NIDS for Real-Time Protocol Analysis and Deep Content Inspection - MITM

Batch Number: 03

Roll Number	Student Name
20211CCS0049	KRISHNA GEETHA P
20211CCS0102	CHANDAN KUMAR MS
20211CCS0112	MANOJ K
20211CCS0129	CHARAN R

Under the Supervision of,

Mr. Tanveer Ahmed
Assistant Professor
School of Computer Science and Engineering
Presidency University

Name of the Program: B.TECH
Name of the HoD: Dr. Ananda Raj S P
Name of the Program Project Coordinator: Dr. Sharmasth Vali Y
Name of the School Project Coordinators: Dr. Sampath A K / Dr. Abdul Khadar A / Mr. Md Ziaur Rahman

Introduction

- In today's digital landscape, network security is a critical aspect of maintaining the integrity and confidentiality of information transmitted across networks. As network systems become increasingly complex, they are also more vulnerable to a wide range of cyber threats.
- One of the most dangerous types of attacks is the Man-in-the-Middle (MITM) attack.
- Our focus is on analyzing network traffic to detect and identify signs of MITM attacks. By doing so, we aim to enhance security measures, prevent data breaches, and ensure that communications within the network remain secure and trusted. Through a combination of traffic analysis, anomaly detection, and advanced security techniques, we can better protect networks from these sophisticated threats.

