LOCAL PASSWORD EXPLOITATION CLASS

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
- Regular on: http://www.isd-podcast.com/

What we plan to cover

- Pulling stored passwords from web browsers/IM clients and other apps
- Hash cracking of Windows passwords, as well as other systems
- Sniffing plain text passwords off the network
- How passwords on one box can be used to worm though other hosts on a network
- Hope it get's you thinking. Exploits are temporary, bad design decisions are forever.

Why exploit local passwords?

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

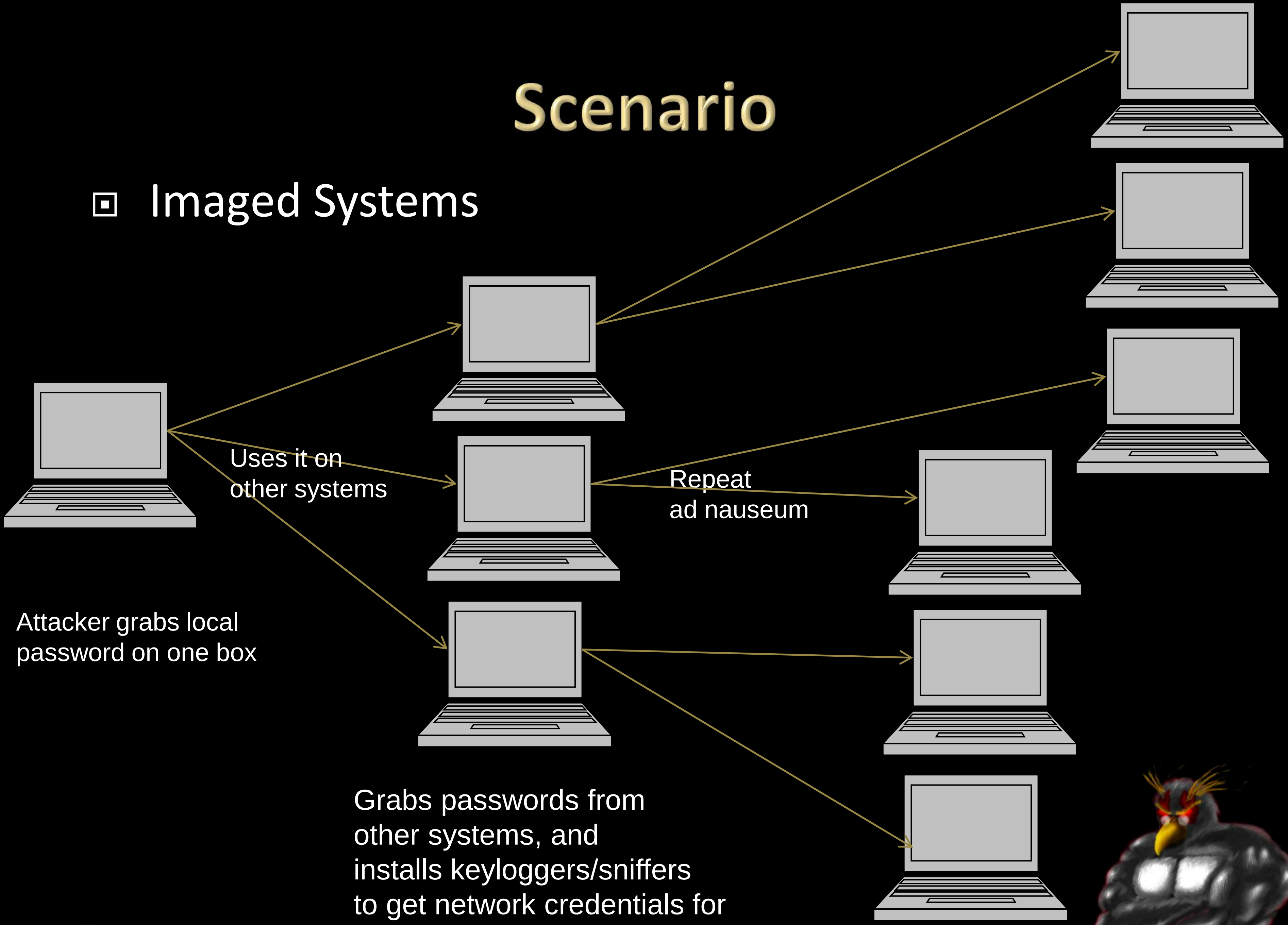
- To escalate privileges on the local host (install games, sniffers, key stroke catchers and other software or just to bypass restrictions).
- Local passwords can be used to gain access to other systems on the network. Admins may reuse the same usernames and passwords on other network hosts (more than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

WHOLE BUNCH OF NEEDED INFORMATION

Does not organize well, but you need to have these factoids in the back of your head for later.

