UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Denkleiers • Leading Minds • Dikgopolo tša Dihlalefi

COS700 Research Report

The Impact of DDoS attacks on the SANReN Network

Student number: u18052640

Supervisor(s):
Dr. Solomon Tekle (sm.tekle@cs.up.ac.za)
Prof. Hein Venter (hventer@cs.up.ac.za)

Peter Okumbe

October 31, 2022

Abstract

The biggest disadvantage of the utilization of computer networks is that they are susceptible to network security breaches and attacks. One of these attacks is the Denial of Service attack (DoS). The most common version of this attack is the Distributed Denial of Device (DDoS) attack which floods a network with traffic in an attempt to make the provided service unavailable. This poses as a huge risk for businesses and organizations that provide services to users over a network, as service downtime leads to a loss in revenue, however most organizations focus more towards drawing the attention of customers and competing against competitors to provide the best services to users rather than focusing on enforcing proactive preventative measures to safeguard their networks from being vulnerable to these said attacks. There is not one specific straightforward technique that exists to completely prevent DDoS attacks from occurring but various defensive countermeasures exist that attempt to mitigate the impact of these attacks when they occur. One of these defensive techniques involves the mitigation of network attack traffic floods by directing this harmful traffic to a honeypot. The goal of this paper aimed to evaluate the impact of DDoS attacks on the South African Research and Education Network (SANReN), as well as to test the effectiveness of the above-mentioned defensive technique to measure the extent at which it can safeguard a network, such as the SANReN, from experiencing the impact of a DDoS attack. The results of the conducted experiment illustrated the negative effect that launched DDoS attacks have on the performance metrics of a targeted Local Area Network (LAN) that would form a part of a larger Wide Area Network (WAN), such as the SANReN network. The results further indicated that the inclusion of the honeypot defensive technique succeeded in mitigating the damage inflicted by the launched DDoS attacks on the targeted network, supporting the need for the continuous development, implementation and testing of defensive techniques to safeguard computer networks from experiencing the negative effects inflicted by network security attacks.

Keywords:

Denial of Service (DoS), Distributed Denial of Service (DDoS), attack, SANReN, LAN, WAN, network, service, defensive, technique, honeypot, floods, traffic, impact

1 Introduction

The internet is a global worldwide system of an interconnected network of computers that provides a variety of information, resources and communication services using standard communication protocols.[1] The internet was build to offer fast and easy global access to data and communications whenever and wherever required. Despite being coined as the largest and most utilized computer network service worldwide, due to its lengthily existence and wide openness [2], it is highly vulnerable to security attacks and greatly invites this idea to attackers.

Computer networks are groups of interlinked computers that communicate with one another to share their resources and data provided by network nodes. A network node consists of any device capable of sending or receiving data, such as a computer or printer. [3] The development and utilization of computer networks helps to provide services that a wide range of users can access over the internet. However, as highlighted earlier, these computer networks are susceptible to network security breaches and attacks. The main aim of a network security attack involves the ability to use various methods to steal, alter or destroy data or information that impacts the availability, reputation and service quality of a network. [4] The occurrence of such security attacks affects both the organization providing the network service and the users making use of the provided service.

One of the most practiced attacks is the Denial of Service (DoS) attack, which attempts to make provided computer resources or services unavailable to its intended users. This is accomplished by flooding the targeted system with traffic, or sending information to the target system to trigger a crash. [5] The most common variant of this attack is the Distributed Denial of Service (DDoS) attack which orchestrates a synchronized DoS attack that derives from multiple sources directed to a single target at the same time, thus increasing the severity and impact of the launched attack. Despite the development of techniques by modern security technologies to defend against most forms of DoS attacks, these attacks still pose a large threat to the safety of the networks in organizations due to the continuous eruption of unique and evolving variants of such attacks. [5]

This research study is focused on investigating the impact of DDoS attacks on a National Research and Education Network (NREN), which is a specialized internet service provider (ISP) that is dedicated to supporting the needs of the research and education communities within a country. [6] The main

goal of an NREN is to act on behalf of the higher education community in providing advanced information technology and communication services for the national and global connection of the networks and resources of academic institutions. [7]

The South African National Research Network (SANReN) is an NREN that is dedicated to science, research, and education that forms a part of a comprehensive approach by the South African government for the development of cyberinfrastructure, which is focused on ensuring the successful participation of South African researchers in the global knowledge production spectrum. [8] The denial of such a service provided by the SANReN network would result in the organization not being able to close or improve the gap that it was aimed at closing through providing the service. In this case for example, an attack targeted at shutting down the services provided by the SANReN network would force users to either deviate towards using the services of another similar service provider [9] or revert back to the struggle of transporting hard-drives amongst each other for the sharing of research, resources and information with one another [8], of which the whole purpose of the creation of the SANReN network was built to avoid.

The success of these attacks results in a loss in revenue on the targeted organization. Network security breaches do not just pose a monetary risk to businesses and organizations, they also pose a huge risk to the safety of the data and integrity of managed systems. [2] Network security attacks can corrupt or destroy data and damage running systems, which in turn would leads to increased costs in an attempt to recover data and restore systems to their original state, therefore proactive countermeasures should be set in place and followed, such as data backups and the implementation of defensive techniques against network security attacks, to protect the targeted systems and data of organizations or to decrease the additional costs, losses and impact inflicted by these attacks. In order to evaluate the impact that DDoS attacks have on a targeted network and determine the strength and effectiveness of a defensive countermeasure against DDoS attacks, the defense mechanism needs to be tested and evaluated against such an attack, which is what this research study expected to achieve.

The remainder of the paper is structured as follows: Section 2 includes the problem statement and solution to solve the research gap, Section 3 describes the methodology and experimental set-up followed in this research study. Section 4 includes a background overview of the purpose, types and classifications of DDoS attacks, honeypots and the SANReN network. Sec-

tion 5 presents the literature study of related work, Section 6 discusses the results of the conducted experiment and Section 7 summarizes and concludes the paper with a discussion on proposed future work.

2 Problem Statement

The goal of this paper aimed to evaluate the impact of DDoS attacks on the performance of a targeted network, such as the SANReN network, and aimed to test the effectiveness of an existing defensive technique that involves redirecting harmful unsolicited network traffic floods to a honeypot, in order to measure the extent at which this defensive technique could safeguard a targeted network from a DDoS attack.

One of the most common mistakes made by most organizations that are susceptible to experiencing network security attacks, such as DDoS attacks, is that they tend to focus more on drawing the attention of customers to utilize their services and striving towards providing the best services to defeat competitors, rather than taking cognizance of the major impact and losses that will be experienced whenever such network security attacks are launched on their respective networks. This lack of earnest focus on enforcing pre-prepared defensive measures to safeguard their networks from such attacks results in these companies and organizations only engaging in reactive measures, in an attempt to restore the state of their networks whenever a DDoS attack occurs, which leads to great losses in financial revenue and time spent on trying to recover their networks. This reactive approach prolongs the server network downtime by only trying to find a solution to eradicate or mitigate the impact of the launched DDoS attack when it has already been executed, in an attempt to restore the targeted network to its original state. The more time that service is denied to users, the more revenue is lost and the more competitors triumph. Therefore, more proactive approaches and techniques need to be set in place and followed by these organizations to mitigate the impact of DDoS attacks on their networks or to decrease the amount of time that it takes an organization to recover their networks whenever they may experience a DDoS attack.

Due to the continuous growth in the popularity and number of variants of DDoS attacks, there is not one specific countermeasure technique that exists to completely prevent DDoS attacks from occurring, however a number of techniques and proactive measures exist that attempt to prevent or minimize the impact of DDoS attacks when they occur on various types of computer

networks.

One of the existing techniques of defending against DDoS attacks involves the utilization of a honeypot to detect and redirect suspected harmful traffic floods aimed at attacking a system. Honeypots are used to act as a trap that simulates the services of a real computer system to lure attackers into capturing their launched attacks and safeguarding a target network from the intended effects of these attacks by rerouting the attack to the honeypot instead of reaching the target network. [10] [11] An influx of harmful attack traffic is aimed at slowing or crashing the availability of a network service but if the harmful attack requests are caught or redirected from the main targeted network, then this decreases the impact of a DDoS attack launched on a network, which denies the attacker from inflicting the mass of the intended damage towards the victim system. This research study therefore aimed to investigate and measure:

- What is the extent at which the implementation of the defensive technique of using a honeypot to detect and redirect suspected attack traffic flood requests from reaching the main targeted network, can safeguard a network, such as the SANReN, from the impact of a DDoS attack?

Whenever a DDoS attack is launched towards a targeted network, various performance metrics are affected on the network [12], therefore in order to understand the severity of the impact that a DDoS attack has on a targeted network and in order to test the effectiveness of a proposed defensive technique against this attack, an experiment can be conducted to measure the effect that a launched DDoS attack and an implemented defensive technique have on the performance metrics of a targeted network.

This research study therefore involved conducting an experiment to test the effectiveness of the above-mentioned defensive technique of capturing and redirecting harmful unsolicited network traffic floods to a honeypot, in an attempt to mitigate the impact of a DDoS attack whenever it is launched towards a targeted network. The experiment involved measuring and analyzing the performance metrics of a network in a simulated testing environment before and after a DDoS attack is executed in the tested network environment, in order to evaluate the impact and severity of the DDoS attack on the network and to measure the extent at which the defensive technique can be effective in safeguarding a network against such attacks.

This research study was focused on investigating and mitigating the impact of DDoS attacks on a National Research and Education Network (NREN),

specifically the SANReN network. This research study did not focus on the entire SANReN network in all areas of South Africa in which the SANReN network connections exist, therefore the research was limited to focus on evaluating and mitigating the impact that a DDoS attack has on a Local Area Network (LAN) that would form a part of a larger Metropolitan Area Network (MAN), which further forms a part of a larger backbone Wide Area Network (WAN), such as the SANReN network MAN connections that have been set across the city of Tshwane (Pretoria) in the Gauteng province, where the Council for Scientific and Industrial Research (CSIR) main site resides. [8]

3 Methodology

Whenever a DDoS attack is launched towards a targeted network, various performance metrics of the network are affected, therefore in order to evaluate the severity of the impact that a launched DDoS attack has on a network and in order to test the effectiveness of a proposed defensive technique against this attack, an experiment can be conducted to measure and analyze the effect that a DDoS attack and an implemented defensive technique have on the performance metrics of a targeted network.

In order to conduct such an experiment, a DDoS attack needs to be launched towards a targeted network to evaluate the impact that it inflicts on the performance metrics of the victim network.

The methodology followed in this research study involved the conduction of an experiment to evaluate the impact that DDoS attacks have on a targeted network and to test the strength and effectiveness of a defensive technique against DDoS attacks that involves the use of a honeypot to detect, redirect and store suspected attack traffic floods in the honeypot, in an attempt to prevent these floods from reaching the main targeted network.

A previous study highlighted some important factors to consider for the testing of a proposed DDoS attack defensive technique. One of these factors states that the utilized defense mechanism should not add an additional overhead or damage on the system that it is being tested on. [4] Therefore, due to the high risk of launching network security attacks on a legitimate network that could cause damage to the data and functionality of the system, and in order to safeguard a tested legitimate network and system from falling victim to such risks, a simulated network environment with the launch of simulated

DDoS attacks was used to conduct this experiment.

3.1 Experiment

The experiment was conducted and tested using a virtual honeypot installed in a virtual machine environment using virtual box [13] to create and run simulated network services and attacks between created virtual machines, in order to safely conduct and test the experiment without causing harm to the main production system or machine used to conduct the experiment. Both an attack machine and a target machine were set up in the virtual box environment. Table 1 below illustrates a list of parameters and software tools used for the conduction of the experiment.

Parameter	**Value**
Experiment Environment	Oracle virtual box
Attack Machine	Kali linux virtual machine
Victim Machine	Windows 7 virtual machine
Attack Tool	Metasploit framework
DDoS Attack Type	TCP SYN Flood
Honeypot Defense Mechanism Tool	KF Sensor
Performance Metric Measurement Tool	TamoSoft Throughput Test
Measured Performance Metrics	Throughput, Response Time, Packet Loss Percentage
Low Rate Attack Packet Size	50 000 bytes
Medium Rate Attack Packet Size	275 000 bytes
High Rate Attack Packet Size	500 000 bytes
Evaluation Time Per Simulation Test	30 seconds
Final Simulation Test Evaluation Time	60 minutes

Table 1: Experiment parameters and software tools

3.1.1 Experimental Set Up

The kali linux attack machine was set up to launch attacks towards the windows 7 victim machine and the kfSensor software tool [14] was installed and implemented in the windows 7 victim machine to simulate a honeypot and act as the honeypot defensive technique used to safeguard the targeted machine against the negative effects of the DDoS attacks that are launched from the kali linux attack machine. The kfSensor software tool acts as a honeypot system that is designed to simulate vulnerable and heavily targeted system services in order to attract, detect and respond to the activities and behaviours of various network security attacks that are launched and executed by attackers. The generation of an emulated service allows the kfSensor honeypot system to reveal the original source of a launched attack without inviting the risk of allowing the service to be compromised.

The TamoSoft Throughput Test software tool is a utility tool that is used for testing the performances of a wired or wireless network. This software tool was used to measure, analyze and record the change in the performance metrics of the targeted victim machine during the conduction of the experiment.

The benefit of the use of a virtual honeypot in a virtual environment is that it has a low maintenance cost, such that even if the virtual honeypot or network is compromised by an attacker at any point during the conduction of the experiment, its state can be easily restored or replaced, which is beneficial for educational, research and testing purposes, unlike the high costs incurred with building a real DDoS attack defense testing environment. The general deployment of real honeypots is more challenging than that of virtual honeypots and another serious negative effect encompassed with the use of real honeypots involves the risk of attackers managing to attack the entirety of a targeted network if an attacker manages to compromise and take control over the honeypot. [15]

Simulation is an important method used in network research, as simulations can be used to conduct experiments and analyze problems related to computer networks under different topologies, protocols, attacks, and amounts of traffic packets sent [12], without the fear or concern of causing harm to a legitimate production system.

3.1.2 Performance metrics

The network performance metrics on which this experiment will be measured and evaluated on include: throughput, response time and percentage of legitimate packets lost. The performance metric that most research studies have concentrated on measuring is response time, which is the time taken for a packet to travel from a client to the target server. Throughput consists of the sending and receiving rate of data in a network, according to the amount of bits transmitted per second. Throughput is divided into good-put (the number of legitimate traffic bits delivered to a certain destination per second) and bad-put (the number of attack traffic bits delivered to a certain destination per second). The percentage of legitimate packets lost metric measures the ratio or percentage of the amount of legitimate packets that get lost or dropped in transmission during an attack. This metric has been defined as a ratio of good-put and throughput [12] and it has also been described as the most important metric for evaluating the impact of such network security attacks, as it assists in reflecting the accuracy of the defensive technique used. [16]

3.1.3 Generation of DDoS attacks

In a DDoS flood attack, the targeted system is flooded with traffic. This may result in slowing down or crashing the services provided by the target system, due to the large influx of attack packets sent to the target system. This prevents legitimate users from gaining access to the services provided by the targeted network.

The Metasploit framework [17], that is widely used for network security penetration testing, was configured and used in the kali linux attack machine [18] to simulate the launch of DDoS attacks towards the targeted machine.

The simulated DDoS attacks were launched on the targeted network at different volumes of attack strength, in order to test and measure the extent at which the defensive technique can protect the network from the attack. These attack strengths were classified into three classes based on the volume of attack traffic packets that was sent for each simulation test: low, medium and high attack traffic.

Three simulation tests were conducted for an attack launched at each specific attack strength rate (low, medium, high) on the targeted network with and without the implemented honeypot defensive technique for an evalua-

tion period of 30 seconds for each simulation test. A final simulation test was conducted for a period of 60 minutes to test whether the honeypot defensive technique would continue to fulfil its functionality of detecting, capturing and recording the attack traffic activity logs of launched DDoS attacks targeted towards a victim system, as well as to test whether the honeypot defensive technique could withstand the effects of launched DDoS attacks over the average tested time period of 60 minutes, for which most DDoS attacks are launched towards a targeted network for.

The results of all simulation tests conducted were evaluated to determine the effect that the launched attacks have on the performance metrics of the targeted network and to measure the effectiveness of the implemented defensive technique by determining the point at which it could safeguard a network from such an attack.

3.1.4 Defensive technique

Once the DDoS attacks were launched on the target network, network traffic was monitored and suspected attack packets that deviated from the average data transmission patterns and behaviours of the legitimate packets was automatically detected, redirected to and stored in the honeypot.

3.1.5 Steps of procedure to conduct experiment:

1. Set up network test environment.
2. Generate legitimate network traffic.
3. Monitor normal network traffic flow and record normal network performance metrics without launched attack and without implemented defense technique.
4. Generate DDoS attack traffic.
5. Monitor network traffic and record change in network performance metrics with launched attack at different strengths without implemented defensive technique.
6. Monitor network traffic and record change in network performance metrics with launched attack at different strengths with implemented defensive technique.

7. Monitor detected and captured attack traffic activity logs of launched attacks with implementation of honeypot defense technique.

8. Analyze impact of launched attack on the measured performance metrics of the target network and analyze the effectiveness of the defensive technique used:

    - The comparison and evaluation of the change in network performance metrics recorded during the conduction of all simulation tests.
    - Simulation tests:
        (a) Before the DDoS attack is launched towards the targeted network without the implementation of the defensive technique used. (30 seconds)
        (b) After the DDoS attack is launched towards the targeted network at different volumes of attack strength (low, medium and high attack traffic rate) without the implementation of the defensive technique used. (30 seconds)
        (c) After the DDoS attack is launched towards the targeted network at different volumes of attack strength (low, medium and high attack traffic rate) with the implementation of the defensive technique used. (30 seconds)
        (d) After the DDoS attack is launched towards the targeted network with the implementation of the defensive technique used for an average tested time period of 60 minutes.

3.1.6 Experiment Evaluation

The performance metrics chosen to evaluate the effect that the DDoS attacks have on the performance of the target network was recorded and compared before and after the DDoS attacks were launched. These metrics were measured in terms of the change in the performance of the network over the specified evaluation time for each simulation test conducted.

The change in the targeted network's performance metrics when the DDoS attack was launched towards the target network without the implementation of any defensive countermeasure against an attack, was compared to the change in the targeted network's performance metrics when the DDoS attack was launched on the network with the implemented honeypot defensive technique.

The best performing metrics out of the conducted simulation tests with and without the defensive technique enforced, was evaluated in order to determine whether the defensive technique was effective or not. An improved performance of the negative effects inflicted on the performance metrics of the targeted network with the implementation of the honeypot defensive technique suggested that the defensive technique used was effective.

In order to further test the effectiveness of the defensive technique, the technique was tested against the launched DDoS attacks at different strengths, based on the volume of attack traffic sent.

The results obtained upon the conclusion of the final simulation test conducted assisted in determining the point at which the defensive technique can withstand such an attack and thus, the level at which it can protect a victim system from these attacks.

4 Background

Due to the growing popularity, wide scope and use of the internet, even more notably now with the increased use of internet and computer network services to conduct, interact and engage in virtual events and activities, such as online meetings, online education, online job interviews, and remote jobs to name a few as a result of the COVID-19 pandemic, more computer networks are becoming vulnerable to network security threats that are constantly evolving, as attackers are gaining more motivation to attack these utilized computer networks and are becoming more determined to find new ways to circumvent existing defensive techniques against these launched attacks.

Coined as one of the most practiced and common versions of network security attacks, a Denial of Service (DoS) attack is an attack that attempts to make provided computer network services unavailable to its intended users. A Distributed Denial of Service (DDoS) Attack orchestrates a synchronized DoS attack that derives from multiple sources directed to a single target at the same time, which increases the severity and impact of the launched attack. Nathalie Weiler describes that even the average layman is well aware of the penetrating effect that a DDoS attack can inflict on a system. [19] The compromised machines that attackers utilize to launch these attacks are referred to as “zombies” or “bots”, therefore a network of these compromised machines that are used to launch DDoS attacks are referred to as a “botnet”.

4.1 DDoS Attack Types and Classification

Two main classes of DDoS attacks exist: bandwidth (flood) and resource (crash) depletion attacks. A bandwidth depletion attack overwhelms a target network with a flood of unsolicited traffic that prevents legitimate traffic from being delivered to the main target system, which slows down the service provided to legitimate users. [11] A resource depletion attack is designed to compromise the resources of a target system. This type of attack targets a server or process on a system, in an attempt to exploit the vulnerabilities in the system and deny it from processing legitimate requests to provide a service by hanging, rebooting or crashing the system. [11] [20]

4.1.1 *Bandwidth Depletion Attacks*

Bandwidth depletion attacks can be further broken down into two types of DDoS attacks: flood and amplification attacks.

Flood Attacks: A DDoS flood attack floods the targeted system with traffic. This may result in slowing down or crashing the service provided by the target system, due to the large influx of attack packets sent to the target system. [20]

Examples of such flood attacks include the UDP, ICMP and TCP flood attacks. A UDP flood attack is a simple attack launched by transmitting a large volume of UDP packets to a targeted network. Filtering rules can easily be used to deflect these transmitted UDP attack packets from reaching the target network. TCP packets can also be used to transmit large volumes of traffic to a targeted network. This type of attack is known as the TCP flood attack. An ICMP flood attack occurs when a large volume of ICMP ECHO packets are launched to a target network, where the targeted system's computer and network resources are compromised upon a reply to each ICMP request sent. This type of attack can be defended against with the use of a rate-limiting rule at points in the network where high bandwidth exists, however this method might result in the loss of legitimate packet requests. [21]

Amplification Attacks: A DDoS amplification attack makes use of a router's broadcast IP address feature to allow for the specification of the destination address as the broadcast IP address, instead of a specific IP address. This allows for packets to be sent to all IP addresses that are within the broadcast address range. [20]

The DDoS *Smurf* and *Fraggle* attack are examples of DDoS amplification attacks. A *smurf attack* is executed through the transmission of ICMP ECHO packet requests to a network system with broadcast addressing support, such as a router, with the target network's IP address set as the source address. [21] The packets are similar to ping requests that are sent with the expectation of a reply from the targeted network system. Unlike the DDoS smurf attack, the DDoS *fraggle attack* makes use of UDP packets instead of ICMP packets to launch the attack. [20]

4.1.2 *Resource Depletion Attacks*

Much like bandwidth depletion attacks, resource depletion attacks can be further broken down into two classes of DDoS attacks: protocol exploit and malformed packet attacks.

Protocol Exploit Attacks: Two types of protocol exploit attacks exist: TCP-SYN, PUSH and ACK attacks. A TCP-SYN attack is a vicious attack that compromises the resources of a target system and prevents the system from responding to legitimate requests by distributing forged TCP SYN requests to the targeted system. The three-way handshake TCP connection set up between the attack and victim systems are exploited with this attack by consuming the resource that handles the "hand-shaking" exchange of transmitted messages between communicating systems in the TCP connection session. [21]

A fake source IP address is used to send large amounts of TCP-SYN packets to the attacked system, in order to force the attacked system to respond to a non-requesting system. The memory and processor resources of the attacked system start to run out due to the lack of returned ACK and SYN packet responses when a large number of SYN requests are processed by the system. [20] A half open connection is created as a result by leaving a packet in the buffer to prevent legitimate requests from being catered for. After a certain amount of time, packets that were left in the buffer are eventually dropped without a reply, however the effect of the increased delay in time of processing requests makes the task of responding to legitimate requests more cumbersome. Differentiating between legitimate and attack traffic also becomes a difficult process with the launch of this attack, as the attacked systems expect to receive a large volume of legitimate TCP connection requests. [21]

PUSH and ACK attacks occur when TCP packets are transmitted to a target system by setting the PUSH and ACK bits to one. The targeted system is instructed by the transmitted packets to unload all data in the TCP buffer and send a message of acknowledgement once complete. This may lead to the crashing of the target system, as it will not be able to process the large influx of packets sent if the PUSH or ACK attack process is repeated with multiple attack agents. [21] [20]

Malformed Packet Attacks: Malformed packet attacks crash a targeted system through the transmission of incorrectly formed IP packets towards the victim system, which are launched by instructed "zombie" attack machines. [20]

Examples of malformed packet attacks include IP address and IP packet options attacks. IP address attacks transmit packets with identical source and destination IP addresses. This may lead to confusing the OS of the targeted system, which may cause the targeted system to crash. An IP packet options attack forces the targeted system to analyze traffic at an elongated processing time by randomizing IP packet fields and setting the quality of service bits to one. More damage can be inflicted on the processing ability of the targeted system if the attack is executed with multiple attack agents to increase the strength and severity of the attack. [20]

4.2 Temporary and Permament DDoS Attack Effect

Much as DDoS attacks can be classified into various types and classes, the effect of DDoS attacks can also be broken down into two classes: temporary and permanent DDoS attack effect.

A temporary DDoS attack effect acts like a temporary outage to cause the denial of a provided network's service/s for a short period of time, such as the launch of DDoS flooding attacks to overwhelm a network with a large number of unsolicited traffic requests, in an attempt to slow down the services provided by the network to its intended users, where as a permanent effect of a launched DDoS attack is aimed at causing long term outages by permanently causing damage to the attacked system.

Examples of permanent effects of DDoS attacks include the corruption of data, crashing of servers, as well as the damaging of system hardware in supreme instances. Permanent effects of launched DDoS attacks can cause a

negative impact towards the reputation of an organization that continuously falls victim to these attacks, as users can begin to lose trust in the quality of the organization's provided services over time, which may lead users towards making use of alternative networks that provide similar services with better quality and security. [11]

This further supports the recommendation for the development and implementation of defensive techniques and routine countermeasures to be followed for the safeguarding of computer networks and systems that are vulnerable towards these attacks.

The launch of a DDoS attack with a temporary effect is favoured for educational, research and testing purposes, as a permanent DDoS attack effect is more prone to causing permanent damage to the main production system or corrupt system data, which would add an additional overhead cost to repair or replace damaged software and hardware that is used to conduct repetitive testing and experimentation.

4.3 Motivation Behind Execution of DDoS Attacks

Due to the growing development and utilization of computer networks, attackers gain more motivation to structure new ways to infiltrate and harm these network systems, which leads to the continuous growing number of launched network security attacks and variants of these attacks. The motivation behind these attacks is mainly not aimed at breaching the data of targeted systems, but rather to negatively harm the reputation of an organization or to practice and engage in blackmail or espionage.

Other examples behind the motivation that drives attackers to engage in launching these attacks involves groups of gamers attempting to increase their reputation through the distribution of DDoS attacks to compromise the services of opponents in order to win games; and organizations attempting to beat competitors by compromising the provided services offered by their competitors, such that users can be drawn to make use of their own favoured and provided services. This can be easily achieved by various individuals, businesses and organizations without the required skill or knowledge to launch network security attacks, as DDoS attacks can be easily hired and executed at a low cost.

DDoS attacks are also used to voice an online opinion regarding the support

or opposition of a specific topic, which is aimed at having a stronger effect than an in-person strike for example. A common reason for the launch of DDoS attacks by various individuals, organizations and governments involves taking revenge against an opposition, a former employee or an opposing political government or party.

Attackers also indirectly make use of DDoS attacks as a distraction for the potential launch of another larger attack with the hope that it will not be noticed, in order for the larger prepared attack to have an even bigger and stronger negative effect on the targeted victim's system, while other attackers simply engage in launching network security attacks from the joy that they receive out of it or to test their level of skill against other fellow attackers in being able to succeed in launching these attacks to compromise targeted systems. [22]

4.4 Impact of DDoS Attacks on E-commerce

The author of an article published by 'TechInsurance' describes that approximately 120 000 dollars is spent by an average medium sized business in restoring services, managing operations and defending against every launched DDoS attack. [23]

Many businesses and organizations struggle with the difficult task of safeguarding their networks or restoring negatively affected services from the effects of launched DDoS attacks. Slow network performance is one of the most common negative effects inflicted by these attacks, which prevents the availability and accessibility of the services provided by the targeted network. Restoring the negatively affected resources and services to the employees, customers or clients of an organization as fast as possible is highlighted as the greatest challenge to face against the launch of a network security attack.

Due to the difficult nature of defending against successful DDoS attacks, the time taken to restore the effects of these successful attacks is prolonged, which forces businesses and organizations to deal with the added cost of managing their operations offline or with a back-up system for the duration of time until the affected services are restored.

