

# Black energy assignment

Youssef sherif

20221041587

Question one

```
(kali@kali)-[~/volatility3]
$ python vol.py -f CYBERDEF-567078-20230213-171333.raw windows.info
Volatility 3 Framework 2.7.0
Progress: 100.00 PDB scanning finished
Variable      Value
Kernel Base   0x804d7000
DTB           0x39000
Symbols file:  ///home/kali/volatility3/volatility3/symbols/windows/ntoskrnl.pdb/47A5AC97343A4A7ABF14EFD9E9933772-2.json.xz
Is64Bit       False
IsPAE         False
layer_name    0 WindowsIntel
memory_layer  1 FileLayer
KdDebuggerDataBlock 0x8054cde0
NTBuildLab    2600.xpsp.080413-2111
CSDVersion    3
KdVersionBlock 0x8054cdb8
Major/Minor   15.2600
MachineType   332
KeNumberProcessors 1
SystemTime    2023-02-13 18:29:11
NtSystemRoot  C:\WINDOWS
NtProductType NtProductWinNt
NtMajorVersion 5
NtMinorVersion 1
PE_MajorOperatingSystemVersion 5
PE_MinorOperatingSystemVersion 1
PE_Machine     332
PE_TimeDateStamp Sun Apr 13 19:27:39 2008
```

Asking chatgpt

- **Kernel Base:** `0x804d7000`
- **Is64Bit:** `False` (indicating a 32-bit system)
- **IsPAE:** `False` (indicating a system without Physical Address Extension)
- **NtMajorVersion:** `5`
- **NtMinorVersion:** `1`
- **MachineType:** `332` (which corresponds to x86)

The `NtMajorVersion` and `NtMinorVersion` values indicate the Windows version:

- `NtMajorVersion`: 5 corresponds to Windows XP
- `NtMinorVersion`: 1 indicates the service pack level (in this case, Windows XP SP3)

Given these details, the appropriate Volatility profile for this memory dump appears to be `WinXPSP3x86`. This profile is designed to handle Windows XP Service Pack 3 (32-bit) systems.

But we will change 3x86 to 2x86

Q1 Which volatility profile would be best for this machine?

Weight : 0 | Solved : 1445 | Average Solve Time: 6min

WinXPSP2x86

## Question two

```
(kali@kali) [~/volatility3]
$ python vol.py -f CYBERDEF-567078-20230213-171333.raw windows.pslist
```

