Debug Windows Kernel

Information Security Inc.

Contents

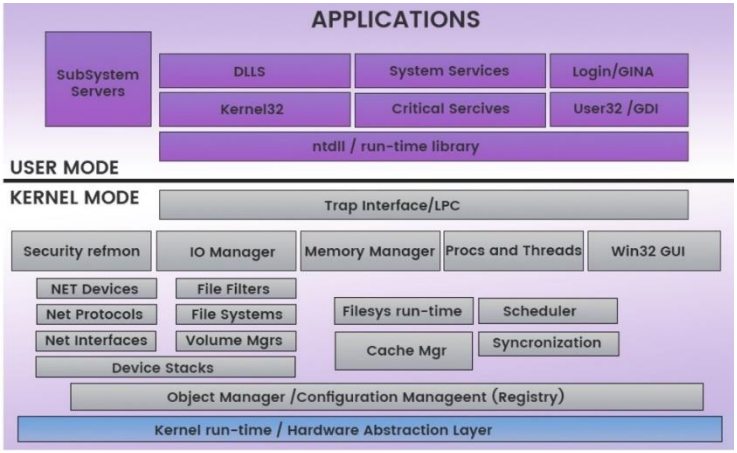
- Windows Architecture
- Debugging Lab
- Setting up the Debugger
- Setting up the Debugee
- Setting up and testing the connection between Debugger and Debugee
- References

Windows Architecture

◎ User-mode and Kernel-mode

- In user-mode, an application starts a user-mode process which comes with its own private virtual address space and handle table
- In kernel mode, applications share virtual address space.

◎ Relationship of application components for user-mode and kernel-mode.

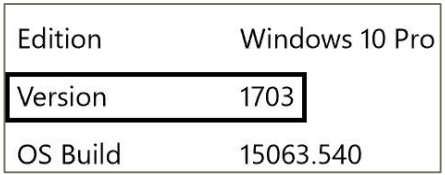


Debugging Lab

◎Lab components

▲ Vmware workstation 12 pro

▲ Two virtual machines: Windows 10 64bit
(one will be the Debugger and one will be the Debugee)

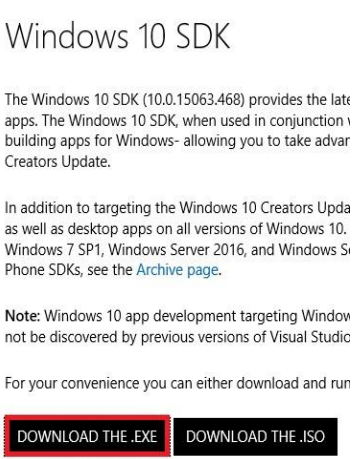


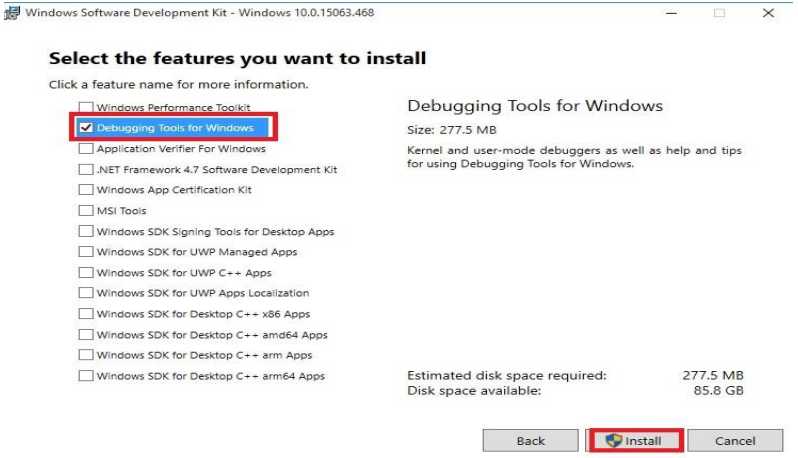
▲ WinDbg (https://developer.microsoft.com/en-us/windows/downloads/windows-10-sdk)

Setting up the Debugger

◎ Debugger is the machine form where we will be watching the Debugee

◎ Download WinSDK and install WinDbg (https://developer.microsoft.com/en-us/windows/downloads/windows-10-sdk)

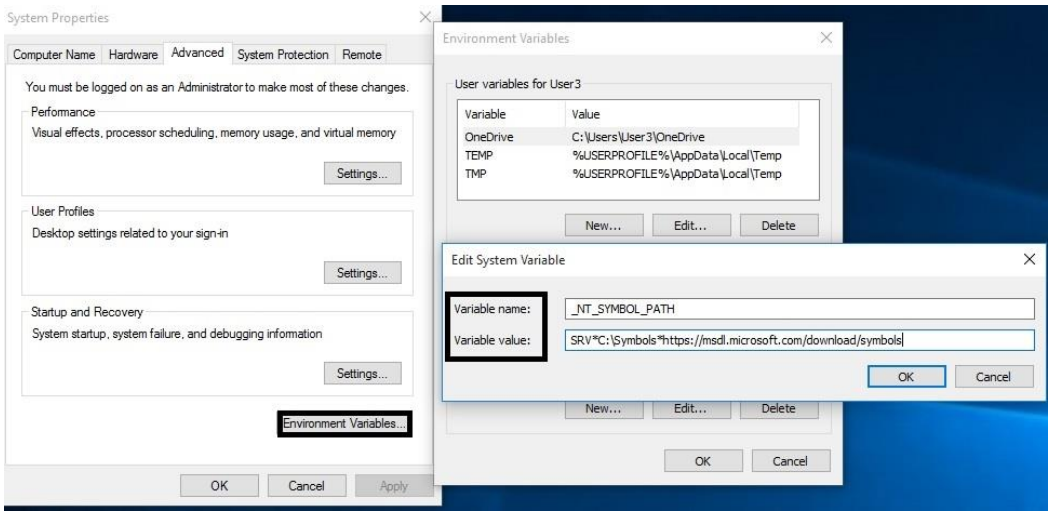




Setting up the Debugger

◎ Adding the Debbuging Symbols (https://en.wikipedia.org/wiki/Symbol_(programming))

Assign a new variable called _NT_SYMBOL_PATH



Setting up the Debugee

◎ Adding one more option in a boot menu using bcdedit

▲ Copy the current settings into a new entry called “ForDebug”

▲ Enable debugging on the created entry “ForDebug”

▲ Verify the debugging interface settings

```
C:\>bcdedit /copy {current} /d "ForDebug"
The entry was successfully copied to {346d1950-9395-11e7-9bde-00505623a295}.

C:\>bcdedit /debug {346d1950-9395-11e7-9bde-00505623a295} on
The operation completed successfully.

C:\>bcdedit /dbgsettings
debugtype               Serial
debugport               1
baudrate                115200
The operation completed successfully.
```

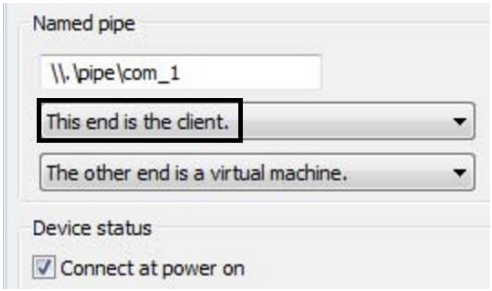
Setting up the connection between Debugger and Debugee

◎ Debugger and Debugge will be communicating via Serial Port COM1, that will be emulated in the host system by a Named Pipe (https://en.wikipedia.org/wiki/Named_pipe)

◎ Debugger and the debuggee need to have the same pipe name set

◎ Debugger will be creating the pipe, while the Debuggee will be connecting to the existing one (Debugger needs to run first)

▲ Debugger config



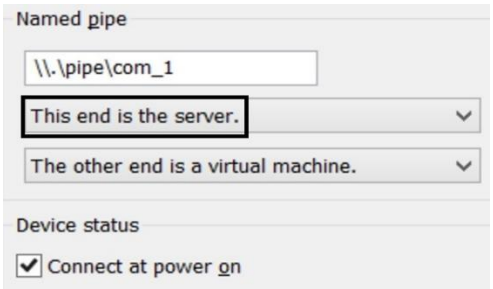
Setting up the connection between Debugger and Debugee

◎ Debugger and Debugge will be communicating via Serial Port COM1, that will be emulated in the host system by a Named Pipe (https://en.wikipedia.org/wiki/Named_pipe)

◎ Debugger and the debuggee need to have the same pipe name set

◎ Debugger will be creating the pipe, while the Debuggee will be connecting to the existing one (Debugger needs to run first)

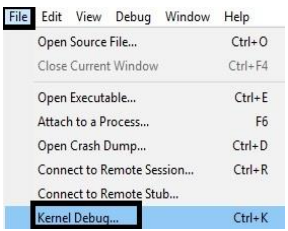
▲ Debugee config



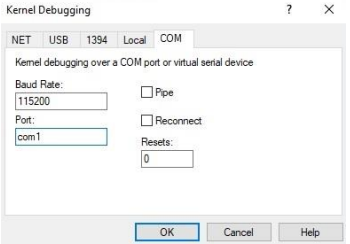
Setting up the connection between Debugger and Debugee

◎ Testing the connection

▲ File -> Kernel Debug



Choosing debugging interface



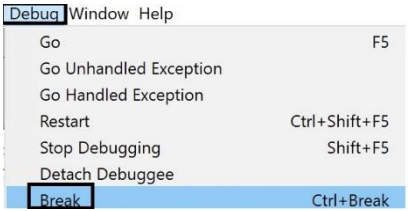
▲ Debugee connects back to the Debugger

```
Microsoft (R) Windows Debugger Version 10.0.15063.468 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

Opened \\.\com1
Waiting to reconnect...
Connected to Windows 10 15063 x64 target at (Thu Sep  7 00:53:29.003 2017 (UTC - 7:00)), ptr64 TRUE
Kernel Debugger connection established.

************* Symbol Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       SRV*C:\Symbols*https://msdl.microsoft.com/download/symbols
Symbol search path is: SRV*C:\Symbols*https://msdl.microsoft.com/download/symbols
Executable search path is:
Windows 10 Kernel Version 15063 MP (1 procs) Free x64
Built by: 15063.0.amd64fre.rs2_release.170317-1834
Machine Name:
Kernel base = 0xfffff800`1d299000 PsLoadedModuleList = 0xfffff800`1d5e55c0
System Uptime: 0 days 0:00:00.070
```

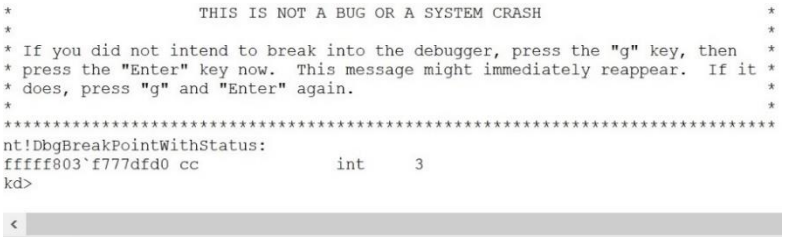
Setting up the connection between Debugger and Debugee

◎ Testing the connection

▲ Interrupting the Debugee, clicking Debug -> Break



▲ **kd** prompt shows -> Debugger is in control of the Debugee



Setting up the connection between Debugger and Debugee

◎ Examine EPROCESS Structure (https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/eprocess)

```
kd> ! process 0 0
**** NT ACTIVE PROCESS DUMP ****
PROCESS ffff930fa1299040
    SessionId: none  Cid: 0004    Peb: 00000000  ParentCid: 0000
    DirBase: 001aa000  ObjectTable: ffffa60a88c03280  HandleCount:   1.
    Image: System

kd> dt nt! EPROCESS ffff930fa1299040
   +0x000 Pcb              : _KPROCESS
   +0x2d8 ProcessLock      : _EX_PUSH_LOCK
   +0x2e0 UniqueProcessId  : 0x00000000`00000004 Void
   +0x2e8 ActiveProcessLinks : _LIST_ENTRY [ 0xfffff803`f7951fe0 - 0xfffff803`f7951fe0 ]
   +0x2f8 RundownProtect   :  EX RUNDOWN REF
```

Setting up the connection between Debugger and Debugee

◎ List all processes

```
kd> !process 0 0
**** NT ACTIVE PROCESS DUMP ****
PROCESS ffff930fa1299040
    SessionId: none  Cid: 0004    Peb: 00000000  ParentCid: 0000
    DirBase: 001aa000  ObjectTable: ffffa60a88c03280  HandleCount: 2723.
    Image: System

PROCESS ffff930fa2ea0400
    SessionId: none  Cid: 027c    Peb: 5770e24000  ParentCid: 0004
    DirBase: 02ec6000  ObjectTable: ffffa60a88ed2ec0  HandleCount:  52.
    Image: smss.exe
```

◎ Show process full details (wordpad.exe)

```
kd> !process 0 7 wordpad.exe
PROCESS ffff930fa4ca17c0
    SessionId: 1  Cid: 01fc    Peb: b431ae6000  ParentCid: 1670
    DirBase: 147d00000  ObjectTable: ffffa60a942ead00  HandleCount: 338.
    Image: wordpad.exe
    VadRoot ffff930fa34e19b0 Vads 415 Clone 0 Private 2329. Modified 62037. Locked 0.
    DeviceMap ffffa60a903e7050
    Token                             ffffa60a947c6060
    ElapsedTime                       00:00:33.262
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         401776
    QuotaPoolUsage[NonPagedPool]      56632
    Working Set Sizes (now,min,max)  (10739, 50, 345) (42956KB, 200KB, 1380KB)
    PeakWorkingSetSize                10924
    VirtualSize                       2097370 Mb
    PeakVirtualSize                   2097378 Mb
    PageFaultCount                    75634
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      3080
```

References

- InfoSec

http://resources.infosecinstitute.com/windows-architecture-and-userkernel-mode/#gref

- Wikipedia

https://en.wikipedia.org/wiki/Architecture_of_Windows_NT

- WinDbg

http://www.windbg.org/