



ASSIGNMENT 7

Network Security

Soheil Shirvani

3720505



- 1) *volatility -f stuxnet.vmem imageinfo*, Provide a screenshot for the output of the above command.

```

root@fcs-security-attacker:~/Desktop/stuxnet.vmem# volatility -f stuxnet.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO Start: volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
6) Home
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (/root/Desktop/stuxnet.vmem/stuxnet.vmem)
PAE type : PAE
DTB : 0x319000L
KDBG : 0x80545ae0L
Number of Processors : 1
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xffdf000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2011-06-03 04:31:36 UTC+0000
Image local date and time : 2011-06-03 00:31:36 -0400
root@fcs-security-attacker:~/Desktop/stuxnet.vmem#

```

- 2) *volatility -f stuxnet.vmem --profile = WinXPSP2x86 pstree*, List all the existing process IDs (PIDs) and parent process IDs (PPID) for running lsass.exe process. Do you think having lower PID and process's data and time can be helpful to distinguish safe from unsafe processes?

Name	Pid	PPid	Thds	Hnds	Time
0x023c8830:system	4	0	59	403	1970-01-01 00:00:00 UTC+0000
0x820df020:smss.exe	376	4	3	19	2010-10-29 17:08:53 UTC+0000
0x821a2da0:csrss.exe	600	376	11	395	2010-10-29 17:08:54 UTC+0000
0x81da5650:winlogon.exe	624	376	19	570	2010-10-29 17:08:54 UTC+0000
0x82073020:services.exe	668	624	21	431	2010-10-29 17:08:54 UTC+0000
0x81fe52d0:vmtoolsd.exe	1664	668	5	284	2010-10-29 17:09:05 UTC+0000
0x81c0cda0:cmd.exe	968	1664	0	-----	2011-06-03 04:31:35 UTC+0000
0x81f14938:ipconfig.exe	304	968	0	-----	2011-06-03 04:31:35 UTC+0000
0x822843e8:svchost.exe	1032	668	61	1169	2010-10-29 17:08:55 UTC+0000
0x822b9a10:wuauc1t.exe	976	1032	3	133	2010-10-29 17:12:03 UTC+0000
0x820ecc10:wscntfy.exe	2040	1032	1	28	2010-10-29 17:11:49 UTC+0000
0x81e61da0:svchost.exe	940	668	13	312	2010-10-29 17:08:55 UTC+0000

lsass.exe process:

Offset(P)	Name	PID	PPid
0x0000000001e47c00	lsass.exe	1928	668
0x0000000001e498c8	lsass.exe	868	668
0x0000000002070020	lsass.exe	680	624

There are 3 lsass.exe in the process list but there should be one lsass instance in the process list. For the first two rows the creation time is the same and for the

last one is around one year earlier which is suspicious. Also, the PID for all these three processes are different which shows this file is a malicious file.

