**Project Report Summary: Basic Intrusion Detection System (IDS)**

Objective

The project implements a lightweight Intrusion Detection System (IDS) using Scapy to capture and analyze network packets in real-time. The system detects suspicious activity based on predefined rules, such as known bad IPs, blocked ports, and potential port scans. Alerts are logged to a file and optionally displayed in the console for immediate visibility.

Brief Description

Core Components :

Packet Capture : Uses Scapy's sniff function to capture IP-based traffic on a specified network interface.

Rule Engine : Evaluates captured packets against a set of predefined rules to detect suspicious activity.

Logging : Logs alerts to a file and optionally prints them to the console for real-time monitoring.

Predefined Rules :

Known Bad IPs : Any traffic involving these IPs triggers an alert.

Blocked Ports : Access attempts to specific ports (e.g., Telnet-23, SMB-445, RDP-3389) trigger an alert.

Port Scan Detection : Detects potential port scans by tracking the number of distinct ports probed by a source IP within a specified time window.

Real-Time Alerts :

Alerts are generated when suspicious activity is detected and logged with timestamps for later analysis.

Command-Line Interface :

The script supports command-line arguments for specifying the network interface, rules file, and log file.

Fallback Mechanism :

If no rules file is provided, the system uses default rules to ensure functionality.

Outcomes

Detection of Suspicious Activity :

The system successfully identifies traffic involving known bad IPs, access attempts to blocked ports, and potential port scans.

Real-Time Monitoring :

Alerts are logged to a file and optionally displayed in the console, enabling real-time monitoring of network activity.

Scalability :

The modular design allows for easy extension of the rule engine to include additional detection mechanisms.

User-Friendly :

The script provides a simple command-line interface for configuration and operation.

Key Insights

Rule-Based Detection :

The use of predefined rules ensures that the system can detect common types of suspicious activity, such as port scans and access to blocked ports.

Port Scan Detection :

Tracking distinct ports probed by a source IP within a time window is an effective way to detect potential port scans.

Logging and Alerts :

Logging alerts with timestamps provides valuable information for post-incident analysis and forensic investigations.

Fallback Rules :

The inclusion of default rules ensures that the system remains functional even if no custom rules file is provided.

Conclusion

This project demonstrates a basic yet effective Intrusion Detection System (IDS) capable of detecting suspicious network activity in real-time. By leveraging Scapy for packet capture and a rule-based engine for evaluation, the system provides a foundation for building more advanced IDS solutions. Its modular design and support for real-time alerts make it suitable for both educational purposes and practical deployment in small-scale environments.