**This script was written by Reut Klaider Levy, 7736/12:S11**

#This script will extract data for you with volatility, bulk-extractor, binwalk, foremost & binutils.

#Then it will extract the passwords of the collected data and will make a report of all extracted data.

$ first function - AMIROOT – this script should run on root user, the function checks if user running on root and if not – ask the user to change to root user.

```
[sudo] password for kali:
Your are root, proceeding
/root
```

$ second function – ALLTOOLS – this function will check if you have all needed tools and if not – will install them.

```
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1739 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bulk-extractor is already the newest version (2.0.0-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 1739 not upgraded.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
binwalk is already the newest version (2.3.4+dfsg1-1).
0 upgraded, 0 newly installed, 0 to remove and 1739 not upgraded.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
foremost is already the newest version (1.5.7-11+b2).
0 upgraded, 0 newly installed, 0 to remove and 1739 not upgraded.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
binutils is already the newest version (2.40-2).
0 upgraded, 0 newly installed, 0 to remove and 1739 not upgraded.
find: '/run/user/1000/gvfs': Permission denied
URL transformed to HTTPS due to an HSTS policy
--2023-02-16 14:04:49--  https://downloads.volatilityfoundation.org/releases/2.6/volatility_2.6_lin64_standalone.zip
Resolving downloads.volatilityfoundation.org (downloads.volatilityfoundation.org)... 162.243.24.16
Connecting to downloads.volatilityfoundation.org (downloads.volatilityfoundation.org)|162.243.24.16|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14737820 (14M) [application/zip]
Saving to: 'volatility_2.6_lin64_standalone.zip'

volatility_2.6_lin64_standalone.zip             100%[=========================================================================================================>]  14.05M  6.40MB/s    in 2.2s

2023-02-16 14:04:52 (6.40 MB/s) - 'volatility_2.6_lin64_standalone.zip' saved [14737820/14737820]

Archive:  volatility_2.6_lin64_standalone.zip
   creating: volatility_2.6_lin64_standalone/
  inflating: volatility_2.6_lin64_standalone/AUTHORS.txt
  inflating: volatility_2.6_lin64_standalone/CREDITS.txt
  inflating: volatility_2.6_lin64_standalone/LEGAL.txt
  inflating: volatility_2.6_lin64_standalone/LICENSE.txt
  inflating: volatility_2.6_lin64_standalone/README.txt
  inflating: volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone
Volatility Installed
bulk extractor already installed
binwalk already installed
foremost already installed
binutils already installed
```

$ third function – FILE – for the script to work and extract data – user will need to specify a file in absolute path. The function checks if file exist and apply file as variable.

```
[!] For extracting Data , you will need to Specify File in absolute path:

[+] File exists
```

$ fourth function – EXTERMINATE – this function will use all tools installed before and will extract all data from given file. This function will save all data based on tool at different location on "ExtractedData" file.

```
[+] Extracting info from given file into ~/Desktop/ExtractedData
mkdir "/root/ExtractedData/bulk_extractor"
bulk_extractor version: 2.0.0
Input file: "/home/kali/Desktop/mem.mem"
Output directory: "/root/ExtractedData/bulk_extractor"
```

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
150720        0x24CC0         Microsoft executable, portable (PE)
353872        0x56650         CRC32 polynomial table, little endian
656418        0xA0422         Copyright string: "Copyright 1985-1998,Phoenix Technologies Ltd.All rights reserved."
819330        0xC8082         Copyright string: "Copyright (C) 2003-2008  VMware, Inc."
819369        0xC80A9         Copyright string: "Copyright (C) 1997-2000  Intel Corporation"
941804        0xE5EEC         ISO 9660 Boot Record,
```

```
Processing: /home/kali/Desktop/mem.mem
|******|
binwalk  bulk_extractor  foremost
[+] Now you have all data carved from /home/kali/Desktop/mem.mem
```

```
[+] The network file is located at /home/kali/Desktop/ExtractedData/bulk_extractor and it's size is 104K
```

