A Major Project Report

On

Automation of Reconnaissance: An Open-Source Tool for Pentesting

Project submitted in partial fulfillment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

BY

NEERADI ARYAN RAJ **(18C91A0561)**

PANNIRU SOWMYA **(18C91A0569)**

PINGILI RAKESH REDDY **(18C91A0575)**

Under the Esteemed guidance of

Dr. NARSIMHA M.Tech,Ph.D

Professor & Head Dept of CSE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE

(COLLEGE OF ENGINEERING)

(Approved by AICTE New Delhi, Permanently Affiliated to JNTU Hyderabad, Accredited by NAAC with 'A' Grade)

Bogaram (V), Keesara (M), Medchal District -501 301.

2021 - 2022

HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE

(COLLEGE OF ENGINEERING)

(Approved by AICTE New Delhi, Permanently Affiliated to JNTU Hyderabad, Accredited by NAAC with 'A' Grade)
Bogaram (V), Keesara (M), Medchal Dist-501301.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the major project entitled "**Automation of Reconnaissance: An Open-Source Tool for Pentesting**" is being submitted by NEERADI ARYAN RAJ (18C91A0561), PANNIRU SOWMYA(18C91A0569), PINGILI RAKESH REDDY (18C91A0575) in Partial fulfillment of the academic requirements for the award of the degree of Bachelor of Technology in "COMPUTER SCIENCE AND ENGINEERING" from HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE, JNTU Hyderabad during the year 2021- 2022.

INTERNAL GUIDE

Dr B. NARSIMHA M.Tech,Ph.D
Professor & Head
Dept. of Computer Science & Engineering

HEAD OF THE DEPARTMENT

Dr B. NARSIMHA M.Tech,Ph.D
Professor & Head
Dept. of Computer Science & Engineering

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who made it possible, who's constant guidance and encouragement crowns all effort with success.

We take this opportunity to express my profound gratitude and deep regards to our Guide **DR. BIRRU DEVENDER, Professor**, Dept. of Computer Science & Engineering, Holy Mary Institute of Technology & Science for his / her exemplary guidance, monitoring and constant encouragement throughout the project work.

Our special thanks to **Dr. B. Narsimha, Head of the Department**, Dept. of Computer Science & Engineering, Holy Mary Institute of Technology & Science who has given immense support throughout the course of the project.

We also thank **Dr**. **P. Bhaskar Reddy,** the **Honorable Director** of my college Holy Mary Institute of Technology & Science for providing me the opportunity to carry out this work.

At the outset, we express my deep sense of gratitude to the beloved **Chairman A. Siddarth Reddy** of **Holy Mary Institute of Technology & Science**, for giving me the opportunity to complete my course of work

We are obliged to **staff members** of Holy Mary Institute of Technology & Science for the valuable information provided by them in their respective fields. We are grateful for their cooperation during the period of my assignment.

Last but not the least we thank our **Parents**, and **Friends** for their constant encouragement without which this assignment would not be possible.

NEERADI ARYAN RAJ **(18C91A0561)**

PANNIRU SOWMYA **(18C91A0569)**

PINGILI RAKESH REDDY **(18C91A0575)**

DECLARATION

This is to certify that the work reported in the present project titled **"Automation of Reconnaissance: An Open-Source Tool for Pentesting"** is a record of work done by us in the Department of Computer Science & Engineering, Holy Mary Institute of Technology and Science.

To the best of our knowledge no part of the thesis is copied from books / journals/ internet and wherever the portion is taken, the same has been duly referred to in the text. The reports are based on the project work done entirely by us not copied from any other source.

NEEADI ARYAN RAJ **(18C91A0561)**

PANNIRU SOWMYA **(18C91A0569)**

PINGILI RAKESH REDDY **(18C91A0575)**

INDEX

Content **PageNo.**

1. INTRODUCTION……..1

1.1 MOTIVATION……1

1.2 PROBLEM DEFINITION……...4

1.3 OBJECTIVE……5

1.4 LIMITATIONS.……...……6

2. LITERATURE SURVEY……9

2.1 EXISTING SYSTEM……...15

2.2 DISADVANTAGES OF EXISTING SYSTEM……..16

2.3 PROPOSED SYSTEM……..…16

2.4 ADVANTAGES OF PROPOSED SYSTEM……..……17

3. SYSTEM ANALYSIS…….….18

3.1 SOFTWARE REQUIREMENTS SPECIFICATION…….18

3.2 SOFTWARE REQUIREMENTS……18

3.3 HARDWAR EREQUIREMENTS……..18

4. SYSTEM DESIGN……..18

4.1 SYSTEM ARCHITECTURE……..19

4.2 USE CASE DIAGRAM……..21

4.3 ACTIVITY DIAGRAM……...…...22

4.4 SEQUENCE DIAGRAM……...….25

4.5 UML DIAGRAM…… 26

5. IMPLEMENTATION AND RESULT 27

5.1 ENVIRONMENTAL SETUP…….27

5.2 MODULE DESCRIPTION…….29

5.3 SOFTWARE DESCRIPTION……30

5.4 SAMPLE CODE……..…...33

5.5 INSTALLATION SCREEN……...….37

5.6 OUTPUT SCREENS……...46

6. SYSTEM TESTING..... 54

6.1 INTRODUCTION……...54

7. CONCLUSION……56

8. REFERENCE……...57

LIST OF FIGURES

Figure No.	Figure Name	Page No.
1	System Architecture for recon	19
2	Use-case Diagram	21
3	Root Activity Diagram	22
4	Activity diagram for recon method	23
5	Types of recon method	24
6	Sequence diagram for recon method	25
7	Basic sketch for recon method	25
8	UML Diagram	26

LIST OF SCREENSHOTS

Image No.	Image Name	Page No.
1	Getting system-update	37
2	Installing Python	37
3	Installation pip	38
4	Installing python3	38
5	Installing subdomain tool	39
6	Using subdomain finding tool	39
7	Installing main go language	40
8	Installing second subdomain tool	40
9	Installing tool extension	41
14	Installing spidering tool	43
17	Installing screenshotting tool	45
18	Path setting and installation completed screen	45
19	Recon started	46
20	Finding the services of live subdomains	46
22	Filtering working domains and failed domains	47
23	Fetching ip address of working domains	48
24	Screenshotting working domains	48
25	Screenshotting non-working domains	49
26	Fetching all url branches of each and every working domain	49
27	Fetching url directories	50
33	Fetching url directories and reconnaissance completed	53

ABSTRACT

The need for Recon automation is rapidly increasing as ethical hackers are being lazy in performing every little check manually. So as to make the Recon process (Info gathering phase) of penetration testing easy, fast and accurate, a Recon framework with highly sophisticated tools written in languages like bash, go and python needs to be developed and made open source to everyone. Manually doing this task can be very intimidating since a lot of time and efforts are needed in accomplishing this task. So, automation of this task can be very handy to the penetration testers and saves a lot of time as they can focus on other tasks of the further tasks of a penetration test. So, our project is automation to the tedious task of information gathering. This Recon Framework just takes the main top-level domain of the organization as the input, does the recon and stores the result in an organized manner in the corresponding directories. The output of this framework is ready to be used to perform further security tests as the results are generated in a neat graspable format and can be passed to other tools to further filter the data according to the ethical hacker's wish and need. In addition to that, the results are displayed in a graphical interface in the form of a web application. So, all a user needs to do is enter the top-level domain name of the organization on which he/she wants to perform penetration testing.