National College of Ireland

Configuration Manual

MSc Internship

Neha Patil
Student ID: x18200192

School of Computing
National College of Ireland

Supervisor: Mr. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Neha Patil……

Student ID: 18200192……..……

Programme: Cyber Security…… **Year:** 2020……..

Module: MSc Internship……..……

Lecturer: Mr. Vikas Sahni……..……

Submission Due Date: 17/8/2020……..……

Project Title: Detecting and preventing Man in The Middle attack using Interlocking protocol and HMAC caused by perpetrator

Word Count: 369…… **Page Count:** 6……..……..……

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.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: ……

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
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.	□

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

Neha Patil
x18200192

1. Summary

The proposed paper describes the procedure to mitigate man in the middle attack using interlocking protocol and HMAC . Various Python scripts are developed for implementing server-client communication, man in the middle and cryptographic model for HMAC. For demonstrating TCP ip communication, Wireshark has been used to capture the traffic. For development of the python script PyCharm software has been used.

2. Tools

The implementation required three major components viz. Wireshark and Python[4], on a base windows machine.

1. **PyCharm**: for developing the python scripts which includes server.py, client.py, Middle_man.py, RSA.py and crypto.py PyCharm2019.2.2 community edition has been used.

2. **Wireshark**: For capturing the network traffic and viewing the communication Wireshark Version 3.2.5 (v3.2.5-0-ged20ddea8138) network analyzer tool has been used.

3. python: Used for developing scripts for server, client, man in the middle and cryptographic model.

3. Download and Installation

1. For Python Installation:

Python 3.8.4 has been installed from the official website.
Following commands has been used to installed required libraries on Python

>>python -m pip install -U pip
>>python -m pip install -U numpy
>>python -m pip install -U sympy

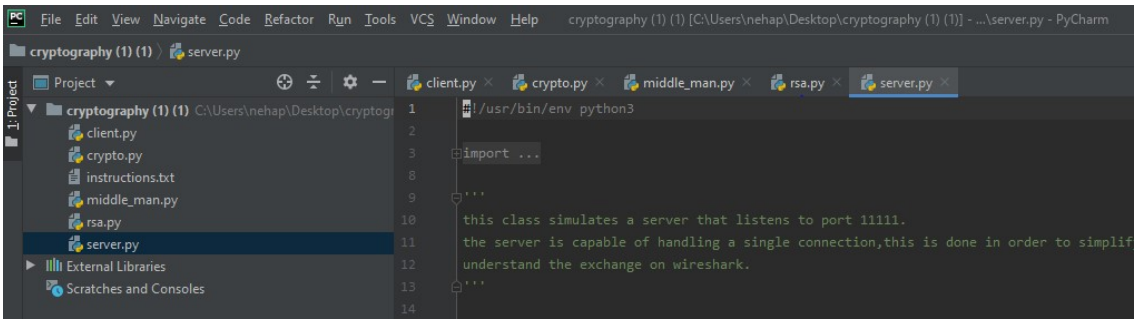
2. For Wireshark Installation:

Download the latest version of Wireshark software from Wireshark's org for analyzing network traffic.

4. Configuration and Execution

1. Python Scripting

We have used PyCharm software for writing the python scripts. We have created a project in PyCharm in which 5 python script have been written namely server.py, client.py, middle_man.py, rsa.py and crypto.py



2. Executing python scripts:

For the execution of python scripts for server, client and middleman we have used command prompt and run the following commands in following sequence.

>>python server.py

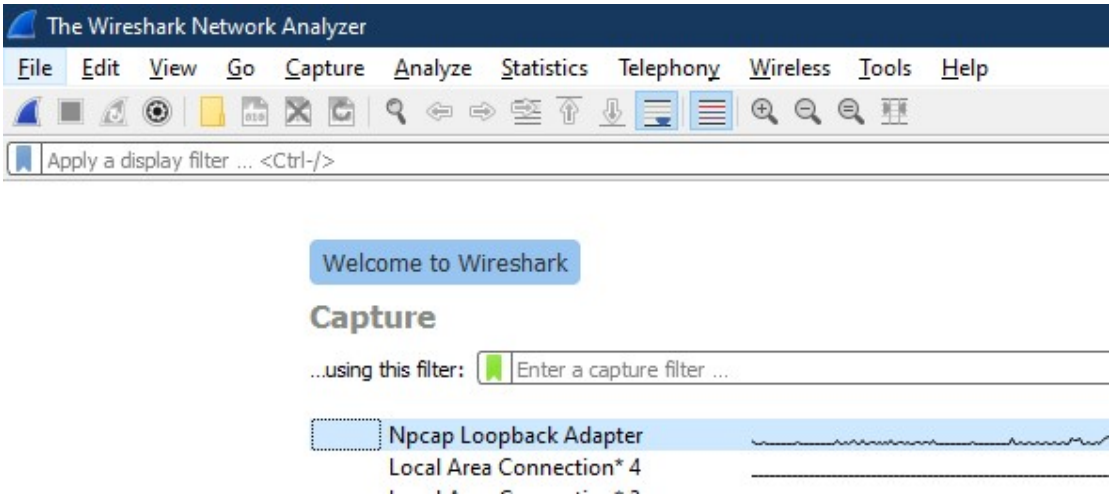
>>python middle_man.py

>>python client.py

3. Wireshark for analyzing:

Wireshark has been used for analyzing network traffic and demonstrating TCP/IP handshake between client, server, and middleman.

Post starting the Wireshark we will select NPCAP Loopback adapter and will click on start capturing packet option which is at top leftmost corner of the tool.



References

[1] "Welcome to Python.org," *Python.org*. [Online]. Available: https://www.python.org/. [Accessed: 12-Dec-2019]

[2] "Wireshark · Download." [Online]. Available: https://www.wireshark.org/download.html. [Accessed: 15-Aug-2020]

[3] "Installation — pip 20.2.2 documentation." [Online]. Available: https://pip.pypa.io/en/stable/installing/. [Accessed: 15-Aug-2020]

[4] "Download PyCharm: Python IDE for Professional Developers by JetBrains," JetBrains. [Online]. Available: https://www.jetbrains.com/pycharm/download/. [Accessed: 15-Aug-2020]