JGi JAIN ONLINE
DEEMED-TO-BE UNIVERSITY

Project Interim Report

Name	Shamanth.B
USN	221VMTR02324
Elective	Cyber Security
Date of Submission	21/05/2024

- **Objectives of the Study:**

- **To Develop an Effective IDS: The primary objective is to design and implement an IDS capable of detecting unauthorized activities or intrusions within a network or system.**

- **To Enhance Cybersecurity: The study aims to contribute to improving cybersecurity measures by developing a reliable system capable of identifying and mitigating potential threats.**

- **To Evaluate Detection Accuracy: Assess the accuracy and effectiveness of the IDS in identifying various types of intrusions, including known and unknown threats.**

- **To Optimize Resource Utilization: Investigate methods to optimize resource utilization, such as memory and processing power, to ensure that the IDS operates efficiently without compromising its detection capabilities.**

- **To Explore Real-time Detection Capabilities: Explore the feasibility of real-time intrusion detection, enabling timely responses to potential threats as they occur.**

- **To Investigate Adaptability and Scalability: Evaluate the adaptability and scalability of the IDS to different network environments and varying levels of network traffic.**

- **To Enhance False Positive Management: Develop strategies to minimize false positives, ensuring that legitimate network activities are not incorrectly flagged as intrusions.**

- **Scope of the Study:**

- **Types of Intrusions: Focus on common threats that home networks might face, such as unauthorized access attempts, malware infections, and unusual network traffic patterns indicative of attacks like port scanning or DoS attacks.**

- **Data Sources: Monitor network traffic data within the home network, including data from routers, switches, and connected devices. Additionally, analyze system logs from devices within the network, such as computers, smart phones, IoT devices, etc.**

- **Detection Techniques: Implement simple detection techniques suitable for home networks, such as signature-based detection for known threats and basic anomaly detection methods to identify unusual behavior.**

- **Deployment Environment: Deploy the IDS within the home network environment, typically as software running on a dedicated device like a Raspberry Pi or a network-attached computer. Considerations for the home network architecture and the number of devices connected should be taken into account.**

- **Performance Metrics: Assess the performance of the IDS based on metrics like detection rate, false positive rate, and resource utilization. Since the home network environment may have limited resources, efficiency is key.**

- **Integration with Existing Systems: Integrate the IDS with existing home network security measures, such as firewalls and antivirus software. Ensure compatibility with common home network setups and devices.**

- **Scalability and Flexibility: Design the IDS to be scalable to accommodate the growth of the home network and flexible enough to adapt to changes in network topology or connected devices.**

- **User-Friendly Interface: Consider providing a user-friendly interface for managing and monitoring the IDS, suitable for home users who may not have technical expertise in cybersecurity.**

- **Methodology:**

- **Requirements Gathering: Understand the specific security needs and constraints of the network environment. Identify the types of threats the IDS should detect and the devices and network segments it will monitor.**

- **Data Collection: Gather network traffic data and system logs from devices within the network. This may involve configuring devices to log relevant information and setting up packet capture tools to monitor network traffic.**

- **Preprocessing: Preprocess the collected data to extract relevant features and prepare it for analysis. This may include converting network traffic data into a usable format, filtering out noise and irrelevant information, and handling missing or incomplete data.**

- **Detection Algorithm Selection: Choose appropriate detection algorithms based on the types of intrusions targeted and the characteristics of the home network environment. For a basic IDS, simple algorithms like signature-based detection or basic anomaly detection may be sufficient.**

- **Implementation: Implement the selected detection algorithms using suitable programming languages and frameworks. This may involve developing custom software or leveraging existing IDS tools and libraries tailored for home network use.**

- **Testing and Evaluation: Evaluate the performance of the implemented IDS using test datasets or simulated attack scenarios. Measure key performance metrics such as detection rate, false positive rate, and response time to assess its effectiveness.**

- **Integration and Deployment: Integrate the IDS into the home network environment, ensuring compatibility with existing network infrastructure and security measures. Deploy the IDS on a dedicated device or network appliance, such as a Raspberry Pi or a home server.**

- **Monitoring and Maintenance: Continuously monitor the performance of the IDS in real-world use and perform regular maintenance tasks such as updating detection rules and algorithms, reviewing logs, and addressing any issues or false positives that arise.**

