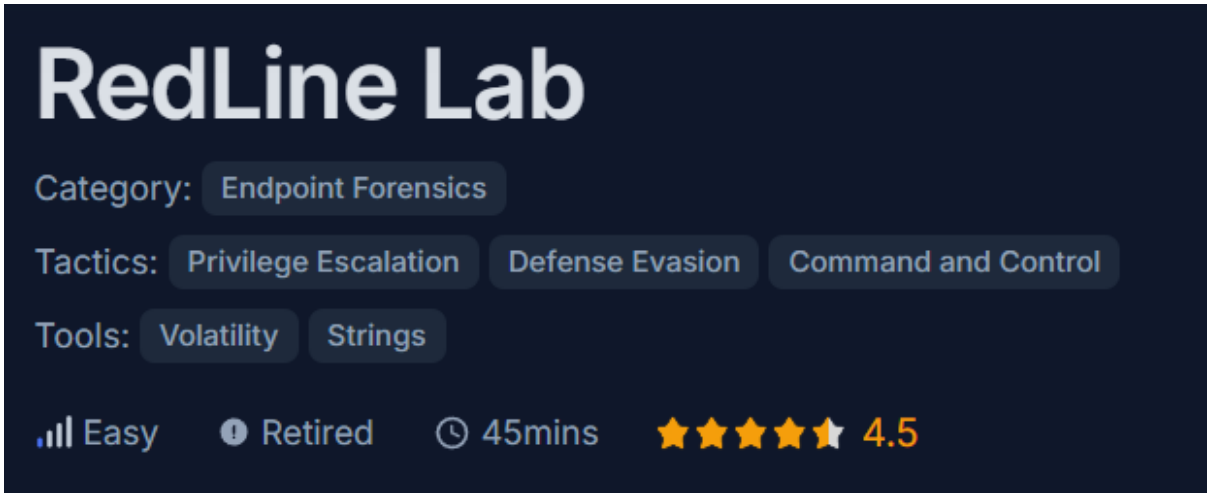
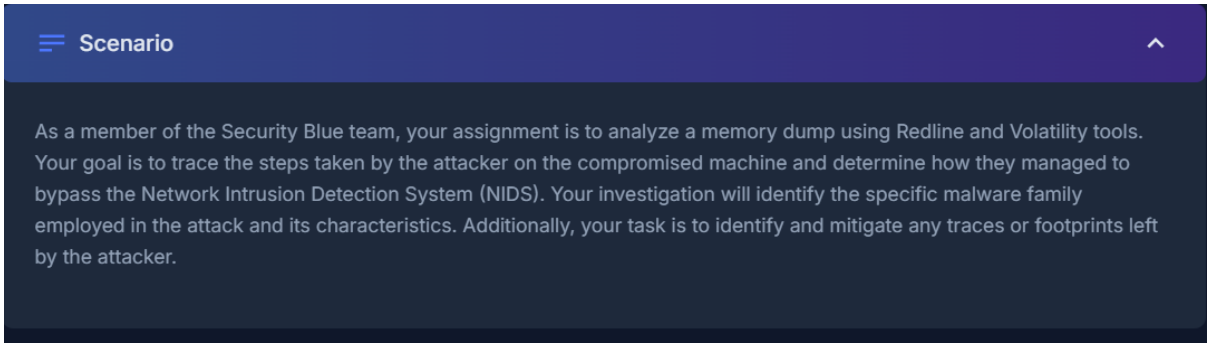


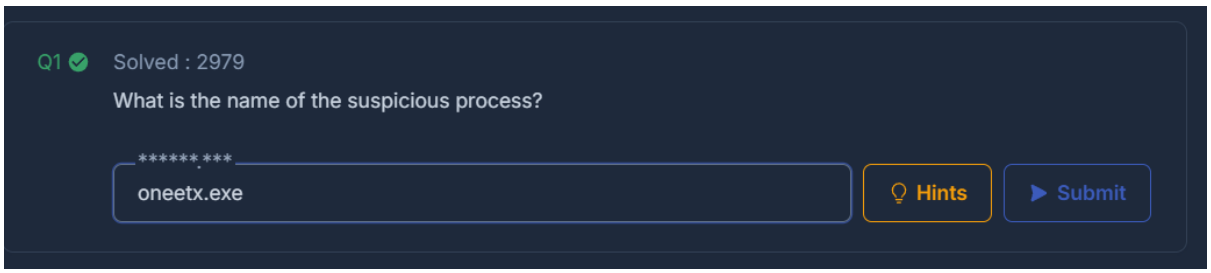


Para identificar le proceso sospechoso con la herramienta volatility3 hice uso de plugins malfind el cual ayuda a idenficar posibles indicios de malware ejecutado en memoria con el comando

