Defcon DSE Bypass workshop – Virtual Machine setup instruction

CSABA FITZL

Table of Contents

Setting up the testing environment

We will need two / three different virtual machines. You may use any virtualization software, but the instructor will use VMware. The software must have snapshot capabilities. You must be familiar using your own environment and have admin rights to do any changes if required. You can get a 30 day trial version of VMware from:
https://my.vmware.com/web/vmware/downloads
The VMs should be set up the following way:

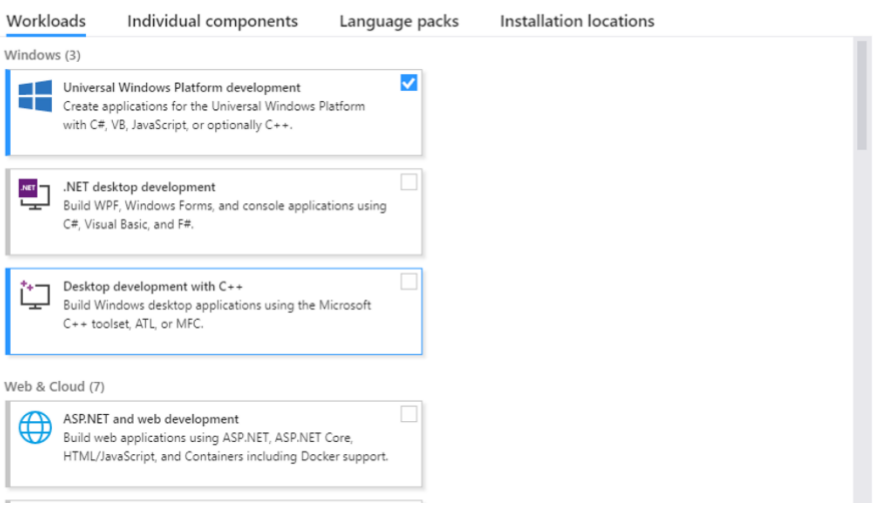
Windows 10 x64

Once installing a Windows 10 x64 version, we need to install the following software:

1. Windows 10 ISO can be downloaded from: https://www.microsoft.com/hu-hu/software-download/windows10ISO
    a. SHA1 hash: 08FBB24627FA768F869C09F44C5D6C1E53A57A6F, Filename: Win10_1803_English_x64.iso
    b. Also known as "en_windows_10_consumer_editions_version_1803_updated_march_2018_x64_dvd_12063379.iso"
2. Visual Studio 2017 Community, available from: https://www.visualstudio.com/downloads/
3. Windows Driver Kit 10, available from: https://go.microsoft.com/fwlink/?linkid=873060
4. Windows Driver Kit 8.1 Update 1, available from: https://www.microsoft.com/en-us/download/details.aspx?id=42273
5. Windows Driver Kit 8, available from: https://go.microsoft.com/fwlink/p/?LinkID=324284
6. Python 2.7.15 x64, available from: https://www.python.org/ftp/python/2.7.15/python-2.7.15.amd64.msi
7. VMWare tools (or other equivalent)
8. WinDBG Preview from the Microsoft Store (optional as the previous ones will install standard WinDBG)
9. If your software supports add a virtual TPM module to the VM, VMware:
    a. Encrypt the VM
    b. https://docs.vmware.com/en/VMware-Workstation-Pro/14.0/com.vmware.ws.using.doc/GUID-6E166EDC-BF27-438D-BA98-CF216A850ACE.html
    c. https://docs.vmware.com/en/VMware-Fusion/10.0/com.vmware.fusion.using.doc/GUID-4EC58A68-BE9E-42F6-B005-4BB63AE5D85B.html
10. Enable BitLocker and **save the recovery key outside the VM**
    a. In case virtual TPM is not supported: https://answers.microsoft.com/en-us/windows/forum/windows_8-security/allow-bitlocker-without-compatible-tmp-module/4c0623b5-70f4-4953-bde4-34ef18045e4f

Installation notes:

1. Install Visual Studio with the below options checked in as minimum:



Workloads | Individual components | Language packs | Installation locations

Windows (3)

☑ Universal Windows Platform development
Create applications for the Universal Windows Platform with C#, VB, JavaScript, or optionally C++.

□ .NET desktop development
Build WPF, Windows Forms, and console applications using C#, Visual Basic, and F#.

□ Desktop development with C++
Build Windows desktop applications using the Microsoft C++ toolset, ATL, or MFC.

Web & Cloud (7)

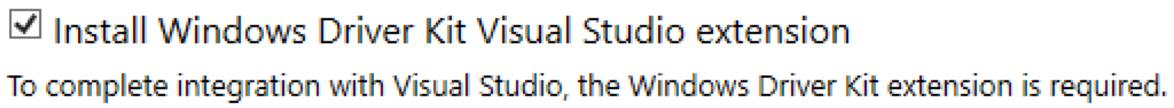
□ ASP.NET and web development
Build web applications using ASP.NET, ASP.NET Core, HTML/JavaScript, and Containers including Docker support.

