

Configuration Manual

MSc Research Project
Masters In Cybersecurity

Mrunali Umesh Sawant
Student ID: x22191135

School of Computing
National College of Ireland

Supervisor: Mr. Joel Aleburu

National College of Ireland
MSc Project Submission Sheet



School of Computing


Mrunali Umesh Sawant

Student Name:
Student ID: X22191135
Programme: Masters in cybersecurity **Year:** Sep 2023-2024
MSc Research Project
Module:
Mr. Joel Aleburu
Supervisor:
Submission Due Date: 12/08/2024
Project Title: Comparative Analysis of Penetration Testing Frameworks for OT Systems
.....

Word Count: **Page Count:**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: 
Date: 12/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Mrunali Umesh Sawant

X22191135

Configuration Manual for Mock Penetration Testing Script

	Table of Contents
1	Introduction
2	System Requirements
3	Environment Setup
	Install Python
	Set Up Virtual Environment
	Install Required Libraries
4	Dataset Preparation
5	Running the Script
6	Analysis of Results
7	Troubleshooting

1 Introduction

This manual provides instructions for configuring and running a Python-based mock penetration testing script. The script simulates penetration testing by generating mock vulnerabilities within a dataset.

2 System Requirements

- **Operating System:** Windows 10/11, macOS, or Linux
- **Python Version:** 3.7 or higher
- **RAM:** Minimum 4 GB (8 GB recommended)
- **Storage:** Minimum 500 MB free space
- **Dependencies:**
 - pandas
 - numpy
 - random

3 Environment Setup

3.1 Install Jupyter or Python

1. Download Jupyter from official [Project Jupyter | Home](#)

OR

Download Python from the official [Python website](#).

2. Install Python or Jupyter by following the on-screen instructions.

Ensure that you check the box to add Python to your system PATH during installation

3.2 Set Up Virtual Environment

1. Open your terminal or command prompt.

2. Navigate to your project directory:

`cd path/to/your/project.`

3. Create a virtual environment:

`python -m venv venv`

4. Activate the virtual environment:

Windows- `venv\Scripts\activate`

Mac Os /Linux- `source venv/bin/activate`

3.3 Install Required Libraries

1. Ensure your virtual environment is activated.

2. Install the necessary Python libraries:

`pip install pandas numpy`

3. If you encounter a notice about an outdated version of pip, you can upgrade it:

`python -m pip install --upgrade pip`

4 Dataset Preparation

1. Place the hai-train1.csv dataset in your project directory.
2. Ensure the dataset file is correctly named and formatted for use with the script

HAI Security Dataset downloadable link: [HAI Security Dataset \(kaggle.com\)](#)

5 Running the script

1. Open your terminal or command prompt.
2. Navigate to your project directory and activate the virtual environment.
3. Run the Python script: `python script_name.py`

Replace `script_name.py` with the actual name of your script.

4. The script will load the dataset, simulate a penetration test, and print the results along with an analysis summary.

6 Analysis of results

After running the script, you will see an analysis summary that includes:

- Total number of vulnerabilities identified.
- Number of vulnerabilities.
- Number of false positives.
- Distribution of metrics
- Box plot of metrics

7 Troubleshooting

Common Issue –

- **Python Not Recognized:** Ensure Python is added to your system PATH.
- **Module Not Found:** Make sure all required libraries are installed and that your virtual environment is activated.
- **Dataset Not Found:** Verify that the `hai-train1.csv` file is in the correct directory.

Useful Commands –

•Activate Virtual Environment:

- Windows: `venv\Scripts\activate`
- macOS/Linux: `source venv/bin/activate`
-

•Deactivate Virtual Environment:

- Run `deactivate` in the terminal.

•List Installed Libraries:

`pip list`

•Update a Library:

`pip install --upgrade library_name`

This manual should guide you through the setup and execution of your mock penetration testing script, ensuring a smooth and trouble-free experience.