

# PILFERING LOCAL DATA: THINGS AN ATTACKER WOULD WANT TO GRAB WITH SHORT TERM LOCAL ACCESS

Adrian Crenshaw



# About Adrian

- ▣ I run Irongeek.com
- ▣ I have an interest in InfoSec education
- ▣ I don't know everything - I'm just a geek with time on my hands
- ▣ (ir)Regular on:  
<http://www.isdpodcast.com/>



# What I plan to cover

- ▣ Core items an attacker would want to locate and copy off of a Windows system with short term access
- ▣ Data that could be found: Passwords, Usernames Docs, Emails, Paths
- ▣ Tools they would use to bypass weak security precautions like file system permissions and OS/BIOs passwords



# Why this talk is sort of a sham

- ▣ If you have short term access, your goal as an attacker should be to extend that access
- ▣ There are just so many options for useful files to grab, so it's hard to decide the most important
- ▣ Still useful from the context of stolen and decommissioned equipment, but then time is not as critical



# HOW ARE WE GETTING AT THE DATA?



# Distros/Boot environments

Just a few:

- ▣ BackTrack Linux  
<http://www.backtrack-linux.org>
- ▣ Bart's PE/UBCD4Win  
<http://www.nu2.nu/pebuilder/>  
<http://www.ubcd4win.com/>
- ▣ Winbuilder/Win7PE SE  
<http://winbuilder.net/> & <http://reboot.pro/12427/>
- ▣ Konboot  
<http://www.piotrbania.com/all/kon-boot/>



# BackTrack Linux

- ▣ Tons of security tools
- ▣ Awesome hardware support for odd wireless needs
- ▣ Well maintained
- ▣ Can do a hard drive install if you wish



Image from <http://www.backtrack-linux.org/screenshots/>



# Bart's PE/UBCD4Win

- Bart's PE can be built from the files on a Windows XP CD
- UBCD4Win is Bart's Pe with a bunch of extras + Multi-boot (DBAN)
- Plugins can be made to add functionality

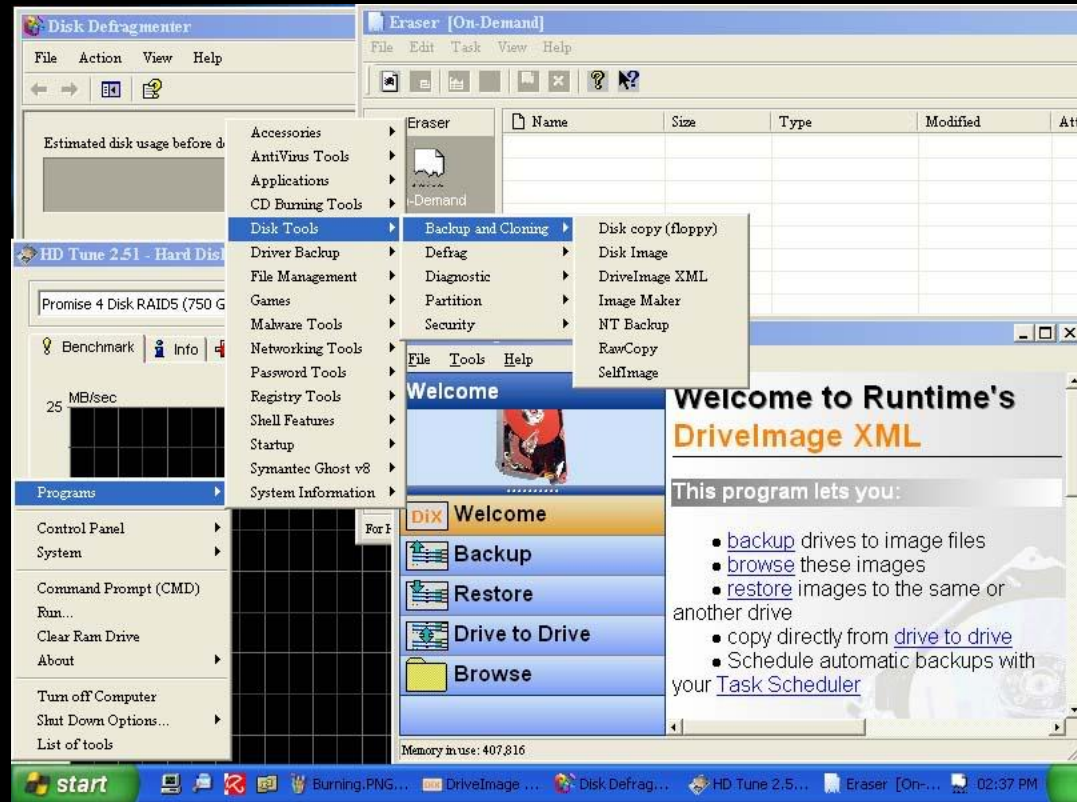


Image from <http://www.ubcd4win.com/screen.htm>





# Winbuilder/Win7PE SE

- ▣ Make a Windows based boot USB/CD/DVD
- ▣ Starting OS needed depends on build
- ▣ Plugins can be made to add functionality
- ▣ Build even up to Win7 SP1 32/64bit
- ▣ Hardcore roll your own

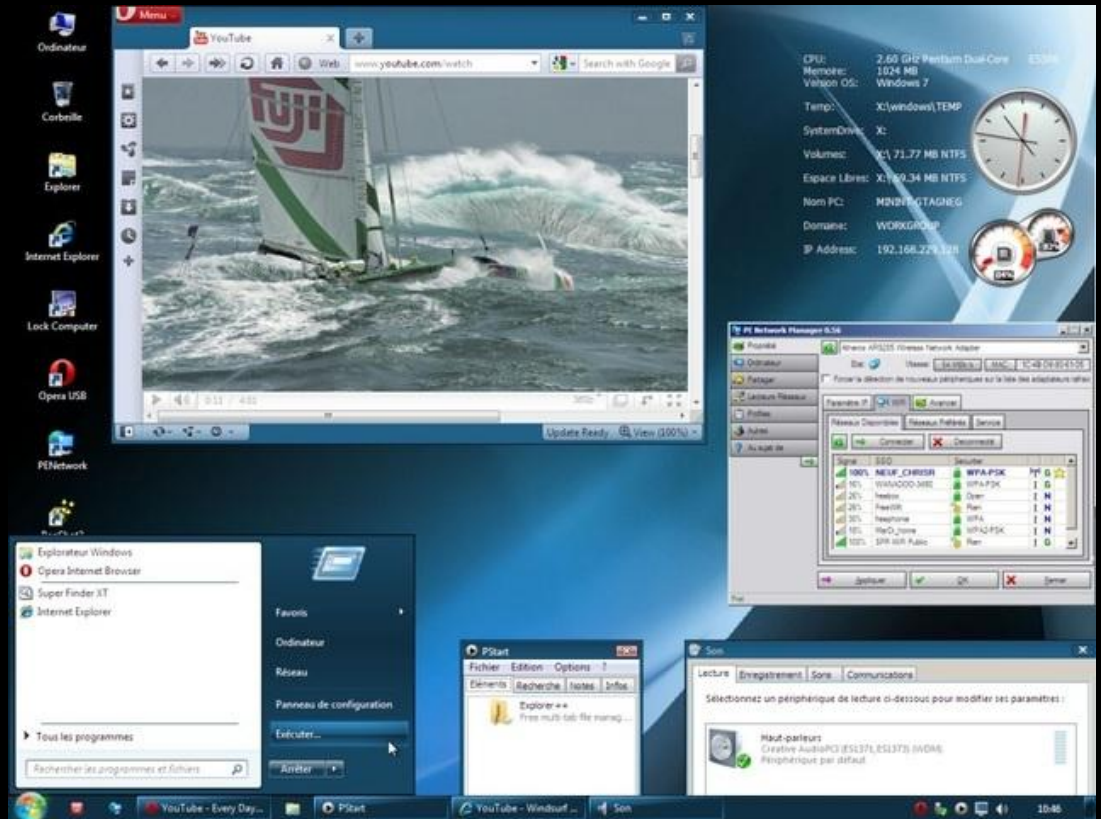


Image from <http://reboot.pro/12427/>



# Konboot

- ▣ Bypass password on some versions of Windows and Linux
- ▣ Changes kernel on boot
- ▣ Login to Linux with “konusr” as username.
- ▣ Use a blank password in Windows
- ▣ Meant to run from a CD/Floppy, sometimes works from a UFD using instructions found here: <http://www.irongeek.com/i.php?page=security/kon-boot-from-usb>



