

# MEMORY ENCRYPT

We open a terminal, create a Python cod using nano, this code Will requests a password and retains it in memory until the second enter.

```
(kali@kali)-[~]
$ nano cod_no_seguro.py

(kali@kali)-[~]
$ python cod_no_seguro.py
Introduce la contraseña: kali
Contraseña almacenada. Presiona Enter para salir...
█
```

In a second window, we install requirements in order to do the next step:

```
(kali@kali)-[~]
$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.0 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [121 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [204 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [915 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]
Fetched 74.6 MB in 8s (9,626 kB/s)
470 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali@kali)-[~]
$ sudo apt install gdb

The following packages were automatically installed and are no longer required:
  icu-devtools libfuse3-3 libglapi-mesa liblbfgsb0 libpython3.12-minimal libpython3.12t64 python3.12-tk strongswan
  libflac12t64 libgeos3.13.0 libcicu-dev libpoppler145 libpython3.12-stdlib python3-setproctitle ruby-zeitwerk
Use 'sudo apt autoremove' to remove them.

Installing:
  gdb

Installing dependencies:
  libbabeltrace1 libdebuginfod-common libdebuginfodt64 libipt2 libsource-highlight-common libsource-highlight4t64

Suggested packages:
  gdb-doc gdbserver libc-dbg

Summary:
  Upgrading: 0, Installing: 7, Removing: 0, Not Upgrading: 470
```

```
(kali@kali)-[~]
$ sudo apt install dump

The following packages were automatically installed and are no longer required:
icu-devtools libfuse3-3 libglapi-mesa liblbfgsb0 libpython3.12-minimal libpython3.12t64 python3.12-tk strongswan
libflac12t64 libgeos3.13.0 libicu-dev libpoppler145 libpython3.12-stdlib python3-setproctitle ruby-zeitwerk
Use 'sudo apt autoremove' to remove them.

Installing:
  dump

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 470
  Download size: 158 kB
  Space needed: 384 kB / 62.4 GB available

Get:1 http://mirror.es.cdn-perfprod.com/kali kali-rolling/main amd64 dump amd64 0.4b49-2 [158 kB]
Fetched 158 kB in 1s (240 kB/s)
Selecting previously unselected package dump.
(Reading database ... 417928 files and directories currently installed.)
Preparing to unpack .../dump_0.4b49-2_amd64.deb ...
Unpacking dump (0.4b49-2) ...
Setting up dump (0.4b49-2) ...
update-alternatives: using /usr/sbin/rmt-dump to provide /usr/sbin/rmt (rmt) in auto mode
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.2.0) ...
Scanning processes ...
Scanning linux images ...
```

Verify if the Python is running:

```
(kali@kali)-[~]
$ ps -ef|grep cod_no

kali      166598  164170  0 10:41 pts/3    00:00:00 python cod_no_seguro.py
kali      171719  167427  0 10:51 pts/5    00:00:00 grep --color=auto cod_no
```

We take the proces ID and run the following commands to find the range of directions of the heap zone:

```
(kali@kali)-[~]
$ sudo cat /proc/164170/maps|grep heap

[python] password for kali:
5590d63af000-5590d656e000 rw-p 00000000 00:00 0 [heap]

(kali@kali)-[~]
$ sudo gdb -p 164170
```

Start Addr	End Addr	Size	Offset	Perms	File
0x00005590dd37000	0x00005590dd4e000	0x17000	0x0	r--p	/usr/bin/zsh
0x00005590dd4e000	0x00005590dddec000	0x9e000	0x17000	r-xp	/usr/bin/zsh
0x00005590dddec000	0x00005590de07000	0x1b000	0xb5000	r--p	/usr/bin/zsh
0x00005590de07000	0x00005590de09000	0x2000	0xcf000	r--p	/usr/bin/zsh
0x00005590de09000	0x00005590de0f000	0x6000	0xd1000	rw-p	/usr/bin/zsh
0x00005590de0f000	0x00005590de23000	0x14000	0x0	rw-p	
0x00005590d63af000	0x00005590d656e000	0x1bf000	0x0	rw-p	[heap]
0x00007f0fb9600000	0x00007f0fb98ad000	0x2ad000	0x0	r--s	/usr/share/zsh/functions/Completion/Unix.zwc
0x00007f0fb98d0000	0x00007f0fb98d3000	0x3000	0x0	r--p	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/computil.so
0x00007f0fb98d3000	0x00007f0fb98e1000	0xe000	0x3000	r-xp	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/computil.so
0x00007f0fb98e1000	0x00007f0fb98e3000	0x2000	0x11000	r--p	/usr/lib/x86_64-linux-gnu/zsh/5.9/zsh/computil.so

We run this comando to create an exacto copy of a memory spcae:

```
(gdb) dump memory /tmp/output.bin 0x00005590d63af000 0x00005590d656e000
(gdb) quit
A debugging session is active.

    Inferior 1 [process 164170] will be detached.

Quit anyway? (y or n) y
Detaching from program: /usr/bin/zsh, process 164170
[Inferior 1 (process 164170) detached]
```

With the bin as output file, we use the strings method to convert it to .txt

```
(kali@kali)-[~]
$ strings /tmp/output.bin > /tmp/output.txt
```

To increase security, we install cryptography:

```
(kali@kali)-[~]
$ sudo apt install python3-venv # Instala venv si no lo tienes
python3 -m venv ~/venv-crypto
source ~/venv-crypto/bin/activate
pip install cryptography

python3-venv is already the newest version (3.13.2-2).
python3-venv set to manually installed.
The following packages were automatically installed and are no longer required:
  icu-devtools libfuse3-3 libglapi-mesa liblbfgsb0 libpython3.12-minimal libpython3.12t64 python3.12-tk strongswan
  libflac12t64 libgeos3.13.0 libicu-dev libpoppler145 libpython3.12-stdlib python3-setproctitle ruby-zeitwerk
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 470
Collecting cryptography
  Downloading cryptography-45.0.2-cp311-abi3-manylinux_2_34_x86_64.whl.metadata (5.7 kB)
Collecting cffi>=1.14 (from cryptography)
  Downloading cffi-1.17.1-cp313-cp313-manylinux_2_17_x86_64_manylinux2014_x86_64.whl.metadata (1.5 kB)
Collecting pycparser (from cffi>=1.14->cryptography)
  Downloading pycparser-2.22-py3-none-any.whl.metadata (943 bytes)
Download cryptography-45.0.2-cp311-abi3-manylinux_2_34_x86_64.whl (4.5 MB)
----- 4.5/4.5 MB 45.6 MB/s eta 0:00:00
Download cffi-1.17.1-cp313-cp313-manylinux_2_17_x86_64_manylinux2014_x86_64.whl (479 kB)
Download pycparser-2.22-py3-none-any.whl (117 kB)
Installing collected packages: pycparser, cffi, cryptography
Successfully installed cffi-1.17.1 cryptography-45.0.2 pycparser-2.22
```

Then, I create another Python file, called `archivo_seguro` where I put this code :

```
from cryptography.fernet import Fernet

import getpass

# Esto generará una clave segura para cifrar/descifrar la contraseña

key = Fernet.generate_key()

cipher_suite = Fernet(key)

def main():

    # Usamos getpass para que la contraseña no se muestre al escribirla

    password = getpass.getpass("Introduce la contraseña: ")

    # Ciframos la contraseña
```

```

encrypted_password = cipher_suite.encrypt(password.encode('utf-8'))

# Limpiamos la memoria del texto claro
password = None

# Para fines de demostración, mostramos la contraseña cifrada
print(f"Contraseña cifrada: {encrypted_password}")

# Deciframos la contraseña (por ejemplo, si necesitas usarla más tarde)
decrypted_password = cipher_suite.decrypt(encrypted_password).decode('utf-8')

# Muestra la contraseña descifrada (por motivos de demostración, no hacer esto
en aplicaciones reales)

#print(f"Contraseña descifrada: {decrypted_password}")

# Limpia la memoria
decrypted_password = None
encrypted_password = None

input("Presiona Enter para salir...")

if __name__ == "__main__":
    main()

```

And when I run it the password isn't visible and it appears hashed

```

(venv-crypto)-(kali@kali)-[~]
└─$ python3 codigo_seguro.py
Introduce la contraseña:
Contraseña cifrada: b'gAAAAABoK1MY3Yt7C2G5kVfo2FPvu0ltC198x95g4wnqww28ZDyv0eso0hHPW7LVssCiuv-ii2vtdfd2ovu0eocYBf6ApSzRcw=='
Presiona Enter para salir...^X@sS^Z
zsh: suspended  python3 codigo_seguro.py

```

Now I try the previous steps with the secure code running:

```

(kali@kali)-[~]
└─$ ps -ef|grep cod
kali   166598  164170  0 11:03 pts/3    00:00:00 python cod_no_seguro.py
kali   189902  172961  0 11:49 pts/7    00:00:00 python3 codigo_seguro.py
kali   191105  172961  0 11:52 pts/7    00:00:00 python3 codigo_seguro.py
kali   191632  189004  0 11:53 pts/8    00:00:00 python3 codigo_seguro.py
kali   191742  191170  0 11:53 pts/9    00:00:00 grep --color=auto cod

```

```
(kali@kali)-[~]
$ sudo cat /proc/191632/maps |grep heap
[sudo] password for kali:
2b002000-2b211000 rw-p 00000000 00:00 0 [heap]

(kali@kali)-[~]
$ sudo gdb -p 191632
GNU gdb (Debian 16.3-1) 16.3
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
```

```
(gdb) info proc mappings
process 191632
Mapped address spaces:

Start Addr      End Addr      Size          Offset         Perms  File
0x000000000400000 0x000000000420000 0x20000      0x0            r--p  /usr/bin/python3.13
0x000000000420000 0x00000000073a000 0x31a000     0x20000        r-xp  /usr/bin/python3.13
0x00000000073a000 0x0000000009ed000 0x2b3000     0x33a000        r--p  /usr/bin/python3.13
0x0000000009ed000 0x0000000009ee000 0x1000       0x5ec000        r--p  /usr/bin/python3.13
0x0000000009ee000 0x000000000af3000 0x91000      0x5ed000        rw-p  /usr/bin/python3.13
0x000000000af3000 0x000000000af3000 0x74000      0x0            rw-p
0x000000002b002000 0x000000002b211000 0x20f000     0x0            rw-p  [heap]
```

Now the password appears hashed:

```
Contraseña [ifrada: b'gAAAAABoK1Pw6WoWwWc_-TFHwrKsPqjdqINF32zZzeHN-le22818vHYNERvV9EsyTRjZ0eC65bZ4jWo9iGcDymEUZLLISbP2qA=='
I/O hierarchy is the abstract base class IOBase. It
interface to a stream. Note, however, that there is no
```

