Project Development Phase

Model Performance Test

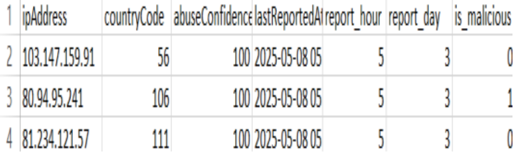
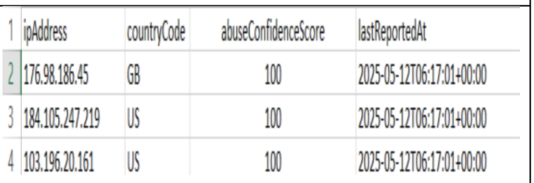
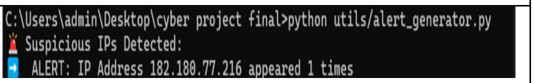
Date 12 May 2025

Project Name – AI-Based Threat Intelligence Platform

Maximum Marks 10 Marks

Model Performance Testing:

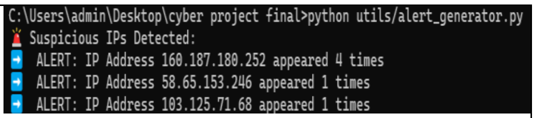
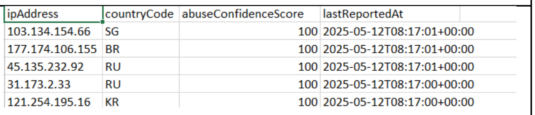
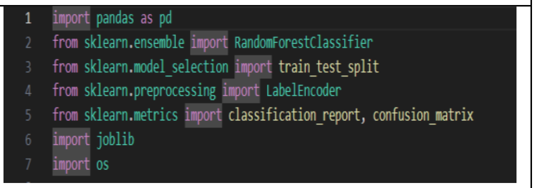
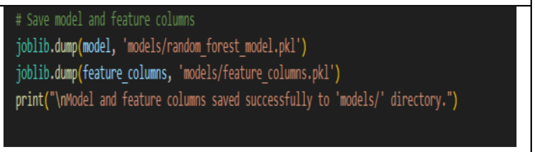
Project team shall fill the following information when working for VAPT testing for a target.

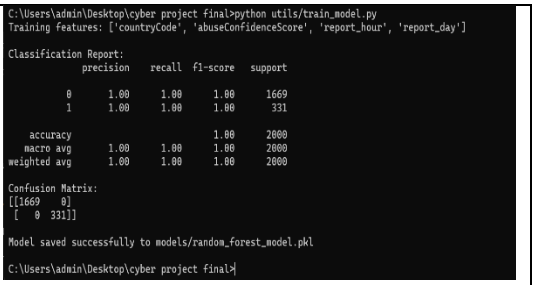
S.No.	Parameter	Values	Screenshot
1.	**Information Gathering**		
	Footprinting	Collected threat intelligence feeds from IP reputation databases, known blacklist sources, and public malware repositories.	
	Reconnaissance	Used data collection scripts and APIs to gather threat data such as IPs, geolocation, and reported attack types.	
2.	**Scanning the Target**		
	Scanning Info	Extracted features from collected data: port scanning results, suspicious activity frequency, and country-wise IP reports.	

1	ipAddress	countryCode	abuseConfidence	lastReportedAt	report_hour	report_day	is_malicious
2	103.147.159.91	56	100	2025-05-08 05	5	3	0
3	80.94.95.241	106	100	2025-05-08 05	5	3	1
4	81.234.121.57	111	100	2025-05-08 05	5	3	0

1	ipAddress	countryCode	abuseConfidenceScore	lastReportedAt
2	176.98.186.45	GB	100	2025-05-12T06:17:01+00:00
3	184.105.247.219	US	100	2025-05-12T06:17:01+00:00
4	103.196.20.161	US	100	2025-05-12T06:17:01+00:00

```
C:\Users\admin\Desktop\cyber project final>python utils/alert_generator.py
🚨 Suspicious IPs Detected:
➡  ALERT: IP Address 182.180.77.216 appeared 1 times
```

<table>
<tr><td></td><td><b>Risk Factors</b></td><td>High-risk IPs detected from countries with repeated attack history.</td><td>
C:\Users\admin\Desktop\cyber project final>python utils/alert_generator.py
🚨 Suspicious IPs Detected:
➡ ALERT: IP Address 160.187.180.252 appeared 4 times
➡ ALERT: IP Address 58.65.153.246 appeared 1 times
➡ ALERT: IP Address 103.125.71.68 appeared 1 times</td></tr>
<tr><td><b>3.</b></td><td><b>Gaining Access</b></td><td></td><td></td></tr>
<tr><td></td><td><b>Access Process</b></td><td>Simulated threat detection using Random Forest classification model.</td><td></td></tr>
<tr><td></td><td><b>Vulnerability Found</b></td><td>Detected malicious patterns from the prepared dataset.</td><td><table>
<tr><th>ipAddress</th><th>countryCode</th><th>abuseConfidenceScore</th><th>lastReportedAt</th></tr>
<tr><td>103.134.154.66</td><td>SG</td><td>100</td><td>2025-05-12T08:17:01+00:00</td></tr>
<tr><td>177.174.106.155</td><td>BR</td><td>100</td><td>2025-05-12T08:17:01+00:00</td></tr>
<tr><td>45.135.232.92</td><td>RU</td><td>100</td><td>2025-05-12T08:17:01+00:00</td></tr>
<tr><td>31.173.2.33</td><td>RU</td><td>100</td><td>2025-05-12T08:17:00+00:00</td></tr>
<tr><td>121.254.195.16</td><td>KR</td><td>100</td><td>2025-05-12T08:17:00+00:00</td></tr>
</table></td></tr>
<tr><td><b>4.</b></td><td><b>Maintaining Access – Automation (AI Implementation)</b></td><td></td><td></td></tr>
<tr><td></td><td><b>AI Tools Used</b></td><td>Scikit-learn (RandomForestClassifier), Pandas, LabelEncoder for data encoding.</td><td>
import pandas as pd
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import LabelEncoder
from sklearn.metrics import classification_report, confusion_matrix
import joblib
import os</td></tr>
<tr><td></td><td><b>Automation Implemented</b></td><td>Automated training, prediction, and labeling of suspicious IPs with alerts.</td><td>
Save model and feature columns
joblib.dump(model, 'models/random_forest_model.pkl')
joblib.dump(feature_columns, 'models/feature_columns.pkl')
print("\nModel and feature columns saved successfully to 'models/' directory.")</td></tr>
<tr><td><b>5.</b></td><td><b>Covering Tracks & Report</b></td><td></td><td></td></tr>
<tr><td></td><td><b>Vulnerability Risk Factors</b></td><td>Provided threat score via model output; flagged top malicious IPs.</td><td></td></tr>
</table>

	VAPT Report	All findings compiled into auto-generated CSV files and dashboard logs for reporting.	

```
C:\Users\admin\Desktop\cyber project final>python utils/train_model.py
Training features: ['countryCode', 'abuseConfidenceScore', 'report_hour', 'report_day']

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00      1669
           1       1.00      1.00      1.00       331

    accuracy                           1.00      2000
   macro avg       1.00      1.00      1.00      2000
weighted avg       1.00      1.00      1.00      2000

Confusion Matrix:
[[1669    0]
 [   0  331]]

Model saved successfully to models/random_forest_model.pkl

C:\Users\admin\Desktop\cyber project final>
```