

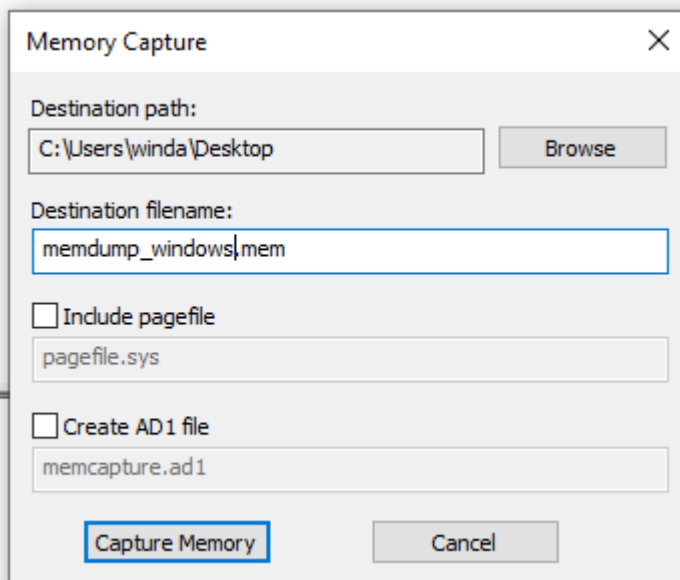
Zadanie 1 – Tworzenie zrzutu pamięci z systemu Windows	2
Zadanie 2 – Tworzenie zrzutu pamięci z systemu Linux	3
Zadanie 3 – Analiza pamięci przy wykorzystaniu programu Volatility	5
5. Odpowiedz na pytania:	5
a. Jakie sugerowane profile są aktualnie podpowiadane przez program?	5
b. Do czego wykorzystywany jest adres KDBG?	5
c. DTB (Directory Table Base) – jest używany do translacji wirtualnego adresu na jaki adres?	5
d. O czym świadczą dane zawarte w KPCR (Kernel Processor Control Region) w odniesieniu do badanego obrazu?	5
6. Volatility wymaga do prawidłowej analizy wskazania profilu badanego obrazu. Wywołaj funkcje wyświetlenia listy procesów systemu:	6
a. Jakie informacje zawierają poszczególne kolumny:	6
b. O czym świadczy znacznik (V) w rubryce Offset?	6
c. Który z niżej opisanych procesów został zakończony i kiedy?	6
d. Dlaczego procesy „System” i „smss.exe” nie posiadają informacji w rubryce Sess?	6
e. Który numer procesu należy do VMwareUser.exe?	7
7. Wykonaj polecenie:	7
8. Wyświetlając listę procesów w formie „drzewa”:	8
a. Co oznaczają wyświetlone wcięcia i kropki?	8
b. Jakiego identyfikatora nie znajdziemy w prezentowanych tabelach?	8
c. Procesem nadrzędnym procesu smss.exe jest...?	8
d. Za co odpowiedzialny jest proces smss.exe?	8
9. Wykorzystując wskaźnik -h odszukaj i wyświetl załadowane biblioteki dll w badanym obrazie na podstawie procesu wscntfy.exe (Podpowiedź: do wyszukanego wskaźnika dodaj -p i podaj id procesu wscntfy.exe).	8
10. Przy pomocy polecenia dlldump wypakuj pliki dll w nowo utworzonym folderze:	9
Czy udało się odzyskać plik: module.124.113f368.77f60000.dll?	10
11. Wyświetl otwarte powiązania „uchwyty” we wskazanym procesie i odpowiedz na pytania:	10
a. Do jakiego procesu należy wskazany PID (1168)?	10
b. Z jakim procesem wskazany PID (1168) posiada aktywny „uchwyt”?	10
c. Podaj PID odnalezionego aktywnego powiązanego procesu.	10
12. Polecenie Getsids wyświetla identyfikatory SID (Security Identifiers) powiązany z procesem. W ten sposób jesteśmy w stanie uchwycić procesy, które mają złośliwy charakter i mogą eskalować uprawnienia. Do jakich uprawnień należy wskaźnik (S-1-5-32-544)?	10
13. Przy wykorzystaniu wtyczki verinfo jesteśmy w stanie wyświetlić informacje o wersjach które zostały osadzone w plikach PE (nie wszystkie pliki posiadają te informacje). Odpowiedz na pytania:	11
b. Podaj jego OS.	11

- c. Podaj wersję pliku: C:\ProgramFiles\VMware\VMware\Tools\TPAutoConnect.exe.
11
- d. Podaj LegalCopyright ww. pliku. 12
14. Wykorzystaj wtyczkę odpowiedzialną za przeglądarkę internetową IE i odpowiedz na pytania: 12
- a. Podaj PID procesu IEXPLORE.EXE. 12
 - b. O której została uruchomiona przeglądarka? 12
 - c. Czy została wyświetlona strona www.yahoo.com? 12
 - d. Czy została wyświetlona strona www.bing.com? 12
15. Proszę o wyeksportowanie procesu pod nazwą wuauclt.exe: Poprawnie wykonane polecenie zwróci do utworzonego folderu plik (executable.468.exe) z procesu. Wykonaj jego analizę poprzez sprawdzenie sumy kontrolnej (np. md5sum) i poddaj go weryfikacji pod kątem obecności złośliwego oprogramowania (www.virustotal.com). Proszę o załączenie wyników z wykonanego działania. 12

Zadanie 1 – Tworzenie zrzutu pamięci z systemu Windows

Instalacja przeszła pomyślnie

Następnie tworzę zrzut pamięci RAM



Zadanie 2 – Tworzenie zrzutu pamięci z systemu Linux

```
(kali㉿kali)-[~]  
$ ./avml  
error: The following required arguments were not provided:  
  <filename>  
  
USAGE:  
  avml [FLAGS] [OPTIONS] <filename>  
  
For more information try --help
```

Udało się zainstalować **avml**

Tworzę zrzut pamięci RAM

```
(kali㉿kali)-[~]  
$ sudo ./avml kali_memory.dmp
```

Ręcznie odnalezienie interesujących nas danych może być problematyczne z uwagi na wielkość pliku

```
[arek@fedora lab6] $ wc -l kali_memory.dmp  
9017189 kali_memory.dmp
```

```
d?EDV  
e?EDV  
a?EDV  
 d?EDV  
\?EDV  
 d?EDV  
@d?EDV  
@d?EDV  
`d?EDV  
@k?EDV
```

Zresztą większość znaków to niezrozumiałe ciągi, niezawierające przydatnych informacji

Tutaj otwarta strona internetowa

```
[arek@fedora lab6] $ strings kali_memory.dmp | grep mbappe
https://duckduckgo.com/?t=ffab&q=mbappe
https://duckduckgo.com/?t=ffab&q=mbappe
https://duckduckgo.com/?t=ffab&q=mbappe
https://duckduckgo.com/?t=ffab&q=mbappe
https://duckduckgo.com/?t=ffab&q=mbappe
https://duckduckgo.com/?t=ffab&q=mbappe
https://duckduckgo.com/?t=ffab&q=mbappe
0^partitionKey=%28https%2Cduckduckgo.com%29,::https://external-content.duckduckg
o.com/ip3/kyliambappe.com.ico
s://duckduckgo.com/?t=ffab&q=mbappe&ia=webm
s://duckduckgo.com/?t=ffab&q=mbappe&ia=webm
0^partitionKey=%28https%2Cduckduckgo.com%29,::https://external-content.duckduckg
o.com/ip3/kyliambappe.com.ico
```

```
https://improving.duckduckgo.com/t/iaoi_wikipedia_fathead_deep?9810174&ss=0&sp=1
&im=1&ism=1&px=0&ul=0&pl=7&wt=Kylian%20Mbapp%C3%A9&ibv=0&timeSincePageLoad=826&t
imeSinceDeepStarted=0&timeSinceDeepFinished=0&q=mbappe&ct=PL&d=d&kl=wt-wt&rl=us-
en&kp=-1&serp_return=0&g=vb&sm=wikipedia_fathead_deep:i:medium&blay=w1n1i1w27r1,
i1e1w1&dsig=about:m&biaexp=b&default_search_atb=b&infoboxexp=d&mrvrtexp=b&pctaex
p=b
duckduckgo.com image https://improving.duckduckgo.com/t/tqpae?5908874&a=ffab&ct=
PL&ex=-1&l=us-en&s=0&ss_mkt=us&q=mbappe&ttc=7274ReleasingTimerHolder for blobURL
: blob:moz-extension://87b7d412-3d15-4a32-8a05-6288bfa3467c/20aed3ca-d3d0-4632-a
143-3836e221a36c
https://duckduckgo.com/t.js?q=mbappe&l=us-en&s=0&dl=en&ct=PL&ss_mkt=us&p_ent=&ex
=-1&dfrsp=1&biaexp=b&infoboxexp=d&mrvrtexp=b
https://duckduckgo.com/?t=ffab&q=mbappe
s://duckduckgo.com/?t=ffab&q=mbappe&ia=webm
```

```
opening ( bg.jpg - Image Viewer [2/7]
pumpkin.jpg - Image Viewer [2/7]
bg.jpg (JPEG Image, 1920
bg.jpg (JPEG Image, 1920
pumpkin.jpg - Image Viewer [2/7]
bg.jpg
pumpkin.jpg
witch.jpg
spooky_house.jpg
scary.jpg
pumpkin(1).jpg
*.jpg
pumpkin.jpg - Image Viewer [2/7]
pumpkin.jpg - Image Viewer [2/7]
/bg.jpg
bg.jpg
```

a tutaj zdjęcie

Za pomocą komendy **strings**
jesteśmy w stanie znaleźć
interesujące nas dane

Zadanie 3 – Analiza pamięci przy wykorzystaniu programu Volatility

5. Odpowiedz na pytania:

```
[arek@fedora volatility_2.6_lin64_standalone] $ ./volatility_2.6_lin64_standalone -f ~/astudia/is/lab6/memory3.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
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/arek/astudia/is/lab6/memory3.vmem)
      PAE type : PAE
      DTB : 0x319000L
      KDBG : 0x80544ce0L
      Number of Processors : 1
      Image Type (Service Pack) : 2
      KPCR for CPU 0 : 0xffdf000L
      KUSER_SHARED_DATA : 0xffdf000L
      Image date and time : 2010-08-15 18:24:00 UTC+0000
      Image local date and time : 2010-08-15 14:24:00 -0400
```

a. Jakie sugerowane profile są aktualnie podpowiadane przez program?

WinXPSP2x86, WinXPSP3x86

```
Volatility debug : Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
```

b. Do czego wykorzystywany jest adres KDBG?

jest to struktura używana przez kernel systemu Windows, w celu debugowania. Jest to lista aktualnie uruchomionych procesów i modułów kernela

c. DTB (Directory Table Base) – jest używany do translacji wirtualnego adresu na jaki adres?

Jest używany do translacji lokalizacji strony pamięci na adres fizyczny

d. O czym świadczą dane zawarte w KPCR (Kernel Processor Control Region) w odniesieniu do badanego obrazu?

o aktualnie używanym wątku

również można wyczytać o ilości procesorów w komputerze

6. Volatility wymaga do prawidłowej analizy wskazania profilu badanego obrazu. Wywołaj funkcje wyświetlenia listy procesów systemu:

```
[root@fedora ~]# volatility_2.6_lin64_standalone $ ./volatility_2.6_lin64_standalone -f ~/astudia/is/lab6/memory3.vmem --profile=WinXPSP2x86 pslist
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x810b1660	System	4	0	58	183	-----	0		
0xffff2ab020	smss.exe	544	4	3	21	-----	0	2010-08-11 06:06:21 UTC+0000	
0xffff1ecda0	csrss.exe	608	544	10	369	0	0	2010-08-11 06:06:23 UTC+0000	
0xffff1ec978	winlogon.exe	632	544	20	518	0	0	2010-08-11 06:06:23 UTC+0000	
0xffff247020	services.exe	676	632	16	269	0	0	2010-08-11 06:06:24 UTC+0000	
0xffff255020	lsass.exe	688	632	19	344	0	0	2010-08-11 06:06:24 UTC+0000	
0xffff218230	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	
0xffff217560	svchost.exe	936	676	10	272	0	0	2010-08-11 06:06:24 UTC+0000	
0x80bf910	svchost.exe	1028	676	71	1341	0	0	2010-08-11 06:06:24 UTC+0000	
0xffff22d558	svchost.exe	1088	676	5	80	0	0	2010-08-11 06:06:25 UTC+0000	
0xffff203b80	svchost.exe	1148	676	14	208	0	0	2010-08-11 06:06:26 UTC+0000	
0xffff1d7da0	spoolsv.exe	1432	676	13	135	0	0	2010-08-11 06:06:26 UTC+0000	
0xffff1b8b28	vmtoolsd.exe	1668	676	5	221	0	0	2010-08-11 06:06:35 UTC+0000	
0xffff1fdc88	VMUpgradeHelper	1788	676	4	100	0	0	2010-08-11 06:06:38 UTC+0000	
0xffff143b28	TPAutoConnSvc.e	1968	676	5	100	0	0	2010-08-11 06:06:39 UTC+0000	
0xffff25a7e0	alg.exe	216	676	6	105	0	0	2010-08-11 06:06:39 UTC+0000	
0xffff364310	wscntfy.exe	888	1028	1	27	0	0	2010-08-11 06:06:49 UTC+0000	
0xffff38b5f8	TPAutoConnect.e	1084	1968	1	61	0	0	2010-08-11 06:06:52 UTC+0000	
0xffff3865d0	explorer.exe	1724	1708	12	341	0	0	2010-08-11 06:09:29 UTC+0000	
0xffff3667e8	VMwareTray.exe	432	1724	1	49	0	0	2010-08-11 06:09:31 UTC+0000	
0xffff374980	VMwareUser.exe	452	1724	6	189	0	0	2010-08-11 06:09:32 UTC+0000	
0x80f94588	wuauc.lt.exe	468	1028	4	134	0	0	2010-08-11 06:09:37 UTC+0000	
0xffff3ad1a8	IEXPLORE.EXE	2044	1724	10	366	0	0	2010-08-15 18:11:17 UTC+0000	
0x80fdc368	logon.scr	124	632	1	15	0	0	2010-08-15 18:21:28 UTC+0000	
0xffff125020	cmd.exe	1136	1668	0	-----	0	0	2010-08-15 18:24:00 UTC+0000	2010-08-15 18:24:00 UTC+0000

a. Jakie informacje zawierają poszczególne kolumny:

- Offset(V) - adres pamięci RAM procesu
- PID - numer id procesu
- PPID - numer id procesu rodzica
- Thds - używana liczba wątków procesu
- Hnds - liczba uchwytów procesu
- Sess - numer id sesji procesu
- Wow64 - czy proces jest 64 bitowy (0 jeśli nie jest)
- Start - czas (data) utworzenia procesu
- Exit - czas (data) zakończenia procesu

b. O czym świadczy znacznik (V) w rubryce Offset?

V - virtual

c. Który z niżej opisanych procesów został zakończony i kiedy?

0xffff125020	cmd.exe	1136	1668	0	-----	0	0	2010-08-15 18:24:00 UTC+0000	2010-08-15 18:24:00 UTC+0000
--------------	---------	------	------	---	-------	---	---	------------------------------	------------------------------

jedynie **cmd.exe 2010-08-15 18:24:00**

d. Dlaczego procesy „System” i „smss.exe” nie posiadają informacji w rubryce Sess?

ponieważ są to procesy systemowe i to one uruchamiają dalsze sesje - tak zwany menedżer sesji

e. Który numer procesu należy do VMwareUser.exe?

```
1 UTC+0000
0xff374980 VMwareUser.exe 452
2 UTC+0000
```

452

7. Wykonaj polecenie:

Jaką zmianę wywołał wskaźnik -P? Porównaj zmianę w procesie VMwareUser.exe.

```
[arek@fedora volatility_2.6_lin64_standalone] $ ./volatility_2.6_lin64_standalone -f ~/astudia/is/lab6/memory3.vmem --profile=WinXPSP2x86 pslist -P
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name      PID  PPID  Thds  Hnds  Sess  Wow64  Start      Exit
-----
0x01214660 System    4     0     58   183   -----  0
0x05471020 smss.exe  544   4     3    21   -----  0 2010-08-11 06:06:21 UTC+0000
0x066f0da0 csrss.exe 608   544   10   369   0        0 2010-08-11 06:06:23 UTC+0000
0x066f0978 winlogon.exe 632   544   20   518   0        0 2010-08-11 06:06:23 UTC+0000
0x06015020 services.exe 676   632   16   269   0        0 2010-08-11 06:06:24 UTC+0000
0x05f47020 lsass.exe 688   632   19   344   0        0 2010-08-11 06:06:24 UTC+0000
0x06384230 vmacthlp.exe 844   676   1    24   0        0 2010-08-11 06:06:24 UTC+0000
0x0115b8d8 svchost.exe 856   676   17   199   0        0 2010-08-11 06:06:24 UTC+0000
0x063c5560 svchost.exe 936   676   10   272   0        0 2010-08-11 06:06:24 UTC+0000
0x01122910 svchost.exe 1028   676   71   1341  0        0 2010-08-11 06:06:24 UTC+0000
0x061ef558 svchost.exe 1088   676   5    80   0        0 2010-08-11 06:06:25 UTC+0000
0x06499b80 svchost.exe 1148   676   14   208   0        0 2010-08-11 06:06:26 UTC+0000
0x06945da0 spoolsv.exe 1432   676   13   135   0        0 2010-08-11 06:06:26 UTC+0000
0x069d5b28 vmtoolsd.exe 1668   676   5   221   0        0 2010-08-11 06:06:35 UTC+0000
0x0655fc88 VMUpgradeHelper 1788   676   4   100   0        0 2010-08-11 06:06:38 UTC+0000
0x0211ab28 TPAutoConnSvc.e 1968   676   5   100   0        0 2010-08-11 06:06:39 UTC+0000
0x05f027e0 alg.exe 216   676   6   105   0        0 2010-08-11 06:06:39 UTC+0000
0x04c2b310 wscntfy.exe 888   1028   1    27   0        0 2010-08-11 06:06:49 UTC+0000
0x049c15f8 TPAutoConnect.e 1084   1968   1    61   0        0 2010-08-11 06:06:52 UTC+0000
0x04a065d0 explorer.exe 1724   1708   12   341   0        0 2010-08-11 06:09:29 UTC+0000
0x04be97e8 VMwareTray.exe 432   1724   1    49   0        0 2010-08-11 06:09:31 UTC+0000
0x04b5a980 VMwareUser.exe 452   1724   6   189   0        0 2010-08-11 06:09:32 UTC+0000
0x010f7588 wuauclt.exe 468   1028   4   134   0        0 2010-08-11 06:09:37 UTC+0000
0x0485d1a8 IEXPLORE.EXE 2044   1724   10   366   0        0 2010-08-15 18:11:17 UTC+0000
0x0113f368 logon.scr 124   632   1    15   0        0 2010-08-15 18:21:28 UTC+0000
0x02e47020 cmd.exe 1136   1668   0   -----  0 2010-08-15 18:24:00 UTC+0000 2010-08-15 18:24:00 UTC+0000
```

Przed

0xff374980	VMwareUser.exe	452	1724	6	189	0	0	2010-08-11 06:09:32 UTC+0000
------------	----------------	-----	------	---	-----	---	---	------------------------------

Po

0x04b5a980	VMwareUser.exe	452	1724	6	189	0	0	2010-08-11 06:09:32 UTC+0000
------------	----------------	-----	------	---	-----	---	---	------------------------------

Zmienił się adres i jego wartość - wcześniej był wirtualny (V) a teraz fizyczny (P)

8. Wyświetlając listę procesów w formie „drzewa”:

```
[arek@fedora volatility_2.6_lin64_standalone] $ ./volatility_2.6_lin64_standalone -f ~/astudia/is/lab6/memory3.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6
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    269 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
                0xff1d7da8: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:wuaucit.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 06:06:30 UTC+0000
                            0xff38b5f0: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
                                          0xff1ecd0: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
```

a. Co oznaczają wyświetlone wcięcia i kropki?

poziom głębi procesu - jeśli ma więcej kropek to znaczy że jest dzieckiem procesu o mniejszej ilości kropek

b. Jakiego identyfikatora nie znajdziemy w prezentowanych tabelach?

Sess

c. Procesem nadrzędnym procesu smss.exe jest...?

