

Отчёт

✎ Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 21:17 *(не сильно сложная комната на форензику, но очень классная на тренировку внимания и анализа данных (づ ◡ ◡)づ)*

Область тестирования и использованные службы.

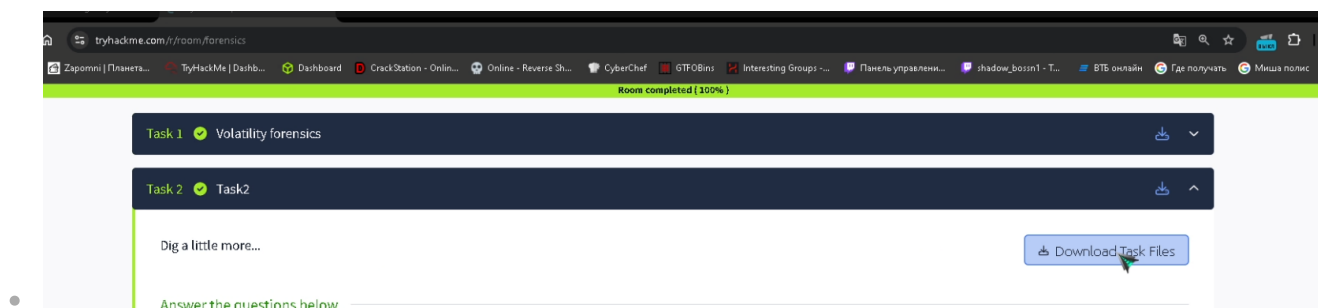
Это задание на форензику, их здесь нет.

Использованные файлы:

- victim.zip - архив от thm.
- victim.raw - файл для анализа.
- [vol.py](#), или [Volatility3](#) - приложение для анализа raw-файлов с memory - сэмплами.
- 1820.dump - дамп трафика от процесса [PID=1820] для анализа.

Порядок действий

1) Скачивание task файлов:



2) Разархивация и анализ общей информации изображения:

- Результаты:

```
(kolya080808@Nikolapc)-[~/forenziks]
$ unzip victim_1556932027367.zip
Archive: victim_1556932027367.zip
  inflating: victim.raw

(kolya080808@Nikolapc)-[~/forenziks]
$ vol.py
Volatility Foundation Volatility Framework 2.6.1
ERROR : volatility.debug : You must specify something to do (try -h)
```

```
(kolya080808@Nikolapc)-[~/forenziks]
$ vol.py -f victim.raw imageinfo

Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kolya080808/forenziks/victim.raw)
PAE type : No PAE
DTB : 0x107000L
KDBG : 0xf800020420a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80002043d00L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2019-05-02 18:11:45 UTC+0000
Image local date and time : 2019-05-02 11:11:45 -0700
```

Получен первый ответ (windows).

3) Анализ запущенных процессов:

