National College of Ireland

Configuration Manual

MSc Research Project
Cybersecurity

Karthic Krishna Srekant
Student ID: X22165291

School of Computing
National College of Ireland

Supervisor: Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Karthic Krishna Srekant
Student ID:	x22165291
Programme:	MSc Cybersecurity **Year:** .....1.....
Module:	MSc Research Project
Lecturer:	30/01/2024
Submission Due Date:	
Project Title:	**AN INDEPTH EXPLORATION OF NETWORK FIREWALL PERFORMANCE, MONITORING EFFICACY AND SECURITY**
Word Count:	..... **Page Count:** .....4.....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: .....Karthic Krishna Srekant.....

Date: .....30/01/2024.....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only

Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Karthic Krishna Srekant
Student ID:x22165291

1 Requirements

- Wireshark installed
- Snort installed
- Server to act as firewall
- Network environment

2 Configuration Setup

Wire shark installation

- Download latest version of Wireshark from official website
- Complete the installation as per commands
- Ensure that it is configured to capture traffic on particular network interface.

Snort Installation

- Download latest version of snort from official website
- Complete the installation as per commands
- Ensure that it is configured as per specific requiring of network

Network Topology setup

- Firewall server with network interface
- Configure IP address and subnet masks

Wire shark configuration

- Open Wireshark and select the appropriate network interface for testing
- Capture filters to focus the traffic type for analysis
- Set display filters for packet analysis of efficiency
- Use of different statistical analysis features

Snort Configuration

- Edit snort and set its configuration to defiedn network variables and preprocessors
- Configure rules based on policies and threats to monitor
- Set output plugin to log snort alerts and events

Testing and exploration

- To evaluate the functionality and threat detection capabilities of the firewall, introduce simulated network traffic.
- Keep updated on Snort alerts for detected security events and Wireshark for in-depth packet analysis.
- Based on the observed outcomes, modify Snort setups and firewall rules.

References

Snort (2023) *Snort setup guides for emerging threats prevention*. Available at: https://www.snort.org/documents (Accessed: 10 December 2023).

Wireshark (2023) *Wireshark user's guide*. Available at: https://www.wireshark.org/docs/wsug_html_chunked/ (Accessed: 10 December 2023).