National College of Ireland

Detecting and Analysis of DDoS Attack using a Collaborative Network Monitoring Stack

MSc Research Project
Cybersecurity

Muhammad Aashiq Moosa
Student ID: 21186995

School of Computing
National College of Ireland

Supervisor: Apurva Kiran Vangujar

National College of Ireland
Project Submission Sheet
School of Computing

National College of Ireland

Student Name:	Muhammad Aashiq Moosa
Student ID:	x21186995
Programme:	Cybersecurity
Year:	2023
Module:	MSc Research Project
Supervisor:	Apurva Kiran Vangujar
Submission Due Date:	14/11/2023
Project Title:	Detecting and Analysis of DDoS Attack using a Collaborative Network Monitoring Stack
Word Count:	4930
Page Count:	14

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Muhammad Aashiq Moosa
Date:	16th September 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

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

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

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Detecting and Analysis of DDoS Attack using a Collaborative Network Monitoring Stack

Muhammad Aashiq Moosa
x21186995

Abstract

In recent years, distributed denial of service (DDoS) assaults have become more common and have developed as a common means of targeting entities. These assaults can be used to make money or to harm an organization's network and systems. Much of the recent research in this area has been on using various machine learning approaches to recognize and thwart these attacks. Even while these techniques frequently have excellent accuracy rates, they sometimes struggle to detect zero-day vulnerabilities or handle heavy network traffic. This research moves its emphasis from DDoS detection to the development of a cost-effective network monitoring stack. The intended solution will deliver real-time insights into a simulated network environment while also incorporating a machine learning engine for improved DDoS detection. This initiative aims to provide organizations with a comprehensive, cost-effective solution that goes beyond DDoS mitigation by emphasizing a more economical and effective monitoring system.

1 Introduction

DDoS is a cyber attack aimed to prevent authorized users from accessing specified services by overloading system resources, network capacity, or other critical components. This type of attack can affect a wide range of network components, including servers, databases, end-user devices, cloud platforms, and others. DDoS assaults can be difficult to distinguish since malicious traffic sometimes mimics normal user activity. DDoS assaults pose a significant danger to service accessibility because their goal is to disrupt legitimate user interactions with servers. These onslaughts may appear as severe traffic surges in a short period of time, extended low traffic, or sustained high traffic Zhang et al. (2017).

According to the figure 1, DDoS attacks increased by 74% in 2022 compared to the previous year. Fintech was especially vulnerable, accounting for 34% of these instances. Furthermore, such attacks have increased twelve fold in financial services Magazine (2023).

DDoS attacks are regarded as one of the most dangerous online threats by Norton. These assaults can occur unexpectedly, affecting any aspect of a website's functionality or assets, resulting in substantial downtime and significant financial losses. DDoS assaults became more common in 2022 than in previous years. There was an increase in both the

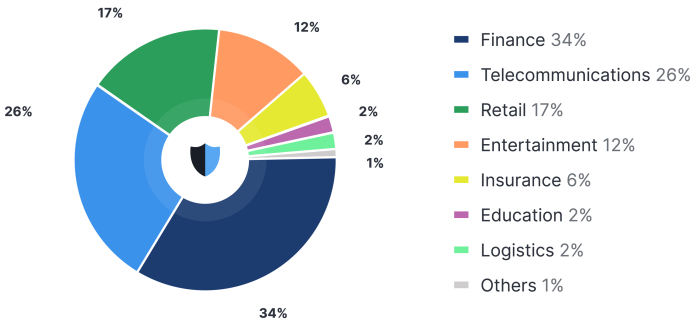

Figure 1: Industries Hit by DDoS Attacks.

number and duration of attacks. For example, in the second quarter of 2021, a typical DDoS attack lasted approximately 30 minutesCook (2023).

DDoS attacks pose a significant risk to networks and businesses. It has the potential to dramatically interrupt business operations and services, resulting in financial loss. The rise of DDoS attacks demonstrates that they are extensively used by attackers for a variety of reasons. There is an urgent need for a low-cost solution or technique for detecting these types of attacks in real time.

Monitoring a network is critical for network management operations and is used for a range of important tasks. A crucial role of network monitoring is the early detection of trends and patterns in network traffic and devices. These observations enable network operators to comprehend the current state of a network and then adjust it in order to improve the observed state Lee et al. (2014).

The proposed idea for this topic's research is to build a collaborative network monitoring solution that monitors and identifies DDoS attacks on a real-time network. The solution will provide an overall picture of the real-time network through a single dashboard. This can assist network monitoring teams to detect and respond to the security threat in real time. The research aims to:

- To conduct literature survey and learn about previously proposed detection techniques.
- To analyse existing DDoS detection techniques and find gaps.
- Implement a collaborative network monitoring solution for detecting and analysing DDoS attacks.
- Eliminate the ambiguity in the tools used and improve the system.
- To evaluate the collaborative network monitoring solution considering different security models.
- To compare the proposed technique and perform an efficiency analysis on the technique and solution.

Table 1: Research Questions

Sr No	Research Question	Objective
RQ 1	**What are the current detection and prevention techniques for DDOS attacks?**	Conduct literature survey
RQ 2	**What are the gaps in the current detection techniques?**	Analyze the existing detection techniques and perform a gap analysis.
RQ 3	**How to enhance the architecture of the stack?**	Eliminate the ambiguous tools used in existing architecture.
RQ 4	**How effective is the designed solution in detecting the attacks?**	Perform an evaluation analysis of the designed solution

1.1 Research Questions and Objectives

Table 1 gives provides the research questions this research intends to pursue. Each research questions is paired with the corresponding objective or approach on how to answer these questions.

1.2 Motivation

In order to monitor and protect a network from potential network assaults, my main motivation for pursuing this project was to develop a cost-effective collaborative monitoring system utilizing open-source tools.

There is a real need for a cost effective solution or technique that can detect different types of attacks in real-time. The idea behind implementing such a solution came to me during my experience working in my previous workplace. Implementing a solution offering that is economical for a small to medium business is the main motivator behind this research.

However, I had intended to test the system against a cyberattack to determine how successful such a reaction may be. For the purpose of assuring the availability and functioning of an organization and its business, DDOS assaults are a crucial research topic because they are challenging to recognize and efficiently manage.

DDoS assaults pose a significant risk to networks and businesses. It has the potential to dramatically interrupt business operations and services, resulting in financial loss. The rise of DDoS attacks demonstrates that they are extensively used by attackers for a variety of reasons. There is an urgent need for a low-cost solution or technique for detecting these types of attacks in real time.

2 Related Work

2.1 DDOS Attack Detection

Existing security methods, however, either do not offer enough protection against these attacks or are only effective against certain DDoS attacks. Understanding the main components of DDoS assaults is essential since they can suddenly modify the used port/protocol or operation mode. Threat detection methods using machine learning (ML) have been thoroughly studied. However, it is unclear which particular characteristics are crucial

and which methods are best for spotting attacks. Detection, filtering, and trace back are the three most used defensive tactics Wyld et al. (2011).
It can be difficult to accurately distinguish between valid and malicious traffic. When there is a lot of traffic, filtering might slow down the network, and traceback only works when there is little traffic. The majority of the detection techniques now in use have lower success rates. When an assault uses real requests for the attack, it can be challenging to distinguish between attack traffic and regular traffic. Due to the enormous amount of data required for analysis, real-time network detection can be challenging Wyld et al. (2011).
Statistical techniques are good at spotting anomalous resource usage patterns that result from DDoS attacks. The inability of statistical analysis to recognize the typical distribution of network packets, which forces its approximation as a consistent distribution, is a drawback of statistical analysis's use for detection. Although ML systems built on data mining have shown to be very accurate at spotting DDoS attacks, they are not without their own set of difficulties. Their prolonged learning period is a noteworthy disadvantage that currently prevents them from being used in real-time operations Wyld et al. (2011).
Two open-source intrusion detection systems (IDSs), Snort and Suricata, were examined in 2017 to see how well they could identify malicious traffic on computer networks. The effectiveness of both IDSs was evaluated at a 10 Gbps network speed. The study found that Suricata utilized more processing resources than Snort but handled network traffic more quickly and with fewer packet drops. Snort was chosen for additional testing because it has a higher detection accuracy. However, the study did find that Snort produced a sizable number of false positive alerts Shah and Issac (2018).
According to Ye et al in 2018, methods like neural network algorithms cannot be used. The researchers built a simulation of an SDN environment using Mininet and Floodlight and developed a DDoS attack model using SVM classification techniques. During testing, they found that this approach had a 95.24 percent accuracy rate Ye et al. (2018).
Later in 2019, Mehr and Ramaurthy investigated how a DDoS attack on the Ryu controller would be executed and detected on an SDN network using a network topology modelled on the Mininet emulator. The authors employed an ML method called SVMs for detection. The simulations' findings show that their detection system significantly lessened the impact of DDoS attacks on the Ryu controller Mehr and Ramamurthy (2019).
In a paper released in 2020, a method for detecting DDoS assaults utilizing three ML algorithms is discussed. KNN, RF, and NB classification algorithms were employed to separate DDoS packets from regular packets based on the delta time and packet size. The detector can identify several DDoS attacks, such as Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and others, with an accuracy rate of 98.5 percent Priya et al. (2020).
A survey of the new and existing methods for categorizing and visualizing network traffic was conducted and published in a paper in 2020. The poll shows that choosing an acceptable image or dashboard depiction of network traffic in a particular situation and set of circumstances is still a challenge Konopa et al. (2020).
According to a 2021 publication, scalability and performance of these techniques are also significant research considerations because of the enormous volume of network traffic, however the majority of research in the field focuses on mechanisms intended to increase detection model accuracy. To process the data, the article makes use of the Apache Spark framework. The results show that decision trees are outperformed by random forests, and that distributed processing enhances performance in terms of pre-processing and training

