

Real-time Network Intrusion Detection: A Research Study of Intrusion Detection Systems Within Organisational Networks

Joseph Ross - BSc Computing (Computer Networks & Cybersecurity)

Email: 1702760@student.uwtsd.ac.uk

1. Introduction

This project investigates the effectiveness of signature-based network intrusion detection systems, a frontline defence against common cyber threats. The study emphasises how such a system may be particularly beneficial to an organisation's security architecture, and establishes where an intrusion detection system will fit into an integrated network. To evaluate the efficiency of this system, Snort IDS is configured with a set of custom rules and tested against 9 active threat vectors.

2. Aim

To investigate the effectiveness of signature-based NIDS integrations using active threat simulation tools.

3. Objectives

The project followed 6 objectives:

- Carry out investigative research that underpins the fundamentals of NIDS integrations.
- Critically evaluate how organisations may benefit from intrusion detection systems.
- Design a network simulation that represents a realistic example of a working NIDS implementation using VirtualBox and Snort IDS.
- Set up an internal network threat using a Linux virtual machine that hosts Legion penetration testing software and other threat simulation tools.
- Launch various attacks against the simulated network, gradually tweaking the IDS rules to increase effectiveness.
- Analyse and evaluate the findings of the practical implementation.

4. Research

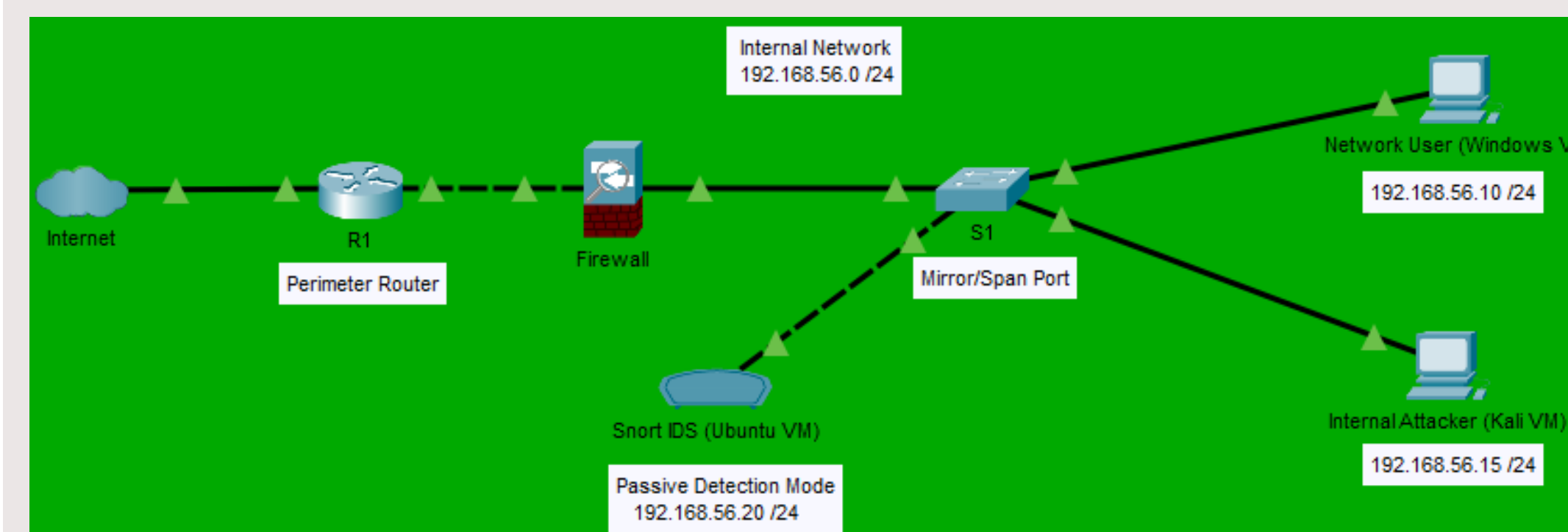
Within the literature review are presented some of the projects key qualitative findings. These include:

- Targeted attacks pose the greatest threat, but common network attacks are the focus of defence and detection.
- Internal threats are the most damaging to organisations.
- Hybrid NIDS solutions are being heavily researched.
- Signature-based IDSs are still the most popular choice, but benefit greatly from anomaly-based detection features.

