FACULTY OF SCIENCE, ENGINEERING AND COMPUTING

School of Computer Science and Mathematics

BSc (Hons) DEGREE
IN
Cyber Security and Digital Forensics

Sahib Ghataura

K2015104

DDoS Mitigation and Prevention Technique Review
03/05/23

GC. Deepak

Kingston University London

Declaration

I have read and understood the University regulations on plagiarism, and I understand the meaning of the word *plagiarism*. I declare that this report is entirely my own work. Any other sources are duly acknowledged and referenced according to the requirements of the School of Computer Science and Mathematics. All verbatim citations are indicated by double quotation marks ("…"). Neither in part nor in its entirety have I made use of another student's work and pretended that it is my own. I have not asked anybody to contribute to this project in the form of code, text, or drawings. I did not allow and will not allow anyone to copy my work with the intention of presenting it as their own work.

Date: 03/05/23

Name: Sahib Ghataura

Signature: SahibG

Table of Contents

List of figures and tables

Glossary of terms

Denial of Service (DoS): A DoS attack is launched only at a small number of IT devices, usually just one. The procedure behind this attack is to disrupt the normal flow of network traffic of the victim server by loading fake traffic to a device connected to the internet, rendering the connection to the network meaningless due to clutter in the service.

Distributed Denial of Service (DDoS): A DDoS attack is a variant of a DoS attack that uses multiple IT devices/systems to completely flood the target's network with a large amount of traffic, similar to the DoS attack, which will overwhelm the target making any connection inaccessible. This is much harder to defend against since its against multiple sources.

Prevention: A strategy that is used to defend against cyber threats. It involves taking action and implementing defences against cyber threats before any attack occurs.

Mitigation: Another strategy that is used to defend against cyber threats. Instead of taking action before the attack, mitigation refers to limiting the damage of an attack that has already taken place. The most notable example of this would be any incident response plan.

Cloud-Computing: Cloud computing is a virtual storage space with resources and applications provided by the organisation that is available whenever the user has access to an IT device. In cloud computing, instead of owning and managing their computing resources, users can access them from cloud service providers.

Network: A group of interconnected IT devices that communicate with each other to share information or connect to the internet. Various communication channels, such as cables, wireless connections and satellites, can connect the network. Networks are used in many different settings, like homes, offices, schools, hospitals and, most importantly, organisations. Networks, as a whole, provide communication and information sharing amongst devices.

Attacker: An attacker in the cyber-security space is attempting to exploit weaknesses and vulnerabilities within IT devices, networks or applications. There can be many motivations; however, they are typically for malicious reasons.

Target: A target in the cyber-security space is someone who is a victim or potential victim of a cyber attack. Targets can vary, ranging from individuals to businesses to sometimes even

whole organisations. Once a target has been selected, attacks can launch various cyber-attacks. Therefore, since anyone can be a target, having prevention and mitigation strategies in place is essential.

1. Introduction and Background

1.1 Introduction

This project will extensively cover one of the most prevalent cyber attacks, the Distributed Denial of Service, commonly called DDoS. This project will be a full review-based report covering all the information needed about the DDoS attacks. The content that will mainly be covered will include, what a DDoS attack is, a brief history of the attack, the different types of DDoS attacks and prevention tools/techniques that can be used to mitigate these attacks. To wrap things up, in the end, there will be an artefact demonstrating how it works, with all the steps covered in a review.

1.2 Background

This type of attack originated in 1996 when Panix, a known internet service provider at the time, was offline for several days by an SYN flood, a type of DDoS technique that has skyrocketed DDoSing as a whole into popularity in the cyber world for years to come (Nicholson, 2022).

Now, Cisco, a known digital communications technology company, has predicted that the attack will increase from 7.9 million in 2018 to 15.4 million in 2023. The value has doubled in only five years; this is truly representative of the increase in internet users in 2023, which is 5.3 billion, i.e., 66% of the global population (Cisco, 2020).

This prolific increase in the frequency of DDoS assaults may be caused by various causes, including a lack of adequate security and defences, the pursuit of financial gain, or even revenge. All of these arguments have their origins in malicious intent, and there is no way that anything positive could result from this situation.

Since this project is about DDoS, a large part naturally involves cloud environments. Following this, some background information on cloud environments will be discussed.

This has seen a significant increase in usage in the last couple of years due to the service's usefulness and stability for efficient work being acknowledged. As of 2022, 94% of

companies utilise cloud environments, this is a considerable statistic, but it is also important to note that this can be partially due to the global pandemic covid-19 in 2020, having an increase of 61%. This was because commuting to workspaces and offices would have been difficult (Flynn, 2022). When a virtual workspace like this is targeted by a cyber attack such as DDoS, it will unfold like any other attack; the connection to the environment will be impossible to connect to.

This means there are more businesses that a vulnerable to DDoS attacks. That is why it is essential that there is a proper education and defences in place for these companies. It is only suitable to assume that their workload and production rate would take an unprecedented hit if a disruption such as DDoS occurs.

1.3 Aims and Objectives

The aims and objectives of this project have been broken down into clear goals in this section:

- Provide a detailed study of what a DDoS attack is
- Research and provide details on prevention and mitigations tools/techniques
- To research and provide information on the most prevalent DDoS tools.
- Detailed demonstration of two DDoS attacks being simulated through the use of virtual machines
- Comparison and Discussion on how both tools performed.

This project aims to provide a complete educational guide on the DDoS cyber attack. It will provide helpful information and demonstrate an attack at work in the artefact. This will include a comprehensive analysis of what takes place in that scenario.

1.4 Stakeholders Analysis

The stakeholders of study are individuals or groups of people that will either contribute to the development of this project or be assisted by the data and information provided throughout. This will create a higher level of interest for them due to various reasons, such as the field they are in or past experiences they have had to do with this problem. It all

depends on the level at which they are at. This particular project was developed with the help of an academic advisor to provide guidance and direction in some areas of this project. The information used throughout was all provided by credible sources, some of which were articles created by other professionals in this field.
For the demographic of this project, it can be for anyone. It can be suited for individuals in the field and small groups. However, it will mainly be dedicated towards larger businesses and organisations that are vulnerable to losing more in a DDoS attack.

1.5 Ethics and Legality

For the ethics of the project, DDoS attacks are important to mention. According to the computer misuse act 1990, it is against the law to interfere with someone else's computer device or prevent access to data/programs when not registered to do so; the only exception is if authorized. No matter the target, organisations, businesses or individuals, DDoS attacks can cause great harm. This is why it is seen as one of the most unethical acts in the entire industry.

In the case of this project, everything will be approved by the university because this is a review-based project. All activities and simulations throughout this project will not harm anyone and are regulated and safe because this is only a study. It is purely for educational purposes (National Crime Agency, 2020).

1.6 Conclusion

The internet has become part of the foundation for this world. This includes individuals, but also organisations and businesses. This is why it is a problem to have DDoS attacks increasing when there is also the rise of online spaces that can be penetrated. These potential targets must take this threat seriously because it can be a detriment to them; defences must be in place to counter this issue. This report has been created to provide the reader with the necessary knowledge to prevent such an attack.

2 Project Management Strategy

An appropriate project management plan must be in place to approach this project while keeping track of the work rate and duration of each task. A plan would ensure that the structure and scope of the entire progression were preserved along the way. The solution was to select a few time management tools and techniques for this project. Everything that needed to be done was covered whilst calculating the duration it would take to complete before the deadline. This section's primary goal is to cover the project management side.

Due to its linear nature and clarity, better built for individual projects, the waterfall technique was selected. There were numerous reasons why this was chosen. However, the most important one was that this technique could provide great flexibility and freedom to complete activities at their own pace.

In order to better visualise the timetable for the project, there was the use of a Gantt chart. The Gantt chart was a significant part of this project's management because it displayed an ideal start and end of each task involved in its progression. When creating a Gantt chart, it is essential to consider any potential delays or errors that may reduce the work rate. An approximate schedule of all the significant events that will take place throughout this project was constructed with the help of the Gantt chart.

The Gantt chart (shown in Figures 1 & 2 below) highlights every primary task that is partaken in this project, each task has a labelled start date and a duration of days expected to be completed. The tasks are almost split up into three main sections: research, report and artefact and analysis. Whilst the tasks are not split up into sections like that, they can be viewed in that way by understanding each task's intention. Each section and the tasks within the sections will be covered now.

The research stage: This stage involves tasks 1-4 of the Gantt chart. This is the primary stage of the project in which research and information gathering occurs. The information researched here will be beneficial later on because it gives an idea about the topic as a whole. This stage primarily involves researching the topics and brainstorming artefacts.

The report and artefact stage: This stage involves tasks 5-8 of the Gantt chart. This stage is mainly focused on completing the earlier stages of the report and writing all the information that does not require the artefact to be completed to fill in. This is the earlier bulk of the report out of the way. It ends with the development and completion of the artefact.

The analysis stage: This stage involves tasks 9-14. This stage is significantly longer than the others, but it contains all the challenges that can only be overcome by completing the entire artefact. At this point, the focus is primarily on conducting an analysis of the artefact and concluding the project with a presentation to the viva examiners.

Task ID	Task	Start Date	Duration (Days)
1	Project Proposal	09-Nov	7
2	Research into DDoS Attack Tools	16-Nov	14
3	Research into DDoS Prevention Tools	30-Nov	14
4	Research into Artefact	14-Dec	14
5	Demonstration	28-Dec	14
6	Report- Introduction and Background	11-Jan	14
7	Report- Project Management	25-Jan	7
8	Develop Artefact	01-Feb	28
9	Report- Literature Review	01-Mar	7
10	Report- Methodology	08-Mar	7
11	Report- Implementation of Artefact	15-Mar	7
12	Report- Critical Review	22-Mar	7
13	Report- Conclusion	29-Mar	14
14	Viva to present	12-Apr	7

Figure 2: Gantt Chart Task Allocation

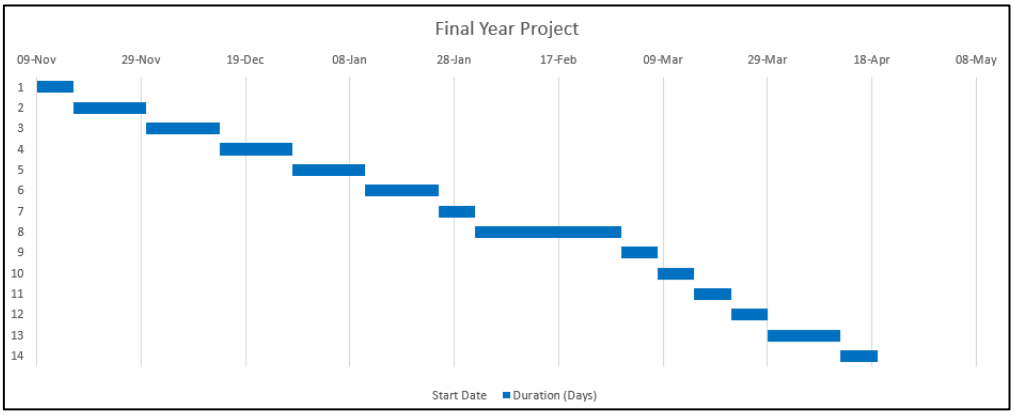

Figure 1: Gantt Chart

The Gantt chart was used for the significant stages of this project; however, for the individual tasks, there was the use of Trello in this project. *Trello* is a web-based project management tool based on Kanban boards used to organise different tasks, whether they need to be done, in progress or completed. This web app allowed for precise task tracking and proper workflow. This was solely used for each section's smaller and more intricate tasks throughout the project. This is shown in Figure 3.