time Kousar et al. (2021).
In 2021, Sun et al. outline a method for leveraging raw data to visually represent several characteristics of network traffic. The raw data was first divided into controlled chunks for this. Then, a supervised neural network and a labeling method based on expert knowledge were used to train a model using a dataset consisting of two weeks' worth of network traffic data. The data from the first week served as the training set and the data from the second week functioned as the validation set. The validation results showed precision values of 0.800 and 0.815 for recognizing malicious SMB and TCP SYN flooding, respectively, and precision scores of 0.980 for detecting ARP flooding Sun et al. (2021).
Another study that was published shown that python open-source code might be created for IDS. The program can detect all types of cyberattacks using ML models, ensuring the security of contemporary networks. This technique can be easily created and replicated on additional intrusion detection datasets to address cybersecurity concerns Yang and Shami (2022).
A 2022 study that employs the Naive Bayes approach to identify DDoS attacks. A prediction model was created using the Nave Bayes method, and the dataset's features were chosen. Ideal features included src ip, dst ip, flow duration, flow iat max, fwd iat max, and bwd iat tot. These findings demonstrate that the accuracy of detecting DDoS assaults using the Nave Bayes approach increased from 65.6 percent without feature selection to 69.6 percent with feature selection. The Naive Bayes technique has a low overall accuracy even if it can distinguish between DDoS attacks and mild attacks Mandala et al. (2022).
A Scattered Denial-of-Service Mitigation Tree Architecture (SDMTA) detection mechanism was suggested in another study that was released in 2022. The essay suggests a fresh approach to DDoS attack mitigation in hybrid cloud environments. The suggested design includes network monitoring to simplify detection procedures. The authors compared the detection rates of their proposed model to those of current state-of-the-art models using a dataset as input. With rates of 99.7%, 98.32%, and 99.92%, respectively, their strategy exceeded the current state-of-the-art model in terms of accuracy, specificity, and sensitivity Kautish et al. (2022).
A research survey that was published in 2023 evaluated DDoS attacks scientifically and offered a hierarchical system to counter them. The study also suggested the best ways to deal with these dangers, particularly the use of fuzzy-based detection techniques to deal with these dangers and plug holes in existing detection systems Javaheri et al. (2023).

2.2 Network Monitoring

A network monitoring solution called NetGraf is introduced in a paper from 2021. This paper's objective is to present NetGraf, a cutting-edge monitoring solution that streamlines many data sources into a single dashboard. Additionally, it offers ML libraries for real-time anomaly discovery and data analysis. In order to track performance trends and notify users when network performance declines, NetGraf uses a database backend. Because it makes the data easy to examine, a monitoring system that employs end-to-end learning to aggregate several metrics and present them in a single dashboard can be very helpful for network operations Mohammed et al. (2021). Network administrators may find it helpful to employ ML algorithms included within the system to monitor a network and raise flags when any anomalies are found.

A real-time network security traffic analysis platform, or NSTAP for short, was created

and evaluated by Maasaoui in 2022. NSTAP looks and analyzes traffic data to find and stop hostile traffic. By utilizing a variety of visualization techniques, including charts, tables, and histograms, we show that the platform is capable of producing insightful and useful insights using basic time-domain analytics on big data sets. This study builds the foundation for upcoming ML-based automation solutions Maasaoui et al. (2022).

2.3 Summary

According to the current trend in identifying DDoS assaults on networks, the majority of research is focused on assessing the usefulness and accuracy of various ML algorithms in detecting DDoS attacks using given datasets. Although little research has been conducted on evaluating the models on a real-time network and determining their performance. The project proposes developing a collaborative network monitoring solution that integrates an intrusion detection system (IDS) utilizing machine learning methods, monitoring a simulated network that would resemble a real-world network, and evaluating the performance of this solution. This study could aid in the development of more effective strategies for guarding against DDoS attacks, which are becoming a growing threat to network security.

3 Methodology

3.1 Research Method

1. **Data Collection**
   In a nutshell, data collection is the process of gathering data relevant to the aims and objectives of a machine learning system. This method eventually results in the creation of a data set containing the data you collected and capable of being used to train an ML model. While it may appear straightforward at first glance, data collection is the first and most crucial stage in the machine learning pipeline. It is a critical component of the ML life cycle's difficult data processing stage Doshi et al. (2018).

2. **Data Processing**
   The data collection stage is frequently the most time-consuming and critical element of any Data Science endeavor. Even if your solution is complex or sophisticated, if the source data is of poor quality, the outcome will be bad. As a result, it is vital to ensure that all relevant data for the planned analytical technique is available, accurate, and in the proper format. A number of tasks must be accomplished at this stage, depending on the unique condition being treated. One such endeavor is to develop a method to generate or capture data that is currently unavailable Wilkinson (2022).

3. **Data Modelling**
   Much of the work in this stage goes into selecting the most effective techniques, making sure the data is prepared for use with those methods, and then training the model. It is advised that several models be used at this point so that they can be contrasted and compared throughout the review process Wilkinson (2022).

4. **Solution Implementation**
   The proposed solution will be built using a similar architecture to that given in Kaur, Mohammed, and Kiran's article from 2021. The configuration would include network elements that would supervise the simulated network and direct the metrics obtained into a single database. The solution's machine learning-based detection component is trained and tested using the accumulated data. A central dashboard then displays the metrics from the monitoring components along with the analytical findings. This gives users a thorough visual understanding of the activity on the network.
   The original approach called for comparing tools that were similar to each other, such as Zabbix and Nagios, to determine which one would work best for the solution architecture. However, it would have be wiser to move forward with an architecture similar to the one utilized in the earlier article due to the duration of the project.

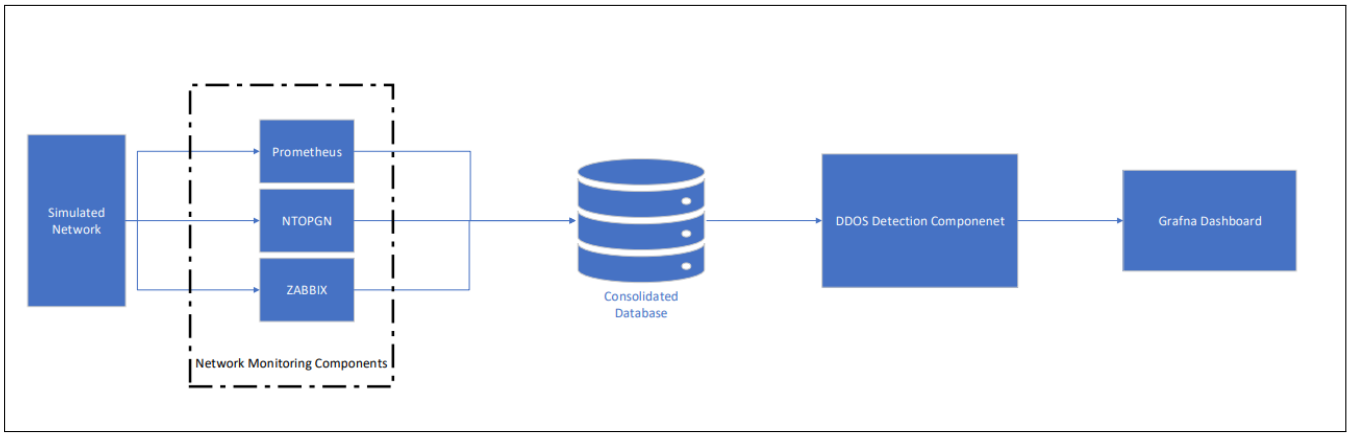

Figure 2: Solution Architecture

Proposed Monitoring tools to be used:

(a) Prometheus: Network Monitoring

(b) NTOPGN: Traffic Analyser

(c) ZABBIX: Network Monitoring and Management tool

5. **Performance Evaluation**
   The last step entails evaluating the effectiveness of the collaborative network monitoring solution in spotting DDoS attacks. This includes evaluating the system's overall value in detecting DDoS attacks as well as the model's precision, false positive and false negative rates Wilkinson (2022).

