PROJ 12: **Kernel Debugging with Livekd and Win Server 2008**

Prof. Alberto LaCava

CY -640

MALWARE ANALYSIS & DEFENSE

Nikhil Patel

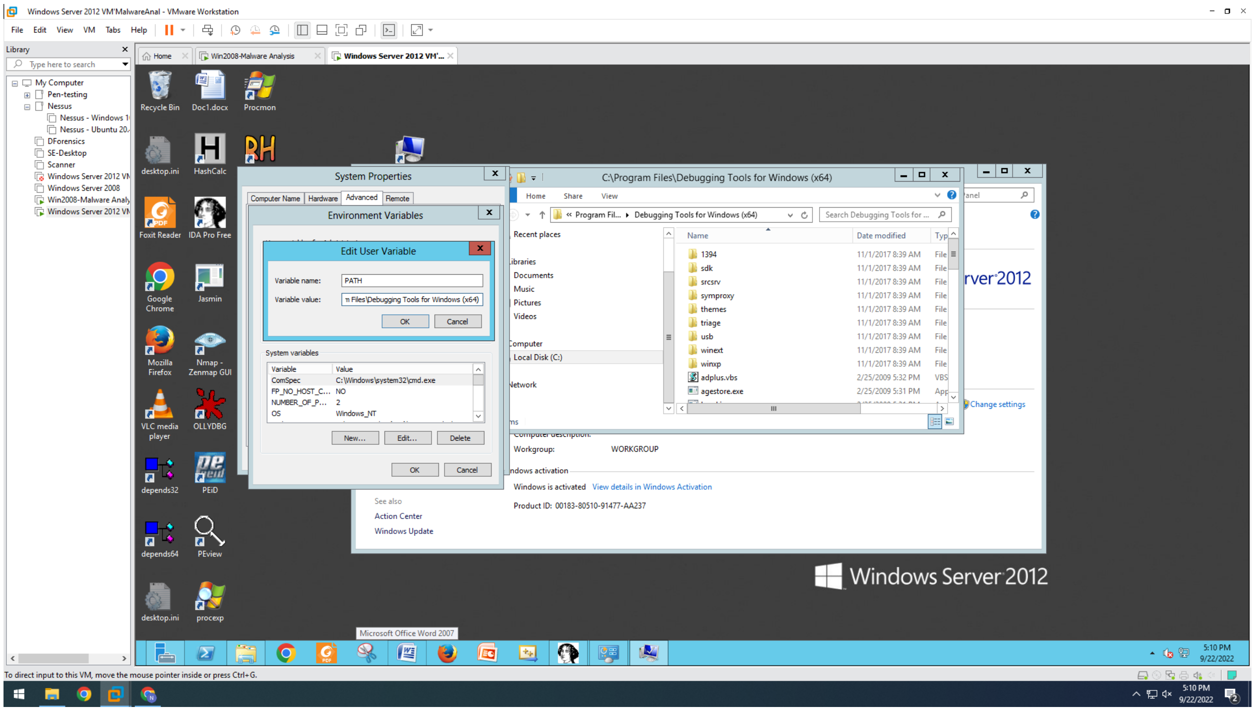
11/09/2022

Introduction: In this lab, we will debug the window kernel with Livekd and Win Server.

Procedure :

Editing the Path

- Open cmd and type “windbg”.
- Now right-click on start > computer properties > advanced > Environment Variables.
- Paste C:\programfile\debugging tools for windows (x86)\



Variable name: PATH

Variable value: n Files\Debugging Tools for Windows (x64)

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_C...	NO
NUMBER_OF_P...	2
OS	Windows_NT

Name	Date modified	Typ
1394	11/1/2017 8:39 AM	File
sdk	11/1/2017 8:39 AM	File
srcsrv	11/1/2017 8:39 AM	File
symproxy	11/1/2017 8:39 AM	File
themes	11/1/2017 8:39 AM	File
triage	11/1/2017 8:39 AM	File
usb	11/1/2017 8:39 AM	File
winext	11/1/2017 8:39 AM	File
winxp	11/1/2017 8:39 AM	File
adplus.vbs	2/25/2009 5:32 PM	VBS
agestore.exe	2/25/2009 5:31 PM	App