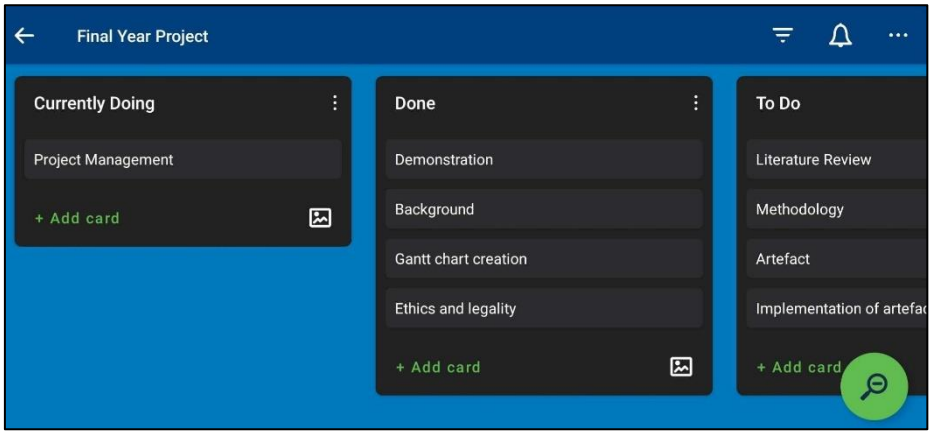

Figure 3: Trello Final Year Project Example

With the combination of the waterfall technique, Gantt chart and Trello tools, an adequate level of management is needed for the entirety of this project, up until the conclusion. These project management strategies coincide very nicely with each other as there will not be any interference.

Before selecting these techniques a few alternatives were up for debate; for example, the agile methodology was under consideration against the chosen waterfall methodology. Whilst both these techniques are good, they are very different. The deciding factor was just about what suited this project more between the two. It was clear that waterfall is simply the better fit for a clear-cut goal and timeline. It offers a lot more of a structured and foreseeable approach. In contrast, agile is more suited towards projects that need adaptability and have changing requirements. It also seemed that waterfall is the better method for an individual project since there are precise requirements and an understanding of what is needed for the final goal.

3 Literature Review

This section reviews some of the most well-known tools and software to conduct or protect systems against DDoS attacks. There will be an in-depth review of both sides of this, where they will fully be elaborated upon, whilst taking notes of their advantages and disadvantages. There will also be some extra research deemed important to know regarding DDoS.

A study conducted by Opeyemi Osanaiye, Kim-Kwang Raymond Choo, and Mqhele Dlodlo (Osanaiye, Choo and Dlodlo, 2016), highlights common attack trends and defences about the DDoS mitigation framework. The article reviews 96 recent publications on the DDoS attack and the defence approach to counter the issue. It examines DDoS attacks and mitigation methods and proposes a taxonomy and the change-point detection-based cloud DDoS mitigation system. There is a great emphasis on the need to mitigate these attacks due to the heavy influx of popularity of the cloud environment's shared resource architecture. According to the article, DDoS attacks can be categorized into two different levels of attacks. Application-bug-level attacks and infrastructure-level attacks. Application-bug-level attacks often target the system's hardware and software vulnerabilities, taking advantage of potential vulnerabilities. In contrast to this, an infrastructure-level DDoS attack would target anything that could be related to cloud computing; this includes components such as storage, network bandwidth, CPU and TCP buffers.
This article also covers some common motivations and goals behind DDoS attacks, including revenge, extortion, political disagreements, and testing.

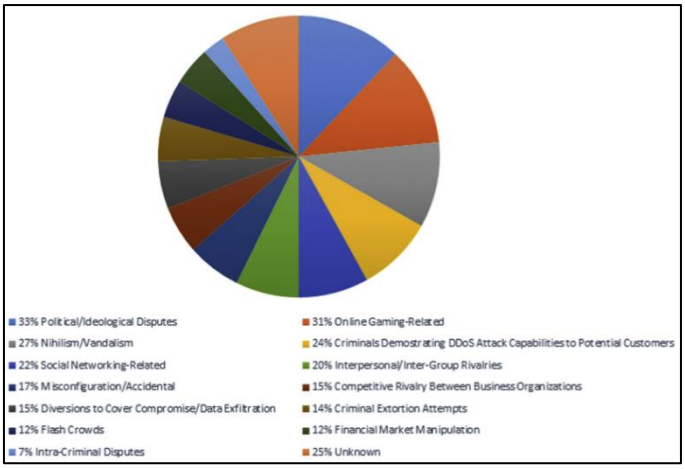

Figure 4: Motivation's behind DDoS attacks

This article goes into some of the tools that are most used by attackers. It explains how these attacks and tools can be used to penetrate networks and systems.

Now there will be an review on some of the most popular types of DDoS attacks and analyzing them by creating a table of advantages and disadvantages they have against each other.

3.1 DDoS Attacking Tools and Applications

- Low Orbit Ion Cannon (LOIC)- This is an open-source attack application. It sends many packets towards its target, rendering them completely useless. The packets that are supported: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and HTTP GET (HTTP flood attacks). (Cloudflare, 2020)

- High Orbit Ion Cannon (HOIC)- Alternative to LOIC that offers higher packet volume and complexity; it is simpler to carry out large-scale web-based attacks in a shorter amount of time, and these attacks would be more challenging to identify, even by some firewall systems. Packets that are supported: HTTP GET and POST requests. (Cloudflare, 2020)

- HTTP Unbearable Load King (HULK)- HULK attacks servers by sending requests that seem legitimate. Due to its capacity to deliver obscured traffic that is difficult to detect, HULK effectively carries out DDoS attacks. These techniques can create attacks that can be challenging to stop. Packets that are supported: HTTPS.(Wallarm, 2019)

- HPING3 – This tool is primarily built for legitimate purposes like network debugging. However, it can be used for DDOS attacks. HPing3 can launch DDoS attacks by overwhelming target systems with a flood of packets. It makes use of specific encryption- and anonymity-based mechanisms. Packets that are supported: TCP, UDP, and ICMP. (Kali, 2022)

The following is a table that details all of the benefits of the tools that are used to attack as well as their limitations against each other. (Kali, 2022)

3.1.1 Tools and Applications Technology Comparison table

Tool	Benefits	Limitations
LOIC	• Has a reputation for being easier to use; someone will less knowledge about the attack would be able to figure it out. • Allows the users to change the attack parameters however they wish; they can change the IP addresses, ports, and the contents they are sending. • Available for anyone to download since it is an open-source tool.	• Has become a standard attack, meaning many organizations and companies have implemented countermeasures against this. • Simple to use but can be complicated to use for someone without technical knowledge about these kinds of tools • Works by focusing on a singular target, making it relatively simple compared to the other tools.
HOIC	• The upgraded version of LOIC because it has the feature to send attacks from different sources at once. It is much harder to defend against. • Like its predecessor LOIC, HOIC is incredibly simple for someone who does not understand as much. • Can be used for testing, so users can test their networks against this type of DDoS attack to ensure their resistance.	• Provides the attacker with anonymousness, but they still are not entirely protected since the users are still able to be traced. • Does not support large-scale DDoS attacks, as it was built for more isolated, individual attacks. Like LOIC. • Defences have adapted to respond and detect these DDoS attacks before any severe damage is taken.

HULK	• Can be used to focus on web servers more than anything else because HULK is built to focus on HTTP services. • Easy for ethical hacking purposes, users can use it to test their systems. • Creates many requests from unique users. It will be more difficult for the system to track and block all that malicious activity.	• Open-source tool, so relies on the community to support it. May hinder the updates. • Primarily designed for personal attacks instead of anything more significant scale. • Decent network defences can counter HULK's usefulness and would be able to prevent an attack.
HPING3	• Effective against unorganized servers but can cause much downtime for the user and server. • Incredibly effective in a pen-testing/ethical hacking environment. • Easy to use for someone who doesn't have extensive knowledge about this.	• Targets independent vulnerabilities in web servers if the servers have been updated/patched. • Will have to rely on other unique commands for protection against being traced back.

Table 1: Tools and Applications Technology Comparison

Now that the DDoS attacks have been covered, the tools that are used to defend against them will be covered.

3.2 DDoS Protection Tools and Techniques

Another study by a group of professionals in the field (Alhijawi et al., 2022), includes a survey about DoS/DDoS mitigation techniques in software-defined networks (SDN). This study aimed to provide a review of potential advances of Denial of service against SDN and how they would be mitigated. The survey categorises all the research accumulated from 2013 to 2020 into six different types of mitigation techniques:

Table-entry-based solutions: A proposed systematic method of comparing two components. General strategy and eviction algorithm to have control over the flow table entries; this

includes rate limiting and timeout adjustment. A packet checker will be used to analyse and distinguish the difference between malicious and regular packets by giving the controller permission to validate original traffic sources by viewing logs.

Scheduling-based solutions: Involvement of implementing a scheduler module with the control layer to manage flow requests that are processing and maintaining a smaller number of queues to keep control and be able to detect DDoS attacks on the SDN.

Architectural-based solutions: This solution is based on all the roles of SDN components. The backup controller pool handles attacks against a distributed SDN controller. The parallel flow installation model modifies the controller to install parallel flow rules instead of linear installation. Hierarchical role-based controller architecture uses multiple controllers to boost and decrease flow processing capacity. The MTD manager monitors the bandwidth and traffic load of the master controller to detect DDoS attacks.

Flow Statistics-based solutions: This solution utilises statistical models based on the frequency of different captured features tested to mitigate DoS attacks. A range of techniques is used, such as analysing a network user's behaviour, monitoring the network traffic to detect any anomalies, restricting the bandwidth of switches that have been previously attacked to measure the randomness of incoming flows.

Machine learning-based solutions: This solution focuses on building and training a model to detect and mitigate systems against attacks automatically. The way this solution is constructed is by using a training dataset; this dataset should include a collection of instances defined using a set of features and associated labels.

Hybrid solutions: This solution is typically a combination of two previously mentioned solutions. An example would be flood defender, which combines table-miss engineering, packet filter and flow rule management techniques. All these techniques will work together to protect against DoS attacks.

3.2.1 System configurations that can help against DDoS attacks

This section will cover several operating system configurations that can help mitigate DDoS attacks' impact. These will not include any external services or software that will be able to be done by the system/router of the target.