3) *volatility -f stuxnet.vmem --profile = WinXPSP2x86 psscan , List two terminated processes and their creation and termination times*

```
root@fcs-security-attacker:~/Desktop/stuxnet.vmem# volatility -f stuxnet.vmem --profile=WinXPSP2x86 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)      Name      PID      PPID      PDB      Time created      Time exited
-----
0000000001e0cda0 cmd.exe    968      1664     0x0a9403a0 2011-06-03 04:31:35 UTC+0000 2011-06-03 04:31:36 UTC+0000
0000000001e47c00 lsass.exe 1928      668     0x0a9403c0 2011-06-03 04:26:55 UTC+0000
0000000001e498c8 lsass.exe 868       668     0x0a940360 2011-06-03 04:26:55 UTC+0000
0000000001e543a0 Procmon.exe 660      1196     0x0a940260 2011-06-03 04:25:56 UTC+0000
0000000001fa5650 winlogon.exe 624      376     0x0a940060 2010-10-29 17:08:54 UTC+0000
0000000001fb8da0 svchost.exe 856       668     0x0a9400e0 2010-10-29 17:08:55 UTC+0000
000000000200eda0 jqs.exe    1580      668     0x0a9401e0 2010-10-29 17:09:05 UTC+0000
0000000002018b28 svchost.exe 1080      668     0x0a940140 2010-10-29 17:08:55 UTC+0000
0000000002061da0 svchost.exe 940       668     0x0a940100 2010-10-29 17:08:55 UTC+0000
000000000206b660 VMwareUser.exe 1356     1196     0x0a9402e0 2010-10-29 17:11:50 UTC+0000
0000000002070020 lsass.exe 680       624     0x0a9400a0 2010-10-29 17:08:54 UTC+0000
0000000002086978 TSVCNCache.exe 324     1196     0x0a940180 2010-10-29 17:11:49 UTC+0000
0000000002114938 ipconfig.exe 304       968     0x0a940380 2011-06-03 04:31:35 UTC+0000 2011-06-03 04:31:36 UTC+0000
00000000021a5390 wmiiprvse.exe 1872      856     0x0a9401c0 2011-06-03 04:25:58 UTC+0000
00000000021c5da0 VMwareTray.exe 1912     1196     0x0a9402c0 2010-10-29 17:11:50 UTC+0000
00000000021e52d0 vmtoolsd.exe 1664      668     0x0a940200 2010-10-29 17:09:05 UTC+0000
00000000021ee8b0 spoolsv.exe 1412      668     0x0a9401a0 2010-10-29 17:08:56 UTC+0000
00000000021f7020 svchost.exe 1200      668     0x0a940160 2010-10-29 17:08:55 UTC+0000
000000000225ada0 alg.exe    188       668     0x0a940240 2010-10-29 17:09:09 UTC+0000
0000000002273020 services.exe 668       624     0x0a940080 2010-10-29 17:08:54 UTC+0000
00000000022df020 smss.exe 376       4       0x0a940020 2010-10-29 17:08:53 UTC+0000
```

Offset(P)	Name	PID	PPID	PBD	Time\C	Time\E
0x0000000001e0cda0	cmd.exe	968	1664	0x0a9403a0	2011-06-03 04:31:35 UTC+0000	2011-06-03 04:31:36 UTC+0000
0x0000000002114938	ipconfig.exe	304	968	0x0a940380	2011-06-03 04:31:35 UTC+0000	2011-06-03 04:31:36 UTC+0000