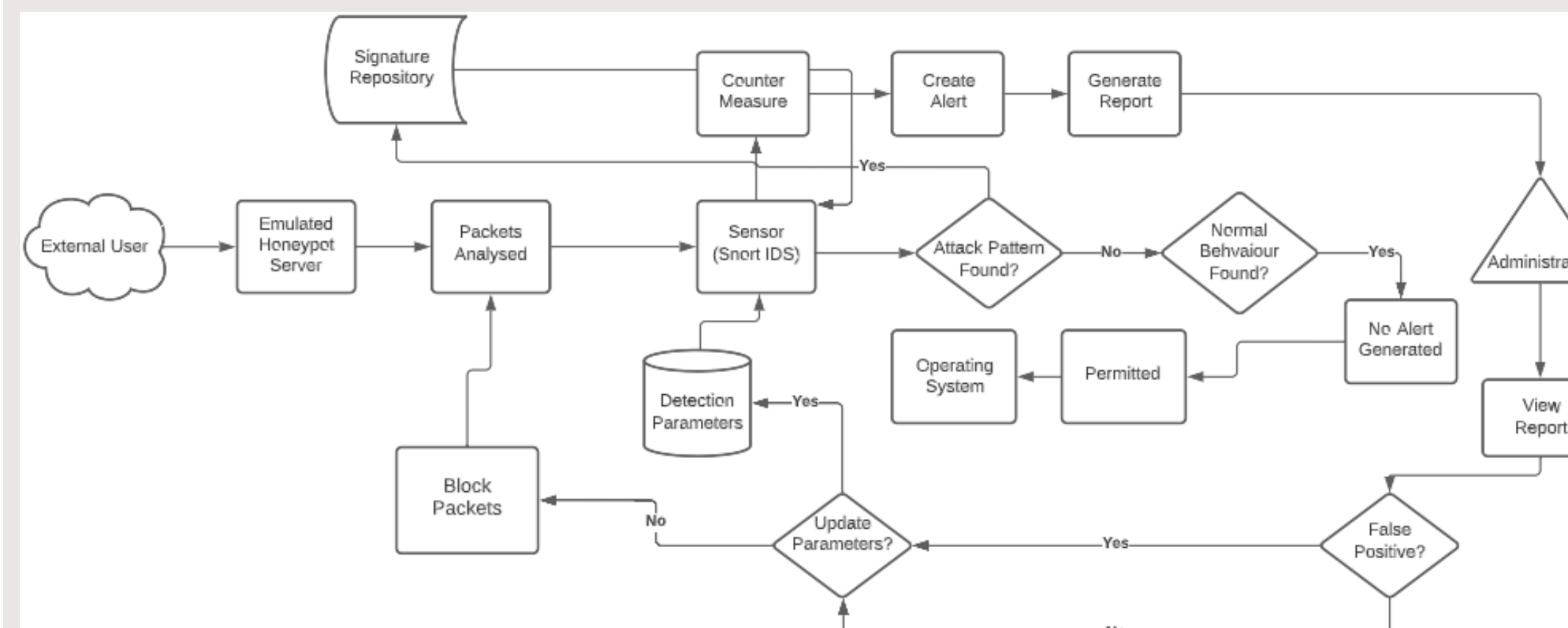
5. Design & Implementation

The project design uses 3 virtual machines connected through host-only adapters, with an additional NAT adapter. Snort IDS is hosted in in-line mode on a Ubuntu VM to receive all network traffic. The attacking machine hosts a Kali Linux user, which acts as an internal attacker targeting a network-connected Windows 10 VM.

