





 [Product](#) [Solutions](#) [Resources](#) [Open Source](#) [Enterprise](#) [Pricing](#)










[Sign in](#)

[Sign up](#)

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

 Sponsor  Notifications  Fork 3.1k  Star 16k

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

Files

fa0f2e1

Go to file

> .github

> build_lists

> linPEAS

> metasploit

> parsers

> winPEAS

> winPEASbat

.gitattributes

README.md

winPEAS.bat

> winPEASexe

README.md

.gitignore

CONTRIBUTING.md

LICENSE

README.md

TODO.md

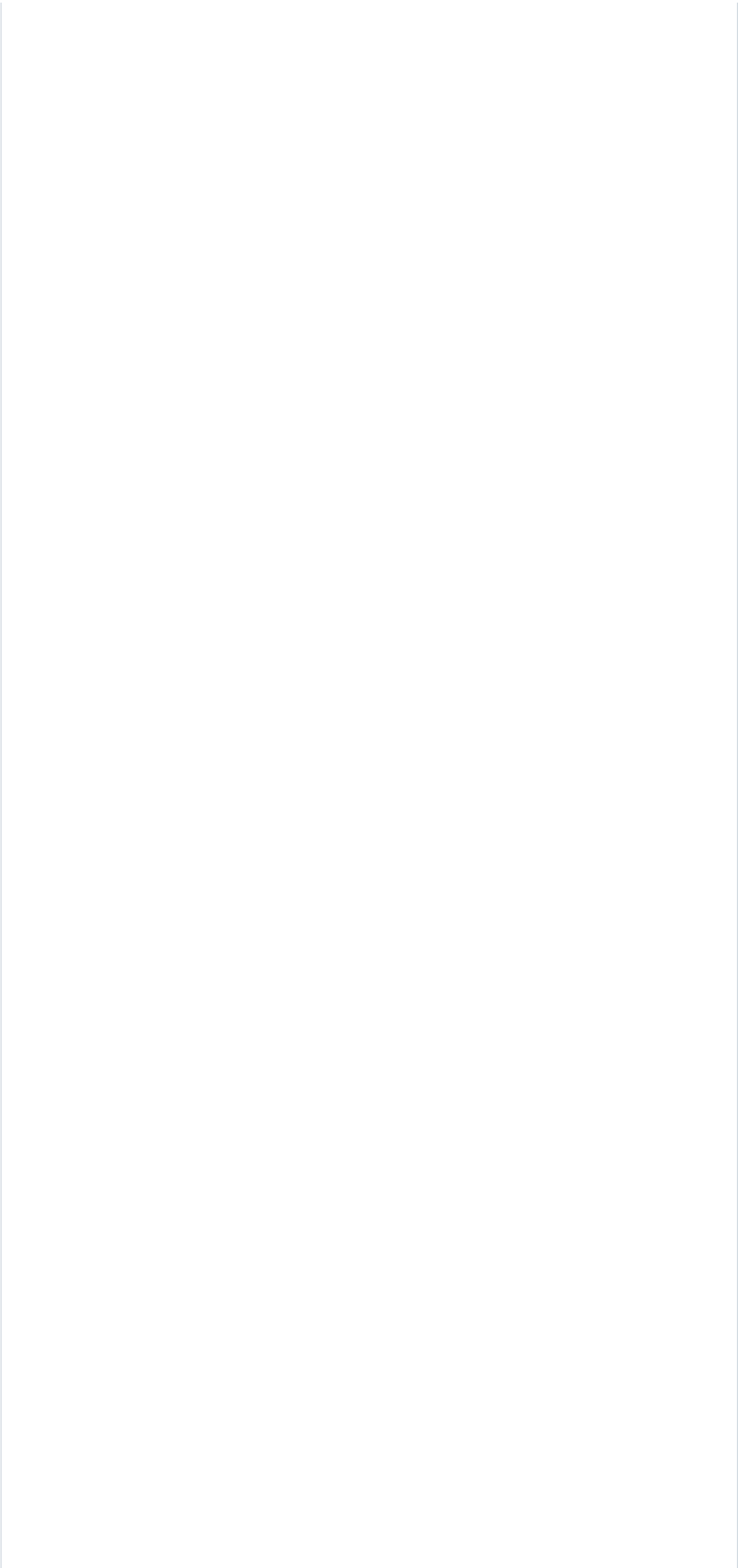
PEASS-ng / winPEAS / winPEASbat / winPEAS.bat

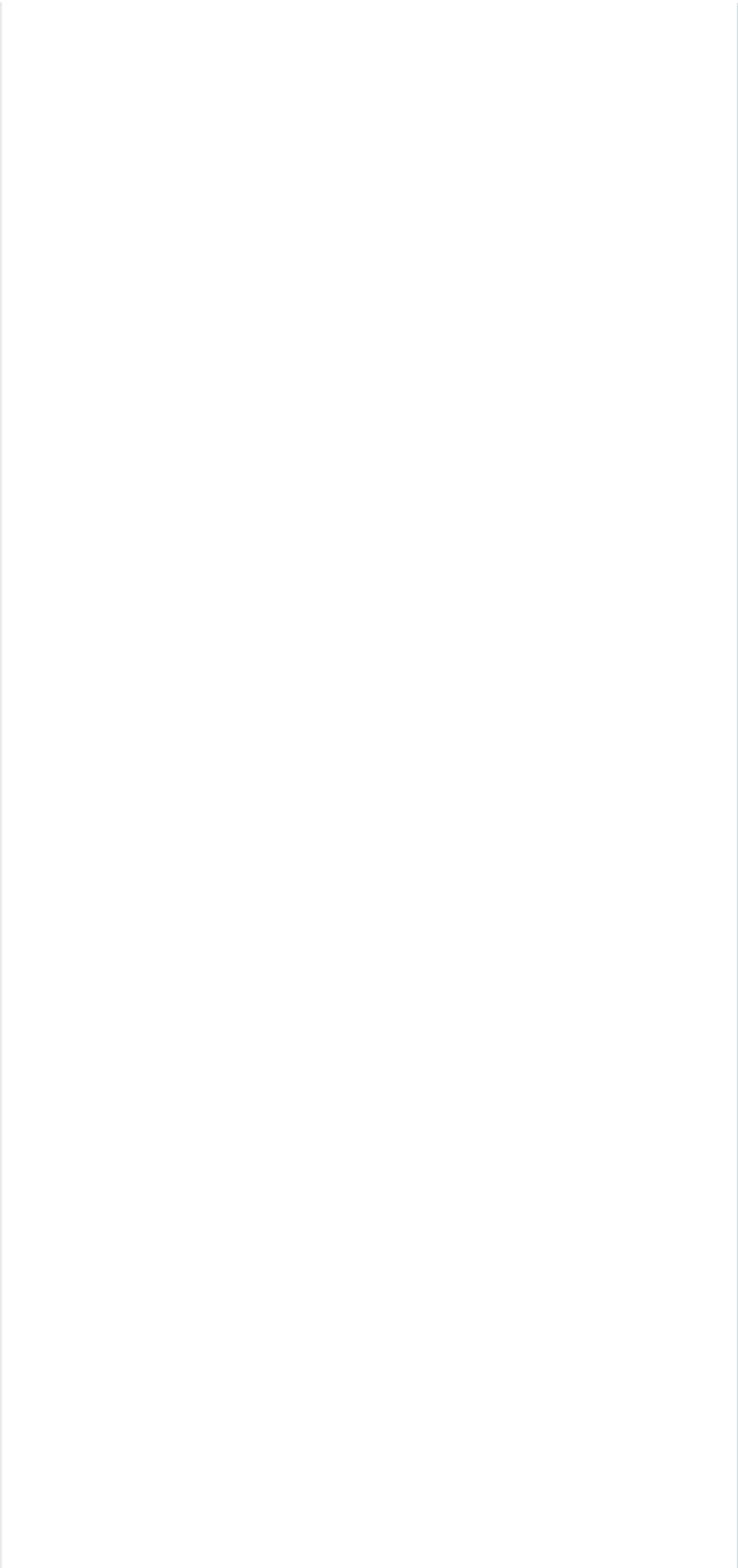
carlospolop change url 585fcc3 · 2 years ago History

