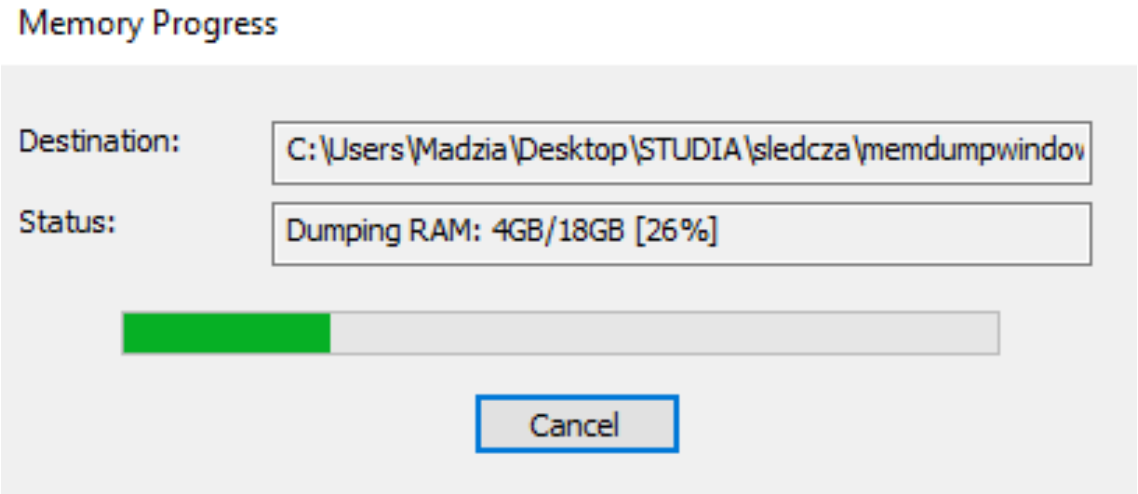
Informatyka Śledcza - Laboratorium 6

Magdalena Ślusarczyk

1 Zadanie 1

Przy użyciu programu FTK Imager został utworzony przeze mnie zrzut pamięci systemu Windows.



2 Zadanie 2

Przy użyciu avml tworzę zrzut pamięci z Linuxa i odczytuję go poleceniem strings.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ chmod 755 avml

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo ./avml nazwa.dmp
[sudo] password for kali:

┌──(kali㉿kali)-[~/Downloads]
└─$ strings nazwa.dmp
strings: nazwa.dmp: Permission denied

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo strings nazwa.dmp
EMiL
PAMS
PAMS
4{,%$l
ZRr=
`|f
\|f1
GRUB
Geom
Hard Disk
Read
```

W takiej formie bardzo ciężko odczytać coś sensownego z wykonanego zrzutu. Uzycie polecenia grep do odszukania odwiedzonej strony:

```
┌──(root💀kali)-[/home/kali/Downloads]
└─# strings ./nazwa.dmp| grep https://upel2.cel.agh.edu.pl/wiet/login/index.php
https://upel2.cel.agh.edu.pl/wiet/login/index.php
https://upel2.cel.agh.edu.pl/wiet/login/index.php
https://upel2.cel.agh.edu.pl/wiet/login/index.php
```

To samo dla odnalezienia wyświetlanego obrazka:

```
┌──(root💀kali)-[/home/kali/Downloads]
└─# strings ./nazwa.dmp| grep kotek-mruczek
kotek-mruczek--naklejka.-naklejka-dla-dzieci.-dekoracje-pokoju
kotek-mruczek--naklejka.-naklejk
kotek-mruczek--naklejka.-naklejk
kotek-mruczek--naklejka.-naklejk@
kotek-mruczek--naklejka.-naklejka-dla-dzieci.-dekoracje-pokoju.jpg
/home/kali/Downloads/kotek-mruczek--naklejka.-naklejka-dla-dzieci.-dekoracje-pokoju.jpg
```

3 Zadanie 3

3.1 Postawowe informacje o obrazie

```
┌──(root💀kali)-[/home/kali/Desktop/vol/volatility-master]
└─# python vol.py -f /home/kali/Desktop/memory3.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/memory3.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2010-08-15 18:24:00 UTC+0000
     Image local date and time : 2010-08-15 14:24:00 -0400
```

Sugerowane przez program profile to WinXPSP2x86 i WinXPSP3x86.
Adres KDGB prowadzi do struktury zawierającej listę procesów i modułów.
DTB służy do translacji adresu wirtualnego na adres fizyczny.
KPCR zawiera informacje na temat procesora.

3.2 Lista procesów

```
┌──(root💀kali)-[/home/kali/Desktop/vol/volatility-master]
└─# python vol.py -f /home/kali/Desktop/memory3.vmem --profile=WinXPSP3x86 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x810b1660 System                    4      0     58      183 ------      0
0xff2ab020 smss.exe                544      4      3       21 ------      0 2010-08-11 06:06:21 UTC+0000
0xff1ecda0 csrss.exe               608    544     10      369      0      0 2010-08-11 06:06:23 UTC+0000
0xff1ec978 winlogon.exe            632    544     20      518      0      0 2010-08-11 06:06:23 UTC+0000
0xff247020 services.exe            676    632     16 --------      0      0 2010-08-11 06:06:24 UTC+0000
0xff255020 lsass.exe               688    632     19      344 ------      0 2010-08-11 06:06:24 UTC+0000
0xff218230 vmacthlp.exe            844    676      1       24      0      0 2010-08-11 06:06:24 UTC+0000
0x80ff88d8 svchost.exe             856    676     17      199      0      0 2010-08-11 06:06:24 UTC+0000
0xff217560 svchost.exe             936    676     10      272      0      0 2010-08-11 06:06:24 UTC+0000
0x80fbf910 svchost.exe            1028    676     71     1341      0      0 2010-08-11 06:06:24 UTC+0000
0xff22d558 svchost.exe            1088    676      5       80      0      0 2010-08-11 06:06:25 UTC+0000
0xff203b80 svchost.exe            1148    676     14      208      0      0 2010-08-11 06:06:26 UTC+0000
0xff1d7da0 spoolsv.exe            1432    676     13      135      0      0 2010-08-11 06:06:26 UTC+0000
0xff1b8b28 vmtoolsd.exe           1668    676      5      221      0      0 2010-08-11 06:06:35 UTC+0000
0xff1fdc88 VMUpgradeHelper        1788    676      4      100 ------      0 2010-08-11 06:06:38 UTC+0000
0xff143b28 TPAutoConnSvc.e        1968    676      5      100      0      0 2010-08-11 06:06:39 UTC+0000
```

offset - adres w pamięci, PID - ID procesu, PPID - ID procesu rodzica, Thds - liczba wątków, Hnds - liczba uchwytów, Sess - session ID, Wow64 - czy jest to proces architektury 32bitowej uruchomiony na systemie 64bitowym.
(V) oznacza adres wirtualny.
Proces cmd.exe został zamknięty 2010-08-15 o godz. 18:24:00.
System i smss.exe nie mają session ID bo startują przed sesjami.
VMwareUser.exe ma PID 452.
Wykonanie wcześniejszego polecenia z opcją -P zmienia offset na adres fizyczny.

Pstree:

