






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

[Code](#) [Blame](#)

[Raw](#)   

```
1  @ECHO OFF & SETLOCAL EnableDelayedExpansion
2  TITLE WinPEAS - Windows local Privilege Escalation Awesome Script
3  COLOR 0F
4  CALL :SetOnce
5
6  REM :: WinPEAS - Windows local Privilege Escalation Awesome Script
7  REM :: Code by carlospolop; Re-Write by ThisLimn0
8
9  REM Registry scan of other drives besides
10 REM /////true or false
11 SET long=false
12
13 :Splash
14 ECHO.
15 CALL :ColorLine "          %E%32m(,.,/(
16 CALL :ColorLine "          %E%32m,/*,..*(
17 CALL :ColorLine " %E%32m,*/(
18 CALL :ColorLine " %E%32m(((
19 CALL :ColorLine " %E%32m(((
20 CALL :ColorLine " %E%32m(((
21 CALL :ColorLine " %E%32m,.,
22 CALL :ColorLine " %E%32m, ,
23 CALL :ColorLine " %E%32m..(
24 CALL :ColorLine " %E%32m.(
25 CALL :ColorLine " %E%32m.(
26 CALL :ColorLine " %E%32m.(
```

```
27 CALL :ColorLine " %E%32m.(%E%92m(#####(/%E%94m*****%E%32m.
28 CALL :ColorLine " %E%32m.(%E%92m(#####(/%E%94m*****%E%32m.
29 CALL :ColorLine " %E%32m.(%E%92m(#####(.**.,(#####(/%E%94m*****%E%32m.
30 CALL :ColorLine " %E%32m.(%E%92m(#####*#####(#####(/%E%94m*****%E%32m.
31 CALL :ColorLine " %E%32m.(%E%92m(#####(/*****#####(%E%94m**%E%32m.
32 CALL :ColorLine " %E%32m.(%E%92m(#####/*****#####%E%32m.(((%E%9
33 CALL :ColorLine " %E%32m.(((%E%92m(#####/%E%32m /((%E%97
34 CALL :ColorLine " %E%32m..(((%E%92m(#####(%E%32m..(((.%E%9
35 CALL :ColorLine " %E%32m...(((%E%92m(#####(%E%32m .((((.%E%97
36 CALL :ColorLine " %E%32m.....(((%E%92m(#####(%E%32m .((((((.%E%97n
37 CALL :ColorLine " %E%32m((((((((.,%E%92m(#####(%E%32m./((((((((.%E%97n
38 CALL :ColorLine " %E%32m(((((((((/, %E%92m,#####(%E%32m/..((((((((.%E%97m"
39 CALL :ColorLine " %E%32m(((((((((/, %E%92m,*/////*,%E%32m ./((((((((.%E%97m"
40 CALL :ColorLine " %E%32m(((((((((((((((((((((((((/%E%97m"
41 ECHO. by carlospolop
42 ECHO.
43 ECHO.
44
45 :Advisory
46 REM // Increase progress in title by n percent
47 CALL :T_Progress 0
48 ECHO./^^!\ Advisory: WinPEAS - Windows local Privilege Escalation Awesome Script
49 CALL :ColorLine " %E%41mWinPEAS should be used for authorized penetration testing and/or education
50 CALL :ColorLine " %E%41mAny misuse of this software will not be the responsibility of the author
51 CALL :ColorLine " %E%41mUse it at your own networks and/or with the network owner's permission.%E
52 ECHO.
53
54 :SystemInfo
55 CALL :ColorLine "%E%32m[*]%E%97m BASIC SYSTEM INFO
56 CALL :ColorLine " %E%33m[+]%E%97m WINDOWS OS"
57 ECHO. [i] Check for vulnerabilities for the OS version with the applied patches
58 ECHO. [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#kernel
59 systeminfo
60 ECHO.
61 CALL :T_Progress 2
62
63 :ListHotFixes
64 wmic qfe get Caption,Description,HotFixID,InstalledOn | more
65 set expl=no
66 for /f "tokens=3-9" %a in ('systeminfo') do (ECHO."%a %b %c %d %e %f %g" | findstr /i "2006
67 IF "%expl%" == "yes" ECHO. [i] Possible exploits (https://github.com/codingo/OSCP-2/blob/master/w
68 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2592799"
69 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS11-080 patch is NOT installed! (Vulns: XP/SP3,2K3/SP3-a
70 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB3143141"
71 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS16-032 patch is NOT installed! (Vulns: 2K8/SP1/2,Vista/
72 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2393802"
```

```
73 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS11-011 patch is NOT installed! (Vulns: XP/SP2/3,2K3/SP2
74 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB982799"
75 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-59 patch is NOT installed! (Vulns: 2K8,Vista,7/SP0-C
76 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB979683"
77 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-21 patch is NOT installed! (Vulns: 2K/SP4,XP/SP2/3,2
78 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2305420"
79 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-092 patch is NOT installed! (Vulns: 2K8/SP0/1/2,Vist
80 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB981957"
81 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-073 patch is NOT installed! (Vulns: XP/SP2/3,2K3/SP2
82 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB4013081"
83 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS17-017 patch is NOT installed! (Vulns: 2K8/SP2,Vista/SP
84 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB977165"
85 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-015 patch is NOT installed! (Vulns: 2K,XP,2K3,2K8,Vi
86 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB941693"
87 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS08-025 patch is NOT installed! (Vulns: 2K/SP4,XP/SP2,2K
88 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB920958"
89 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS06-049 patch is NOT installed! (Vulns: 2K/SP4-ZwQuerySy
90 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB914389"
91 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS06-030 patch is NOT installed! (Vulns: 2K,XP/SP2-Mrxsmb
92 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB908523"
93 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS05-055 patch is NOT installed! (Vulns: 2K/SP4-APC Data-
94 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB890859"
95 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS05-018 patch is NOT installed! (Vulns: 2K/SP3/4,XP/SP1/
96 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB842526"
97 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS04-019 patch is NOT installed! (Vulns: 2K/SP2/3/4-Utili
98 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB835732"
99 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS04-011 patch is NOT installed! (Vulns: 2K/SP2/3/4,XP/SP
100 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB841872"
101 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS04-020 patch is NOT installed! (Vulns: 2K/SP4-POSIX)
102 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2975684"
103 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS14-040 patch is NOT installed! (Vulns: 2K3/SP2,2K8/SP2,
104 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB3136041"
105 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS16-016 patch is NOT installed! (Vulns: 2K8/SP1/2,Vista/
106 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB3057191"
107 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS15-051 patch is NOT installed! (Vulns: 2K3/SP2,2K8/SP2,
108 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2989935"
109 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS14-070 patch is NOT installed! (Vulns: 2K3/SP2-TCP/IP)
110 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2778930"
111 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS13-005 patch is NOT installed! (Vulns: Vista,7,8,2008,2
112 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2850851"
113 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS13-053 patch is NOT installed! (Vulns: 7SP0/SP1_x86-sch
114 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB2870008"
115 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS13-081 patch is NOT installed! (Vulns: 7SP0/SP1_x86-tra
116 ECHO.
117 CALL :T_Progress 2
118
```