Volatility 3 Framework 2.7.0  
Progress: 100.00 PDB scanning finished

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0x89c037f8	55	245	N/A	False	N/A	Disabled	
368	4	smss.exe	0x89965020	3	19	N/A	False	2023-02-14 04:54:15.000000	N/A	Disabled
592	368	csrss.exe	0x89a98da0	11	321	0	False	2023-02-14 04:54:15.000000	N/A	Disabled
616	368	winlogon.exe	0x89a88da0	18	508	0	False	2023-02-14 04:54:15.000000	N/A	Disabled
660	616	services.exe	0x89938998	15	240	0	False	2023-02-14 04:54:15.000000	N/A	Disabled
672	616	lsass.exe	0x89aa0020	21	335	0	False	2023-02-14 04:54:15.000000	N/A	Disabled
832	660	VBoxService.exe	0x89aaa3d8	9	115	0	False	2023-02-14 04:54:15.000000	N/A	Disabled
880	660	svchost.exe	0x89aab590	21	295	0	False	2023-02-13 17:54:16.000000	N/A	Disabled
968	660	svchost.exe	0x89a9f6f8	10	244	0	False	2023-02-13 17:54:17.000000	N/A	Disabled
1060	660	svchost.exe	0x89730da0	51	1072	0	False	2023-02-13 17:54:17.000000	N/A	Disabled
1108	660	svchost.exe	0x897289a8	5	78	0	False	2023-02-13 17:54:17.000000	N/A	Disabled
1156	660	svchost.exe	0x899aadda0	13	192	0	False	2023-02-13 17:54:17.000000	N/A	Disabled
1484	1440	explorer.exe	0x89733938	14	489	0	False	2023-02-13 17:54:18.000000	N/A	Disabled
1608	660	spoolsv.exe	0x897075d0	10	106	0	False	2023-02-13 17:54:18.000000	N/A	Disabled
480	1060	wscntfy.exe	0x89694388	1	28	0	False	2023-02-13 17:54:30.000000	N/A	Disabled
540	660	alg.exe	0x8969d2a0	5	102	0	False	2023-02-13 17:54:30.000000	N/A	Disabled
376	1484	VBoxTray.exe	0x89982da0	13	125	0	False	2023-02-13 17:54:30.000000	N/A	Disabled
636	1484	msmsgs.exe	0x8994a020	2	157	0	False	2023-02-13 17:54:30.000000	N/A	Disabled
1380	1484	taskmgr.exe	0x89a0b2f0	0	-	0	False	2023-02-13 18:25:15.000000	2023-02-13 18:26:21.000000	Disabled
964	1484	rootkit.exe	0x899dd740	0	-	0	False	2023-02-13 18:25:26.000000	2023-02-13 18:25:26.000000	Disabled
1960	964	cmd.exe	0x89a18da0	0	-	0	False	2023-02-13 18:25:26.000000	2023-02-13 18:25:26.000000	Disabled
528	1484	notepad.exe	0x896c5020	0	-	0	False	2023-02-13 18:26:55.000000	2023-02-13 18:27:46.000000	Disabled
1432	1484	notepad.exe	0x89a0d180	0	-	0	False	2023-02-13 18:28:25.000000	2023-02-13 18:28:40.000000	Disabled
1444	1484	notepad.exe	0x899e6da0	0	-	0	False	2023-02-13 18:28:42.000000	2023-02-13 18:28:47.000000	Disabled
276	1484	DumpIt.exe	0x89a0fda0	1	25	0	False	2023-02-13 18:29:08.000000	N/A	Disabled

Q2 How many processes were running when the image was acquired?

Weight : 0 | Solved : 1395 | Average Solve Time: 32min

19

Count only the process with the NA field because exit-time column indicates the terminated process that has a time that means the process has ended

## Question three

480	1060	wscntfy.exe	0x89694388	1	28	0	False	2023-02-13 17:54:30.000000	N/A	Disabled
540	660	alg.exe	0x8969d2a0	5	102	0	False	2023-02-13 17:54:30.000000	N/A	Disabled
376	1484	VBoxTray.exe	0x89982da0	13	125	0	False	2023-02-13 17:54:30.000000	N/A	Disabled
636	1484	msmsgs.exe	0x8994a020	2	157	0	False	2023-02-13 17:54:30.000000	N/A	Disabled
1880	1484	taskmgr.exe	0x89a0b2f0	0	-	0	False	2023-02-13 18:25:15.000000	2023-02-13 18:26:21.000000	Disabled
964	1484	rootkit.exe	0x899dd740	0	-	0	False	2023-02-13 18:25:26.000000	2023-02-13 18:25:26.000000	Disabled
1960	964	cmd.exe	0x89a18da0	0	-	0	False	2023-02-13 18:25:26.000000	2023-02-13 18:25:26.000000	Disabled

Q3 What is the process ID of cmd.exe?