- Результат:

```
(kolya080808@Nikolapc)-[~/forenziks]
$ vol.py -f victim.raw --profile=Win7SP1x64 pslist

Volatility Foundation Volatility Framework 2.6.1
Offset(V)      Name                PID  PPID  Thds  Hnds  Sess  Wow64  Start                Exit
-----
0xffffffff8001252040 System              4      0     88    624  -----  0  2019-05-03 06:32:24 UTC+0000
0xffffffff800234d0a0 smss.exe            268     4      2     29  -----  0  2019-05-03 06:32:24 UTC+0000
0xffffffff8002264550 csrss.exe           360    352     9    363    0  0  2019-05-03 06:32:34 UTC+0000
0xffffffff80027d67d0 csrss.exe           408    400     7    162    1  0  2019-05-03 06:32:35 UTC+0000
0xffffffff8002b601c0 wininit.exe         416    352     3     76    0  0  2019-05-03 06:32:35 UTC+0000
0xffffffff8002b71680 winlogon.exe         444    400     3    111    1  0  2019-05-03 06:32:35 UTC+0000
0xffffffff8002c69b30 services.exe         504    416     6    184    0  0  2019-05-03 06:32:36 UTC+0000
0xffffffff80027d9b30 lsass.exe           512    416     6     534    0  0  2019-05-03 06:32:37 UTC+0000
0xffffffff80027d81f0 lsm.exe             520    416    10    143    0  0  2019-05-03 06:32:37 UTC+0000
0xffffffff80029cd3e0 svchost.exe          620    504     9    345    0  0  2019-05-03 06:32:40 UTC+0000
0xffffffff8002d38b30 VBoxService.exe    688    504    12    135    0  0  2019-05-03 06:32:40 UTC+0000
0xffffffff8002a1bb30 svchost.exe          752    504     7    235    0  0  2019-05-02 18:02:51 UTC+0000
0xffffffff8002d70650 svchost.exe          852    504    22    473    0  0  2019-05-02 18:02:51 UTC+0000
0xffffffff8002d9c780 svchost.exe          892    504    17    427    0  0  2019-05-02 18:02:51 UTC+0000
0xffffffff8002dbe9e0 svchost.exe          920    504    29    878    0  0  2019-05-02 18:02:51 UTC+0000
0xffffffff8002e3db30 svchost.exe          400    504    10    281    0  0  2019-05-02 18:02:56 UTC+0000
0xffffffff8002e57890 svchost.exe          1004   504    20    379    0  0  2019-05-02 18:02:56 UTC+0000
0xffffffff8002fdab0 spoolsv.exe          1140   504    12    279    0  0  2019-05-02 18:02:57 UTC+0000
0xffffffff8002f2cb30 svchost.exe          1268   504    17    297    0  0  2019-05-02 18:02:59 UTC+0000
0xffffffff8002f81460 svchost.exe          1368   504    20    295    0  0  2019-05-02 18:02:59 UTC+0000
0xffffffff8003148b30 taskhost.exe         1788   504     8    159    1  0  2019-05-02 18:03:09 UTC+0000
0xffffffff8003172b30 explorer.exe        1860   1756    19    645    1  0  2019-05-02 18:03:09 UTC+0000
0xffffffff800315eb30 dnm.exe             1896    892     3     69    1  0  2019-05-02 18:03:09 UTC+0000
0xffffffff800300d700 VBoxTray.exe         1600   1860    13    141    1  0  2019-05-02 18:03:25 UTC+0000
0xffffffff8003367060 SearchIndexer        2180    504    11    629    0  0  2019-05-02 18:03:32 UTC+0000
0xffffffff80033f6060 WmiPrvSE.exe         2076    620     5    113    0  0  2019-05-02 18:03:55 UTC+0000
0xffffffff8003162060 svchost.exe          1820    504    11    317    0  0  2019-05-02 18:05:09 UTC+0000
0xffffffff8003371540 wmpnetwk.exe         2404    504    14    440    0  0  2019-05-02 18:05:10 UTC+0000
0xffffffff80014eeb30 taskhost.exe        1148    504     8    176    0  0  2019-05-02 18:09:58 UTC+0000
```

Найден второй ответ (2180).

4) Анализ последних открытых директорий пользователем:

- Результат:

```

*****
Registry: \\?\C:\Users\victim\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\1\0
Last updated: 2019-04-11 13:32:18 UTC+0000
Value Mru File Name Modified Date Create Date Access Date File Attr Path
-----
0 0 Temp 1970-01-01 00:00:00 UTC+0000 1970-01-01 00:00:00 UTC+0000 1970-01-01 00:00:00 UTC+0000 DIR Local\Temp
*****
Registry: \\?\C:\Users\victim\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\0
Last updated: 2019-04-27 10:33:47 UTC+0000
Value Mru File Name Modified Date Create Date Access Date File Attr Path
-----
0 0 victim 2019-04-10 15:59:34 UTC+0000 2019-04-10 15:58:54 UTC+0000 2019-04-10 15:59:34 UTC+0000 DIR C:\Users\victim
*****
Registry: \\?\C:\Users\victim\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\1
Last updated: 2019-04-27 10:34:47 UTC+0000
Value Mru File Name Modified Date Create Date Access Date File Attr Path
-----
0 0 Microsoft 1970-01-01 00:00:00 UTC+0000 1970-01-01 00:00:00 UTC+0000 1970-01-01 00:00:00 UTC+0000 DIR C:\ProgramData\Microsoft
*****
Registry: \\?\C:\Users\victim\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\2
Last updated: 2019-04-27 10:38:03 UTC+0000
Value Mru File Name Modified Date Create Date Access Date File Attr Path
-----
0 0 Capture 2019-04-27 10:36:06 UTC+0000 2019-04-18 00:49:00 UTC+0000 2019-04-27 10:36:06 UTC+0000 DIR C:\Program Files (x86)\Capture
*****
Registry: \\?\C:\Users\victim\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\2\0
Last updated: 2019-04-27 10:48:33 UTC+0000
Value Mru File Name Modified Date Create Date Access Date File Attr Path
-----
0 0 deleted files 2019-04-27 10:38:26 UTC+0000 2019-04-27 10:38:24 UTC+0000 2019-04-27 10:38:24 UTC+0000 NI, DIR Z:\logs\deleted files
*****
Registry: \\?\C:\Users\victim\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\5\2\2
Last updated: 2019-04-23 06:14:25 UTC+0000