Code Blame Executable File · 654 lines (594 loc) · 34.5 KB Raw Copy Download Toggle

```
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(.,./(((((((((((((((((((((((, */E%97m"
16 CALL :ColorLine " %E%32m,/*,..*((((((((((((((((((((((((((((((((((((((((,E%97m"
17 CALL :ColorLine " %E%32m,*/((((((((((((((((((((((((, %E%92m.*//(**,%E%32m .*(((((*E%
18 CALL :ColorLine " %E%32m((((((((((((((((((( * %E%94m*****E%32m,,/##### %E%32m.( * ,
19 CALL :ColorLine " %E%32m(((((((((((((((/ * %E%94m*****E%32m/##### %E%32m.(
20 CALL :ColorLine " %E%32m(((((.%E%92m.%E%94m*****E%97m/@@@@/%E%94m***
21 CALL :ColorLine " %E%32m,,.%E%92m.%E%94m*****E%97m@@@@@@@@@/%E%94m
22 CALL :ColorLine " %E%32m, ,.%E%92m.%E%94m*****E%97m#@#@#@#@#/%E%94m*
23 CALL :ColorLine " %E%32m..(%E%92m(#####E%94m*****E%97m/#@@@@@@@@/%E%94m*
24 CALL :ColorLine " %E%32m.( (%E%92m(#####(/%E%94m*****E%97m/@#@#@#/%E%94m*
25 CALL :ColorLine " %E%32m.(%E%92m(#####(/%E%94m*****
26 CALL :ColorLine " %E%32m.(%E%92m(#####(/%E%94m*****
27 CALL :ColorLine " %E%32m.(%E%92m(#####(/%E%94m*****
28 CALL :ColorLine " %E%32m.(%E%92m(#####(%E%94m*****
29 CALL :ColorLine " %E%32m.(%E%92m(#####(. ***(, #####( ..***(/%E%94m***
30 CALL :ColorLine " %E%32m.(%E%92m(#####(#####(#####(#####(/%E%94m***
31 CALL :ColorLine " %E%32m.(%E%92m(#####(*****(#####(#####(%E%9
32 CALL :ColorLine " %E%32m.( (%E%92m(#####(*****(#####(#####E%
33 CALL :ColorLine " %E%32m.((( (%E%92m(#####(#####/%E%3
34 CALL :ColorLine " %E%32m..((( (%E%92m(#####(#####(%E%32m
35 CALL :ColorLine " %E%32m...((( (%E%92m(#####(#####(%E%32m .
36 CALL :ColorLine " %E%32m.....((( (%E%92m(#####(#####(%E%32m .((
37 CALL :ColorLine " %E%32m(((((((. ,%E%92m(#####(#####(%E%32m../(((
38 CALL :ColorLine " %E%32m(((((((/, %E%92m,#####(#####(%E%32m../((((
39 CALL :ColorLine " %E%32m(((((((/, . %E%92m,*/////*,%E%32m ./(((((((
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
50 CALL :ColorLine " %E%41mAny misuse of this software will not be the responsibility of
51 CALL :ColorLine " %E%41mUse it at your own networks and/or with the network owner's p
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. [! Check for vulnerabilities for the OS version with the applied patches
```

```
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-escal
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" | find
67 IF "%expl%" == "yes" ECHO. [i] Possible exploits (https://github.com/codingo/OSCP-2/b
68 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
69 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS11-080 patch is NOT installed! (Vulns: XP/S
70 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
71 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS16-032 patch is NOT installed! (Vulns: 2K8/
72 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
73 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS11-011 patch is NOT installed! (Vulns: XP/S
74 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
75 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-59 patch is NOT installed! (Vulns: 2K8,V
76 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
77 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-21 patch is NOT installed! (Vulns: 2K/SP
78 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
79 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-092 patch is NOT installed! (Vulns: 2K8/
80 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
81 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-073 patch is NOT installed! (Vulns: XP/S
82 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
83 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS17-017 patch is NOT installed! (Vulns: 2K8/
84 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
85 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS10-015 patch is NOT installed! (Vulns: 2K,X
86 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
87 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS08-025 patch is NOT installed! (Vulns: 2K/S
88 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
89 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS06-049 patch is NOT installed! (Vulns: 2K/S
90 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
91 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS06-030 patch is NOT installed! (Vulns: 2K,X
92 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
93 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS05-055 patch is NOT installed! (Vulns: 2K/S
94 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
95 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS05-018 patch is NOT installed! (Vulns: 2K/S
96 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
97 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS04-019 patch is NOT installed! (Vulns: 2K/S
98 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
99 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS04-011 patch is NOT installed! (Vulns: 2K/S
100 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
101 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS04-020 patch is NOT installed! (Vulns: 2K/S
102 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
103 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS14-040 patch is NOT installed! (Vulns: 2K3/
104 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
105 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS16-016 patch is NOT installed! (Vulns: 2K8/
106 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
107 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS15-051 patch is NOT installed! (Vulns: 2K3/
108 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
109 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS14-070 patch is NOT installed! (Vulns: 2K3/
110 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
111 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS13-005 patch is NOT installed! (Vulns: Vist
112 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
113 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS13-053 patch is NOT installed! (Vulns: 7SP0
114 IF "%expl%" == "yes" wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C
115 IF "%expl%" == "yes" IF errorlevel 1 ECHO.MS13-081 patch is NOT installed! (Vulns: 7SP0
116 ECHO.
117 CALL :T_Progress 2
118
```




```

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
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_
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 WIT
620             findstr /s/n/m/i password *.xml *.ini *.txt *.cfg *.config 2>nul | find
621             ECHO.
622             CALL :ColorLine " %E%33m[%E%97m FILES WHOSE NAME CONTAINS THE WORD PASS C
623             dir /s/b *pass* == *cred* == *.config* == *.cfg 2>nul | findstr /v /i "\\wi
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... !Perce
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!"

```

654 **EXIT** /B