Firewall

Firewalls are network security devices that can control and filter traffic in and out of the network according to the organisation's security policies. The goal of a firewall is to allow harmless traffic to enter whilst preventing dangerous traffic from entering the network. A firewall is typically viewed as a barrier between a private network, such as homes and offices, compared to more public spaces. (Cisco, 2019)

Rate Limiting

Rate limiting controls the network traffic by limiting the frequency of specific actions within a set amount of time. This can filter out certain types of malicious bot activities. An example of this is trying to log into an account or resetting a password. Whilst this defence does offer benefits, it is only partially full-proof when it comes to countering malicious activities. (Cloudflare, 2021)

IP spoofing Protection

IP spoofing is sending packets with modified source addresses to hide to sender's identity or potentially frame another IT device. Attackers often use IP spoofing to target large organisations and businesses with DDoS attacks. It is recommended that organisations configure their operating systems to protect against IP spoofing. This can help prevent attackers from disguising their IP addresses and bypassing security measures. (Cloudflare, 2019)

Network Isolation

Network Isolation involves dividing the network into separate sections called virtual local area networks (VLANs). These divides are established based on the functionality or assets

that are deemed upon them by the organisation. An increasing number of organisations are making their way to implementing segmented networks; however, it is essential to note that this strategy may be expensive. (Knight, 2020)

Now there will be coverage of Cloud-based DDoS protection services that are available for customers to buy. These tools/services are a lot more likely to be bought by an organisation or company because they all cost, and for an established company, it will be better to have a well-known and prominent service instead of a few network configurations set up by an IT staff member. A description of each and a table will be provided of the advantages and disadvantages they have against each other. These tools and applications are all DDoS protection services that are capable of automatically detecting and mitigating any anomalies or unusual traffic.

3.2.2 Cloud-based DDoS protection services

- SolarWinds Security Management System- This system tracks traffic and prevents attacks instead of relying only on local firewalls and traditional IP filters. When it detects garbage traffic, this system can generate emergency alerts, block requests, and maintain server traffic flow.

- Cloudflare- Cloudflare practically pioneered the modern DDoS service. Many firms choose it as their top option because of the company's enormous capacity to absorb extremely significant traffic floods. Although it began as a DDoS defense service, Cloudflare has grown into additional edge services and can now combine DDoS defense with malware defense, content delivery, and failover defense.

- Amazon Web Services (AWS) Shield- Amazon Shield is undoubtedly intended to be a competitor to Cloudflare. Its free tier is a significant marketing benefit when attempting to attract small business consumers. The AWS Shield has one feature, which makes it less appealing. In other words, the EC2 system and other AWS accounts are the only ones this solution is intended to protect, since it gets rather costly with membership tiers.

- Link11- This is a specific DDoS defense system. The technology is well-known for promptly identifying DDoS attacks. No one wants legitimate traffic to be slowed down or banned, therefore a DDoS security system's capacity to operate quickly and accurately identify fraudulent traffic can make or break it. Link11 enhances its DDoS blocking service with AI.

The following is a table that details all of the benefits of the tools used to protect against DDoS attacks and their limitations against each other.

3.2.3 Cloud-based DDoS protection services Technology Comparison table

Tool	Benefits	Limitations
SolarWinds Security management System	• Can set up automation to block malicious behaviour, such as any unknown packets or intrusion attempts. • Can offer a decent range of integrations for the user to collect data, unusual behaviours and attempts of intrusion • It offers the user various templates and monitors, making it simple for them to start immediately.	• Designed for larger networks of devices, so small groups/individuals couldn't fully utilize the software. • Rather complex, so it would require a decent amount of time to understand and learn how to use it. • Can be an issue with cost as the build, software, hardware, and additional cost from ongoing maintenance would accumulate.
Cloudflare	• Has an impressive reputation, as it is known to have mitigated some of the most significant attacks in history. • Offers a variety of packages; therefore, it's suitable for different environments. • It has a variety of edge locations to keep all the data available to the user during an attack.	• There is a decent learning curve for this compared to some of its competitors. • Does not display performance analytics when there are no attacks detected. • Limited control over how much of the data is cached by the user. This can result in unnecessary storage space being taken up.

AWS Shield	• Centralized option to protect all assets from one system. • Pre-existing AWS customers will receive the shield if they have other AWS products • Provides detailed reports and analytics on attacks, such as the attack type and how long it will be for (duration).	• Setting up can be rather complex without knowledge of AWS systems. • Designed to work better alongside other AWS software, not a good option for users who are not AWS customers. • More advanced protections require an additional cost for more features and protection.
Link11	• Not too demanding on computer resources, so there is not much need to buy new hardware. • Uses Artificial Intelligence to locate new forms of DDoS attacks • Automatically creates new, already configured dashboards so it is easy to use.	• It can be found to be more suited for organisations and larger businesses, so it will not be the best fit for smaller companies or individuals. • There is no premise option, so the software application is not hosted on-site

Table 2: Cloud-based DDoS protection services Technology Comparison Table

The review and comparison of all the different types of attacks and prevention tools has concluded, and now it is time to do an in-depth analysis of how they work in practice. This will involve a clear-cut investigation of a step-by-step process of an attack happening. This will demonstrate how an attack is orchestrated and give a better idea of how they perform.

It will illustrate how easy it is to conduct these attacks, so it will indirectly enforce the acknowledgement of prevention tools and techniques. Moreover, the point of this project is to provide the knowledge needed to the reader about all there is to know about DDoS attacks and prevention and mitigation strategies. Every step will be analysed and documented so the reader understands what is happening.

4 Methodology

The following stages of this project will be conducted with the knowledge and approach gained from this literature review. It gave an understanding of how each DDoS tool works whilst learning how they differ. From this knowledge, a DDoS attack simulation will be demonstrated, and all the necessary details will be described. The methodology section will cover some of the hardware and software requirements and critical information for the artefact. The DDoS attack will be conducted using the LOIC and HPing3 since they are both open source and simple to use.

4.1 Hardware and Software

In the process of creating the artefact, some hardware and software specifications will be a crucial part of delivering this. Both will be essential in creating the artefact because it is a very computer-resource-orientated experiment. There needs to be a reassurance that the IT device will be competent to perform it without any possible technical issues.

Heres a table of some of the essential hardware and software that will included in this artefact:

Hardware	Software
• Storage: Minimum 15GB • CPU: Intel Core i5 7400 • Graphics: NVIDEA Geforce GTX 1070 • RAM: 8GB Dual Channel • A Decent Network Connection	• Oracle VM Virtual Box Manager • Bitnami.OVA • Kali_Linux_2021.2.OVA • Xubuntu.OVA

Table 3: Hardware and Software

In this table, the most critical piece of software that will be used is the Oracle VM Virtual Box Manager. *Virtualbox* is an open-source and free operating system virtualization software made by the Oracle organization. It acts as a host for the user to run virtual machines. A virtual machine simulates a physical computer/operating system that runs on a host computer. If multiple virtual machines run simultaneously, they all share the host's

hardware resources, such as the processor, RAM, storage and GPU. This is why it can be pretty intense to use VirtualBox. A wide selection of operating systems can be hosted by Virtualbox, which is suitable for the user.

As the table shows, a decent level of hardware is being utilized. Oracle VM Virtual Box Manager with several VMs being used would be demanding on the hardware if the user had decent quality and performance. When using Oracle VM Virtualbox, the hardware needs to meet the requirements of both Virtualbox and the Virtual operating systems the user plans to use.

The 8GB RAM and CPU will be the most essential hardware. Both need to be decent, but the RAM is interchangeable depending on how many VMs the user plans to run simultaneously.

Due to the limitations of hardware involved for the artefact (lack of resources). This artefact will demonstrate a DoS attack. DDoS and DoS are both the same attack. However, a DoS attack targets a single source that floods a system or network with traffic, while a DDoS attack is a type of attack where multiple sources flood a system or network with traffic. Both types of attacks can cause significant damage to the targeted system or network by consuming its resources and making it unavailable to legitimate users.

4.2 Overview of LOIC

Available to anyone and open source network testing tool, it can be used for pen testing and DDoS/Dos attacks. There are two modes available, a manual mode, which allows the user to enter a targets IP address or URL and then execute the attack or automatic mode, which allows for the tool to be set up so it's connected to an internet relay chat (IRC server), where it will receive commands from the server.

LOIC has a high reputation amongst DDoS attacking tools since it has been used for various attacks, including a massive attack on the Recording Industry Association of America in 2010. This attack was a protest against groups that abuse copyright laws. This links with how LOIC is used in negative ways; in this instance, it was used to send a message. (PCMag, 2010)

LOIC has three types of protocols/services that will be utilised in this experiment:

UDP: This protocol is used to send and receive datagrams over networks. Unlike TCP (which can also be used for this attack), UDP doesn't create a connection before the transmission of data, so in normal circumstances, there will be a chance that the recipient receives no data.

TCP: This is a protocol that is based on the connection made that is used to transfer data/packets over the internet. In contrast to UDP, TCP is more reliable because it will connect the two addresses and guarantee data transfer.

TCP SYN packets will be utilised; this type of TCP packet is used to initiate the process of establishing an entirely new TCP connection, whereas regular TCP packets refer to any TCP connection that is not under the influence of an SYN packet or if its already an established connection.

4.3 Overview of Hping3

An open source network testing and packet analyzer tool. It is a common tool used for security auditing such as testing firewalls and networks. It is used in the command line and comes preinstalled on Kali Linux. It can be used for various attacks and utilises ICMP, UDP and TCP protocols.

ICMP: This protocol sends error messages and status information regarding network conditions. ICMP is an essential protocol for network devices since it is used for communication between them.

Ping attack: A ping attack is one of the attacks that can be utilised with HPing3. This attack sends many ICMP packets to the target, so the network becomes completely overwhelmed and unable to respond to any regular traffic.

Syn Flood: SYN flood is a type of DoS attack that will send a large number of SYN packets to the target server; this will overwhelm the target's resources and prevent any regular traffic from being processed and, in turn, completely disrupt the availability of the target system or network.

4.4 Overview of Wireshark

Wireshark is a network protocol analyser tool used for network analysis and security checks. It can capture and display all of the network traffic to the user in real-time and it can help provide information on all the packet transmissions. It is free and supports operating systems, such as Windows, macOS and Linux. It comes preinstalled on Kali Linux.

4.5 Overview of GUFW

GUFW is an accessible graphical interface firewall powered by an Uncomplicated firewall (UFW). Its predecessor UFW is a well-received net filter firewall, GUFW, which will be used in this project, is an easy-to-use GUI version that allows for simple tasks such as allowing and blocking Ips/Ports and creating rules to add to the firewall (Ubuntu, 2014).

This will find more usage at the end of the artefact when used against HPing3. The command “sudo apt-get install gufw” will be installed through the terminal.

5 Implementation of Artefact

The section is for implementing the artefact. The simulation will include screenshots of every step taken along the way, with a clear description of what is happening in the screenshot. There are 3 stages, creating the target virtual machine, which is going to be used as the victim in the demonstration. A step by step of attacking the target VM using LOIC and HPing3 DoS attack. There will be an discussion of the results after both attacks have been conducted.

5.1 Demonstration of LOIC

Once downloaded and installed the LOIC tool is very linear and straightforward for the user to understand. This will be shown in the demonstration.

5.2 LOIC Demonstration Machine's set up

Figure 5 shows the User Interface for Oracle VM virtualbox, this is where the user can manage all of the VM's, such as changing the network settings, the dedicated RAM and the display settings.