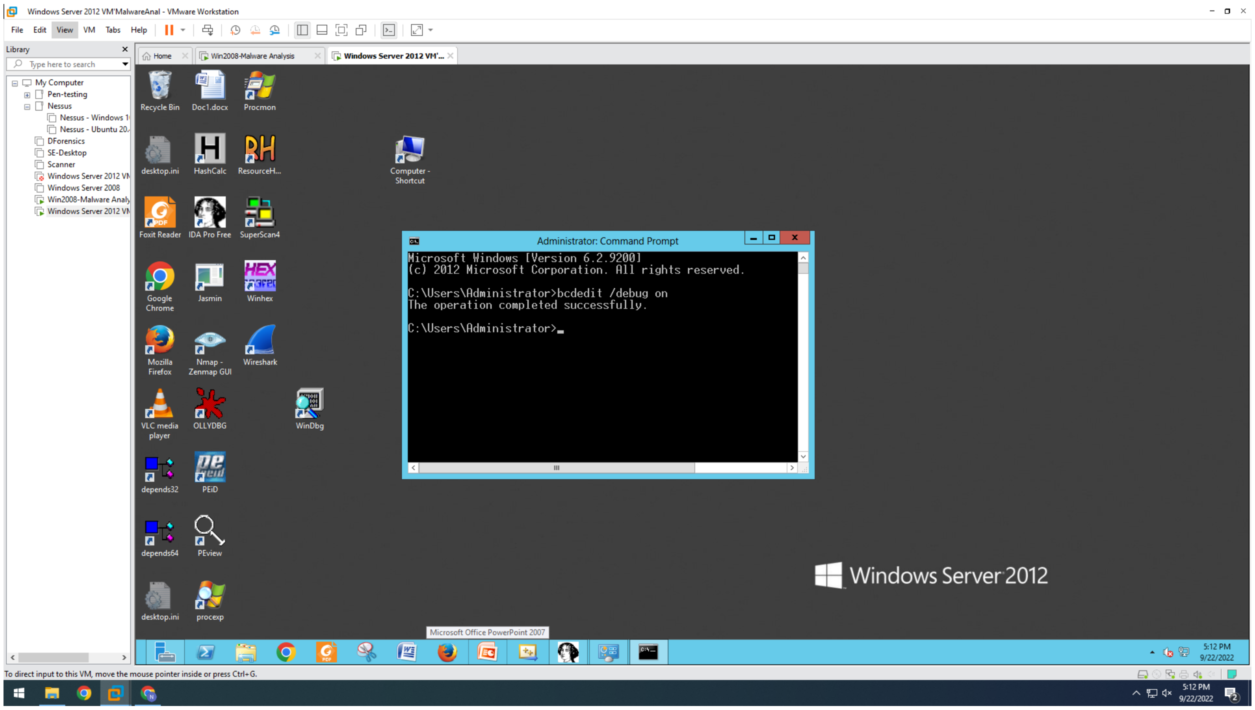
Workgroup: WORKGROUP

Windows is activated View details in Windows Activation

Product ID: 00183-80510-91477-AA237

Setting up Local Kernel-Mode Debugging

- Go to cmd and type “bcdedit /debug on”.



