Network Traffic Analysis and Anomaly Detection Report

Introduction

This report outlines the methodology and findings of a network traffic analysis project aimed at identifying Distributed Denial of Service (DDoS) attacks. Utilizing Wireshark for packet capture and Snort for intrusion detection, this analysis focuses on monitoring traffic patterns, implementing rule-based detection, and analyzing alerts related to potential security threats.

Objectives

- To capture and analyze real-time network traffic.
- To identify potential DDoS attempts based on packet count thresholds.
- To implement alerting mechanisms using Snort for automated threat detection.
- To investigate alerts and cross-reference suspicious activities with known threat databases.

Methodology

Step 1: Setting Up Wireshark

1. **Installation**:
   - Wireshark was downloaded from the official website and installed on the monitoring system.
2. **Capture Configuration**:
   - The appropriate network interface was selected for packet capturing, and a capture was initiated to monitor all IP traffic.

Step 2: Packet Capture and Analysis

1. **Packet Capture**:
   - Network traffic was captured over a specified period to gather sufficient data for analysis.

2. **Traffic Analysis**:
   - Display filters were applied in Wireshark to focus on specific source IP addresses. The statistics feature was utilized to count packets sent from each source.
3. **Identifying DDoS Patterns**:
   - Anomalies were identified by observing packet counts, particularly looking for instances where a source IP sent more than 100 packets within a one-minute window.

Step 3: Implementing Alerting with Snort

1. **Snort Installation**:
   - Snort was installed and configured as a network intrusion detection system (NIDS).
2. **Rule Creation**:
   - A Snort rule was created to alert on more than 100 packets from the same source within a minute:
3. **Running Snort**:
   - Snort was initiated in packet capture mode to monitor the same interface as Wireshark, enabling real-time alert generation.

Step 4: Analyzing Alerts

1. **Alert Investigation**:
   - Upon receiving alerts from Snort, the corresponding packets were analyzed in Wireshark.
   - Specific source IPs and packet details were scrutinized to understand the nature of the detected threats.
2. **Cross-referencing Suspicious Activity**:
   - Suspicious source IPs were checked against threat intelligence databases like VirusTotal and Cisco Talos Intelligence to assess their reputation and historical behavior.

Findings

- Several instances of high packet counts from specific source IPs were recorded, indicating potential DDoS attempts.

- Alerts triggered by Snort matched the identified patterns in Wireshark, confirming the effectiveness of the rule-based detection.
- Cross-referencing revealed that some suspicious IPs had a history of malicious activity.

Recommendations

- **Continuous Monitoring**: Establish a routine for monitoring network traffic and Snort alerts to ensure timely detection of anomalies.
- **Rule Updates**: Regularly review and update Snort rules to adapt to evolving network conditions and emerging threats.
- **Network Hardening**: Implement additional security measures, such as rate limiting and firewalls, to mitigate the impact of potential DDoS attacks.

Conclusion

The integration of Wireshark for packet capture and Snort for intrusion detection has proven effective in identifying and analyzing potential DDoS attempts. This approach enables timely detection of network anomalies, providing a robust framework for enhancing network security.