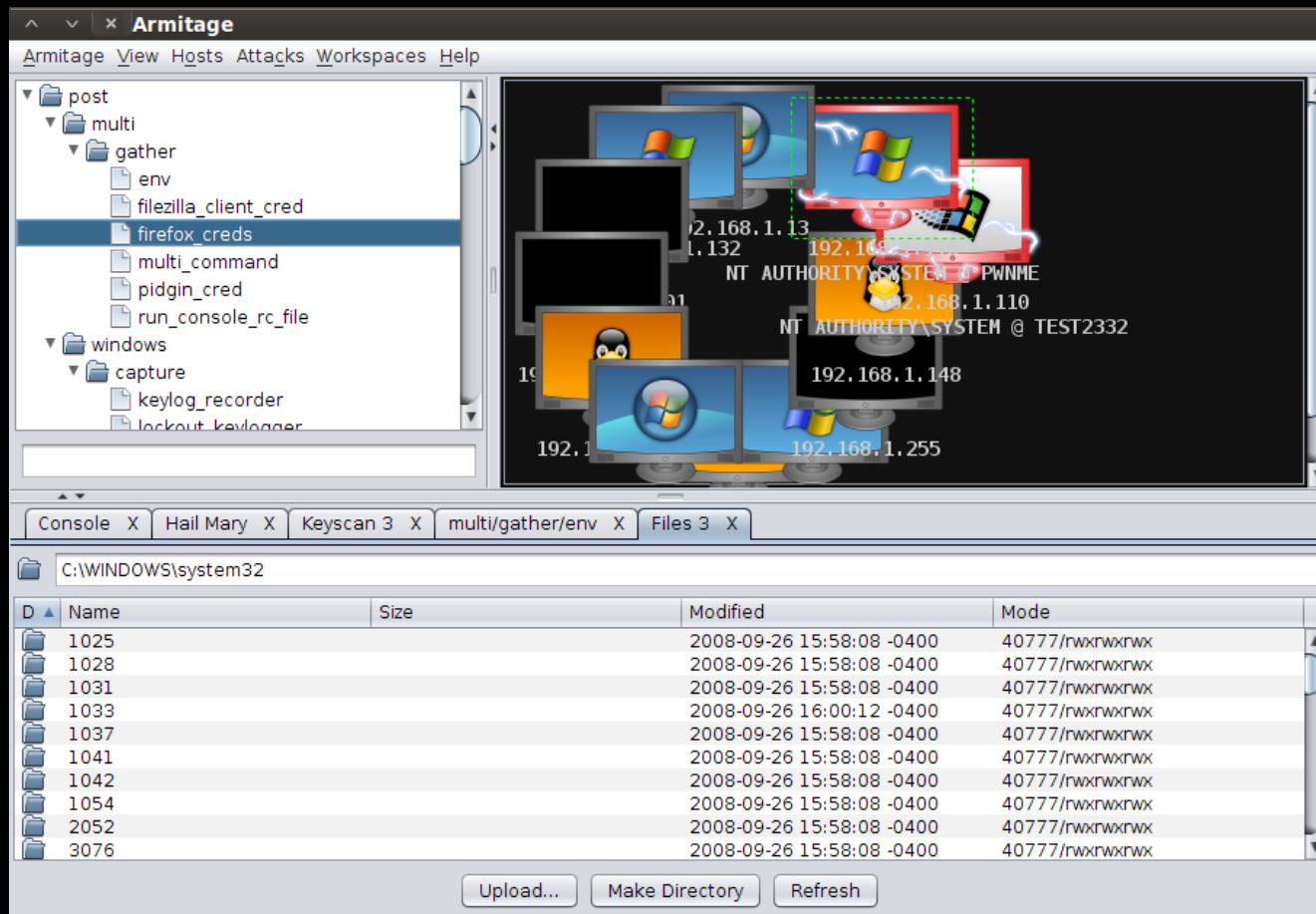
Image from <http://www.piotrbania.com/all/kon-boot/>



# Remote exploits as well

- Metasploit/Armitage

<http://www.fastandeasyhacking.com/>

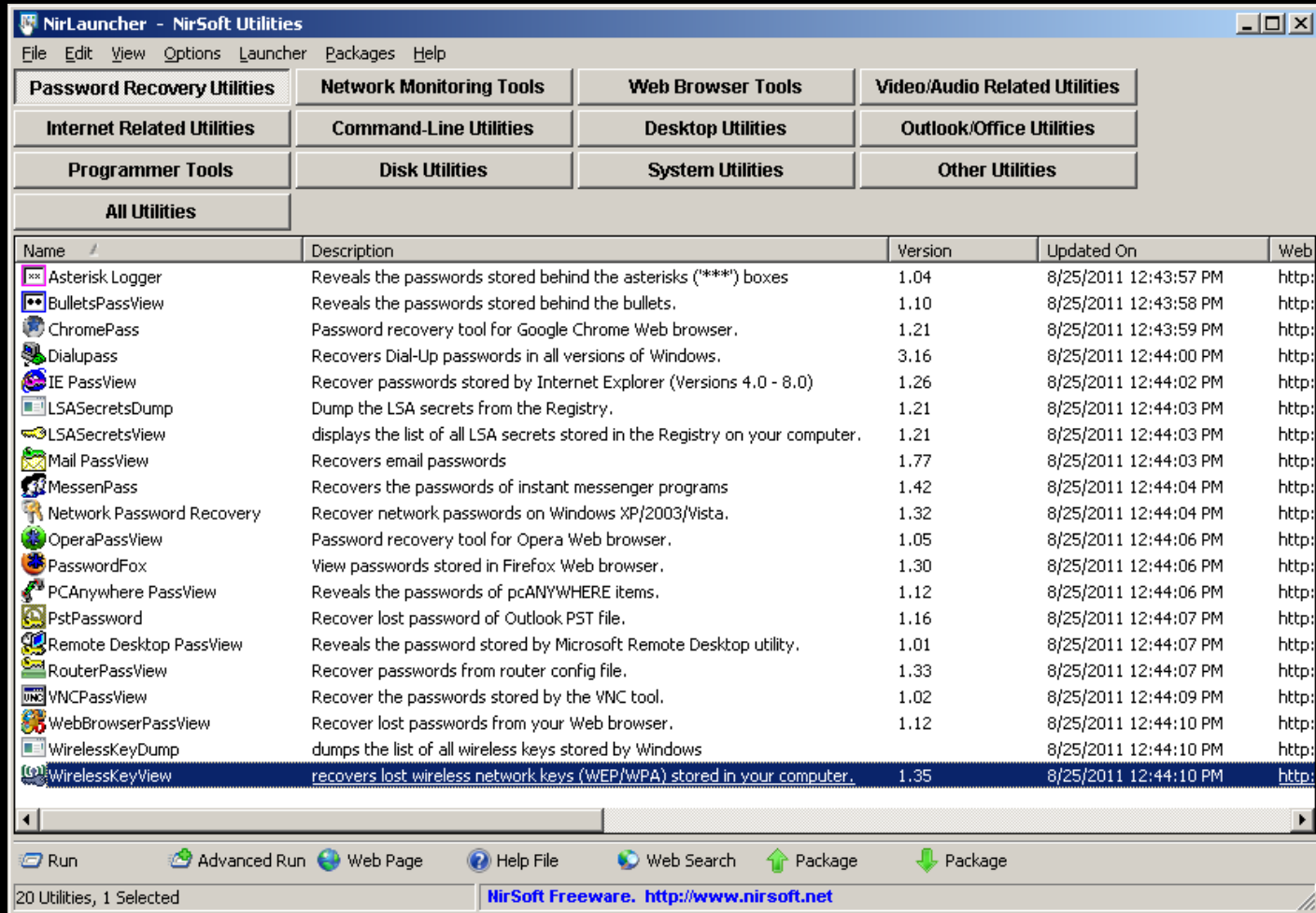


# SOME USEFUL TOOLS



# NirSoft Tools

▣ <http://launcher.nirsoft.net/>



The screenshot shows the NirLauncher application window with the following categories and tool list:

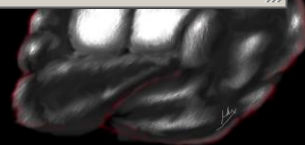
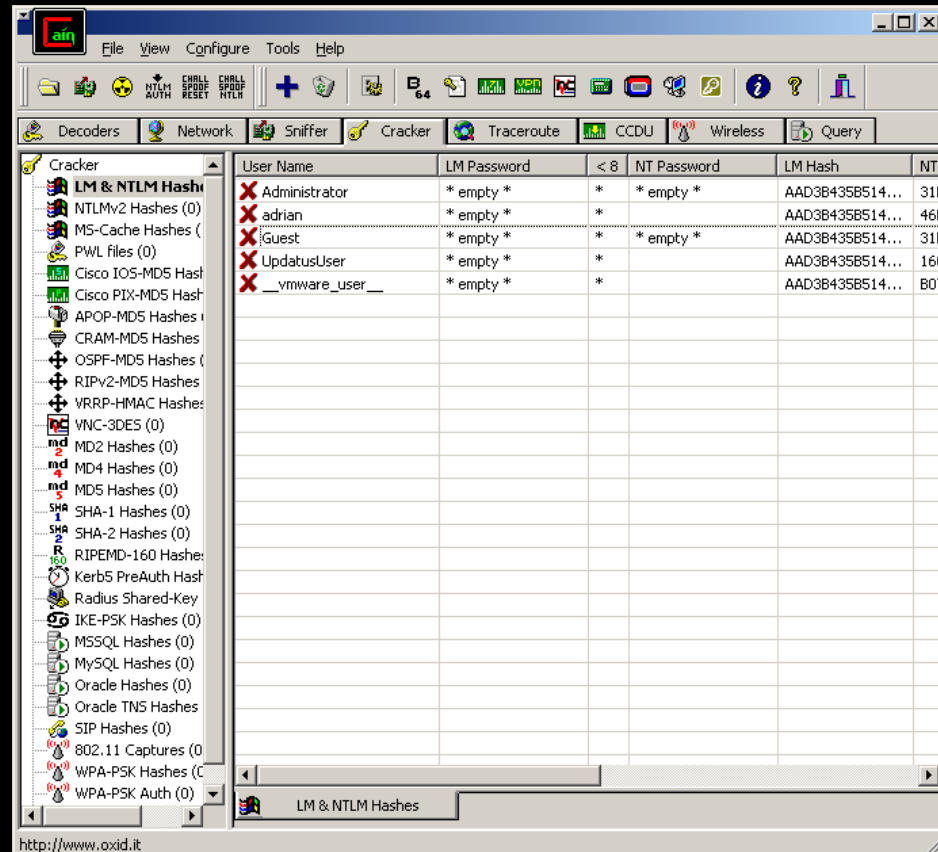
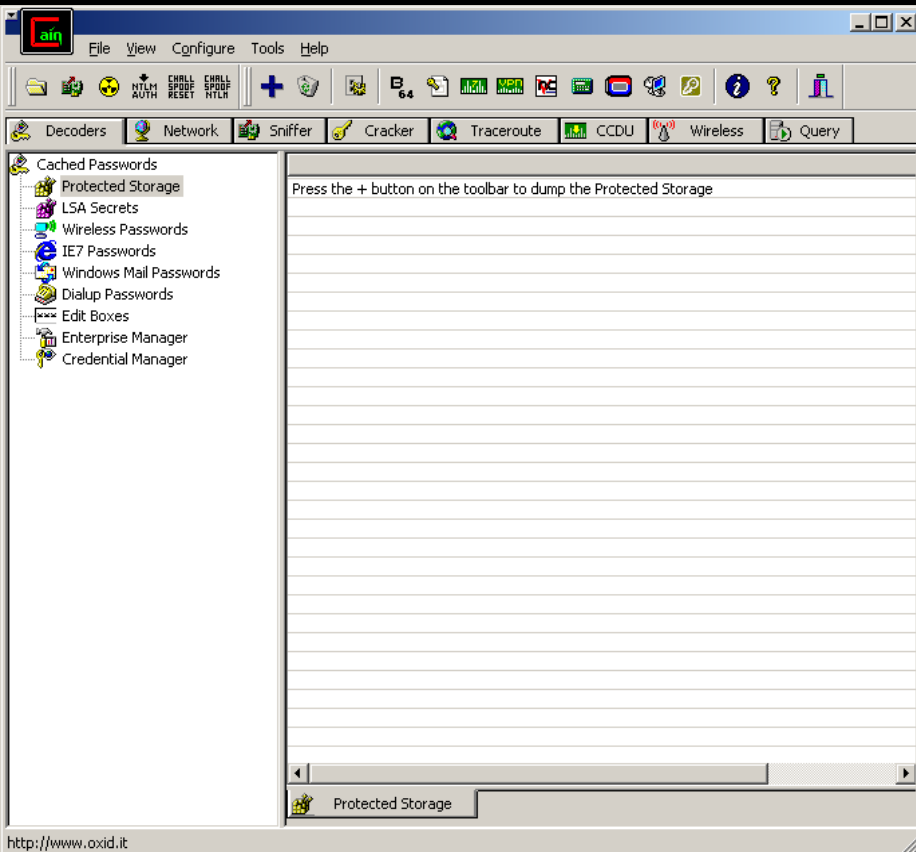
Name	Description	Version	Updated On	Web
Asterisk Logger	Reveals the passwords stored behind the asterisks ("***) boxes	1.04	8/25/2011 12:43:57 PM	http:
BulletsPassView	Reveals the passwords stored behind the bullets.	1.10	8/25/2011 12:43:58 PM	http:
ChromePass	Password recovery tool for Google Chrome Web browser.	1.21	8/25/2011 12:43:59 PM	http:
Dialuppass	Recovers Dial-Up passwords in all versions of Windows.	3.16	8/25/2011 12:44:00 PM	http:
IE PassView	Recover passwords stored by Internet Explorer (Versions 4.0 - 8.0)	1.26	8/25/2011 12:44:02 PM	http:
LSASecretsDump	Dump the LSA secrets from the Registry.	1.21	8/25/2011 12:44:03 PM	http:
LSASecretsView	displays the list of all LSA secrets stored in the Registry on your computer.	1.21	8/25/2011 12:44:03 PM	http:
Mail PassView	Recovers email passwords	1.77	8/25/2011 12:44:03 PM	http:
MessenPass	Recovers the passwords of instant messenger programs	1.42	8/25/2011 12:44:04 PM	http:
Network Password Recovery	Recover network passwords on Windows XP/2003/Vista.	1.32	8/25/2011 12:44:04 PM	http:
OperaPassView	Password recovery tool for Opera Web browser.	1.05	8/25/2011 12:44:06 PM	http:
PasswordFox	View passwords stored in Firefox Web browser.	1.30	8/25/2011 12:44:06 PM	http:
PCAnywhere PassView	Reveals the passwords of pcANYWHERE items.	1.12	8/25/2011 12:44:06 PM	http:
PstPassword	Recover lost password of Outlook PST file.	1.16	8/25/2011 12:44:07 PM	http:
Remote Desktop PassView	Reveals the password stored by Microsoft Remote Desktop utility.	1.01	8/25/2011 12:44:07 PM	http:
RouterPassView	Recover passwords from router config file.	1.33	8/25/2011 12:44:07 PM	http:
VNCPassView	Recover the passwords stored by the VNC tool.	1.02	8/25/2011 12:44:09 PM	http:
WebBrowserPassView	Recover lost passwords from your Web browser.	1.12	8/25/2011 12:44:10 PM	http:
WirelessKeyDump	dumps the list of all wireless keys stored by Windows		8/25/2011 12:44:10 PM	http:
WirelessKeyView	recovers lost wireless network keys (WEP/WPA) stored in your computer.	1.35	8/25/2011 12:44:10 PM	http:

At the bottom of the window, there are buttons for Run, Advanced Run, Web Page, Help File, Web Search, Package (up and down arrows), and a status bar showing "20 Utilities, 1 Selected" and "NirSoft Freeware. <http://www.nirsoft.net>".



# Cain

□ <http://www.oxid.it/cain.html>



# PASSWORDS

and hashes



# Windows System Trifecta

- ▣ C:\Windows\System32\config
  - SAM
  - SYSTEM
  - SECURITY
- ▣ Grab These Files!!!
- ▣ NTUSER.DAT may also be useful as it maps to HKEY\_CURRENT\_USER
- ▣ Hell, get SOFTWARE to while you are at it!





# Why these files?

- ▣ Cain
  - LSA Secrets:SYSTEM and SECURITY
  - Cached passwords:SYSTEM and SECURITY
  - SAM Hashes: SAM and SYSTEM
  
- ▣ WirelessKeyView will do via Windows dir on Windows XP



# Why exploit local passwords?

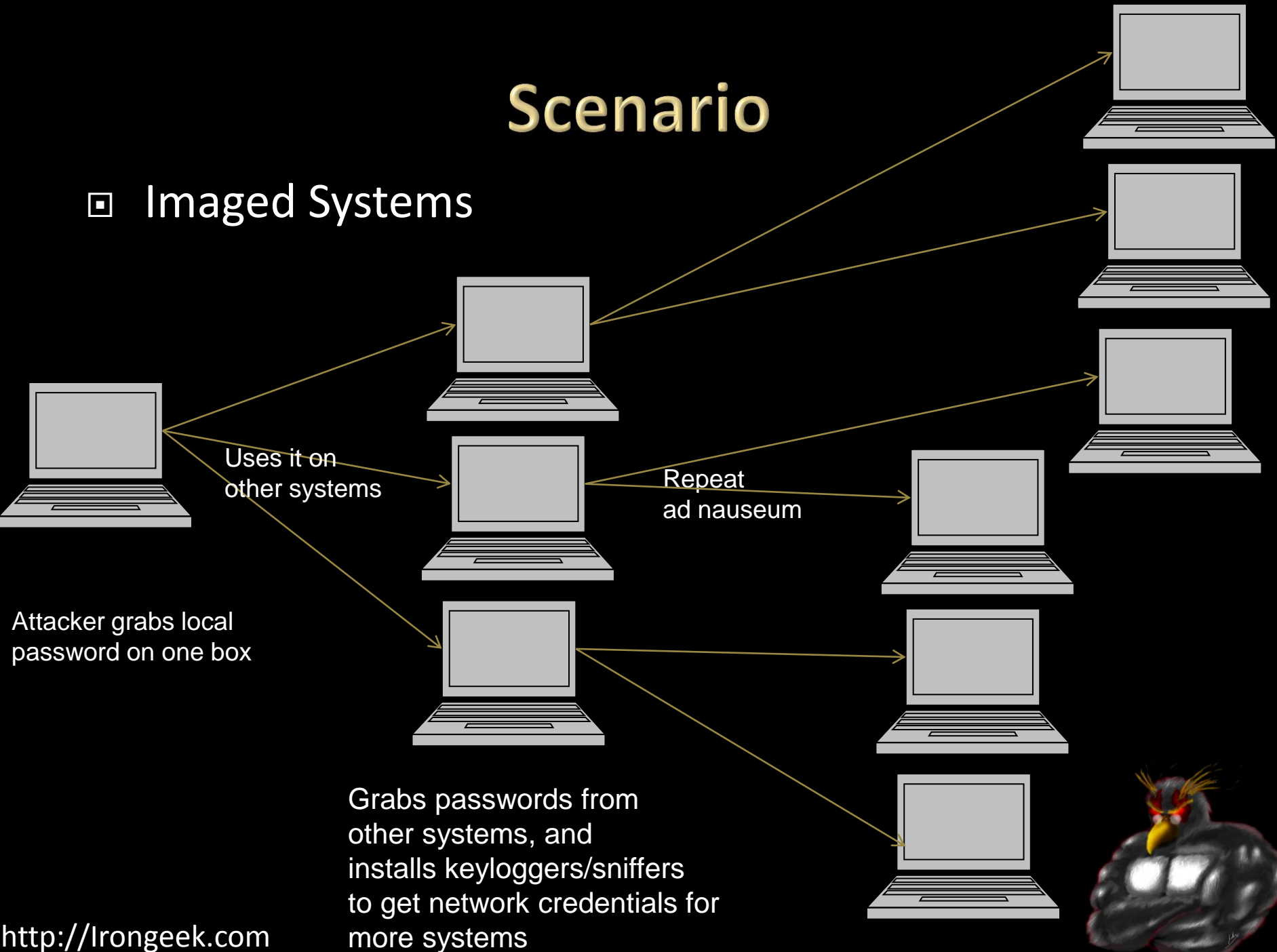
There are several reasons why an attacker may want to find local passwords:

- ❑ To escalate privileges on the local host (install games, sniffers, key stroke catchers and other software or just to bypass restrictions).
- ❑ Local passwords can be used to gain access to other systems on the network. Admins may reuse the same usernames and passwords on other network hosts (more than likely if they use hard drive imaging). Similar themes are also often used for password selection.
- ❑ Just for the fun of doing it.



# Scenario

## ▣ Imaged Systems



# Glossary

Cracking a Password: De-obfuscating a password's representation.

Brute force attack: Using all possible character combinations till a match for the password is found. Also known as an incremental attack in John the Ripper.

Dictionary attack: Using each entry in a word list until a match for the password is found.

Hashing: Applying a mathematical formula to a piece of text to get a shorter number or string.

One way hash: A hash where the original string the hash was derived from can not be easily found by a simple method.

Plain text: The un-obfuscated or un-encrypted form of a string. Opposite of cipher text.

Password Hash: The "hashed" version of a password that's stored for later authentication.

Reversible Encryption (Obfuscation): Encryption that is easily reversed if the algorithm is known. Example: ROT13.

Salt: A number used to seed a hashing or encryption algorithm to add to the possible number of outcomes the ciphertexts.



# Hash Examples

Type	Hash
plaintext	badpass
MD2	9C5B091C305744F046E551DB45E7C036
MD4	640061BD33AA12D92FC40EA87EA408DE
MD5	F1BFC72887902986B95F3DFDF1B81A5B
SHA-1	AF73C586F66FDC99ABF1EADB2B71C5E46C80C24A
SHA-2 (256)	4F630A1C0C7DD182D2737456E14C89C723C5FCE25CAE39DA4B93F00E90A365CB
SHA-2 (384)	8E3B1BB56624C227996941E304B061FD864868AA3DB92A1C82AE00E336BE90809E60BB2A29FC1692189DE 458B6300016
SHA-2 (512)	6109E5BDF21C7CC650DC211CF3A3706FAB8D50B132762F6D597BE1BD499E357FAF435FAB220FA40A106770 7D0E0C28F39C1EC41F435C4D820E8AB225E37489E3
RIPMD-160	595FD77AA71F1CE8D7A571CB6ABDA2A502BA00D4
LM	4CF3B1913C3FF376
NT	986CA892BEAB33D1FC2E60C22EC133B7
MySQL323	0AFDA7C85EE805C2
MySQLSHA1	229749C080B28D3AEFAB78279C4668E6E12F20FA
Cisco PIX	RtJk8qcKDPR.2D/E
VNC Hash	DAD3B1EB680AD902



# Great Resources

- ❑ Password Storage Locations For Popular Windows Applications  
[http://www.nirsoft.net/articles/saved\\_password\\_location.html](http://www.nirsoft.net/articles/saved_password_location.html)  
Also, using tools to reverse engineer what his apps were doing helped a bunch
- ❑ Bunch of my stuff on hacking SAM/SYSTEM hashes  
<http://www.irongeek.com/i.php?page=security/cracking-windows-vista-xp-2000-nt-passwords-via-sam-and-syskey-with-cain-ophcrack-saminside-bkhive-etc>
- ❑ Question Defense  
<http://www.question-defense.com/>
- ❑ Ron's Password Lists  
<http://www.skullsecurity.org/wiki/index.php/Passwords>



# Assumptions and Workarounds

- ▣ In most cases, these tools/attacks will require physical access to a box
- ▣ In some cases you will...
  1. ...need to be logged into the target account on the box.
  2. ...just need access to the file system.
  3. ...you must be logged in as the target account, and not have changed the password using a boot CD. 😊



# Windows Profile Info

- ▣ I used C:\ in this presentation as the root drive, but it could be something else
- ▣ Some differences in subdirectories when it comes to profiles
- ▣ Win 7/Vista  
C:\Users
- ▣ Windows XP  
C:\Documents and Settings\  
Let's use <profile> as shorthand





# AppData

- ▣ Enable the viewing of system and hidden files and folders
- ▣ Windows 7/Vista
  - <profile>\AppData\Local
  - <profile>\AppData\LocalLow
  - <profile>\AppData\Roaming
- ▣ Windows XP (sort of)
  - <profile>\Application Data , maps to Roaming
  - <profile>\Local Settings\Application Data, maps to Local
- ▣ Go read  
<http://download.microsoft.com/download/3/b/a/3ba6d659-6e39-4cd7-b3a2-9c96482f5353/Managing%20Roaming%20User%20Data%20Deployment%20Guide.doc>



# More Details

- ▣ <profile>\AppData\Roaming  
Synchronized with the server if roaming profiles are used.
- ▣ <profile>\AppData\Local  
Specific to that computer, even with roaming profiles enabled. Also meant for larger files.
- ▣ <profile>\AppData\LocalLow  
Same use as LocalLow, but with lower integrity level and can be written to in protected mode.



# Windows local accounts: LM

LAN Manager (Used in older Windows Operating System)

1. Convert password to upper case.
2. Pad the plaintext with null characters to make it 14 bytes long.
3. Split into two 7 character (byte) chunks.
4. Use each 7 byte chunks separately as keys to DES encrypt the magic value ("KGS!@#\$%" or in HEX 0x4b47532140232425).
5. Concatenate the two cipher texts from step four to produce the hash.
6. Store the hash in the SAM file.



# Windows local accounts: NTLM

## NT Manager

1. Take the Unicode mixed-case password and use the Message Digest 4 (MD4) algorithm to obtain the hash.
2. Store the hash in the SAM file.



# Open Source/Free tools for cracking the SAM

- ▣ FGDump (Pwddump)  
<http://www.foofus.net/~fizzgig/fgdump>
- ▣ Cain  
<http://www.oxid.it/cain.html>
- ▣ Backtrack 5R1 DVD (SAMDump2 and other tools)  
<http://www.backtrack-linux.org/>



# A few notes on using SAMDump from Backtrack

```
fdisk -l  
mkdir /media/sda1  
mount /dev/sda1 /media/sda1 -o force  
samsdump2  
/media/sda1/Windows/System32/config/SYSTEM  
/media/sda1/Windows/System32/config/SAM >hashes.txt
```



# Cached Domain Credentials

- ❑ Cracking Cached Domain/ADS Passwords

By default Windows systems in a domain or Active Directory tree cache the credentials of the last ten previously logged in users. This is done so that the users can still login again if the Domain Controller or ADS tree can not be reached either because of Controller failure or network problems. These cached passwords are stored as encrypted (using NL\$KM LSA) hashes in the local systems registry at the values:

HKEY\_LOCAL\_MACHINE\SECURITY\CACHE\NL\$1

through

HKEY\_LOCAL\_MACHINE\SECURITY\CACHE\NL\$10

- ❑ I've read the algorithm for MSCacheV1 is:

**MD4(MD4(Unicode(\$pass)).Unicode(strtolower(\$username)))**

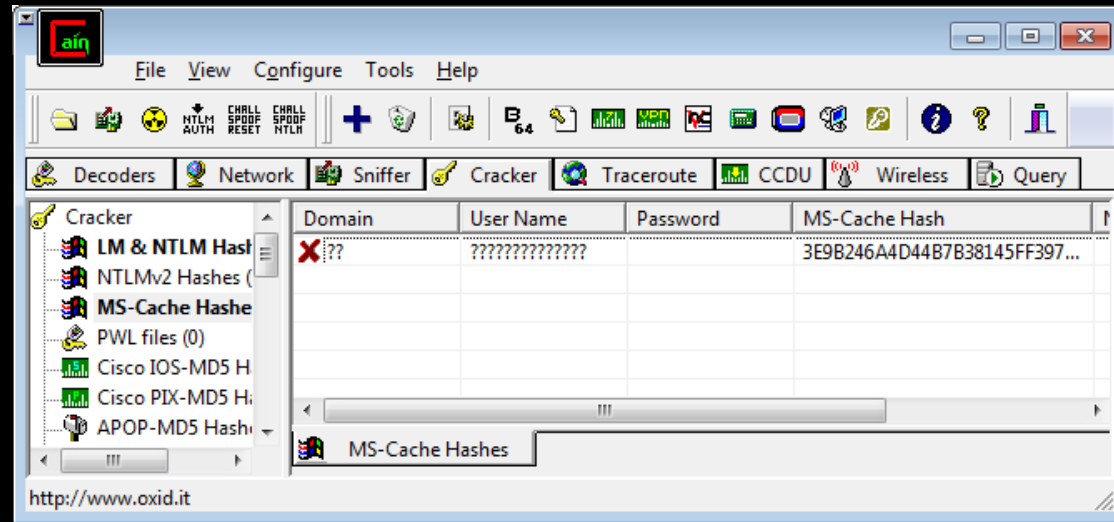
according to the folks at <http://www.insidepro.com>

- ❑ MSCacheV2 adds even more issues



# Win 7 + Cain ~~does not seem to work~~

## ▣ Cain



## ▣ Hashcat <http://hashcat.net>

format:

98bc149b523691e3e51a91b6596e9750:somedomainuser





# Cracking Creds Countered

- ▣ Credential Cache Cracking Countermeasures
  1. Choose stronger domain passwords. Use more than just alpha-numeric characters and perhaps throw in some extended ASCII characters by way of the Alt+num-pad method.
  2. For those who are still paranoid and have a VERY reliable connection to their domain controller, they can follow these steps to disable the caching of passwords and credentials: Set the registry value

HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon\CachedLogonsCount

to 0 then reboot. This can also be done with the Local Security Policy or with a GPO.