In this instance the VM's Bitnami Wordpress will be used to create a wordpress machine, Xubuntu will be used to open that and host it on the browser and Kali Linux will be used as the attacker.

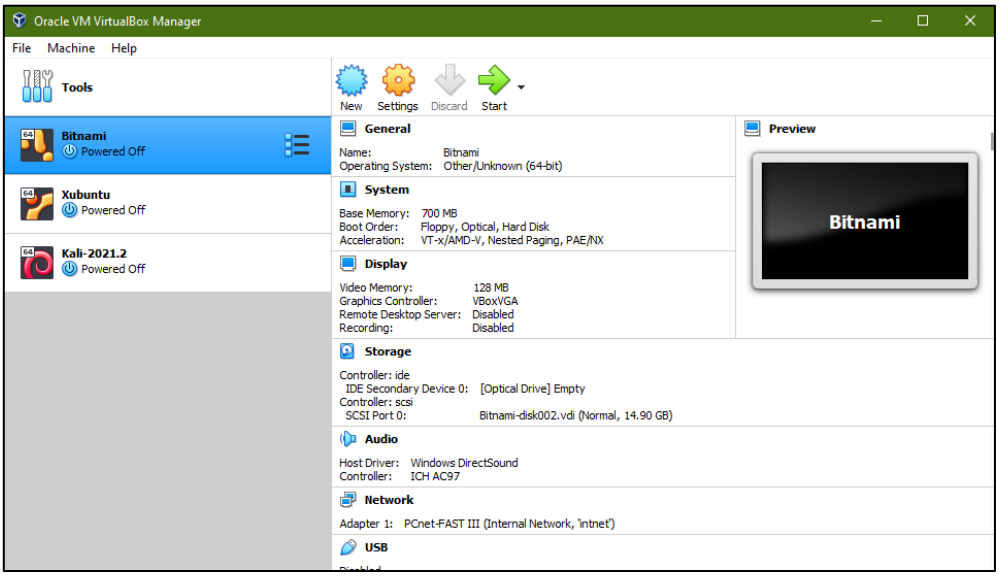

Figure 5: Oracle VM virtualbox UI

Next an IP address and gateway was assigned to both machines. Both machines were set to internal network so they are able be on the same network and connect and were given an IP address. The gateway of both machines need to be the same, however the IP address is inpependent on the machine but it needs to correlate with the gateway. When the gateway on both machines is 192.168.206.1, and the IP is within that range for both (Figure 6).

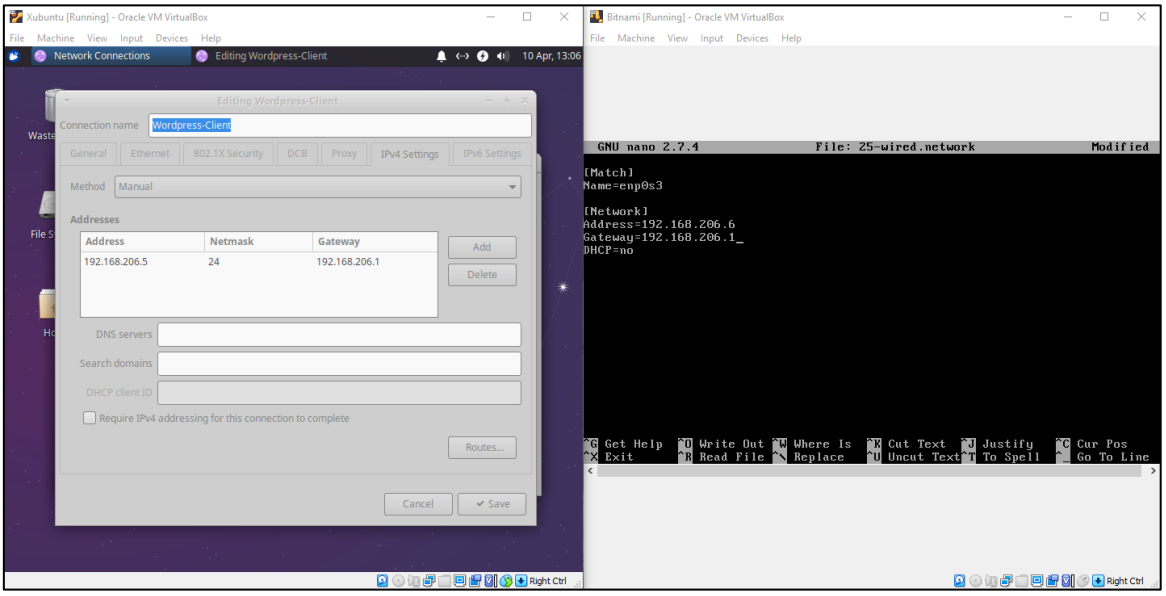

Figure 6: Network Configuration for LOIC

After changing both networks to internal and changing the IP configuration, its important that both VMs are able to ping eachother. Pinging each other on an internal network verifies that the two machines are connected and can communicate. This is essential for any network communication between the machines (Figure 7).

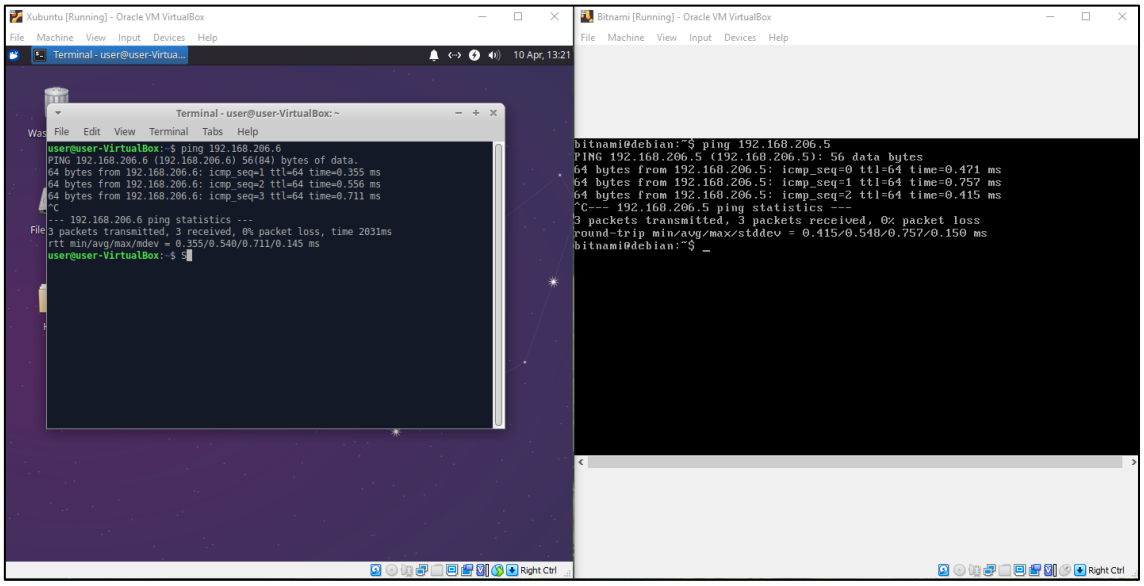

Figure 7: Both machines pinging eachother

When entering the Bitnamis IP address into the Xubuntu Machine Web browser, a wordpress webpage is displayed. This will be used as a target for the attacks (figure 8).

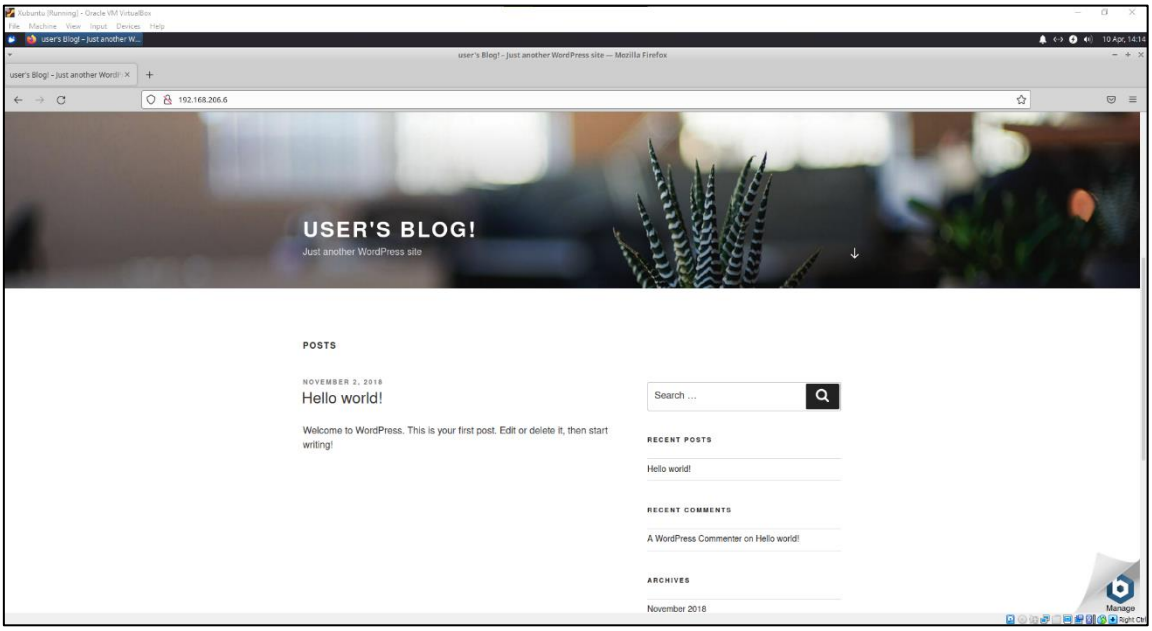

Figure 8: Bitnami Wordpress Webpage

5.3 DoS attack using Low Orbit Ion Cannon (LOIC)

Figure 9 shows all of the VMs that are going to be used in this experiment. Bitnami and Xubuntu are going to be working alongside eachother. And the Kali Linux machine has been launched (left side of the screenshot).

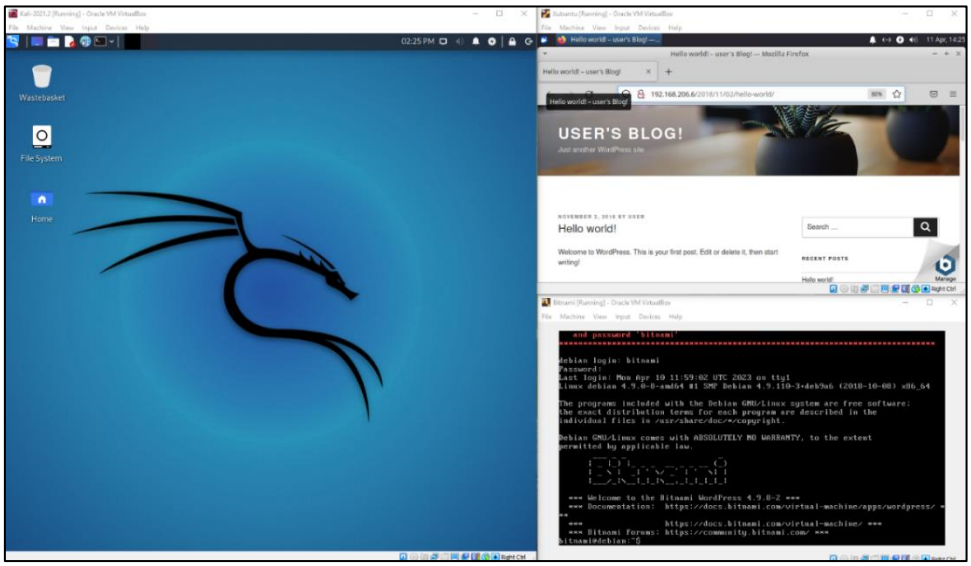

Figure 9: All machines alongside eachother

Figure 10 shows the installation of the mono package. This package provides a set of commands that are used to execute/run cross-platform applications. It will be used in this experiment.

