Text

Description automatically generated

**Activity based:**

**C2P2 Project Report 1**

**ITNS**

**Project Module - I**

**Submitted to Vishwakarma University, Pune**

**Under the Initiative of**

**Contemporary Curriculum, Pedagogy, and Practice (C2P2)**

**By**

**Name : Armaan Sameer Naik**

**SRN No. : 202101635**

**Roll No. : 36**

**Div : D**

**Batch : D-2**

**Third Year Engineering**

**Faculty Incharge: - Prof. Vivek Thorat**

**Date Of Project 1: - 8/2/23**

**Department of Computer Engineering**

**Faculty of Science and Technology**

**Academic Year**

**2023-2024 Term-II**

**Report 1**

***Project Topic*: Keylogger & URL-Obfuscator**

**A] Introduction:**   
In an era dominated by digital advancements, the security of information and communication systems is of paramount importance. As technology continues to evolve, so do the challenges associated with safeguarding sensitive data and ensuring the integrity of communication channels. The field of Information Technology (IT) Network Security plays a crucial role in addressing these challenges, focusing on protecting computer systems, networks, and the data they handle from unauthorized access, attacks, and data breaches.

This project delves into the realm of IT Network Security, exploring two Python-based tools: a keylogger and a URL obfuscator. However, it is imperative to note that the creation and deployment of tools like keyloggers and URL obfuscators can have severe ethical and legal implications. This introduction will provide an overview of the project's objectives, components, ethical considerations, and recommendations.

**B] Objective:**  
The objective of this project is to implement a keylogger and URL obfuscator using Python. However, it is important to note that the implementation of such tools raises ethical concerns and may be illegal. It is strongly advised not to engage in activities that compromise the privacy and security of individuals.

**C] Project Components:  
  
1. Keylogger:**

The keylogger is designed to record keystrokes by utilizing the keyboard library in Python.

The log\_key function captures key events and logs them to a file named keylog.txt.

The keylogger function starts the keylogger and waits for keyboard events.

**2. URL Obfuscator:**

The URL obfuscator aims to generate obfuscated URLs using a combination of random characters and common domain names.

The obfuscate\_url function takes a URL as input and performs various manipulations, such as adding random characters, replacing certain parts, and appending special characters.

The url\_obfuscator function interacts with the user to input a URL, attempts to reach the URL using the requests library, and then generates an obfuscated version of the URL. The obfuscated URL is saved to a file named Obfuscated URL.txt.

**D] Tools Required:**

**1. Python:**

Ensure that Python is installed on your system. You can download and install Python from the official Python website.

**2. Keyboard Module:**

The keylogger utilizes the keyboard module for capturing keyboard events. Install it using the following command:

pip install keyboard

**2.** **Requests Module:**

The URL obfuscator uses the requests module to make HTTP requests. Install it with:

pip install requests

**3. Operating System Compatibility:**

The code includes platform-dependent commands for clearing the screen (os.system('clear' if os.name != 'nt' else 'cls')). Ensure compatibility with your operating system.

**4. Notepad (for Windows):**

The code includes a command to open Notepad on Windows (os.system(f'notepad.exe {os.path.dirname(\_\_file\_\_)}' + "/Obfuscated URL.txt")). Make sure Notepad is available on your system.

**E]** **Ethical Considerations:**

The implementation of a keylogger and URL obfuscator raises significant ethical concerns. Keyloggers are often associated with malicious intent, as they can be used to capture sensitive information without the user's consent. URL obfuscation can also be misused for phishing attacks or other malicious activities.

**F]** **Recommendations:**

1. **Ethical Programming Practices:**

Focus on programming projects that adhere to ethical guidelines and legal standards.

Engage in activities that contribute positively to the field of IT, such as ethical hacking or cybersecurity.

1. **Legal Compliance:**

Be aware of and comply with legal regulations regarding the development and use of software tools.

Avoid creating or distributing tools that can be used for unauthorized access or compromise the security of systems.

1. **Educational Opportunities:**

Consider pursuing educational opportunities in ethical hacking, network security, or related fields.

Obtain certifications that demonstrate ethical hacking skills, such as Certified Ethical Hacker (CEH) or Offensive Security Certified Professional (OSCP).

**G]** **Outcome:**

The outcome of the provided Python code results in the implementation of a keylogger and a URL obfuscator, each serving distinct purposes. However, it is important to emphasize the ethical considerations associated with the usage of such tools.

1. **Keylogger:**

* **Functionality:**

The keylogger is designed to capture keyboard events and log them to a file named keylog.txt.

It utilizes the keyboard module to monitor key presses.

* **Execution:**

The keylogger is activated by calling the keylogger() function, which starts capturing key events.

The logging is persistent until the program is manually terminated.

* **Outcome:**

The recorded keystrokes are stored in the keylog.txt file, providing a record of user input.

1. **URL Obfuscator:**

* **Functionality:**

The URL obfuscator takes a user-input URL and attempts to reach it using the requests module.

If successful, it generates an obfuscated version of the URL and saves it to a file named Obfuscated URL.txt.

* **Execution:**

The user interacts with the program by entering a URL when prompted.

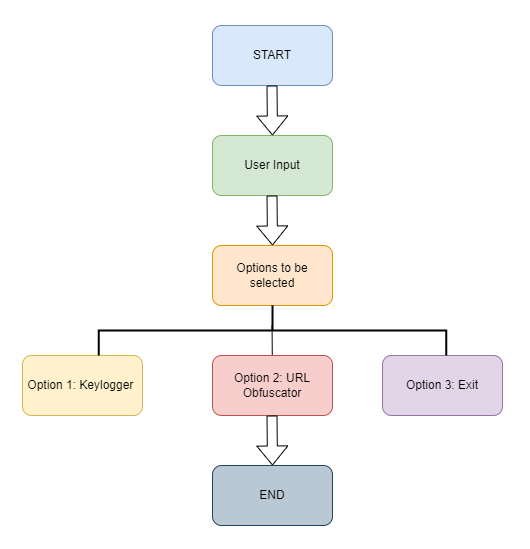
The program attempts to reach the URL, and upon success, generates an obfuscated version.

* **Outcome:**

The obfuscated URL is saved to the Obfuscated URL.txt file.

The file is then opened using Notepad on Windows, providing the user with the obfuscated URL.

**H]** **Flowchart:**



Reference Link: <https://app.diagrams.net/>

**Explanation:**

1. **Start:**

The program begins its execution.

1. **User Input:**

The user is presented with a menu to choose an option (Keylogger, URL Obfuscator, or Exit).

1. **Keylogger Option (1):**

If the user chooses the Keylogger option:

The keylogger() function is called.

The keylogger starts capturing keyboard events using the keyboard module.

The program waits until the user decides to exit manually.

1. **URL Obfuscator Option (2):**

If the user chooses the URL Obfuscator option:

The url\_obfuscator() function is called.

The user is prompted to input a URL.

The program attempts to reach the URL using the requests module.

If successful, an obfuscated version is generated and saved to a file (Obfuscated URL.txt).

The file is opened using Notepad on Windows.

The user is prompted to press Enter to exit.

1. **Exit Option (3):**

If the user chooses the Exit option:

The program breaks out of the loop and ends.

End:

1. **End:**

The program concludes its execution.

**I]** **Case Studies:**

**Misuse of Keyloggers:**

A company's internal network security was compromised when an employee unknowingly downloaded and executed a file containing a keylogger. The attacker gained unauthorized access to sensitive information, leading to data breaches and financial losses. This highlights the real-world consequences of keylogger misuse.

**Phishing with URL Obfuscation:**

A phishing campaign targeted users by using obfuscated URLs in fake emails. The URLs, when clicked, redirected users to fraudulent websites mimicking legitimate platforms. Many users fell victim to the scam, resulting in compromised login credentials and financial losses. This case underscores the risks associated with URL obfuscation used in malicious activities.

**J]** **Conclusion:**

The provided Python code demonstrates technical proficiency in implementing a keylogger and URL obfuscator. However, the ethical implications and security risks associated with such tools cannot be overlooked. In the rapidly evolving landscape of cybersecurity, responsible coding practices are paramount.

While the code showcases technical skills, responsible coding practices and ethical considerations are fundamental. Continuous education, awareness, and adherence to legal standards are essential for developers to contribute positively to the field of IT network security.