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

SRM
UNIVERSITY
(Under section 3 of UGC Act 1956)

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
Assistant Professor
Project Guide
SRM University, NCR Campus
Modinagar

Mr. Madan Kumar
Head of the Department

SRM University, NCR Campus
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

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

LIST OF FIGURES