|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Title :** **Project Registration & Progress Review** | | **FF No. 180** |  |
|  | | | | | |
|  | | | | | |
| **Department: Computer Engineering** | | **Academic Year:2024-25** | | | |
| **Semester :II** | | **Group No. : TY 12** | | | |
| **Project Title:** **Network Intrusion Detection System** | | | | | |
| **Project Area: Network, Machine Learning** | | | | | |
| **Group Members Details:** | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sr. No. | Class & Div. | Roll No. | G.R.No. | Name of Student | Contact No. | Email ID |
| 1 | CS-A | 39 | 12210098 | Astha Chaudhari | 9284905269 | astha.chaudhari22@vit.edu |
| 2 | CS-A | 41 | 12210003 | Harshal Chaudhari | 9579766952 | harshal.chaudhari22@vit.edu |
| 3 | CS-A | 42 | 12210370 | Sanskar Chaudhari | 9002593004 | sanskar.chaudhari22@vit.edu |

|  |
| --- |
| Name of Internal Guide: Dr. Aarti Agarkar . Contact No : 9822903916  Email ID: aarti.agarkar@vit.edu |

|  |
| --- |
| Project approved / Not approved  **Guide Project Coordinator Head of Department** |

T

**FF No** **180**

**Introduction**

With the exponential growth of networks and digital infrastructure, the risk of cyberattacks and unauthorized access has also surged. A robust security mechanism to detect and prevent such threats is essential. A Network Intrusion Detection System (NIDS) combines both signature-based and anomaly-based techniques to identify known attack patterns and detect unusual or malicious activities in real-time. This project aims to develop a hybrid NIDS leveraging modern tools, machine learning algorithms, and deep packet inspection for comprehensive network security.

**Problem Statement**

Traditional intrusion detection systems (IDS) face challenges in adapting to new attack vectors and recognizing novel patterns of malicious activities. Signature-based systems are limited to predefined rules, failing to detect zero-day attacks, while anomaly-based systems often struggle with false positives. The lack of integration between these two approaches and the absence of efficient real-time analysis methods leave networks vulnerable to both sophisticated attacks and subtle intrusions. Therefore, there is a need for a hybrid intrusion detection system that combines the strengths of both approaches while minimizing their weaknesses.

**Objectives**

* Develop a hybrid IDS that integrates signature-based and anomaly-based detection mechanisms.
* Capture and analyze network traffic using tools like Wireshark, Tcpdump, and Scapy for data collection.
* Implement deep packet inspection (DPI) to extract payload features and detect packet-level anomalies.
* Train a machine learning model (e.g., Isolation Forest) for anomaly-based detection of unusual network behavior.
* Design custom detection rules for signature-based detection using tools like Snort or Suricata.
* Extract and select features such as packet size, source/destination ports, protocol type, flags, bytes sent/received, and authentication attempts for analysis.
* Optimize feature selection through dimensionality reduction techniques like PCA (Principal Component Analysis).
* Combine NetFlow metadata and system logs to provide comprehensive insights into network activities.
* Build a real-time monitoring dashboard to visualize detected intrusions and anomalies.

**Methodology**

1. **Data Collection**
   * Capture network traffic using packet capture tools: Wireshark, Tcpdump, Scapy.
   * Collect system logs and user authentication data.
   * Utilize NetFlow to gather metadata about network flows.
2. **Signature-Based Detection**
   * Develop custom detection rules for specific attack patterns (e.g., known malware signatures, brute force login attempts).
   * Use tools like Snort or Suricata for rule-based intrusion detection.

**FF No** **180**

1. **Anomaly-Based Detection**
   * Extract features like packet size, source/destination ports, protocol, flags, bytes sent/received, failed login attempts, etc.
   * Perform feature selection using PCA to reduce dimensionality and improve model performance.
   * Train a machine learning model (Isolation Forest) to detect anomalies in the data.
2. **Deep Packet Inspection (DPI)**
   * Extract packet payloads using Scapy.
   * Inspect payload content using Suricata rules for specific malicious patterns.
3. **Real-Time Intrusion Detection**
   * Develop a hybrid detection framework that combines the outputs of both signature-based and anomaly-based approaches.
   * Implement a real-time dashboard to visualize alerts and provide actionable insights into detected intrusions.
4. **Evaluation and Optimization**
   * Test the system using simulated network attacks and benign traffic scenarios.
   * Evaluate performance metrics such as detection rate, false positive rate, and system latency.

**Expected Outcome**

1. **Accurate Detection of Intrusions**
   * A robust hybrid IDS capable of identifying both known and unknown threats with high accuracy.
2. **Minimized False Positives**
   * A finely tuned anomaly detection model to reduce false alarms while ensuring sensitivity to unusual activities.
3. **Comprehensive Feature Analysis**
   * Insights into key network traffic patterns and payload content for effective threat identification.
4. **Real-Time Monitoring**
   * A real-time dashboard for network administrators to monitor, investigate, and respond to intrusions.
5. **Scalable and Modular Solution**
   * A flexible and extensible system that can adapt to evolving attack vectors and integrate with other security tools.

By addressing the limitations of existing IDS systems, this project will contribute to enhancing the cybersecurity landscape, making networks more resilient to a wide range of threats.

**FF No** **180**

|  |  |  |  |
| --- | --- | --- | --- |
| Group No. | **TY12** | | |
| Activity | Review Schedule | Progress Review Report submitted | Signature of Guide |
| Review 1 | Mid Sem. Semester | Yes / No |  |
| Review 2 | End of Semester | Yes / No |  |

Format of Progress Review Report:

|  |
| --- |
| **Review No.: 1 Group No.: TY12 Date:** |
| **Progress Review Report** |
| **Signature of Guide:** |

**FF No** **180**

|  |
| --- |
| **Review No.: 2 Group No.: TY12 Date:** |
| **Progress Review Report** |
| **Signature of Guide:** |