**Lab 2: Keylogger**

**Objectives:**

* Understand the concept of keyloggers, their code and functionality, and ethical considerations in using them
* Learn how to deploy and use keyloggers to capture user information on a target machine
* Develop skills in analyzing keylogger data and identifying ways to prevent keylogger malware infections

**Equipment:**

* Two virtual machines running on a host computer, such as VirtualBox or VMware
* A keylogger program from Moriarty Matrix
* Basic knowledge of networking and Linux command line

**Part 1: Deploying Keylogger on the Victim Machine**

1. Download and install the keylogger program on the attacker machine.
2. Deploy the keylogger program on the victim machine using one of the following methods: phishing link, phishing email, direct installation, Bluetooth, USB, FTP, shared folder, etc.
3. Create a fake account on a popular website such as ProtonMail, Instagram, Facebook, and YouTube.

**Part 2: Capturing User Information**

1. Use the keylogger program to capture keystrokes on the victim machine and retrieve the keylogger data on the attacker machine.
2. Analyze the keylogger data to obtain login credentials and other personal information of the victim.
3. Use the obtained information to change the victim's account information and password.

**Part 3: Preventing Keylogger Malware Infections**

1. Analyze the keylogger program and identify its functionality and code.
2. Identify ways to prevent keylogger malware infections, such as avoiding suspicious email links and attachments, using antivirus software, and keeping software up-to-date.
3. Describe the preventive measures in detail.

**Rubric:**

* Successful completion of Part 1: Deploying Keylogger on the Victim Machine: 20 points
* Successful completion of Part 2: Capturing User Information: 50 points
* Successful completion of Part 3: Preventing Keylogger Malware Infections: 20 points
* Quality of documentation and explanation of steps taken: 10 points

**In-depth Rubric:**

**Part 1: Deploying Keylogger on the Victim Machine**

* 5 points: Keylogger program is successfully downloaded and installed on the attacker machine.
* 5 points: Keylogger program is successfully deployed on the victim machine using a chosen method.
* 5 points: An account (recommend a fake one) is created on a website such as ProtonMail, Instagram, Facebook, and YouTube.
* 5 points: Proper documentation is provided explaining the steps taken to deploy the keylogger program on the victim machine.

**Part 2: Capturing User Information**

* 10 points: Keystrokes are successfully captured on the victim machine using the keylogger program.
* 20 points: Keylogger data is successfully retrieved on the attacker machine and analyzed to obtain login credentials and other personal information of the victim.
* 10 points: The obtained information is successfully used to change the victim's account information and password.
* 10 points: Proper documentation is provided explaining the steps taken to capture user information using the keylogger program.

**Part 3: Preventing Keylogger Malware Infections**

* 5 points: The keylogger program's functionality and code are successfully analyzed.
* 10 points: Effective ways to prevent keylogger malware infections are identified and explained, including avoiding suspicious email links and attachments, using antivirus software, and keeping software up-to-date.
* 5 points: Suggestions for preventing keylogger malware infections are tailored to the specific context of the lab.
* **Quality of documentation and explanation of steps taken:**

Other: Points: The lab report is presented in a clear and organized manner, with all necessary information included. Clear and detailed documentation is provided for all parts of the lab, including deployment of the keylogger program, capturing user information, and preventing keylogger malware infections.