```
[+] Here are the exe files carved:
00000294.exe  00084088.exe  00185592.exe  00186824.exe  00188816.exe  00237840.exe  00239008.exe  00239944.exe  00243616.exe  00265896.exe  00402416.exe  01046936.exe  01047296.exe  01048288.exe
00002360.exe  00152808.exe  00186024.exe  00186848.exe  00189392.exe  00238248.exe  00239216.exe  00240560.exe  00244920.exe  00265920.exe  00403912.exe  01046952.exe  01047384.exe  01048360.exe
00002544.exe  00152944.exe  00186520.exe  00187120.exe  00235160.exe  00238584.exe  00239360.exe  00240632.exe  00245000.exe  00266184.exe  00414112.exe  01047088.exe  01047632.exe
00008912.exe  00165136.exe  00186592.exe  00187216.exe  00235776.exe  00238864.exe  00239624.exe  00241072.exe  00245184.exe  00267048.exe  00442184.exe  01047168.exe  01047648.exe
00081552.exe  00176864.exe  00186624.exe  00187264.exe  00236024.exe  00238880.exe  00239632.exe  00242136.exe  00245464.exe  00298704.exe  00442480.exe  01047192.exe  01047952.exe
00081880.exe  00176928.exe  00186712.exe  00187544.exe  00236776.exe  00238920.exe  00239648.exe  00242952.exe  00246288.exe  00391744.exe  00445104.exe  01047224.exe  01047992.exe
00083368.exe  00185168.exe  00186720.exe  00188760.exe  00237016.exe  00239084.exe  00239696.exe  00243264.exe  00250368.exe  00396352.exe  01046568.exe  01047240.exe  01048096.exe
The Passwords found on /home/kali/Desktop/mem.mem are saved at strings_pass.txt
```

$ fifth function- Volatility- this function will check the system info, then using volatility tool it will check given file processes, connections and registry. This function will only work if next function will apply it.

```
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/kali/Desktop/mem.mem)
                      PAE type : PAE
                           DTB : 0x2fe000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2012-07-22 02:45:08 UTC+0000
     Image local date and time : 2012-07-21 22:45:08 -0400
running processes list:
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------
0x823c89c8 System                    4      0     53      240 ------      0
0x822f1020 smss.exe                368      4      3       19 ------      0 2012-07-22 02:42:31 UTC+0000
0x822a0598 csrss.exe               584    368      9      326      0      0 2012-07-22 02:42:32 UTC+0000
0x82298700 winlogon.exe            608    368     23      519      0      0 2012-07-22 02:42:32 UTC+0000
0x81e2ab28 services.exe            652    608     16      243      0      0 2012-07-22 02:42:32 UTC+0000
0x81e2a3b8 lsass.exe               664    608     24      330      0      0 2012-07-22 02:42:32 UTC+0000
```

```
running connection list:
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address           Pid
---------- ------------------------ ------------------------ ---
0x81e87620 172.16.112.128:1038      41.168.5.140:8080        1484
running registry list:
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe18e5b60 0x093f8b60 \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1a19b60 0x0a5a9b60 \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
0xe18398d0 0x08a838d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe18614d0 0x08e624d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe183bb60 0x08e2db60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe17f2b60 0x08519b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
```

$ sixth function- CheckVolatility – this function will check profile using volatility and if able will apply volatility function.

```
WinXPSP2x86
[+] Running Volatility
```

$seventh function – Report – this function will make a report of all data extracted, and will let you know how many files were extracted with each tool.

```
The number of files extracted using bulk-extractor is:
64
The number of files extracted using binwalk is:
1
The number of files extracted using foremost is:
8
A List of all extracted files was saved in - Report.txt
script execution was 1127 seconds
  adding: ExtractedData/ (stored 0%)
  adding: Report.txt (deflated 65%)
```

$ eight function –ZipData - this function will zip all data extracted with the report on a file named EveryThing.zip on your Desktop.

```
The files have been zipped into EveryThing.zip on ~/Desktop
```

```
Thank you for using my script
```