# NintendoHunt Challenge

Scenario:

You have been hired as a soc analyst to investigate a potential security breach at a company. The company has recently noticed unusual network activity and suspects that there may be a malicious process running on one of their computers. Your task is identifying the malicious process and gathering information about its activity.

Task 1:
What is the process ID of the currently running malicious process?

I used the pstree plugin and tried to find the PID, I noticed several of suspicious processes and took me sometime to figure it out but at the end I noticed the svchost.exe was running under explorer.exe which is suspicious

```
. 0xffffc20c69d00580:userinit.exe                     4756    732      0 ------ 2018-08-01 19:20:57 UTC+0000
.. 0xffffc20c69cfe580:explorer.exe                    4824   4756    125      0 2018-08-01 19:20:58 UTC+0000
... 0xffffc20c6ddad580:svchost.exe                    8560   4824     10      0 2018-08-01 20:13:10 UTC+0000
... 0xffffc20c6e495080:cmd.exe                        8868   4824      0 ------ 2018-08-01 19:40:14 UTC+0000
```

Answer: 8560

Task 2:
What is the md5 hash hidden in the malicious process memory?

I used the memdump plugin on the process PID 8560 and used strings on it

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/memdump.mem' --profile=Win10x64_17134 memdump --pid=8560 --dump-dir='/home/remnux/Malware'
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing svchost.exe [  8560] to 8560.dmp
```

Then I found some string which says "the flag is" and a Base64.
After decoding I found the MD5

```
[
    {
        "contents": "da391kdasdaadssssssss    t.h.e. fl.ag.is. M2ExOTY5N2YyOTA5NWJjMjq5YTk2ZTQ1MDQ2Nzk2ODA=",
        "settings":
        {
            "buffer_size": 85,
            "line_ending": "Windows"
        }
    }
```

Answer: 3a19697f29095bc289a96e4504679680

Task 3:
What is the process name of the malicious process parent?

Same like task 1

```
. 0xffffc20c69d00580:userinit.exe                     4756    732      0 ------ 2018-08-01 19:20:57 UTC+0000
.. 0xffffc20c69cfe580:explorer.exe                    4824   4756    125      0 2018-08-01 19:20:58 UTC+0000
... 0xffffc20c6ddad580:svchost.exe                    8560   4824     10      0 2018-08-01 20:13:10 UTC+0000
... 0xffffc20c6e495080:cmd.exe                        8868   4824      0 ------ 2018-08-01 19:40:14 UTC+0000
```

Answer: explorer.exe

Task 4:
What is the MAC address of this machine's default gateway?

I tried several ways with netstat, netscan, I tried to use printkey on several keys like "Microsoft \Windows NT\CurrentVersion\NetworkList" and "System\CurrentControlSet\Services\Tcpip \Parameters\Interfaces" but didn't find nothing so I used the hint which says to use: "Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged"

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/memdump.mem' --profile=Win10x64_17134 hivescan | grep -i tcp
Volatility Foundation Volatility Framework 2.6.1
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/memdump.mem' --profile=Win10x64_17134 printkey -K "Microsoft\Windows NT\CurrentVersion\NetworkList"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \SystemRoot\System32\Config\SOFTWARE
Key name: NetworkList (S)
Last updated: 2018-08-01 18:50:26 UTC+0000

Subkeys:
  (S) DefaultMediaCost
  (S) NewNetworks
  (S) Nla
  (S) Permissions
  (S) Profiles
  (S) Signatures

Values:
REG_SZ                  : (S) 192.228.79.201
REG_DWORD     FirstNetwork    : (S) 8
REG_SZ        RootDnsIpv6Addr : (S) 2001:478:65::53
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/memdump.mem' --profile=Win10x64_17134 printkey -K "Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \SystemRoot\System32\Config\SOFTWARE
Key name: Unmanaged (S)
Last updated: 2018-08-01 18:50:26 UTC+0000

Subkeys:
  (S) 010103000F0000F0080000000F0000F8E3E937A4D0CD0A314266D2986CB7DED5D8B43B828FEEDCEFFD6DE7141DC1D15D

Values:
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/memdump.mem' --profile=Win10x64_17134 printkey -K "Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged\010103000F0000F0080000000F0000F8E3E937A4D0CD0A314266D2986CB7DED5D8B43B828FEEDCEFFD6DE7141DC1D15D"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \SystemRoot\System32\Config\SOFTWARE
Key name: 010103000F0000F0080000000F0000F8E3E937A4D0CD0A314266D2986CB7DED5D8B43B828FEEDCEFFD6DE7141DC1D15D (S)
Last updated: 2018-08-01 18:50:26 UTC+0000

Subkeys:

Values:
REG_SZ        ProfileGuid     : (S) {5968BD0F-BFBC-4B67-9ED8-237BD3DDABF3}
REG_SZ        Description     : (S) Network
REG_DWORD     Source          : (S) 8
REG_SZ        DnsSuffix       : (S) localdomain
REG_SZ        FirstNetwork    : (S) Network
REG_BINARY    DefaultGatewayMac : (S)
0x00000000  00 50 56 f6 d8 07                                     .PV...
remnux@remnux:~/volatility$
```

Then I saw a Subkey with a long name so I used printkey again on the Subkey and found the MAC

Answer: 00:50:56:fe:d8:07

Task 5:
What is the name of the file that is hidden in the alternative data stream?

I didn't knew what exactly alternative data stream is so I just learned about it as much I could understand and I used the hint to parser the MFT and grepped for "ads name" and then there will be $DATA with some string


Answer: yes.txt

Task 6:
What is the full path of the browser cache created when the user visited "www.13cubed.com" ?

I used the hint which says to grep for the domain in the MFT file


Answer: Users\CTF\AppData\Local\Packages\MICROS~1.MIC\AC\#!001\MICROS~1\Cache
\AHF2COV9\13cubed[1].htm