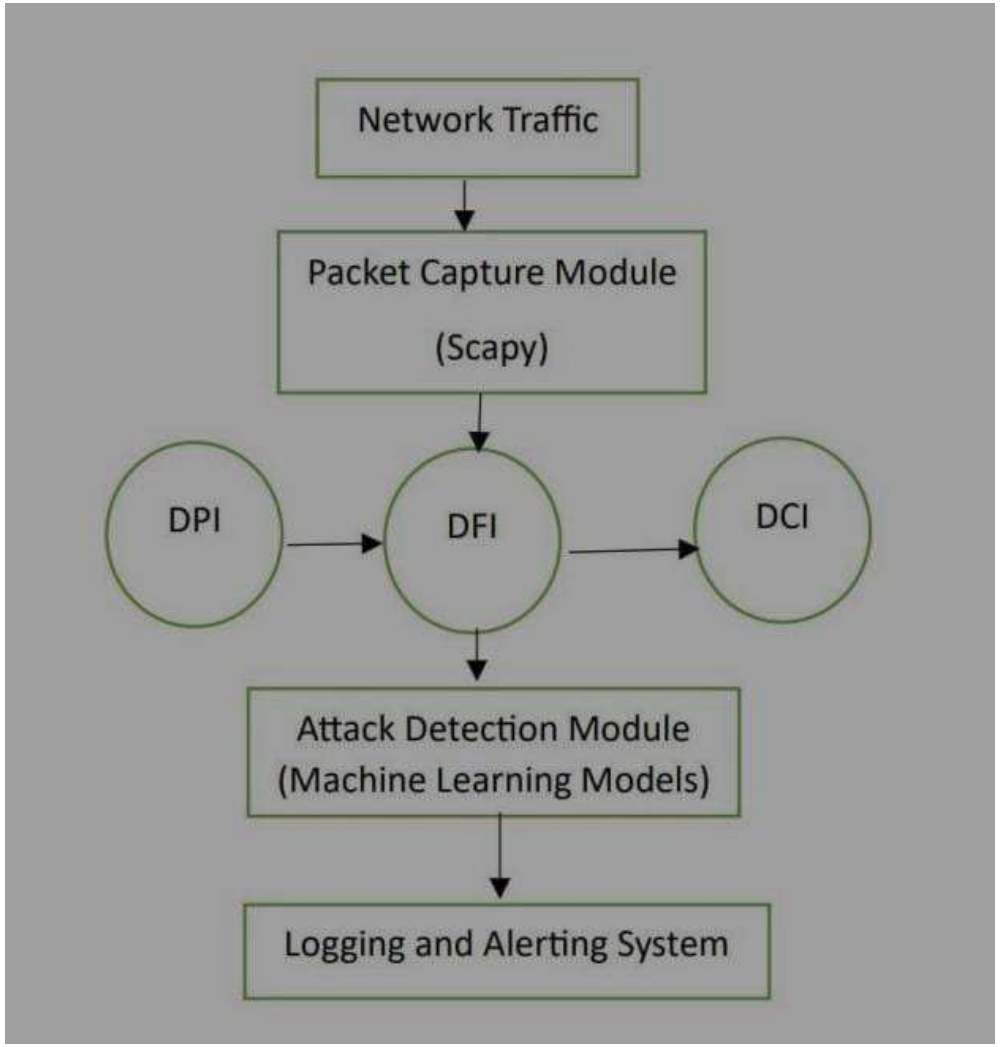
Objectives

- Analyzing incoming packets
- Identify protocol
- Alerting to admin
- Detecting dangerous IP address
- Improve Scalability

Proposed Method

- Hybrid Detection Techniques
- Real-Time Protocol Analysis
- Encrypted Traffic Analysis
- Automated Threat Intelligence Integration