6. **Visualization Modelling**
   It's critical to provide a thorough dashboard with metrics the users will find useful and relevant Mohammed et al. (2021). For the purpose of dashboard and visualising Grafana is used. This would make it easier to grasp the data graphically and provide an overall view of what is taking place on the network. Based on the information gathered and examined by the machine learning component, the dashboard would also immediately alert users to any irregularities.

3.2 Research Resources

The study by Kaur, Mohammed, and Kiran (2021) served as inspiration for the solution architecture. On Graphical Network Simulator-3 (GNS3), a network software emulator, a real-time network will be developed and simulated in order to generate real-time network data. In order to provide enough data to train and test the machine learning model and increase its accuracy and precision, the monitoring component of the solution will monitor the data over time.
Figure 3 shows the simulated network, which is designed and emulated in the GNS3 emulator.

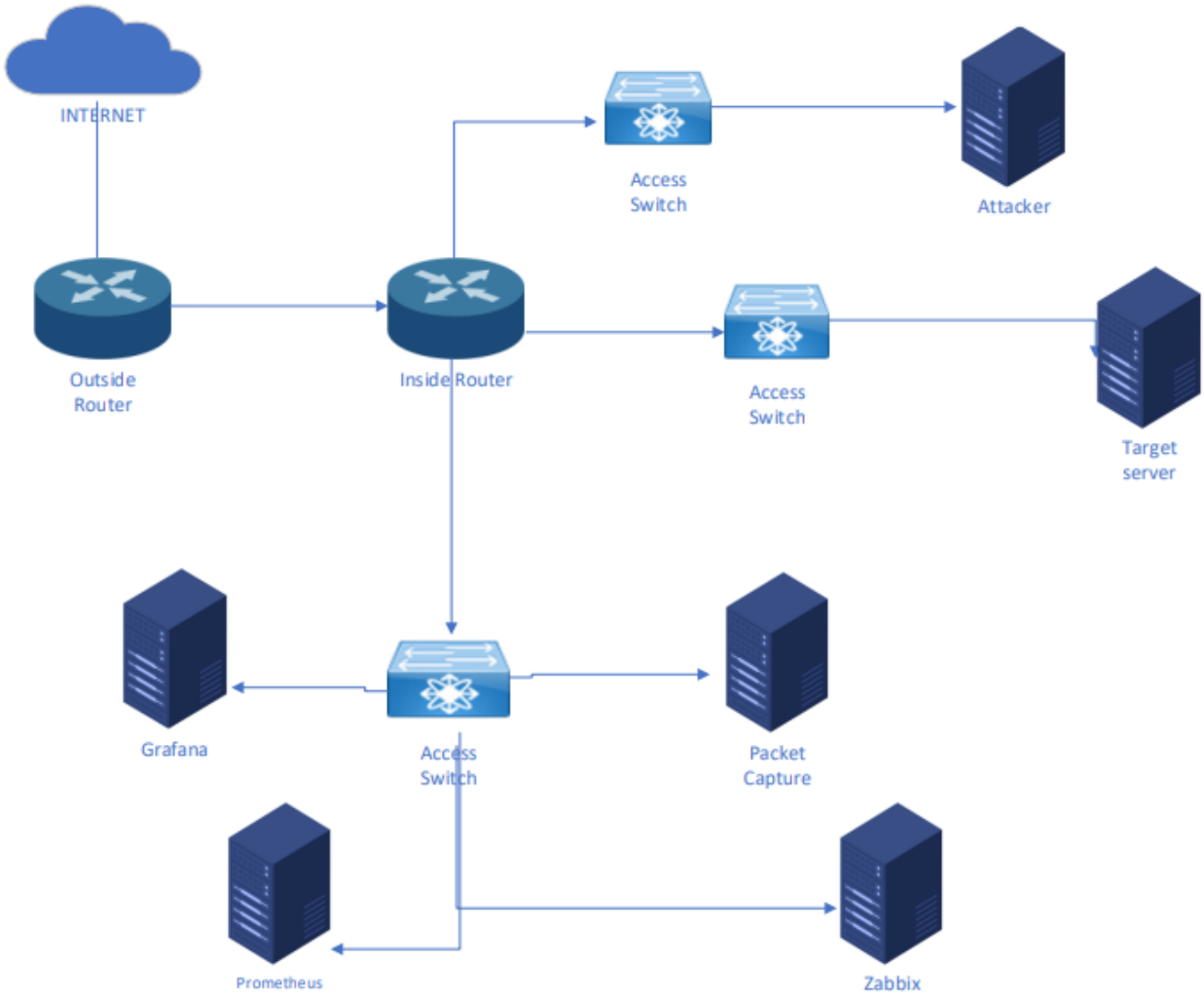

Figure 3: Network Diagram for Network Simulation

3.3 Evaluation

Performance criteria including true positive rate, false positive rate, precision, and recall would be utilized as the benchmarks to assess the model's effectiveness. The effectiveness of the approach in recognizing and detecting these attacks will be tested by simulating various DDoS attack types on the simulated network using various DDoS attack tools.

3.4 Ethical Considerations of the Research

DDoS assaults on a network will be studied and simulated as part of the research proposal. The network and DDoS assault simulation will be carried out in a controlled, isolated virtual environment to minimize any potential risks.