- 4) *volatility -f stuxnet.vmem --profile = WinXPSP2x86 dlllist*, What is load count for static and dynamic DLL load in the output of the above command and how is it controlled?

```

Volatility Foundation Volatility Framework 2.6
*****
System pid: 4
Unable to read PEB for task.
*****
ss.exe pid: 376
Command line : \SystemRoot\System32\smss.exe
*****
Base      Size      LoadCount  LoadTime      Path
-----
0x48580000 0xf000      0xffff        0x00000000      \SystemRoot\System32\smss.exe
0x7c900000 0xaf000     0xffff        0x00000000      C:\WINDOWS\system32\ntdll.dll
*****
csrss.exe pid: 600
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:
UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
Service Pack 3
*****
Base      Size      LoadCount  LoadTime      Path
-----
0x4a800000 0x5000      0xffff        0x00000000      \??\C:\WINDOWS\system32\csrss.exe
0x7c900000 0xaf000     0xffff        0x00000000      C:\WINDOWS\system32\ntdll.dll
0x75b40000 0xb000      0xffff        0x00000000      C:\WINDOWS\system32\CSRSRV.dll
0x75b50000 0x10000     0x3           0x00000000      C:\WINDOWS\system32\basesrv.dll
0x75b60000 0x40000     0x2           0x00000000      C:\WINDOWS\system32\winsrv.dll
*****
0x77e70000 0x92000     0xffff        0x00000000      C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000 0x11000     0xffff        0x00000000      C:\WINDOWS\system32\Secur32.dll
0x77c10000 0x58000     0xffff        0x00000000      C:\WINDOWS\system32\msvcrt.dll
0x5f770000 0xc000      0xffff        0x00000000      C:\WINDOWS\system32\NCOBJAPI.dll
0x76080000 0x65000     0xffff        0x00000000      C:\WINDOWS\system32\MSVCP60.dll
0x7dbd0000 0x51000     0xffff        0x00000000      C:\WINDOWS\system32\SCESRV.dll
0x776c0000 0x12000     0xffff        0x00000000      C:\WINDOWS\system32\AUTHZ.dll
0x7e410000 0x91000     0xffff        0x00000000      C:\WINDOWS\system32\USER32.dll
0x77f10000 0x49000     0xffff        0x00000000      C:\WINDOWS\system32\GDI32.dll
0x769c0000 0xb4000     0xffff        0x00000000      C:\WINDOWS\system32\USERENV.dll
0x7dba0000 0x21000     0xffff        0x00000000      C:\WINDOWS\system32\umpnpmgr.dll
0x76360000 0x10000     0xffff        0x00000000      C:\WINDOWS\system32\WINSTA.dll
0x5b860000 0x55000     0xffff        0x00000000      C:\WINDOWS\system32\NETAPI32.dll
0x5cb70000 0x26000     0x1           0x00000000      C:\WINDOWS\system32\ShimEng.dll
0x47260000 0xf000      0x1           0x00000000      C:\WINDOWS\AppPatch\AcAdProc.dll
0x77b40000 0x22000     0x2           0x00000000      C:\WINDOWS\system32\Apphelp.dll
0x77c00000 0x8000      0x4           0x00000000      C:\WINDOWS\system32\VERSION.dll
0x77b70000 0x11000     0x1           0x00000000      C:\WINDOWS\system32\eventlog.dll
0x76bf0000 0xb000      0x3           0x00000000      C:\WINDOWS\system32\PSAPI.dll
0x71ab0000 0x17000     0xb           0x00000000      C:\WINDOWS\system32\WS2_32.dll
0x71aa0000 0x8000      0x9           0x00000000      C:\WINDOWS\system32\WS2HELP.dll
0x76f50000 0x8000      0x1           0x00000000      C:\WINDOWS\system32\wtsapi32.dll
0x76c30000 0x2e000     0x1           0x00000000      C:\WINDOWS\system32\WINTRUST.dll
0x77a80000 0x95000     0x4           0x00000000      C:\WINDOWS\system32\CRYPT32.dll
0x77b20000 0x12000     0x5           0x00000000      C:\WINDOWS\system32\MSASN1.dll
0x76c90000 0x28000     0x2           0x00000000      C:\WINDOWS\system32\IMAGEHLP.dll
0x81a20000 0x2c5000    0x1           0x00000000      C:\WINDOWS\system32\xpsp2res.dll
*****
0x73d70000 0x50000     0x1           0x00000000      C:\WINDOWS\system32\Oxtheme.dll
0x773d0000 0x103000    0x2           0x00000000      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b641
ctl32.dll
*****
0x5d090000 0x9a000     0x1           0x00000000      C:\WINDOWS\system32\comctl32.dll
0x76a80000 0x64000     0x1           0x00000000      C:\WINDOWS\system32\RPCSS.dll
0x71ab0000 0x17000     0x18          0x00000000      C:\WINDOWS\system32\WS2_32.dll
0x71aa0000 0x8000      0x1a          0x00000000      C:\WINDOWS\system32\WS2HELP.dll
0x700670000 0x2c5000    0x1           0x00000000      C:\WINDOWS\system32\xpsp2res.dll
0x76800000 0x36000     0x1           0x00000000      C:\WINDOWS\system32\rsaenh.dll
0x71a50000 0x3f000     0x5           0x00000000      C:\WINDOWS\system32\mswsock.dll
0x662b0000 0x58000     0x1           0x00000000      C:\WINDOWS\system32\hnetcfg.dll
0x71a90000 0x8000      0x1           0x00000000      C:\WINDOWS\system32\wshtcpip.dll
0x76f20000 0x27000     0x4           0x00000000      C:\WINDOWS\system32\DNSAPI.dll
0x76d60000 0x19000     0x3           0x00000000      C:\WINDOWS\system32\iphlpapi.dll
0x76fb0000 0x8000      0x1           0x00000000      C:\WINDOWS\system32\winnr.dll
0x76f60000 0x2c000     0x1           0x00000000      C:\WINDOWS\system32\WLDAP32.dll
0x76fc0000 0x6000      0x1           0x00000000      C:\WINDOWS\system32\rasadhlp.dll
0x76fd0000 0x7f000     0x2           0x00000000      C:\WINDOWS\system32\CLBCATQ.DLL
0x77050000 0xc5000     0x2           0x00000000      C:\WINDOWS\system32\COMRes.dll
0x00d00000 0x138000    0x1           0x00000000      C:\WINDOWS\system32\KERNEL32.DLL.ASLR.0360c8ee
0x5b860000 0x55000     0x2           0x00000000      C:\WINDOWS\system32\NETAPI32.dll
0x76bf0000 0xb000      0x2           0x00000000      C:\WINDOWS\system32\PSAPI.dll
0x771b0000 0xaa000     0x2           0x00000000      C:\WINDOWS\system32\WININET.dll
0x77a80000 0x95000     0x2           0x00000000      C:\WINDOWS\system32\CRYPT32.dll
0x77b20000 0x12000     0x2           0x00000000      C:\WINDOWS\system32\MSASN1.dll
0x71ad0000 0x9000      0x2           0x00000000      C:\WINDOWS\system32\WSOCK32.dll
*****

