BlackEnergy Challenge

Scenario:

A multinational corporation has been hit by a cyber attack that has led to the theft of sensitive data. The attack was carried out using a variant of the BlackEnergy v2 malware that has never been seen before. The company's security team has acquired a memory dump of the infected machine, and they want you, as a soc analyst, to analyze the dump to understand the attack scope and impact.

Task 1:
Which volatility profile would be best for this machine?

I used the imageinfo plugin

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/CYBERDEF-567078-20230213-171333.raw' imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/remnux/CYBERDEF-567078-20230213-171333.raw)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054cde0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2023-02-13 18:29:11 UTC+0000
     Image local date and time : 2023-02-13 10:29:11 -0800
```

Answer: WinXPSP2x86

Task 2:
How many processes were running when the image was acquired?

I used the pslist and counted the process without duplicates

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/CYBERDEF-567078-20230213-171333.raw' --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x89c037f8 System                    4      0     55      245 ------      0
0x89965020 smss.exe                368      4      3       19 ------      0 2023-02-14 04:54:15 UTC+0000
0x89a98da0 csrss.exe               592    368     11      321      0      0 2023-02-14 04:54:15 UTC+0000
0x89a88da0 winlogon.exe            616    368     18      508      0      0 2023-02-14 04:54:15 UTC+0000
0x89938998 services.exe            660    616     15      240      0      0 2023-02-14 04:54:15 UTC+0000
0x89aa0020 lsass.exe               672    616     21      335      0      0 2023-02-14 04:54:15 UTC+0000
0x89aaa3d8 VBoxService.exe         832    660      9      115      0      0 2023-02-14 04:54:15 UTC+0000
0x89aab590 svchost.exe             880    660     21      295      0      0 2023-02-13 17:54:16 UTC+0000
0x89a9f6f8 svchost.exe             968    660     10      244      0      0 2023-02-13 17:54:17 UTC+0000
0x89730da0 svchost.exe            1060    660     51     1072      0      0 2023-02-13 17:54:17 UTC+0000
0x897289a8 svchost.exe            1108    660      5       78      0      0 2023-02-13 17:54:17 UTC+0000
0x899adda0 svchost.exe            1156    660     13      192      0      0 2023-02-13 17:54:17 UTC+0000
0x89733938 explorer.exe           1484   1440     14      489      0      0 2023-02-13 17:54:18 UTC+0000
0x897075d0 spoolsv.exe            1608    660     10      106      0      0 2023-02-13 17:54:18 UTC+0000
0x89694388 wscntfy.exe             480   1060      1       28      0      0 2023-02-13 17:54:30 UTC+0000
0x8969d2a0 alg.exe                 540    660      5      102      0      0 2023-02-13 17:54:30 UTC+0000
0x89982da0 VBoxTray.exe            376   1484     13      125      0      0 2023-02-13 17:54:30 UTC+0000
0x8994a020 msmsgs.exe              636   1484      2      157      0      0 2023-02-13 17:54:30 UTC+0000
0x89a0b2f0 taskmgr.exe            1880   1484      0 --------      0      0 2023-02-13 18:25:15 UTC+0000   2023-02-13 18:26:21 UTC+0000
0x899dd740 rootkit.exe             964   1484      0 --------      0      0 2023-02-13 18:25:26 UTC+0000   2023-02-13 18:25:26 UTC+0000
0x89a18da0 cmd.exe                1960    964      0 --------      0      0 2023-02-13 18:25:26 UTC+0000   2023-02-13 18:25:26 UTC+0000
0x896c5020 notepad.exe             528   1484      0 --------      0      0 2023-02-13 18:26:55 UTC+0000   2023-02-13 18:27:46 UTC+0000
0x89a0d180 notepad.exe            1432   1484      0 --------      0      0 2023-02-13 18:28:25 UTC+0000   2023-02-13 18:28:40 UTC+0000
0x899e6da0 notepad.exe            1444   1484      0 --------      0      0 2023-02-13 18:28:42 UTC+0000   2023-02-13 18:28:47 UTC+0000
0x89a0fda0 DumpIt.exe              276   1484      1       25      0      0 2023-02-13 18:29:08 UTC+0000
```

Answer: 19

Task 3:
What is the process ID of cmd.exe?

Same like task 2

Answer: 1960

Task 4:
What is the name of the most suspicious process?

Same like task 2, rootki look suspicious

Answer: rootkit.exe

Task 5:
Which process shows the highest likelihood of code injection?

I used the malfind plugin and found the process

```
Process: svchost.exe Pid: 880 Address: 0x980000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 9, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000980000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x0000000000980010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x0000000000980020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000000000980030  00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00   ................
```

Answer: svchost.exe

Task 6:
There is an odd file referenced in the recent process. Provide the full path of that file.

I used the handles plugin on the PID 880 of the svchost.exe and saw some path with a file

```
0x89a00f90    880      0x33c   0x12019f File            \Device\{9DD6AFA1-8646-4720-836B-EDCB1085864A}
0x89af0cf0    880      0x340   0x12019f File            \Device\HarddiskVolume1\WINDOWS\system32\drivers\str.sys
0xe1155570    880      0x344    0xf003f Key             MACHINE\SOFTWARE\CLASSES
0xe1139bb0    880      0x348    0xf003f Key             MACHINE\SOFTWARE\CLASSES
```

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

Task 7:
What is the name of the injected dll file loaded from the recent process?