DDoS attacks greatly and negatively affect the provided services and business of online retailers. The impact of successful DDoS attacks may lead to an increase in the cost of customer service, sales and marketing. The

success of these attacks may also poses a risk to and damage the trust and relationship built between customers and clients, which may disrupt business opportunities in future. Further costs can be incurred on the targeted business or organization if the launched attacks negatively affect clients and prompt them to file cyber liability lawsuits against the organization. Businesses and organizations are encouraged to obtain cyber liability insurance that is included in most error and omission policies for online retail and technology businesses and organizations, in order to manage this risk. [23]

Successfully launched DDoS attacks can also results in a loss in time and clients of the attacked organization with the additional overhead of stress placed on the organization's IT staff in an attempt to find a way to revert the effects of the launched DDoS attack and make the negatively affected services available again, therefore the correct defensive mechanisms against these attacks need to be implemented to assist in safeguarding an organization's network from the severe effects that these attacks can inflict with enough momentum. [24]

Targeted resources and systems can be negatively affected for hours, days or weeks, depending on the severity of the launched DDoS attack. The author of an article published by 'kaspersky' mentions that an average of 20 000 dollars can be lost by an organization in every hour of a successfully launched attack. Most causes of successful DDoS attacks are formed as a result of trojan viruses infecting vulnerable computer systems with weakly enforced security measures or the opening of unknown spam emails and the downloading of erroneous files by the employees of an organization. [24]

Additional and reliable anti-DDoS attack mechanisms, such as the disabling of unrecognized network services, identifying regular and irregular network traffic, and automatic scanning of network services to detect common and various DDoS attacks should be regularly and continuously enforced by organizations, in order to protect their networks from such network security attacks. Consumption patterns of high network traffic with no clear cause often indicate the attempts of an attackers to test and gauge the strength of a network's implemented and enforced defense mechanisms. [24]

Nisreen Innab and Aziza Alamri mention that the implementation of resilience organizational planning is imperative in an attempt to prevent the impact of DDoS attacks. They further highlight that as much as evaluating the impact of DDoS attacks is a technical matter, the fact that it is also a business matter should not be ignored. [2]

4.5 DDoS Attack Defensive Techniques

A number of DDoS mitigation and defense techniques exist and have been proposed by various research authors, but there is not one fixed and specific technique that exists to prevent all types of DDoS attacks, due to the continuous growth and evolution of variants of these attacks. Jonah Burgess describes that it is difficult to keep defensive mechanisms up to date and the primary aim of most research in this field involves finding ways to maintain and maximize the quality of service for legitimate users that make use of the provided services of a network, especially when the network is under an attack. [25].

Y. Chen et al. also express the importance and necessity of deriving solutions for both current and future variants of DDoS attacks, instead of only making use of and reacting with specific counter techniques against these attacks. [26] No system is regarded completely safe with the implementation of these countermeasures [27], however the early detection and discovery of a DDoS attack can assist in reducing the damage inflicted by an attacker. [26] [28]

Therefore continuous research will always be required for the development of new defensive counter methods and the testing and enhancement of existing methods, in order to ensure the safeguarding of networks against such attacks. One of the existing defensive techniques that is used as a contingency plan in defending against and reducing the effects caused by DDoS attacks, involves the use of a honeypot. [27]

4.6 Honeypots

A honeypot is a defense technique used to protect a network from a network security attack, most specifically DDoS attacks. It acts as a trap that simulates the services of a real computer system [11] to lure attackers into capturing their launched attacks and safeguard a target network from the intended effects of the launched attacks by detecting, capturing and rerouting the attack traffic to the honeypot instead of reaching the target network. A honeypot tricks the attacker into believing that the honeypot is an important part of the targeted network and the goal of the use of a honeypot is to try and convince the attacker that they have successfully achieved their goal of harming the targeted network. [19]

Once the malicious attacks have been captured in the honeypot, the recorded

logs and information stored by the honeypot about the activities of attackers and their launched attacks can be used by owners of victim systems, such as a network administrator, to monitor and understand the behaviour of attackers, their strategies and motives, as well as to understand the type of attacks that are launched, such as which attacks are most commonly targeted towards the network, in order to track the behaviours of attackers and develop or enhance network security mechanisms to safeguard the network from such attacks or new variants of these attacks in the future.

Honeypots can be classified into two categories, based on the level of interaction that attackers are able to interact with the system: [29]

- *Low-Interaction Honeypots:* Simulate the actions and services of real computer systems to lure attackers and detect attacks by simulating operating system and port services in order to gain information about launched attacks. An attacker only has a limited interaction with the simulated targeted system. [29] Low interaction honeypots limit the attacker to interact with a few simulated pre-configured services, therefore they have a low risk of being compromised by attackers, as they cannot be used to attack other systems due to the fact that there is no real physical computer system and not many services available for the attacker to interact with and obtain control of.

- *High-Interaction Honeypots:* Make use of real computer systems to detect and gain information about attacks and understand the behaviour, tactics, motives and tools used by attackers. This is achieved by providing full access to an attacker to attack the targeted system in order to gain the desired information about these launched attacks. High interaction honeypots are high risk as they are prone to the possibility of attackers gaining full control over them. [29]

High interaction honeypots are hard to detect and have a high maintenance level due to the use of real computer systems and services, where as low interaction honeypots make use of fewer resources and emulate computer systems and services, making them easier to maintain and replace, resulting in a lower maintenance level and cost, as compared to high interaction honeypots. [11]

Honeypots can also be classified into two categories based on the type of design that it is implemented with in a network environment. Both physical and virtual honeypots exist.

A *physical honeypot* is a honeypot that is designed using real computer systems on a real network, where as a *virtual honeypot* simulates real computer systems by hosting a virtual machine that responds to network traffic that is directed to the virtual honeypot. [30]

A virtual honeypot can simulate a network of hosts running various operating systems, therefore allowing a number of honeypots to be used on a single physical server. These honeypots do not require use of additional resources and computer systems, therefore they are easier to maintain and replace with low maintenance and replacement costs, unlike physical honeypots. If an attacker compromises a virtual honeypot, it can easily be replaced or restored to its original state. [25]

4.7 The South African Research and Education Network (SANReN)

This research study is focused on investigating the impact of DDoS attacks on a National Research and Education Network (NREN), specifically the South African Research and Education Network (SANReN), which is a specialized internet service provider (ISP) that is dedicated to supporting the needs of the research and education communities within a country. [6] The main goal of an NREN is to act on behalf of the higher education community in providing advanced information technology and communication services for the national and global connection of the networks and resources of academic institutions. [7]

The SANReN network is operated by the Tertiary Education and Research Network of South Africa (TENET), whose main objective is to provide research and education services for the benefit of enabling collaborative internetworking by universities in South Africa, as well as associated research and support institutions. [31] [32]

The SANReN network is an NREN that consists of a large backbone Wide Area Network (WAN), which connects Metropolitan Area Networks (MANs) across the different provinces and cities in South Africa. A Metropolitan Area Network (MAN) further connects Local Area Networks (LANs) across specific parts and areas of a city within a country.

The SANReN network has a Metropolitan Area Network (MAN) connection across the city of Tshwane (Pretoria) in the Gauteng province. [33]

The SANReN network MAN connections in the city of Tshwane (Pretoria) connects LANs between different institutions in different areas of Tshwane (Pretoria), including the National Library of Pretoria, the National Research Foundation, the Council for Scientific and Industrial Research (CSIR), and the National Integrated Cyberinfrastructure System (NCIS), as well as various campuses of tertiary educational institutions, of which include: the University of Pretoria, Belgium Campus and the Tshwane University of Technology. [34]

The University of Pretoria campuses on which the SANReN network MAN connections exist include: Main campus, Groenkloof campus, Mamelodi campus, Medical campus, Onderstepoort campus and Hillcrest campus. [34]

A number of supported services are deployed and under development on the SANReN network. One of the most commonly used and well-known supported services is *eduroam*, which is a world-wide WiFi roaming service developed for communities in education and research that provides students, researchers and staff with the ability to access connectivity to the internet across their respective campuses and institutions through the use of WiFi. [35]

The *eduroam* supported network service that is deployed on the SANReN network, is made available for students, researchers and staff present on the above-mentioned University of Pretoria campuses to access internet connectivity through the use of WiFi. [35]

Other services supported by the SANReN network include: the Computer Security and Response Team (CSIRT), the Performance Enhancement Response Team (PERT), as well as the South Africa Identity Federation (SAFIRE), which is a national academic identity federation for the South African research and education community. [35]

SAFIRE also provides a number of extended supported participant service providers, such as eduroam, Varisty Vibe, FileSender, the African Research Cloud, and the Data Intensive Research Initiative of South Africa. [36]

With the great effect that the on-going worldwide COVID-19 pandemic has had on the health of people, as well as businesses and organizations, a large population of research authors in many institutions across the world have been directing the focus of their knowledge and resources towards understanding the virus in order to develop vaccines and suggest other methods

to fight and combat against the virus. A fundamental form of this practice involves the sharing of knowledge, data, and results and NRENs serve in promoting the cooperation and collaboration between the academic and research communities of a country by sharing and easily accessing international accumulated research and data through interconnected local and global networks on the internet. This is a prime example of the important of the existence and safeguarding of NRENs, as it greatly supports researchers in the COVID-19 research platform. [37]

5 Related Work

S. Selvakumar and P. Arun Raj Kumar describe that DDoS attacks have become the main threat to the stability of internet operations. This attack can be easily implemented with the utilization of DDOS attack simulation software and tools that can be easily downloaded from the internet by any ordinary user. The above-mentioned authors further included an analysis on the comparison of existing popular DDoS attack tools. [28]

Michael Foley describes that the biggest challenge faced by the general public is the lack of knowledge and awareness of how the internet works. [7] This lack of knowledge of how the internet works can greatly disadvantage organizations in not being aware of the threats that computer networks are vulnerable to in order to take the necessary precautions to defend their networks against such threats, which therefore in turn assists attackers in easily achieving their goal of harming targeted systems.

