Snort IDS - Final Project Report

Submitted by: Mohamed Nabil Abdul Rahiman Date: July 27, 2025

**Executive Summary**

After four weeks of structured learning and practical implementation, I have successfully completed my Snort-based Intrusion Detection System (IDS) project. The project encompassed the full lifecycle of IDS development, from rule creation to alert tuning and performance optimization.

Custom Snort Rules Developed:

* ICMP Detection - Triggers on any incoming ICMP (ping) packets
* Web Admin Page Access Detection - Identifies HTTP GET requests targeting /admin
* TCP Port Scan Detection - Flags sequential TCP SYN packets indicative of port scanning
* Flood Detection Rules - Covers HTTP, TCP, and UDP flood attempts
* SSH Brute-Force Detection - Detects repeated SSH login attempts

Each rule was assigned a unique SID, thoroughly tested, and fine-tuned for accuracy and efficiency.

Simulated Attacks:

* TCP SYN port scans using Nmap
* SSH brute-force attacks using Hydra
* HTTP and UDP flooding techniques

Snort successfully detected these simulated threats, and alerts were verified for accuracy.

False Positive Mitigation:

* Refined content matching
* IP/Port range adjustments
* Alert suppression rules

Outcomes:

* Deep understanding of Snort rules and syntax
* Skills in detection tuning and alert optimization
* Experience in real-time traffic monitoring and attack simulation

**Week 1: Snort Setup and Rule Creation**

* Installed Linux environment (Kali)
* Installed Snort via package manager
* Verified installation and setup

Snort Rules Developed:

alert icmp any any -> any any (msg:"ICMP Packet Detected"; sid:1000001; rev:1;)

alert udp any any -> any 53 (msg:"Suspicious DNS query for badsite.com"; content:"badsite.com"; nocase; sid:1000002; rev:1;)

alert tcp any any -> any 21 (msg:"FTP login attempt detected"; flow:to\_server,established; content:"USER "; nocase; sid:1000003; rev:1;)

Rules were integrated into /etc/snort/rules/local.rules and snort.conf was updated accordingly.

**Week 2: Attack Simulation and Detection**

Simulated Attacks:

* TCP Port Scan using Nmap: nmap -sS [target IP]
* SSH Brute Force using Hydra: hydra -l root -P passwords.txt ssh://[target IP]

Verification:

* Snort triggered alerts for each simulated scenario
* Alerts were verified in the log format:

[1:1000001:1] "ICMP Packet Detected" {ICMP} source\_ip -> dest\_ip

Snort was executed in detection mode:

sudo snort -c /etc/snort/snort.lua -i eth0 -A alert\_fast

**Week 3: Alert Analysis and Optimization**

False Positives Identified:

* DNS queries to trusted sites
* Legitimate FTP logins

Suppression Methods:

* Edited threshold.conf to suppress repeated noisy alerts
* Narrowed detection rules to specific IPs and content patterns

Tuning:

* Revisions in rule logic
* Improved protocol and port filtering
* Removed overly broad matches to reduce noise

**Week 4: Finalization and Review**

Summary of Key Learnings:

* Successfully created and managed a functioning IDS environment
* Practiced rule creation, traffic simulation, and alert analysis
* Mastered core Snort configuration techniques
* Developed critical skills in log analysis, suppression tuning, and performance optimization

The project is a comprehensive application of NIDS principles using Snort, with practical experimentation and successful deployment of a mini-IDS.

Mohamed Nabil Abdul Rahiman