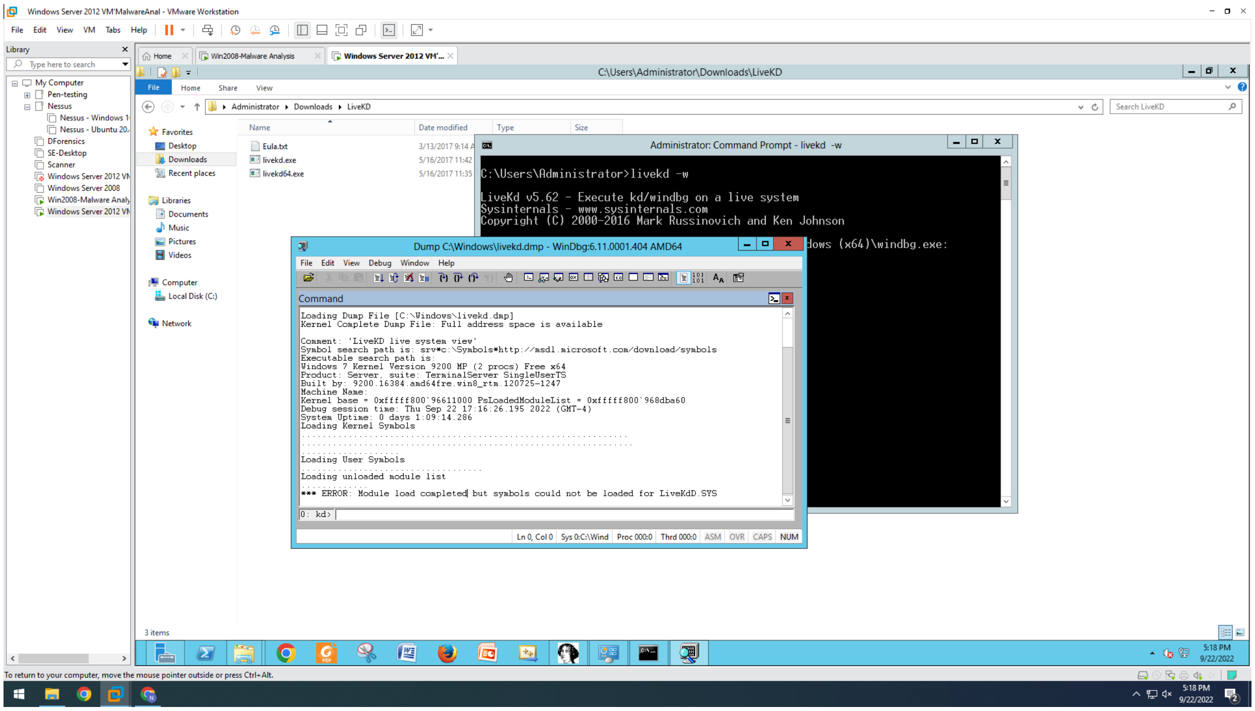
```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>bcdedit /debug on
The operation completed successfully.

C:\Users\Administrator>_
```

Getting LiveKD

- Go to download LiveKD > open folder > right-click on LiveKD.zip and extract all.
- Copy C:\USers\Administrator\Downloads\LiveKD\livekd.exe C:\windows\system32.



```
C:\Users\Administrator>livekd -w

LiveKd v5.62 - Execute kd/windbg on a live system
Sysinternals - www.sysinternals.com
Copyright (C) 2000-2016 Mark Russinovich and Ken Johnson

dows (x64)\windbg.exe:
```

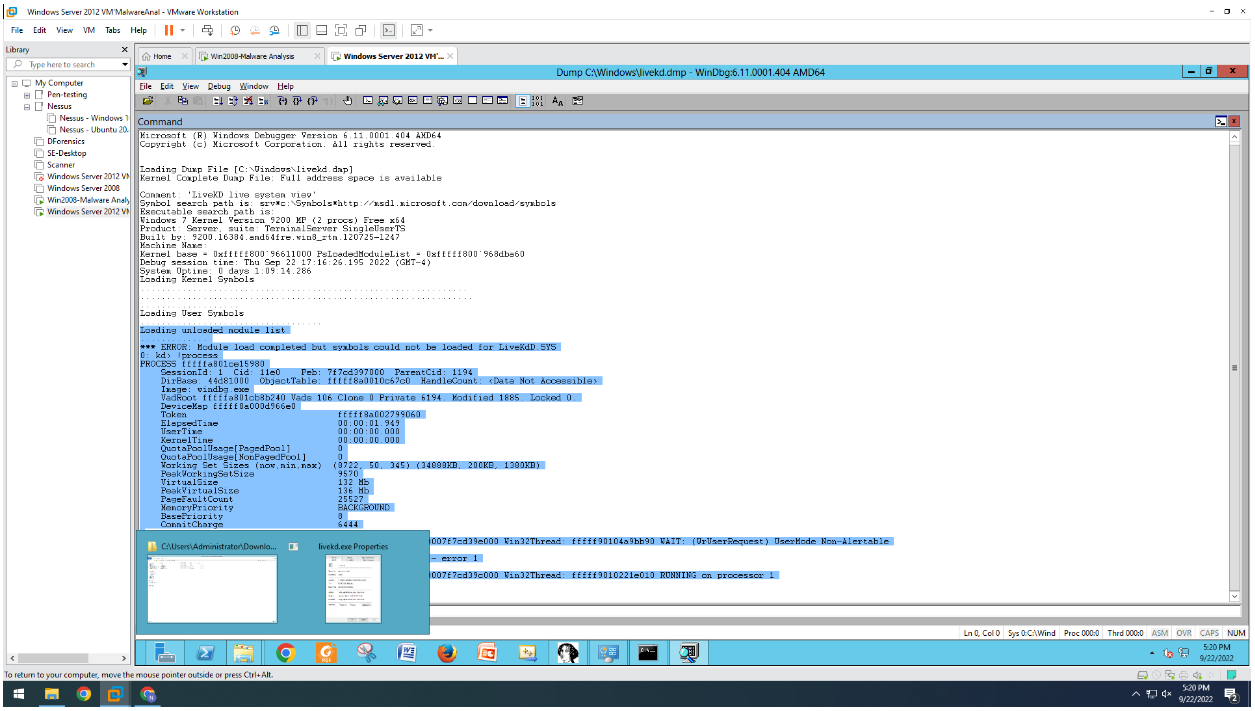
```
Loading Dump File [C:\Windows\livekd.dmp]
Kernel Complete Dump File: Full address space is available

Comment: 'LiveKD live system view'
Symbol search path is: srv*c:\Symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows 7 Kernel Version 9200 MP (2 procs) Free x64
Product: Server, suite: TerminalServer SingleUserTS
Built by: 9200.16384.amd64fre.win8_rtm.120725-1247
Machine Name:
Kernel base = 0xfffff800`96611000 PsLoadedModuleList = 0xfffff800`968dba60
Debug session time: Thu Sep 22 17:16:26.195 2022 (GMT-4)
System Uptime: 0 days 1:09:14.286
Loading Kernel Symbols
...............................................................
................................................................
...................
Loading User Symbols
...................................
Loading unloaded module list
.............
*** ERROR: Module load completed but symbols could not be loaded for LiveKdD.SYS

0: kd>
```