3. Use same “Fascist Methods” as before for restricting physical access to the computer.



# Unknown Apps: System Process Monitoring Apps and Demo

- ▣ ProcessActivityView  
[http://www.nirsoft.net/utils/process\\_activity\\_view.html](http://www.nirsoft.net/utils/process_activity_view.html)
- ▣ RegFromApp  
[http://www.nirsoft.net/utils/reg\\_file\\_from\\_application.html](http://www.nirsoft.net/utils/reg_file_from_application.html)
- ▣ Procmon  
<http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx>



# Unknown Apps: Don't know how it's hashed?

- ▣ Compare the hash to know examples of other hashes
- ▣ Get a copy of the app, use the password “password” and search for the resulting hash on Google
- ▣ Get the source code
- ▣ How good are you at reverse engineering with a debugger?



# Browser Passwords: Firefox

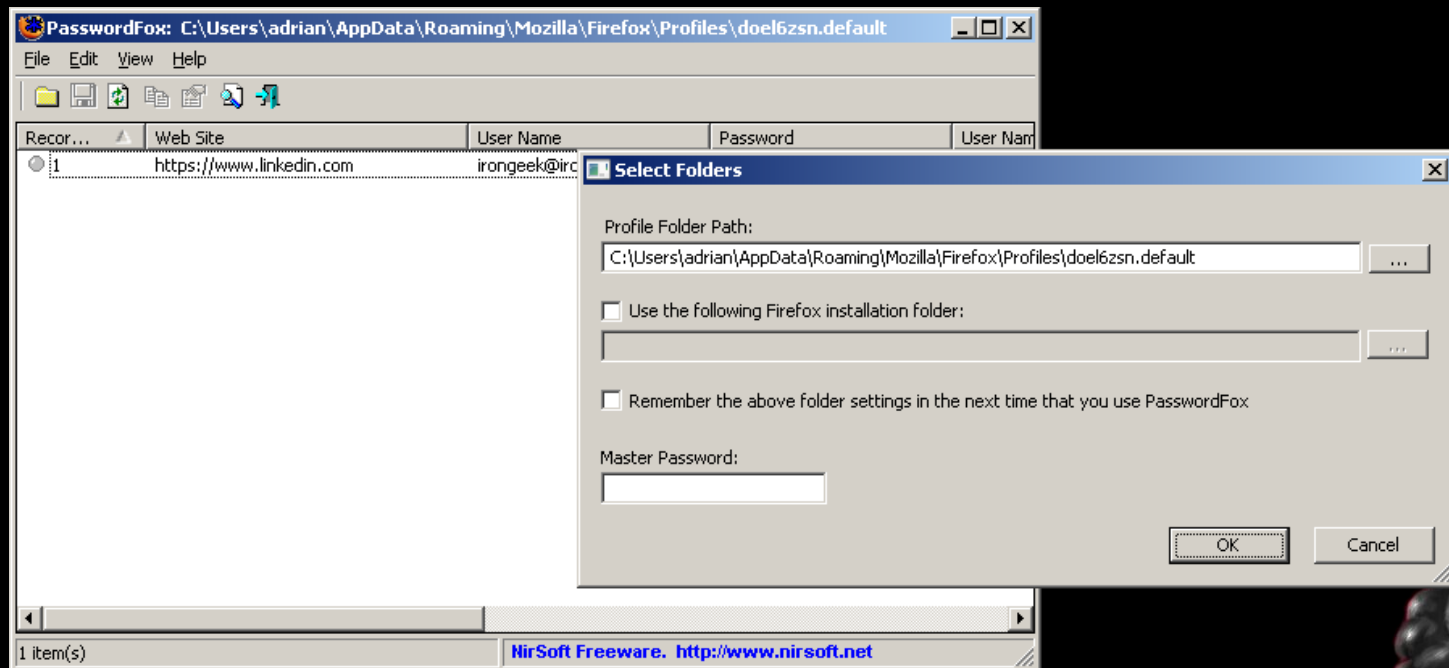
Stored in an SQLite database, but needing some key files

<profile>\AppData\Roaming\Mozilla\Firefox\Profiles\<Firefox Profile>\secmod.db

<profile>\AppData\Roaming\Mozilla\Firefox\Profiles\<Firefox Profile> \cert8.db

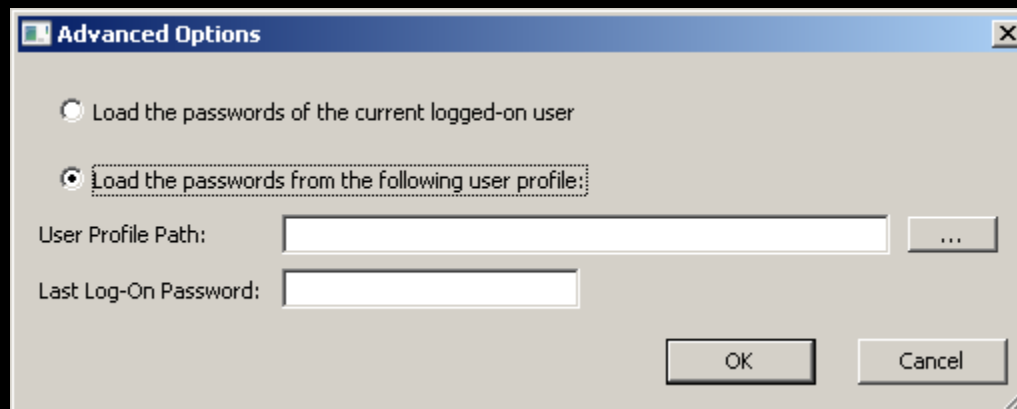
<profile>\AppData\Roaming\Mozilla\Firefox\Profiles\ <Firefox Profile>\key3.db

<profile>\AppData\Roaming\Mozilla\Firefox\Profiles \<Firefox Profile>\ signons.sqlite



# Browser Passwords: Internet Explorer

- ▣ IE 4-6: Sprt in registry called Protected storage:  
HKEY\_CURRENT\_USER\Software\Microsoft\Protected Storage System Provider
- ▣ IE 7+: All auto complete passwords in reg at  
HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2  
Have to know the URL to decrypt, but can guess common URLs.
- ▣ HTTP passwords for IE 7 in “Credential” directory under profile  
<Windows Profile>\AppData\Roaming\Microsoft\Credentials



# Great Apps

- ▣ PSPV

<http://www.nirsoft.net/utils/pspv.html>

- ▣ PasswordFox

<http://www.nirsoft.net/utils/passwordfox.html>

- ▣ IE Passview

[http://www.nirsoft.net/utils/internet\\_explorer\\_password.html](http://www.nirsoft.net/utils/internet_explorer_password.html)

