - Neither are zip files (usually)
  - Windows EFS may not protect you either
- But we cannot see data that has been encrypted using a proven algorithm (e.g. PGP volumes)

# What credentials can we steal?

- Almost anything on the hard disk!
  - All local Windows password hashes
  - Cached Windows logons
  - Dial-up credentials
  - E-mail passwords
  - Cached web credentials
  - Etc.



# Can we connect to the corporate network?

- Very probably!
  - We know the local Windows passwords
  - If you use two-factor authentication, where is your SecurID card and PIN kept?
  - Perhaps the help desk will be very helpful?
  - Perhaps we can use a Trojan to get access later

## Can we introduce a Trojan?

- Since we are local Administrator, yes!
  - We can turn off anti-virus
  - We can turn off the personal firewall
  - We can hide the Trojan using a rootkit
- Game over!



## However ...







## **ATA Password Reset**



#### Home / Products / Repair station

#### Overview

Repair Station is data recovery software which allows you:

- to diagnose and repair system area problems of hard disk drives,
- to remove passwords from drives locked with an ATA-password (security level HIGH or MAXIMUM).

We appreciate your feedback on our web site

#### © First Base Technologies 2008



Slide 58

© First Base Technologies 2008





## **Need more information?**

### Peter Wood Chief of Operations First•Base Technologies

peterw@firstbase.co.uk

http://fbtechies.co.uk http://white-hats.co.uk http://peterwood.com

