A Project Report on

**Network Traffic Monitoring with Attack and Intrusion Detection System**

A dissertation submitted in the partial fulfillment of the requirement for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

INFORMATION TECHNOLOGY

Submitted by

Vyom Bhatia, Maitraiye Saxena, Shabad Sawhney, Vivek Kumar

Regn. No: 1081230004, 1081230005, 1081230006, 1081230008

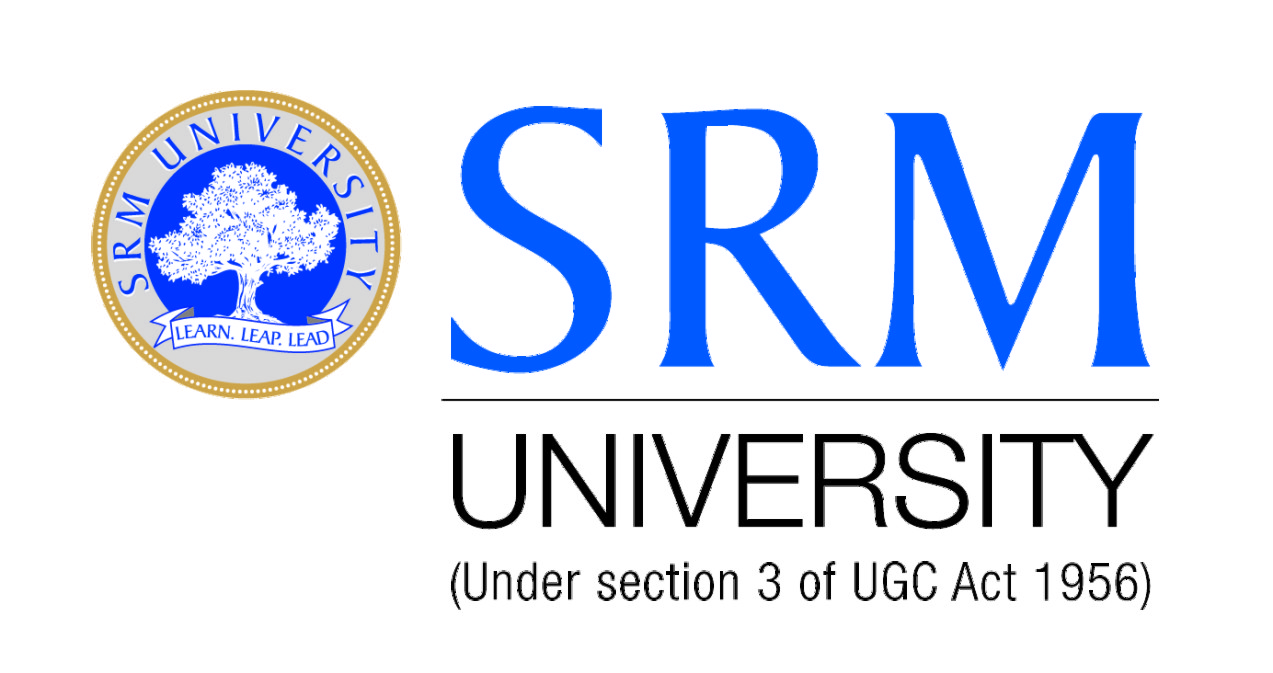
Under the guidance of

Mr. Chiranjit Dutta

Assistant Professor

Department of Information technology

**May 2016**



**DEPARTMENT OF INFORMATION TECHNOLOGY**

**SRMUNIVERSITY, NCR CAMPUS, MODINAGAR-201204**

**GHAZIABAD, UTTAR PRADESH**

**DECLARATION**

We**, *Vyom Bhatia, Maitraiye Saxena, Shabad Sawhney, Vivek Kumar* (Reg.No.*1081230004, 1081230005, 1081230006, 1081230008*)** hereby declare that the work which is being presented in the dissertation “***Network Traffic Monitoring with Attack and Intrusion Detection System*”** is the record of authentic work carried out by us under the supervision of **Mr. Chiranjit Dutta** in the Department of Information Technology, SRM University, NCR Campus, Modinagar, Ghaziabad (U.P.) and submitted in the partial fulfillment for the award of the degree of **Bachelor of Technology** in Information Technology. This work has not been submitted to any other University or Institute for the award of any Degree/Diploma.

