LAB 6: WINDOWS FORENSICS – PART I

Lab Requirements

1. Microsoft Windows virtual machine

Content

Part I: Collecting Volatile Information _____ *1*

Part I: Collecting Volatile Information

STEP 1: Collecting time and date.

```
# &: the first command is executed followed by the second
C:> date /t & time /t
    Tue 02/15/2022
12:41 PM
```

STEP 2: List logged-on users.

```
# Download Sysinternals Suite to be able to use the following commands.
C:\work\tools> psloggedon Users
  logged on locally:
       2/15/2022 11:50:10 AM     WINDEV2112EVAL\User

  No one is logged on via resource shares.
```

NOTE 2-1: psloggedon is part of the Sysinternals Suite. You can download the suite at https://download.sysinternals.com/files/SysinternalsSuite.zip

STEP 3: List logged-on sessions using `logonsessions`. You can use the -p option to list the processes running in each session. Remark that there is more than one active sessions, and not only one as we might think.

```
# list the logged-on sessions. Use findstr list the session IDs only
C:\work\tools> logonsessions | findstr “logon session” LogonSessions
   v1.41 - Lists logon session information
   [0] Logon session 00000000:000003e7:
   [1] Logon session 00000000:00009cc8:
   [2] Logon session 00000000:0000a149:
   [3] Logon session 00000000:0000a161:
   [4] Logon session 00000000:000003e4:
   [5] Logon session 00000000:0000fe84:
   [6] Logon session 00000000:0000feab:
   [7] Logon session 00000000:000003e5:
   [8] Logon session 00000000:0001b944:
   [9] Logon session 00000000:0001b99e:
C:\work\tools> logonsessions -p
   ...
   [9] Logon session 00000000:0001b99e:
       User name:    WINDEV2112EVAL\User
       Auth package: NTLM
       Logon type:   Interactive
       Session:      1
       Sid:          S-1-5-21-1516808570-3660347512-3657706960-1001
       Logon time:   2/15/2022 11:50:08 AM
   Logon server: WINDEV2112EVAL
       DNS Domain:
       UPN:
        2992: svchost.exe
   3000: sihost.exe
        3036: svchost.exe
        3344: taskhostw.exe
        1832: ctfmon.exe
        5076: explorer.exe
        5128: svchost.exe
        4956: StartMenuExperienceHost.exe

```

NOTE 3-1: Use the options -c and -ct to display the output as comma-separated values or tabdelimited values, respectively.

STEP 4: Collecting information about network connections using `netstat`.

```
# -a: all connections.
# -p protocol: select a protocol among TCP, UDP, TCPv6, UDPv6
# -r: display the routing table
# -b: display the executable involved with the connection
# -e: display the network statistics
C:\work\tools> netstat -a
```

```
  Active Connections
    Proto  Local Address          Foreign Address        State
    TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
    TCP    172.16.200.130:139     0.0.0.0:0              LISTENING
    TCP    172.16.200.130:49790   40.83.247.108:443      ESTABLISHED
    TCP    172.16.200.130:62586   52.184.217.20:443      ESTABLISHED
    TCP    172.16.200.131:139     0.0.0.0:0              LISTENING
    UDP    [fe80::1d7b:4ff:1bea:9b1a%4]:1900  *:*
    UDP    [fe80::1d7b:4ff:1bea:9b1a%4]:49305  *:*
  UDP    [fe80::692d:26f4:c2e6:88c6%20]:1900  *:*
    UDP    [fe80::692d:26f4:c2e6:88c6%20]:49306  *:*
```

STEP 4: Collecting process information using `tasklist`, *`listdll`*, and *`handle`*.

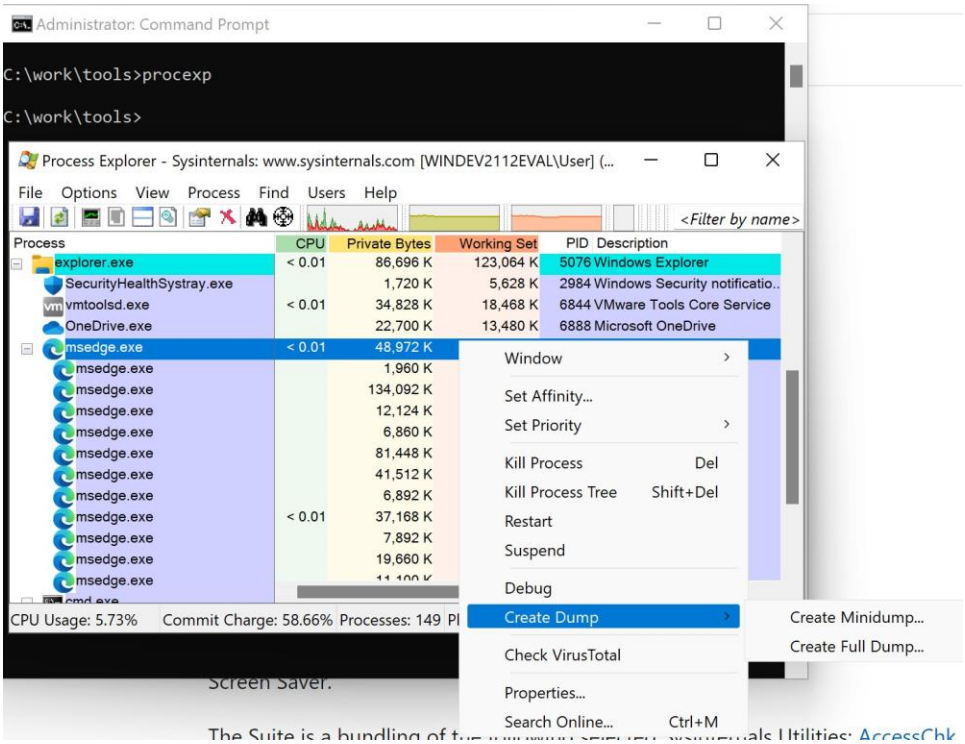
```
C:\work\tools> tasklist
  Image Name                     PID Session Name        Session#    Mem Usage
  ========================= ======== ================ =========== ============
  System Idle Process              0 Services                   0          8 K
  System                           4 Services                   0         84 K
  Secure System                   56 Services                   0     14,452 K
  Registry                       108 Services                   0     13,688 K
  smss.exe                       340 Services                   0        972 K
  wininit.exe                    568 Services                   0      2,280 K
  csrss.exe                      612 Console                    1      3,276 K
  services.exe                   632 Services                   0      5,760 K
  ...
```

```
# user /FI (filter) to filter processes based on a specific parameter: PID,
# IMAGENAME, SESSION, SESSIONAME, CPUTIME, STATUS, …
C:\work\tools> tasklist /FI “PID gt 700”
  Image Name                     PID Session Name        Session#    Mem Usage
  ========================= ======== ================ =========== ============
  msedge.exe                    7092 Console                    1      4,024 K
  msedge.exe                    7176 Console                    1     18,040 K
  msedge.exe                    7184 Console                    1      6,832 K
  svchost.exe                   8168 Console                    1      9,756 K
  svchost.exe                   7436 Services                   0      6,640 K
  SgrmBroker.exe                7356 Services                   0      6,788 K
  svchost.exe                   7988 Services                   0      4,836 K
  msedgewebview2.exe            7616 Console                    1     14,588 K
  dllhost.exe                   7608 Console                    1      5,376 K
  tasklist.exe                  8184 Console                    1      8,712 K
  clip.exe                      7688 Console                    1      4,364 K
```

STEP 5: Collecting process information using `pslist`. Options: -d threads, -m memory, -x memory and threads, and pid.

```
# a truncated output
C:\work\tools> pslist -x
   Name                Pid      VM      WS    Priv Priv Pk   Faults   NonP Page
   Registry            108  122496   13848    4844   45212    89881     12  243
   Tid Pri    Cswtch           State     User Time   Kernel Time   Elapsed Time
    112   8         1   Wait:Executive  0:00:00.000   0:00:00.000    4:25:39.920
    428   9      2081   Wait:Executive  0:00:00.000   0:00:00.421    4:25:25.918
    432   8      7865   Wait:Executive  0:00:00.000   0:00:01.171    4:25:25.918
   436   8        60   Wait:Executive  0:00:00.000   0:00:00.031    4:25:25.918
   ...
```

STEP 5: Examine process memory using `procexp`.



NOTE 5-1: You can create a full memory dump of a given process as shown in the above window.

NOTE 5-2: You can perform malware analysis of a given service by selecting “Check VirusTotal” from the list.

STEP 6: Examine the print spool. Windows stores the printing tasks in a spool file (.spl) and a shadow file (.shd). These files are located in the c:\windows\system32\spool\PRINTERS folder.