Name : Aditya Prashant Nikam
Class: BE (AI & DS)
Roll no.: 31
Subject : Cyber Security

GROUP B (ASSIGNMNET NO.: 12)

Title:
Design and implement program/ use open source tool to analyze the packets in IoT environment

Problem Statement :
Design and implement program/ use open source tool to analyze the packets in IoT environment

Outcome:
The implemented program, utilizing open source packet analysis tools, successfully captures, monitors, and analyzes network packets within the IoT environment. It provides insights into network traffic patterns, device interactions, and potential anomalies. This data helps improve network performance, troubleshoot connectivity issues, and enhance security by detecting unusual or malicious packet behavior, ultimately contributing to the optimization and security of the IoT ecosystem.

Theory:

1. Introduction:

- Provide an overview of the assignment's objectives, which involve the analysis of network packets in IoT environments.
- Emphasize the importance of packet analysis for understanding and securing IoT networks.

2. IoT Network Complexity:

- Discuss the intricacies of IoT network environments, highlighting the challenges they present in terms of diversity, scale, and communication protocols.

3. Packet Analysis Tools:

- Introduce open source packet analysis tools, such as Wireshark and tcpdump, and explain their relevance for capturing and inspecting network packets.
- Discuss the capabilities and features of these tools.

4. Packet Analysis in IoT:

- Explain the significance of packet analysis in an IoT context, which includes monitoring device communication, diagnosing network issues, and identifying security threats.
- Discuss the types of information that can be extracted from network packets.

5. Designing the Packet Analysis Program:

- Describe the design principles of a custom program or script for packet analysis, including language selection (e.g., Python, C++, Java), data collection, and analysis methods.
- Outline the scope of the program (e.g., real-time monitoring, offline analysis).

6. Implementation of Packet Analysis:

- Provide code snippets, technical details, and configurations for implementing the program or using open source tools for packet analysis.
- Discuss the network interfaces and capture options.

7. Packet Capture and Storage:

- Explain how captured packets are stored and organized for analysis, covering file formats, databases, or storage options.
- Address data retention and privacy considerations.

8. Packet Analysis Techniques:

- Detail the techniques for analyzing captured packets, including filters, protocol decoding, traffic visualization, and pattern recognition.
- Discuss the application of these techniques to IoT use cases.

9. Testing and Validation:

- Describe the testing and validation procedures to ensure the program's or tool's accuracy and effectiveness in packet analysis.
- Discuss the handling of diverse IoT communication protocols.

10. Reporting and Visualization:

- Explain how analysis results are reported and visualized, emphasizing the importance of clear insights and actionable information.
- Discuss the integration with security information and event management (SIEM) systems.

Conclusion:

- Summarize the key takeaways from the assignment, highlighting the essential role of packet analysis in understanding, securing, and optimizing IoT environments.
- Emphasize the ongoing importance of network monitoring and analysis in IoT.