Министерство образования республики Молдова

Технический Университет Молдовы

Департамент Программной Инженерии и Автоматики

О т ч ё т

Лабораторная работа №6

По предмету: Infractiuni informatice si tehnici de investigare

Выполнил студ. гр. SI-202 Абабий Эдуард

Проверил Масютин Максим

Кишинёв – 2023

Scopul acestui laborator este de a-i învăța pe studenți să extragă și să analize fișierele de Registru pentru orice artefacte relevante.

Sarcina:

1. Completați câmpurile libere de mai jos cu informația corespunzătoare, obținută în urma analizei fișierelor!

Rezolvarea sarcinilor:

Folosiți produsul din NTUSER.DAT pentru a răspunde la următoarele întrebări.

1. Din ce fus orar sunt datele și orele care apar pentru artefactele de registru?

   UTC

2. Câte documente word au fost vizualizate recent prin Explorer? Care au fost numele de fișiere?
   2 / To do list.docx / 2017 enhancement quote.docx

```
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx
LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)
MRUListEx = 1,0
  1 = To do list.docx
  0 = 2017 enhancement quote.docx
```

3. Au fost alte documente menționate în NTUSER.DAT? Dacă da, de ce acestea nu s-au regăsit în Registru?
   Да, они подверглись записи, но не открывались из file explorer

```
Document 0
LastWrite: Thu Jan  1 00:00:00 1970 UTC
Datetime: 2017-07-25T11:23
File Path: C:\Users\Rock Hammerfist\Documents\To do list.docx
Position: 0 0

Document 1
LastWrite: Thu Jan  1 00:00:00 1970 UTC
Datetime: 2017-08-01T10:57
File Path: C:\Users\Rock Hammerfist\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\BeerMenu.docx
Position: 1745732857 0
```

4. Pe ce cale a fost accesat acesta și la ce oră? (Sugestie: adăugați în cronologie)
   Файл был открыт 1 августа 14:56:30 2017
   %USERPROFILE%/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/BeerMenu.docx

```
**Word**
----------
Security key LastWrite: Thu Jan  1 00:00:00 1970 Z
Tue Aug  1 14:56:30 2017 Z : %USERPROFILE%/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/BeerMenu.docx
```

5. A fost instalat CCleaner și dacă da, când?
   Да, 18 марта 18 20:58:39 2017 года

```
Sat Mar 18 20:58:39 2017 - C:\Users\Rock Hammerfist\Downloads\cc_setup532.exe
```

6. Ce a fost executat pe 8/1/17 la 17:56:12? În ce cheie s-a găsit acesta? (Sugestie: adăugați în cronologie)

   Был запущен файл javainstall.exe

```
Tue Aug  1 17:56:12 2017 Z
  {F38BF404-1D43-42F2-9305-67DE0B28FC23}\javainstall.exe (1)
```

7. Ce aplicații au fost setate la autorun? Având în vedere că este NTUSER.DAT, ce înseamnă acest lucru?
   9129837.exe / OneDrive.exe / CCleaner64.exe были установлены в автозапуск. Имея ввиду, что файл NTUSER.DAT, это значит что эти программы были установлены в автозапуск для пользователя Rock Hammerfist

```
Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)
  ttool: C:\Windows\9129837.exe
  OneDrive: "C:\Users\Rock Hammerfist\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
  CCleaner Monitoring: "C:\Program Files\CCleaner\CCleaner64.exe" /MONITOR
```

Folosiți produsul din SOFTWARE pentru a răspunde la următoarele întrebări.

1. Câte dispozitive USB au fost introduse în acest sistem? Care cheie v-a spus acest lucru?

   4 / ключём для поиска было USB

```
RemovDev
Microsoft\Windows Portable Devices\Devices
LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)

Device    : DISK&VEN_KANGURU&PROD_FLASHBLU&REV_PMAP
LastWrite : Thu Jan  1 00:00:00 1970 (UTC)
SN        : 58970B02D6C00020&0
Drive     : UNTITLED

Device    : DISK&VEN_PNY&PROD_USB_2.0_FD&REV_1100
LastWrite : Thu Jan  1 00:00:00 1970 (UTC)
SN        : AD4B33D110000014280
Drive     : USB20FD

Device    : DISK&VEN_UT163&PROD_USB2FLASHSTORAGE&REV_0.00
LastWrite : Thu Jan  1 00:00:00 1970 (UTC)
SN        : 0000000000083A80
Drive     : E:\

Device    : DISK&VEN_UT165&PROD_USB2FLASHSTORAGE&REV_0.00
LastWrite : Thu Jan  1 00:00:00 1970 (UTC)
SN        : 000000000018CA80
Drive     : Untitled

----------------------------------------
```

2. Ce programe au fost setate la autorun?

   MSASCuil.exe / vmtoolsd.exe

```
Microsoft\Windows\CurrentVersion\Run
LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)
  SecurityHealth - %ProgramFiles%\Windows Defender\MSASCuiL.exe
  VMware User Process - "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
```

3. Comparativ cu NTUSER.DAT, sunt aceleași programe? Dacă nu, de ce?

   Нет, это не те же программы. NTUSER.DAT содержит в себе настройки для определенного пользователя, а SOFTWARE сохраняет информацию вне зависимости от пользователя

4. Ce versiune de Windows a fost instalată pe acest sistem? Când a fost instalată aceasta?

   Windows 10 Pro, установлена 5 июля 14:34:02 2017 года

```
EditionSubstring :
RegisteredOrganization :
CurrentMinorVersionNumber : 0
CurrentMajorVersionNumber : 10
CurrentVersion : 6.3
UBR : 483
ReleaseId : 1703
CurrentBuild : 15063
CurrentBuildNumber : 15063
InstallationType : Client
SoftwareType : System
SystemRoot : C:\Windows
PathName : C:\Windows
BuildBranch : rs2_release
CompositionEditionID : Professional
EditionID : Professional
RegisteredOwner : Windows User
ProductName : Windows 10 Pro
CurrentType : Multiprocessor Free
ProductId : 00330-80111-56309-AA714
BuildLab : 15063.rs2_release.170317-1834
InstallDate : Wed Jul  5 14:34:02 2017 (UTC)
InstallTime : Wed Jul  5 14:34:02 2017 (UTC)
BuildGUID : ffffffff-ffff-ffff-ffff-ffffffffffff
BuildLabEx : 15063.0.amd64fre.rs2_release.170317-1834
```

Folosiți produsul din SYSTEM pentru a răspunde la următoarele întrebări.

1. Care este numele gazdei sistemului victimă?

   DESKTOP-M1MPF90

```
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = DESKTOP-M1MPF90
TCP/IP Hostname = DESKTOP-M1MPF90
```

2. Care este dimensiunea maximă pentru Security Event log?

   Максимальный размер для Security Event Log – 20.00 MB

```
Security \ Thu Jan  1 00:00:00 1970Z
  File              = %SystemRoot%\System32\winevt\Logs\Security.evtx
  DisplayNameFile   = %SystemRoot%\system32\wevtapi.dll
  MaxSize           = 20.00MB
  Retention         = 0 sec
```

3. Ce adresă IP a fost atribuită ultima dată adaptorului de rețea?

   192.168.95.131

```
ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
Adapter: {5e3a751e-7abd-4587-8ea9-2ca2c0b5807f}
LastWrite Time: Thu Jan  1 00:00:00 1970 Z
  EnableDHCP                    1
  Domain
  NameServer                    192.168.95.130
  DhcpIPAddress                 192.168.95.131
  DhcpSubnetMask                255.255.255.0
  DhcpServer                    192.168.95.254
```

4. La ce fus orar a fost configurat sistemul?

   UTC Eastern Standard Time

```
TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)
  DaylightName    -> @tzres.dll,-111
  StandardName    -> @tzres.dll,-112
  Bias            -> 300 (5 hours)
  ActiveTimeBias -> 240 (4 hours)
  TimeZoneKeyName-> Eastern Standard Time
----------------------------------------
```

Folosiți instrumentul lui Eric Zimmerman AppCompatCacheParser pentru a răspunde la următoarele întrebări. Deschideți un prompt de comandă(cmd) și navigați către folderul unde ați salvat instumentul descărcat și tapați comanda “AppCompatCacheParser.exe –f SYSTEM --csv *filename*”.

1. Se afișează aici vreunul dintre programele setate la autorun? Care este marcajul temporal?

   9129837.exe Год создания 2008, несмотря на то, что система была установлена в 2017 году

1	C:\Windows\9129837.exe	12.11.2008 06:07	NA
2	C:\Windows\notepad.exe	18.03.2017 20:58	NA

2. Are acest marcaj vreunul dintre alte programe?

   Javainstall.exe

1	C:\Windows\9129837.exe	12.11.2008 06:07	NA
2	C:\Windows\notepad.exe	18.03.2017 20:58	NA
3	C:\Windows\bfsvc.exe	03.06.2017 08:51	NA
4	C:\Windows\HelpPane.exe	03.06.2017 08:59	NA
5	C:\Windows\hh.exe	18.03.2017 20:57	NA
6	C:\Windows\javainstall.exe	12.11.2008 06:07	NA

3. Chiar dacă marcajul temporal este oprit, ce ar putea însemna faptul că au același marcaj temporal?

   Есть 2 варианта:
   1. Этот файл мог попасть в компьютер после запуска javainstall.exe и это может быть троян или шпионское ПО.
   2. Этот файл попал иным способом в компьютер и является трояном-загрузчиком, которому для полноценной работы необходим был файл javainstall.exe, который он успешно загрузил и запустил

4. Există vreun artefact care ar arăta că PSEXEC a fost rulat? Care este marcajul temporal și posibila semnificație criminalistică? (Sugestie: PSEXEC este un instrument Sysinternals care permite utilizatorului să ruleze de la distanță aplicații pe un sistem. Atunci când este executat, numele fișierului nu este psexec.exe, dar este aproape de acesta.) (Sugestie: adăugați în cronologie)

   fDenyTSConnections показывает что подключений на момент не было, но 1 подключение было отказано, возможно, что PSEXEC был запущен

12	C:\Windows\PSEXESVC.exe	01.08.2017 17:48	NA

```
ControlSet001\Control\Terminal Server
LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)

Reference: http://support.microsoft.com/kb/243215

  ProductVersion = 5.1

  fDenyTSConnections = 0
  1 = connections denied
```

Вывод: В данном лабораторной работе я научился работать с файлами HIVE и анализировать их. Благодаря такому способу, можно узнать какие шаги и пути предпринял злоумышленник.