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

GROUP B (ASSIGNMNET NO.: 11)

Title:

Install and use open source tools to Identifying various types of attacks on IoT device. Analyze the risks associated with the attacks. Write a C++/Java/Python program to identify at least one such attack.

Problem Statement :

Install and use open source tools to Identifying various types of attacks on IoT device. Analyze the risks associated with the attacks. Write a C++/Java/Python program to identify at least one such attack.

Outcome:

Program Outcome:

The program successfully identifies at least one type of attack on an IoT device using open-source tools and C++/Java/Python programming. The program detects the specific attack based on predefined patterns or signatures, providing timely alerts to mitigate potential security breaches.

Theory:

1. Introduction:

- Provide an overview of the assignment's objectives, which include using open source tools to identify attacks on IoT devices, analyzing potential risks, and implementing a detection program.
- Highlight the importance of securing IoT devices in the face of evolving threats.

2. IoT Device Security Challenges:

- Discuss the unique challenges and vulnerabilities associated with IoT device security, such as resource constraints, diverse communication protocols, and remote deployment.

3. Open Source Security Tools:

- Introduce a selection of open source security tools that can be used to analyze IoT device security, such as Wireshark for network analysis and Snort for intrusion detection.
- Explain how these tools assist in identifying and analyzing various types of attacks.

4. Types of IoT Attacks:

- Enumerate common IoT attack types, including denial of service (DoS), Man-in-the-Middle (MitM), and unauthorized access.
- Explain the potential consequences of these attacks, such as data theft, device manipulation, and service disruption.

5. Risks and Impact Analysis:

- Analyze the risks associated with each attack type, considering their potential impact on IoT device functionality and data security.
- Discuss the financial, privacy, and safety implications of these risks.

6. Design and Implementation of Attack Detection:

- Describe the program's design, focusing on the chosen attack type (e.g., DoS) and the methods used for detection.
- Specify the programming language (C++, Java, or Python) to be used for the implementation.

7. Open Source Tool Utilization:

- Explain how open source tools can be employed to capture and analyze network traffic, which may be indicative of the attack being targeted.
- Discuss the setup and configuration of these tools for detection purposes.

8. Program Implementation:

- Provide code snippets and technical details for the development of the detection program.
- Address the program's logic, algorithm, and data analysis methods.

Conclusion:

- Summarize the key findings and insights gained from the assignment, emphasizing the critical role of open source tools and detection programs in IoT device security.
- Highlight the importance of continuous monitoring and vigilance in safeguarding IoT ecosystems.