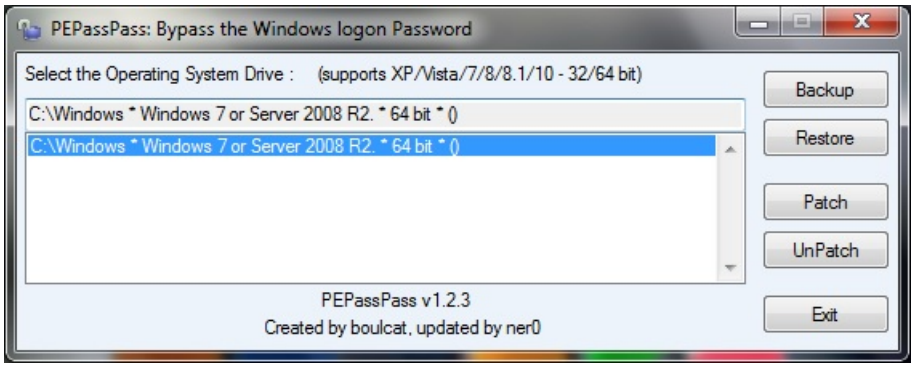
PEPassPass



PEPassPass is developed from Holmes.Sherlock's **PassPass** (Bypass the Password).

PassPass is a nifty Grub4DOS (BIOS) batch script **to disable/re-enable Windows logon password validation.**

PEPassPass is an AutoIt executable to disable/re-enable Windows logon password validation, too.

It is intended to be run from either Windows PE or from a second NT installation, if any, to patch the first one.

A possible use case is systems equipped with UEFI where Grub4DOS may fail to boot.

For such systems, one needs to boot either Grub4DOS, hence PassPass in Legacy/BIOS compatible mode, or Windows PE/second NT installation to boot PEPassPass from.

In short, an addition to the original PassPass, really much faster if Grub4Dos is available. 1.Boot to grub4dos, 2.Patch the file, 3.Continue booting your patched Windows OS.

PEPassPass is able to patch Windows XP/Vista/7/8/8.1 for both 32-bit and 64-bit versions.

Technical Details :

The script tries to locate all existing Windows installations and corresponding Windows editions as well.

Thereafter, after changing permissions, it replaces the CMP instruction responsible for password verification with a 'benign' sequence of bytes.

For reverting back the changes, the process is just the opposite.

The whole idea is derived from **WindowsGate** and **Astr0baby's tutorial**

Usage :

PEPassPass.exe : Displays the GUI, Select the OS drive and use buttons, Backup, Restore, Patch or UnPatch.
PEPassPass.exe /Source : Extract the embedded source in same folder.

Test :

1.Download latest version and include in your WinPE, BIOS and/or UEFI.

2.Backup `/<Windows directory>/system32/msv1_0.dll` of a target installation protected by password at logon.

(Backup **msv1_0.dll** For **Windows XP, Vista, 7, 8, 8.1** and **NtlmShared.dll** For **Windows 10,11**)

Backup file: `/<Windows directory>/system32/msv1_0.dll.bak`

3.Patch it. The Backup file: `/<Windows directory>/system32/msv1_0.dll.bak` is created if not exist,Backup not done.

4.Test whether the patch is working by being able to log on with arbitrary password or without password.

5.Unpatch it.

6.Test whether unpatch is working by being not able to log in with all but only with the correct password.

AutoIt Version : 3.3.14.2

Author : boulcat

Credit for PassPass:

Holmes.Sherlock - For Original PassPass (Bypass the Password), a nifty Grub4DOS batch script to disable/re-enable Windows logon password validation.

Credit for PEPassPass:

Wonko the sane - For ideas, code snippets, information. The script embeds his DLL version detection script.

Ectomorph a.k.a. Damian Bakowski - For his 'unannounced' patch for **32-bit** version of **msv1_0.dll**.

Astr0baby - For his reversing tutorial.

Steve Si – For including support for PassPass in his wonderful tool Easy2Boot.

ner0 – For adding support for Windows 10 / Server 2016-2019.

License :

This program is distributed as freeware in the hope that it will be usefull but without any warrenty expressed or implied.

You are free to modify this script but I would appreciate if you shared your changes with me and include the source code in the program, as it is done.

Take credit for your fixes, improvements but thanks to don't take credit for work you did not do.

Changelog :

v1.2.3 - 12/08/2021 - Fixed support for **Windows 10 1809 / Server 2019**.

v1.2.2 - 07/08/2021 - Reverse engineered MsvpPasswordValidate function to add support for latest versions of **Windows 10**.

v1.2.1 - 06/12/2016 - Fixed an issue with the compiled version.

v1.2.0 - 27/11/2016 - Added **Windows 10** support, using **NtlmShared.dll**.

v1.1.0 - 18/09/2014 - Browse all the folders from the drive and search if **System32\msv1_0.dll** exist to get the "**Windows**" folder. Use the values of the combo rather than looking again at OSVersion and OSArch.

v1.0.3 - 17/09/2014 - Add Permissions on **msv1_0.dll** and exclude the **X:** drive reserved for WinPE.

v1.0.2 - 16/09/2014 - Test OSArch **32** or **64** bit from winlogon.exe

v1.0.0 - 16/09/2014 - Initial Release

Sources :

PassPass : **http://reboot.pro/index.php?showtopic=18588**

PEPassPass : **http://reboot.pro/index.php?showtopic=20045**

PassPassLive : **http://reboot.pro/index.php?showtopic=19499**