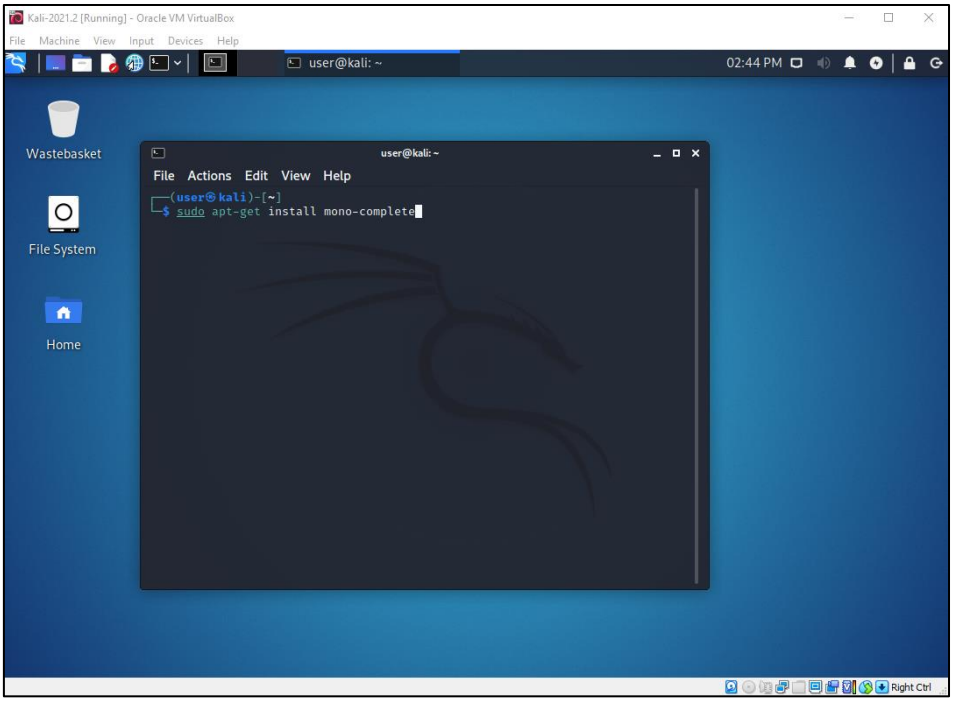

Figure 10: Installation of mono-complete

Next is the installation of LOIC, search “LOIC download” into the web browser and click on the sourceforge.net link and that will take the user to the download page. Click on download on the left hand side of the screen. A prompt will appear, saying that the file may be dangerous, however in this instance it’s safe to download (figure 11).

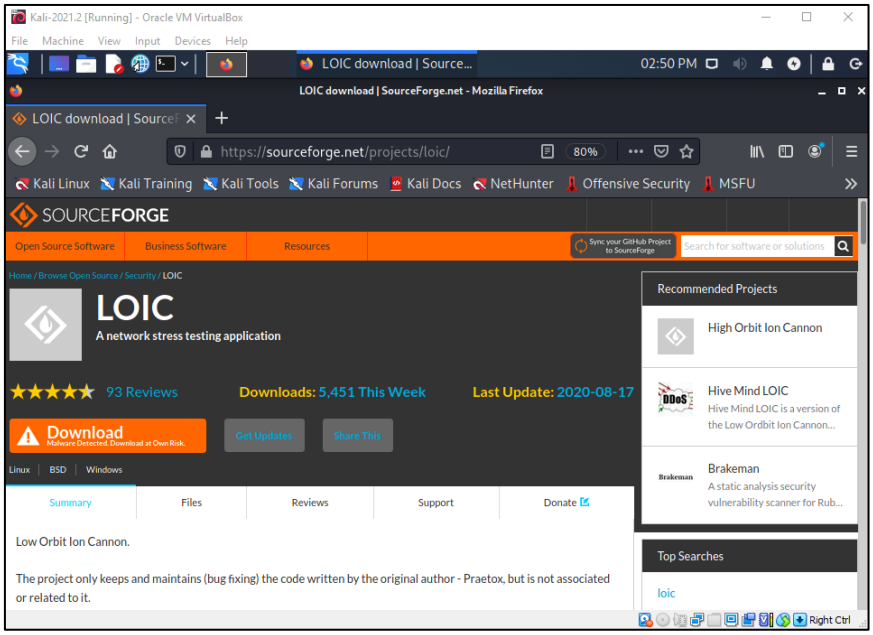

Figure 11: LOIC download

Go to the directory of which the user downloaded the LOIC application. In figure 12 It is the downloads directory. It is then extracted there.

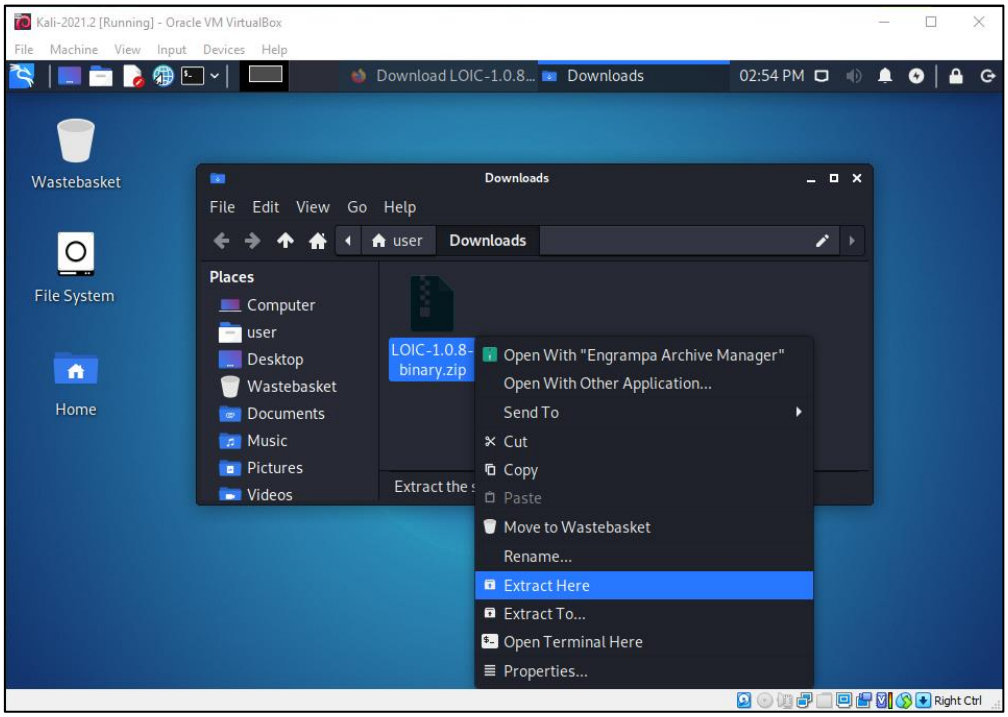

Figure 12: LOIC file download in downloads directory

Next go to the directory of where LOIC is downloaded in a terminal and run the command "mono LOIC.exe" to execute the LOIC file (figure 13).

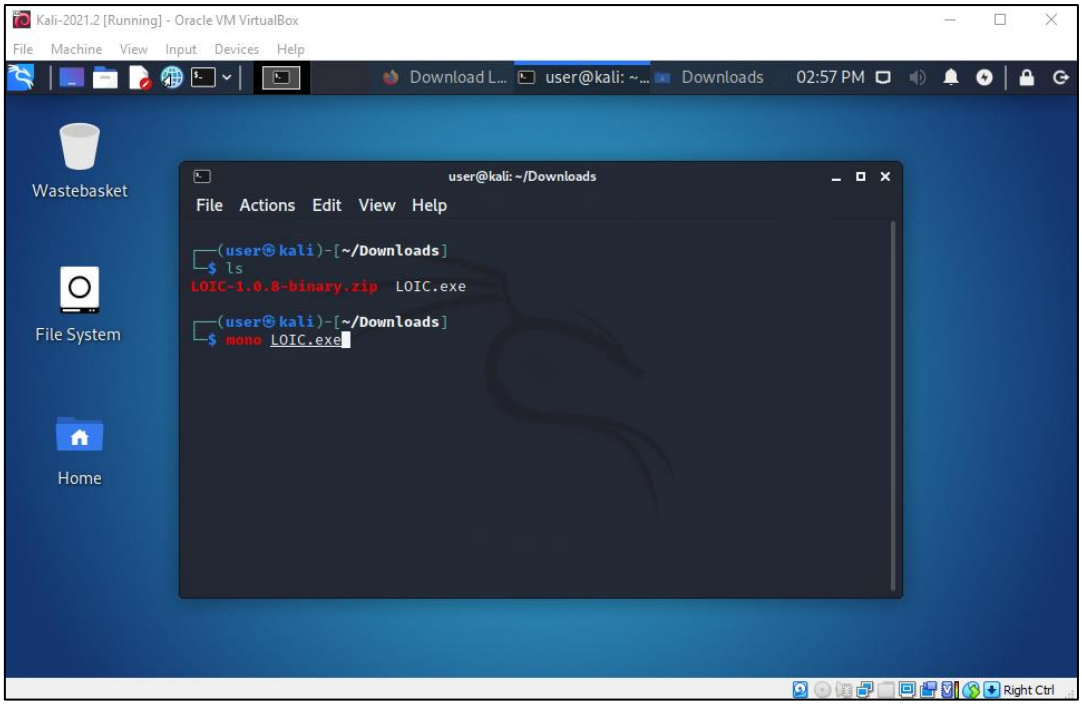

Figure 13: Use of mono package to open LOIC application

After entering that command (figure 14) the LOIC application should open and the user will be greeted with an array of options for an attack. These will be used throughout the attack.

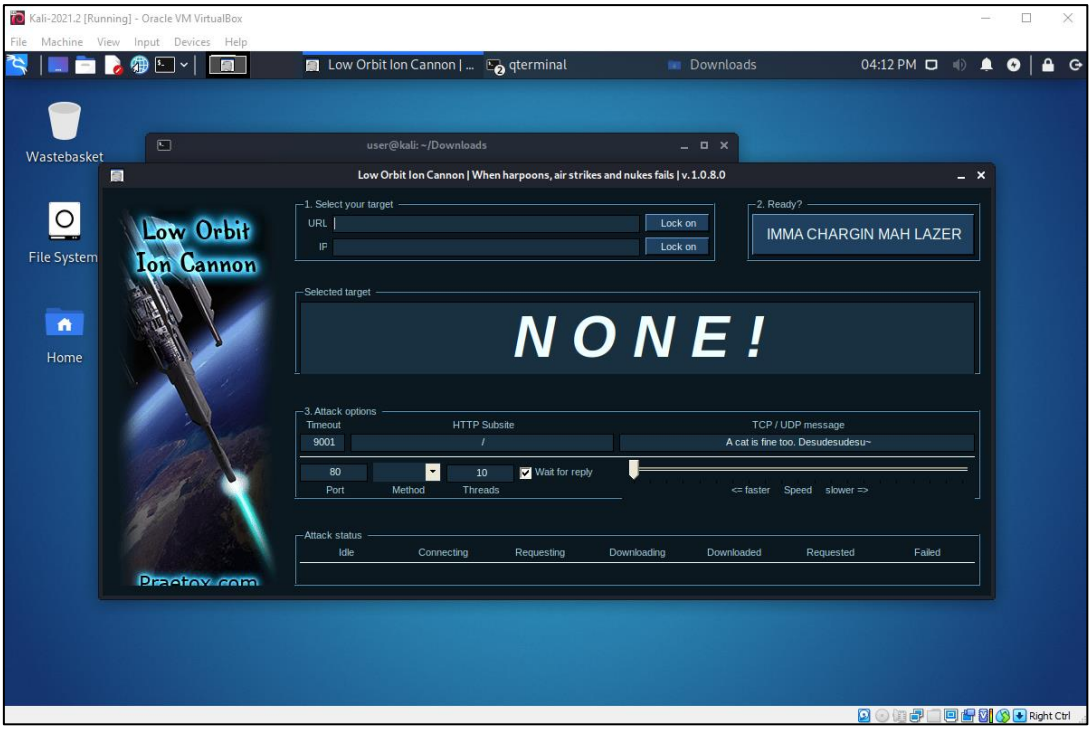

Figure 14: LOIC application user interface

Figure 15 Shows wireshark being opened. As mentioned in the methodology, wireshark comes preinstalled on Kali-linux virtual machines.

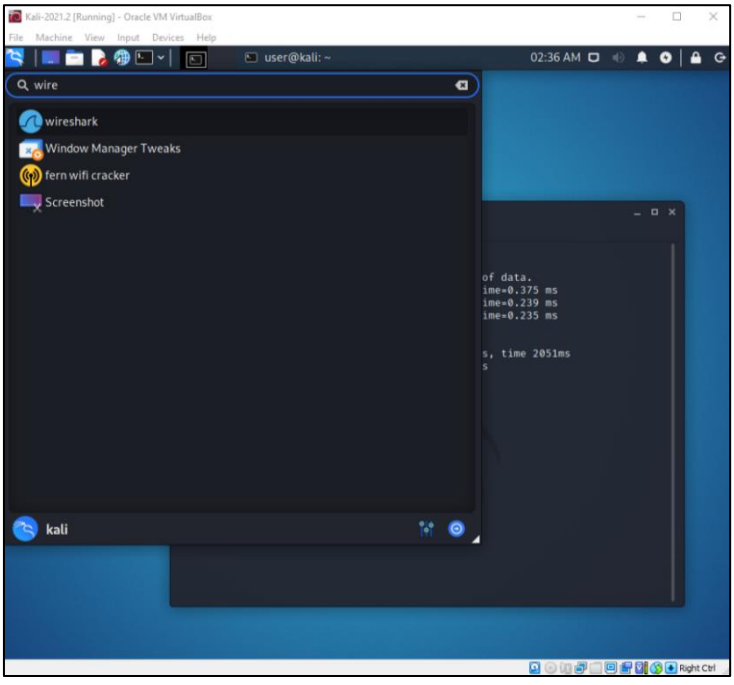

Figure 15: Search for wireshark application in Kali VM

Figure 16 shows the beginning of the LOIC DoS attack, in this attack the Bitnami-Wordpress server will be targeted, because that is host. The IP address 192.168.206.6 is entered. For the first attack the protocol TCP is used.

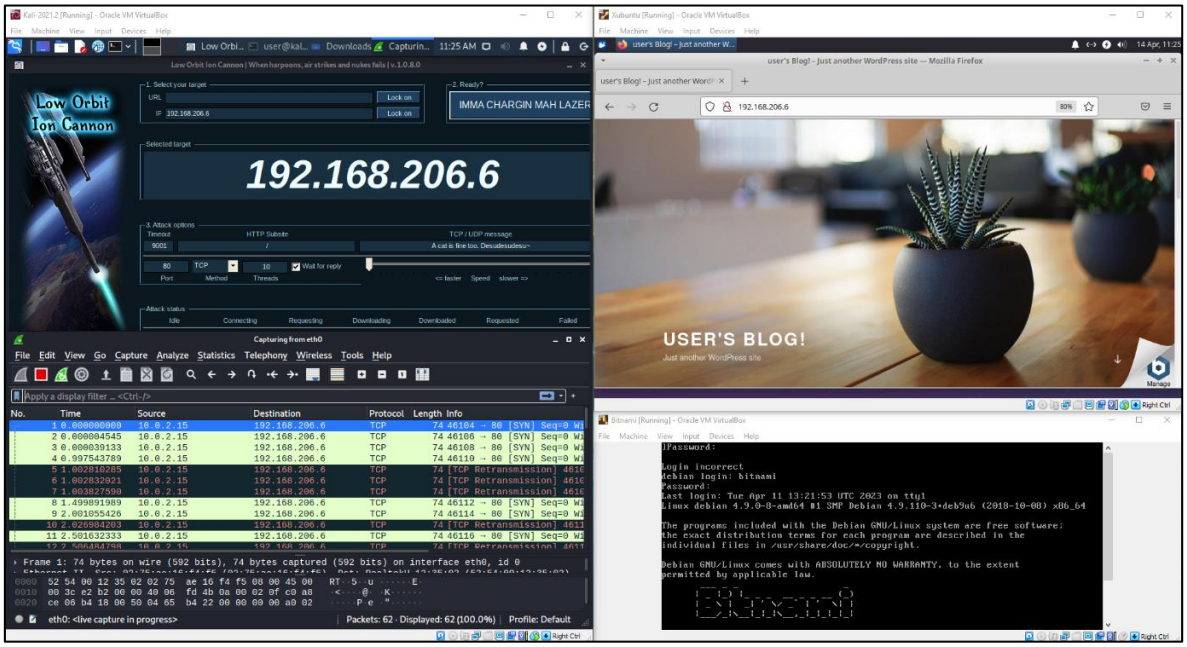

Figure 16: Both attack and target VM's for LOIC TCP attack

Figure 17 shows the wireshark TCP scan in full depth. As seen there is a ton of TCP SYN packets being transmitted towards the target IP, this caused the machine to completely slow down and become unresponsive. It isn't enough to make it disconnect but it will make it lag.

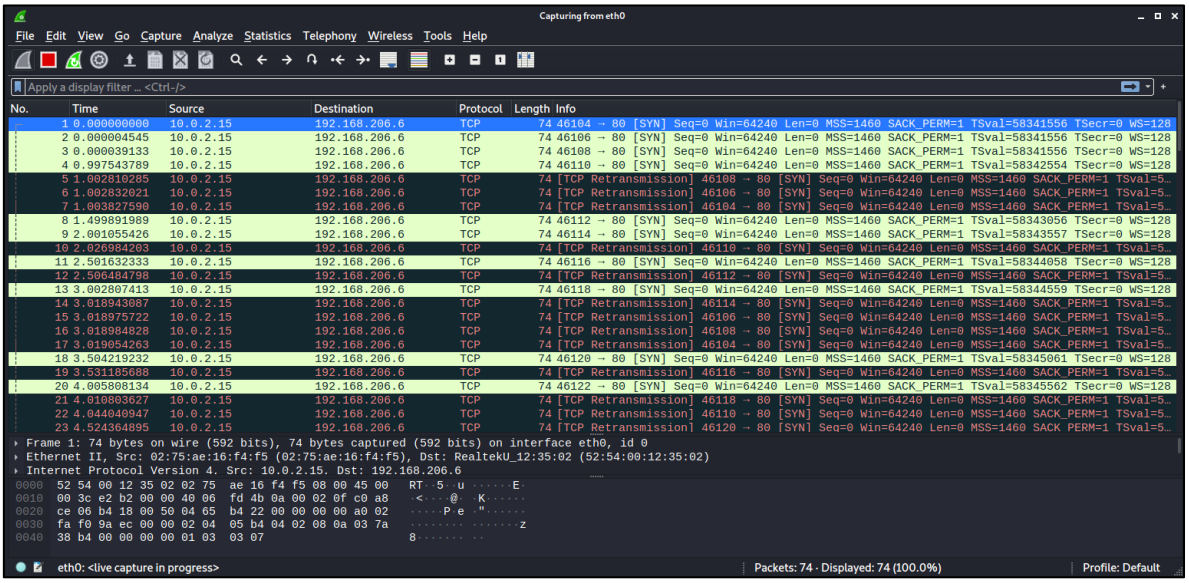

Figure 17: Full screen analysis of LOIC TCP attack

Figure 18 shows another attack on the Bitnami-wordpress target server, this time the use of UDP packets is there, this will be very similar to the TCP packets

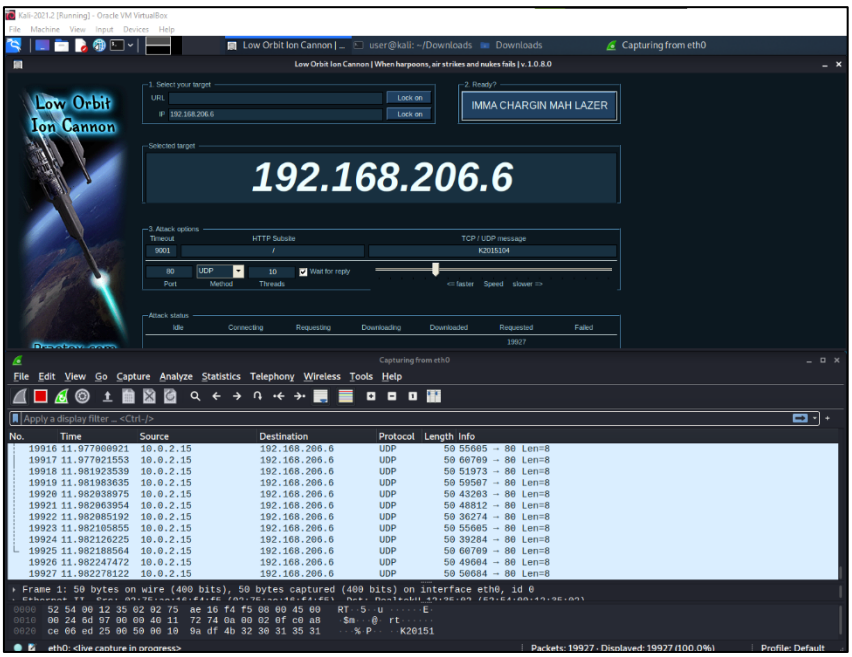

Figure 18: Attacking VM for LOIC UDP attack

Figure 19 shows the wireshark UDP scan in full depth, the source is the 10.0.2.15, because that is the IP address of the attacking machine. The destination is the IP address of the Bitnami-wordpress which is 192.168.206.6. As seen in the Time section, all of these packets are sent under 1 second. This many packets being sent in such a short amount of time will cause disruption.

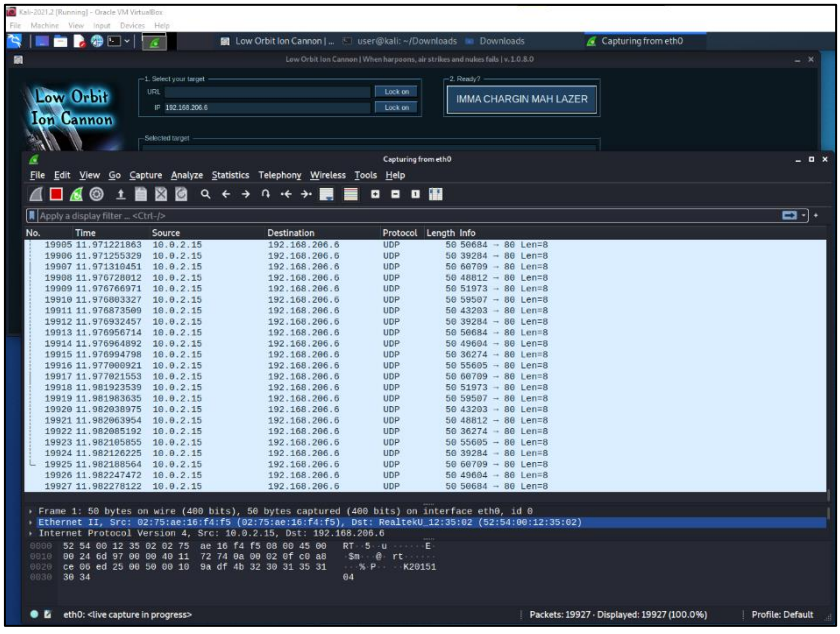

Figure 19: Full screen analysis of LOIC UDP attack

5.4 DoS attack using HPING3

As mentioned in the methodology, 2 different types of HPing3 attacks will be demonstrated. The Ping attack and the SYN Flood attack.

5.5 HPING3 Demonstration Machine's set up

This attack will be shown using two kali linux virtual machines. This is because Kali Linux comes preinstalled with wireshark, so it will easier to do. Both of the machines are shown in Figure 20.

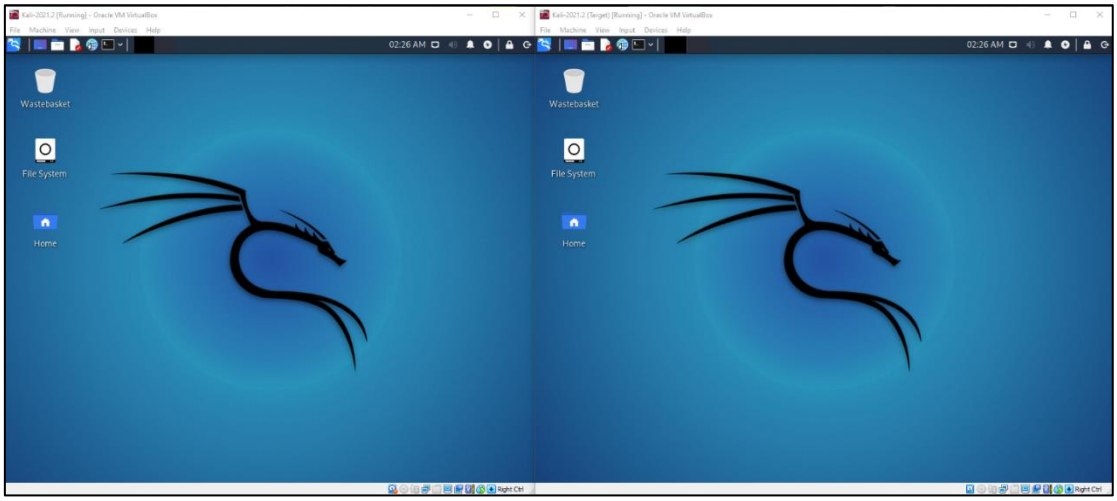

Figure 20: Both machines alongside eachother

Figure 21 shows the network configuration for both kali machines, both were set to internal network and have separate IP addresses, but they are within the same network to conduct the attack.

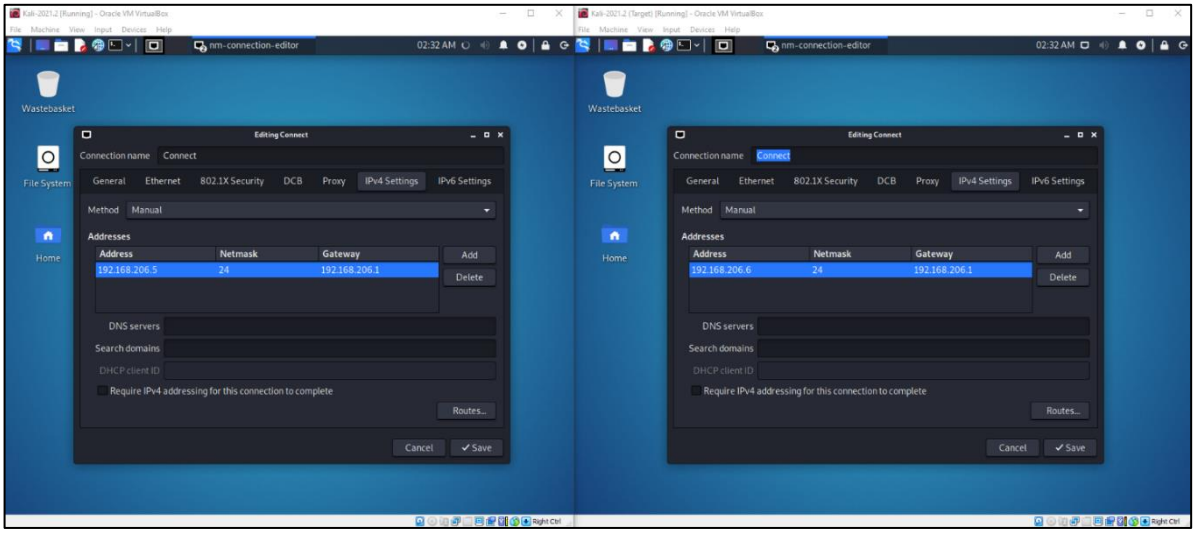

Figure 21: Network configuration for HPing3

Figure 22 shows both machines pinging eachother, this is just to make sure that both are able to connect without any issues.

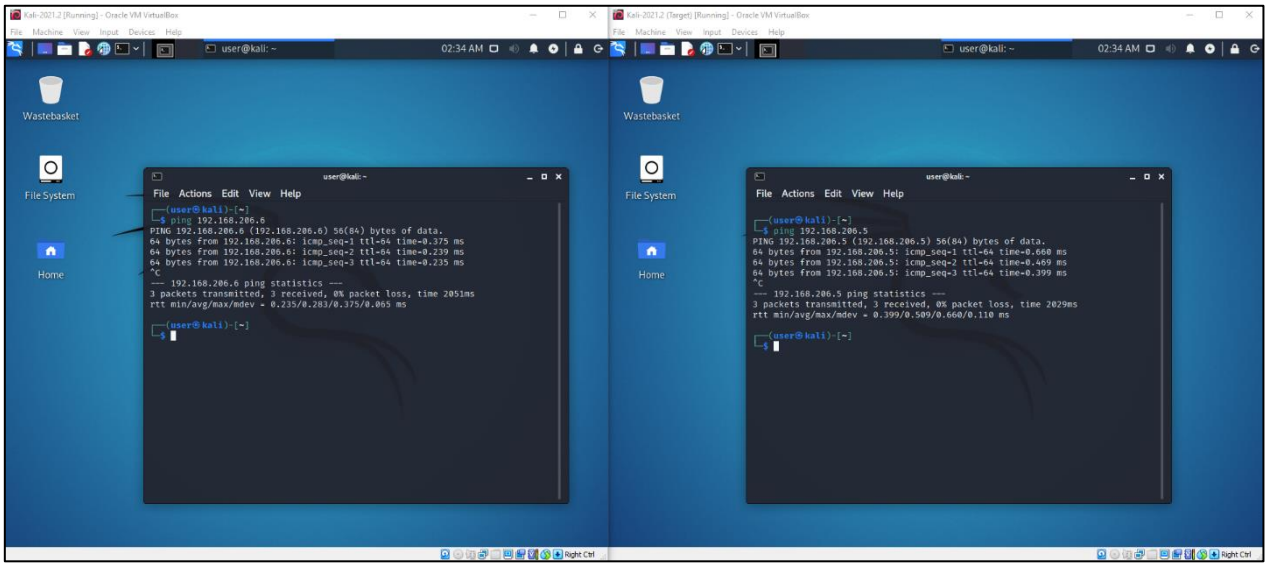

Figure 22: Both machines pinging eachother

Figure 23 shows that the wireshark application has been opened and simple ping from one machine to the other. This shows the wireshark is fully working and tracking all of the data transmissions for both machines.

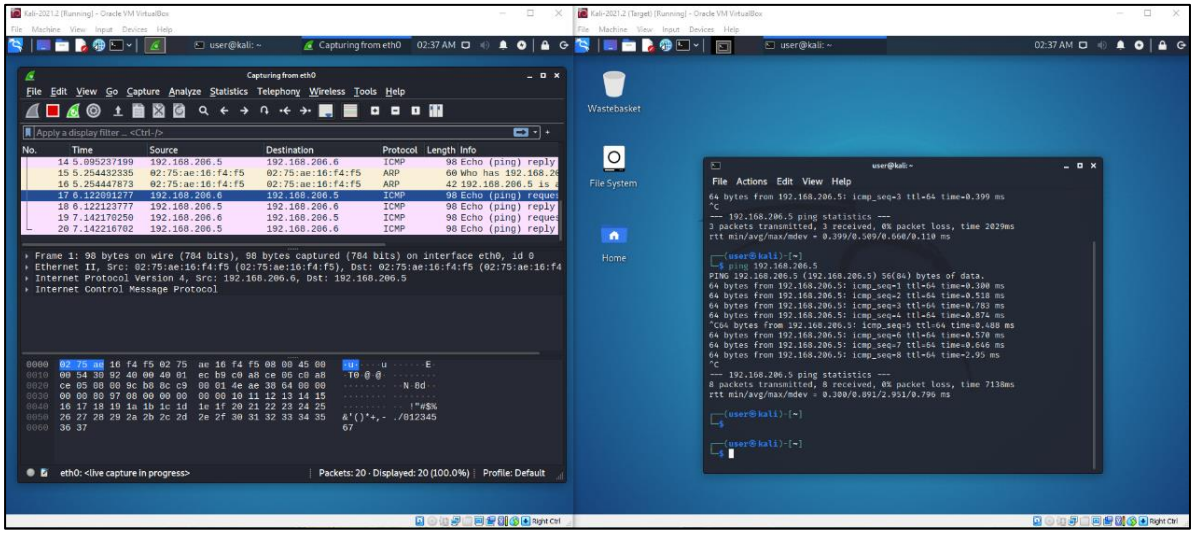

Figure 23: Demonstration of attack and wireshark working through pinging

5.6 HPING3 Ping attack

The set up is complete and now this is the first usage of the hping3 DoS attack. The goal of this attack is to ping the target multiple times using ICMP packets.

```
sudo hping3 -1 -c 5 192.168.206.6
```

There are multiple parts to this command:

- sudo: Grants the user super user, which is essentially admin permissions
- hping3: Declaring usage of hping3
- -1: Declares the usage of ICMP packets, so a ping attack
- -c 5: A counter for the number of pings that is going to be sent
- 192.168.206.6: IP address of the target machine

The command and result (figure 24) show that the attack worked as expected.