```

Получен третий ответ (deleted_files).

5) Анализ открытых портов у пользователя.

- Результат:

```

windows Print Desktop Windows (verbose details)
wintree Print Z-Order Desktop Windows Tree
windscan Pool scanner for window stations
yarascan Scan process or kernel memory with Yara signatures

(kolya080808B Nikolapc)-[~/forenziks]
$ vol.py -f victim.raw --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P) Proto Local Address Foreign Address State PId Owner Created
0x5c201ca0 UDPv4 0.0.0.0:5005 ** 2464 wmpnetwk.exe 2019-05-02 18:05:14 UTC+0000
0x5c201ca0 UDPv4 ::5005 ** 2464 wmpnetwk.exe 2019-05-02 18:05:14 UTC+0000
0x5c49cbb0 UDPv4 0.0.0.0:59471 ** 1368 svchost.exe 2019-05-02 18:03:06 UTC+0000
0x5c4a31c0 UDPv4 0.0.0.0:59472 ** 1368 svchost.exe 2019-05-02 18:03:06 UTC+0000
0x5c4a31c0 UDPv6 ::59472 ** 1368 svchost.exe 2019-05-02 18:03:06 UTC+0000
0x5c4ac600 UDPv4 0.0.0.0:3702 ** 1368 svchost.exe 2019-05-02 18:03:14 UTC+0000
0x5c4ac600 UDPv6 ::3702 ** 1368 svchost.exe 2019-05-02 18:03:14 UTC+0000
0x5c510b30 UDPv4 0.0.0.0:3702 ** 1368 svchost.exe 2019-05-02 18:03:14 UTC+0000
0x5c537ec0 UDPv4 0.0.0.0:3702 ** 1368 svchost.exe 2019-05-02 18:03:14 UTC+0000
0x5c600360 UDPv4 0.0.0.0:0 ** 1004 svchost.exe 2019-05-02 18:02:56 UTC+0000
0x5c600360 UDPv6 ::0 ** 1004 svchost.exe 2019-05-02 18:02:56 UTC+0000
0x5c6918e0 UDPv4 0.0.0.0:5355 ** 1004 svchost.exe 2019-05-02 18:02:56 UTC+0000
0x5c6918e0 UDPv6 ::5355 ** 1004 svchost.exe 2019-05-02 18:02:56 UTC+0000
0x5c692940 UDPv4 0.0.0.0:5005 ** 2464 wmpnetwk.exe 2019-05-02 18:05:14 UTC+0000
0x5c692ae0 UDPv4 0.0.0.0:5355 ** 1004 svchost.exe 2019-05-02 18:02:56 UTC+0000
0x5c7bac70 UDPv4 0.0.0.0:5004 ** 2464 wmpnetwk.exe 2019-05-02 18:05:14 UTC+0000
0x5c7bac70 UDPv6 ::5004 ** 2464 wmpnetwk.exe 2019-05-02 18:05:14 UTC+0000
0x5c7f9600 UDPv4 0.0.0.0:3702 ** 1368 svchost.exe 2019-05-02 18:03:14 UTC+0000
0x5c7f9600 UDPv6 ::3702 ** 1368 svchost.exe 2019-05-02 18:03:14 UTC+0000
0x5c44e1b0 TCPv4 0.0.0.0:5357 0.0.0.0:0 LISTENING 4 System
0x5c44e1b0 TCPv6 ::5357 ::0 LISTENING 4 System

```

Получен четвертый ответ (UDP:5005).