```


5) *volatility -f stuxnet.vmem --profile = WinXPSP2x86 dlllist -p 1928, Provide the output of the previous command.*

```

root@fcs-security-attacker:~/Desktop/stuxnet.vmem# volatility -f stuxnet.vmem --profile=WinXPSP2x86 dlllist -p 1928
Volatility Foundation Volatility Framework 2.6
*****
lsass.exe pid: 1928
Command line : "C:\WINDOWS\system32\lsass.exe"
Service Pack 3
*****
Use Size LoadCount LoadTime Path
-----
0x01000000 0x6000 0xffff C:\WINDOWS\system32\lsass.exe
0x7c900000 0xaf000 0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000 0xf6000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000 0x9b000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000 0x92000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000 0x11000 0xffff C:\WINDOWS\system32\Secur32.dll
0x7e410000 0x91000 0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000 0x49000 0xffff C:\WINDOWS\system32\GDI32.dll
0x00870000 0x138000 0x1 C:\WINDOWS\system32\KERNEL32.DLL.ASLR.0360b7ab
0x76f20000 0x27000 0x2 C:\WINDOWS\system32\DNSAPI.dll
0x77c10000 0x58000 0x27 C:\WINDOWS\system32\msvcrt.dll
0x71ab0000 0x17000 0xa C:\WINDOWS\system32\WS2_32.dll
0x71aa0000 0x8000 0x8 C:\WINDOWS\system32\WS2HELP.dll
0x76d60000 0x19000 0x2 C:\WINDOWS\system32\IPHLPAPI.DLL
0x5b860000 0x55000 0x2 C:\WINDOWS\system32\NETAPI32.dll
0x774e0000 0x13d000 0x5 C:\WINDOWS\system32\ole32.dll
0x77120000 0x8b000 0x4 C:\WINDOWS\system32\OLEAUT32.dll
0x77120000 0x8b000 0x4 C:\WINDOWS\system32\OLEAUT32.dll
0x76bf0000 0xb000 0x2 C:\WINDOWS\system32\PSAPI.DLL
0x7c9c0000 0x817000 0x2 C:\WINDOWS\system32\SHELL32.dll
0x77f60000 0x76000 0x8 C:\WINDOWS\system32\SHLWAPI.dll
0x769c0000 0xb4000 0x2 C:\WINDOWS\system32\USERENV.dll
0x77c00000 0x8000 0x2 C:\WINDOWS\system32\VERSION.dll
0x771b0000 0xaa000 0x2 C:\WINDOWS\system32\WININET.dll
0x77a80000 0x95000 0x2 C:\WINDOWS\system32\CRYPT32.dll
0x77b20000 0x12000 0x2 C:\WINDOWS\system32\MSASN1.dll
0x771ad0000 0x9000 0x2 C:\WINDOWS\system32\WSOCK32.dll
0x773d0000 0x103000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000 0x9a000 0x1 C:\WINDOWS\system32\comctl32.dll
root@fcs-security-attacker:~/Desktop/stuxnet.vmem#

