WinDbg: User & Kernel Mode Debugging

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

Windows Debuggers

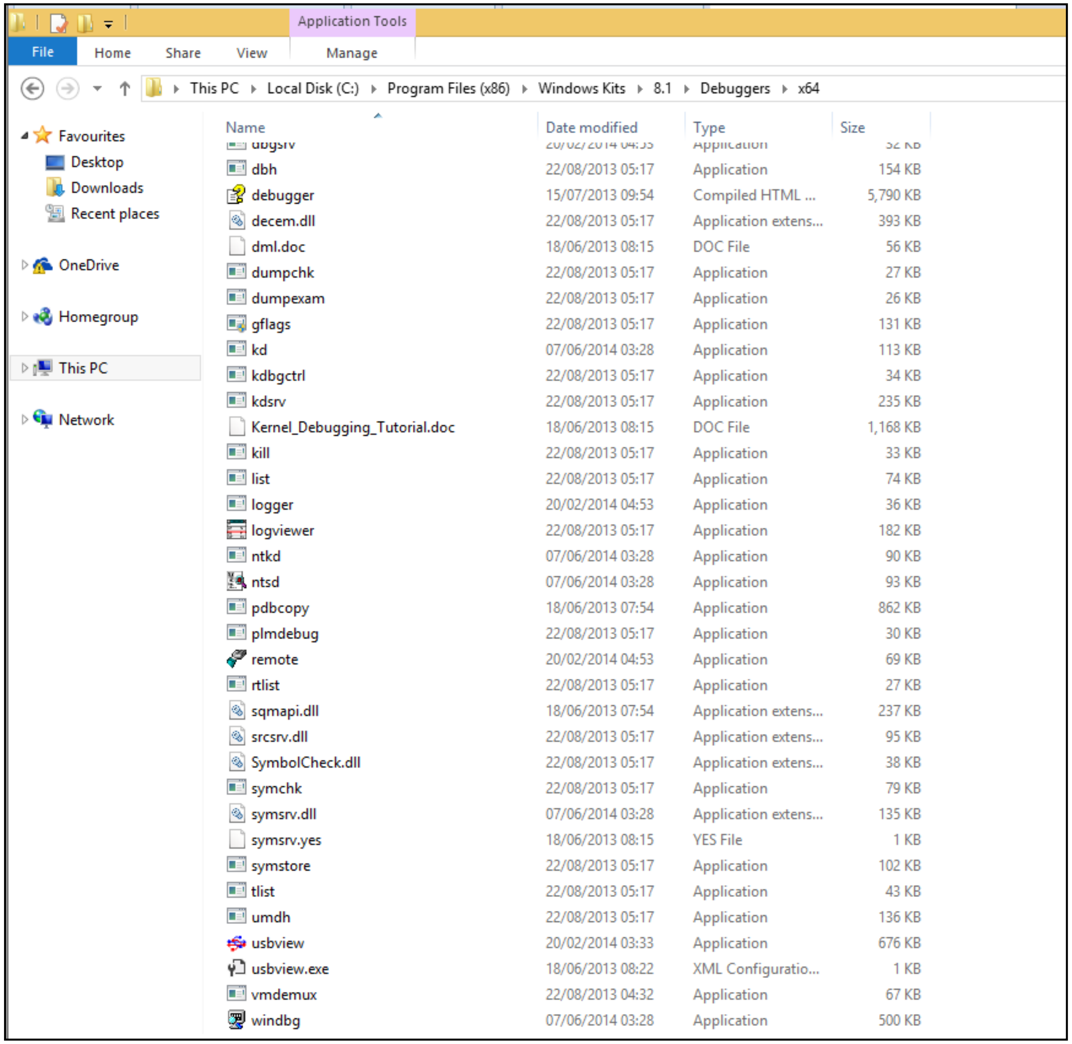
Windows Debuggers

Debugger	User Mode	Kernel Mode
Visual Studio IDE (WDK 8)	✓	✓
WinDbg	✓	✓
KD and NTKD		✓
CDB	✓	
NTSD	✓	

Important Points

- Visual Studio has integrated Windows Debugger (WDK 8.0 onwards)
- WinDbg is GUI based, rest are character based console programs
- KD and NTKD are alike
- CDB and NTSD are alike
- “N” version spawns a new window ,while the other inherits
- Kernel mode debugging typically requires 2 running machines – Host and Target

Where are my Debuggers?

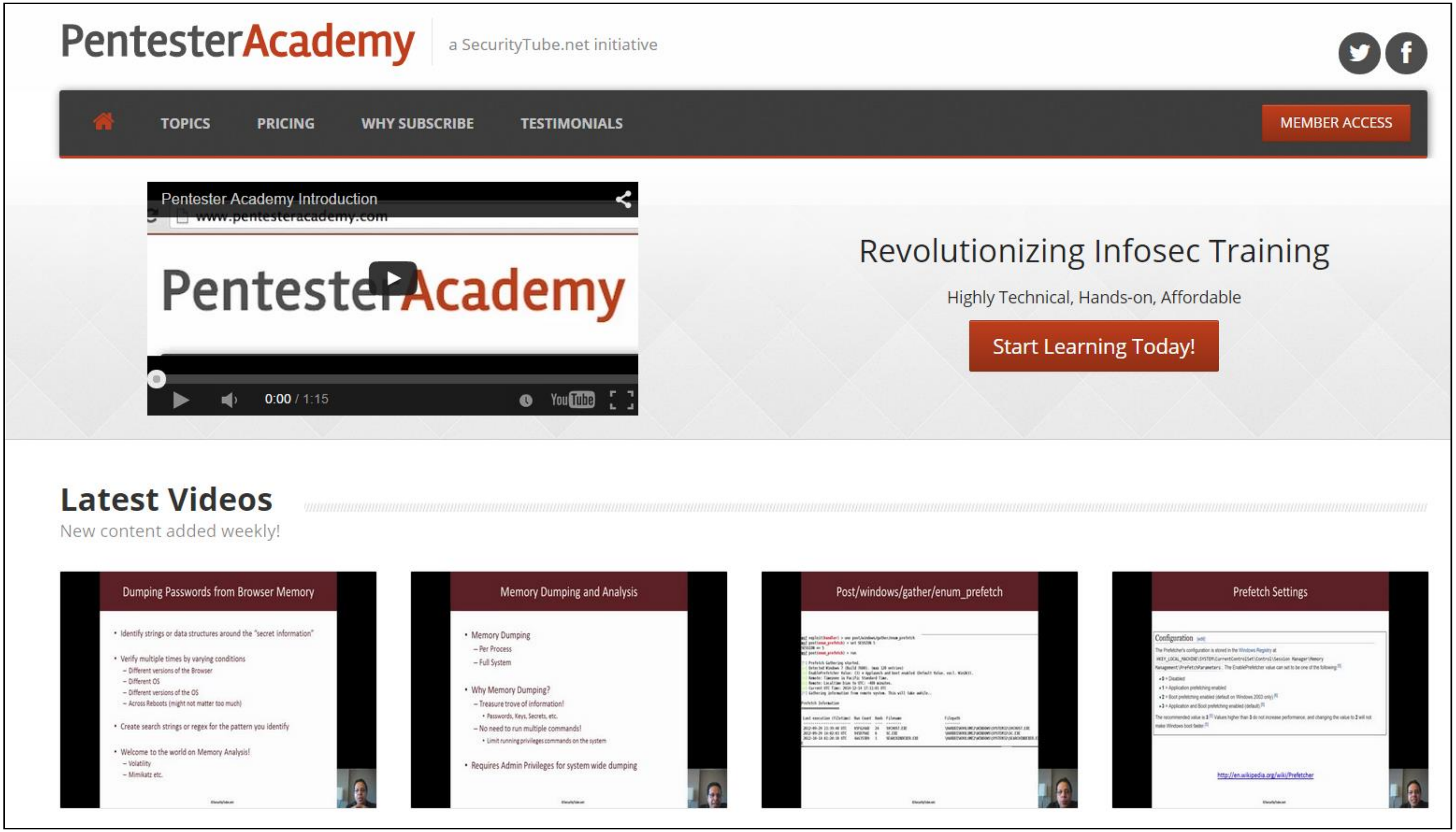


This PC › Local Disk (C:) › Program Files (x86) › Windows Kits › 8.1 › Debuggers › x64

Name	Date modified	Type	Size
dbgsrv	20/02/2014 04:53	Application	32 KB
dbh	22/08/2013 05:17	Application	154 KB
debugger	15/07/2013 09:54	Compiled HTML ...	5,790 KB
decem.dll	22/08/2013 05:17	Application extens...	393 KB
dml.doc	18/06/2013 08:15	DOC File	56 KB
dumpchk	22/08/2013 05:17	Application	27 KB
dumpexam	22/08/2013 05:17	Application	26 KB
gflags	22/08/2013 05:17	Application	131 KB
kd	07/06/2014 03:28	Application	113 KB
kdbgctrl	22/08/2013 05:17	Application	34 KB
kdsrv	22/08/2013 05:17	Application	235 KB
Kernel_Debugging_Tutorial.doc	18/06/2013 08:15	DOC File	1,168 KB
kill	22/08/2013 05:17	Application	33 KB
list	22/08/2013 05:17	Application	74 KB
logger	20/02/2014 04:53	Application	36 KB
logviewer	22/08/2013 05:17	Application	182 KB
ntkd	07/06/2014 03:28	Application	90 KB
ntsd	07/06/2014 03:28	Application	93 KB
pdbcopy	18/06/2013 07:54	Application	862 KB
plmdebug	22/08/2013 05:17	Application	30 KB
remote	20/02/2014 04:53	Application	69 KB
rtlist	22/08/2013 05:17	Application	27 KB
sqmapi.dll	18/06/2013 07:54	Application extens...	237 KB
srcsrv.dll	22/08/2013 05:17	Application extens...	95 KB
SymbolCheck.dll	22/08/2013 05:17	Application extens...	38 KB
symchk	22/08/2013 05:17	Application	79 KB
symsrv.dll	07/06/2014 03:28	Application extens...	135 KB
symsrv.yes	18/06/2013 08:15	YES File	1 KB
symstore	22/08/2013 05:17	Application	102 KB
tlist	22/08/2013 05:17	Application	43 KB
umdh	22/08/2013 05:17	Application	136 KB
usbview	20/02/2014 03:33	Application	676 KB
usbview.exe	18/06/2013 08:22	XML Configuratio...	1 KB
vmdemux	22/08/2013 04:32	Application	67 KB
windbg	07/06/2014 03:28	Application	500 KB

Windows 8.1

Pentester Academy



PentesterAcademy a SecurityTube.net initiative

Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Latest Videos

New content added weekly!

Dumping Passwords from Browser Memory

- Identify strings or data structures around the "secret information"
- Verify multiple times by varying conditions
  - Different versions of the Browser
  - Different OS
  - Different versions of the OS
  - Across Reboots (might not matter too much)
- Create search strings or regex for the pattern you identify
- Welcome to the world on Memory Analysis!
  - Volatility
  - Mimikatz etc.

Memory Dumping and Analysis

- Memory Dumping
  - Per Process
  - Full System
- Why Memory Dumping?
  - Treasure trove of information!
    - Passwords, Keys, Secrets, etc.
  - No need to run multiple commands!
    - Limit running privileges commands on the system
- Requires Admin Privileges for system wide dumping

Post/windows/gather/enum_prefetch

```
msf exploit(handler) > use post/windows/gather/enum_prefetch
msf post(enum_prefetch) > set SESSION 1
SESSION => 1
msf post(enum_prefetch) > run

[*] Prefetch Gathering started.
[+] Detected Windows 7 (Build 7600). (max 128 entries)
[+] EnablePrefetcher Value: (3) = Applaunch and boot enabled (Default Value, excl. Win2K3).
[+] Remote: Timezone is Pacific Standard Time.
[+] Remote: LocalTime bias to UTC: -480 minutes.
[+] Current UTC Time: 2014-12-14 17:11:01 UTC
[*] Gathering information from remote system. This will take awhile..

Prefetch Information
====================

 Last execution (FILETime)  Run Count  Hash  Filename           Filepath
 -------------------------  ---------  ----  --------           --------
 2012-09-29 [illegible] UTC  [illegible]  24   SVCHOST.EXE        \WINDOWS\SYSTEM32\SVCHOST.EXE
 2012-09-29 [illegible] UTC  [illegible]  6    SC.EXE             \WINDOWS\SYSTEM32\SC.EXE
 2012-10-18 [illegible] UTC  [illegible]  1    SEARCHINDEXER.EXE  \WINDOWS\SYSTEM32\SEARCHINDEXER.EXE
```

Prefetch Settings

Configuration [edit]

The Prefetcher's configuration is stored in the Windows Registry at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters . The EnablePrefetcher value can set to be one of the following:[5]

- 0 = Disabled
- 1 = Application prefetching enabled
- 2 = Boot prefetching enabled (default on Windows 2003 only)[6]
- 3 = Application and Boot prefetching enabled (default)[5]

The recommended value is 3.[5] Values higher than 3 do not increase performance, and changing the value to 2 will not make Windows boot faster.[5]

http://en.wikipedia.org/wiki/Prefetcher