- **User Education and Awareness: Provide guidance and resources to home users on how to interpret and respond to IDS alerts effectively. Educate users on best practices for securing their home network and devices to complement the IDS's capabilities.**

➢ **Research Design :**

- **Research Objectives: Clearly define the objectives of the study, including the specific aims and goals of implementing the IDS for the home network.**

- **Data Collection Methods:**

◆ **Primary Data: Gather primary data by conducting Case studies with home network users to understand the security needs and challenges.**

◆ **Secondary Data: Collect secondary data from existing literature, research papers, and online resources related to home network security and IDS implementation.**

- **Experimental Design:**

◆ **Setup: Set up a test environment to simulate a home network with typical devices and network configurations.**

- ◆ **Implementation: Implement the basic IDS using selected detection techniques and algorithms.**
- ◆ **Testing: Conduct experiments to evaluate the performance of the IDS under various conditions, including different types of attacks and levels of network traffic.**

- **Data Analysis:**

- ◆ **Analyze the collected data to assess the effectiveness of the implemented IDS in detecting intrusions and mitigating security threats.**
- ◆ **Use appropriate statistical methods and metrics to measure performance, such as detection rate, false positive rate, and response time.**

- **Results Interpretation:**

- ◆ **Interpret the results of the experiments and data analysis to draw conclusions regarding the effectiveness and feasibility of the basic IDS for home networks.**
- ◆ **Discuss the implications of the findings in relation to the research objectives.**

- **Limitations and Future Research:**

- ◆ **Acknowledge any limitations of the study, such as constraints in data collection or experimental design.**
- ◆ **Suggest areas for future research to address unresolved questions or further investigate related topics.**

➢ **Data Collection Method**

- **Packet Capture and Analysis:**

Use packet sniffing tools like Wireshark or Snort to capture and analyze network traffic on network. This method helps identify abnormal traffic patterns, such as unusual port scans or malicious payloads.

- Router Logs Monitoring:

Access the logs of home router to monitor incoming and outgoing connections, DHCP leases, and firewall events. Router logs can provide valuable insights into unauthorized access attempts or suspicious activities.

- Endpoint Monitoring:

Installing host-based IDS software on computers and devices within home network. These tools monitor system logs, file changes, and network connections to detect potential intrusions or malware infections on individual devices.

- DNS Query Logging:

Enable DNS query logging on home router or DNS server to track domain name resolutions. Analyzing DNS logs can help identify communication with malicious domains or potential phishing attempts.

- Network Flow Analysis:

Use network flow analysis tools to monitor and analyze traffic patterns within home network. This method helps detect unusual spikes in traffic volume or unusual communication behaviors that may indicate a security threat.

- Intrusion Detection Alerts:

Configuring IDS to generate alerts for suspicious activities or known attack signatures. These alerts can be sent via email or notifications to alert potential security incidents in real-time.

- User Behavior Monitoring:

Monitors user activities and behaviors on network. Keep an eye out for unusual login attempts, access patterns, or changes in user behavior that may indicate compromised accounts or insider threats.

- **Data Analysis Tools:**

In order to effectively analyze and interpret the data collected by the Intrusion Detection System (IDS) deployed in the home network environment, a selection of powerful data analysis tools was carefully chosen. These tools are integral to the process of identifying, assessing, and responding to potential security threats within the network. The following data analysis tools were selected based on their reliability, functionality, and suitability for small-scale deployments:

- **Snort:**

Snort was chosen as the primary network intrusion detection system (NIDS) due to its reputation for real-time traffic analysis and extensive rule-based detection capabilities. It provides a robust framework for monitoring and detecting suspicious network activity.

- **Security Onion:**

Security Onion serves as the central platform for managing and analyzing data collected by the IDS. It integrates multiple open-source tools, including Snort, Elasticsearch, Logstash, and Kibana, into a unified solution for network security monitoring and threat detection.

- **Wireshark:**

Wireshark is utilized for detailed packet-level analysis and troubleshooting when necessary. While Security Onion provides packet capture and analysis capabilities, Wireshark offers additional flexibility for in-depth analysis of network traffic.