Black energy assignment

Youssef sherif

20221041587

Question one

```
-(<mark>kali⊛kali</mark>)-[~/volatility3]
$ python vol.py -f CYBERDEF-567078-20230213-171333.raw windows.info
Volatility 3 Framework 2.7.0
Progress: 100.00 PDB scanning finished
                    Value
                   0×804d7000
DTB 0×39000
Symbols file:///home/kali/volatility3/volatility3/symbols/windows/ntoskrnl.pdb/47A5AC97343A4A7ABF14EFD9E9933772-2.json.xz
Is64Bit False
IsPAE False
layer_name 0 WindowsInt
memory_layer 1 FileLayer
                    0 WindowsIntel
KdDebuggerDataBlock 0×8054cde0
                    2600.xpsp.080413-2111
NTBuildLab
CSDVersion
KdVersionBlock 0×8054cdb8
Major/Minor
MachineType
                  15.2600
332
KeNumberProcessors
SystemTime 2023-02-13 18:29:11
NtSystemRoot C:\WINDOWS
NtProductType NtProductWinNt
NtMajorVersion 5
NtMinorVersion 1
PE MajorOperatingSystemVersion 5
PE MinorOperatingSystemVersion
PE Machine
PE TimeDateStamp
                              Sun Apr 13 19:27:39 2008
```

Asking chatgpt

- Kernel Base: `0×804d7000`
- 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)

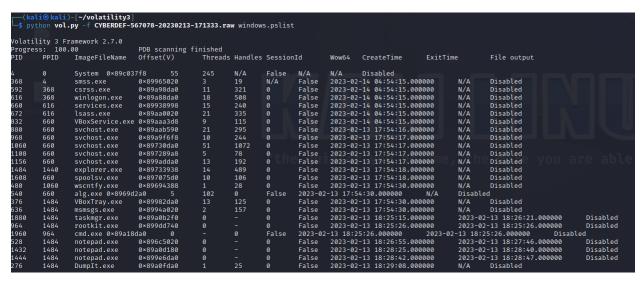
The 'NTMajorVersion' and 'NTMinorVersion' values indicate the Windows version:

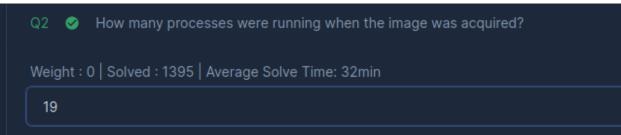
- `NTMajorVersion`: 5 corresponds to Windows XP
- * `NTMinorVersion`: 1 indicates the service pack level (in this case, Windows XP SP3)
- these details, the appropriate Volatility profile for this memory dump appears to be 'WinXPSP3×86'. This profile is designed to handle Windows XP Service Pack 3 (32-bit) systems.

But we will change 3x86 to 2x86



Question two





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

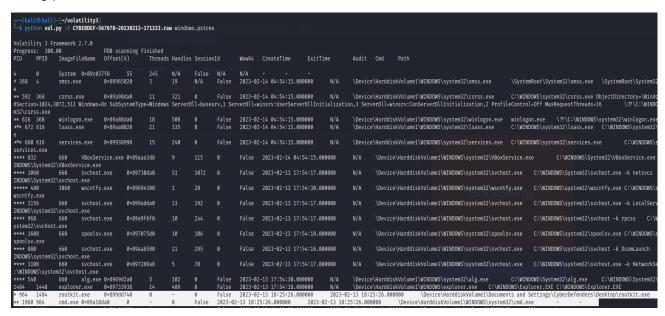
1000	000	Spootsv.cxc	007707340	10	100	•	racsc	2023 02 13 17.34.10.0	, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	N/ A	DIJUDICU	UDITIL	
480	1060	wscntfy.exe	0×89694388		28		False	2023-02-13 17:54:30.0	00000	N/A	Disabled		
540	660	alg.exe 0×8969	d2a0 5	102		False	2023-02	2-13 17:54:30.000000	N/A	Disable	d		0.70
376	1484	VBoxTray.exe	0×89982da0	13	125		False	2023-02-13 17:54:30.0	00000	N/A	Disabled		070
636	1484	msmsgs.exe	0×8994a020		157		False	2023-02-13 17:54:30.0	00000	N/A	Disabled		250
1880	1484	taskmgr.exe	0×89a0b2f0				False	2023-02-13 18:25:15.0	00000	2023-02	-13 18:26:21	.000000	Disabled
964	1484	rootkit.exe	0×899dd740				False	2023-02-13 18:25:26.0	00000	2023-02	-13 18:25:26	.000000	Disabled
1960	964	cmd.exe 0×89a1	8da0 0	-	0	False	2023-02	2-13 18:25:26.000000	2023-02	-13 18:2	5:26.000000	Disable	d

```
Q3  What is the process ID of cmd.exe?

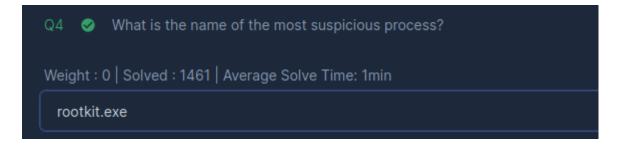
Weight: 0 | Solved: 1466 | Average Solve Time: 1min
```

Question four

Using pstree command



Because it has cmd.exe as a child



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	0×980000	0×988fff	VadS	PAGE_EXECUTE	_READWRITE	9	1	Disabled	MZ header	
4d 5a	90 00 03 00 00 00	0 MZ									
04 00	00 00 ff ff 00 00	0									
b8 00	0 00 00 00 00 00 00	0									
40 00	0 00 00 00 00 00 00	0 0									
00 00	0 00 00 00 00 00 00	0									
00 00	0 00 00 00 00 00 00	0									
00 00	0 00 00 00 00 00 00	0									
00 00	00 00 f8 00 00 00	0	4d 5a 90 00 0	3 00 00 00	0 04 00 00 00	ff ff 00 00) b8 0	0 00 00	00 00 00 00	40 00 00 00 00 00 00 0	00 00

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



Question six

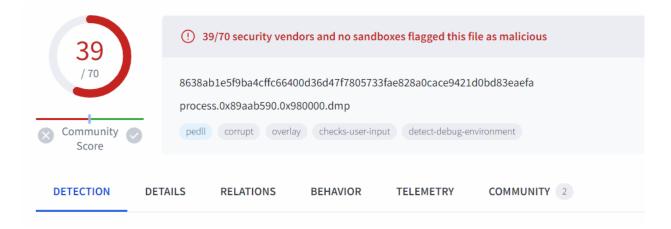
```
| Ckali@ kali | = \textstyle | Type | CyBERDEF - 567078 - 20230213 - 171333 \textstyle range | range |
```

Dump the process

Take the hash

```
(kali® kali)-[~/Downloads]
$ md5sum pid.880.vad.0×980000-0×988fff.dmp
20020a9d850bd496954d8c21dfa614be pid.880.vad.0×980000-0×988fff.dmp
```

Check in virustotal



```
-(kali®kali)-[~/Downloads]
 -$ strings -n 10 pid.880.vad.0×980000-0×988fff.dmp
!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
ConfGetNodeBvName
ConfGetNodeTextA
ConfGetNodeTextW
ConfGetPlgNode
ConfGetRootNode
DownloadFile
PlgSendEvent
RkLoadKernelImage
RkProtectObject
SrvAddRequestBinaryData
SrvAddRequestStringData
xCYBERDEF-567078_40BF25D3
C:\WINDOWS\system32\drivers\str.sys
3L3\3b3r3|3
9>9E9N9T9t9v9
535B5M5e7v7
</=(>@>G>0>T>X>\>
```

Check the strings in the file

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

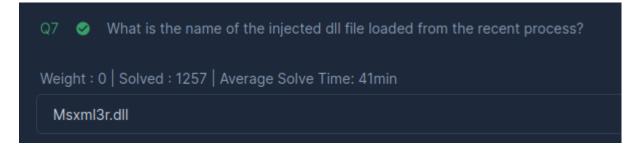
Weight: 0 | Solved: 1277 | Average Solve Time: 53min

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

Question seven

Volatility 3 Framework 2.7.0										
Progress: 100.00 PDB scanning finished										
Pid	Process Base	InLoad InInit	InMem	Mappedi	Path					
880	svchost.exe	0×6f880000	True	True	True	\WINDOWS\AppPatch\AcGenral.dll				
880	svchost.exe	0×1000000	True	False	True	\WINDOWS\system32\svchost.exe				
880	svchost.exe	0×670000	True	True	True	\WINDOWS\system32\xpsp2res.dll				
880	svchost.exe	0×9a0000	False	False	False	\WINDOWS\system32\msxml3r.dll				
880	svchost.exe	0×5ad70000	True	True	True	\WINDOWS\system32\uxtheme.dll				
880	svchost.exe	0×5cb70000	True	True	True	\WINDOWS\system32\shimeng.dll				
880	svchost.exe	0×5b860000	True	True	True	\WINDOWS\system32\netapi32.dll				
880	svchost.exe	0×5d090000	True	True	True	\WINDOWS\system32\comctl32.dll				
880	svchost.exe	0×68000000	True	True	True	\WINDOWS\system32\rsaenh.dll				
880	svchost.exe	0×7c900000	True	True	True	\WINDOWS\system32\ntdll.dll				
880	svchost.exe	0×77dd0000	True	True	True	\WINDOWS\system32\advapi32.dll				
880	svchost.exe	0×76f60000	True	True	True	\WINDOWS\system32\wldap32.dll				
880	svchost.exe	0×76b40000	True	True	True	\WINDOWS\system32\winmm.dll				
880	svchost.exe	0×769c0000	True	True	True	\WINDOWS\system32\userenv.dll				
880	svchost.exe	0×71bf0000	True	True	True	\WINDOWS\system32\samlib.dll				
880	svchost.exe	0×71ab0000	True	True	True	\WINDOWS\system32\ws2_32.dll				
880	svchost.exe	0×71aa0000	True	True	True	\WINDOWS\system32\ws2help.dll				
880	svchost.exe	0×71a50000	True	True	True	\WINDOWS\system32\mswsock.dll				
880	svchost.exe	0×71ad0000	True	True	True	\WINDOWS\system32\wsock32.dll				
880	svchost.exe	0×760f0000	True	True	True	\WINDOWS\system32\termsrv.dll				
880	svchost.exe	0×74f70000	True	True	True	\WINDOWS\system32\icaapi.dll				
880	svchost.exe	0×74980000	True	True	True	\WINDOWS\system32\msxml3.dll				
880	svchost.exe	0×722b0000	True	True	True	\WINDOWS\system32\sensapi.dll				
880	svchost.exe	0×75110000	True	True	True	\WINDOWS\system32\mstlsapi.dll				
880	svchost.exe	0×76a80000	True	True	True	\WINDOWS\system32\rpcss.dll				
880	svchost.exe	0×76b20000	True	True	True	\WINDOWS\system32\atl.dll				
880	svchost.exe	0×76c90000	True	True	True	\WINDOWS\system32\imagehlp.dll				
880	svchost.exe	0×76c30000	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



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

