

The seven deadly sins of DLP

Know your enemy

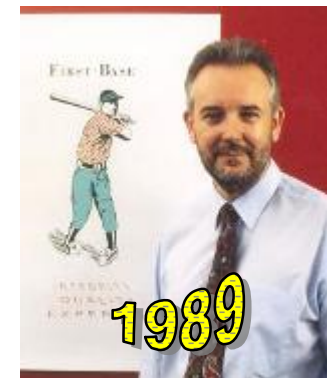


Peter Wood
Chief Executive Officer
First • Base Technologies



Who am I ?

- Worked in computers & electronics since 1969
- Founded First Base Technologies in 1989
(one of the first ethical hacking firms)
- Primary roles:
 - Network penetration tester
 - Social engineer
 - Conference speaker
 - TV and radio security 'expert'
 - Security author
 - Active member of BCS, IISP and ISACA
 - aka Famous Pete Wood Security (FPWS)





Thinking like a hacker

- **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**
- not just computers



SNMP for hackers

- If you know the read string (default *public*) you can read the entire MIB for that device
- If you know the read-write string (default *private*) you may be able to change settings on that device
- You may be able to 'sniff' community strings off the network if they've been changed from the defaults
- You may be able to control a router or switch:
 - Intercept traffic and read sensitive information
 - 'Crash' the network repeatedly
 - Lock the device out, requiring physical access to reset it
- You may be able to list users, groups, shares etc. on servers
- You may be able to subvert wireless network security



Sin #1

Insecure network infrastructure

- SNMP on by default when not used
- SNMP default community strings in use
- SNMP v3 seldom implemented
- Easy-to-guess or default passwords
- Passwords shared between staff & never changed
- Infrastructure is rarely tested or audited
- Clear standards, regular network discovery checks and lots of training is the defence



Windows is complicated

- Windows permissions are confusing
- Default groups can be a problem ('everyone')
- There isn't enough granularity:
 - Domain Admins / Enterprise Admins
 - Account Operators / Server Operators (seldom used)
 - The rest!
- Confusion between domain accounts and local accounts
- Windows password weaknesses are not understood
- Usually way too many 'Domain Admins'



Sin #2

Insecure Windows domains

- Badly configured permissions
- Too much access for too many accounts
- Too many privileged accounts
- Obviously named service accounts
- Easy-to-guess passwords
- No idea how to make a strong password (don't know about LM hashes!)
- Unpatched systems, because inside is safe!
- Clear standards, regular penetration tests and lots of training is the defence



Laptop hacking





Just read the disk

“Without a username and password I was able to use a boot CDROM to bypass the login password and copy the document files from my hard drive to my iPod in about 3 minutes 15 seconds.”

```
Drives
HDD 00a
  Logical E:
  Logical D:
  Extended
  Logical E:
  Logical F:
  Unallocated
HDD 01a
  Unallocated
HDD 02a
  Extended
  Unallocated
  Logical G:
```

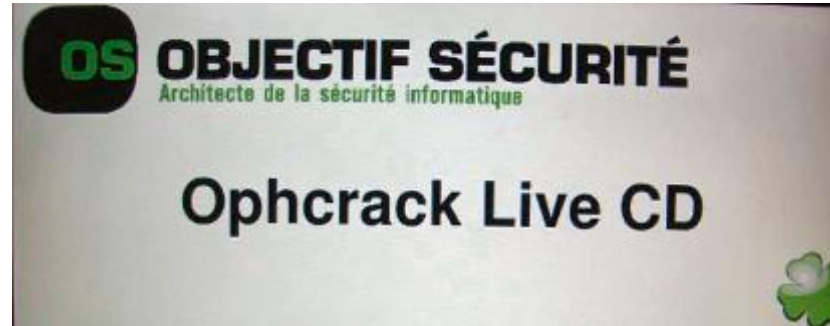
```
Logical drive C:
C:\
  Name      Size      Attrb     Date      Time
  MICROSOFT <<FOLDER>> ..... 04.02.2002 16:16
  MULTIMEDIA <<FOLDER>> ..... 14.10.2001 22:29
  PLATFORM <<FOLDER>> ..... 15.03.2002 16:15
  PROGRAM <<FOLDER>> ..... 14.10.2001 08:11
  RECYCLED <<FOLDER>> ...S... 26.11.2001 17:55
  RECYCLER <<FOLDER>> ..... 07.02.2002 22:55
  Temp <<FOLDER>> ..... 15.03.2002 16:13
  WINNT <<FOLDER>> ..... 14.10.2001 08:06
  Winlog <<FOLDER>> ..... 11.04.2002 13:57
  AUTOEXEC.BAT 0 A..... 14.10.2001 08:14
  CONFIG.SYS 0 A..... 14.10.2001 08:14
  IO.SYS 0 A..... 14.10.2001 08:14
  NBT <<FOLDER>> 8555648 A..... 18.03.2002 17:29
  MSDOS.SYS 0 A..... 14.10.2001 08:14
  NTFSROOT.COM 20480 A..... 14.10.2001 22:28
  boot.ini 200 A..S.. 14.10.2001 08:57
  ntldr 156496 A..... 14.10.2001 22:28
  pagefile.sys 134217720 A..... 04.02.2002 16:21
```