4 Design Specification

The virtual simulated network and stack are created and designed on a single physical system, a laptop. The configuration of the machine is as follows:

- Performance Oriented CPU: Intel(R) Core(TM) i7-1065G7 CPU
- RAM: 16 GB DDR4
- Storage: 500 GB SSD Storage

The network is simulated in GNS3 and the monitoring stack is installed on the GNS3 dynamips components and VMs. The spesfications of the stack components are as follows.

Table 2: Architecture Specifications

Sr No	Software Tool	OS	Ram	Storage	CPU
1	Grafna	ubuntu 22.04	1 GB	10 GB	1v
2	Prometheus	ubuntu 22.04	1 GB	10 GB	1v
3	Zabbix	centos 7	2 GB	20 GB	2v
4	Target Web Server	ubuntu 22.04	1 GB	10 GB	1v
5	Attacker machine	ubuntu 22.04	1 GB	10 GB	1v

5 Implementation

5.1 Initial network setup

Figure 3 shows the design of the network implemented. The initial setup involves setting up the network to monitor and generate traffic. The network consists of 3 internal network segments using routers to route traffic between the nodes. The network is split as below.

1. 192.168.10.0/24 - The monitoring solution
2. 192.168.20.0/24 - The attacker machine simulating the DDOS attack
3. 192.168.30.0/24 - The target machine hosting a web server for the DDOS attack

The routers are also connected to a nat cloud to provide external internet access to the nodes.

The first router called the Outside Router that provides external internet connectivity to the internal network. The second router called the Inside Router provides network connectivity between the internal nodes of the network. The inside router acts as the primary gateway for the internal networks and its nodes.

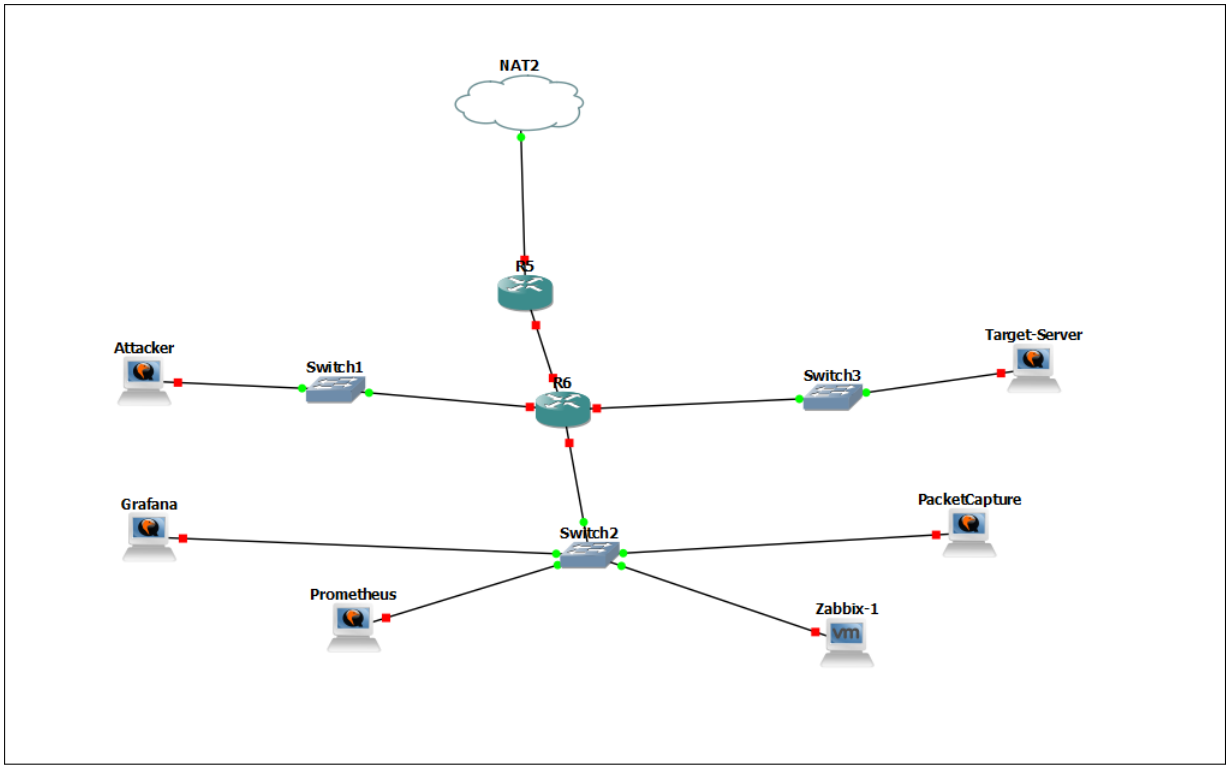

Figure 4: Network implemented for Simulation in GNS3

5.2 Monitoring Solution

The monitoring solution involves the following componenets

1. Zabbix
2. Prometheus
3. Grafana

Zabbix is hosted in an centos virtual machine and given the IP address 192.168.10.10/24. The tool monitors the internal nodes for various metrics using SNMPv2 for the networking devices and using the zabbix agent for the Ubuntu virtual machines. The metrics are then queried by Grafana to provide a dashboard for visualization and monitoring the health of the network.

Prometheus is hosted in an Ubuntu virtual machine and given the IP address as 192.168.10.155/24. Prometheus is able to scrape the network for various metrics for the network using its plugins called "node exporter" and "snmp exporter".

Grafana is hosted in an Ubuntu virtual machine as well and given the IP address 192.168.10.13/24. The data source plugins for the zabbix and prometheus tools are then added in grafana which is then used to query the data from the respective tools for visualization. Since the focus of this research was on DDoS attack, the metrics collected was focused on network related such as packets transmitted and received. The dashboard panels where designed to visualise unusual network spikes or performance spikes which could mean a DDoS attack is occurring.

5.3 Detection Logic

The logic used in this research involves comparing the network passed through the network to a threshold. If the network is above the threshold there is a possible DDOS attack occurring and further investigation through the visualised dashboard in Grafana can lead to the source and target of the attack.

5.4 Challenges

Initial implementation plan included implementing a packet analysis tool that could give insights into the type of network traffic transmitted within the network. However, during the project timeline several technical challenges emerged. The tools considered for implementation were either ntopng, zeek or tshark.

Grafana though having plenty of plugins to integrate with data sources, unfortunately the tool is limited and does not have integration connectors or API connector to the mentioned tools. This meant having to use a "middle man" to communicate between the packet analysis tool and Grafana. At first attempt influxdb a time series database was used. The packet analysis tool however was not able to store its data in influxdb. Next was to try and use elasticsearch to store the time series data in indexes which could then be sent to grafana for visualization. However, even though the tool stored the packet captures in indexes to elasticsearch, grafana was unable to query the data and hence the packet capture could not be visualised in the Dashboard.

Due to the these challenges and time constraints the packet analysis tool was omitted. However a collaborative tool that provides visualization and dashboards for the overall health of the network as well as insights on the traffic of the network under one "view" for a User or an Admin can prove to be a powerful solution offering.

6 Solution View

As mentioned before grafana serves as the front-end one panel one view visualization of the network. It presents various dashboard panels from the modules integrated with grafana that are monitoring the solution. Below are the screenshots of the view from grafana.

Figure 5: Server Host Metrics

Figure 5 shows the server host metrics of one of the nodes (Target Web Server) being monitored. The dashboard shows metrics like CPU usage, network bandwidth as well as disk usage of the node. A spike in the performance in these graph could hint to a DDoS

Figure 6: Network Metrics

activity.
The Figure 6 shows the server shows the network overview of the simulated infrastructure, like network traffic, system uptime, etc. Threshold values are set to monitor and detect if a DDoS activity occurs. If the threshold is crossed, the panel of the dashboard would be marked as red indicating a spike which would notify a user of a suspicious activity.

Organizations may keep one step ahead of intruders by displaying critical indicators, configuring intelligent warnings, and enabling quick drill-downs. This ensures uninterrupted service and robust network security in a cost effective-manner.

7 Conclusion and Future Work

The aim of this project is to build a collaborative network monitoring stack that provides a single view to its user the overall health of the infrastructure and network and to protect it from network level attacks like DDoS attacks. Though not the desired result, the stack deployed was able to gather information on the network's health and network metrics, which was utilised to detect less sophisticated DDoS attacks. The purpose of a of a collaborative monitoring stack has immense potential. The stack can be built further to add more modules like threat intelligence feeds, application layer monitoring or organizational identity monitoring that can prove to be useful metrics to visualise under one single view of a dashboard to monitor an organization and bolster its security against many cyberattacks.

References

Cook, S. (2023). 20+ ddos attack statistics and facts for 2018-2023, `https://www.comparitech.com/blog/information-security/ddos-statistics-facts/`.

Doshi, R., Apthorpe, N. and Feamster, N. (2018). Machine learning ddos detection for consumer internet of things devices, *2018 IEEE Security and Privacy Workshops (SPW)*, IEEE, pp. 29–35.

Javaheri, D., Gorgin, S., Lee, J.-A. and Masdari, M. (2023). Fuzzy logic-based ddos attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives, *Information Sciences* .

Kautish, S., Reyana, A. and Vidyarthi, A. (2022). Sdmta: Attack detection and mitiga-

tion mechanism for ddos vulnerabilities in hybrid cloud environment, *IEEE Transactions on Industrial Informatics* **18**(9): 6455–6463.

Konopa, M., Fesl, J. and Janeček, J. (2020). Promising new techniques for computer network traffic classification: A survey, *2020 10th International Conference on Advanced Computer Information Technologies (ACIT)*, IEEE, pp. 418–421.

Kousar, H., Mulla, M. M., Shettar, P. and Narayan, D. (2021). Ddos attack detection system using apache spark, *2021 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, pp. 1–5.

Lee, S., Levanti, K. and Kim, H. S. (2014). Network monitoring: Present and future, *Computer Networks* **65**: 84–98.

Maasaoui, Z., Hathah, A., Bilil, H., Mai, V. S., Battou, A. and Lbath, A. (2022). Network security traffic analysis platform-design and validation, *2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA)*, IEEE, pp. 1–5.

Magazine, I. (2023). 2022: Ddos year-in-review, `https://www.infosecurity-magazine.com/blogs/2022-ddos-yearinreview/`.

Mandala, S., Ramadhan, A. I., Rosalinda, M., Yafooz, W. M. and Khohar, R. H. (2022). Ddos detection by using information gain-naïve bayes, *2022 2nd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA)*, IEEE, pp. 283–288.

Mehr, S. Y. and Ramamurthy, B. (2019). An svm based ddos attack detection method for ryu sdn controller, *Proceedings of the 15th international conference on emerging networking experiments and technologies*, pp. 72–73.

Mohammed, B., Kiran, M. and Enders, B. (2021). Netgraf: An end-to-end learning network monitoring service, *2021 IEEE Workshop on Innovating the Network for Data-Intensive Science (INDIS)*, IEEE, pp. 12–22.

Priya, S. S., Sivaram, M., Yuvaraj, D. and Jayanthiladevi, A. (2020). Machine learning based ddos detection, *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*, IEEE, pp. 234–237.

Shah, S. A. R. and Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to snort system, *Future Generation Computer Systems* **80**: 157–170.

Sun, Y., Ochiai, H. and Esaki, H. (2021). Multi-type anomaly detection based on raw network traffic, *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, pp. 1–2.

Wilkinson, P. (2022). Five stages of every data science project, `http://web.archive.org/web/20080207010024/http://www.808multimedia.com/winnt/kernel.htm`.

Wyld, D. C., Wozniak, M., Chaki, N., Meghanathan, N. and Nagamalai, D. (2011). *Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15-17, 2011, Proceedings*, Vol. 196, Springer.

Yang, L. and Shami, A. (2022). Ids-ml: An open source code for intrusion detection system development using machine learning, *Software Impacts* **14**: 100446.

Ye, J., Cheng, X., Zhu, J., Feng, L. and Song, L. (2018). A ddos attack detection method based on svm in software defined network, *Security and Communication Networks* **2018**.

Zhang, B., Zhang, T. and Yu, Z. (2017). Ddos detection and prevention based on artificial intelligence techniques, *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, IEEE, pp. 1276–1280.