Scenario

- Imaged Systems



Attacker grabs local password on one box

Uses it on other systems

Repeat ad nauseum

Grabs passwords from other systems, and installs keyloggers/sniffers to get network credentials for more systems

Methodology

Target Audience: Workstation Installers, System Admins, Security Folk and General Gear-heads.

Presentation Format:

1. Explain the background of the exploit.
2. Show the exploit.
3. Point the audience towards countermeasures, if there are specific ones.

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 know 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 know. Example: ROT13.

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

Hash Examples

Type	Hash
plaintext	badpass
MD2	9C5B091C305744F046E551DB45E7C036
MD4	640061BD33AA12D92FC40EA87EA408DE
MD5	F1BFC72887902986B95F3DFDF1B81A5B
SHA-1	AF73C586F66FDC99ABF1EADB2B71C5E46C80C24A
SHA-2 (256)	4F630A1C0C7DD182D2737456E14C89C723C5FCE25CAE39DA4B93F00E90A365CB
SHA-2 (384)	8E3B1BB56624C227996941E304B061FD864868AA3DB92A1C82AE00E336BE90809E60BB2A29FC1692189DE458B6300016
SHA-2 (512)	6109E5BDF21C7CC650DC211CF3A3706FAB8D50B132762F6D597BE1BD499E357FAF435FAB220FA40A1067707D0E0C28F39C1EC41F435C4D820E8AB225E37489E3
RIPEMD-160	595FD77AA71F1CE8D7A571CB6ABDA2A502BA00D4
LM	4CF3B1913C3FF376
NT	986CA892BEAB33D1FC2E60C22EC133B7
MySQL323	0AFDA7C85EE805C2
MySQLSHA1	229749C080B28D3AEFAB78279C4668E6E12F20FA
Cisco PIX	RtJk8qcKDPR.2D/E
VNC Hash	DAD3B1EB680AD902

Hash Example Demo

- As Aricon suggested: http://www.insidepro.com/hashes.php?lang=eng

- Cain http://www.oxid.it/cain.html

Great Resources

- Password Storage Locations For Popular Windows Applications
  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

Platforms Used

- Windows 7
  http://www.microsoft.com/
- Ubuntu
  http://www.ubuntu.com/
- Backtrack
  http://www.backtrack-linux.org/
- UBCD4Win
  http://www.ubcd4win.com

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\

Windows System Trifecta

- C:\Windows\System32\config
  SAM
  SYSTEM
  SECURITY
- Grab These Files!!!

Note on Anti-Virus

- It’s going to scream blood murder about these tools
- If running them on a system that may try to delete them you have a few options:

1. Disable real time protection
2. Ok them as the warnings pop up
3. Run from read only media like a CD-ROM
4. Run from the CD partition of a U3 thumbdrive

Getting file system access

- Pull the drive
- Use a boot CD
- Rely on weak permissions

Getting an account/changing an account password

- Do a hash insertion using chntpw http://home.eunet.no/pnordahl/ntpasswd/
- Konboot may be an option (Linux and Windows) http://www.piotrbania.com/all/kon-boot/
- Use Sala's Password Renew from UBCD4Win http://www.kood.org/windows-password-renew/
- Crack a password using one of the Techniques covered later
- If a password revealing tool only works while logged in to a given account, use a tool that does not on a different vector, then see if that password was reused
- Keyloggers

Demo: Boot CDs

Let’s get some file system access:

- UBCD4Win
  - Sala’s Password Renew
- BackTrack
  - SAMdump2

BROWSER PASSWORDS

IE, Firefox Etc.