F1-Help Tab-Long names CTRL-Previous Ctrl-C-Copy
Active@ NTFS Reader for DOS v 1.0 2002 (C) Active Data Recovery Software
CFRECS http://www.ntfs.com

NTFS Reader DOS Boot Disk provides read access to NTFS drives from the MS DOS environment. It supports long filenames as well as compressed and fragmented files. **NTFS Reader for DOS** allows you to preview the files on NTFS and copy them from NTFS to FAT volumes or network drives. In order to use the software you need to copy the **readntfs.exe** file to a bootable floppy disk and boot from it.



... or crack a local password



Ophcrack is a free Windows password cracker based on rainbow tables by the inventors of the method. It comes with a Graphical User Interface and runs on multiple platforms.

XPADMIN	LONGHOR	N	L0ngh0rn
LMAdmin	YA6PT3P	J1	yA6pT3pJ1



... or change a local password

A screenshot of a web browser window. The address bar shows the URL: http://home.eunet.no/~pnordahl/ntpasswd/bootdisk.html. The browser has several tabs open, including 'FBTechies', 'White-Hats Group', 'Google', 'Hunger Site', 'BBCi', 'IDE files', '192.com', and 'Amazon.co.uk'. The search bar contains the text 'Linux NT boot CD'. The main content of the page is titled 'Offline NT Password & Registry Editor, Bootdisk'. The text on the page describes a bootdisk for editing NT passwords and lists hardware requirements and warnings.

Address <http://home.eunet.no/~pnordahl/ntpasswd/bootdisk.html> Go

Links [FBTechies](#) [White-Hats Group](#) [Google](#) [Hunger Site](#) [BBCi](#) [IDE files](#) [192.com](#) [Amazon.co.uk](#) »

Google Search Web Search Site News PageRank Page Info Up »

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, i2o 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



Sin #3

Insecure laptops and desktops

- Physical security on Windows desktops and laptops doesn't exist
- Native Windows security is ineffective if you have physical access
- Everything is visible: e-mails, spreadsheets, documents, passwords
- If it's on your machine – it can be stolen!
- Encryption is the best defence, coupled with lots of training