Summary

> Visual Studio core editor
∨ Universal Windows Platform development
Included
✓ Blend for Visual Studio
✓ .NET Native and .NET Standard
✓ NuGet package manager
✓ Universal Windows Platform tools
✓ Windows 10 SDK (10.0.17134.0)

Optional
□ USB Device Connectivity
□ C++ Universal Windows Platform tools
☑ Graphics debugger and GPU profiler for DirectX
☑ Windows 10 SDK (10.0.16299.0) for UWP: C#, VB, JS
☑ Windows 10 SDK (10.0.15063.0) for UWP: C#, VB, JS
☑ Windows 10 SDK (10.0.14393.0)
☑ Windows 10 SDK (10.0.10586.0)
☑ Windows 10 SDK (10.0.10240.0)

2. You will need to register a Microsoft account if we don't have one in order to run Visual Studio
3. When installing WDK, be sure to select this option at the end:



☑ Install Windows Driver Kit Visual Studio extension

To complete integration with Visual Studio, the Windows Driver Kit extension is required.

Windows 7 x64 and 8.1 x64 (8.1 is optional)

Once installing a Windows 7/8.1 x64 version, we need to install the following software:

1. Windows 7 x64 ISO: https://archive.org/details/en_windows_7_professional_with_sp1_x64_dvd_u_676939_201612
   a. SHA1 hash: 0bcfc54019ea175b1ee51f6d2b207a3d14dd2b58
2. KB3118401, available from: https://support.microsoft.com/en-us/help/3118401/update-for-universal-c-runtime-in-windows or https://www.microsoft.com/en-us/download/details.aspx?id=51161
3. Windows SDK 10, available from: https://go.microsoft.com/fwlink/p/?LinkId=536682
4. Python 2.7.15 x64, available from: https://www.python.org/ftp/python/2.7.15/python-2.7.15.amd64.msi
5. VMWare tools (or other equivalent)

The SDK will also install .NET framework 4.5 on Windows 7.

Testing installation

IMPORTANT NOTICE
READ THIS BEFORE YOU PROCEED

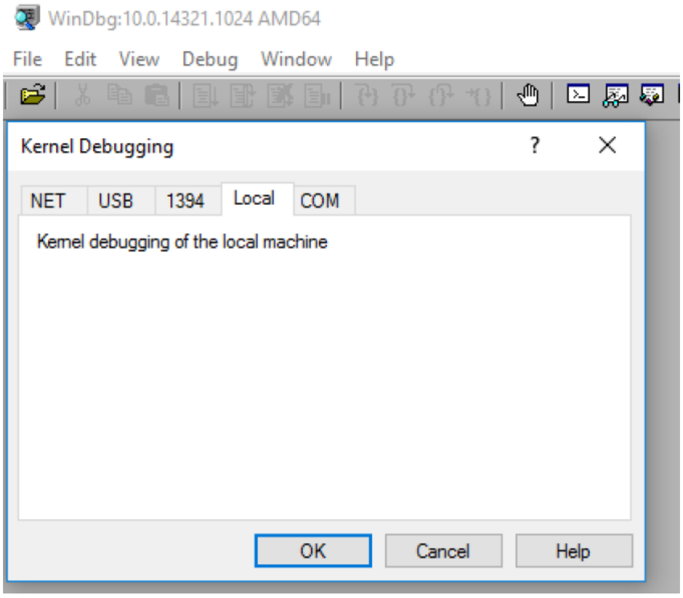
If you already have BitLocker enabled with TPM be sure to have the BitLocker recovery key, otherwise you will lose access to your machine. Once you change the boot options with bcdedit, BitLocker will ask for the recovery key after restart.

Once everything is installed we need to enable debugging mode. Start cmd.exe with Admin privileges and run the following command:

```
bcdedit.exe -set DEBUG ON
```

and then restart the machine.

To test if the machine is setup properly, start WinDBG (x64) with administrative privileges, go to File -> Kernel Debug, and select Local.


WinDbg:10.0.14321.1024 AMD64
File Edit View Debug Window Help
Kernel Debugging
NET
USB
1394
Local
COM
OK
Cancel
Help

Kernel debugging of the local machine

Run the following commands:

```
.symfix
.reload
dd ci!g_CiOptions L1
```

```
For Windows 7 also run:
```

```
dd nt!g_CiEnabled L1
```

and you should get something like this on Windows 7:

```
Microsoft (R) Windows Debugger Version 10.0.14321.1024 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

Connected to Windows 7 7601 x64 target at (Sun Jun 10 10:41:45.346 2018 (UTC + 2:00)), ptr64
TRUE
Symbol search path is: srv*
Executable search path is:
Windows 7 Kernel Version 7601 (Service Pack 1) MP (1 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 7601.17514.amd64fre.win7sp1_rtm.101119-1850
Machine Name:
Kernel base = 0xfffff800`02a4e000 PsLoadedModuleList = 0xfffff800`02c93e90
Debug session time: Sun Jun 10 10:41:53.315 2018 (UTC + 2:00)
System Uptime: 0 days 0:00:56.203
lkd> .symfix
lkd> .reload
Connected to Windows 7 7601 x64 target at (Sun Jun 10 10:42:00.987 2018 (UTC + 2:00)), ptr64
TRUE
Loading Kernel Symbols
...............................................................
................................................................
.............................
Loading User Symbols
................................................................
....................................
Loading unloaded module list
........
lkd> dd ci!g_CiOptions L1
fffff880`00c05e30  00000006
lkd> dd nt!g_CiEnabled L1
fffff800`02c74eb8  00000001
```

and on Windows 10:

```
Microsoft (R) Windows Debugger Version 10.0.17674.1000 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

Connected to Windows 10 17134 x64 target at (Sun Jun 10 14:23:17.504 2018 (UTC + 2:00)), ptr64
TRUE
Symbol search path is: srv*
Executable search path is:
```

```
Windows 10 Kernel Version 17134 MP (1 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 17134.1.amd64fre.rs4_release.180410-1804
Machine Name:
Kernel base = 0xfffff803`0e21f000 PsLoadedModuleList = 0xfffff803`0e5dc1d0
Debug session time: Sun Jun 10 14:23:24.190 2018 (UTC + 2:00)
System Uptime: 0 days 0:06:42.526
lkd> .symfix
lkd> .reload
Connected to Windows 10 17134 x64 target at (Sun Jun 10 14:25:38.781 2018 (UTC + 2:00)), ptr64
TRUE
Loading Kernel Symbols
................................................................
.................................................................
............................................................
Loading User Symbols
.................................................................
.............
Loading unloaded module list
..........
lkd> dd ci!g_CiOptions L1
fffff804`71fedcb0  00000006
```

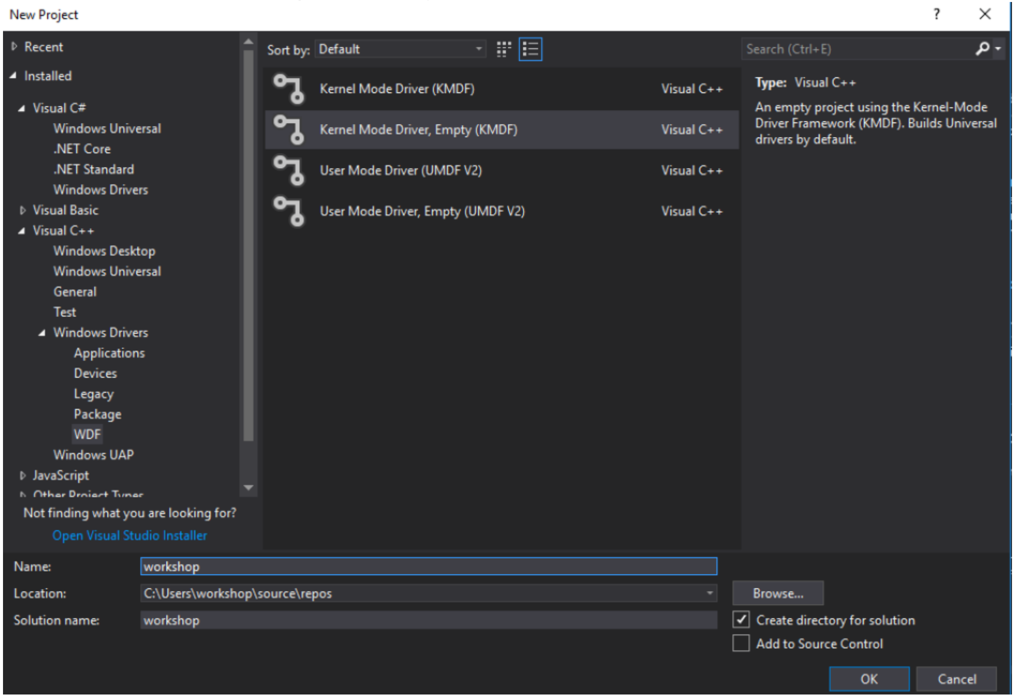
Once everything tested, disable debug mode. Start cmd.exe with Admin privileges and run the following command:

```
bcdedit.exe -set DEBUG OFF
```

and then restart the machine.

On Windows 10 please also start Visual Studio and try the following:

1. Start a new project, and select Visual C++ -> Windows Drivers -> WDF -> Kernel Mode Driver Empty (KMDF)
    a. Give it a name: e.g.: workshop



Type: Visual C++

An empty project using the Kernel-Mode Driver Framework (KMDF). Builds Universal drivers by default.

Name: workshop

Location: C:\Users\workshop\source\repos

Solution name: workshop

☑ Create directory for solution

☐ Add to Source Control