Python3 vol.py -f <direccion de memoria> windows.malfind

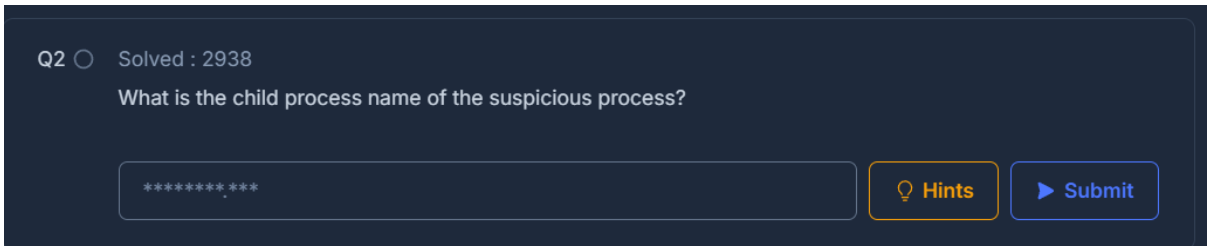
```
11:20:29 csi@csi /opt/volatility3
❯ python3 vol.py -f /home/csi/Downloads/temp_extract_dir/MemoryDump.mem windows.malfind
Volatility 3 Framework 2.0.2
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Hexdump Disasm

5896    oneetx.exe      0x400000        0x437fff        VadS    PAGE_EXECUTE_READWRITE  56      1       Disabled
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 01 00 00 ........
0x400000:       dec     ebp
0x400001:       pop     edx
0x400002:       nop
0x400003:       add     byte ptr [ebx], al
0x400005:       add     byte ptr [eax], al
0x400007:       add     byte ptr [eax + eax], al
0x40000a:       add     byte ptr [eax], al
```

visualizando encontré este proceso sospecho asi dando con la primera flag



La flag: oneetx.exe

Flag 2

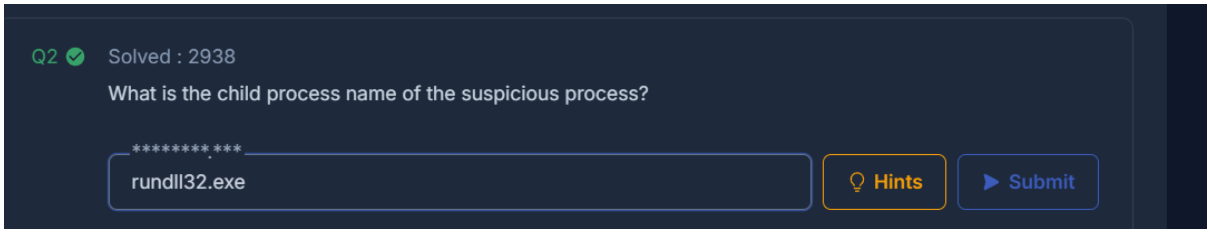


Para encontrar esta flag utilizaremos el plugins pslist para ubicar el proceso hijo de este programa la metodologia para encontrarlo seria partiendo del proceso padre filtrar con el comando grep su pid

Python3 vol.py -f <direccion de memoria> windows.pslit | grep 5895

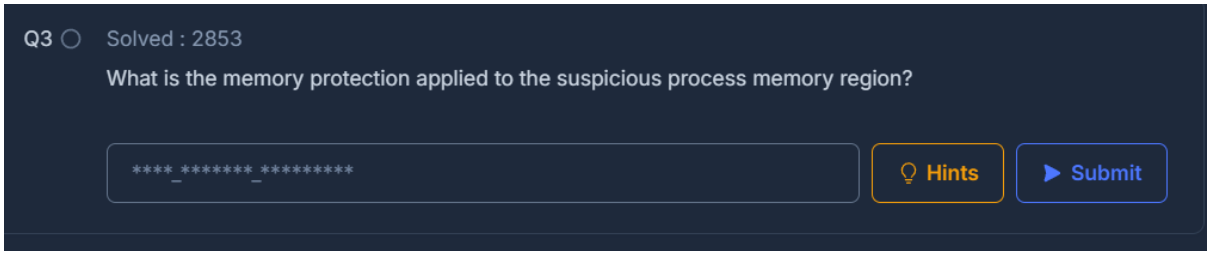
```
11:30:50 csi@csi /opt/volatility3
❯ python3 vol.py -f /home/csi/Downloads/temp_extract_dir/MemoryDump.mem windows.pslist | grep 5896
5896    8844    oneetx.exe      0xad8189b41080  5       -       1       True    2023-05-21 22:30:56.000000      N/A     Disabled
7732    5896    rundll32.exe    0xad818d1912c0  1       -       1       True    2023-05-21 22:31:53.000000      N/A     Disabled
```