6) Анализ нежелательно запущенных процессов:

- Результат:

```
(kolya080808 Nikolapc)-[~/forenziks]
$ vol.py -f victim.raw --profile=Win7SP1x64 malfind
Volatility Foundation Volatility Framework 2.6.1
Process: explorer.exe Pid: 1860 Address: 0x3ee0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x000000003ee0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000003ee0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000003ee0020 00 00 ee 03 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x000000003ee0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

0x000000003ee0000 0000          ADD [EAX], AL
0x000000003ee0002 0000          ADD [EAX], AL
0x000000003ee0004 0000          ADD [EAX], AL
0x000000003ee0006 0000          ADD [EAX], AL
0x000000003ee0008 0000          ADD [EAX], AL
0x000000003ee000a 0000          ADD [EAX], AL
0x000000003ee000c 0000          ADD [EAX], AL
0x000000003ee000e 0000          ADD [EAX], AL
0x000000003ee0010 0000          ADD [EAX], AL
0x000000003ee0012 0000          ADD [EAX], AL
0x000000003ee0014 0000          ADD [EAX], AL
0x000000003ee0016 0000          ADD [EAX], AL
0x000000003ee0018 0000          ADD [EAX], AL
0x000000003ee001a 0000          ADD [EAX], AL
0x000000003ee001c 0000          ADD [EAX], AL
0x000000003ee001e 0000          ADD [EAX], AL
0x000000003ee0020 0000          ADD [EAX], AL
0x000000003ee0022 ee          OUT DX, AL
0x000000003ee0023 0300          ADD EAX, [EAX]
0x000000003ee0025 0000          ADD [EAX], AL
0x000000003ee0027 0000          ADD [EAX], AL
```

```
Process: svchost.exe Pid: 1820 Address: 0x24f0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 128, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000024f0000 20 00 00 00 e0 ff 07 00 0c 00 00 00 01 00 05 00 .....
0x0000000024f0010 00 42 00 50 00 30 00 70 00 00 00 00 00 00 00 00 .B.P.0.p.~.....
0x0000000024f0020 48 8b 45 28 c7 00 00 00 00 00 c7 40 04 00 00 00 H.E(.....@....
0x0000000024f0030 00 48 8b 45 28 48 8d 40 08 48 89 c2 48 8b 45 20 .H.E(H.@.H..H.E.

0x0000000024f0000 2000          AND [EAX], AL
0x0000000024f0002 0000          ADD [EAX], AL
0x0000000024f0004 e0ff          LOOPNZ 0x24f0005
0x0000000024f0006 07          POP ES
0x0000000024f0007 000c00       ADD [EAX+EAX], CL
0x0000000024f000a 0000          ADD [EAX], AL
0x0000000024f000c 0100          ADD [EAX], EAX
0x0000000024f000e 050004200    ADD EAX, 0x420000
0x0000000024f0013 50          PUSH EAX
0x0000000024f0014 0030          ADD [EAX], DH
0x0000000024f0016 007000       ADD [EAX+0x0], DH
0x0000000024f0019 60          PUSHA
0x0000000024f001a 0000          ADD [EAX], AL
0x0000000024f001c 0000          ADD [EAX], AL
0x0000000024f001e 0000          ADD [EAX], AL
0x0000000024f0020 48          DEC EAX
0x0000000024f0021 8b4528       MOV EAX, [EBP+0x28]
0x0000000024f0024 c70000000000 MOV DWORD [EAX], 0x0
0x0000000024f002a c7400400000000 MOV DWORD [EAX+0x4], 0x0
0x0000000024f0031 48          DEC EAX
0x0000000024f0032 8b4528       MOV EAX, [EBP+0x28]
0x0000000024f0035 48          DEC EAX
0x0000000024f0036 8d4008       LEA EAX, [EAX+0x8]
```

```

Process: wmpnetwk.exe Pid: 2464 Address: 0x280000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 16, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x000000000280000 41 ba 80 00 00 00 48 b8 38 a1 e6 ff fe 07 00 00 A.....H.8.....
0x000000000280010 48 ff 20 90 41 ba 81 00 00 00 48 b8 38 a1 e6 ff H...A.....H.8...
0x000000000280020 fe 07 00 00 48 ff 20 90 41 ba 82 00 00 00 48 b8 ....H...A.....H.
0x000000000280030 38 a1 e6 ff fe 07 00 00 48 ff 20 90 41 ba 83 00 8.....H...A...

0x000000000280000 41                INC ECX
0x000000000280001 ba80000000        MOV EDX, 0x80
0x000000000280006 48                DEC EAX
0x000000000280007 b838a1e6ff        MOV EAX, 0xffe6a138
0x00000000028000c fe07              INC BYTE [EDI]
0x00000000028000e 0000              ADD [EAX], AL
0x000000000280010 48                DEC EAX
0x000000000280011 ff20              JMP DWORD [EAX]
0x000000000280013 90                NOP
0x000000000280014 41                INC ECX
0x000000000280015 ba81000000        MOV EDX, 0x81
0x00000000028001a 48                DEC EAX
0x00000000028001b b838a1e6ff        MOV EAX, 0xffe6a138
0x000000000280020 fe07              INC BYTE [EDI]
0x000000000280022 0000              ADD [EAX], AL
0x000000000280024 48                DEC EAX
0x000000000280025 ff20              JMP DWORD [EAX]
0x000000000280027 90                NOP
0x000000000280028 41                INC ECX
0x000000000280029 ba82000000        MOV EDX, 0x82
0x00000000028002e 48                DEC EAX
0x00000000028002f b838a1e6ff        MOV EAX, 0xffe6a138
0x000000000280034 fe07              INC BYTE [EDI]
0x000000000280036 0000              ADD [EAX], AL
0x000000000280038 48                DEC EAX
0x000000000280039 ff20              JMP DWORD [EAX]
0x00000000028003b 90                NOP
0x00000000028003c 41                INC ECX
0x00000000028003d ba                DB 0xba
0x00000000028003e 83                DB 0x83
0x00000000028003f 00                DB 0x0

```

Найден пятый ответ (1860;1820;2464).

7) Анализ tcr дампа по запущенным процессам (PID 1820,1860,2464)

- Результат:

```

(kolya080808@Nikolapc)-[~/forenziks]
$ vol.py -f victim.raw --profile=Win7SP1x64 -p 1860,1820,2464 memdump -D .
Volatility Foundation Volatility Framework 2.6.1
*****
writing explorer.exe [ 1860] to 1860.dmp
*****

```

```

(kolya080808@Nikolapc)-[~/forenziks]
$ strings 1820.dmp | grep www.go
www.google.ru
www.google.com
www.google.co.uk
www.go2it.ru
www.go4win.ru
www.gocaps.ru
www.goporn.ru

```

```

(kolya080808 Nikolapc) - [~/forenziks]
$ strings 1820.dmp | grep www.i
www.ikdy.cn
www.italu.com
www.ikarus.at
www.interoo.net
www.italu.com.br
www.intv.ru
www.ikaka.cn
www.imdb.com
www.ika-rus.com
www.i-seclab.org
www.ikaka.com
www.icsalabs.com

```

```

(kolya080808 Nikolapc) - [~/forenziks]
$ strings 1820.dmp | grep www.ic
www.icsalabs.com
www.icubed.com
www.ica.com

```

```

(kolya080808 Nikolapc) - [~/forenziks]
$ strings 1820.dmp | grep '\<202\....\.233\....\>'
202.107.233.211

```

```

(kolya080808 Nikolapc) - [~/forenziks]
$ strings 1820.dmp | grep '\<...\.200\...\.164\>'
http://209.200.12.164/drm/provider_license_v7.php

```

```

(kolya080808 Nikolapc) - [~/forenziks]
$ strings 1820.dmp | grep '\<209\.190\....\....\>'
http://209.190.122.186/drm/license-savenow.asp

```

Получены несколько ответов.

8) Анализ переменных окружения процессов.

- Результат:

```

(kolya080808 Nikolapc) - [~/forenziks]
$ vol.py -f victim.raw --profile=Win7SP1x64 envvars | grep 2464
Volatility Foundation Volatility Framework 2.6.1
2464 wmpnetwk.exe 0x000000000002c47a0 ALLUSERSPROFILE C:\ProgramData
2464 wmpnetwk.exe 0x000000000002c47a0 APPDATA C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
2464 wmpnetwk.exe 0x000000000002c47a0 CommonProgramFiles C:\Program Files\Common Files
2464 wmpnetwk.exe 0x000000000002c47a0 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
2464 wmpnetwk.exe 0x000000000002c47a0 CommonProgramW6432 C:\Program Files (x86)\Common Files
2464 wmpnetwk.exe 0x000000000002c47a0 COMPUTERNAME VICTIM-PC
2464 wmpnetwk.exe 0x000000000002c47a0 ComSpec C:\Windows\system32\cmd.exe
2464 wmpnetwk.exe 0x000000000002c47a0 FP_NO_HOST_CHECK NO
2464 wmpnetwk.exe 0x000000000002c47a0 LOCALAPPDATA C:\Windows\ServiceProfiles\NetworkService\AppData\Local
2464 wmpnetwk.exe 0x000000000002c47a0 NUMBER_OF_PROCESSORS 1
2464 wmpnetwk.exe 0x000000000002c47a0 OANOCACHE 1
2464 wmpnetwk.exe 0x000000000002c47a0 OS Windows_NT
2464 wmpnetwk.exe 0x000000000002c47a0 Path C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;
2464 wmpnetwk.exe 0x000000000002c47a0 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
2464 wmpnetwk.exe 0x000000000002c47a0 PROCESSOR_ARCHITECTURE AMD64
2464 wmpnetwk.exe 0x000000000002c47a0 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 42 Stepping 7, GenuineIntel
2464 wmpnetwk.exe 0x000000000002c47a0 PROCESSOR_LEVEL 6
2464 wmpnetwk.exe 0x000000000002c47a0 PROCESSOR_REVISION 2a07
2464 wmpnetwk.exe 0x000000000002c47a0 ProgramData C:\ProgramData
2464 wmpnetwk.exe 0x000000000002c47a0 ProgramFiles C:\Program Files
2464 wmpnetwk.exe 0x000000000002c47a0 ProgramFiles(x86) C:\Program Files (x86)
2464 wmpnetwk.exe 0x000000000002c47a0 ProgramW6432 C:\Program Files
2464 wmpnetwk.exe 0x000000000002c47a0 PSModulePath C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
2464 wmpnetwk.exe 0x000000000002c47a0 PUBLIC C:\Users\Public
2464 wmpnetwk.exe 0x000000000002c47a0 SystemDrive C:
2464 wmpnetwk.exe 0x000000000002c47a0 SystemRoot C:\Windows
2464 wmpnetwk.exe 0x000000000002c47a0 TEMP C:\Windows\TEMP
2464 wmpnetwk.exe 0x000000000002c47a0 TMP C:\Windows\TEMP
2464 wmpnetwk.exe 0x000000000002c47a0 USERDOMAIN WORKGROUP
2464 wmpnetwk.exe 0x000000000002c47a0 USERNAME VICTIM-PC$
2464 wmpnetwk.exe 0x000000000002c47a0 USERPROFILE C:\Windows\ServiceProfiles\NetworkService

```

Найден последний ответ (OANOCACHE).

Эта комната кажется простой, однако это не так. Она довольно сложная для тех, кто не установил тулзы. А в остальном - разобраться в программе и тадам! Готово!

Спасибо TryHackMe за прекрасную комнату по форензике!

Найденные уязвимости

Это задание на форензику, их здесь нет.

Видео выполнения