The study conducted by S. Selvakumar and P. Arun Raj Kumar mentions that most ISP organizations do not inform customers whenever their services are under attack, which is encouraged by a fear of losing their customer base. The motivating factors that encourage the launch of a DDoS attack include: loss in revenue, slow network performance and denial of service. [28] Just a few minutes of service downtime can pose a huge loss in revenue for businesses and organizations. [38]

Nisreen Innab and Aziza Alamri conducted a study on cases related to the impact of DDoS attacks on e-commerce and the control that was followed for each case. The first case described a DDoS attack that was launched on the Ubisoft gaming company that targeted many famous games and affected the company. The proposed solution was to filter out illegitimate users from an increase of legitimate users. The company implemented a defensive tech-

nique of redirecting users to another working server as an additional solution to mitigate the impact of the attack. [2]

N. Innab et al. highlight the difficulty involved in attempting to react fast enough to prevent the risk of loss once a DDoS attack is executed. They further recommend that organizations should set plans in advance to defend against these attacks. A one set specific method or technique to counter against these attacks does not exist, however some actions exist that attempt to make the mission of an attacker more challenging in achieving their intended goals. [39]

Luo Wenliang and Han Wenzhi summarized the principle of DDoS attack from the defensive perspective. A flowchart diagram of a defense system process against a DDoS attack for targeted servers is described. The defense system is based on the ability to respond in time as soon as an attack occurs and makes use of two maintained databases: IP Address Database (IAP) - address of the normal packets that get sent to the website frequently and Attack IP Address Database (AIAD) - address of the attack packet sent when the attack is launched. They then analyzed DDoS attack prevention in software defined networks (SDNs) and the source, intermediate network, victim and distributed defense strategies of the attack are elaborated. From the discussion of the 3 defense strategies (source policy, intermediate network, and victim end strategy), it is also made clear that no single-point strategy can completely prevent DDoS attacks. [40]

Akashdeep Bhardwaj et al. mention that most DDoS mitigation solutions proposed in previous research studies only assist in preventing very few aspects of a full DDoS attack. Attackers are constantly focused on continuously coming up with new variations and techniques in an attempt to bypass existing and newly developed countermeasures. Therefore, more research is required when trying to design and develop an effective DDoS attack countermeasure solution. [4]

R. Sanjeetha et al. describe that the detection and mitigation of DDoS attacks is separated into three phases: the DDoS attack instigation, detection and mitigation phase. A variety of different DDoS mitigation techniques is also discussed in the study [41], while Zargar Saman Taghavi et al. [42] classified the advantages and disadvantages of various DDoS attack defense techniques.

S. Selvakumar and P. Arun Raj Kumar conducted a survey study that lists

the critical resources in a collaborative environment and the possible attacks that each resource is vulnerable to, as well as the expected impacts as a result of the executed attacks. [28]

The three primary components that jointly determine all the elements of a launched DDoS attack, which influences the impact on the infrastructure of a network and the effectiveness of a defensive technique include: the legitimate traffic, attack traffic and the topology. [21]

Akashdeep Bhardwaj et al. listed important parameters and factors to consider for the development of an effective DDoS detection mitigation technique. The study further highlighted the importance of measuring the accuracy of a defense mechanism used, in terms of the sensitivity and reliability of the desired outcomes. [4]

Taieb Znati and Xiaoyu Liang mention that the successful detection of a DDoS attack requires the correct identification of attacks and decreasing the number of false alarms. In the study, the authors adopted the evaluation of widely used metrics to analyze the effectiveness of DDoS detection mechanisms. These metrics include: Accuracy, Sensitivity, and Specificity. [43]

Monika Sachdev et al. reveal that the impact of a DDoS attack on the performance metrics of a target system is closely related with measuring the effectiveness of DDoS defensive techniques. [12] Y. You. revealed that most measurements of existing defensive techniques compare the change in good put under various conditions: without the attack, under the attack, and with the defense mechanism. [44]

Hanfia Aabdullah conducted a risk analysis and risk management methodology to address WLAN intrusion attacks and expose the vulnerabilities of WLANs to the confidentiality, integrity and availability of information processed by these networks. The study suggested that a more adept approach at exposing these vulnerabilities would be to make use of a honeypot. The study also mentions that it would be possible to determine the different types of attacks that can occur and observe the various behaviours of WLAN intruders, through the use of a honeypot. The study further mentions that the utilization of a honeypot will does not affect the operations of a system, therefore it poses no risk to a network. [45]

Asmaa Munshi et al. classified existing defensive techniques of DDoS attacks into various detection classes. They discuss a system workflow detec-

tion class that describes the implementation of using a honeypot database to store harmful traffic floods [10], while Ronierison Maciel et al. introduced a framework for modeling and clustering the activity patterns of an attacker based on the data contained in a honeypot. [46]

Hrishikesh Arun Deshpande proposed the idea of using a network of virtual honeypot machines that mimic specific servers to create a honeypot farm. Launched malicious traffic is redirected to and stored in the honey farm in order to protect the target network from attacks. The study further mentions that the proposed idea can be integrated with existing security infrastructure to enhance the security of a network to protect it from various DDoS attacks. [11]

Niels Provos describes the difference between physical and virtual honeypots. The author mentions the benefit of the utilization of a virtual honeypot, as additional computer systems are not required. [30] Hazem Sallowm et al. indicates that use of physical honeypots results in a waste of resources and a high level of maintenance. [29] Furthermore, Hrishikesh Arun Deshpande highlights that virtual honeypots can be easily replaced or restored with minimal cost, even if targeted and harmed by an attacker, due to their low level of required maintenance. [11]

According to a previous study conducted by Roland van Rijswijk-Deij et al. to investigate the impact of DDoS attacks on the behaviour of customers of targeted service providers, the authors mention that a successful attack can lead to a loss of customers in a market where the importance of service availability is critical. They introduced a framework to capture the behaviour of the customer domains of a Managed Domain Name Server (MDNS) service provider and the framework was used to study two previously occurred DDoS attack events. The study revealed that the impact of DDoS attacks brings about a change in customer behaviour as users tend to lean towards utilizing multiple service providers when the currently utilized service provider is under an attack. [9]

From the literature assessed above, it has been highlighted that DDoS attacks have become one of the biggest threats to the safety and security of online managed systems. These attacks greatly affect the development and growth of various network applications owned by organizations, especially in terms of the integrity of systems and data, customer base and revenue. Most of the research studies reveal that there is no single straightforward technique or countermeasure to completely prevent the threat or impact of a

DDoS attack. These attacks are constantly evolving and adapting, therefore it is impossible to find one fixed defensive technique that defends against all types of DDoS attacks. Continuous research and study on erupting DDoS attacks and defensive countermeasures needs to be done in order to find new and effective ways of defending against the impact that these attacks can inflict. Various techniques have to be continuously developed, evaluated and tested to determine if certain countermeasures would pose as a good fit to protect networks from such attacks, therefore this research study focuses on testing the extent at which an existing defensive technique can be effective in safeguarding a network from the impact of a DDoS attack.

6 Discussion

The change in each of the tested network performance metrics was measured and analyzed over a period of 30 seconds for each simulation test during the conduction of the experiment, as displayed in the graph visualizations of the results below. The results of the change in each network performance metric measured before and after the launch of the simulated DDoS attacks at each attack strength level with and without the implementation of the honeypot defense technique in the targeted network, is discussed below.

The normal change in the performance metrics of the targeted network before experiencing the effects of the launched simulated DDoS attacks, reflected an average throughput of 7 400 mbps, with an average network response time of 0.6 ms and an average packet loss percentage of 33%, as illustrated in the performance metric graph visualizations in figure 1 below.

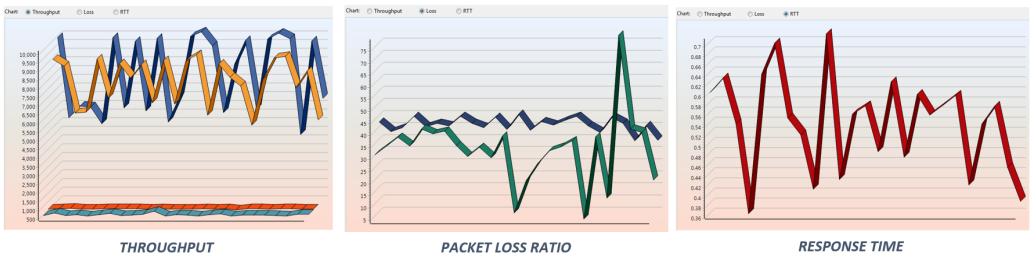

Figure 1: Normal change in the performance metrics of the targeted network

6.1 Throughput

The throughput (or bandwidth) of a network system is described as the amount of data that is successfully transmitted through a network from a source point to a destination point in a given amount of time. Throughput is usually measured in bits per second (bps). [47] The change in the normal average throughput of the target network reflected a significant drop after the launch of the simulated DDoS attack over the measured simulation test time of 30 seconds for each attack strength level, as displayed in figure 2 below. The average network throughput reflected a decrease of 100 mbps for the low strength rate attack and a decrease of 800 mbps for the medium strength rate attack. The high rate attack inflicted the most impact on the performance of the targeted network with a decrease of the average normal throughput by 925 mbps.