Weight : 0 | Solved : 1466 | Average Solve Time: 1min

1960

Question four

Using pstree command

```
(kali@kali) ~/volatility3
python vol.py -f CYBERDEF-567078-20230213-171333.raw windows.pstree

Volatility 3 Framework 2.7.0
Progress: 100.00 PDB scanning finished

PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime Audit Cmd Path
4 0 System 0x89c037f8 55 245 3 N/A False N/A N/A - - - \Device\HarddiskVolume1\WINDOWS\system32\smss.exe \SystemRoot\System32\smss.exe \SystemRoot\System32\
* 368 4 smss.exe 0x89965020 3 19 N/A False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\csrss.exe C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Wind
** 592 368 csrss.exe 0x89a98da0 11 321 0 False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\csrss.exe C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Wind
dSection=1024,3072,512 Windows-On SubSystemType=Windows ServerDll=baserv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16 \??\C:\WINDO
m32\csrss.exe
** 616 368 winlogon.exe 0x89a88da0 18 508 0 False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\winlogon.exe winlogon.exe \??\C:\WINDOWS\system32\winlogon.exe
** 672 616 lsass.exe 0x89aa0020 21 335 0 False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe C:\WINDOWS\system32\lsass.exe C:\WINDOWS\system32\
e
** 660 616 services.exe 0x89938998 15 240 0 False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\services.exe C:\WINDOWS\system32\services.exe C:\WINDOWS\s
services.exe
**** 832 660 VBoxService.exe 0x89aaa3d8 9 115 0 False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\VBoxService.exe C:\WINDOWS\System32\VBoxService.exe
INDOWS\System32\VBoxService.exe
**** 1060 660 svchost.exe 0x89730da0 51 1072 0 False 2023-02-13 17:54:17.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe C:\WINDOWS\System32\svchost.exe -k netsvcs
INDOWS\System32\svchost.exe
**** 480 1060 wscntfy.exe 0x89694388 1 28 0 False 2023-02-13 17:54:30.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\wscntfy.exe C:\WINDOWS\system32\wscntfy.exe C:\WINDOWS\s
wscntfy.exe
**** 1156 660 svchost.exe 0x899adda0 13 192 0 False 2023-02-13 17:54:17.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServ
INDOWS\System32\svchost.exe
**** 968 660 svchost.exe 0x89a9f6f8 10 244 0 False 2023-02-13 17:54:17.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe C:\WINDOWS\system32\svchost.exe -k rpcss C:\W
ystem32\svchost.exe
**** 1608 660 spoolsv.exe 0x897075d0 10 106 0 False 2023-02-13 17:54:18.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\spoolsv.exe C:\WINDOWS\system32\spoolsv.exe C:\WINDOWS\s
spoolsv.exe
**** 880 660 svchost.exe 0x89aab590 21 295 0 False 2023-02-13 17:54:16.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch
INDOWS\System32\svchost.exe
**** 1108 660 svchost.exe 0x897289a8 5 78 0 False 2023-02-13 17:54:17.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe C:\WINDOWS\system32\svchost.exe -k NetworkSe
:WINDOWS\system32\svchost.exe
**** 540 660 alg.exe 0x8969d2a0 5 102 0 False 2023-02-13 17:54:30.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\alg.exe C:\WINDOWS\System32\alg.exe C:\WINDOWS\System32\
1484 1440 explorer.exe 0x89733938 14 489 0 False 2023-02-13 17:54:18.000000 N/A \Device\HarddiskVolume1\WINDOWS\explorer.exe C:\WINDOWS\Explorer.EXE C:\WINDOWS\Explorer.EXE
* 964 1484 rootkit.exe 0x899dd740 0 - 0 False 2023-02-13 18:25:26.000000 2023-02-13 18:25:26.000000 \Device\HarddiskVolume1\Documents and Settings\CyberDefenders\Desktop\rootkit.exe
** 1960 964 cmd.exe 0x89a18da0 0 - 0 False 2023-02-13 18:25:26.000000 2023-02-13 18:25:26.000000 \Device\HarddiskVolume1\WINDOWS\system32\cmd.exe - -
```

Because it has cmd.exe as a child

Q4 What is the name of the most suspicious process?

