

Threat Intelligence Feed Processor

Student Name:Karthik morapally

Objective: To create a simple cybersecurity tool that checks IP addresses in system logs and detects malicious ones using a local threat database.

Tools used:

Python

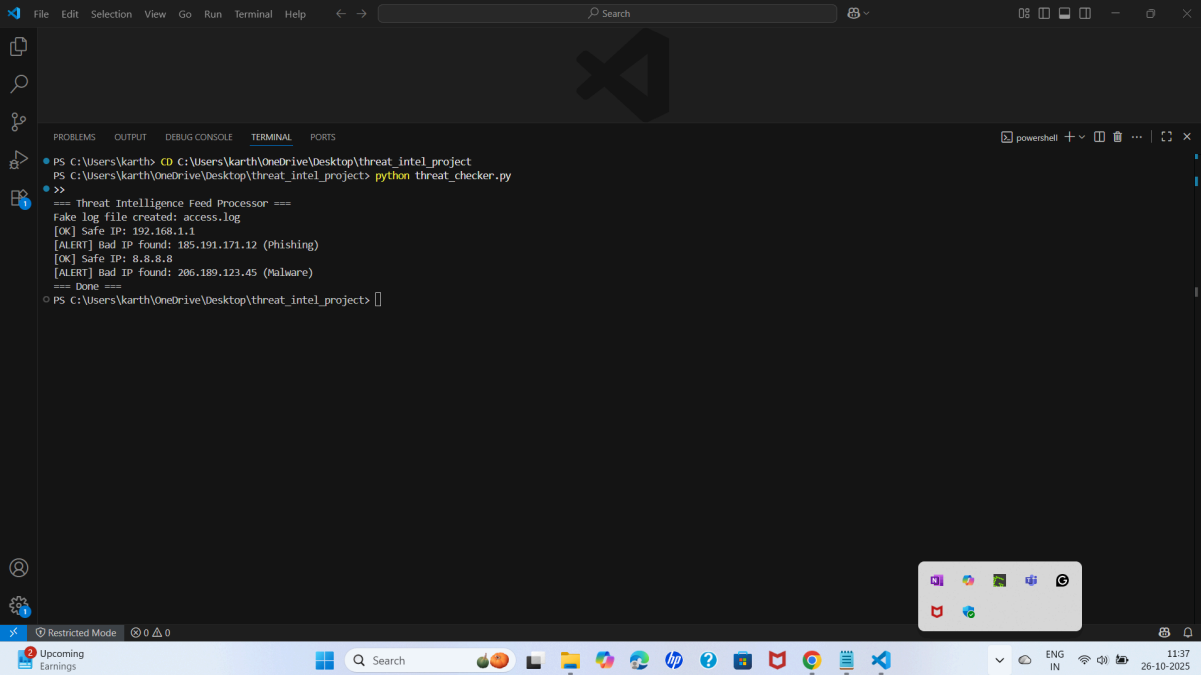
SQLite (for database)

Text files (for logs)

Steps Performed:

1. Created a Python script (`threat_checker.py`)
2. Added a small database of malicious IPs
3. Created a fake log file (`access.log`)
4. Scanned the log file to detect malicious IPs
5. Displayed alerts for suspicious ones

Output:



```
PS C:\Users\karth> cd C:\Users\karth\OneDrive\Desktop\threat_intel_project
PS C:\Users\karth\OneDrive\Desktop\threat_intel_project> python threat_checker.py
>>
=== Threat Intelligence Feed Processor ===
Fake log file created: access.log
[OK] Safe IP: 192.168.1.1
[ALERT] Bad IP found: 185.191.171.12 (Phishing)
[OK] Safe IP: 8.8.8.8
[ALERT] Bad IP found: 206.189.123.45 (Malware)
=== Done ===
PS C:\Users\karth\OneDrive\Desktop\threat_intel_project>
```

Conclusion:

This project demonstrates how cybersecurity analysts can use threat intelligence to detect malicious IPs in log files.