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

Internet Explorer

- IE 4-6: Sport 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
- ChromePass
  http://www.nirsoft.net/utils/chromepass.html

Demo some web password revealers

- Cain
- PasswordFox
- IE Passview

RDP AND VNC

There is a “Remote Chance” we can get these passwords ☺

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

Remote Desktop Protocol (RDP)

- Apparently use to be saved in the .RDP file
- Now seems to be in the same place as Network Credentials

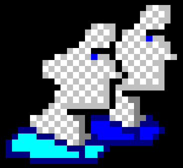
Demo: VNC and RDP

- Cain
  http://www.oxid.it/cain.html
- VNCPassView
  http://www.nirsoft.net/utils/vnc_password.html
- RDPV
  http://www.nirsoft.net/utils/remote_desktop_password.html
- NetPass
  http://www.nirsoft.net/utils/network_password_recovery.html

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
- 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/utils/mspass.html



MSN Messenger
Windows Messenger (In Windows XP)
Windows Live Messenger
Yahoo Messenger (Versions 5.x and 6.x)
Google Talk
ICQ Lite 4.x/5.x/2003
AOL Instant Messenger v4.6 or below, AIM 6.x, and AIM Pro.
Trillian
Miranda
GAIM/Pidgin
MySpace IM
PaltalkScene
Digsby

Demo

- MessenPass

STUPID WEB APP

Huh?

Why would you put the current user’s password in a form behind a bunch of asterisks?

AOA: ANY OLD ASTERISKS

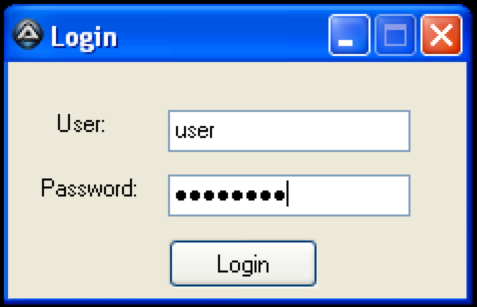
I’ll show you mine if you show me yours!

On screen, but behind a cover character

- Uses a Windows style for the control called ES_PASSWORD
- Not all apps use this to hide the characters, for example Windows User management tools, Firefox and some others