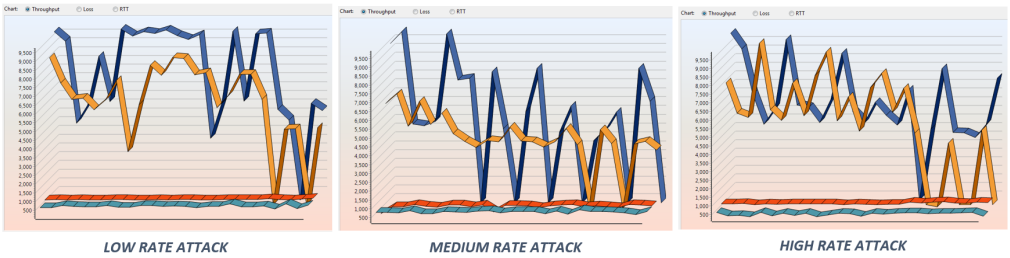

Figure 2: Change in network throughput with the launch of the simulated DDoS attacks at each attack strength level

6.2 Response Time

The network response time (or latency) of a network system refers to the amount of time that data sent through a network takes to reach its destination point from its source point. Network response time (or latency) is usually measured in miliseconds (ms). [47] The change in the normal average response time of the target network reflected a significant increase after the launch of the simulated DDoS attack over the measured simulation test time of 30 seconds for each attack strength level, as displayed in figure 3 below. The average network response time reflected an increase of 0.1 ms for the low strength rate attack and an increase of 0.2 ms for both the medium and high strength rate attack.

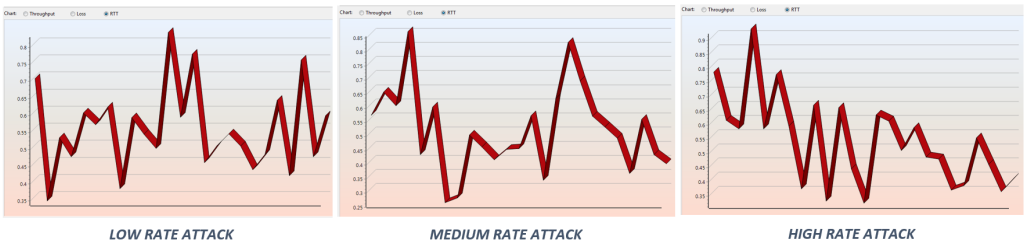

Figure 3: Change in network response time with the launch of the simulated DDoS attacks at each attack strength level

6.3 Packet Loss Percentage

The packet loss percentage is usually measured as a ratio percentage of the amount of packets that fail to reach their intended destination by getting lost or dropped during the transmission of data that is sent through a network. [47] The change in the normal average packet loss percentage of the target network reflected a significant decrease after the launch of the simulated DDoS attack over the measured simulation test time of 30 seconds for each attack strength level, as displayed in figure 4 below. The average network packet loss percentage reflected a decrease of 14.8% for the low strength rate attack, a decrease of 17.7% for the medium strength rate attack and a decrease of 20.25% for the high strength rate attack.

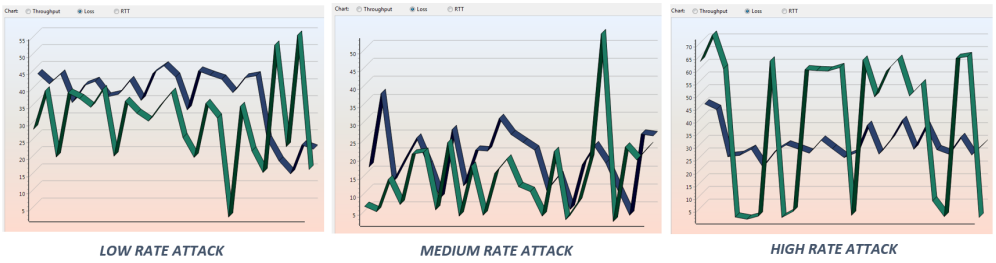

Figure 4: Change in network packet loss percentage with the launch of the simulated DDoS attacks at each attack strength level

Congestion forms a common cause of the result of dropped packets in a network. An increase in the packet loss percentage of a network could also be as a result of devices that intentionally drop packets that are sent to a

network to achieve specific purposes, such as routing or limiting the throughput of traffic sent to the network. [48]

Throughput is inversely proportional to the response time (or latency) and packet loss percentage performance metrics of a network, therefore the optimization of throughput involves the minimization of network response time and packet loss percentage, as an increase in the response time and packet loss percentage of a network decreases the average throughput and speed of the network, which results in the negative effect of the poor delivery of network performance to the intended users of the network.

The most common cause of an increase in the response time of a network involves multiple users attempting to make use of the services provided by a network at the same time, which decreases the throughput of the network and results in the negative effect of poor delivery of network performance to the intended users. Therefore, the launch of a DDoS attack to flood a targeted network with unsolicited traffic simulates the act of multiple users attempting to utilize the provided services of a network at the same time, which stresses the network, increases network latency and decreases the average throughput of the network, thus resulting in poor network performance. [49]

6.4 Change in network performance metrics with implementation of honeypot

Once the honeypot service was activated to defend and safeguard the targeted network against the launched attacks, the honeypot service managed to suppress the damage inflicted by the launched attacks on the targeted network by detecting, capturing and recording the attack traffic activity logs of the launched attacks at each attack strength level. The average throughput performance metric of the targeted network improved with an increase of 45 mbps for the low strength attack, 61 mbps for the medium strength attack and 66.5 mbps for the high strength attack after the tested period of 30 seconds for each simulation test conducted. The average network response time improved with a decrease of 0.1 ms for the low strength attack, 0.3 ms for the medium strength attack and 0.4 ms for the high strength attack.

These results indicate that the inclusion of the honeypot allowed the honeypot service to suppress the damage inflicted by the launched DDoS attack on the target network and slightly improve the performance of the targeted

network compared to the negatively affected performance of the targeted network when the attack was launched without the implementation of the honeypot defense technique.

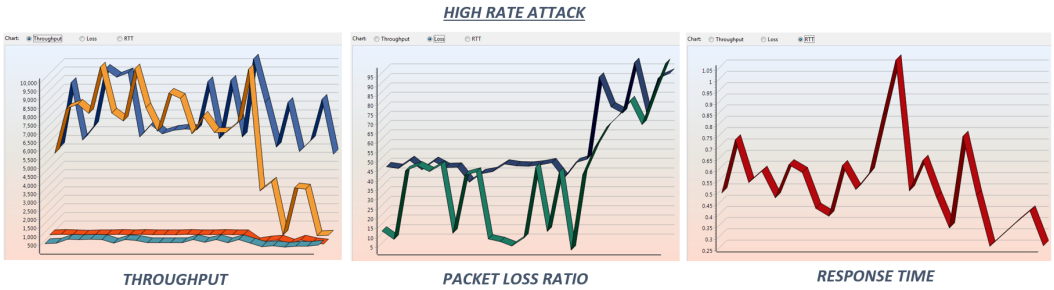

Figure 5: Change in network performance metrics with the launch of the simulated DDoS attacks and the implementation of the honeypot service

6.5 Final simulation test results

An implemented defensive mechanism used to defend against network security attacks should be able to remain active and functional in safeguarding the defended network for the entire period that the attack is launched towards the victim network for. The average time required for a DDoS attack to inflict mass damage on a targeted Local Area Network (LAN) system varies and is dependent on the type of DDoS attack developed.

The author of an article published on 'cisco' [50] mentions that 33% of most DDoS attacks last for a period of 60 minutes, while 60% of DDoS attacks last for a period of less than 24 hours and 15% of DDoS attacks can last for a period of up to one month. Therefore, a final simulation test was conducted to test the point at which the kfSensor hoenypot service would be able to maintain and fulfil its intended and expected functionality of safeguarding a targeted network against a DDoS attack by detecting and capturing the attack traffic activity logs of the simulated DDoS attack that is launched over an average tested time period of 60 minutes, which has been described as the time period that most DDoS attacks are executed towards a targeted network for.

The change in the performance metrics of the targeted machine was recorded and analyzed throughout the length of the conducted simulation test. Before the launch of the simulated DDoS attack, the normal average throughput of the targeted machine reflected a value of 3 500 mbps, with a normal average network response time of 0.7 ms and a normal average packet loss percentage of 35.25%. Figure 6 below illustrates graphs that represent the normal change in the victim machine's performance metrics before the conduction of the final simulation test.

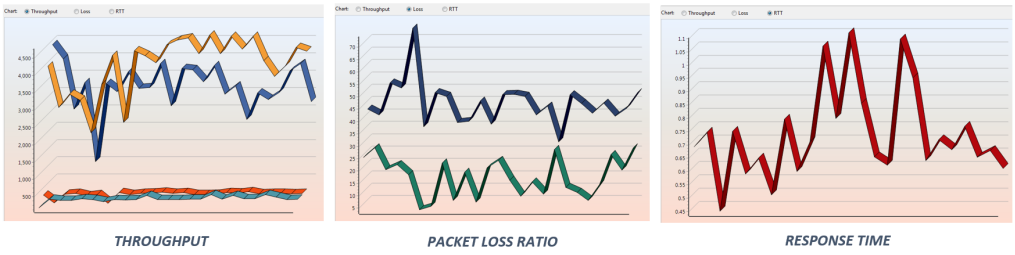

Figure 6: Normal change in the performance metrics of the targeted network

Within the first 30 minutes of the duration of the simulated test, the change in the average throughput performance metric of the victim machine decreased by 825 mbps. The average network response time decreased by 0.2 ms, where as the average packet loss percentage reflected a decrease of 1.9775%.

