Individual Project (CS3IP16)

Department of Computer Science

University of Reading

Project Initiation Document

## PID Sign-Off

|  |  |
| --- | --- |
| **Student No.** |  |
| **Student Name** |  |
| **Email** |  |
| **Degree programme** (BSc CS/BSc CSwIY) |  |
|  |  |
| **Supervisor Name**  *(Consultation with supervisor is mandatory)* |  |
|  | Supervisor to sign PID form on Bb (grade centre) |
| **Date** |  |

# SECTION 1 – General Information

## Project Identification

|  |  |
| --- | --- |
| **1.1** | **Project Title** |
|  | The Automatic R.A.T. Machine |
| **1.2** | **Please describe the project with key-phrases (max 5)** |
|  | LLM powered automatic remote access trojan for penetration testers. |
| **1.3** | **E-logbook maintenance agreed with supervisor**  *Use Google doc, OneDrive, or any mobile App whereby you will be able to generate a PDF copy* |
|  |  |
| **1.4** | **GitLab link for maintain source code and research data**  *Any change in GitLab link and Source code repository MUST be explicitly mention in final report* |
|  |  |

# SECTION 2 – Project Description

|  |  |
| --- | --- |
| **2.1** | **Summarise the project’s background in terms of research field /application domain (max 100 words).** |
|  | The project researches the applications of artificial intelligence, specifically large language models to aid and speed up the work of penetration testers. The goal is to make a self contained device that will use its own reasoning capabilities in order to gain an initial foothold on a network for a penetration tester. The main area of research for this project understanding how to guide a GPT based agent to complete such a complex task. |
| **2.2** | **Summarise the project aims, objectives and outputs (max 250 words).** These aims, objectives, and outputs should appear as the tasks, milestones and deliverables in your project plan (fill out Section 3). |
|  | The aim of this project is to understand to what extent a simple language model can be used to carry out complex tasks. The project will compose of a task manager, which guides the model into carrying out a structured plan and numerous language model based agents which can accomplish tasks in whichever way is most fit for the situation. If successful, the project should be able to conduct a penetration test on a wide variety of systems without explicitly being programmed to do so.   * Understand how to make a reliable GPT based agent using langchain (or similar alternative libraries) * Research whether the performance of the models can be improved via methods such as fine-tuning or adding vector databases of security information. * Implement a task manager system to keep track of the process of the penetration test and guides the model to its next steps. * Implement the software side of the program. * Implement a reporting mechanism that logs all actions taken by the device and sends it to the operator. * Create a raspberry pi based self contained device to house the system. * Create a way for the system to communicate with the operator remotely. This will most likely require an LTE connection and a web interface or app to control the device from. * Evaluate the performance by testing it on simulated networks and systems. * Document the entire process to aid with report creation. |

|  |  |
| --- | --- |
| **2.3** | **Initial project specification – roughly indicate key features and functions of your finished program/application. Indicate possible method, data source, technology etc. (max 400 words)** (Sensible and relevant Charts, Table, and Figures can be used) |
|  | Key features:   1. The project should have the ability to scan networks and identify devices that could be considered targets for a penetration tester. 2. The project should have the ability to attempt to exploit a selected target without interrupting its normal operating behaviour. 3. If successfully exploited. The project should have the ability to take control of the device, hide its tracks, and set the device up for an operator to take over. The project should be able to do this without negatively affecting the devices operation. 4. The project should be self-contained in a raspberry pi –like device and have LTE connection to communicate with the operator, regardless of network connection. 5. The project should provide some sort of dashboard or communication method with the operator. 6. The project should log or report what things it has tried to save time for the operators. |
| **2.4** | **Describe the social, legal and ethical issues that apply to your project. Does your project require ethical approval? (If your project requires a questionnaire/interview for conducting research and/or collecting data, you will need to apply for an ethical approval)** |
|  |  |
| **2.5** | **Identify the items you may need to purchase for your project. A cost upto £200 can be applied (include VAT and shipping if known). You need to have consent of your supervisor. Your request will be assessed by the department.** |
|  | USB – LTE adapter for communication: 20£  M.2 LTE module: 40£  OpenAI API credits: 140£ (will likely cost more, I will pay the rest personally) |
| **2.6** | **State whether you need access to specific resources within the department or the University e.g. special devices and workshop** |
|  | no |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **SECTION 3 - Project Plan** | | | | | | | | | | | | | |
| Please provide your project plan.  Below is an example project plan, you can use any tool or software to generate yours. | | | | | | | | | | | | | |
| **Project stage** [this is only indicative – write your own stages] | **START DATE: ../../…. <enter the project start date here>****Project Weeks** | | | | | | | | | | | | |
| 0-3 | 3-6 | 6-9 | 9-12 | 12-15 | 15-18 | 18-21 | 21-24 | 24-27 | 27-30 | 30-33 | 33-36 | 36-39 |
| 1 Background Research |  |  |  |  |  |  |  |  |  |  |  |  |  |
| * 1. … |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.2 … |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 Analysis/Design |  |  |  |  |  |  |  |  |  |  |  |  |  |
| .. |  |  |  |  |  |  |  |  |  |  |  |  |  |
| .. |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 Develop prototype |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 Testing/evaluation/validation |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 Assessments |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |