Configuration Manual

MSc Research Project
Masters in Cybersecurity

Forename Sri Sairam S
Student ID: x21144761

School of Computing
National College of Ireland

Supervisor: Noel Cosgrave

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Sri Sairam S	
Student ID:	X21144761	
Programme:	Masters in cybersecurity	**Year:**2022-2023
Module:	Thesis	
Lecturer:	09/08/2023	
Submission Due Date:	14/08/2023	
Project Title:	Detection of man in the middle attack on fog layer using Intrusion Detection Systems	
Word Count: 1022	**Page Count: 7**	

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: Sri Sairam S

Date: 13/08/2023

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

Sri Sairam S
X21144761

1 Introduction

This document provides a comprehensive overview of the appropriate implementation and execution of the man in the middle (MITM) attack detection with Intrusion Detection Systems (IDS). The experiment was conducted by utilizing a network simulator and a manually generated dataset. The following approach was employed to assess the effectiveness of the Intrusion Detection System (IDS).

2 System requirements

The study is carried out on an Oracle VM Virtual Box virtualization and GNS3 network simulator and Two VMs kali Linux and Ubuntu (IDS)

Host machine specification

Table 1: Host machine specification

Component	Specification
Processor	AMD Ryzan 4000 series
CPU Cores	6
Clock Speed	3.00 GHz
Memory (RAM)	16 GB
RAM Type	DDR4
Storage	239GB SSD
Operating system	Windows 11
Network interface	Wireless
Virtualization	Enabled

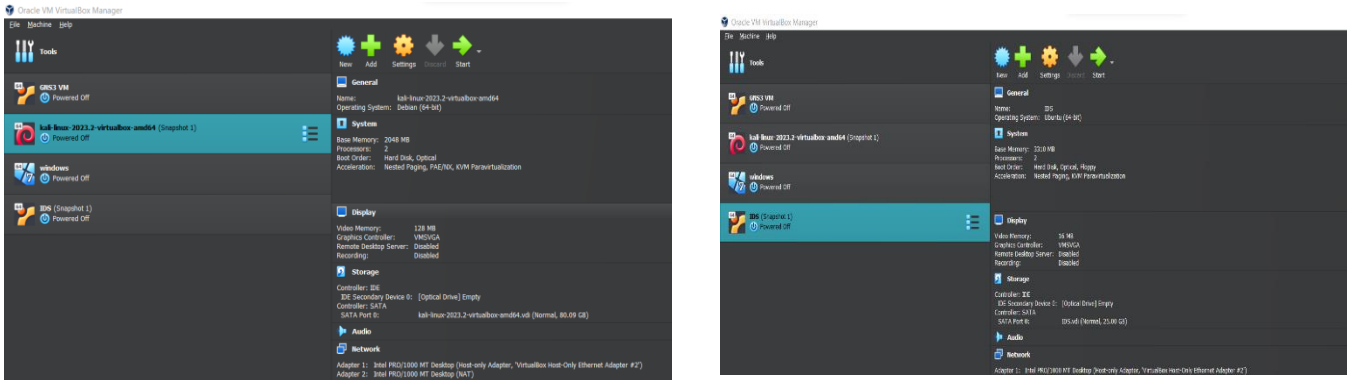

Figure 2: Virtualization setup

3 Tools

Tools used:

GNS3 – The GNS3 tool was utilized in order to mimic the network topology for the project. I had the opportunity to experiment with various setups, settings, and network adapters within the virtual machine environment.

Snort- The Intrusion Detection System (IDS) tool utilized in the project for the purpose of detecting Man-in-the-Middle (MITM) attacks within the fog layer was Snort. The Snort software package is equipped with a set of preconfigured rules, but, for the purposes of our project, we have authored a collection of rules that are stored in the local.rules file.

NMAP –Used this tool to collect data pertaining the devices and services present within a network. Additionally, the task involves the identification of open ports and susceptible services.

SCAPY – This software enables users to create and transmit personalized network packets, capture, and analyse network traffic, and execute diverse network-related functions.

ETTERCAP – used to Launch ARP spoofing attack, ICMP redirect host attack.

Wireshark – To monitor network.

Oracle VM box – used to create virtual machines like kali, ubuntu, IDS.

4 Download and Installation

Snort IDS installation in ubuntu:

Sudo apt update
Sudo apt install snort

GNS3 – Installed from GNS3.org official site.

Download oracle VM box from official site

Ettercap, Wireshark, Nmap – Default kali Linux tools

Scapy installation:
Sudo apt install scapy
Verify installation
from scapy.all import*

if the import statement runs without any errors, then scapy is installed successfully.