```
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
```

Sam system

d. Za co odpowiedzialny jest proces smss.exe?

jest to menadżer sesji systemu Windows

9. Wykorzystując wskaźnik -h odzyskaj i wyświetl załadowane biblioteki dll w badanym obrazie na podstawie procesu wscntfy.exe (Podpowiedź: do wyszukanego wskaźnika dodaj -p i podaj id procesu wscntfy.exe).

```
:wscntfy.exe 888
```

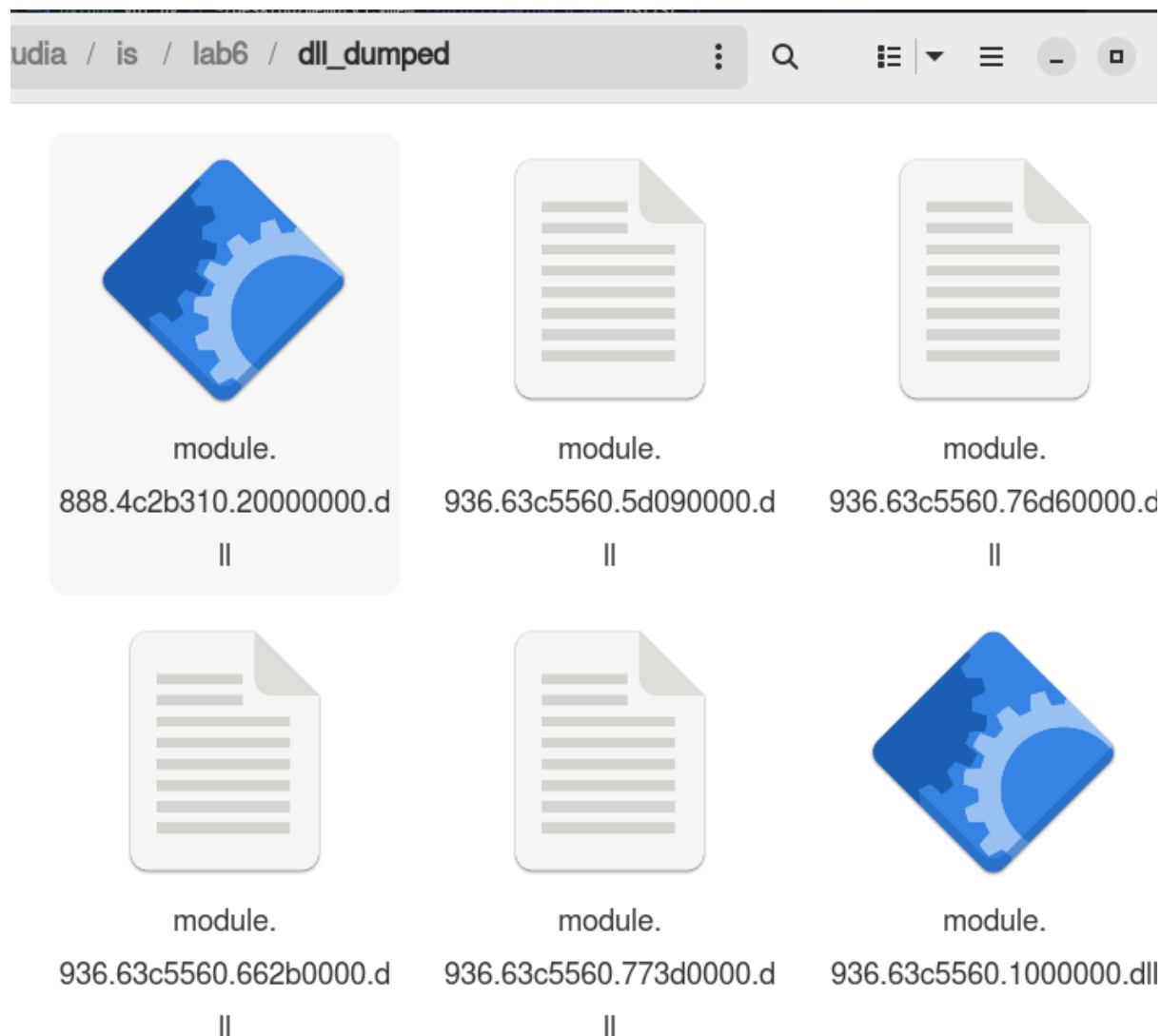
Najpierw trzeba znaleźć numer PID procesu - 888


```
[arek@fedora volatility_2.6_lin64_standalone] $ ./volatility_2.6_lin64_standalone -f ~/astudia/is/lab6/memory3.vmem --profile=WinXPSP2x86 -p 888 dlllist
Volatility Foundation Volatility Framework 2.6
-----
wscntfy.exe pid: 888
Command line : C:\WINDOWS\system32\wscntfy.exe
Service Pack 2

Base      Size  LoadCount Path
-----
0x01000000 0x6000 0xffff C:\WINDOWS\system32\wscntfy.exe
0x7c900000 0xb0000 0xffff C:\WINDOWS\system32\kernel32.dll
0x7c800000 0xf4000 0xffff C:\WINDOWS\system32\user32.dll
0x77c10000 0x50000 0xffff C:\WINDOWS\system32\GDI32.dll
0x77f10000 0x46000 0xffff C:\WINDOWS\system32\USER32.dll
0x77c90000 0x814000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77d00000 0x9b000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77f60000 0x76000 0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x773d0000 0x102000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84ff99comctl32.dll
0x20000000 0x2c5000 0x1 C:\WINDOWS\system32\Xpsp2res.dll
0x5ad70000 0x30000 0x2 C:\WINDOWS\system32\uxtheme.dll
```

10. Przy pomocy polecenia dlldump wypakuj pliki dll w nowo utworzonym folderze:

```
[arek@fedora volatility_2.6_lin64_standalone] $ ./volatility_2.6_lin64_standalone -f ~/astudia/is/lab6/memory3.vmem --profile=WinXPSP2x86 dlldump -D ~/astudia/is/lab6/dll_dumped
Volatility Foundation Volatility Framework 2.6
-----
Process(V) Name Module Base Module Name Result
-----
0xffff2ab020 smss.exe 0x0485b0000 smss.exe Error: DLLBase is paged
0xffff2ab020 smss.exe 0x07c900000 Error: DLLBase is paged
0xffff1ecd0a csrss.exe 0x04a680000 csrss.exe Error: e_magic 6268 is not a valid DOS signature.
0xffff1ecd0a csrss.exe 0x07c900000 Error: DLLBase is paged
0xffff1ecd0a csrss.exe 0x075b40000 CSRSRV.dll Error: DLLBase is paged
0xffff1ecd0a csrss.exe 0x077d40000 USER32.dll OK: module.608.66feda0.77d40000.dll
0xffff1ecd0a csrss.exe 0x077e70000 RPORT4.dll Error: DLLBase is paged
0xffff1ecd0a csrss.exe 0x075e90000 sxs.dll Error: DLLBase is paged
0xffff1ecd0a csrss.exe 0x077dd0000 ADVAPI32.dll Error: DLLBase is paged
0xffff1ecd0a csrss.exe 0x075b50000 basesrv.dll Error: DLLBase is paged
0xffff1ecd0a csrss.exe 0x07c800000 KERNEL32.dll Error: DLLBase is paged
0xffff1ecd0a csrss.exe 0x077f10000 GDI32.dll Error: DLLBase is paged
0xffff1ecd0a csrss.exe 0x075b60000 winsrv.dll OK: module.608.66feda0.75b60000.dll
0xffff1ecd0a csrss.exe 0x075b60000 Error: DLLBase is paged
```



Czy oddało się odzyskać plik: module.124.113f368.77f60000.dll?

```
0x00000000 logon.scr 0x00000000 SHELWAPI.dll OK: module.124.113f368.77f60000.dll
[arek@fedora volatility_2.6_lin64_standalone] $ ll ~/astudia/is/lab6/dll_dumped/ | grep module.124.113f368.77f60000.dll
-rw-r--r--. 1 arek arek 474112 Dec 28 14:18 module.124.113f368.77f60000.dll
```

Tak

11. Wyświetl otwarte powiązania „uchwyty” we wskazanym procesie i odpowiedz na pytania:

- Do jakiego procesu należy wskazany PID (1168)?
- Z jakim procesem wskazany PID (1168) posiada aktywny „uchwyt”?
- Podaj PID odnalezionego aktywnego powiązanego procesu.

```
[arek@fedora volatility_2.6_lin64_standalone] $ ./volatility_2.6_lin64_standalone -f ~/astudia/is/lab6/memory3.vmem --profile=WinXPSP2x86 handles -p 1168 -t Process
Volatility Foundation Volatility Framework 2.6
Offset(V)  Pid  Handle  Access Type  Details
-----
ERROR : volatility.debug : Cannot find PID 1168. If its terminated or unlinked, use psscan and then supply --offset=OFFSET
```

Brak takiego procesu o podanym PID

12. Polecenie Getsids wyświetla identyfikatory SID (Security Identifiers) powiązany z procesem. W ten sposób jesteśmy w stanie uchwycić procesy, które mają złośliwy charakter i mogą eskalować uprawnienia. Do jakich uprawnień należy wskaźnik (S-1-5-32-544)?

```
[arek@fedora volatility_2.6_lin64_standalone] $ ./volatility_2.6_lin64_standalone -f ~/astudia/is/lab6/memory3.vmem --profile=WinXPSP2x86 getsids | grep S-1-5-32-544
Volatility Foundation Volatility Framework 2.6
System (4): S-1-5-32-544 (Administrators)
smss.exe (544): S-1-5-32-544 (Administrators)
csrss.exe (608): S-1-5-32-544 (Administrators)
winlogon.exe (632): S-1-5-32-544 (Administrators)
services.exe (676): S-1-5-32-544 (Administrators)
lsass.exe (688): S-1-5-32-544 (Administrators)
vmacthlp.exe (844): S-1-5-32-544 (Administrators)
svchost.exe (856): S-1-5-32-544 (Administrators)
svchost.exe (1028): S-1-5-32-544 (Administrators)
spoolsv.exe (1432): S-1-5-32-544 (Administrators)
vmtoolsd.exe (1668): S-1-5-32-544 (Administrators)
VMUpgradeHelper (1788): S-1-5-32-544 (Administrators)
TPAutoConnSvc.e (1968): S-1-5-32-544 (Administrators)
wscntfy.exe (888): S-1-5-32-544 (Administrators)
TPAutoConnect.e (1084): S-1-5-32-544 (Administrators)
explorer.exe (1724): S-1-5-32-544 (Administrators)
VMwareTray.exe (432): S-1-5-32-544 (Administrators)
VMwareUser.exe (452): S-1-5-32-544 (Administrators)
wuauclt.exe (468): S-1-5-32-544 (Administrators)
IEXPLORE.EXE (2044): S-1-5-32-544 (Administrators)
logon.scr (124): S-1-5-32-544 (Administrators)
cmd.exe (1136): S-1-5-32-544 (Administrators)
```

administratora

13. Przy wykorzystaniu wtyczki verinfo jesteśmy w stanie wyświetlić informacje o wersjach które zostały osadzone w plikach PE (nie wszystkie pliki posiadają te informacje).

Odpowiedz na pytania:

a. Jaką wersję posiada plik: C:\WINDOWS\system32\SAMLIB.dll?

```
C:\WINDOWS\system32\SAMLIB.dll
File version      : 5.1.2600.2180
Product version   : 5.1.2600.2180
Flags             :
OS                : Windows NT
File Type         : Dynamic Link Library
File Date         :
CompanyName       : Microsoft Corporation
FileDescription   : SAM Library DLL
FileVersion       : 5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
InternalName      : SAMLlib.DLL
LegalCopyright    : \xa9 Microsoft Corporation. All rights reserved.
OriginalFilename  : SAMLlib.DLL
ProductName       : Microsoft\xae Windows\xae Operating System
ProductVersion    : 5.1.2600.2180
```

5.1.2600.2180

b. Podaj jego OS.

Windows NT

c. Podaj wersję pliku:

C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe.

```
C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
File version      : 7.17.512.1
Product version   : 7.17.512.1
Flags             :
OS                : Windows NT
File Type         : Application
File Date         :
CompanyName       : ThinPrint AG
FileDescription   : TPAutoConnect User Agent
FileVersion       : 7,17,512,1
InternalName      : TPAutoConnect
LegalCopyright    : Copyright (c) 1999-2009 ThinPrint AG
OriginalFilename  : TPAutoConnect.exe
ProductName       : TPAutoConnect
ProductVersion    : 7,17,512,1
```

7.17.512.1

d. Podaj LegalCopyright ww. pliku.

Copyright © 1999-2009 ThinPrint AG

14. Wykorzystaj wtyczkę odpowiedzialną za przeglądarkę internetową IE i odpowiedz na pytania:

```
[arek@fedora volatility_2.6_lin64_standalone] $ ./volatility_2.6_lin64_standalone -f ~/astudia/is/lab6/memory3.vmem --profile=WinXPSP2x86 iehistory
Volatility Foundation Volatility Framework 2.6
*****
Process: 1724 explorer.exe
Cache type "DEST" at 0x1387cd
Last modified: 2010-08-15 14:11:24 UTC+0000
Last accessed: 2010-08-15 18:11:26 UTC+0000
URL: Administrator@http://www.msn.com
Title: MSN.com
*****
Process: 2044 IEXPLORE.EXE
Cache type "DEST" at 0x24bdf45
Last modified: 2010-08-15 14:11:24 UTC+0000
Last accessed: 2010-08-15 18:11:26 UTC+0000
URL: Administrator@http://www.msn.com
Title: MSN.com
```

a. Podaj PID procesu IEXPLORE.EXE.

2044

b. O której została uruchomiona przeglądarka?

14:11

c. Czy została wyświetlona strona www.yahoo.com?

nie

d. Czy została wyświetlona strona www.bing.com?

nie

15. Proszę o wyeksportowanie procesu pod nazwą wuauclt.exe: Poprawnie wykonane polecenie zwróci do utworzonego folderu plik (executable.468.exe) z procesu. Wykonaj jego analizę poprzez sprawdzenie sumy kontrolnej (np. md5sum) i poddaj go weryfikacji pod kątem obecności złośliwego oprogramowania (www.virustotal.com). Proszę o załączenie wyników z wykonanego działania.

```
:24 UTC+0000
... 0x80f94588:wuauclt.exe 468 1028
:37 UTC+0000
```

Najpierw sprawdzam jego PID

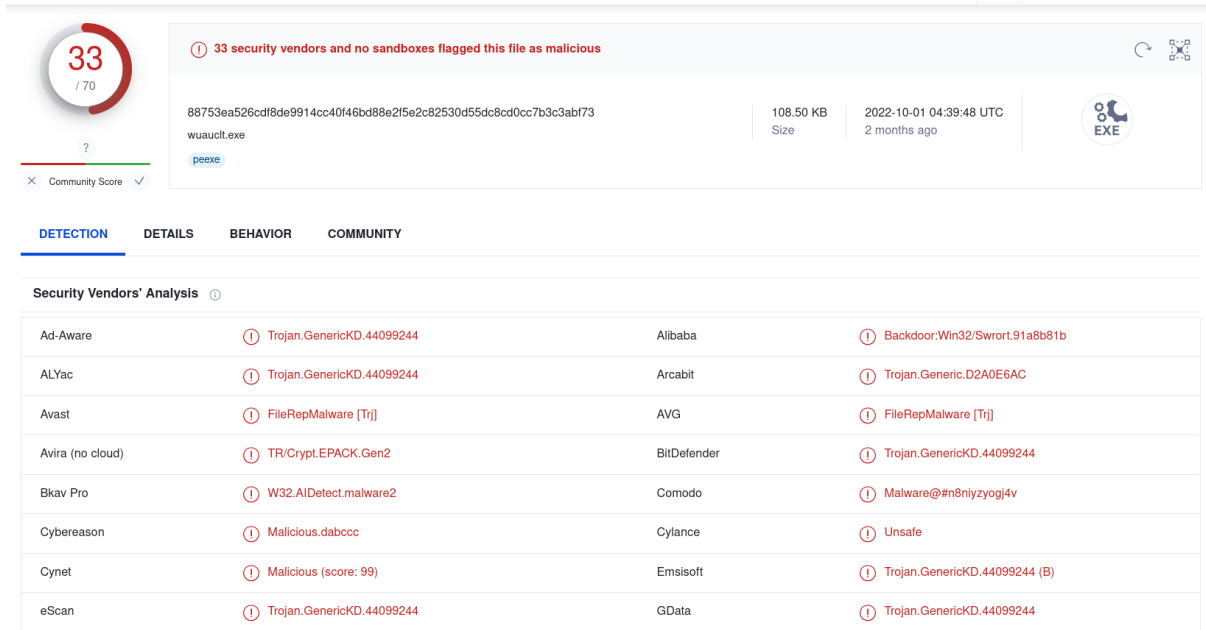
```
[arek@fedora ~]$ ./volatility_2.6_lin64_standalone -f ~/astudia/is/lab6/memory3.vmem --profile=WinXPSP2x86 procdump -p 468 --dump-dir ~/astudia/is/lab6/file
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
-----
0x00f94500 0x00400000 wuauclt.exe OK: executable.468.exe
```

Następnie za pomocą komendy *procdump* eksportuje plik

```
[arek@fedora file] $ md5sum executable.468.exe
21c183cdabccc7675b50258313812bc7 executable.468.exe
```

md5sum: **21c183cdabccc7675b50258313812bc7**

Uzyskany hash wrzucam do strony **virustotal.com**



33 / 70

33 security vendors and no sandboxes flagged this file as malicious

88753ea526cdf8de9914cc40f46bd88e2f5e2c82530d55dc8cd0cc7b3c3abf73

wuauclt.exe

Size 108.50 KB

2022-10-01 04:39:48 UTC

2 months ago

EXE

Community Score

DETECTION DETAILS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Ad-Aware	Trojan.GenericKD.44099244	Alibaba	Backdoor:Win32/Swori.91a8b81b
ALYac	Trojan.GenericKD.44099244	Arcabit	Trojan.Generic.D2A0E6AC
Avast	FileRepMalware [Trj]	AVG	FileRepMalware [Trj]
Avira (no cloud)	TR/Crypt.EPACK.Gen2	BitDefender	Trojan.GenericKD.44099244
Bkav Pro	W32.AIDetect.malware2	Comodo	Malware@#n8niyzyogj4v
Cybereason	Malicious.dabccc	Cylance	Unsafe
Cynet	Malicious (score: 99)	Emsisoft	Trojan.GenericKD.44099244 (B)
eScan	Trojan.GenericKD.44099244	GData	Trojan.GenericKD.44099244

ewidentnie plik jest złośliwy - jest trojanem przeznaczonym na system Windows


History ⓘ

Creation Time	2004-08-04 06:00:27 UTC
First Submission	2014-10-22 07:02:38 UTC
Last Submission	2022-10-01 01:35:15 UTC
Last Analysis	2022-10-01 04:39:48 UTC







Names ⓘ

wuauclt.exe
executable.468.exe
module.468.10f7588.400000.dll
468.wuauclt.exe

Powstał naprawdę dawno temu - w 2004 roku
i figuruje pod wieloma nazwami



88753ea526cdf8de9914cc40f46bd88e2f5e2c82530d55dc8cd0cc7b3c3abf73



Add to Collection





Basic Properties

Type	Win32 EXE
Size	108.50 kB
First Seen	2014-10-22 07:02:38
Last Seen	2022-10-01 01:35:15
Submissions	8
File Name	wuauclt.exe

Relations

It doesn't have relations.

Please, introduce 3 or more characters to perform a search in the graph



Filtered Nodes 0 / 1

Reset all filters


Remove filtered nodes

Remove visible nodes


HELP

Apply to selection

File Type

1 / 1  peexe OR AND NOT RESET

Entity Type



1 / 1  File OR AND NOT RESET

Relationships

RESET

Detections

RESET

From  To  No detections | With detections

1 _

0.8 _

0.6 _

0.4 _

0.2 _

0 _

0 6 12 18 24 30

First Seen RESET

Nie ma powiązań z innymi przedsiębiorstwami/wirusami/oprogramowaniem