Liam Calder V00963268
CSC 466
February 7 2025

Lightweight DDoS Alarm System:
Comparative Analysis of Detection Methods for Home Networks

Problem Statement:
DoS attacks are a growing threat that can seriously disrupt network operations, especially resource-constrained home networks. While robust Intrusion Detection Systems (IDS) like Snort, Suricata, and Fail2Ban exist, they're generally too heavy and complex for small-scale deployments. I want to develop a simple, real-time alarm system that quickly detects common DoS attacks (e.g., TCP SYN Floods and UDP Floods) while using minimal system resources.

Motivation & Background:
Most IDS systems focus on enterprise-level networks, leaving home users with fewer lightweight options. My interest in cybersecurity and protecting my home network has driven me to want to build my own DDoS alarm explore and compare different detection techniques. In this project, I plan to analyze two approaches: threshold-based heuristics and a basic anomaly detection model (using methods like clustering, autoencoders, or other techniques I may discover). In short, I aim to learn and understand the trade-offs between speed, accuracy, and resource usage in developing my IDS.

Proposed Approach:
I'll build a modular DoS alarm system that lets me switch between two detection methods:

- Threshold-Based Heuristics: Monitoring for signs like excessive SYN packets or sudden bandwidth spikes.
- Anomaly Detection: Using a basic model to flag deviations from normal traffic patterns.

I'll simulate DoS attacks on my home network and log key performance metrics, such as false positives, false negatives, detection time, and resource overhead. I'll use these to compare the two methods and determine their strengths and weaknesses.

Proposed Deliverables:

- A functional DoS alarm system that can switch between detection methods.
- A set of experiments comparing the performance of threshold-based and anomaly detection approaches.
- Complete documentation (including installation instructions, usage guidelines, and a detailed analysis report).
- A public Git repository hosting all the project code.
- Final presentation video and a report summarizing the methodology, experimental results, and conclusions.

Proposed Deliverables Schedule:

- Feb 7: Submit Proposal and Git
- Feb 7 – 21: Research DoS detection methods, design the system architecture, and start coding the threshold-based module.
- Feb 21 (First Update): Present initial design, literature review findings, and progress on the threshold-based module.
- Feb 21 – Mar 7: Develop the anomaly detection module, set up DoS attack simulations, and integrate basic real-time alerting and logging.
- Mar 7 (Midterm Update): Demonstrate working prototypes of both detection methods and share preliminary experimental data.
- Mar 7 – 21: Optimize and integrate both modules into one system, enhance alerting (e.g., via console or email), and start comprehensive testing.
- Mar 21 (Third Update): Present updated performance results and optimizations.
- Mar 21 – Apr 4: Run final experiments, prepare complete documentation, and create final presentation slides.
- Apr 4 (Final Presentation): Demonstrate the fully integrated DoS alarm system and present the comparative analysis.
- Apr 11 (Final Report): Submit the final report with all documentation.

Resources Needed:
I already have my public GitHub repository set up. The remaining resources include my home network, an IDE, and access to relevant research papers.

Website:
https://github.com/dromech/ddos_alarm

References:
https://www.sciencedirect.com/science/article/pii/S2772671124001256?via%3Dihub#refdata001

https://ieeexplore.ieee.org/document/10486696/authors#authors