***Vyom Bhatia, Maitraiye Saxena, Shabad Sawhney, Vivek Kumar***

**BONAFIDE CERTIFICATE**

Certified that this project work entitled *“****Network Traffic Monitoring with Attack and Intrusion Detection System****”*is the bonafide work of *Vyom Bhatia, Maitraiye Saxena, Shabad Sawhney, Vivek Kumar* (*Reg.No.1081230004, 1081230005, 1081230006, 1081230008*) who carried out the research under my supervision. Certified further, that to the best of my knowledge the work reporting here in does not form part of any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

**Mr. Chiranjit Dutta Mr. Madan Kumar**

Assistant Professor Head of the Department

Project Guide

SRM University, NCR Campus SRM University, NCR Campus

Modinagar Modinagar

Internal Examiner External Examiner

**ACKNOWLEDGEMENT**

We feel an immense amount of pleasure in submitting this project report on **“Network Traffic Monitoring with Attack and Intrusion Detection System**” as partial fulfillment for the award of the Degree of B.Tech. in Information Technology. The satisfaction and euphoria that accompany the successful completion of any project would be incomplete without a mention of people who made it possible and whose constant guidance and encouragement crown all the efforts.

First and foremost, we would like to express our hearty gratitude to **Dr.(Prof.) Manoj Kumar Pandey**, Director, SRM University, NCR Campus, Ghaziabad for his support and encouragement throughout the work and for providing the suitable environment to carry out the work.

We feel compelled to articulate my thankfulness to **Mr. Madan Kumar, HOD,Department of Information Technology,** SRM University for his encouragement which was a source of inspiration.

We also extend our heartfelt gratitude to **Mr. Dinesh Kumar**, Project Coordinator, whose constant motivation and support made me enthusiastic throughout the work.

We would also like to express our sincere gratitude to our advisor, **Mr. Chiranjit Dutta** for his invaluable guidance and cooperation throughout the work. His constant encouragement and vision enabled me to take this new endeavor to the success path.

In the last but not least we are indebted to all the teaching and non-teaching staff members of our college for helping us directly or indirectly by all means throughout the course of our study and project work.

**ABSTRACT**

Every organization, irrespective of its size depends on networking technologies. These networks hold the working of entire organization and thus are very important part of the organization. Being the backbone of the business, it is vulnerable to attacks from crackers and rival organizations to gain unauthorized information or to cause harm to the business of the organization. The aim of the project is to protect the network infrastructure of the organization by developing a software to monitor the network and detect malicious activities on it. In order to demonstrate the working of the software, different attacks have been developed to crack into the network infrastructure. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to the administrator, whereasnetwork traffic monitoring is the process of sniffing, reviewing, analysing and managing network traffic for any abnormality or process that can affect network performance, availability and/ or security.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Contents** | **Page No.** |
|  | Declaration | ii |
|  | Bonafide Certificate | iii |
|  | Acknowledgement | iv |
|  | Abstract | v |
|  | List of Abbreviations | ix |
|  | List of Tables | x |
|  | List of Figures | xii |
| 1. | INTRODUCTION | 1 |
|  | 1.1 Introduction | 2 |
|  | 1.2 History | 2 |
|  | 1.3 Literature Survey | 3 |
|  | 1.3.1 Basic Terminology | 3 |
|  | 1.3.2 NIDS | 4 |
|  | 1.3.3 Network Traffic Monitoring | 4 |
| 2. | ANALYSIS AND MODELLING | 5 |
|  | 2.1 Introduction | 6 |
|  | 2.2 Data Flow Diagram | 6 |
|  | 2.3 IP Scanner Module | 9 |
|  | 2.4 System Query Module | 10 |
|  | 2.5 Network Traffic Monitoring and Intrusion Detection | 11 |
| 3. | METHODOLOGY AND FUNCTIONALITY | 13 |
|  | 3.1 Introduction | 14 |
|  | 3.2 Network Traffic Monitoring Module | 17 |
|  | 3.3 Attacks and Intrusion Detection Module | 19 |
|  | 3.3.1 Attack Detection | 19 |
|  | 3.3.1.1 DoS Attack | 20 |
|  | 3.3.1.2 SYN Flood Attack | 21 |
|  | 3.3.1.3 Brute Force Attack | 23 |
|  | 3.3.1.4 DNS Spoofing Attack | 23 |
|  | 3.3.1.5 MAC Flood Attack | 25 |
|  | 3.3.2 Intrusion Detection | 26 |
|  | 3.4 Integration and User Interface | 28 |
| 4. | SOFTWARE REQUIREMENT SPECIFICATION | 31 |
|  | 4.1 Purpose | 32 |
|  | 4.2 Scope of the Project | 32 |
|  | 4.3 Technologies Used | 32 |
|  | 4.3.1 Ubuntu Operating System | 32 |
|  | 4.3.2 VMWare Player | 33 |
|  | 4.3.3 Tkinter | 33 |
|  | 4.3.4 Scapy Library | 34 |
|  | 4.3.5 Gedit | 34 |
|  | 4.3.6 Psutil Library | 34 |
|  | 4.3.7 Language | 35 |
|  | 4.4 System Requirements | 35 |
|  | 4.4.1 Hardware Requirements | 35 |
|  | 4.4.2 Software Requirements | 35 |
|  | 4.5 Description of Main Functionality | 36 |
| 5. | SCREENSHOTS | 37 |
| 6. | RESULT | 46 |
| 7. | CONCLUSION AND FUTURE WORK | 49 |
|  | 7.1 Conclusion | 50 |
|  | 7.2 Future Work | 51 |
|  | REFERENCES | 54 |

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Abbreviation** | **Full form** |
| 1. | Msg | Message |
| 2. | Admin | Administrator |
| 3. | IP | Internet Protocol |
| 4. | DoS | Denial of Service |
| 5. | IDS | Intrusion Detection System |
| 6. | NIDS | Network Intrusion Detection System |
| 7. | ARP | Address Resolution Protocol |
| 8. | SSH | Secure Shell |
|  |  |  |

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Index No.** | **Table Name** |
| 1. | 4.1 | Hardware Requirements |
| 2. | 4.2 | Software Requirements |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Index No.** | **Figure Name** |
| 1. | 2.1 | 0 Level Data Flow Diagram |
| 2. | 2.2 | IP Scanner Module |
| 3. | 2.3 | System Query Module |
| 4. | 2.4 | Network Traffic Monitoring and Intrusion Detection Module |
| 5. | 3.1 | Division of Modules |
| 6. | 3.2 | Three-Way Handshake between the Client and the Server |
| 7. | 3.3 | SYN Flooding blocks Other Clients to Perform Three-Way Handshake with the Server |
| 8. | 5.1 | Server and User Address |
| 9. | 5.2 | Zucknet Address |
| 10. | 5.3 | Startup Scan with MAC IP Address binding and Live Traffic Monitoring |
| 11. | 5.4 | Users Tab |
| 12. | 5.5 | Report Histogram for Manual Analysis |
| 13. | 5.6 | Refresh IP Scan |
| 14. | 5.7 | Send Message Tab |
| 15. | 5.8 | Broadcast and Unicast Message |
| 16. | 5.9 | Broadcast Message send and Receive |
| 17. | 5.10 | Unicast Message send and Receive |
| 18. | 5.11 | FTP Brute Force Attack detection |
| 19. | 5.12 | SSH Attack Detection |
| 20. | 5.13 | MAC Flood Detection |
| 21. | 5.14 | Telnet Brute Force Attack |
| 22. | 5.15 | DDoS Attack Detection |
| 23. | 5.16 | Telnet Brute Force Attack Detection |
| 24. | 5.17 | SYN Flood Attack Detection |
| 25. | 5.18 | DNS Spoof Detection |