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

GROUP B (ASSIGNMNET NO.: 05)

Title:

Design and implement program to detect and report invalid login attempts and malicious activities to embedded device.

Problem Statement:

Design and implement program to detect and report invalid login attempts and malicious activities to embedded device.

Outcome:

The program designed and implemented successfully monitors login attempts and detects invalid login activities on the embedded device. It reports suspicious activities, enhancing the device's security and providing timely alerts to administrators, ensuring the system's integrity and protection against potential threats.

Theory:

1. Introduction:

- Define the need for an intrusion detection system in embedded devices, emphasizing the growing importance of security.
- Explain the objectives of the assignment: to develop a program that monitors login attempts and identifies malicious activities.

2. Understanding Embedded Device Security:

- Discuss the unique challenges and constraints associated with security in embedded devices, including resource limitations and the need for real-time monitoring.

3. Types of Invalid Login Attempts and Malicious Activities:

- Describe common forms of invalid login attempts and malicious activities, such as brute force attacks, unauthorized access, and anomalous behavior.

4. Designing the Intrusion Detection Program:

- Explain the architecture and components of the intrusion detection system, including data collection, analysis, and response.
- Discuss the use of machine learning, rule-based systems, or other techniques for identifying suspicious behavior.

5. Data Collection and Monitoring:

- Detail the data sources and methods used to collect login and system activity data.
- Explain how the program continuously monitors and logs events.

6. Anomaly Detection:

- Describe the algorithms and methods employed for detecting anomalies in login attempts and system behavior.
- Discuss the importance of establishing a baseline for normal activity.

7. Reporting and Alerting:

- Explain the process of reporting and alerting when invalid login attempts or malicious activities are detected.
- Discuss the methods of notifying system administrators or taking automated actions.

8. Implementation on Embedded Device:

- Provide technical details of implementing the intrusion detection program on the embedded device.
- Address compatibility and resource utilization concerns.

9. Testing and Validation:

- Describe the testing procedures to ensure the program's accuracy and effectiveness.
- Discuss how the system responds to simulated intrusion attempts.

10. Case Studies and Use Cases:

- Present examples of how the intrusion detection system can be applied to specific embedded device scenarios, such as IoT devices or industrial controllers.

Conclusion:

- Summarize the key takeaways from the assignment, emphasizing the importance of proactive security measures in embedded devices.
- Highlight the value of the developed program in enhancing security.