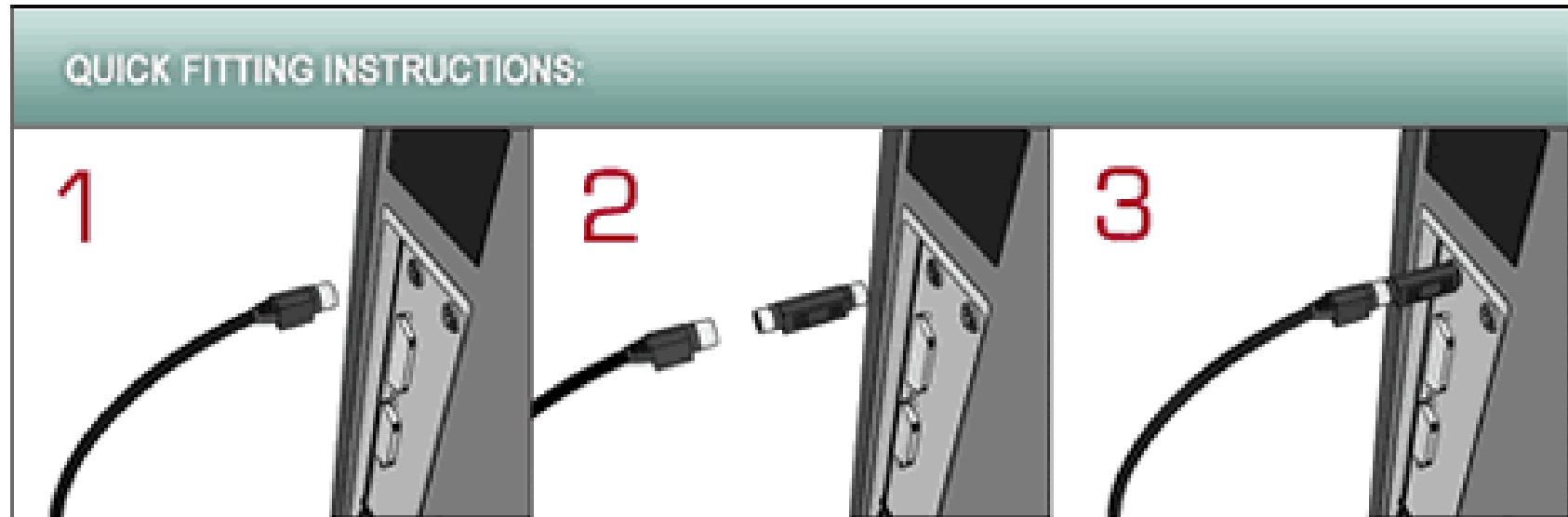
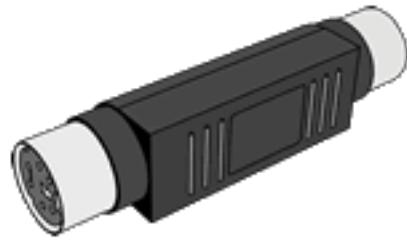
Sin #4 Insecure buildings

- Cleaners:
 - No vetting
 - Out-of-hours access
 - Cleans desks (and under them)
 - Takes out large black sacks
- Inadequate visitor control
- Tailgating
- Lack of challenge / reporting
- Clear standards, regular physical penetration tests and lots of training is the defence





Hardware keyloggers





Sin #5

Insecure workspaces

- No clear desk policy
- Machines left logged on
- No supervision of visitors
- No physical inspections
- Lack of challenge / reporting
- Clear standards, regular inspections, physical penetration tests and lots of training is the defence



USB devices

- Memory sticks
- iPods
- USB bling





Sin #6

Insecure USB connectivity

- Inadequate policy on MP3 players
- Lack of controls on USB ports
- Implicit trust of staff
- No physical inspections
- Lack of challenge / reporting
- Clear standards, USB port controls, regular inspections and lots of training is the defence



Home workers and public WiFi

- Home wireless networks used for business
- Public hotspots used for work
- Convenience versus security
- False sense of security provided by VPNs





Eavesdropping

Packet sniffing unprotected WiFi can reveal:

- logons and passwords for unencrypted sites
- all plain-text traffic
(e-mails, web browsing, file transfers, etc)

```
Content-Type: application/x-www-form-urlencoded  
Content-Length: 49  
  
username=bill%40microsoft.com&password=mypasswordHTTP/1.1 200 OK  
Date: Tue, 06 Apr 2010 13:46:03 GMT
```



Active attacks

Once connected to the network an attacker can:

- conduct man-in-the-middle attacks (including SSL and TLS)
- redirect traffic
- spoof legitimate machines
- hijack PDAs, iPhones, etc

SSL/TLS man-in-the-middle attack tool

sslsniff is designed to create man-in-the-middle (MITM) attacks for SSL/TLS connections, and dynamically generates certs for the domains that are being accessed on the fly. The new certificates are constructed in a certificate chain that is signed by any certificate that is provided. sslsniff also supports other attacks like null-prefix or OCSP attacks to achieve silent interceptions of connections when possible.



