Министерство науки и высшего образования Российской Федерации
Брянский государственный технический университет

Методические указания к выполнению практической работы №4 для слушателей программы повышения квалификации «Основы компьютерной криминалистики и методики реагирования на инциденты информационной безопасности»

Брянск
БГТУ
2022

Используя систему своего компьютера и утилит NIrSoft, составить протокол.

ПРОТОКОЛ № 4 от 2022 г.

Комиссия в составе:

Начала осмотр в:

Осмотр окончен:

Особенности осмотра:

Описание конфигурации устройств и программного обеспечения компьютера:

Объект осмотра:

Имя компьютера, на котором проводится осмотр: оперативная **память**:

Программы участвующие в анализе дампа-памяти:

Регистрация:

Перед комиссией поставлены следующие вопросы:

1. Присутствуют ли в системе открытые пароли?
   В дампе памяти не обнаружено

2. С какого сайта произошло последнее скачивание файла, что это за файл?
   С торрента bittorent, файл download.exe

3. Какие программы были запущены последние в памяти компьютера?
   Блокнот и командная строка

```
0xfffffa801b1fd960 notepad.exe           3304   3132      2       79      1      0 2018-08-04 19:34:10 UTC+0000
0xfffffa801a572b30 cmd.exe               3916   1428      0 --------      0      0 2018-08-04 19:34:22 UTC+0000   2018-08-04 19:34:22 UTC+0000
```

```
rocess: 4084 chrome.exe 2018-08-04 19:29:30 UTC+0000
rocess: 576 chrome.exe 2018-08-04 19:29:31 UTC+0000
rocess: 1808 chrome.exe 2018-08-04 19:29:32 UTC+0000
rocess: 3924 chrome.exe 2018-08-04 19:29:51 UTC+0000
rocess: 2748 chrome.exe 2018-08-04 19:31:15 UTC+0000
rocess: 3820 Rick And Morty 2018-08-04 19:32:55 UTC+0000
rocess: 3720 vmware-tray.ex 2018-08-04 19:33:02 UTC+0000
rocess: 3648 chrome.exe 2018-08-04 19:33:38 UTC+0000
rocess: 1796 chrome.exe 2018-08-04 19:33:41 UTC+0000
rocess: 3304 notepad.exe 2018-08-04 19:34:10 UTC+0000
mage: 0xfffffa801a2e1160, Address fffff960000e0000, Name: win32k.sys
mage: 0xfffffa801944c5f0, Address fffff960007b0000, Name: cdd.dll
```

4. В какое время была замечена последняя сессия пользования компьютером?
   Process: 3304 notepad.exe **2018-08-04 19:34:10 UTC+0000**

В момент осмотра установлены:

Результаты осмотра:

Комиссия постановила:

Подписи членов комиссии:

Используя команды в volatility заполнить протокол.

ПРОТОКОЛ № 4 от 2022 г.

Комиссия в составе:

Начала осмотр в:

Осмотр окончен:

Особенности осмотра:

Описание конфигурации устройств и программного обеспечения компьютера:

Объект осмотра:

Имя компьютера, на котором проводится осмотр: оперативная **память**:

Программы участвующие в анализе дампа-памяти:

Регистрация:

Перед комиссией поставлены следующие вопросы:

1. Являются ли представленный дамп памяти работоспособным
   Да, является

```
D:\Volatility>volatility -f OtterCTF.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\Volatility\OtterCTF.vmem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002c430a0L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002c44d00L
                KPCR for CPU 1 : 0xfffff880009ef000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2018-08-04 19:34:22 UTC+0000
     Image local date and time : 2018-08-04 22:34:22 +0300
```

2. Содержат ли какие-то процессы подозрительные расположения файлов?
   Да, содержат

```
0xfffffa801aa00a90 chrome.exe            3924   4076     16      228      1      0 2018-08-04 19:29:51 UTC+0000
0xfffffa801a7f98f0 chrome.exe            2748   4076     15      181      1      0 2018-08-04 19:31:15 UTC+0000
0xfffffa801b486b30 Rick And Morty        3820   2728      4      185      1      1 2018-08-04 19:32:55 UTC+0000
0xfffffa801a4c5b30 vmware-tray.ex        3720   3820      8      147      1      1 2018-08-04 19:33:02 UTC+0000
0xfffffa801b18f060 WebCompanionIn        3880   1484     15      522      0      1 2018-08-04 19:33:07 UTC+0000
0xfffffa801a635240 chrome.exe            3648   4076     16      207      1      0 2018-08-04 19:33:38 UTC+0000
0xfffffa801a5ef1f0 chrome.exe            1796   4076     15      170      1      0 2018-08-04 19:33:41 UTC+0000
```

```
D:\Volatility>volatility -f OtterCTF.vmem --profile=Win7SP1x64 dlllist -p 3820
Volatility Foundation Volatility Framework 2.6
************************************************************************
Rick And Morty pid:   3820
Command line : "C:\Torrents\Rick And Morty season 1 download.exe"
Note: use ldrmodules for listing DLLs in Wow64 processes

Base                             Size          LoadCount Path
-------------------- ---------- ---------- ------ ----
0x0000000000400000           0x56000            0xffff C:\Torrents\Rick And Morty season 1 download.exe
0x00000000776f0000           0x1a9000           0xffff C:\Windows\SYSTEM32\ntdll.dll
0x0000000075210000           0x3f000               0x3 C:\Windows\SYSTEM32\wow64.dll
0x000000000751b0000           0x5c000               0x1 C:\Windows\SYSTEM32\wow64win.dll
0x000000000751a0000            0x8000               0x1 C:\Windows\SYSTEM32\wow64cpu.dll
```

3. Какие сайты часто посещались владельцем дампа-памяти?

Выгрузив в xls результаты команды netscan, и сделав сводную таблицу с подсчетом кол-ва адресов из поля address,

Названия строк	Количество по полю Address
185.154.111.20:60405	1
188.129.94.129:25128	1
191.177.124.34:21011	1
191.253.122.149:59163	1
196.250.217.22:32815	1
209.236.6.89:56500	1
212.92.105.227:8999	1
23.37.43.27:80	4
38db:c41a:80fa:ffff:38db:c41a:80fa:ffff:0	1
45.27.208.145:51414	1

получим, что чаще всего посещались ресурсы:

Названия строк	Количество по полю Address
23.37.43.27:80	4
104.18.20.226:80	2
122.62.218.159:11627	2
4847:d418:80fa:ffff:4847:d418:80fa:ffff:0	2
56.219.196.26:0	2
72.55.154.81:80	2
77.126.30.221:13905	2

Самый частый ресурс 23.37.43.27:80

4. Присутствуют ли в дампе памяти вредоносные программы, т.е. приводящие к несанкционированному уничтожению, блокированию, модификации, копированию информации с носителей ПЭВМ без предварительного уведомления об этих операциях собственника компьютерной информации?

Да, присутствуют. Порождены процессом 3820 download.exe

```
Volatility Foundation Volatility Framework 2.6
************************************************************************
vmware-tray.ex pid:   3720
Command line : "C:\Users\Rick\AppData\Local\Temp\RarSFX0\vmware-tray.exe"
Note: use ldrmodules for listing DLLs in Wow64 processes


Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x0000000000ec0000           0x6e000            0xffff C:\Users\Rick\AppData\Local\Temp\RarSFX0\vmware-tray.exe
0x00000000776f0000          0x1a9000            0xffff C:\Windows\SYSTEM32\ntdll.dll
0x0000000075210000           0x3f000               0x3 C:\Windows\SYSTEM32\wow64.dll
0x00000000751b0000           0x5c000               0x1 C:\Windows\SYSTEM32\wow64win.dll
0x00000000751a0000            0x8000               0x1 C:\Windows\SYSTEM32\wow64cpu.dll

D:\Volatility>
```

executable.3720.exe – троян, сразу удалился антивирусом после выполнения:

```
D:\Volatility>volatility -f OtterCTF.vmem --profile=Win7SP1x64 procdump -p 3720 --dump-dir=D:\Volatility\dump
Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa801a4c5b30 0x0000000000ec0000 vmware-tray.ex       OK: executable.3720.exe
```

Еще подозрительный файл dotNetFx40_Full_x86_x64.exe

```
2010-03-18 20:16:28 UTC+0000|[SHIMCACHE]| \??\C:\Caeac7f1d3b263fea4486e\Setup.exe|
2018-08-04 18:45:41 UTC+0000|[SHIMCACHE]| \??\C:\Users\Rick\Downloads\dotNetFx40_Full_x86_x64.exe|
2011-04-06 23:16:16 UTC+0000|[SHIMCACHE]| \??\C:\cb01b266df358d92e406578d\Setup.exe|
2018-08-01 19:21:14 UTC+0000|[SHIMCACHE]| \??\C:\Users\Rick\Downloads\NDP40-KB2468871-v2-x64.exe|
2018-07-23 22:48:16 UTC+0000|[SHIMCACHE]| \??\C:\Users\Rick\Desktop\vmware-tray.exe|
2010-11-21 03:23:47 UTC+0000|[SHIMCACHE]| \??\C:\Windows\System32\fsquirt.exe|
2009-07-14 01:14:18 UTC+0000|[SHIMCACHE]| \??\C:\Windows\SysWOW64\DllHost.exe|
```

5. Под каким пользователем велись подозрительные операции?
   Под единственным пользователем Rick

В момент осмотра установлены:

Результаты осмотра:

Комиссия постановила:

Подписи членов комиссии: