**Anomaly based Intrusion Detection System using Machine Learning**

**Professional Interview Questions**

**General IDS Questions (Functionality, Usage, Importance, Risks, Challenges)**

1. Can you describe your general experience with managing or using intrusion detection systems in a professional cybersecurity environment?
2. How are IDS typically deployed in workplace networks to monitor and protect against cyber threats?
3. What role do IDS play in the overall cybersecurity strategy of an organization, and how important are they compared to other security tools?
4. What are the primary operational challenges you’ve encountered when using IDS in the workplace, particularly in dynamic or high-traffic networks?
5. In your experience, what are the most significant risks associated with relying on IDS for threat detection in professional settings?
6. How do false positive alerts from IDS impact security operations, and what strategies have you seen used to manage them effectively?
7. How do IDS integrate with other security systems, such as Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM), or Security Orchestration, Automation, and Response (SOAR) platforms, in your workplace experience?
8. What factors influence the choice between anomaly-based and signature-based IDS in workplace cybersecurity strategies?
9. How do organizations evaluate the effectiveness of IDS in the workplace, and what metrics or criteria are most valued?
10. What are your thoughts on the effectiveness of anomaly-based IDS for detecting modern threats, such as Denial of Service attacks, compared to traditional approaches?
11. In your experience, how suitable are older datasets like NSL-KDD for developing or evaluating IDS, compared to newer datasets like CICIDS-2017?