Network topology:

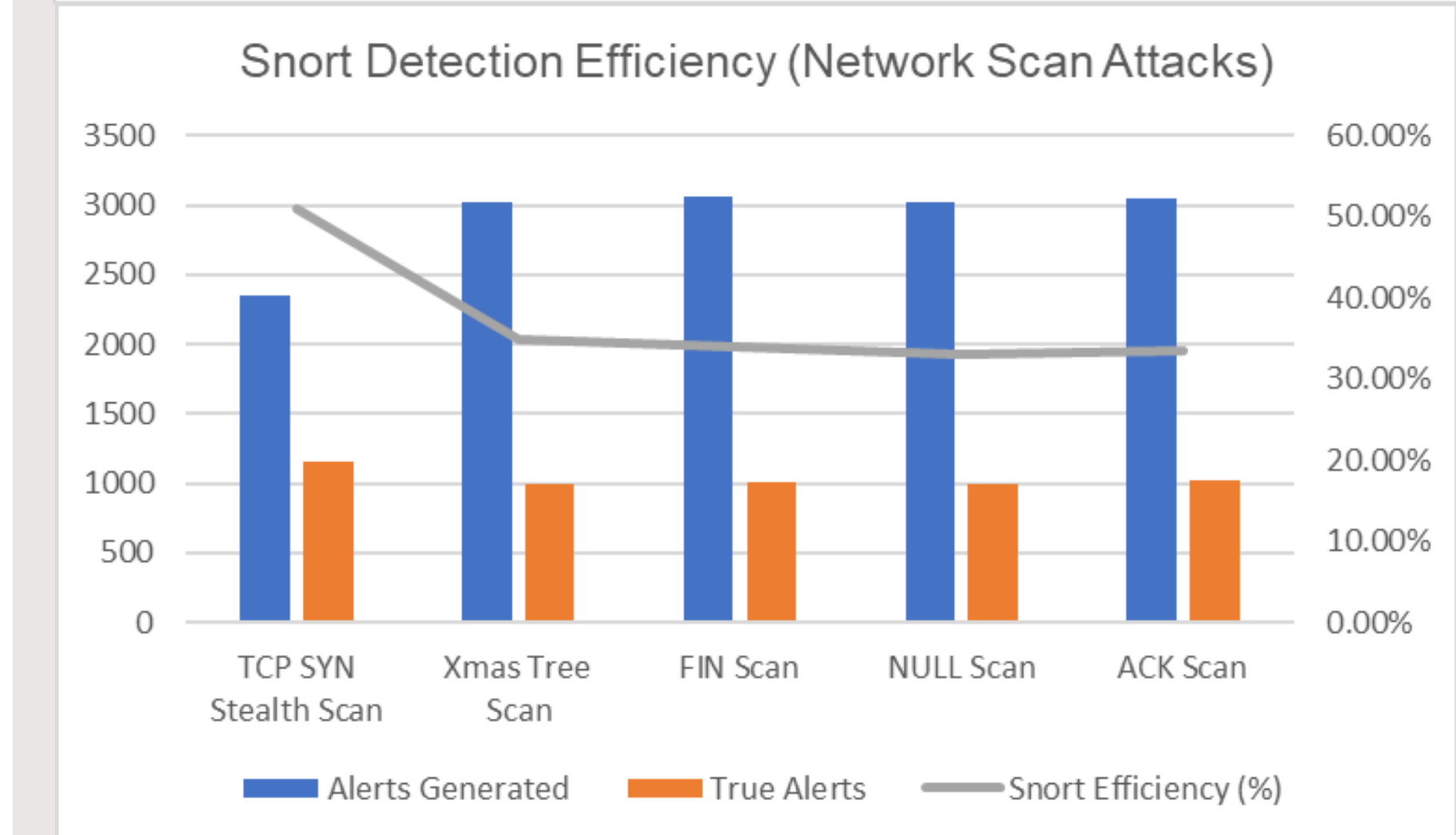
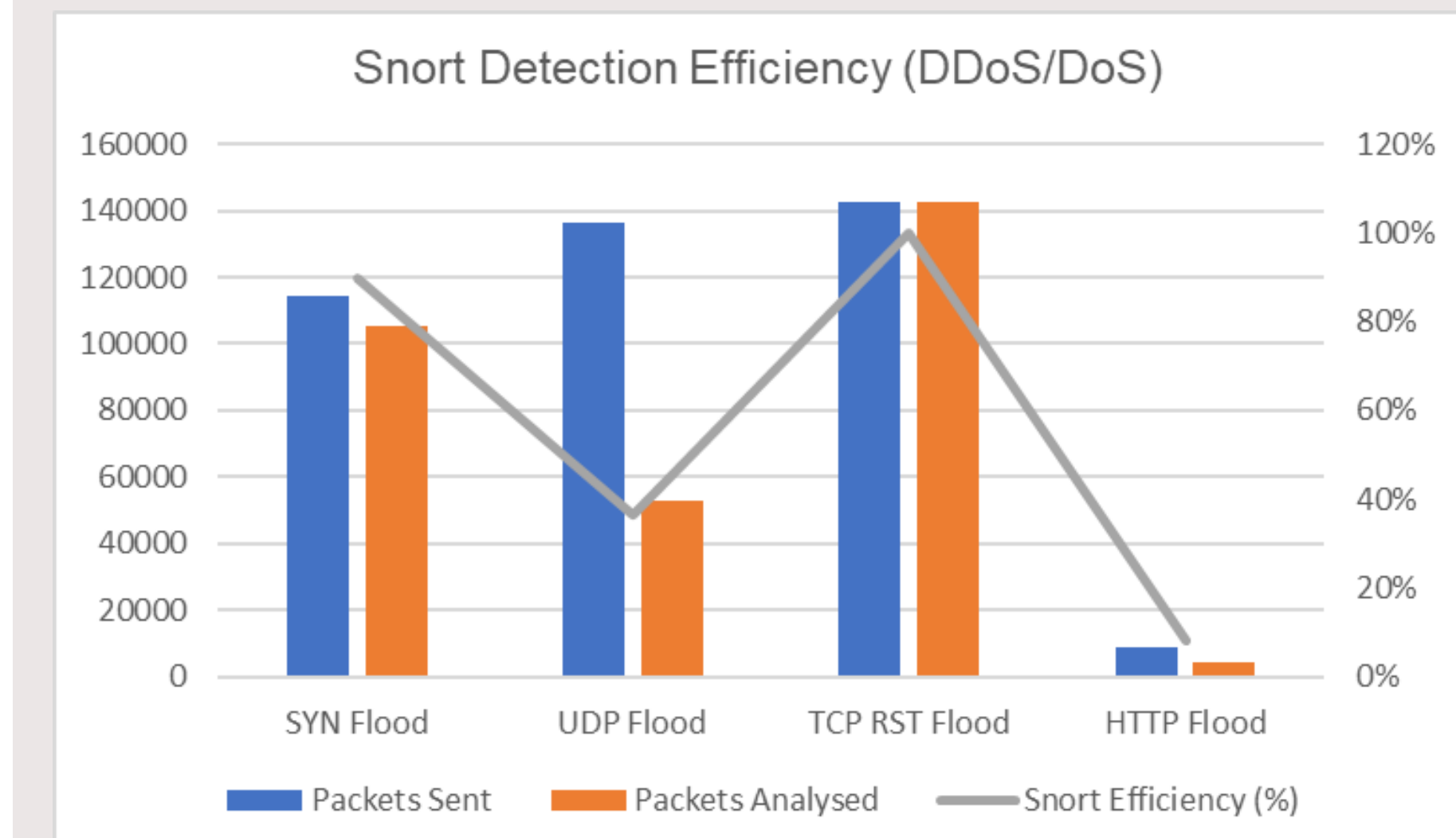


Signature detection process:



6. Results

An experiment was conducted to test Snort's detection efficiency. To do this, 4 DDoS/DoS and 5 network enumeration attacks were launched from the attacker VM toward the victim VM using the internal network. The results of the testing stage are shown below.



7. Conclusion

Although the outcome of the project was successful, the results of the final analysis were surprising as the Snort efficiency rate was lower than expected. It is however understood that this was due to the enabling of some generic detection rules in the configuration. The aim of the project was met and all objectives completed to a satisfactory manner.