Sign in

peass-ng / **PEASS-ng** Public

Notifications | Fork 3.1k | Star 16k

Code | Issues 22 | Pull requests 2 | Actions | Projects | Security | Insights

PEASS-ng / winPEAS / winPEASbat / **winPEAS.bat**

Executable File · 654 lines (594 loc) · 34.5 KB

Code | Blame | Raw

```
@ECHO OFF & SETLOCAL EnableDelayedExpansion
TITLE WinPEAS - Windows local Privilege Escalation Awesome Script
COLOR 0F
CALL :SetOnce

REM :: WinPEAS - Windows local Privilege Escalation Awesome Script
REM :: Code by carlospolop; Re-Write by ThisLimn0

REM Registry scan of other drives besides
REM /////true or false
SET long=false

:Splash
ECHO.
CALL :ColorLine "            %E%32m((,..,/((((((((((((((((((((/,  */%E%97m"
CALL :ColorLine "     %E%32m,/*,..*((((((((((((((((((((((((((((((((((,%E%97m"
CALL :ColorLine "   %E%32m,*/((((((((((((((((((/,  %E%92m.*//((//**,%E%32m .*((((((*%E%97m"
CALL :ColorLine "   %E%32m((((((((((((((((* %E%94m*****%E%32m,,,/########## %E%32m.(* ,((((((%E%97m
CALL :ColorLine "   %E%32m(((((((((((/* %E%94m******************%E%32m/####### %E%32m.(. ((((((%E%9
CALL :ColorLine "   %E%32m((((((.%E%92m.%E%94m******************%E%97m/@@@@@/%E%94m***%E%92m/######
CALL :ColorLine "   %E%32m,,.%E%92m.%E%94m**********************%E%97m@@@@@@@@@@(%E%94m***%E%92m,##
CALL :ColorLine "   %E%32m, ,%E%92m%E%94m**********************%E%97m#@@@@@#@@@@%E%94m*********%E%9
CALL :ColorLine "   %E%32m..((%E%92m(##########%E%94m*********%E%97m/#@@@@@@@@@/%E%94m*************
CALL :ColorLine "   %E%32m.((%E%92m(################(/%E%94m******%E%97m/@@@@@#%E%94m*************
CALL :ColorLine "   %E%32m.(%E%92m(########################(/%E%94m************************%E%32m..
CALL :ColorLine "   %E%32m.(%E%92m(##############################(/%E%94m********************%E%32m.
CALL :ColorLine "   %E%32m.(%E%92m(##################################(/%E%94m***************%E%32m.
CALL :ColorLine "   %E%32m.(%E%92m(######################################(%E%94m************%E%32m.
CALL :ColorLine "   %E%32m.(%E%92m(######(,.***.,(###################(..***(/%E%94m*********%E%32m.
CALL :ColorLine "   %E%32m.(%E%92m(######*(#####((##################((######/(%E%94m********%E%32m.
CALL :ColorLine "   %E%32m.(%E%92m(##################(/**********(################(%E%94m**%E%32m..
CALL :ColorLine "   %E%32m.((%E%92m(####################/*******(###################%E%32m.((((%E%9
CALL :ColorLine "   %E%32m.((((%E%92m(############################################/%E%32m  /((%E%97
CALL :ColorLine "   %E%32m..((((%E%92m(#########################################(%E%32m..(((((.%E%9
CALL :ColorLine "   %E%32m....((((%E%92m(#####################################(%E%32m .((((((.%E%97
CALL :ColorLine "   %E%32m.....((((%E%92m(##################################(%E%32m .(((((((.%E%97m
CALL :ColorLine "   %E%32m(((((((((. ,%E%92m(############################(%E%32m../(((((((((.%E%97m
CALL :ColorLine "       %E%32m((((((((/,  %E%92m,####################(%E%32m/..((((((((((.%E%97m"
CALL :ColorLine "             %E%32m(((((((((/,.  %E%92m,*//////*,.%E%32m ./(((((((((((.%E%97m"
CALL :ColorLine "                %E%32m(((((((((((((((((((((((((((/%E%97m"
ECHO.                       by carlospolop
ECHO.
ECHO.

:Advisory
REM // Increase progress in title by n percent
CALL :T_Progress 0
ECHO./^^!\ Advisory: WinPEAS - Windows local Privilege Escalation Awesome Script
CALL :ColorLine "   %E%41mWinPEAS should be used for authorized penetration testing and/or educatio
CALL :ColorLine "   %E%41mAny misuse of this software will not be the responsibility of the author
CALL :ColorLine "   %E%41mUse it at your own networks and/or with the network owner's permission.%E
ECHO.

:SystemInfo
CALL :ColorLine "%E%32m[*]%E%97m BASIC SYSTEM INFO
CALL :ColorLine " %E%33m[+]%E%97m WINDOWS OS"
