# Brave Lab (Cyber Defenders) - Walkthrough

Sunday, September 15, 2024 8:20 PM

#### Story:

A memory image was taken from a seized Windows machine. As a security blue team analyst, analyze the image and answer the provided questions.

# Q1: What time was the RAM image acquired according to the suspect system? (YYYY-MM-DD HH:MM:SS)

 I used Volatility3's windows.info.Info plugin to determine that the memory image was captured on 2021-04-30 at 17:52:19.

```
SystemTime 2021-04-30 17:52:19+00:00
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine 34404
PE TimeDateStamp Tue Oct 11 07:04:26 1977
```

#### Q2: What is the SHA256 hash value of the RAM image?

• I used 'sha256sum' command to find the sha256 of the image.

#### Q3: What is the process ID of "brave.exe"?

• I used 'Pstree' plugin to find the PID of 'Brave.exe'

# Q4: How many established network connections were there at the time of acquisition? (number)

• I used 'netscan' plugin and filtered by 'Grep' utility 'Established'.

```
(kali@ kali) -[~/Desktop/volatility3]

5 python3 vol.py -f ../20210430-Win10Home-20H2-64bit-mendump.mem windows.netscan | grep 'ESTABLISHED'

0xbF0f6a36220.0TCPV4 | 10.0.2.150 scan49833fin52,230.222.68 | 443 | LT7ALI25HD | 2812 | svchost.exe | 2021-04-30 | 17:50:07.000000 | UTC |

0xbF0f6a36220.0TCPV4 | 10.0.2.15 | 49829 | 142,250.191.208 | 443 | LSTABLISHED | 2812 | svchost.exe | 2021-04-30 | 17:51:25.000000 | UTC |

0xbF0f6a3635200 | TCPV4 | 10.0.2.15 | 49824 | 52,131.196.254 | 443 | LSTABLISHED | 2812 | svchost.exe | 2021-04-30 | 17:51:25.000000 | UTC |

0xbF0f6a535200 | TCPV4 | 10.0.2.15 | 49842 | 52,131.196.254 | 443 | LSTABLISHED | 5104 | SearchApp.exe | 2021-04-30 | 17:51:25.000000 | UTC |

0xbF0f6a546400 | TCPV4 | 10.0.2.15 | 49837 | 20.0.79.197.200 | 443 | LSTABLISHED | 5104 | SearchApp.exe | 2021-04-30 | 17:51:18.000000 | UTC |

0xbF0f6d51c400 | TCPV4 | 10.0.2.15 | 49838 | 13.107.3.254 | 443 | LSTABLISHED | 5104 | SearchApp.exe | 2021-04-30 | 17:51:18.000000 | UTC |

0xbF0f6d51c400 | TCPV4 | 10.0.2.15 | 49838 | 13.107.3.254 | 443 | LSTABLISHED | 5104 | SearchApp.exe | 2021-04-30 | 17:51:18.000000 | UTC |

0xbF0f6d51c400 | TCPV4 | 10.0.2.15 | 49838 | 23.101.202.002 | 443 | LSTABLISHED | 5104 | SearchApp.exe | 2021-04-30 | 17:51:136.000000 | UTC |

0xbF0f6d51c400 | TCPV4 | 10.0.2.15 | 49845 | 23.101.202.002 | 443 | LSTABLISHED | 1156 | MSMpEng.exe | 2021-04-30 | 17:51:136.000000 | UTC |

0xbF0f6d51c400 | TCPV4 | 10.0.2.15 | 49845 | 23.101.202.002 | 443 | LSTABLISHED | 1156 | MSMpEng.exe | 2021-04-30 | 17:51:136.000000 | UTC |

0xbF0f6d51c400 | TCPV4 | 10.0.2.15 | 49845 | 23.101.202.002 | 443 | LSTABLISHED | 1156 | MSMpEng.exe | 2021-04-30 | 17:51:136.000000 | UTC |

0xbF0f6d51c400 | TCPV4 | 10.0.2.15 | 49845 | 23.101.202.002 | 443 | LSTABLISHED | 1156 | MSMpEng.exe | 2021-04-30 | 17:51:136.000000 | UTC |

0xbF0f6d51c400 | TCPV4 | 10.0.2.15 | 49845 | 23.101.202.202 | 443 | LSTABLISHED | 1156 | MSMpEng.exe | 2021-04-30 | 17:51:136.000000 | UTC |

0xbF0f6d51c400 | TCPV4 | 10.0.2.15 | 49845 | 23.101.202.202
```

### Q5: What FQDN does Chrome have an established network connection with?

 I used the IP connected via Chrome and looked it up on AbuseIPDB, which led me to the registered domain 'protonmail.ch'.

## Q6: What is the MD5 hash value of process executable for PID 6988?

 I executed the following command: python3 vol.py -f ../20210430-Win10Home-20H2-64bit-memdump.mem windows.pslist --pid= 6988 --dump to dump the process. After dumping the process, I used the md5sum command to find the MD5 hash.

### Q7: What is the word starting at offset 0x45BE876 with a length of 6 bytes?

To address this question, I used 'HxD', I loaded the memory dump to the HxD and used the 'Go To'
operation and put the offest (45BE876) and found the 6 bytes word is hacker

```
6E 6C 6F 61 64 09 66 69 6C 65 7A 69 6C 6C 61 09 nload.filerilla. 61 77 6B 20 72 65 6D 6F 76 65 20 6F 6F 6C 79 20 awk remove only 74 68 65 20 66 69 72 73 74 20 66 69 65 6C 64 09 the first field. 67 72 65 70 20 6F 72 09 68 61 63 6B 69 6E 67 20 grep or hacking 74 6F 6F 6C 61 09 68 61 63 6B 69 6E 67 20 grep or hacking 6B 67 72 6F 75 6E 64 09 62 65 74 74 65 72 63 61 kground.betterca 6B 67 72 6F 75 6E 64 09 62 65 74 74 65 72 63 61 kground.betterca 74 69 61 6C 73 09 62 65 74 74 65 72 63 61 kground.betterca 74 69 61 6C 73 09 62 65 74 74 65 72 63 61 70 20 tials.bettercap
```

# Q8: What is the creation date and time of the parent process of "powershell.exe"? (YYYY-MM-DD HH:MM:SS)

• You are able to use 'Pstree' plugin to see when the 'Explorer.exe' created (2021-04-30 17:39:48)

### Q9: What is the full path and name of the last file opened in notepad?

• You are able to see the file path and the filename via 'Pstree' plugin

#### Q10: How long did the suspect use Brave browser? (hh:mm:ss)

 To address this question, I used 'windows.registry.userassist.UserAssist' plugin to find how much time the user used Brave browser.

```
- (kali@ kali)-[-/Desktop/volatility3]
- $ python3 vol.py - f .../20210430-Win10Home-20H2-64bit-memdump.mem windows.registry.userassist.UserAssist | grep 'Brave'
0x-880333cda0000
000 UTC Value
0x-88033cda0000
000 UTC Value
0x-880333cda0000
000 UTC Value
0x-880333cda0000
000 UTC Value
0x-880333cda0000
000 UTC Value
0x-88033cda0000
000 UTC Value
0x-880333cda0000
000 UTC V
```