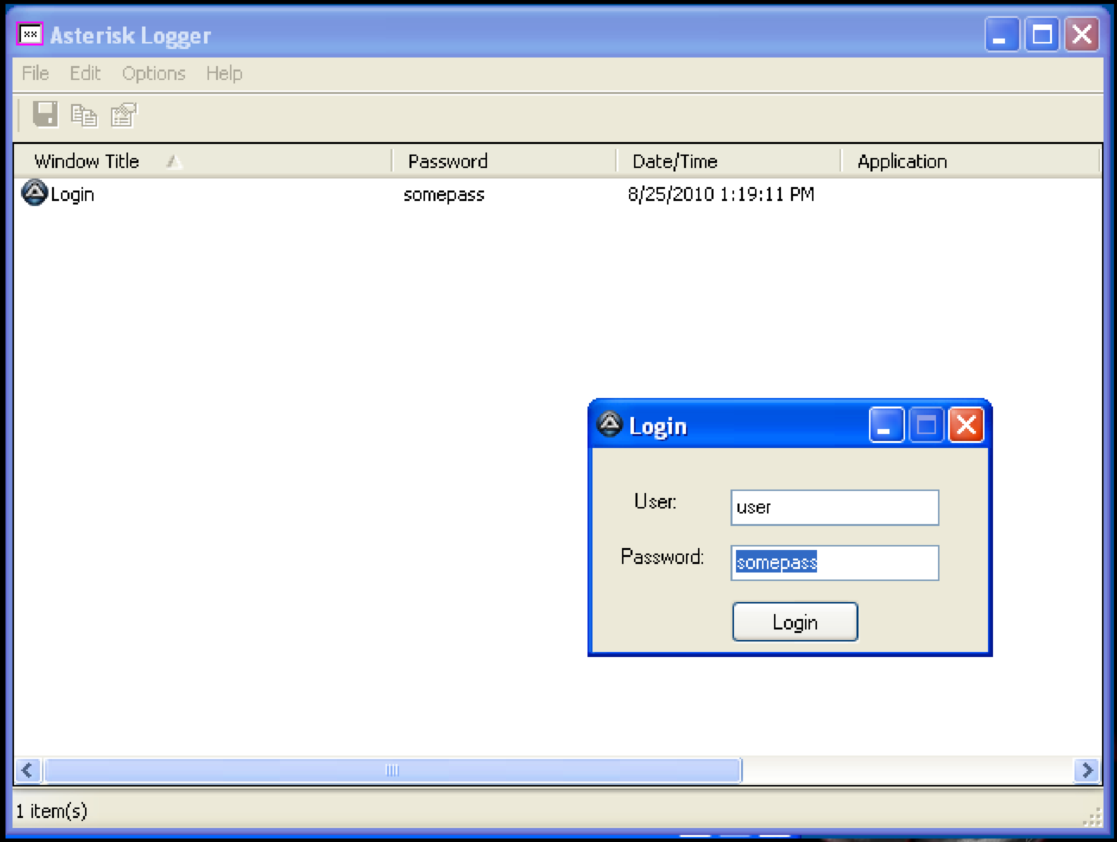
Your results may vary

- Asterisk Logger http://www.nirsoft.net/utils/astlog.html
- Worked in XP but not 7



User: user

Password: ●●●●●●●●●



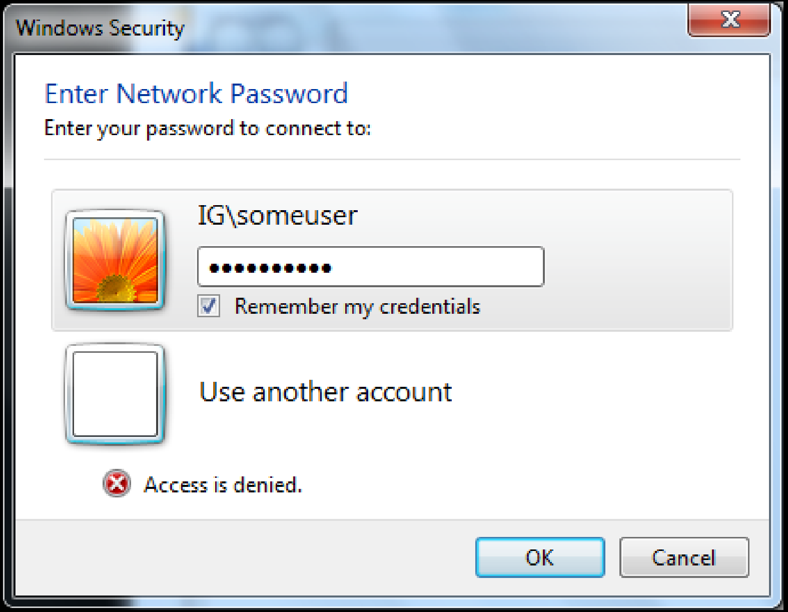
Window Title	Password	Date/Time	Application
Login	somepass	8/25/2010 1:19:11 PM	

1 item(s)

User: user

Password: somepass

NETWORK SHARES



Enter Network Password

Enter your password to connect to:

IG\someuser

●●●●●●●●●●●

☑ Remember my credentials

Use another account

Access is denied.

http://Irongeek.com

Network Shares

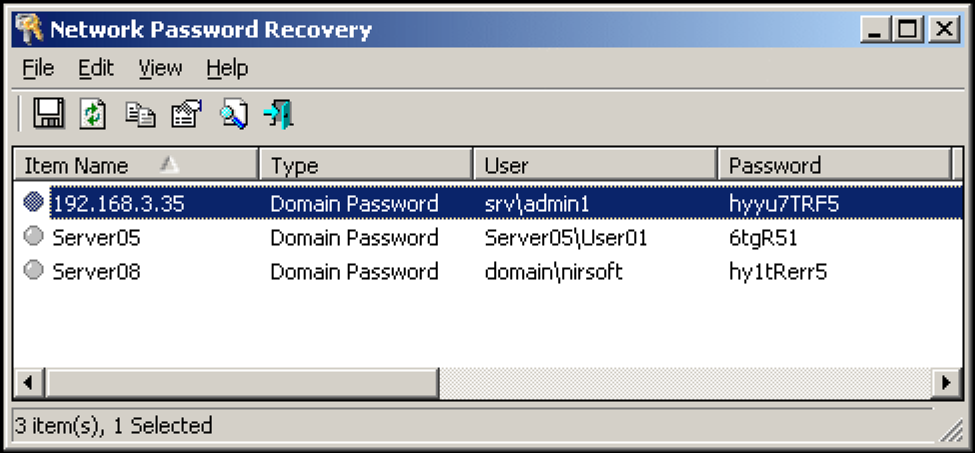
- Stored in:

- 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>

Demo: Network Password Recovery

- Network Password Recovery
  http://www.nirsoft.net/utils/network_password_recovery.html



Item Name	Type	User	Password
192.168.3.35	Domain Password	srv\admin1	hyyu7TRF5
Server05	Domain Password	Server05\User01	6tgR51
Server08	Domain Password	domain\nirsoft	hy1tRerr5

3 item(s), 1 Selected

OUTLOOK PST

Great hash collision example

Why find the password when you can cause a cache collision?