```

6) *volatility -f stuxnet.vmem --profile = WinXPSP2x86 pstree | egrep*

'(services.exe|lsass.exe|winlogon.exe)' | tee pstree.txt , Provide the output of the previous command

```

root@fcs-security-attacker:~/Desktop/stuxnet.vmem# volatility -f stuxnet.vmem --profile=WinXPSP2x86 pstree | egrep '(services.exe|lsass.exe|winlogon.exe)' | tee pstree.txt
Volatility Foundation Volatility Framework 2.6
.. 0x81da5650:winlogon.exe 624 376 19 570 2010-10-29 17:08:54 UTC+0000
... 0x82073020:services.exe 668 624 21 431 2010-10-29 17:08:54 UTC+0000
... 0x81c47c00:lsass.exe 1928 668 4 65 2011-06-03 04:26:55 UTC+0000
... 0x81c498c8:lsass.exe 868 668 2 23 2011-06-03 04:26:55 UTC+0000
... 0x81e70020:lsass.exe 680 624 19 342 2010-10-29 17:08:54 UTC+0000
root@fcs-security-attacker:~/Desktop/stuxnet.vmem#

```

- 7) *volatility -f stuxnet.vmem --profile = WinXPSP2x86 sockets | egrep '(Off|---[680|1928|868])' | tee sockets.txt*, Provide the output of the previous command.

```
root@fcs-security-attacker:~/Desktop/stuxnet.vmem# volatility -f stuxnet.vmem --profile=WinXPSP2x86 sockets | egrep '(Off|---[680|1928|868])' | tee sockets.txt
Volatility Foundation Volatility Framework 2.6
Offset(V)  PID  Port  Proto Protocol  Address  Create Time
-----
0x81dc2008  680  500   17  UDP         0.0.0.0  2010-10-29 17:09:05 UTC+0000
0x81da4d18  680   0    255 Reserved  0.0.0.0  2010-10-29 17:09:05 UTC+0000
0x82060008  680  4500  17  UDP         0.0.0.0  2010-10-29 17:09:05 UTC+0000
```

- 8) *volatility -f stuxnet.vmem --profile = WinXPSP2x86 dlllist -p 1928 2 >/dev/null | wc -l*

```
root@fcs-security-attacker:~/Desktop/stuxnet.vmem# volatility -f stuxnet.vmem --profile=WinXPSP2x86 dlllist -p 1928 2>/dev/null | wc -l
35
```

volatility -f stuxnet.vmem --profile = WinXPSP2x86 dlllist -p 868 2 >/dev/null | wc -

```
root@fcs-security-attacker:~/Desktop/stuxnet.vmem# volatility -f stuxnet.vmem --profile=WinXPSP2x86 dlllist -p 868 2>/dev/null | wc -l
15
```

volatility -f stuxnet.vmem --profile = WinXPSP2x86 dlllist -p 680 2 >/dev/null | wc -l

```
root@fcs-security-attacker:~/Desktop/stuxnet.vmem# volatility -f stuxnet.vmem --profile=WinXPSP2x86 dlllist -p 680 2>/dev/null | wc -l
64
```