Weight : 0 | Solved : 1461 | Average Solve Time: 1min

rootkit.exe

Question five

The combination of **PAGE\_EXECUTE\_READWRITE** protection and the presence of an executable header (**mz**) in memory indicates a potential code injection scenario. Code injection often involves modifying memory regions within legitimate processes to execute malicious code

```

880    svchost.exe    0x980000    0x988fff    VadS    PAGE_EXECUTE_READWRITE    9    1    Disabled    MZ header
4d 5a 90 00 03 00 00 00 MZ.....
04 00 00 00 ff ff 00 00 .....
b8 00 00 00 00 00 00 00 .....
40 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 f8 00 00 00 .....
                                4d 5a 90 00 03 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00

```

Using python vol.py -f CYBERDEF-567078-20230213-171333.raw windows.malfind

Q5 Which process shows the highest likelihood of code injection?

Weight : 0 | Solved : 1416 | Average Solve Time: 13min

svchost.exe

Question six

```

(kali@kali)~/volatility3
$ python vol.py -f CYBERDEF-567078-20230213-171333.raw -o /home/kali/Downloads windows.malfind --pid 880 --dump
Volatility 3 Framework 2.7.0
Progress: 100.00
PDB scanning finished
PID Process Start VPN End VPN Tag Protection CommitCharge PrivateMemory File output Notes Hexdump Disasm
880 svchost.exe 0x980000 0x988fff VadS PAGE_EXECUTE_READWRITE 9 1 pid.880.vad.0x980000-0x988fff.dmp MZ header
4d 5a 90 00 03 00 00 00 MZ.....
04 00 00 00 ff ff 00 00 .....
b8 00 00 00 00 00 00 00 .....
40 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 f8 00 00 00 .....
                                4d 5a 90 00 03 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00
00

```

Dump the process

Take the hash

```

(kali@kali)~/Downloads
$ md5sum pid.880.vad.0x980000-0x988fff.dmp
20020a9d850bd496954d8c21dfa614be pid.880.vad.0x980000-0x988fff.dmp

```

Check in virustotal

39 / 70

Community Score

39/70 security vendors and no sandboxes flagged this file as malicious

8638ab1e5f9ba4cffc66400d36d47f7805733fae828a0cace9421d0bd83eafa

process.0x89aab590.0x980000.dmp

pedll corrupt overlay checks-user-input detect-debug-environment

DETECTION

DETAILS

RELATIONS

BEHAVIOR


TELEMETRY

COMMUNITY 2

```
(kali㉿kali)-[~/Downloads]
$ strings -n 10 pid.880.vad.0x980000-0x988fff.dmp Kali NetHunter Exploit-Dr
!This program cannot be run in DOS mode.
Ht_HtGht1Ht
cmd.exe /C
{3D5A1694-CC2C-4ee7-A3D5-A879A9E3A623}
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
Content-Type: application/x-www-form-urlencoded
user32.dll
advapi32.dll
wininet.dll
ws2_32.dll
DispatchCommand
DispatchEvent
GetLastError
GetCurrentProcessId
ExitThread
CloseHandle
KERNEL32.dll
USER32.dll
CoCreateInstance
CoInitializeEx
OLEAUT32.dll
WS2_32.dll
InterlockedExchange
VirtualQuery
ConfAllocGetTextByNameA
ConfAllocGetTextByNameW
ConfGetListNodeByName
ConfGetNodeByName
ConfGetNodeTextA
ConfGetNodeTextW
ConfGetPlgNode
ConfGetRootNode
DownloadFile
PlgSendEvent
RkLoadKernelImage
RkProtectObject
SrvAddRequestBinaryData
SrvAddRequestStringData
?456789;;≤
!"#$%&'()*+,-./0123456789:;<=
xCYBERDEF-567078_40BF25D3
C:\WINDOWS\system32\drivers\str.sys
3L3\3b3r3|3
9>9E9N9T9t9y9
535B5M5e7v7
</=(>@>G>O>T>X>\>
```

Check the strings in the file

File can not run in dos mode means that the file is malicious and exexecutable file and contains macros

Q6  There is an odd file referenced in the recent process. Provide the full path of that file.


Weight : 0 | Solved : 1277 | Average Solve Time: 53min

C:\WINDOWS\system32\drivers\str.sys

### Question seven

```
└─$ python3 vol.py -f CYBERDEF-567078-20230213-171333.raw windows.ldrmodules --pid 880
Volatility 3 Framework 2.7.0
Progress: 100.00
PDB scanning finished
Pid Process Base InLoad InInit InMem MappedPath
880 svchost.exe 0x6f880000 True True True \WINDOWS\AppPatch\AcGenral.dll
880 svchost.exe 0x1000000 True False True \WINDOWS\system32\svchost.exe
880 svchost.exe 0x670000 True True True \WINDOWS\system32\xpsp2res.dll
880 svchost.exe 0x9a0000 False False False \WINDOWS\system32\msxml3r.dll
880 svchost.exe 0x5ad70000 True True True \WINDOWS\system32\uxtheme.dll
880 svchost.exe 0x5cb70000 True True True \WINDOWS\system32\shimeng.dll
880 svchost.exe 0x5b860000 True True True \WINDOWS\system32\netapi32.dll
880 svchost.exe 0x5d090000 True True True \WINDOWS\system32\comctl32.dll
880 svchost.exe 0x68000000 True True True \WINDOWS\system32\rsaenh.dll
880 svchost.exe 0x7c900000 True True True \WINDOWS\system32\ntdll.dll
880 svchost.exe 0x77dd0000 True True True \WINDOWS\system32\advapi32.dll
880 svchost.exe 0x76f60000 True True True \WINDOWS\system32\ldap32.dll
880 svchost.exe 0x76b40000 True True True \WINDOWS\system32\winmm.dll
880 svchost.exe 0x769c0000 True True True \WINDOWS\system32\userenv.dll
880 svchost.exe 0x71bf0000 True True True \WINDOWS\system32\saml.dll
880 svchost.exe 0x71ab0000 True True True \WINDOWS\system32\ws2_32.dll
880 svchost.exe 0x71aa0000 True True True \WINDOWS\system32\ws2help.dll
880 svchost.exe 0x71a50000 True True True \WINDOWS\system32\mswsock.dll
880 svchost.exe 0x71ad0000 True True True \WINDOWS\system32\wssock32.dll
880 svchost.exe 0x760f0000 True True True \WINDOWS\system32\termsrv.dll
880 svchost.exe 0x74f70000 True True True \WINDOWS\system32\icaapi.dll
880 svchost.exe 0x74980000 True True True \WINDOWS\system32\msxml3.dll
880 svchost.exe 0x722b0000 True True True \WINDOWS\system32\sensapi.dll
880 svchost.exe 0x75110000 True True True \WINDOWS\system32\mstlsapi.dll
880 svchost.exe 0x76a80000 True True True \WINDOWS\system32\rpcss.dll
880 svchost.exe 0x76b20000 True True True \WINDOWS\system32\atl.dll
880 svchost.exe 0x76c90000 True True True \WINDOWS\system32\imagehlp.dll
880 svchost.exe 0x76c30000 True True True \WINDOWS\system32\wintrust.dll
```

Msxml3r.dll the only process that has all inload, ininit and inmem all are false the three of them which indicates its hidden or maybe rootkit that trying to hide its presence

Q7  What is the name of the injected dll file loaded from the recent process?

Weight : 0 | Solved : 1257 | Average Solve Time: 41min

Msxml3r.dll



InLoad: Indicates if the DLL is loaded during the initial process load

InInit: Indicates if the DLL is initialized

InMem: Indicates if the DLL is currently in memory

Question eight

```
880      svchost.exe      0x980000
4d 5a 90 00 03 00 00 00 MZ.....
04 00 00 00 ff ff 00 00 .....
b8 00 00 00 00 00 00 00 .....
40 00 00 00 00 00 00 00 @.....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 f8 00 00 00 .....
```

Q8 ☒ What is the base address of the injected dll?

Weight : 0 | Solved : 1234 | Average Solve Time: 47min

0x980000