A red sign with white text

Description automatically generated School of Computing and Creative Technologies

**Assessment Submission – Cover Sheet**

## **Student Details**

|  |  |
| --- | --- |
| **Student Number** | Sahifa Syed |
| **Student Name** | 23051901 |

# **Submission Files**

You **must** submit,

1. A cover sheet (this sheet).
2. A zipped folder that contains four sub-folders titled ‘Task 1’, ‘Task 2’, ‘Task 3’, and ‘Task 4’. Each sub-folder should contain all the files related to the task.

|  |  |
| --- | --- |
| **Task** | **Files submitted** |
| Task-1 Folder | **Portfolio\_Task1.ipynb :** Jupyter notebook with all code that provides the answers for the given tasks.  ***Instructions:***   1. *Ensure* ***Anaconda*** *and* ***Jupyter Notebook*** *are installed.* 2. *Open* ***Portfolio\_Task1.ipynb*** *in Jupyter Notebook.* 3. *Make sure any given data files are in the* ***same folder*** *(e.g., Downloads) as the notebook.* 4. ***Run all cells*** *(****Kernel > Restart & Run All****) if necessary.* |
| Task-2 Folder | **Portfolio Task 2.ipynb :** Jupyter notebook with all code and visuals to demonstrate attacks and network protocols.  **Instructions:**   1. Ensure **Anaconda** and **Jupyter Notebook** are installed. 2. Open **Portfolio Task 2.ipynb** in Jupyter Notebook. 3. Make sure any given data files are in the **same folder** (e.g., Downloads) as the notebook. 4. **Run all cells** (**Kernel > Restart & Run All**) if necessary. |
| Task-3 Folder | **Portfolio Task 3.ipynb :** Jupyter notebook with all code and markdown commentary.  ***Instructions:***   1. *Ensure* ***Anaconda*** *and* ***Jupyter Notebook*** *are installed.* 2. *Open* ***Portfolio Task 3.ipynb*** *in Jupyter Notebook.* 3. *Make sure any given data files are in the* ***same folder*** *(e.g., Downloads) as the notebook.* 4. ***Run all cells*** *(****Kernel > Restart & Run All****) if necessary.* |
| Task-4 Folder | **Data Collection Suggestions :** *Part 1* – Uses table layout as given in brief to demonstrate and give suggestions to the local government on the collection of data and preparation of the dashboard  **portfolio\_task\_4.ipynb :** *Part 2* - Jupyter Notebook visualising network and endpoint monitoring data using plotly.  **network\_traffic.csv :** Dummy dataset containing network traffic metrics.  **endpoint\_metrics.csv :** Dummy dataset containing endpoint metrics.  **Instructions to run the files:**   1. Open portfolio\_task\_4.ipynb in Jupyter Notebook. 2. Make sure network\_traffic.csv and endpoint\_metrics.csv are in the **same folder** as the notebook. 3. Run all cells (Kernel > Restart & Run All) to generate visualisations. 4. Required Python packages:    * pandas    * plotly |

You can **optionally** provide additional information or comments specific to the sub-tasks within a task.

# **Task 1**

|  |  |  |
| --- | --- | --- |
|  | **Task** | **Comments** |
| 1 | Load the dataset, find out and print the total number of rows and columns in the dataset. |  |
| 2 | Your dataset will have one or more columns containing dates, find out and print how many dates are null, incorrect or incomplete. Apply the dataset context and domain knowledge while investigating ‘incorrect’ dates. |  |
| 3 | Fix the incorrect dates. Provide (print, visualise) evidence of fixed dates. |  |
| 4 | Prepare and visualise a correlation matrix between the following numerical columns,   * 'replies\_count' * 'participants\_count' * 'likes' * 'comments' * 'shares' |  |
| 5 | For the discrete/categorical columns ‘language’ and ‘author‘, find out how many values are ‘null’ or ‘empty’. Apply a data imputation technique of your choice to replace missing values in any one of the three columns (‘language’ and ‘author’) |  |
|  | **Total** |  |

# **Task 2**

|  |  |  |
| --- | --- | --- |
|  | **Task** | **Comments** |
| 1 | Investigate and conclude whether there is evidence of a flooding attack in the file.  If yes, what is the type of the attack and how many flooding packets were found out of total packets.  For example,  File 1 – No flooding attack – 0/500 flooding packets  File 2 – SYN flood – 421/500 flooding packets |  |
| 2 | In files where there is evidence of a flooding attack, present your results visually, as follows,   * A pie chart to show the ratio of possible flood attacks. * A bar chart to show the distribution of packet types by protocol in the file. |  |
|  | **Total** |  |

# **Task 3**

|  |  |  |
| --- | --- | --- |
|  | **Task** | **Comments** |
| 1 | Load the files using a Python script. |  |
| 2 | Print all the Section headers. |  |
| 3 | Print all the imported libraries. |  |
| 4 | Print all the exported symbols. |  |
| 5 | Print all the string features of length four or more characters. |  |
| 6 | Create a list of following suspicious imports ( ‘GetProcAddress’ 'CreateRemoteThread', ‘TerminateProcess’, 'VirtualAlloc', and 'WriteProcessMemory') and write a script to check if the calls exits in a sample file.  If a file has more than 50% matches, it should be considered malicious. |  |
|  | **Total** |  |

# **Task 4**

|  |  |  |
| --- | --- | --- |
|  | **Task** | **Comments** |
| 1 | Data collection advise for network traffic monitoring. |  |
| 2 | Data collection advise for endpoints monitoring. |  |
| 3 | Data collection advise for data backups monitoring. |  |
| 4 | Data collection advise for staff readiness monitoring. |  |
| 5 | Prototype dashboard using two input files. |  |
| 6 | Effective layout and design of the dashboard. |  |
|  | **Total** |  |