Network Traffic Dataset Generation & Analysis to identify Security Threats

A PROJECT REPORT

Submitted in partial fulfilment of the requirement of

BACHELOR OF TECHNOLOGY

IN

INFORMATION TECHNOLOGY

Submitted By

Aarav Tyagi (20107001)

Dushyant Parashar (20107022)

Under the Supervision of

Mr Suhel Ahamed

TO

DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF STUDIES ENGINEERING AND TECHNOLOGY

GURU GHASIDAS VISHWAVIDYALAYA

30th April 2024

DEPARTMENT OF INFORMATION TECHNOLOGY
GURU GHASIDAS VISHWAVIDYALAYA
BILASPUR - 495009, INDIA

CERTIFICATE

This is to certify that the project report entitled "Network Traffic Dataset Generation & Analysis to Identify Security Threats" submitted by Aarav Tyagi(20107001) and Dushyant Parashar(20107022) to Guru Ghasidas Vishwavidyalaya towards partial fulfilment of requirements for the award of degree of Bachelor of Technology in Information Technology is a record of bonafide work carried out by him under my supervision and guidance during April 2024.

HEAD
Department of Information Technology
SoS, Engg. & Technology
Guru Ghasidas Vishwavidyalaya
(Central University) Bilaspur (C.G.)

Date: April 30, 2024

Place : Bilaspur

Mr SuhelAhamed

Department of InformationTechnology

Guru Ghasidas Vishwavidyalaya
Bilaspur - 495009, India

ABSTRACT

In response to evolving cybersecurity threats, this project focuses on generating a sophisticated network traffic dataset aimed at enhancing the effectiveness of threat detection systems. Utilizing a customized simulation environment, this dataset incorporates a diverse range of attack scenarios to mirror real-world network vulnerabilities. The core of this dataset is derived from a controlled lab setting using virtual machines and honeypot technologies to simulate authentic network interactions and attacks. This approach not only fills a critical gap in current cybersecurity research by providing rich, real-time data but also offers a foundational dataset that can be used to train and improve machine learning models for future threat detection and cybersecurity measures.

Using a combination of virtualized environments and honeypot technology, the simulator captures detailed network traffic and attack patterns. Analysis of the generated data provides unique insights into attacker behaviors and potential vulnerabilities, offering a significant contribution to the development of more robust security systems.