110


```
581     reg query HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v password 2>nul
582     CALL :T_Progress 2
583     ECHO.Looking inside HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\WinLogon
584     reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr /i "Default
585     CALL :T_Progress 2
586     ECHO.Looking inside HKLM\SYSTEM\CurrentControlSet\Services\SNMP
587     reg query HKLM\SYSTEM\CurrentControlSet\Services\SNMP /s 2>nul
588     CALL :T_Progress 2
589     ECHO.Looking inside HKCU\Software\TightVNC\Server
590     reg query HKCU\Software\TightVNC\Server 2>nul
591     CALL :T_Progress 2
592     ECHO.Looking inside HKCU\Software\SimonTatham\PuTTY\Sessions
593     reg query HKCU\Software\SimonTatham\PuTTY\Sessions /s 2>nul
594     CALL :T_Progress 2
595     ECHO.Looking inside HKCU\Software\OpenSSH\Agent\Keys
596     CALL :T_Progress 2
597     reg query HKCU\Software\OpenSSH\Agent\Keys /s 2>nul
598     cd %USERPROFILE% 2>nul && dir /s/b *password* == *credential* 2>nul
599     cd ..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\
600     dir /s/b /A:-D RDCMan.settings == *.rdg == SCClient.exe == *_history == .sudo_as_admin_successful =
601     cd inetpub 2>nul && (dir /s/b web.config == *.log & cd ..)
602     ECHO.
603     CALL :T_Progress 2
604
605     :ExtendedDriveScan
606     if "%long%" == "true" (
607         CALL :ColorLine " %E%33m[+]%E%97m REGISTRY WITH STRING pass OR pwd"
608         reg query HKLM /f passw /t REG_SZ /s
609         reg query HKCU /f passw /t REG_SZ /s
610         reg query HKLM /f pwd /t REG_SZ /s
611         reg query HKCU /f pwd /t REG_SZ /s
612         ECHO.
613         ECHO. [i] Iterating through the drives
614         ECHO.
615         for /f %x in ('wmic logicaldisk get name^| more') do (
616             set tdrive=%x
617             if "!tdrive:~1,2!" == ":" (
618                 %%x
619                 CALL :ColorLine " %E%33m[+]%E%97m FILES THAT CONTAINS THE WORD PASSWORD WITH EXTENSION:
620                 findstr /s/n/m/i password *.xml *.ini *.txt *.cfg *.config 2>nul | findstr /v /i "\
621         ECHO.
622         CALL :ColorLine " %E%33m[+]%E%97m FILES WHOSE NAME CONTAINS THE WORD PASS OR PWD"
```

```
622             CALL :ColorLine " %E%33m[+]%E%9/m FILES WHOSE NAME CONTAINS THE WORD PASS CRED OR .CON
623             dir /s/b *pass* == *cred* == *.config* == *.cfg 2>nul | findstr /v /i "\\windows\\"
624             ECHO.
625             )
626         )
627         CALL :T_Progress 2
628     ) ELSE (
629         CALL :T_Progress 2
630     )
631     TITLE WinPEAS - Windows local Privilege Escalation Awesome Script - Idle
632     ECHO.---
633     ECHO.Scan complete.
634     PAUSE >NUL
635     EXIT /B
636
637     :::Subroutines
638
639     :SetOnce
640     REM :: ANSI escape character is set once below - for ColorLine Subroutine
641     SET "E=0x1B["
642     SET "PercentageTrack=0"
643     EXIT /B
644
645     :T_Progress
646     SET "Percentage=%~1"
647     SET /A "PercentageTrack=PercentageTrack+Percentage"
648     TITLE WinPEAS - Windows local Privilege Escalation Awesome Script - Scanning... !PercentageTrack!%%
649     EXIT /B
650
651     :ColorLine
652     SET "CurrentLine=%~1"
653     FOR /F "delims=" %%A IN ('FORFILES.EXE /P %~dp0 /M %~nx0 /C "CMD /C ECHO.!CurrentLine!'"') DO ECHO.%%
654     EXIT /B
```