- ▣ ChromePass

<http://www.nirsoft.net/utils/chromepass.html>



# VNC



- ▣ Depends on Version

I know old ones could be found here:

TightVNC:

HKEY\_CURRENT\_USER\Software\ORL\WinVNC3

HKEY\_LOCAL\_MACHINE\SOFTWARE\ORL\WinVNC3

HKEY\_USERS\.DEFAULT\Software\ORL\WinVNC3

RealVNC:

HKEY\_CURRENT\_USER\Software\RealVNC\WinVNC4

HKEY\_LOCAL\_MACHINE\SOFTWARE\RealVNC\WinVNC4

HKEY\_USERS\.DEFAULT\Software\RealVNC\WinVNC4

- ▣ The password is DES encrypted, but since the fixed key (23 82 107 6 35 78 88 7) is know, it was trivial to decrypt.
- ▣ UltraVNC  
Same basic algorithm, two bytes added on the end (not sure why) and stored in:  
C:\Program Files\UltraVNC\ultravnc.ini
- ▣ Try Cain or Nir's VNCPassView to decode



# Remote Desktop Protocol (RDP)

- ▣ Apparently use to be saved in the .RDP file
- ▣ Now seems to be in the same place as Network Credentials
- ▣ Try RDPV from Nir, Or Cain





# Instant Messaging Varies

▣ So many, it would suck to list them, so let's ask Nir:  
[http://www.nirsoft.net/articles/saved\\_password\\_location.html](http://www.nirsoft.net/articles/saved_password_location.html)

▣ I use PidginPortable from my Desktop, so for it:  
<Windows Profile>\Desktop\PidginPortable\Data\settings\purple

▣ Doing it by hand sucks

▣ MessenPass

<http://www.nirsoft.net/utis/mypass.html>



MSN Messenger

Windows Live Messenger

Google Talk

AOL Instant Messenger v4.6 or below, AIM 6.x, and AIM Pro.

Trillian

MySpace IM

Miranda

PaltalkScene

Windows Messenger (In Windows XP)

Yahoo Messenger (Versions 5.x and 6.x)

ICQ Lite 4.x/5.x/2003

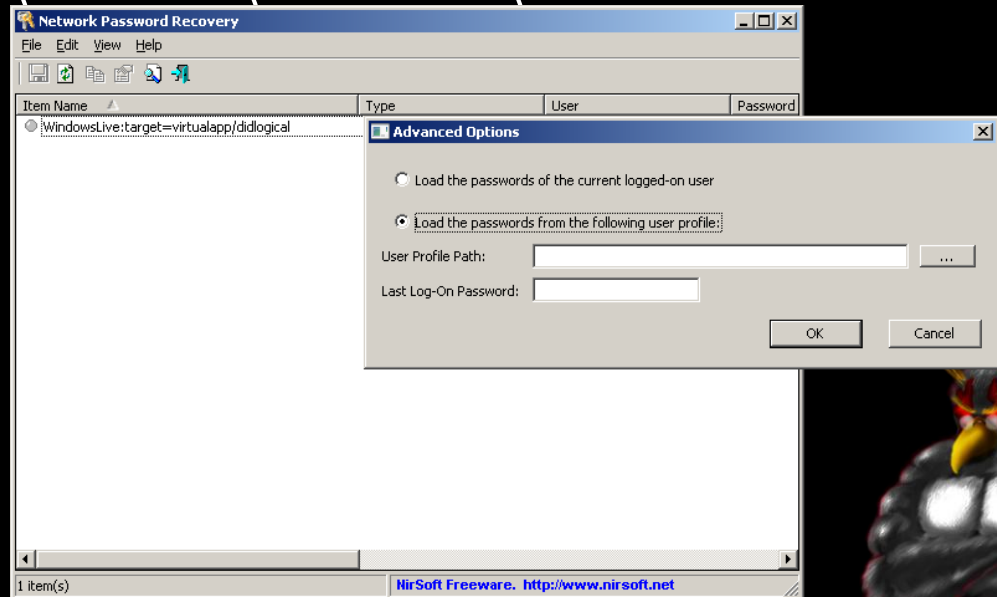
GAIM/Pidgin

Digsby



# Network Shares

- Windows XP/2003: <Profile>\Application Data\Microsoft\Credentials\<User SID>\Credentials and [Windows Profile]\Local Settings\Application Data\Microsoft\Credentials\[User SID]\Credentials
- Windows Vista:  
<Profile>\AppData\Roaming\Microsoft\Credentials\<Random ID>  
<Profile>\AppData\Local\Microsoft\Credentials\<Random ID>



# Wireless

## Forget cracking it, just look it up!

- ▣ Based on interface number
- ▣ Vista/Windows 7 store in:  
C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces
- ▣ XP in:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\<Interface Guid>
- ▣ They appear to be encrypted, but apparently the key is available to programs with the right privileges

Details obtained from here:

[http://www.nirsoft.net/utils/wireless\\_wep\\_key\\_faq.html](http://www.nirsoft.net/utils/wireless_wep_key_faq.html)



# OTHER DATA



# Outlook Cache (if in Cached Exchange Mode)

- ▣ Find and .OST file in  
C:\Users\\AppData\Local\Microsoft\Outlook
- ▣ Open with Kernel OST Viewer  
<http://www.nucleustechnologies.com/download-ost-viewer.php>



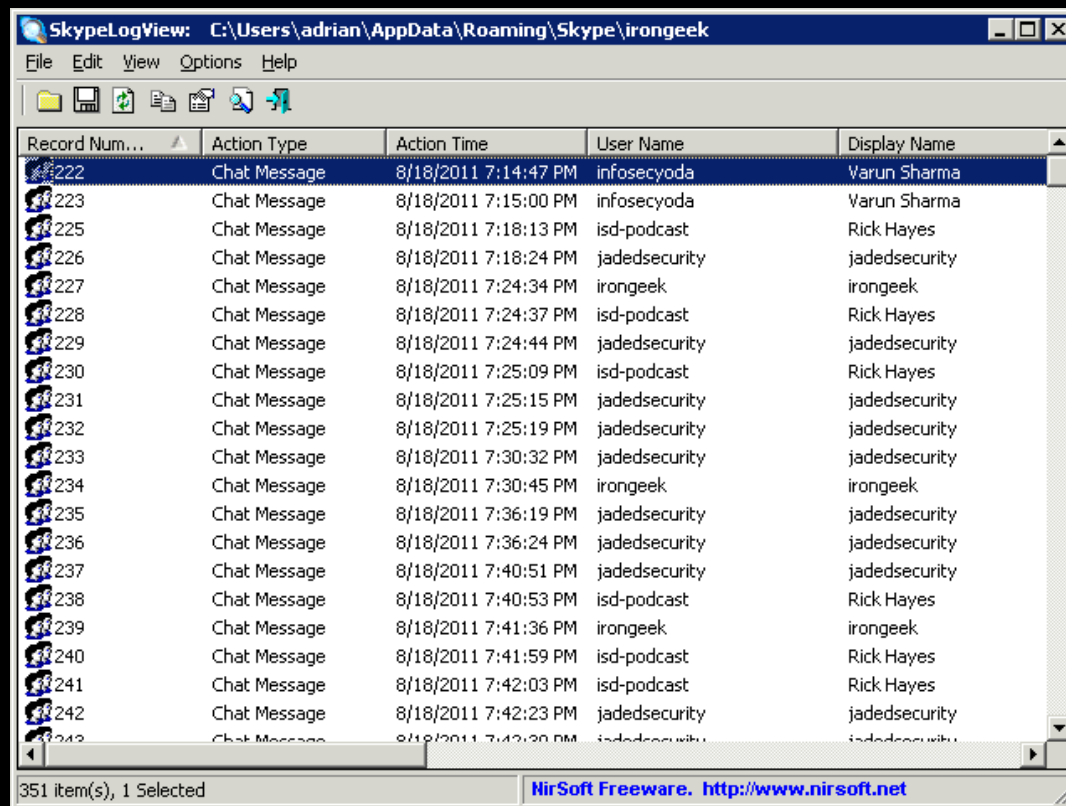
# Outlook 2010 Attachments Temp

- ▣ Outlook Attachments Temp  
<Profile>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook
- ▣ If the item was open when Outlook was closed, it may be here
- ▣ May have to forcefully browse to this by typing in the path



# Skype logs

- Database file in:  
<Profile>\AppData\Roaming\Skype\<Skype ID>



The screenshot shows the SkypeLogView application window. The title bar reads "SkypeLogView: C:\Users\adrian\AppData\Roaming\Skype\irongeek". The menu bar includes "File", "Edit", "View", "Options", and "Help". Below the menu bar is a toolbar with icons for file operations. The main area is a table with the following columns: "Record Num...", "Action Type", "Action Time", "User Name", and "Display Name". The table contains 17 rows of chat messages, with the first row (Record 222) selected. The status bar at the bottom indicates "351 item(s), 1 Selected" and "NirSoft Freeware. <http://www.nirsoft.net>".

Record Num...	Action Type	Action Time	User Name	Display Name
222	Chat Message	8/18/2011 7:14:47 PM	infosecyoda	Varun Sharma
223	Chat Message	8/18/2011 7:15:00 PM	infosecyoda	Varun Sharma
225	Chat Message	8/18/2011 7:18:13 PM	isd-podcast	Rick Hayes
226	Chat Message	8/18/2011 7:18:24 PM	jadedsecurity	jadedsecurity
227	Chat Message	8/18/2011 7:24:34 PM	irongeek	irongeek
228	Chat Message	8/18/2011 7:24:37 PM	isd-podcast	Rick Hayes
229	Chat Message	8/18/2011 7:24:44 PM	jadedsecurity	jadedsecurity
230	Chat Message	8/18/2011 7:25:09 PM	isd-podcast	Rick Hayes
231	Chat Message	8/18/2011 7:25:15 PM	jadedsecurity	jadedsecurity
232	Chat Message	8/18/2011 7:25:19 PM	jadedsecurity	jadedsecurity
233	Chat Message	8/18/2011 7:30:32 PM	jadedsecurity	jadedsecurity
234	Chat Message	8/18/2011 7:30:45 PM	irongeek	irongeek
235	Chat Message	8/18/2011 7:36:19 PM	jadedsecurity	jadedsecurity
236	Chat Message	8/18/2011 7:36:24 PM	jadedsecurity	jadedsecurity
237	Chat Message	8/18/2011 7:40:51 PM	jadedsecurity	jadedsecurity
238	Chat Message	8/18/2011 7:40:53 PM	isd-podcast	Rick Hayes
239	Chat Message	8/18/2011 7:41:36 PM	irongeek	irongeek
240	Chat Message	8/18/2011 7:41:59 PM	isd-podcast	Rick Hayes
241	Chat Message	8/18/2011 7:42:03 PM	isd-podcast	Rick Hayes
242	Chat Message	8/18/2011 7:42:23 PM	jadedsecurity	jadedsecurity
243	Chat Message	8/18/2011 7:42:20 PM	jadedsecurity	jadedsecurity



# Look in the logs

- ▣ Windows XP  
C:\Windows\System32\config in \*.evt files
- ▣ Vista and newer  
C:\Windows\System32\winevt\Logs in \*.evtx files
- ▣ Did the user type the name in the wrong place?  
<http://www.irongeek.com/i.php?page=security/pebkac-attack-passwords-in-logs>





# Printer Spool

- ▣ Sometimes a print job will get stuck here, and we all know what useful information people sometimes print.
- ▣ Location:  
C:\Windows\System32\spool\PRINTERS
- ▣ Try some of the tool listed at the bottom of this page:  
<http://www.undocprint.org/formats/winspool/spl>
- ▣ O&K Printer Viewer and LBV SPLViewer recommended



# So many others...

- ❑ Internet Explorer History  
<profile>\AppData\Local\Microsoft\Windows\History
- ❑ IE Cookies  
<profile>\AppData\Roaming\Microsoft\Windows\Cookies
- ❑ Firefox Cached Pages  
<profile>\AppData\Local\Mozilla\Firefox\Profiles\<some profile number>.default\Cache
- ❑ Firefox Form History File  
<profile>\ AppData\Roaming\Mozilla\Firefox\Profiles\<some profile number>.default\formhistory.sqlite
- ❑ Firefox Cookies  
<profile>\AppData\Roaming\Mozilla\Firefox\Profiles\<some profile number>.default\cookies.sqlite



# A word on automation

- ▣ Look at using an autorun payload off of a U3
- ▣ Video on Russell Butturini's payload:  
<http://www.irongeek.com/i.php?page=videos/incident-response-u3-switchblade>
- ▣ See this wiki:  
[http://www.hak5.org/w/index.php/USB\\_Hacksaw](http://www.hak5.org/w/index.php/USB_Hacksaw)



# Other Resources: Videos

- ▣ Making Windows 7 SP1 32/64bit Boot CD/DVD/USBs with Winbuilder Video  
[http://www.irongeek.com/i.php?page=videos/oisf-2011#Making\\_Windows\\_7\\_SP1\\_32/64bit\\_Boot\\_CD/DVD/USBs\\_with\\_Winbuilder](http://www.irongeek.com/i.php?page=videos/oisf-2011#Making_Windows_7_SP1_32/64bit_Boot_CD/DVD/USBs_with_Winbuilder)
- ▣ Password Exploitation Class Video  
<http://www.irongeek.com/i.php?page=videos/password-exploitation-class>
- ▣ Portable Boot Devices (USB/CD/DVD):Or in Canadian, what is this all about?  
<http://www.irongeek.com/i.php?page=videos/portable-boot-devices-usb-cd-dvd>



# Other Resources

- ▣ Forensically interesting spots in the Windows 7, Vista and XP file system and registry

<http://www.irongeek.com/i.php?page=security/windows-forensics-registry-and-file-system-spots>

- ▣ Building a boot USB, DVD or CD based on Windows 7 with WinBuilder and Win7PE SE Tutorial

<http://www.irongeek.com/i.php?page=security/winbuilder-win7pe-se-tutorial>

- ▣ Mubix's Windows Post Exploitation List

[https://docs.google.com/document/d/1U10isynOpQtrIK6ChuReu-K1WHTJm4fgG3joiuz43rw/edit?hl=en\\_US](https://docs.google.com/document/d/1U10isynOpQtrIK6ChuReu-K1WHTJm4fgG3joiuz43rw/edit?hl=en_US)

- ▣ Mubix's Linux Post Exploitation

[https://docs.google.com/document/d/1ObQB6hmVvRPCgPTRZM5NMH034VDM-1N-EWPRz2770K4/edit?hl=en\\_US](https://docs.google.com/document/d/1ObQB6hmVvRPCgPTRZM5NMH034VDM-1N-EWPRz2770K4/edit?hl=en_US)



# Events

- ▣ Louisville Infosec  
<http://www.louisvilleinfosec.com/>
- ▣ DerbyCon 2011, Louisville Ky  
<http://derbycon.com/>
- ▣ So many others  
<http://hack3rcon.org/>  
<http://skydogcon.com>  
<http://phreaknic.info>  
<http://notacon.org/>  
<http://www.outerz0ne.org/>



# QUESTIONS?

42