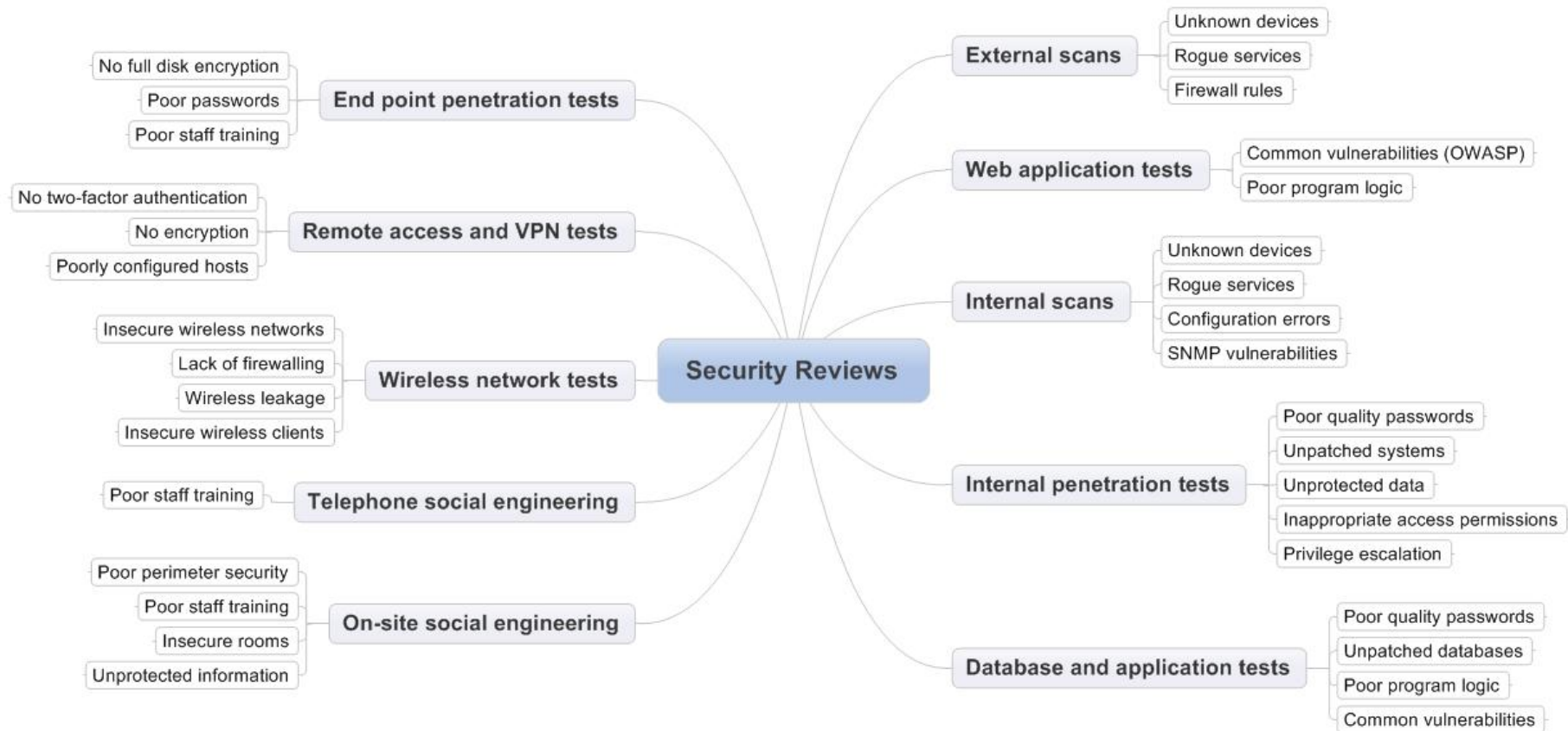
Sin #7

Insecure home and public WiFi

- No encryption (or only WEP)
- Plain text traffic (email, unencrypted sites)
- SSL VPNs on unencrypted wireless
- Wireless networks are hubs!
- Wireless is radio!
- Clear standards, WPA2 encryption, regular tests and lots of training is the defence



Pragmatic security reviews





Need more information?

Peter Wood

Chief Executive Officer

First • Base Technologies LLP

peterw@firstbase.co.uk

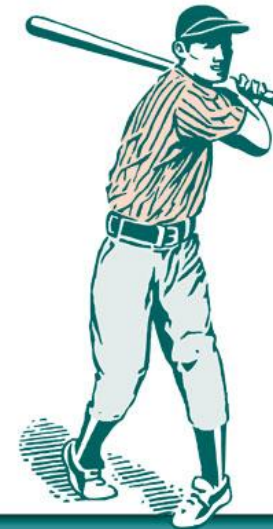
Twitter: [peterwoodx](#)

Blog: fpws.blogspot.com

<http://firstbase.co.uk>

<http://white-hats.co.uk>

<http://peterwood.com>



FIRST • BASE
technologies