ECHO.   [i] Check for vulnerabilities for the OS version with the applied patches
ECHO.   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#kernel
systeminfo
ECHO.
CALL :T_Progress 2

:ListHotFixes
wmic qfe get Caption,Description,HotFixID,InstalledOn | more
set expl=no
for /f "tokens=3-9" %%a in ('systeminfo') do (ECHO."%%a %%b %%c %%d %%e %%f %%g" | findstr /i "2000
IF "%expl%" == "yes" ECHO.   [i] Possible exploits (https://github.com/codingo/OSCP-2/blob/master/W
IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2592799"
IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS11-080 patch is NOT installed! (Vulns: XP/SP3,2K3/SP3-a
IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB3143141"
IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS16-032 patch is NOT installed! (Vulns: 2K8/SP1/2,Vista/
IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2393802"
```

```
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS11-011 patch is NOT installed! (Vulns: XP/SP2/3,2K3/SP2
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB982799"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-59 patch is NOT installed! (Vulns: 2K8,Vista,7/SP0-C
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB979683"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-21 patch is NOT installed! (Vulns: 2K/SP4,XP/SP2/3,2
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2305420"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-092 patch is NOT installed! (Vulns: 2K8/SP0/1/2,Vist
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB981957"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-073 patch is NOT installed! (Vulns: XP/SP2/3,2K3/SP2
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB4013081"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS17-017 patch is NOT installed! (Vulns: 2K8/SP2,Vista/SP
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB977165"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-015 patch is NOT installed! (Vulns: 2K,XP,2K3,2K8,Vi
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB941693"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS08-025 patch is NOT installed! (Vulns: 2K/SP4,XP/SP2,2K
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB920958"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS06-049 patch is NOT installed! (Vulns: 2K/SP4-ZwQuerySy
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB914389"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS06-030 patch is NOT installed! (Vulns: 2K,XP/SP2-Mrxsmb
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB908523"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS05-055 patch is NOT installed! (Vulns: 2K/SP4-APC Data-
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB890859"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS05-018 patch is NOT installed! (Vulns: 2K/SP3/4,XP/SP1/
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB842526"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS04-019 patch is NOT installed! (Vulns: 2K/SP2/3/4-Utili
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB835732"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS04-011 patch is NOT installed! (Vulns: 2K/SP2/3/4,XP/SP
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB841872"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS04-020 patch is NOT installed! (Vulns: 2K/SP4-POSIX)
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2975684"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS14-040 patch is NOT installed! (Vulns: 2K3/SP2,2K8/SP2,
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB3136041"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS16-016 patch is NOT installed! (Vulns: 2K8/SP1/2,Vista/
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB3057191"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS15-051 patch is NOT installed! (Vulns: 2K3/SP2,2K8/SP2,
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2989935"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS14-070 patch is NOT installed! (Vulns: 2K3/SP2-TCP/IP)
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2778930"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS13-005 patch is NOT installed! (Vulns: Vista,7,8,2008,2
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2850851"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS13-053 patch is NOT installed! (Vulns: 7SP0/SP1_x86-sch
    IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2870008"
    IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS13-081 patch is NOT installed! (Vulns: 7SP0/SP1_x86-tra
    ECHO.
    CALL :T_Progress 2
```

```
reg query HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v password 2>nul
CALL :T_Progress 2
ECHO.Looking inside HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\WinLogon
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr /i "DefaultD
CALL :T_Progress 2
ECHO.Looking inside HKLM\SYSTEM\CurrentControlSet\Services\SNMP
reg query HKLM\SYSTEM\CurrentControlSet\Services\SNMP /s 2>nul
CALL :T_Progress 2
ECHO.Looking inside HKCU\Software\TightVNC\Server
reg query HKCU\Software\TightVNC\Server 2>nul
CALL :T_Progress 2
ECHO.Looking inside HKCU\Software\SimonTatham\PuTTY\Sessions
reg query HKCU\Software\SimonTatham\PuTTY\Sessions /s 2>nul
CALL :T_Progress 2
ECHO.Looking inside HKCU\Software\OpenSSH\Agent\Keys
CALL :T_Progress 2
reg query HKCU\Software\OpenSSH\Agent\Keys /s 2>nul
cd %USERPROFILE% 2>nul && dir /s/b *password* == *credential* 2>nul
cd ..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..
dir /s/b /A:-D RDCMan.settings == *.rdg == SCClient.exe == *_history == .sudo_as_admin_successful =
cd inetpub 2>nul && (dir /s/b web.config == *.log & cd ..)
ECHO.
CALL :T_Progress 2

:ExtendedDriveScan
if "%long%" == "true" (
    CALL :ColorLine " %E%33m[+]%E%97m REGISTRY WITH STRING pass OR pwd"
        reg query HKLM /f passw /t REG_SZ /s
        reg query HKCU /f passw /t REG_SZ /s
        reg query HKLM /f pwd /t REG_SZ /s
        reg query HKCU /f pwd /t REG_SZ /s
        ECHO.
        ECHO.   [i] Iterating through the drives
        ECHO.
        for /f %%x in ('wmic logicaldisk get name^| more') do (
                set tdrive=%%x
                if "!tdrive:~1,2!" == ":" (
                        %%x
            CALL :ColorLine " %E%33m[+]%E%97m FILES THAT CONTAINS THE WORD PASSWORD WITH EXTENSION:
                findstr /s/n/m/i password *.xml *.ini *.txt *.cfg *.config 2>nul | findstr /v /i "\
            ECHO.
            CALL :ColorLine " %E%33m[+]%E%97m FILES WHOSE NAME CONTAINS THE WORD PASS CRED
            CALL :ColorLine " %E%33m[+]%E%97m FILES WHOSE NAME CONTAINS THE WORD PASS CRED or .conf
            dir /s/b *pass* == *cred* == *.config* == *.cfg 2>nul | findstr /v /i "\\windows\\"
            ECHO.
                )
        )
        CALL :T_Progress 2
) ELSE (
        CALL :T_Progress 2
)
TITLE WinPEAS - Windows local Privilege Escalation Awesome Script - Idle
ECHO.---
ECHO.Scan complete.
PAUSE >NUL
EXIT /B

:::-Subroutines

:SetOnce
REM :: ANSI escape character is set once below - for ColorLine Subroutine
SET "E=0x1B["
SET "PercentageTrack=0"
EXIT /B

:T_Progress
SET "Percentage=%~1"
SET /A "PercentageTrack=PercentageTrack+Percentage"
TITLE WinPEAS - Windows local Privilege Escalation Awesome Script - Scanning... !PercentageTrack!%%
EXIT /B

:ColorLine
SET "CurrentLine=%~1"
FOR /F "delims=" %%A IN ('FORFILES.EXE /P %~dp0 /M %~nx0 /C "CMD /C ECHO.!CurrentLine!"') DO ECHO.%
EXIT /B
```