9) *volatility -f stuxnet.vmem --profile = WinXPSP2x86 malfind -p 1928*

```
root@fcs-security-attacker:~/Desktop/stuxnet.vmem# volatility -f stuxnet.vmem --profile=WinXPSP2x86 malfind -p 1928
Volatility Foundation Volatility Framework 2.6
Process: lsass.exe Pid: 1928 Address: 0x80000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x00000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x00000010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 .....

0x00000000 4d          DEC EBP
0x00000001 5a          POP EDX
0x00000002 90          NOP
0x00000003 0003       ADD [EBX], AL
0x00000005 0000       ADD [EAX], AL
0x00000007 000400     ADD [EAX+EAX], AL
0x0000000a 0000       ADD [EAX], AL
0x0000000c ff         DB 0xff
0x0000000d ff00      INC DWORD [EAX]
0x0000000f 00b800000000 ADD [EAX+0x0], BH
0x00000015 0000       ADD [EAX], AL
0x00000017 004000     ADD [EAX+0x0], AL
0x0000001a 0000       ADD [EAX], AL
0x0000001c 0000       ADD [EAX], AL
0x0000001e 0000       ADD [EAX], AL
0x00000020 0000       ADD [EAX], AL
0x00000022 0000       ADD [EAX], AL
0x00000024 0000       ADD [EAX], AL
0x00000026 0000       ADD [EAX], AL
0x00000028 0000       ADD [EAX], AL
0x0000002a 0000       ADD [EAX], AL
0x0000002c 0000       ADD [EAX], AL
```

```
0x01000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x01000010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x01000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x01000030 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 .....

0x01000000 4d          DEC EBP
0x01000001 5a          POP EDX
0x01000002 90          NOP
0x01000003 0003       ADD [EBX], AL
0x01000005 0000       ADD [EAX], AL
0x01000007 000400     ADD [EAX+EAX], AL
0x0100000a 0000       ADD [EAX], AL
0x0100000c ff         DB 0xff
0x0100000d ff00      INC DWORD [EAX]
0x0100000f 00b800000000 ADD [EAX+0x0], BH
0x01000015 0000       ADD [EAX], AL
0x01000017 004000     ADD [EAX+0x0], AL
0x0100001a 0000       ADD [EAX], AL
0x0100001c 0000       ADD [EAX], AL
0x0100001e 0000       ADD [EAX], AL
0x01000020 0000       ADD [EAX], AL
0x01000022 0000       ADD [EAX], AL
0x01000024 0000       ADD [EAX], AL
0x01000026 0000       ADD [EAX], AL
0x01000028 0000       ADD [EAX], AL
0x0100002a 0000       ADD [EAX], AL
0x0100002c 0000       ADD [EAX], AL
```

```
Process: lsass.exe Pid: 1928 Address: 0x6f0000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x006f0000 29 87 7f ae 00 00 00 00 ff ff ff ff 77 35 00 01 .....w5..
0x006f0010 4b 00 45 00 52 00 4e 00 45 00 4c 00 33 00 32 00 .....K.E.R.N.E.L.3.2.
0x006f0020 2e 00 44 00 4c 00 4c 00 2e 00 41 00 53 00 4c 00 .....D.L.L.A.S.L.
0x006f0030 52 00 2e 00 30 00 33 00 36 00 30 00 62 00 37 00 .....R..0.3.6.0.b.7.

0x006f0000 29877fae0000 SUB [EDI+0xae7f], EAX
0x006f0006 0000       ADD [EAX], AL
0x006f0008 ff         DB 0xff
0x006f0009 ff         DB 0xff
0x006f000a ff         DB 0xff
0x006f000b ff7735     PUSH DWORD [EDI+0x35]
0x006f000e 0001       ADD [ECX], AL
0x006f0010 4b         DEC EBX
0x006f0011 004500     ADD [EBP+0x0], AL
0x006f0014 52         PUSH EDX
0x006f0015 004e00     ADD [ESI+0x0], CL
0x006f0018 45         INC EBP
0x006f0019 004c0033   ADD [EAX+EAX+0x33], CL
0x006f001d 0032       ADD [EDX], DH
0x006f001f 002e       ADD [ESI], CH
0x006f0021 0044004c   ADD [EAX+EAX+0x4c], AL
0x006f0025 004c002e   ADD [EAX+EAX+0x2e], CL
0x006f0029 004100     ADD [ECX+0x0], AL
```



```

Process: lsass.exe Pid: 868 Address: 0x10000000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 2, Protection: 6

0x01000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x01000010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x01000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x01000030 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 .....

0x01000000 4d DEC EBP
0x01000001 5a POP EDI
0x01000002 90 NOP
0x01000003 0003 ADD [EBX], AL
0x01000005 0000 ADD [EAX], AL
0x01000007 000400 ADD [EAX+EAX], AL
0x0100000a 000000 ADD [EAX], AL
0x0100000c ff DB 0xff
0x0100000d ff00 INC DWORD [EAX]
0x0100000f 00b80000000000 ADD [EAX+0x0], BH
0x01000015 0000 ADD [EAX], AL
0x01000017 00400000 ADD [EAX+0x0], AL
0x0100001a 0000 ADD [EAX], AL
0x0100001c 0000 ADD [EAX], AL
0x0100001e 0000 ADD [EAX], AL
0x01000020 0000 ADD [EAX], AL
0x01000022 0000 ADD [EAX], AL