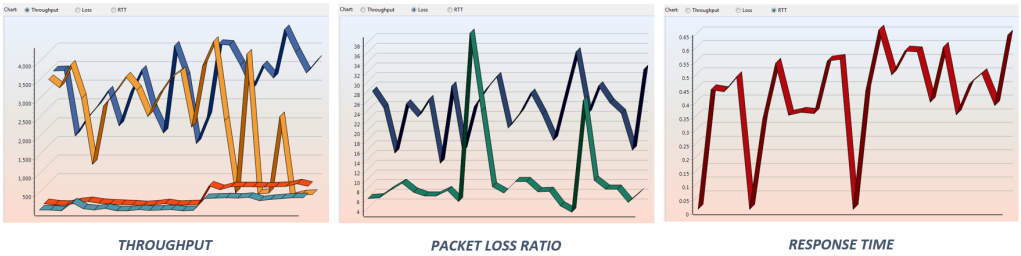

Figure 7: Change in network performance metrics within 30 minutes of final conducted simulation test

Upon conclusion of the 60 minute simulated test, the final change in the throughput performance metric of the targeted machine reflected an average value of 2 950 mbps, with the final change in the network response time reflecting an average of 0.5 ms and the final change in the packet loss percentage reflecting an average of 18.045%.

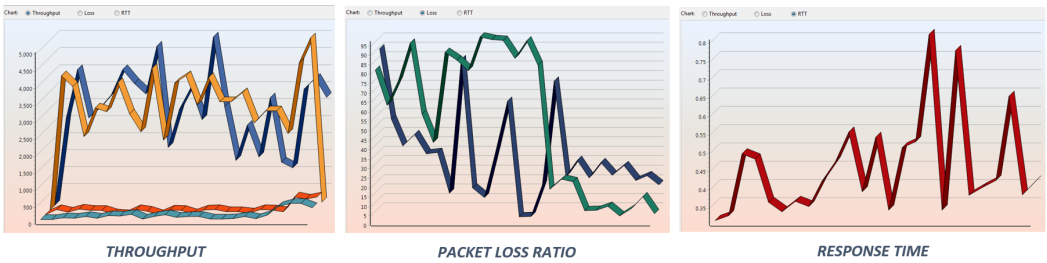

Figure 8: Change in network performance metrics upon conclusion of final simulation test conducted

The measurements, comparisons and results of each measured performance metric of the targeted network during the conduction of the experiment clearly illustrates and shows the negative effect that a launched DDoS attack has on the performance of a targeted machine once the attack is launched towards it. The results further illustrate that the implemented honeypot defense technique was able to withstand, mitigate and suppress the negative effect imposed by the attacks on the targeted network.

The kfSensor honeypot software service did not result in becoming compromised or non-responsive in fulfilling its expected and intended task of detecting, capturing and recording the activity logs of attacks launched towards the targeted network. The kfSensor honeypot service continuously captured and recorded attack traffic activity logs for the launched attacks in real time throughout the launch of the simulated DDoS attack over the final simulation tested time period of 60 minutes. Figure 9 below illustrates a snapshot of the recorded attack traffic activity logs that were captured by the kfSensor honeypot service upon the start and conclusion of the final 60 minute simulation test.

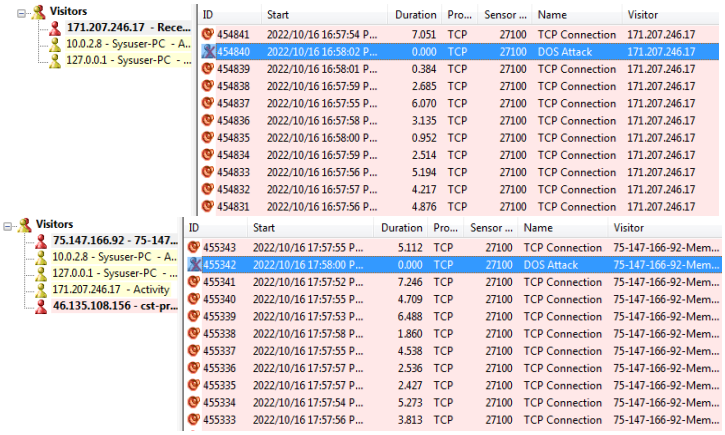

Figure 9: Snapshot of recorded attack traffic activity logs captured by the kfSensor honeypot service

Ralph Edward Sutton, Jr. mentions that one of the main goals of the utilization of a honeypot is to provide early warnings of potential attacks, identify flaws in constructed network security strategies, and improve the overall security awareness of an organization. It is further highlighted that a honeypot acts more as a detection and response tool, rather than a network security prevention tool. [51] The success of an implemented honeypot in a targeted system aims to falsely reassure attackers that they are not being monitored when engaging in the execution of attacks targeted towards a victim system.

Therefore failure to obtain, track and analyze these generated attack traffic event logs in the required amount of time, denies the owners of the attacked systems, such as a network administrator, with the ability to track, assess and better understand the activities, behaviours, trends and routines of attackers that launch these different types of attacks. This could also deny owners of attacked systems with the ability to discover what type of attacks or combination of attacks are launched and learn where the weaknesses of their systems exist that need to be redesigned in order to proactively set efficient defensive countermeasures in place to better prepare for the safeguarding of their network/s from such attacks in the future before more damage is inflicted towards the victim systems or to even take legal action against the attackers that continuously target systems to launch these different types of attacks towards. [19]

Although the tested honeypot service was able to safeguard the targeted

network against the launched simulated DDoS attacks by detecting and capturing attack traffic activity logs that owners of targeted systems can assess for further analysis to assist in better preparation for the implementation of defensive countermeasures to protect their victim systems from being vulnerable to experiencing the negative effects inflicted by these launched attacks, the effects inflicted by real and stronger DDoS attacks that are launched from multiple compromised attack machines directed at causing damage to a larger targeted Wide Area Network (WAN) system, such as the SANReN network, for a longer period of time, might be too much for a single standard honeypot service to fully safeguard and protect the targeted network against such attacks.

The experiment was not conducted to simulate and test the strength and effectiveness of a honeypot defense technique in defending against the effects inflicted by a DDoS attack on a complete and larger Wide Area Network (WAN), such as the SANReN network, but the experiment was rather conducted to simulate, measure, test and analyze the effectiveness of the utliization of a honeypot in defending against the effects that a launched DDoS attack would have on a smaller Local Area Network (LAN) that forms a part of a larger Metropolitan Area Network (MAN), such as the University of Pretoria Main Campus LAN, which forms a part of the larger SANReN MAN connections that are set across the city of Tshwane (Pretoria) in the Gauteng province.

It is therefore recommended to implement and make use of a stronger form of the proposed single standard honeypot defensive mechanism in a larger Wide Area Network (WAN) topology to defend the network against attacks, such as the proposed implementation of a honeynet by Hazem Sallowm et al. that consists of a combination of honeypots [29] or the implementation of a honeypot service that supports and allows a longer period of service availability and a larger limit for the number of unsolicited traffic packets received that can be detected and captured for the recording of attack traffic activity logs for launched attacks, in order to properly defend targeted systems against real and stronger variants or types of DDoS attacks.

7 Conclusion

Based on the results obtained from the conduction of this experiment to understand the ramifications of the effects inflicted by a DDoS attack on a targeted Local Area Network (LAN), it can be concluded that a LAN that is attacked and compromised by an attacker through a network security attack, such as a DDoS attack, will negatively impact the combined functionality and provision of services of the larger Wide Area Network (WAN) that it forms a part of, as services will be unable to be extended or provided to users in the particular region or area that the attacked and compromised LAN resides.

Therefore, users of the provided services in the compromised LAN region will be forced to relocate to another area that forms a part of the larger WAN, where services are running and not disrupted, such as moving to a different city or province in South Africa that has connections to the SANReN network, in order to access the services provided by the SANReN network. Users would also have to search for another area where services are functioning correctly or ask other users that are in areas with uninterrupted services to complete their respective tasks for them with the use of the available provided services in the specific area. This all adds an additional time and travel overhead cost to search for or move to another uninterrupted LAN region within the greater WAN, which denies users the freedom and comfort of making use of the provided LAN services in the area in which they are in or the area that they have relocated to for the specific reason of accessing the services provided in the specific hotspot area.

Unsolicited activities executed on a network are more likely to be detected by honeypots rather than other traditional intrusion detection systems, therefore honeypots can be used and combined with other existing network security attack defense mechanisms, such as firewalls, encryption or authentication services [11] to both record the activity logs of every launched attack, as well as properly safeguard targeted systems against launched attacks, thus increasing the efficiency of the security of victim systems. [52]

By studying the activities and behaviours of attackers, owners of vulnerable and targeted networks can track and go through an in-depth examination of the trends and routines of attackers and their attacks both during and after the launch of these attacks [30] to better create and implement more suitable and secure defensive systems that can potentially allow targeted networks to become less vulnerable to experiencing the negative effects inflicted by future attacks, such as the loss of network services provided to users or loss

of system data and business revenue. [51]

The results obtained through the conduction of this experiment can be used by organizations to determine whether the honeypot defensive technique would act as an effective and efficient solution to implement in their respective network topologies for the safeguarding of their networks from such attacks. The proposed honeypot defensive technique can also be compared against other defensive mechanisms by organizations to determine which technique would be a stronger best fit option to use in strengthening the safety and security of their networks.

Proposed future work can be focused on the implementation and testing of the strength and effectiveness of an enhanced version of the proposed single standard honeypot defensive technique as stated earlier, in safeguarding a network in a larger Wide Area Network (WAN) topology against the impact of real and more severe DDoS attacks that are launched from multiple compromised attack machines over longer periods of time.

References

[1] M. A. Dennis, "Definition of the Internet." Online: https://www.britannica.com/technology/Internet/Foundation-of-the-Internet, 2022. Accessed: May 15, 2022.

[2] N. Innab and A. Alamri, "The Impact of DDoS on E-commerce," 2018.

[3] Javapoint, "Computer Network Types." Online: https://www.javatpoint.com/types-of-computer-network, 2021. Accessed: May 17, 2022.

[4] A. Bhardwaj, G. Subrahmanyam, V. Avasthi, H. Sastry, and S. Goundar, "DDoS Attacks, New DDoS Taxonomy and Mitigation Solutions – A Survey," 2016.

[5] P. Networks, "Computer Network Types." Online: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos, 2022. Accessed: May 17, 2022.

[6] SABEN, "About SABEN." Online: https://www.saben.ac.za/about/#:~:text=A%20National%20Research%20and%20Education,every%20corner%20of%20the%20globe., 2022. Accessed: May 20, 2022.

[7] M. Foley, "The Role and Status of National Research and Education Networks (NRENs) in Africa," 2014.

[8] N. SANReN, "SANReN (the network & the group)." Online: https://www.sanren.ac.za/relationships/, 2020. Accessed: May 20, 2022.

[9] Abhishta, R. van Rijswijk-Deij, and L. J. Nieuwenhuis, "Measuring the Impact of a Successful DDoS Attack on the Customer Behaviour of Managed DNS Service Providers," 2018.

[10] A. Munshi, N. A. Alqarni, and N. A. Almalki, "DDoS Attack on IoT Devices," 2020.

[11] H. A. Deshpande, "Honeymesh: Preventing distributed denial of service attacks using virtualized honeypots," *International Journal of Engineering Research & Technology (IJERT)*, vol. 4, no. 8, pp. 263–267, 2015.

[12] K. Kumar, M. Sachdeva, and G. Singh, "An Emulation Based Impact Analysis of DDoS Attacks on Web Services during Flash Events," 2011.

[13] Oracle, "Oracle VM VirtualBox." Online: https://www.virtualbox.org/, 2007. Accessed: August 01, 2022.

[14] kfSensor, "kfSensor: Advanced Windows Honeypot System." Online: http://www.keyfocus.net/kfsensor/, 2022. Accessed: September 30, 2022.

[15] B. Posey, "SolutionBase: Configuring a Honeypot for your network using KF Sensor." Online: https://www.techrepublic.com/article/solutionbase-configuring-a-honeypot-for-your-network-using-kf-sensor/, 2005. Accessed: August 12, 2022.

[16] M. Sachdeva1, G. Singh, K. Kumar, and K. Singh, "Measuring Impact of DDOS Attacks on Web Services," 2010.

[17] H. Moore, "Metasploit: The World's Most Used Penetration Testing Framework." Online: https://www.metasploit.com/, 2003. Accessed: September 12, 2022.

[18] H. Moore, "Metasploit Framework." Online: https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/, 2003. Accessed: September 12, 2022.

[19] N. Weiler, "Honeypots for Distributed Denial of Service Attacks," 2002.

[20] S. M. Hussain and G. R. Beigh, "Impact of DDoS Attack (UDP Flooding) on Queuing Models," 2013.

[21] M. Poongothai and M. Sathyakala, "Simulation and Analysis of DDoS Attacks," 2012.

[22] P. Security, "DDoS Top 6: Why Hackers Attack." Online: https://www.pentasecurity.com/blog/ddos-top-6-hackers-attack/, 2016. Accessed: August 15, 2022.

[23] TechInsurance, "How much will a DDoS attack cost your small business?." Online: https://www.techinsurance.com/resources/ddos-small-business-costs#:~:text=DDoS%20consequences%20can%20include%20significant,and%20jeopardize%20future%20business%20opportunities, 2022. Accessed: August 15, 2022.

[24] kaspersky, "Distributed Denial of Service: Anatomy and Impact of DDoS Attacks." Online: https://usa.kaspersky.com/resource-center/preemptive-safety/how-does-ddos-attack-work, 2022. Accessed: August 15, 2022.

[25] J. Burgess, "Modern DDoS Attacks and Defences - Survey," 2016.

[26] Y. Chen, K. Hwang, and W. Ku, "Collaborative detection of ddos attacks over multiple network domains," *EEE Transactions on Parallel and Distributed Systems*, vol. 18, p. 649 – 1662, Dec. 2007.

[27] M. M. Chawan., "Jamming attacks and their prevention in wireless networks," *International Journal of Latest Engineering Research and Applications*, vol. 2, no. 6, pp. 59–63, 2017.

[28] P. A. R. Kumar and S. Selvakumar, "Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms," 2009.

[29] H. Sallowm, M. Assora, M. Alchaita, and M. Aljnidi, "A hybrid honeypot scheme for distributed denial of service attack," *Electrical and Computer Engineering*, vol. 1, no. 1, pp. 33–39, 2015.

[30] N. Provos, "Honeyd: A Virtual Honeypot Daemon," 2003.

[31] N. SANReN, "The South African NREN." Online: `https://www.sanren.ac.za/south-african-nren/`, 2020. Accessed: May 20, 2022.

[32] TENET, "TENET — Tertiary Education & Research Network of South Africa." Online: `https://www.tenet.ac.za/`, 2022. Accessed: August 15, 2022.

[33] N. SANReN, "South African NREN Metropolitan Networks." Online: `https://www.sanren.ac.za/metropolitan-rings/`, 2020. Accessed: May 20, 2022.

[34] TENET, "Traffic Graphs for SANReN-TENET Network." Online: `https://graphs.tenet.ac.za/iris/api2/tenet/home`, 2020. Accessed: August 15, 2022.

[35] N. SANReN, "SANReN Services." Online: `https://www.sanren.ac.za/services/`, 2020. Accessed: August 15, 2022.

[36] SAFIRE, "Current Service Providers." Online: `https://safire.ac.za/participants/sp/list/`, 2022. Accessed: August 15, 2022.

[37] ASREN, "How NRENs support the COVID-19 Research Platform." Online: `https://asrenorg.net/?q=content/how-nrens-support-covid-19-research-platform`, 2021. Accessed: May 15, 2022.

[38] K. Kumar, *Protection from Distributed Denial of Service (DDoS) Attacks in ISP Domain*. PhD thesis, Indian Institute of Technology, 2007.

[39] N. Innab, H. Al-Rashoud, R. Al-Mahawes, and W. Al-Shehri, "Evaluation of the effective anti-phishing awareness and training in governmental and private organization in riyadh," in *21st Saudi Computer Society National Computer Conference (NCC)*, 2018.

[40] L. Wenliang and H. Wenzhi, "DDOS Defense Strategy in Software Definition Networks," 2019.

[41] S. R, P. Benoor, and A. Kanavalli, "Mitigation of DDoS attacks in Software Defined Networks at application level," 2019.

[42] Z. S. Taghavi, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE communications surveys and tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[43] X. Liang and T. Znati, "An empirical study of intelligent approaches to DDoS detection in large scale networks," 2019.

[44] Y. You, "A defense framework for flooding based DDoS Attacks," 2007.

[45] H. Abdullah, "A Risk Analysis And Risk Management Methodology For Mitigating Wireless Local Area Networks (WLANs) Intrusion Security Risks," 2006.

[46] R. Maciel, J. Araujo, C. Melo, P. Pereira, J. Dantas, J. Mendonca, and P. Maciel, "Impact Evaluation of DDoS Attacks Using IoT Devices," 2021.

[47] A. Lamberti, "How to Measure Network Performance: 9 Network Metrics." Online: `https://obkio.com/blog/how-to-measure-network-performance-metrics/`, 2022. Accessed: September 20, 2022.

[48] Opsview, "What Is Packet Loss And How Does It Affect Your Network?." Online: `https://www.opsview.com/resources/network/blog/what-packet-loss-and-how-does-it-affect-your-network#:~:text=What%20are%20the%20affects%20of,of%20a%20requirement%20for%20accuracy`, 2022. Accessed: September 20, 2022.

[49] D. Stuff, "What Is Throughput in Networking? Bandwidth Explained." Online: `https://www.dnsstuff.com/`

network-throughput-bandwidth, 2019. Accessed: October 09, 2022.

[50] cisco, "What Is a DDoS Attack?." Online: https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html, 2022. Accessed: October 09, 2022.

[51] J. Ralph Edward Sutton, "How To Build and Use a Honeypot." Online: https://docplayer.net/7151974-Honeypot-as-the-intruder-detection-system.html, 2014. Accessed: July 15, 2022.

[52] K. Shridhar and N. Gautam, "A prevention of ddos attacks in cloud using honeypot," *International Journal of Science and Research (IJSR)*, vol. 3, no. 11, pp. 2378–2383, 2014.

[53] D. Gautam and P. V. Tokekar, "An Approach To Analyze The Impact Of Ddos Attack On Mobile Cloud Computing," 2017.

[54] A. Balobaid, W. Alawad, and H. Aljasim, "A Study on the Impacts of DoS and DDoS Attacks on Cloud and Mitigation Techniques," 2016.

[55] M. Jiang, C. Wang, X. Luo, M. Miu, and T. Chen, "Characterizing the Impacts of Application Layer DDoS Attacks," 2017.

[56] V. Kansal and M. Dave, "Proactive DDoS Attack Detection and Isolation," 2017.

[57] O. Yevsieieva and S. M. Helalat, "Analysis of the Slow HHTP DOS and DDOS Attacks on the Cloud Environment," 2017.

[58] A. Abhishta, R. Joosten, S. Dragomiretskiy, and L. J. Nieuwenhuis, "Impact of Successful DDoS Attacks on a Major Crypto-currency Exchange," 2019.

[59] M. A. Saleh and A. A. Manaf, "Optimal Specifications for a Protective Framework Against HTTP-based DoS and DDoS Attacks," 2014.