Using LiveKD

- Open the cmd as administrator and type “livekd -w”.
- Press Y and hit enter.
- Take a screenshot



```
Microsoft (R) Windows Debugger Version 6.11.0001.404 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.


Loading Dump File [C:\Windows\livekd.dmp]
Kernel Complete Dump File: Full address space is available

Comment: 'LiveKD live system view'
Symbol search path is: srv*c:\Symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows 7 Kernel Version 9200 MP (2 procs) Free x64
Product: Server, suite: TerminalServer SingleUserTS
Built by: 9200.16384.amd64fre.win8_rtm.120725-1247
Machine Name:
Kernel base = 0xfffff800`96611000 PsLoadedModuleList = 0xfffff800`968dba60
Debug session time: Thu Sep 22 17:16:26.195 2022 (GMT-4)
System Uptime: 0 days 1:09:14.286
Loading Kernel Symbols
...............................................................
................................................................
..................
Loading User Symbols
..................................
Loading unloaded module list
.............
*** ERROR: Module load completed but symbols could not be loaded for LiveKdD.SYS
0: kd> !process
PROCESS fffffa801ce15980
    SessionId: 1  Cid: 11e0    Peb: 7f7cd397000  ParentCid: 1194
    DirBase: 44d81000  ObjectTable: fffff8a0010c67c0  HandleCount: <Data Not Accessible>
    Image: windbg.exe
    VadRoot fffffa801cb8b240 Vads 106 Clone 0 Private 6194. Modified 1885. Locked 0.
    DeviceMap fffff8a000d966e0
    Token                             fffff8a002799060
    ElapsedTime                       00:00:01.949
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         0
    QuotaPoolUsage[NonPagedPool]      0
    Working Set Sizes (now,min,max)  (8722, 50, 345) (34888KB, 200KB, 1380KB)
    PeakWorkingSetSize                9570
    VirtualSize                       132 Mb
    PeakVirtualSize                   136 Mb
    PageFaultCount                    25527
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      6444

                                    007f7cd39e000 Win32Thread: fffff90104a9bb90 WAIT: (WrUserRequest) UserMode Non-Alertable

                                    - error 1

                                    007f7cd39c000 Win32Thread: fffff9010221e010 RUNNING on processor 1
```

<u>Conclusion</u>: To conclude with the lab, We learned numerous strategies for performing a data encoding method, as well as WinHex.