```

```

root@kali:~# security-attacker -D Desktop/stuxnet_vmm# volatility -f stuxnet_vmm --profile=WinXPSP2x86 malfind -p 868
Volatility Foundation Volatility Framework 2.6
Process: lsass.exe Pid: 868 Address: 0x00000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6
# Staged
0x00000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x00000010 1b 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 .....
#
0x00000000 4d mems      DEC EBP
0x00000001 5a      POP EDX
0x00000002 90      NOP
0x00000003 0003     ADD [EBX], AL
0x00000005 0000     ADD [EAX], AL
0x00000007 000400    ADD [EAX+EAX], AL
0x00000009 0000     ADD [EAX], AL
0x0000000c ff 05     DB 0xff
0x0000000d ff00    INC DWORD [EAX]
0x0000000f 00b300000000 ADD [EAX+0x0], BH
0x00000015 0000     ADD [EAX], AL
0x00000017 004000    ADD [EAX+0x0], AL
0x0000001a 0000     ADD [EAX], AL
0x0000001c 0000 HomeDir  ADD [EAX], AL
0x0000001e 0000     ADD [EAX], AL
0x00000020 0000 calons     ADD [EAX], AL
0x00000022 0000     ADD [EAX], AL
0x00000024 0000     ADD [EAX], AL
0x00000026 0000     ADD [EAX], AL

```



```

0x00000028 0000 Home ADD [EAX], AL
0x0000002a 0000 ADD [EAX], AL
0x0000002c 0000 ADD [EAX], AL
0x0000002e 0000 ADD [EAX], AL
0x00000030 0000 ADD [EAX], AL
0x00000032 0000 ADD [EAX], AL
0x00000034 0000 ADD [EAX], AL
0x00000036 0000 ADD [EAX], AL
0x00000038 0000 ADD [EAX], AL
0x0000003a 0000 ADD [EAX], AL
0x0000003c 0001 OR [ECX], AL
0x0000003e 0000 ADD [EAX], AL

Process: lsass.exe Pid: 868 Address: 0x1000000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 2, Protection: 6

0x01000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x01000010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x01000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x01000030 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 .....

0x01000000 4d5h DEC EBP
0x01000001 5a POP EDX
0x01000002 90CS-HomeDir NOP
0x01000003 0003 ADD [EBX], AL
0x01000005 0000 ADD [EAX], AL
0x01000007 000400 ADD [EAX+EAX], AL
0x0100000a 0000 ADD [EAX], AL
0x0100000c ff DB 0xff

0x01000020 0000 RRS ADD [EAX], AL
0x01000022 0000 ADD [EAX], AL
0x01000024 0000 RRR ADD [EAX], AL
0x01000026 0000 ADD [EAX], AL
0x01000028 0000 ADD [EAX], AL
0x0100002a 0000 ADD [EAX], AL
0x0100002c 0000 ADD [EAX], AL
0x0100002e 0000 ADD [EAX], AL
0x01000030 0000 ADD [EAX], AL
0x01000032 0000 ADD [EAX], AL
0x01000034 0000 ADD [EAX], AL
0x01000036 0000 ADD [EAX], AL
0x01000038 0000 ADD [EAX], AL
0x0100003a 0000 -HomeDir ADD [EAX], AL
0x0100003c d000 ROL BYTE [EAX], 0x1
0x0100003e 0000 locations ADD [EAX], AL

```

volatility -f stuxnet.vmem --profile =
WinXPSP2x86 malfind -p 680

```

root@fcs-security-attacker:~/Desktop/stuxnet.vmem# volatility -f stuxnet.vmem --profile=WinXPSP2x86 malfind -p 680
Volatility Foundation Volatility Framework 2.6

```

10) Explain the hook injection technique and briefly explain how volatility can be applied to detect malicious hooks.

Hook injection describes a way to load malware that takes advantage of Windows hooks, which are used to intercept messages destined for applications. Malware authors can use hook injection to accomplish two things: To be sure that malicious code will run whenever a particular message is intercepted, to be sure that a particular DLL will be loaded in a victim process's memory space. users generate events that are sent to the OS, which then sends messages created by those events to threads registered to receive them. The right side of the figure shows one way that an attacker can insert a malicious DLL to intercept messages.

The plugin dlllist in the Volatility Framework can also be used to list all DLLs for a given process in memory and find DLLs injected with the CreateRemoteThread and LoadLibrary technique. This technique does not hide the DLL and therefore will not be detected by the plugin malfind. The first command well use is the malfind command. This command is used to find injected code inside the processes memory. It does this by looking for sections of allocated memory (by looking at the VAD tree data structure) and checking if they have hints of executable code that are not mapped to any file on the disk