- Outlook PSTs uses CRC32 as the hash algorithm
- Unlike others, this one is simple to create a collisions for
- Any word that hashes to the same value is as good as the original password as far as Outlook is concerned

Demo: PST Password Recovery

- PSTPassword http://www.nirsoft.net/utils/pst_password.html

WIRELESS

Forget cracking it, just look it up!

Stored

- 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

Demo

- Show files in C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces
- Cain http://www.oxid.it/cain.html
- WirelessKeyView http://www.nirsoft.net/utils/wireless_key.html

SNIFFING THEM OFF THE WIRE

Your passwords smell funny

My favorite tools

- Wireshark
  http://www.wireshark.org/
- Cain
  http://www.oxid.it/cain.html
- Ettercap
  http://ettercap.sourceforge.net/
- NetworkMiner (Great for collecting files)
  http://networkminer.sourceforge.net/
- Most of the Linux tools will be on BackTrack Distro
  http://www.backtrack-linux.org/

Demo

- Wireshark
- Cain

WINDOWS

SAM I AM

Two types of hashes: 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.

Two types of hashes: 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 (Pwdump)
  http://www.foofus.net/~fizzgig/fgdump
- Cain
  http://www.oxid.it/cain.html
- Backtrack 4 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
samdump2
/media/sda1/Windows/System32/config/SYSTEM
/media/sda1/Windows/System32/config/SAM >hashes.txt
```

Demo: Simple Windows Hash Crack Example

- Using Cain again, just to make it simple

Time Memory Tradeoffs

RainbowCrack was designed to show off the faster time-memory trade-off technique. Since NT and LM hashes contain no salts, all possible hashes for a certain character set can be pre-generated. These pre-generated hashes (a Rainbow Table) can be loaded into memory and compared to the stored hash much quicker than generating each hash on the fly. You can make your own Rainbow Tables with the free tools that the Rainbow crack project provides, but that takes time. You can also buy pre-generated Rainbow Tables from them.

SAM Cracking Prevention

Practical Methods:

- Choose stronger local passwords. Use more than just alpha-numeric characters and perhaps throw in some extended ASCII characters by way of the Alt+num-pad method.
- Turn off LM Hash storage in the SAM via local policy, registry or GPO. http://support.microsoft.com/kb/q299656/
  On by default in Vista and after
- If you use a password longer than 14 characters no LM hash will be stored. Try using a pass phrase.
- Change local password frequently, then rely on domain passwords if possible.
- Don’t use the same local admin password on public and staff boxes.

Fascist Method (Not practical in most cases):

- Use the BIOS to disable booting from anything but the hard drive, put on a bios password and lock the case.
- Configure SysKey to require a password or a disk at boot time. (syskey.exe)

LINUX/UNIX

What stupid passwords lurk in the heart of the users? The Shadow Knows!!!

Parts of a *nix hash

- Pulled from Backtack 4 R1 /etc/passwd
  $6$GkfJ0/H/$IDtJEzDO1vh8VyDG5rnnLLMXwZl.cikulTg4wtXjq98Vlcf/PA2D1QsT7VHSsu46B/od4IJlqENMtc8dSpBEa1
- Blue part = Hash type
  Green= Salt
  Yellow = Resulting hash of password with given salt
- $1 = MD5 $2 = Blowfish
  $5 = SHA-256 $6 = SHA-512
- Helpful links:
  http://en.wikipedia.org/wiki/Crypt_%28Unix%29
  http://www.insidepro.com/eng/passwordspro.shtml

WINDOWS CACHED CREDS

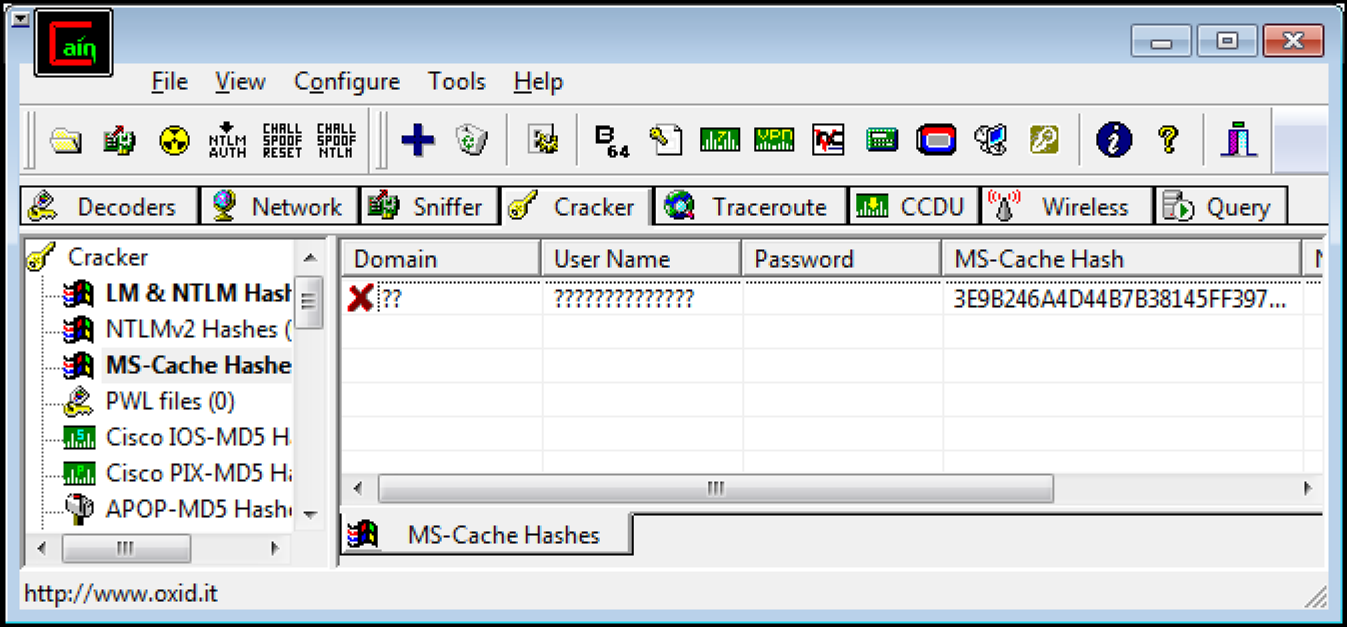
Stored Stuff

- 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 is:
  MD4(MD4(Unicode($pass)).Unicode(strtolower($username)))
  according to the folks at http://www.insidepro.com

Win 7 + Cain does not seem to work



Domain	User Name	Password	MS-Cache Hash
??	??????????????		3E9B246A4D44B7B38145FF397...

- Hashcat format:
  98bc149b523691e3e51a91b6596e9750:somedomainuser
  http://hashcat.net

Demo:Crack Cached Creds from SYSTEM and SECURITY hive

We will have to use the XP hives I’ve copied

- Cain
- Hashcat (May or may not show this)

Stored Stuff

- While these cached password are harder to crack than LM or NT hashes it’s not impossible.
- Arnaud Pilon and team created a tool for dumping the cached hashes called Cachedump. They have also provided patches for John the Ripper that allow you to crack the hashes.
- You can now also use Cain v2.68 or higher

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

Find out what’s doing what

System Process Monitoring Apps and Demo

- ProcessActivityView http://www.nirsoft.net/utils/process_activity_view.html

- RegFromApp http://www.nirsoft.net/utils/reg_file_from_application.html

- Procmon http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx

Don’t know how it’s hashed?

- 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?

OTHER WEIRD VECTORS

Think outside the login box ☺

Inverse Bruteforce
Using lack of originality to your advantage

1. You know someone out there has one of George Carlin “7 words”.
2. Less likely to trip account lock outs.

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

Look in the logs

- Did the user type the name in the wrong place?
  http://www.irongeek.com/i.php?page=security/pebkac-attack-passwords-in-logs

Events

- Shoecon, Sept 18, Atlanta GA http://www.shoecon.org/
- Louisville Infosec http://www.louisvilleinfosec.com/
- DerbyCon 2011, Louisville Ky http://derbycon.com/
- Phreaknic/Notacon/Outerz0ne http://phreaknic.info http://notacon.org/ http://www.outerz0ne.org/

QUESTIONS?

42