Memory Forensics

Memory Analysis: A Nightmare

- Currently the state of open source memory analysis is a bit rough
- Microsoft is making this a bit more difficult than they should
- Projects like Volatility do a great job, but without clean memory maps full analysis is difficult
- Other up and coming projects like Velociraptor are really cool, but not quite there yet
  - Velociraptor will be added in a future iteration of this class
  - Good thing you can always come back
- But, the concepts are the same for Open Source and commercial analysis

Volatility

Volatility 2.6 (Windows 10 / Server 2016)

This release improves support for Windows 10 and adds support for Windows Server 2016, Mac OS Sierra 10.12, and Linux with KASLR kernels. A lot of bug fixes went into this release as well as performance enhancements (especially related to page table parsing and virtual address space scanning). See below for a more detailed list of the changes in this version.

This release also coincides with the Community repo - a collection of Volatility plugins written and maintained by authors in the forensics community. Many of these are the result of the last 4 years of Volatility plugin contests, but some were just written for fun. Either way, its an entire arsenal of plugins that you can easily extend into your existing Volatility installation.

Released: December 2016

- Volatility 2.6 Windows Standalone Executable (x64)
- Volatility 2.6 Mac OS X Standalone Executables (x64)
- Volatility 2.6 Linux Standalone Executables (x64)
- Volatility 2.6 Source Code (.zip)
- Integrity Hashes
- View the README
- View the CREDITS

Release Highlights

Memory Analysis: Network

```
C:\tools\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f memdump.vmem netscan --profile=Win10x64_
10586
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner
 Created
0xa98dc80b0b80     UDPv4    192.168.192.145:49233          *:*                                   4        System
 2020-11-30 17:40:29 UTC+0000
0xa98dc84e1220     UDPv4    0.0.0.0:0                      *:*                                   1320     svchost.exe
 2020-11-30 20:40:29 UTC+0000
0xa98dc93576f0     UDPv4    0.0.0.0:0                      *:*                                   1320     svchost.exe
 2020-11-30 18:40:29 UTC+0000
0xa98dc93576f0     UDPv6    :::0                           *:*                                   1320     svchost.exe
 2020-11-30 18:40:29 UTC+0000
0xa98dc97c1710     UDPv4    0.0.0.0:0                      *:*                                   2372     dasHost.exe
 2020-11-30 17:40:37 UTC+0000
0xa98dc97c1710     UDPv6    :::0                           *:*                                   2372     dasHost.exe
 2020-11-30 17:40:37 UTC+0000
0xa98dc9ae3420     UDPv4    0.0.0.0:0                      *:*                                   1952     svchost.exe
 2020-11-30 17:40:31 UTC+0000
0xa98dc9ae3420     UDPv6    :::0                           *:*                                   1952     svchost.exe
 2020-11-30 17:40:31 UTC+0000
0xa98dc9ae3740     UDPv4    0.0.0.0:0                      *:*                                   1952     svchost.exe
```

Memory Analysis: Processes

```
C:\tools\volatility_2.6_win64_standalone> volatility_2.6_win64_standalone.exe -f memdump.vmem pslist --profile=Win10x64_
10586
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit

------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ -----
-------------------------
0xffffa98dc80576c0 System                    4      0     85        0 ------      0 2020-11-30 17:40:26 UTC+0000

0xffffa98dc9836480 smss.exe                512      4      2        0 ------      0 2020-11-30 17:40:26 UTC+0000

0xffffa98dc9a56080 csrss.exe               588    580      9        0      0      0 2020-11-30 17:40:27 UTC+0000

0xffffa98dc98e6080 smss.exe                656    512      0 --------      1      0 2020-11-30 17:40:27 UTC+0000

0xffffa98dc9f74800 wininit.exe             664    580      1        0      0      0 2020-11-30 17:40:27 UTC+0000

0xffffa98dca06b080 csrss.exe               672    656     11        0      1      0 2020-11-30 17:40:27 UTC+0000

0xffffa98dca06a340 winlogon.exe            744    656      2        0      1      0 2020-11-30 17:40:27 UTC+0000
```

Memory Analysis: DLL and Command Line

```
C:\tools\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f memdump.vmem --profile=Win10x64_10586 dl
llist -p 5452
Volatility Foundation Volatility Framework 2.6
************************************************************************
TrustMe.exe pid:   5452
Command line : "C:\Users\Sec504\Downloads\TrustMe.exe"


Base                             Size          LoadCount Path
-------------------- ---------------------- ------------------ ----
0x0000000000400000           0x16000                0x0 C:\Users\Sec504\Downloads\TrustMe.exe
0x00007ffaf6290000           0x1d1000               0x0 C:\Windows\SYSTEM32\ntdll.dll
0x00000000594e0000           0x52000                0x0 C:\Windows\System32\wow64.dll
0x0000000059540000           0x77000                0x0 C:\Windows\System32\wow64win.dll
0x00000000594d0000            0xa000                0x0 C:\Windows\System32\wow64cpu.dll

C:\tools\volatility_2.6_win64_standalone>
```