Asi encontrado el subproceso que sería el rundll32.exe



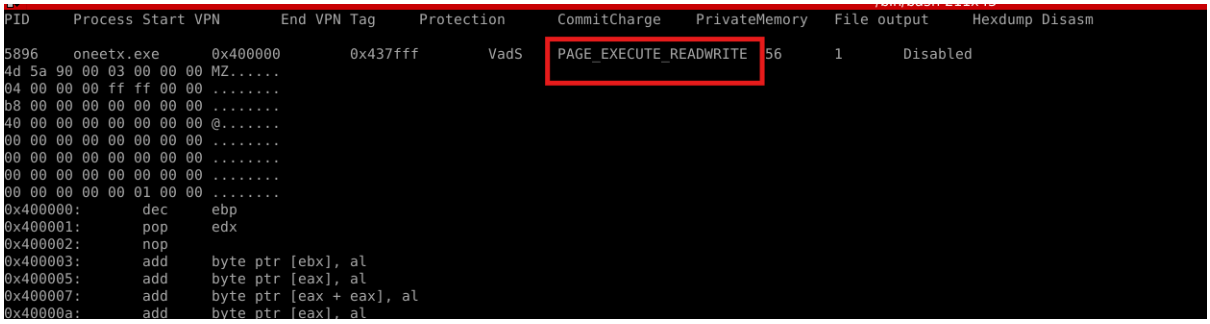
La flag: **rundll32.exe**

Flag 3

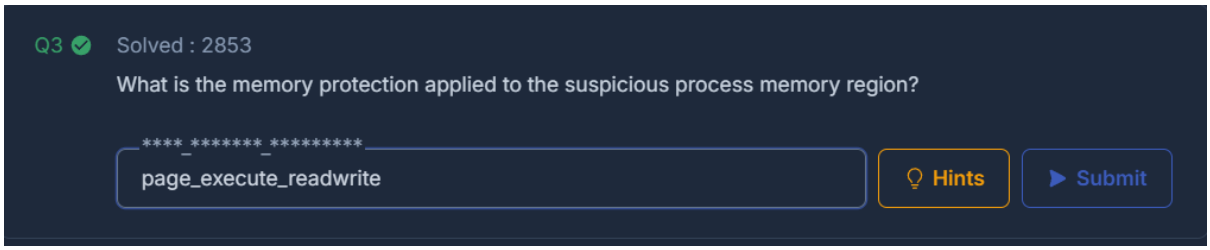


Para emcontrar esta tercera flag retocedemos hasta nuestro anterior plugins de identificacion maliciosa pero ahora con el fin de buscar la apliccaion de proteccion de este.

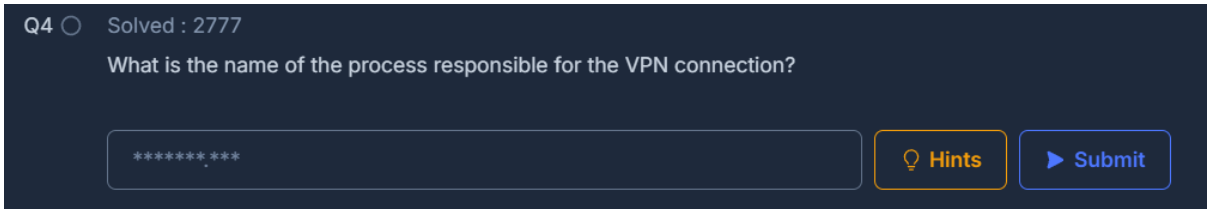
Python3 vol.py -f <direccion de memoria> windows.malfind



La flag: **PAGE_EXECUTE_READWRITE**



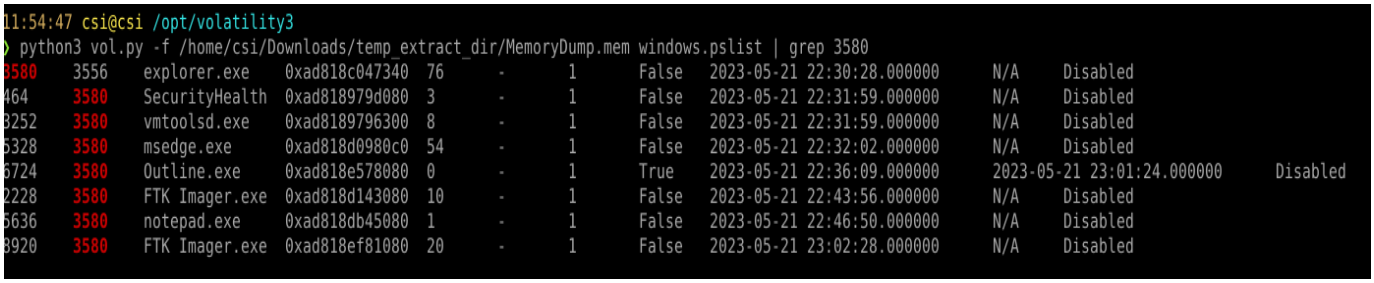
Flag 4



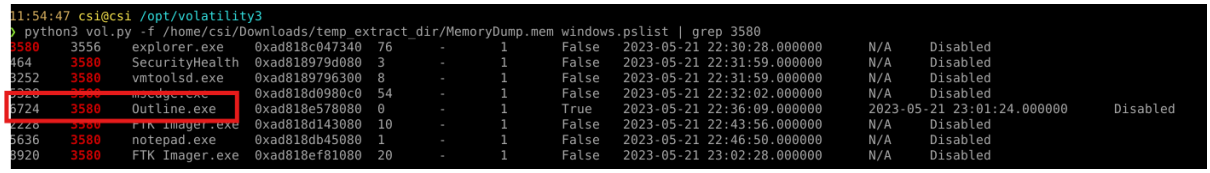
para realizar esta flag realize una investigacion sobre las aplicaciones en ejecucion de los .exe que habian esta activo utilizando el comando

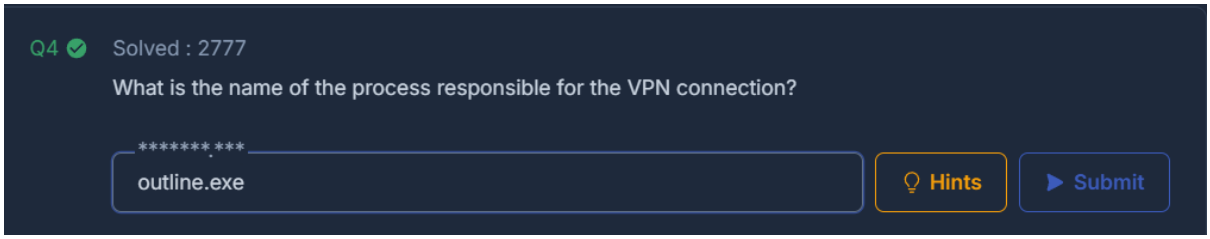
Python3 vol.py -f <direccion de memoria> windows.pslits | grep 3580

Para buscar el proceso de explorer.exe



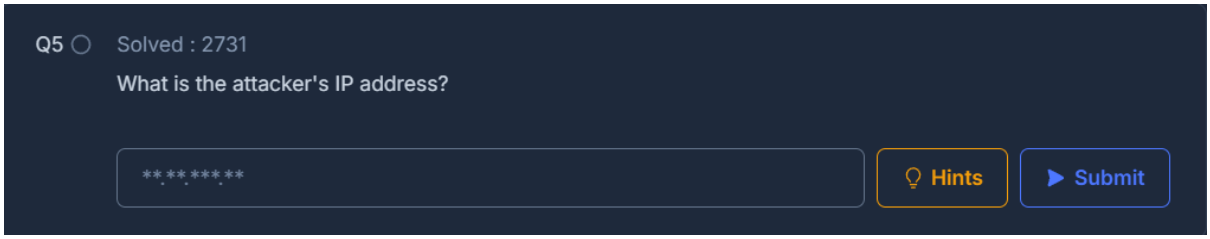
visualizando los procesos encontrado descartamos algunos como el FTK imager y lo que se ejecutan en segundo plano en el sistema operativo nuestra aplicacion de vpn siendo **outline.exe**





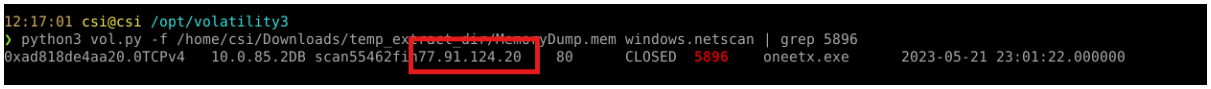
La flag: outline.exe

Flag 5



Para buscar la direccion ip atacante utilizaremos el plugin de **netscan** y partiendo de que ya sabemos cual es el pid malicioso siendo el **5896** utilizamos el comando

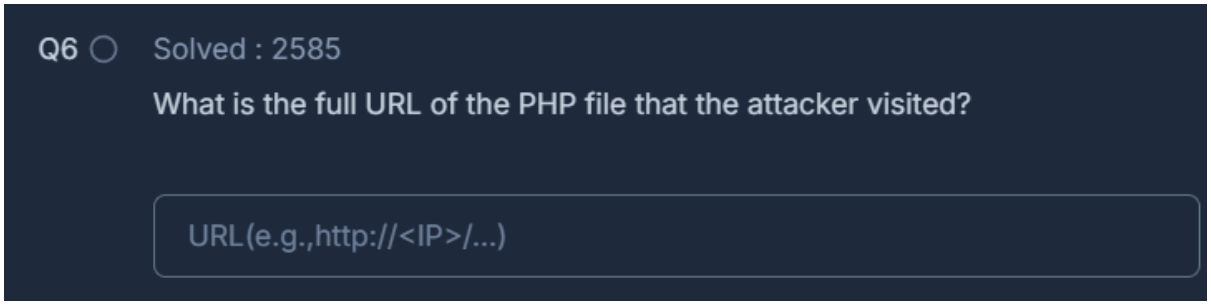
Python3 vol.py -f <direccion de memoria> windows.netscan | grep 5896



asi aplicando este filtro encontramos la ip atacante que es la **77.91.124.20**

La flag: 77.91.124.20

Flag 6



Para enocntrar la URL del cual fue descarga el malware primero me propuse a buscar el usuario desde donde se descargo con el comando

Python3 vol.py -f <direccion de memoria> windows.sessions

para ver todos los usarios del sistema

```
-       5340    msedge.exe      -       2023-05-21 22:32:59.000000
-       5704    RuntimeBroker.  DESKTOP-2HF6AEV/Tammam  2023-05-21 22:32:44.000000
-       1764    dllhost.exe     -       2023-05-21 22:32:48.000000
-       1916    SearchApp.exe   -       2023-05-21 22:33:05.000000
-       7312    ApplicationFra  DESKTOP-2HF6AEV/Tammam  2023-05-21 22:35:44.000000
-       6724    Outline.exe     -       2023-05-21 22:36:09.000000
-       4224    Outline.exe     -       2023-05-21 22:36:23.000000
-       7160    SearchApp.exe   -       2023-05-21 22:39:13.000000
-       4628    tun2socks.exe   -       2023-05-21 22:40:10.000000
-       6048    taskhostw.exe   -       2023-05-21 22:40:20.000000
-       8264    RuntimeBroker.  -       2023-05-21 22:40:33.000000
-       6644    SkypeApp.exe    -       2023-05-21 22:41:52.000000
-       5656    RuntimeBroker.  -       2023-05-21 21:58:19.000000
-       8952    TextInputHost.  DESKTOP-2HF6AEV/Tammam  2023-05-21 21:59:11.000000
-       5808    HxTsr.exe       -       2023-05-21 21:59:58.000000
-       2388    msedge.exe      -       2023-05-21 22:05:35.000000
-       6292    msedge.exe      -       2023-05-21 22:06:15.000000
-       3876    taskhostw.exe   -       2023-05-21 22:08:02.000000
-       372     SkypeBackgroun  -       2023-05-21 22:10:00.000000
-       6076    ShellExperienc  -       2023-05-21 22:11:36.000000
-       7336    RuntimeBroker.  -       2023-05-21 22:11:39.000000
-       7964    msedge.exe      -       2023-05-21 22:22:09.000000
-       6544    msedge.exe      -       2023-05-21 22:22:35.000000
-       8896    msedge.exe      -       2023-05-21 22:28:21.000000
-       5156    msedge.exe      -       2023-05-21 22:28:22.000000
-       5896    oneetx.exe      -       2023-05-21 22:30:56.000000
-       7732    rundll32.exe    -       2023-05-21 22:31:53.000000
-       2228    FTK Imager.exe  -       2023-05-21 22:43:56.000000
-       5636    notepad.exe     -       2023-05-21 22:46:50.000000
-       7540    smartscreen.ex  DESKTOP-2HF6AEV/Tammam  2023-05-21 23:02:26.000000
-       8920    FTK Imager.exe  DESKTOP-2HF6AEV/Tammam  2023-05-21 23:02:28.000000
-       5480    oneetx.exe      -       2023-05-21 23:03:00.000000
/A     -       1280    MemCompression  -       2023-05-21 22:27:49.000000
```

El usario llamado **Tammam**

Luego decide buscarlo atraves del filtros con **strings y grep**

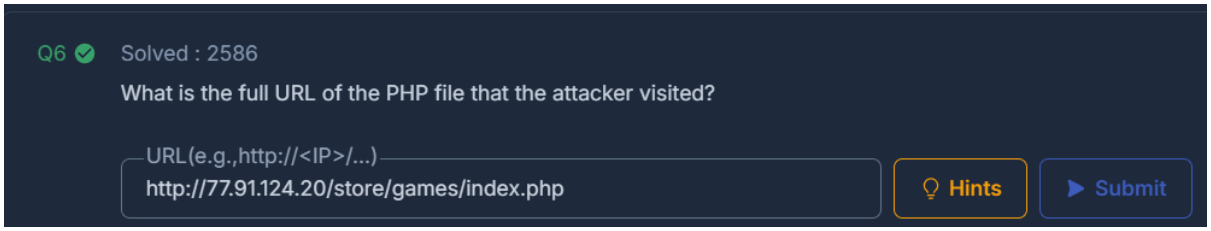
Filtre teniendo estos parametros en mente

La ip atacante 77.91.124.20

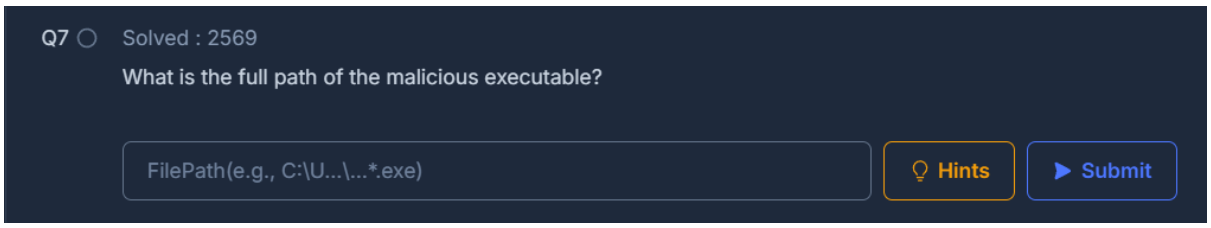
Siendo el comando **strings memoryDump.mem | grep 77.91.124.20**

```
❯ strings MemoryDump.mem | grep 77.91.124.20
http://77.91.124.20/ E
77.91.124.20/stor
http://77.91.124.20/store/gamel
ttp://77.91.124.20/store/games/i
77.91.124.20
http://77.91.124.20/ E
http://77.91.124.20/DSC01491/
77.91.124.20
http://77.91.124.20/DSC01491/
http://77.91.124.20/store/games/index.php
77.91.124.20
77.91.124.20
77.91.124.20
77.91.124.20
77.91.124.20
http://77.91.124.20/store/games/index.php
http://77.91.124.20/store/games/index.php
```

La flag: **http://77.91.124.20/store/games/index.php**

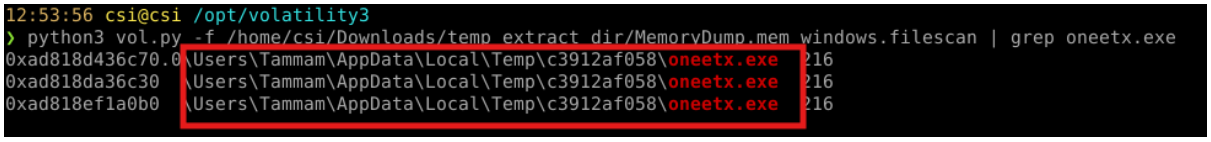


Flag 7



para encontrar esta flag observando que nos pide el full path del ejecuable malicioso utilizaremos el plugin de volatilite llamado **File.scan** y filtrado por el nombre de nuestro programa malicioso siendo **oneetx.exe**

Python3 vol.py -f <direccion de memoria> windows.filescan | grep oneetx.exe



la flag: C:\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe