Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

gladiatx0r / Powerless Public

Notifications Fork 131 Star 473

Code Issues 1 Pull requests Actions Projects Security Insights

Files

04f553b

Go to file

Powerless.bat

README.md

Powerless / Powerless.bat

deus-ex-silicium added conditional for finding cacls executable 29d11c2 · 5 years ago History

Code Blame 247 lines (210 loc) · 12.4 KB Raw

```
@echo off
set userprofile=%cd%
mode con:cols=160 lines=9999
Cd c:\

echo ------ System Info (Use full output in conjunction with windows-exploit-suggester.
:: https://github.com/GDSSecurity/Windows-Exploit-Suggester
systeminfo
echo.

echo ----- Architecture -------
SET Processor
echo.

echo ------ Users and groups (check individual user with 'net user USERNAME' ) Check us
:: Note, in CTF boxes its not uncommon to see other low level users on the machine. It
echo Current User: %username%
whoami /all
echo --- All users, accounts and groups ---
net users
net accounts
net localgroup

echo ------- Administrators --------
net localgroup administrators

echo ------- Environment Variables -------
set
echo.

echo ------- Additional Drives (if not run as part of a batch job replace double percen
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
echo.

echo --------------------------------------- Search for Quick Wins ------------------
echo -------- Listing contents of user directories ---------
:: In CTF machines it is VERY common for there to be artifacts used for privilege escal
dir "C:\Users\" /a /b /s 2>nul | findstr /v /i "Favorites\\" | findstr /v /i "AppData\\
dir "C:\Documents and Settings\" /a /b /s 2>nul | findstr /v /i "Favorites\\" | findstr
echo.

echo -------- Exploring program directories and C:\ ---------
:: These directory listings are not recursive. They are meant to give you a general ove
echo --- Program Files ---
dir "C:\Program Files" /b
echo --- Program Files (x86) ---
dir "C:\Program Files (x86)" /b
echo --- Root of C:\ ----
dir "C:\" /b
echo.

echo --- Inetpub (any config files in here? May need to manually drill into this folder
:: The root web folder can at times be extensive, and thus we do not always want to sho
dir /a /b C:\inetpub\

echo --- Broad search for Apache or Xampp ---
dir /s /b apache* xampp*
dir /s /b apache* xampp*
echo.

echo ---Search for Configuration and sensitive files---
echo -- Broad search for config files --
:: If the .NET framework is installed you will get a bunch of config files which are ty
dir /s /b php.ini httpd.conf httpd-xampp.conf my.ini my.cnf web.config
echo -- Application Host File --
type C:\Windows\System32\inetsrv\config\applicationHost.config 2>nul
echo -- Broad search for unattend or sysprep files --
dir /b /s unattended.xml* sysprep.xml* sysprep.inf* unattend.xml*
echo -- Stored Passwords --
:: To use stored cmdkey credentials use runas with /savecred flag (e.g. runas /savecred
cmdkey /list
echo.

echo -- Checking for any accessible SAM or SYSTEM files --
dir %SYSTEMROOT%\repair\SAM 2>nul
dir %SYSTEMROOT%\System32\config\RegBack\SAM 2>nul
dir %SYSTEMROOT%\System32\config\SAM 2>nul
dir %SYSTEMROOT%\repair\system 2>nul
dir %SYSTEMROOT%\System32\config\SYSTEM 2>nul
dir %SYSTEMROOT%\System32\config\RegBack\system 2>nul
dir /a /b /s SAM.b*
echo.

echo -- Broad search for vnc kdbx or rdp files --
dir /a /s /b *.kdbx *vnc.ini *.rdp
echo.

echo --- Searching Registry for Passwords ---
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr
reg query HKLM /f password /t REG_SZ /s /k
reg query HKCU /f password /t REG_SZ /s /k
reg query "HKCU\Software\ORL\WinVNC3\Password"
reg query "HKLM\SYSTEM\Current\ControlSet\Services\SNMP"
reg query "HKCU\Software\SimonTatham\PuTTY\Sessions"
echo.

echo --- AlwaysInstallElevated Check ---
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated
echo.

echo --- Program Files and User Directories where everybody (or users) have full or mod
where /q icacls
IF ERRORLEVEL 1 (
    echo icacls is missing, performing checks using cacls for older versions of Windows
    FOR /F "tokens=* USEBACKQ" %%F IN (`where cacls`) DO (SET cacls_exe=%%F)
) ELSE (
    FOR /F "tokens=* USEBACKQ" %%F IN (`where icacls`) DO (SET cacls_exe=%%F)
)
%cacls_exe% "C:\Program Files\*" 2>nul | findstr "(F)" | findstr "Everyone"
%cacls_exe% "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr "Everyone"
%cacls_exe% "C:\Program Files\*" 2>nul | findstr "(F)" | findstr "BUILTIN\Users"
%cacls_exe% "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr "BUILTIN\Users"
%cacls_exe% "C:\Program Files\*" 2>nul | findstr "(M)" | findstr "Everyone"
%cacls_exe% "C:\Program Files (x86)\*" 2>nul | findstr "(M)" | findstr "Everyone"
%cacls_exe% "C:\Program Files\*" 2>nul | findstr "(M)" | findstr "BUILTIN\Users"
%cacls_exe% "C:\Program Files (x86)\*" 2>nul | findstr "(M)" | findstr "BUILTIN\Users"
%cacls_exe% "C:\Documents and Settings\*" 2>nul | findstr "(F)" | findstr "Everyone"
%cacls_exe% "C:\Documents and Settings\*" 2>nul | findstr "(M)" | findstr "Everyone"
```

```
REG QUERY "HKLM\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine" /v PowerShellVersion

echo ------- Network shares -------
net share

echo ------- Programs that run at startup ------
:: Note on some legacy Windows editions WMIC may fail to install/start/freeze in which
wmic startup get caption,command

echo -------- Path (is dll hijacking possible?) ------
echo Getting system + user path from command line (check permissions using cacls [path]
echo %path%
echo.
:: I couldnt find a way to only get system path in DOS (user path does not matter for t
:: https://github.com/ankh2054/windows-pentest/blob/master/Powershell/folderperms.ps1
:: powershell.exe -ExecutionPolicy Bypass -noLogo -Command "[Environment]::GetEnvironme
:: Or let the script do all the work for you
:: powershell.exe -executionpolicy bypass -file folderperm.ps1

echo ------- Scheduled Tasks Names Only -------
:: Look for any interesting/non-standard scheduled tasks, then view the scheduled task
schtasks /query /fo LIST 2>nul | findstr "TaskName"
echo.

echo ------- Scheduled Tasks Details (taskname, author, command run, run as user) -----
schtasks /query /fo LIST /v | findstr "TaskName Author: Run: User:"
echo.

echo ------- Services Currently Running (check for Windows Defender or Anti-virus) ----
net start
echo.

echo ------- Link Running Processes to started services --------
tasklist /SVC
```

```
echo.

echo ------- Processes verbose output (who is running what?) --------
:: Pay close attention to this list. Especially for those tasks run by a user other tha
tasklist /v
echo.

echo ------- Patches (also listed as part of systeminfo) -------
:: Note on some legacy Windows editions WMIC may fail to install/start/freeze in which 
:: Systeminfo may at times fail to list all patches (instead showing 'file x' or someth
wmic qfe get Caption,Description,HotFixID,InstalledOn

echo ------- Firewall ------
netsh firewall show state
netsh firewall show config
netsh advfirewall firewall dump

echo ------ Network information ------
ipconfig /all

:: Routing and ARP tables accessible with these commands... uncomment if you wish, I di
REM route print
REM arp -A
echo.

echo ------- Current connections and listening ports -------
:: Reverse port forward anything that is not accessible remotely, and run nmap on it. I
netstat -ano
echo.
echo ------- REVERSE PORT FORWARD MULTIPLE PORTS AT ONCE: plink.exe -l username -pw mys
echo.

echo --- Broad search for any possible config files which may contain passwords ---
:: The following broad config file and credential searches could result in many results
dir /s /b *pass* *cred* *vnc* *.config*
echo.

echo --- Starting broad search in the background for any files with the word password i
start /b findstr /sim password *.xml *.ini *.txt *.config *.bak 2>nul
echo.
```