```
┌──(root💀kali)-[/home/kali/Desktop/vol/volatility-master]
└─# python vol.py -f /home/kali/Desktop/memory3.vmem --profile=WinXPSP3x86 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x810b1660:System                                     4      0     58    183 1970-01-01 00:00:00 UTC+0000
. 0xff2ab020:smss.exe                                544      4      3     21 2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe                           632    544     20    518 2010-08-11 06:06:23 UTC+0000
... 0xff255020:lsass.exe                             688    632     19    344 2010-08-11 06:06:24 UTC+0000
... 0xff247020:services.exe                          676    632     16 ------ 2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe                        1668    676      5    221 2010-08-11 06:06:35 UTC+0000
..... 0xff125020:cmd.exe                            1136   1668      0 ------ 2010-08-15 18:24:00 UTC+0000
.... 0x80ff88d8:svchost.exe                          856    676     17    199 2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0:spoolsv.exe                         1432    676     13    135 2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe                         1028    676     71   1341 2010-08-11 06:06:24 UTC+0000
..... 0x80f94588:wuauclt.exe                         468   1028      4    134 2010-08-11 06:09:37 UTC+0000
..... 0xff364310:wscntfy.exe                         888   1028      1     27 2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe                          936    676     10    272 2010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e                     1968    676      5    100 2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e                    1084   1968      1     61 2010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe                         1088    676      5     80 2010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe                         844    676      1     24 2010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0:alg.exe                              216    676      6    105 2010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe                         1148    676     14    208 2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper                     1788    676      4    100 2010-08-11 06:06:38 UTC+0000
... 0x80fdc368:logon.scr                             124    632      1     15 2010-08-15 18:21:28 UTC+0000
.. 0xff1ecda0:csrss.exe                              608    544     10    369 2010-08-11 06:06:23 UTC+0000
 0xff3865d0:explorer.exe                            1724   1708     12    341 2010-08-11 06:09:29 UTC+0000
. 0xff3667e8:VMwareTray.exe                          432   1724      1     49 2010-08-11 06:09:31 UTC+0000
. 0xff374980:VMwareUser.exe                          452   1724      6    189 2010-08-11 06:09:32 UTC+0000
. 0xff3ad1a8:IEXPLORE.EXE                           2044   1724     10    366 2010-08-15 18:11:17 UTC+0000
```

Wcięcia i kropki wskazują na procesy - dzieci.
W tabeli nie ma session ID.

Procesem nadrzędnym procesu smss.exe jest System.
smss.exe jest częścią systemu Windows - menadżerem sesji.

3.3 Biblioteki dll

Udało się odzyskać plik module.124.113f368.77f60000.dll

```
┌──(root💀kali)-[/home/kali/Desktop/dlldump]
└─# find . -name "module.124.113f368.77f60000.dll"
./module.124.113f368.77f60000.dll
```

3.4 Uchwyty

```
┌──(root💀kali)-[/home/kali/Desktop/vol/volatility-master]
└─# python vol.py -f /home/kali/Desktop/memory3.vmem --profile=WinXPSP3x86 handles -p 1668 -t Process
Volatility Foundation Volatility Framework 2.6.1
Offset(V)     Pid     Handle     Access Type            Details
---------- ------ ---------- ---------- --------------- -------
0xff125020   1668      0x378   0x1f0fff Process         cmd.exe(1136)
```

PID należy do procesu vmtoolsd.exe. Posiada on aktywny uchwyt do procesu cmd.exe, który ma PID 1136.

3.5 Uprawnienia

Wskaźnik (S-1-5-32-544) należy do uprawnień administratora.

3.6 Wersje plików

Plik: SAMLIB.dll
Wersja: 5.1.2600.2180, OS: Windows NT
Plik: TPAutoConnect.exe.
Wersja: 7.17.512.1, LegalCopyright: Copyright (c) 1999-2009 ThinPrint AG

3.7 Przeglądarka

PID IEXPLORE.EXE: 2044
Godzina uruchomienia: 18:11:17
Yahoo nie została uruchomiona, ale bing tak:

```
**************************************************
Process: 2044 IEXPLORE.EXE
Cache type "URL " at 0xa77400
Record length: 0x180
Location: http://www.bing.com/partner/primedns.gif
Last modified: 2007-05-30 19:42:28 UTC+0000
Last accessed: 2010-08-15 18:11:22 UTC+0000
File Offset: 0x180, Data Offset: 0x94, Data Length: 0xa4
File: primedns[1].gif
Data: HTTP/1.1 200 OK
Content-Length: 43
Content-Type: image/gif
ETag: 325472601571F31E1BF00674C368D3350000002B

~U:administrator
```

3.8 Wirus

```
┌──(root💀kali)-[/home/kali/Desktop/vol/volatility-master]
└─# python vol.py -f /home/kali/Desktop/memory3.vmem --profile=WinXPSP3x86 procdump -p 468 -D /home/kali/Desktop/virus/
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x80f94588 0x00400000 wuauclt.exe          OK: executable.468.exe

┌──(root💀kali)-[/home/kali/Desktop/vol/volatility-master]
└─# md5sum /home/kali/Desktop/virus/executable.468.exe
21c183cdabccc7675b50258313812bc7  /home/kali/Desktop/virus/executable.468.exe
```

Po sprawdzeniu md5sum w virustotal okazuje się, że jest to trojan: