Training download contents

host.zip

Unzip the contents of host.zip to the c:\cm folder on the host system. The following directory structure would be created.

Folder	Description
bin	The workspace for UWP version of WinDBG to attach to the guest VM as a kernel debugger using serial port.
build	Windows executables from the Guest VM, made available on the host for analysis.
dbgext	WinDBG extension DLLs. All these DLLs are publicly available and some of them are open source. These DLLs will only load in the 64-bit version of WinDBG.
dump	System and process memory dumps which may be used in the class for the hands-on labs.
script	CMD scripts to perform the following tasks on the host: Build an application or driver from .vcxproj – module_build.cmd Stage the build output to a given share on the VM – module_stage.cmd Create a test signing certificate – sign_create.cmd Sign a driver binary – sign_driver.cmd
src	This folder is only required for the programming classes. The content of this folder is course specific and will be provided on the first day of the course. The sub-folders will be organized as follows: \labs - Template source code for hands-on labs. \src - Sample source code code-walkthroughs and demos. \sols - Solutions for hands-on labs. Provided on the last day of class.
sysint	Microsoft Windows SysInternals Tools.
tool	Various publicly available tools required for the hands-on labs.

© 2000 - 2021 CodeMachine Inc.

https://t.me/learningnets

guest.zip

If you have downloaded a pre-configured VMware VM, then the contents of guest.zip are already available in the c:\pub directory of your VM and you can skip this setup.

Unzip the contents of guest.zip to the \\winlabvm\pub folder on the guest system. The following directory structure would be created.

Folder	Description
bin	Contains some user and kernel mode tools which may be required for demos and hands-on labs.
mimikatz	Precompiled version of the open-source tool Mimikatz. https://github.com/gentilkiwi/mimikatz
processhacker	Precompiled version of the open-source tool ProcessHacker. https://github.com/processhacker/processhacker
script	CMD scripts to perform the following tasks in the Guest VM: Install a driver – driver_install.cmd Copy a driver to %systemroot%\system32\drivers – driver_copy.cmd Start a driver – driver_start.cmd Stop a driver – driver_stop.cmd Install, copy and start a driver (all in one) – driver_run.cmd
sym	Unzip the contents of sym.zip here. This folder is the symbol cache for Windows bootable .ISO file hosted on OneDrive [*en_windows_10_business_editions_version_20h2_x64.iso*]. Since the Guest VM will not connect to the Internet, this symbol cache provides pre-downloaded symbols to tools such as WinDBG, ProcessHacker, ProcMon, ProcessExplorer, etc.
sysint	Microsoft Windows SysInternals Tools for use in the Guest VM.
tool	Various publicly available tools which may be required for the demos and hands-on labs.
windbg	Minimal distribution of the classic WinDBG (v10.0.18362.84) for use in the Guest VM. Includes both the 32-bit and 64-bit versions.

sym.zip

If you have downloaded a pre-configured VMware VM, then the contents of sym.zip are already available in the c:\pub\sym directory of your VM and you can skip this setup.

sym.zip contains the symbols for the Windows binaries in the guest VM in symbol server format. Unzip the contents of sym.zip to the \\winlabvm\pub\sym folder on the guest system.

https://t.me/learningnets