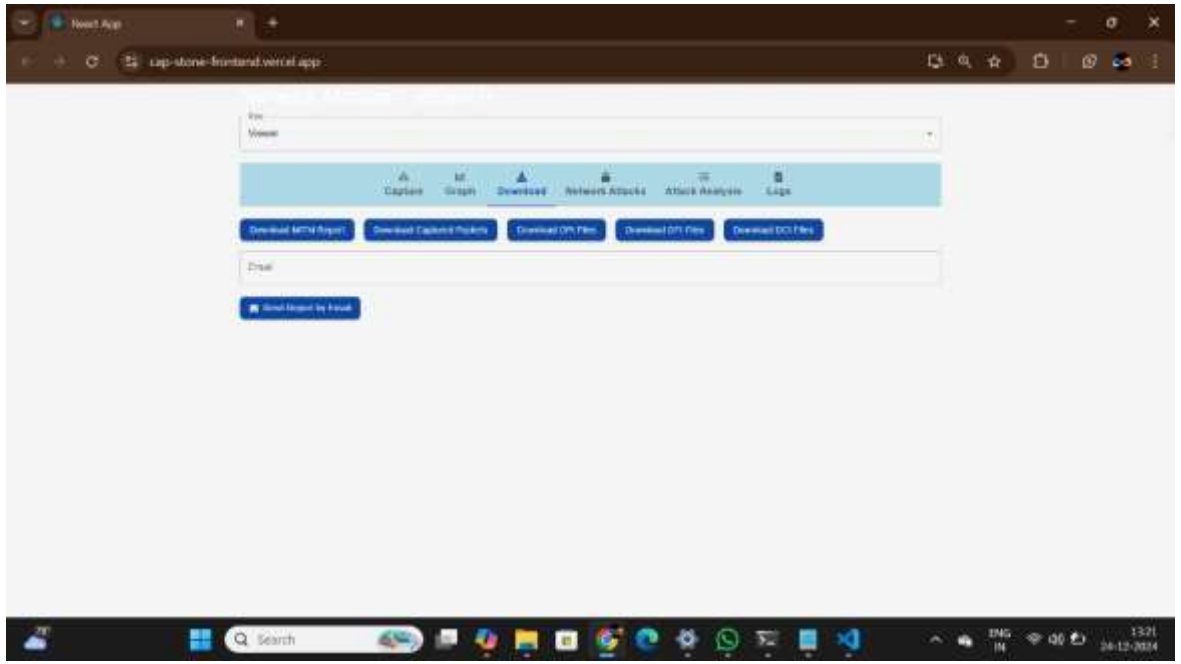
Architecture

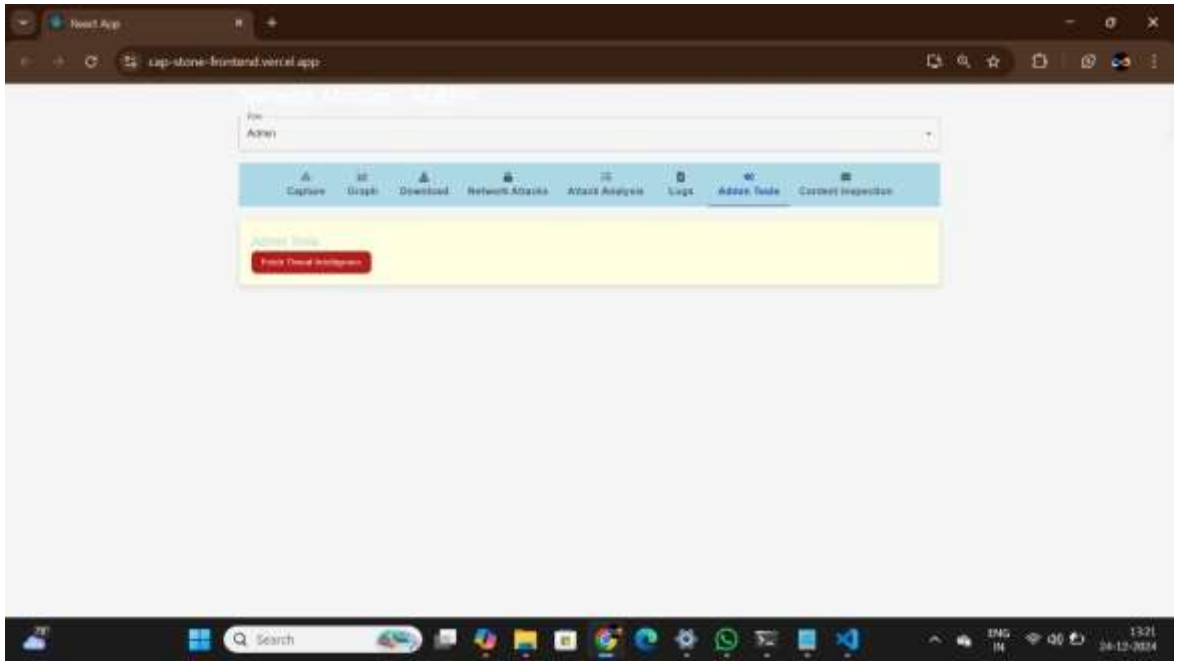


software components

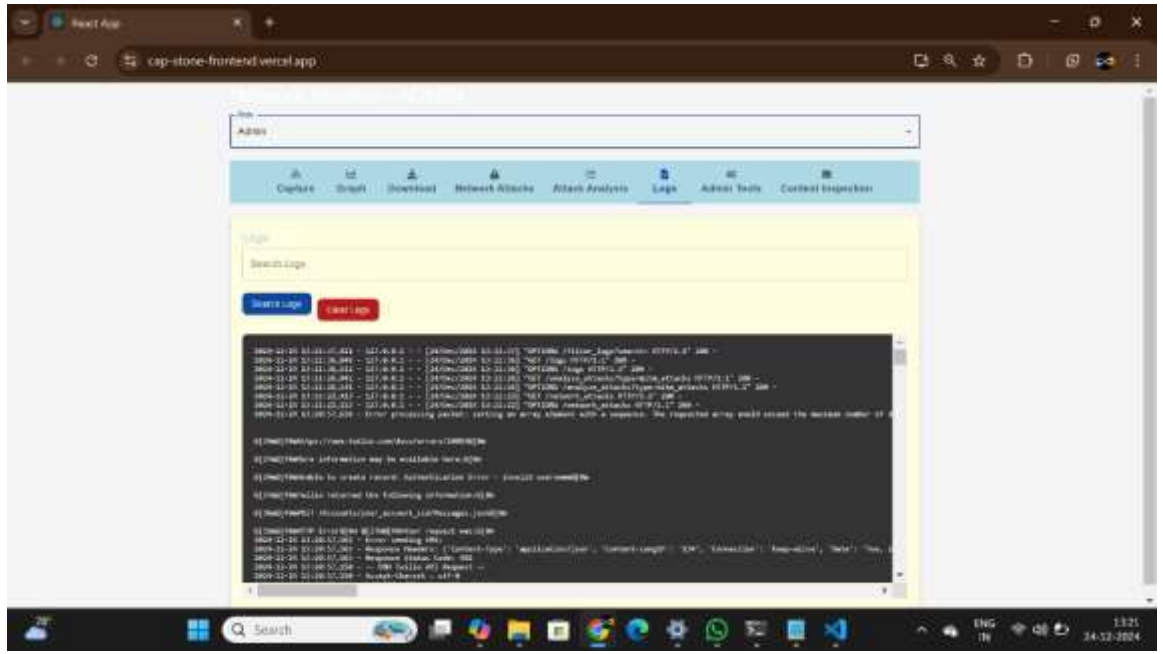
1.Python complier
2.command prompt
3.online tool(to deploy)

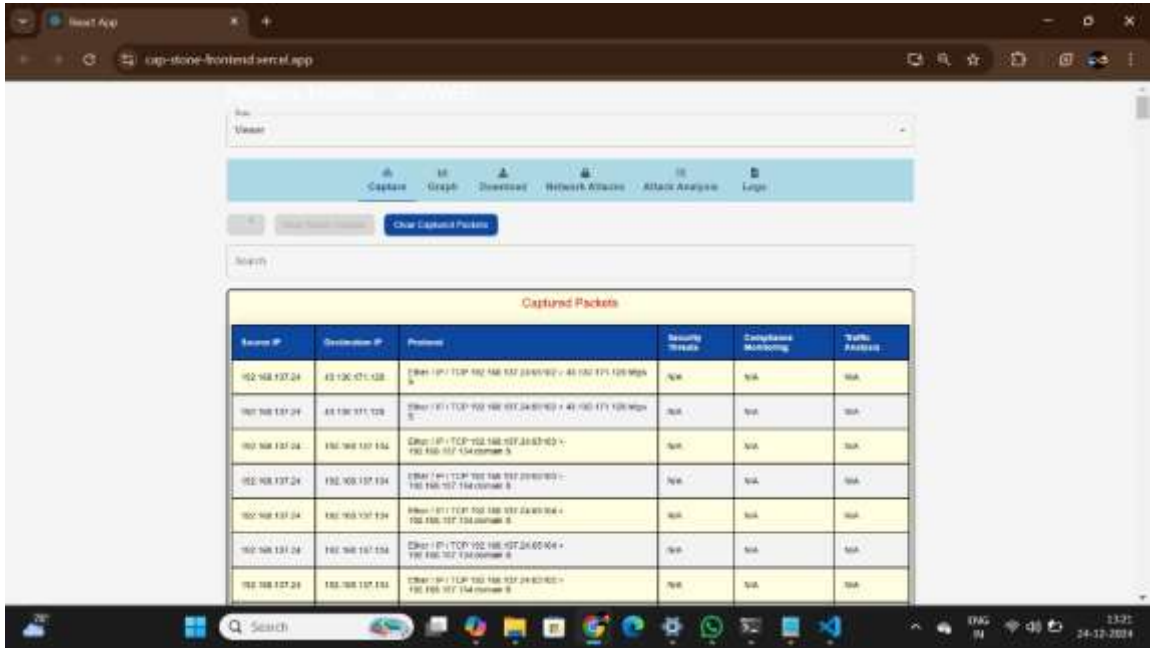
Screenshots



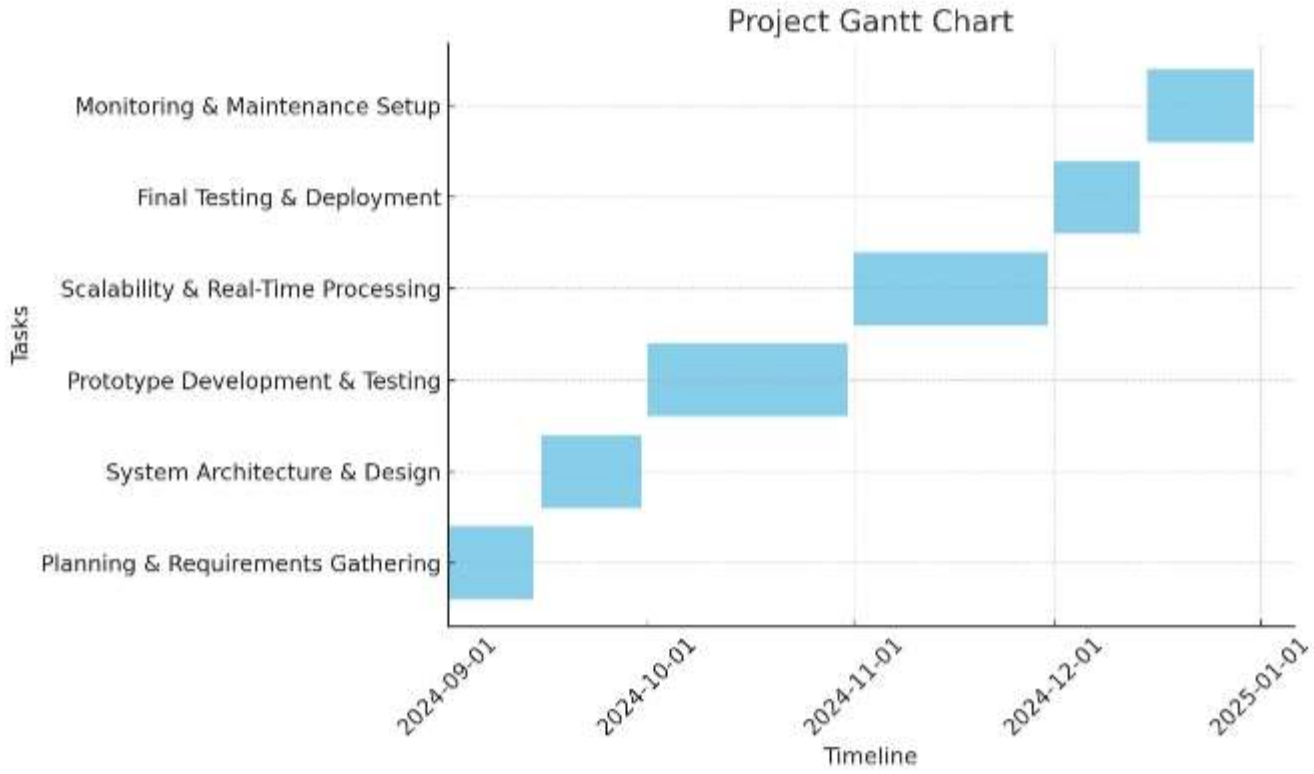


Screenshots





Timeline of Project



Expected Outcomes

- Capturing the real time network packets
- Identify and analysis the possible threat or attackers IP address and protocol
- Analysing the possible MIMA on the network or system
- Detected Suspicious IP address and protocol are captured into log files and for further analysis

Conclusion

- Advanced Network Intrusion Detection Systems (NIDS) with real-time protocol analysis and deep content inspection are vital for detecting Man-in-the-Middle (MITM) attacks.
- They identify anomalies in traffic, examine altered data streams, and inspect encrypted content for malicious changes.
- Though resource-intensive, these NIDS enhance network security by providing deeper insights and faster responses, making them crucial for protecting against sophisticated MITM threats.

Github Link

Github Link

https://github.com/geetha7019/Capstone_Project

References

- R. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems."
- W. Stallings, "Network Security Essentials: Applications and Standards."
- A. Moore et al., "Anomaly Detection for Network Security: A Survey."
- G. Vigna, "Intrusion Detection: A Machine Learning Perspective."
- P. Barford and V. Selinger, "Anomaly Detection in Network Traffic."
- M. S. Abusita and N. S. Al-Sharif, "A Survey on Intrusion Detection Systems," Journal of Cyber Security Technology, vol. 1, no. 4, pp. 307-330, 2017.
- Wireshark (2024). Wireshark User Guide. Wireshark Documentation
- OpenSSL (2024). OpenSSL User Guide. OpenSSL Documentation.
- Udemy (2024). Real-Time Network Traffic Analysis with Wireshark.
- Coursera (2024). Network Security & Database Systems. University of Maryland.
- Santos, I., & Silva, L. (2019). "Deep Packet Inspection for Intrusion Detection: A Survey." International Journal of Computer Science and Information Technology, 11(2), 77-90.
- Snort (2024). Snort: The World's Most Popular Open Source Intrusion Detection System. Snort Documentation

Project work mapping with SDG

The Project work carried out here is mapped to SDG-3 Good Health and Well-Being.

The project work carried here contributes to the well-being of the human society. This can be used for Analyzing and detecting blood cancer in the early stages so that the required medication can be started early to avoid further consequences which might result in mortality.

Thank You