UNIVERSITY OF LIVERPOOL

CYBER SECURITY SOCIETY

Memory Forensics

Volatility

What is memory forensics?

- The term memory refers to the contents of the RAM on your computer, this is where your computer stores the majority of information about what is currently happening on the computer
- A memory image is a capture of the state of memory at a point in time
  - It is quite difficult to take memory images properly as the contents of memory are always changing (there is hardware and software solutions for doing this)

Why is memory forensics useful

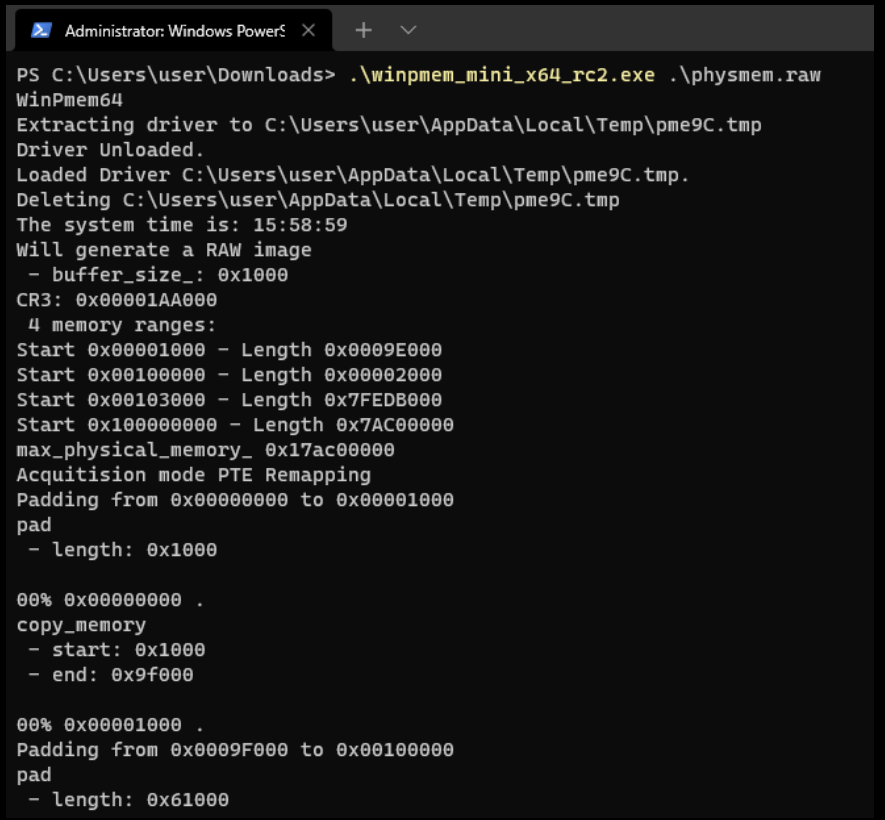
- By capturing an image of the computers memory you are able to store and analyse the entire state of the computer at that point in time
  - Running programs
  - Open files
  - OS Information
  - Passwords
  - Etc…

Creating a memory image

- Windows
  - FTKImager
  - Mdd
  - WinPMem (open source)
- Linux
  - /dev/mem (might be restricted, dd)
  - /dev/fmem (need to load kernel module, dd)
  - LiMe (need to load kernel module)

WinPMem

- Download from github
- Run as admin



LiMe

- Download from github
- Compile (make)
- Load module: sudo insmod lime*.ko “path=/mem.lime format=”lime”
- Can also be configured to send over network

Installing volatility

- `sudo apt-get update`
- `sudo apt-get install python3-pip`
- `python3 -m pip install volatility3`
  - If you get a warning about .local/bin not being in PATH
    - `echo 'export PATH="$PATH:~/.local/bin"' >> ~/.bashrc`
    - `source ~/.bashrc`

Volatility versions

- Volatility 3 came out “relatively” recently and is still in beta
- A lot of help you find online will be for volatility 2
  - Use this cheatsheet to compare
- It works best for windows dumps but has some support for linux and mac
  - By default contains the symbols tables for windows, but you need to compile your own symbol tables for each mac/linux version

Using volatility

```
┌──(crewmate㉿amogos)-[~/Downloads]
└─$ vol --help
```

- This outputs the list of plugins and what each of them do

```
┌──(crewmate㉿amogos)-[~/Downloads]
└─$ vol -f ./physmem.raw windows.info
Volatility 3 Framework 1.0.1
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0×f80716600000
DTB     0×1aa000
Symbols file:///home/crewmate/.local/lib/python3.9/site-packages/volatility3/symbols/windows/ntkrnlmp.pdb/1F9BB45B28B806E4D18925C06E924B8C-1.json.xz
Is64Bit True
IsPAE   False
primary 0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0×f8071720f378
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      2
SystemTime      2021-11-30 15:58:59
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Thu Oct 10 11:21:38 2097
```

- For windows images just specify the file with -f then the plugin you wish to use
- For additional help on the plugin add --help to the end

Running processes

```
┌──(crewmate㉿amogos)-[~/Downloads]
└─$ vol -f ./memory.dmp windows.pslist
Volatility 3 Framework 1.0.1
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0×de0f69080040  126     -       N/A     False   2021-11-30 15:33:54.000000      N/A     Disabled
92      4       Registry        0×de0f691b8040  4       -       N/A     False   2021-11-30 15:33:52.000000      N/A     Disabled
336     4       smss.exe        0×de0f69b9f040  2       -       N/A     False   2021-11-30 15:33:54.000000      N/A     Disabled
440     432     csrss.exe       0×de0f6f3d6140  10      -       0       False   2021-11-30 15:33:59.000000      N/A     Disabled
532     432     wininit.exe     0×de0f6f54a080  1       -       0       False   2021-11-30 15:34:00.000000      N/A     Disabled
548     524     csrss.exe       0×de0f6f551140  13      -       1       False   2021-11-30 15:34:00.000000      N/A     Disabled
624     524     winlogon.exe    0×de0f6f5990c0  5       -       1       False   2021-11-30 15:34:00.000000      N/A     Disabled
644     532     services.exe    0×de0f6f59b140  6       -       0       False   2021-11-30 15:34:00.000000      N/A     Disabled
676     532     lsass.exe       0×de0f6f543080  9       -       0       False   2021-11-30 15:34:00.000000      N/A     Disabled
784     644     svchost.exe     0×de0f6f90b300  13      -       0       False   2021-11-30 15:34:00.000000      N/A     Disabled
796     624     fontdrvhost.ex  0×de0f6f90d200  5       -       1       False   2021-11-30 15:34:00.000000      N/A     Disabled
804     532     fontdrvhost.ex  0×de0f6f90e080  5       -       0       False   2021-11-30 15:34:00.000000      N/A     Disabled
904     644     svchost.exe     0×de0f6f976240  12      -       0       False   2021-11-30 15:34:00.000000      N/A     Disabled
952     644     svchost.exe     0×de0f6f9ad300  5       -       0       False   2021-11-30 15:34:00.000000      N/A     Disabled
```

- For more info can use windows.pstree or windows.cmdline

Open files

- windows.filescan
- windows.filedump (--pid pid)
- windows.handles (--pid pid)

Windows password stores

```
┌──(crewmate㉿amogos)-[~/Downloads]
└─$ vol -f ./memory.dmp windows.hashdump
Volatility 3 Framework 1.0.1
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        58f98a1ef46b9c42b2ef8784f633939b
user    1001    aad3b435b51404eeaad3b435b51404ee        57d583aa46d571502aad4bb7aea09c70
```

Challenges

- Install volatility
- Challenges: Forensics/Cached