I checked for dll in -help and found some plugin

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/CYBERDEF-567078-20230213-171333.raw' --profile=WinXPSP2x86 -h | grep -i dll
Volatility Foundation Volatility Framework 2.6.1
                dlldump         Dump DLLs from a process address space
                dlllist         Print list of loaded dlls for each process
                ldrmodules      Detect unlinked DLLs
```

Then I used the plugin ldrmodules on the PID 880

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/CYBERDEF-567078-20230213-171333.raw' --profile=WinXPSP2x86 ldrmodules --pid=880
Volatility Foundation Volatility Framework 2.6.1
Pid      Process              Base       InLoad InInit InMem MappedPath
-------- -------------------- ---------- ------ ------ ----- ----------
     880 svchost.exe          0x6f880000 True   True   True  \WINDOWS\AppPatch\AcGenral.dll
     880 svchost.exe          0x01000000 True   False  True  \WINDOWS\system32\svchost.exe
     880 svchost.exe          0x77f60000 True   True   True  \WINDOWS\system32\shlwapi.dll
     880 svchost.exe          0x74f70000 True   True   True  \WINDOWS\system32\icaapi.dll
     880 svchost.exe          0x76f60000 True   True   True  \WINDOWS\system32\wldap32.dll
     880 svchost.exe          0x77c00000 True   True   True  \WINDOWS\system32\version.dll
     880 svchost.exe          0x5ad70000 True   True   True  \WINDOWS\system32\uxtheme.dll
     880 svchost.exe          0x76e80000 True   True   True  \WINDOWS\system32\rtutils.dll
     880 svchost.exe          0x771b0000 True   True   True  \WINDOWS\system32\wininet.dll
     880 svchost.exe          0x76c90000 True   True   True  \WINDOWS\system32\imagehlp.dll
     880 svchost.exe          0x76bc0000 True   True   True  \WINDOWS\system32\regapi.dll
     880 svchost.exe          0x77dd0000 True   True   True  \WINDOWS\system32\advapi32.dll
     880 svchost.exe          0x76f20000 True   True   True  \WINDOWS\system32\dnsapi.dll
     880 svchost.exe          0x77be0000 True   True   True  \WINDOWS\system32\msacm32.dll
     880 svchost.exe          0x7e1e0000 True   True   True  \WINDOWS\system32\urlmon.dll
     880 svchost.exe          0x68000000 True   True   True  \WINDOWS\system32\rsaenh.dll
     880 svchost.exe          0x722b0000 True   True   True  \WINDOWS\system32\sensapi.dll
     880 svchost.exe          0x76e10000 True   True   True  \WINDOWS\system32\adsldpc.dll
     880 svchost.exe          0x76b40000 True   True   True  \WINDOWS\system32\winmm.dll
     880 svchost.exe          0x773d0000 True   True   True  \WINDOWS\Win5x5\x86 Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
     880 svchost.exe          0x71a50000 True   True   True  \WINDOWS\system32\mswsock.dll
     880 svchost.exe          0x5b860000 True   True   True  \WINDOWS\system32\netapi32.dll
     880 svchost.exe          0x00670000 True   True   True  \WINDOWS\system32\xpsp2res.dll
     880 svchost.exe          0x76e90000 True   True   True  \WINDOWS\system32\rasman.dll
     880 svchost.exe          0x77a80000 True   True   True  \WINDOWS\system32\crypt32.dll
     880 svchost.exe          0x71ab0000 True   True   True  \WINDOWS\system32\ws2_32.dll
     880 svchost.exe          0x77cc0000 True   True   True  \WINDOWS\system32\activeds.dll
     880 svchost.exe          0x71ad0000 True   True   True  \WINDOWS\system32\wsock32.dll
     880 svchost.exe          0x774e0000 True   True   True  \WINDOWS\system32\ole32.dll
     880 svchost.exe          0x77920000 True   True   True  \WINDOWS\system32\setupapi.dll
     880 svchost.exe          0x7e410000 True   True   True  \WINDOWS\system32\user32.dll
     880 svchost.exe          0x7c900000 True   True   True  \WINDOWS\system32\ntdll.dll
     880 svchost.exe          0x77f10000 True   True   True  \WINDOWS\system32\gdi32.dll
     880 svchost.exe          0x77120000 True   True   True  \WINDOWS\system32\oleaut32.dll
     880 svchost.exe          0x5cb70000 True   True   True  \WINDOWS\system32\shimeng.dll
     880 svchost.exe          0x74980000 True   True   True  \WINDOWS\system32\msxml3.dll
     880 svchost.exe          0x009a0000 False  False  False \WINDOWS\system32\msxml3r.dll
     880 svchost.exe          0x77e70000 True   True   True  \WINDOWS\system32\rpcrt4.dll
```

I copied everything and asked the ChatGPT

The injected DLL file loaded from the recent process is:

The injected DLL file loaded from the recent process is:

msxml3r.dll

The DLL **msxml3r.dll** stands out for the following reasons:

1. **False InLoad, InInit, and InMem flags:** The DLL's load status shows `False` for all the flags (`InLoad`, `InInit`, and `InMem`), indicating it may not have been properly initialized or fully loaded in memory. This is unusual compared to other DLLs in the list, where these flags are `True`, which suggests they are functioning normally.

Answer: msxml3r.dll

Task 8:
What is the base address of the injected dll?

Same as task 5

```
Process: svchost.exe Pid: 880 Address: 0x980000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 9, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000980000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x0000000000980010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x0000000000980020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000000000980030  00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00   ................
```

Answer: 0x980000