5 Configuration and Execution

1. GNS3 Network Topology:

Simulated the network with GNS3 to create a environment for fog layer

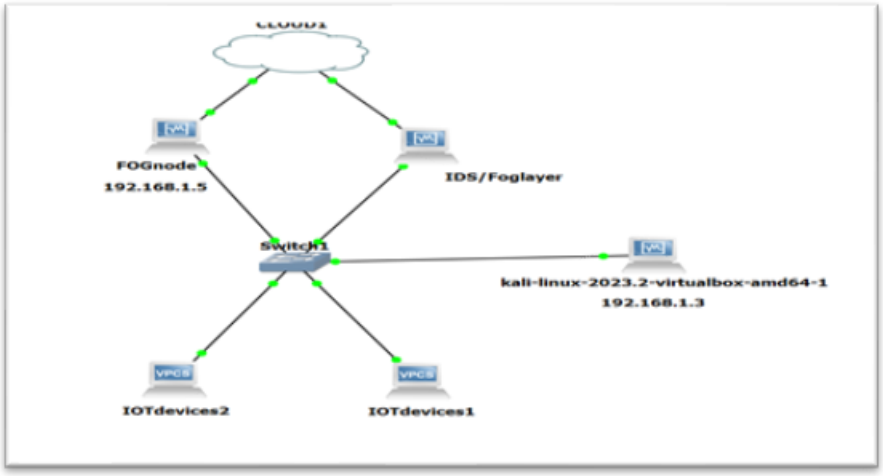

Figure 1: GNS3 network simulation

2. Oracle VM Box

There are two machines. The implementation of Kali Linux and Ubuntu for Intrusion Detection Systems (IDS) has been carried out in this approach. The virtual machines have been configured with a Host-only adaptor, enabling communication between them.

3. Snort Configuration

Configure the Snort Intrusion Detection System (IDS) to utilize the network interface of the host-only network as its listening port and Configure the Snort to record events and alarms, directing them to a designated file for subsequent analysis.

Creating MITM Detection Rule:

Created a customized Snort rule to recognize ARP communications with mismatched MAC addresses for a particular IP address.

alert udp any 67 -> any any (msg:"Possible MITM Attack"; content:"|00 02|"; content:"|00 01 08 00|"; content:"|06|"; content:"|04|"; content:"|00 02|"; content:"|00 01 08 00|"; content:"|06|"; content:"|04|"; sid:1000002; rev:1;)

alert tcp any any -> any any (msg:"Possible MITM Attack"; content:"HTTP/1.1 200 OK"; flow:to_client,established; sid:1000001; rev:1;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Possible MITM ATTACK"; dsize:0; itype:8; reference:arachnids,162; classtype:attempted-recon; sid:469; rev:3;)

Created a customized Snort rule to recognize ICMP redirect host attack.

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect host"; icode:1; itype:5; reference:arachnids,135; reference:cve,1999-0265; classtype:bad-unknown; sid:472; rev:4;)

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect net"; icode:0; itype:5; reference:arachnids,199; reference:cve,1999-0265; classtype:bad-unknown; sid:473; rev:4;)

Created a customized snort rule to recognize DHCP spoofing attack.

alert ip any any -> any any (msg:"DHCP Spoofing identified"; sameip; reference:bugtraq,2666; reference:cve,1999-0016; reference:url,www.cert.org/advisories/CA-1997-28.html; classtype:bad-unknown; sid:527; rev:8;)

alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"DHCP spoofing identified"; fragbits:R; classtype:misc-activity; sid:523; rev:5;)

Start the snort IDS in Fog layer (Ubuntu)

snort -A console -q -c /etc/snort/snort.conf -i enp0s3

4. **Generate MITM attack from Kali Linux.**

Attack 1

ICMP redirect attack with scapy

```
from scapy.all import IP, ICMP
from scapy.sendrecv import send
ip = IP()
ip.src = '192.168.1.1'
ip.dst = '192.168.1.6'
print(ip.show())  # Display IP packet information

icmp = ICMP()
icmp.type = 5
icmp.code = 1
icmp.gw = '192.168.1.3'
print(icmp.show())  # Display ICMP packet information

ip2 = IP()
ip2.src = '192.168.1.6'
ip2.dst = '10.1.1.1'
print(ip2.show())  # Display IP packet information

packet = ip/icmp

send(packet)
```

Attack 2

ARP spoofing

Using Ettercap,

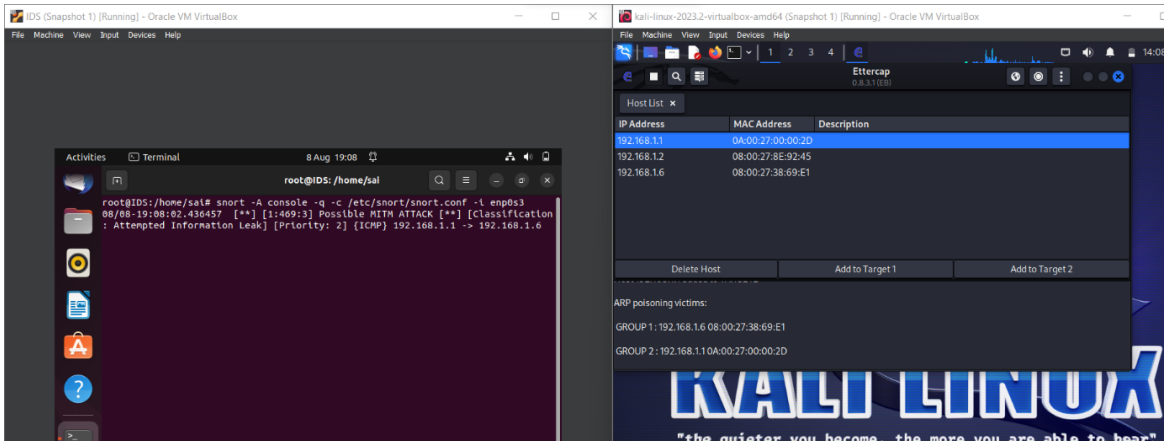

Figure 2: ARP spoofing attack in Ettercap

Attack 3

DHCP spoofing,