The result is exactly as expected on wireshark, it shows 5 echo requests and replies of ICMP protocol which is what was sent from the attacking machine. This command is harmless and highly unlikely to cause an network issues. This is purely for testing purposes.

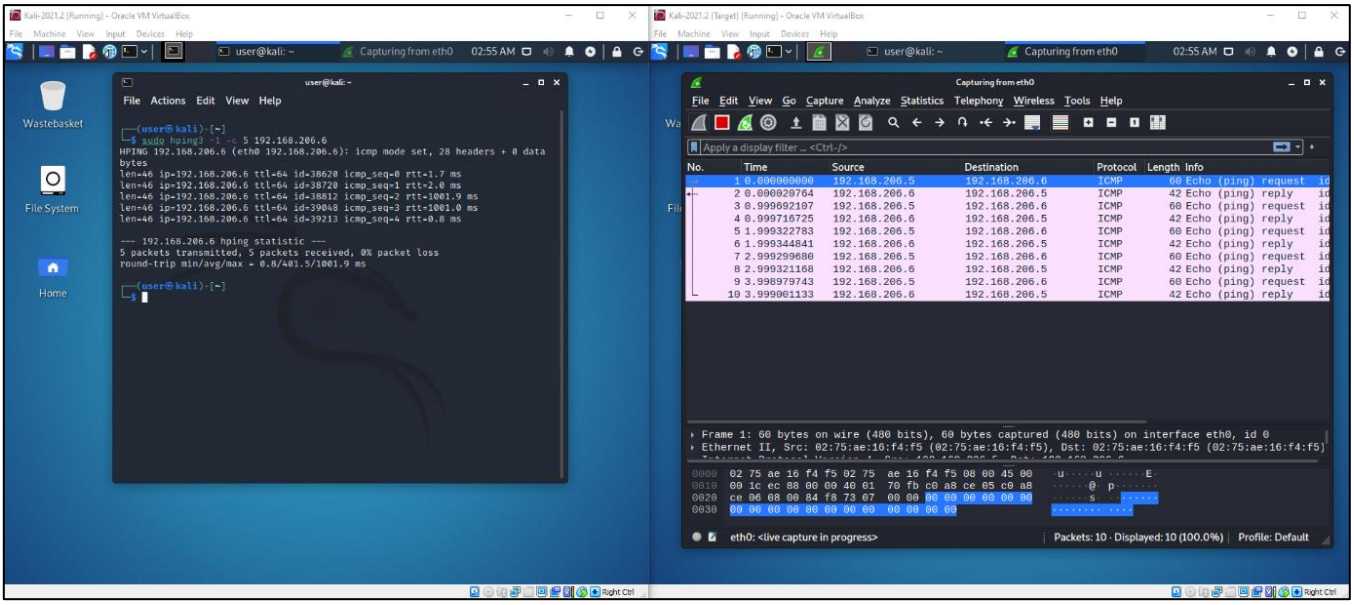

Figure 24: Demonstration of ping attack

The next command (figure 25) that will be shown is a variation of the previous one. That was a simple ping attack, however this one will be used to send packets as quick as possible. From an attacking standpoint, this won't be the first choice however it can still be used to generate a lot of traffic so it should be used cautiously.

```
sudo hping3 -1 --fast 192.168.206.6
```

There are multiple parts to this command:

- sudo: Grants the user super user, which is essentially admin permissions
- hping3: Declaring usage of hping3
- -1: Declares the usage of ICMP packets, so a ping attack
- --fast: Specifies that the packets should be sent as fast as possible
- 192.168.206.6: IP address of the target machine

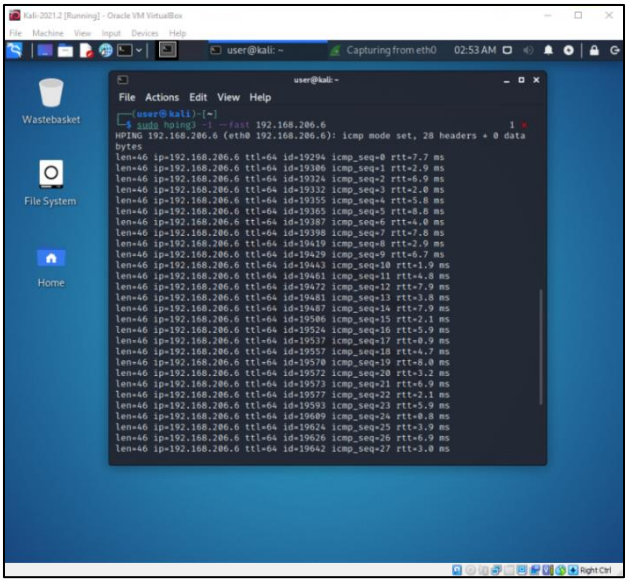

Figure 25: Demonstration of fast ping attack

The results (figure 26) shows theres a bombardment of ICMP packets flooding the machine, this causes denial of service since there is such heavy network congestion. Attempting to run anything over the internet would be slow and potentially wouldn't load.

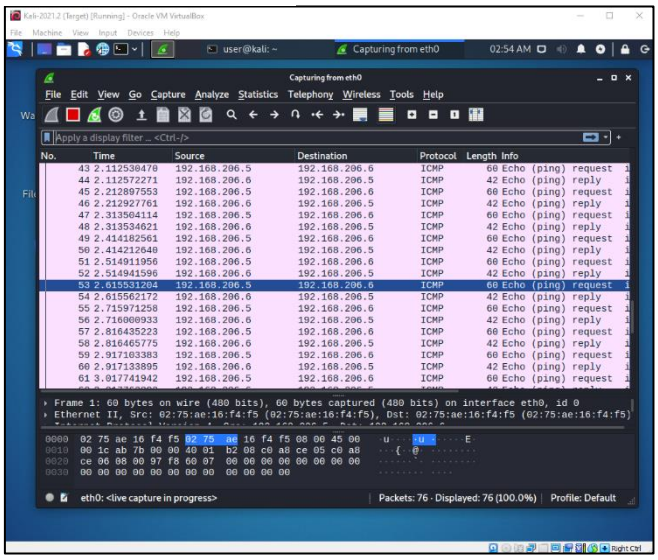

Figure 26: Results of fast ping attack

This command (figure 27) is used to send a single ICMP packet to the target IP address. What is different about this one is that a randomly generated source IP address is going to be used as the source. This makes tracing the source much harder.

```
sudo hping3 -1 --rand-source -c 1 192.168.206.6
```

There are multiple parts to this command:

- sudo: Grants the user super user, which is essentially admin permissions
- hping3: Declaring usage of hping3
- -1: Declares the usage of ICMP packets, so a ping attack
- --rand-source: Specifies that the IP address source is going to be randomly generated
- -c 1: A counter for the number of packets that are going to be sent
- 192.168.206.6: IP address of the target machine

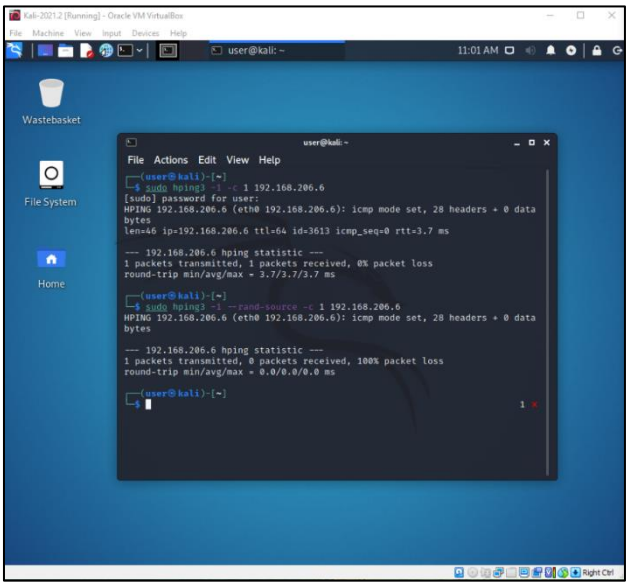

Figure 27: Demonstration of HPing3 random source attack

The results (figure 28) show No. 7 in the wireshark has a source of 286.23.93.169. This is not the correct source and it was randomly generated. This can be effective for stealth, since it will be hard for the attacker to be traced.

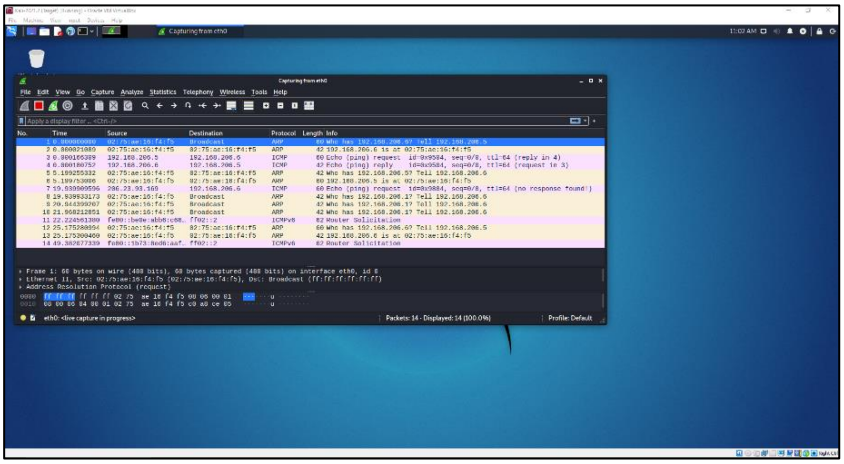

Figure 28: Results of HPing3 random source attack

5.7 HPing3 Syn Flood

This command (figure 29) is used to send to send a single TCP SYN packet to the target IP address. This command is primarily for demonstrating what occurs when sending a single SYN packet.

```
sudo hping3 -S -c 1 -p 80 192.168.206.6
```

There are multiple parts to this command:

- sudo: Grants the user super user, which is essentially admin permissions
- hping3: Declaring usage of hping3
- -S: Specifies that SYN should be declared in the packet sent
- -c 1: A counter for the number of pings that is going to be sent
- -p 80: Port number of target machine
- 192.168.206.6: IP address of the target machine

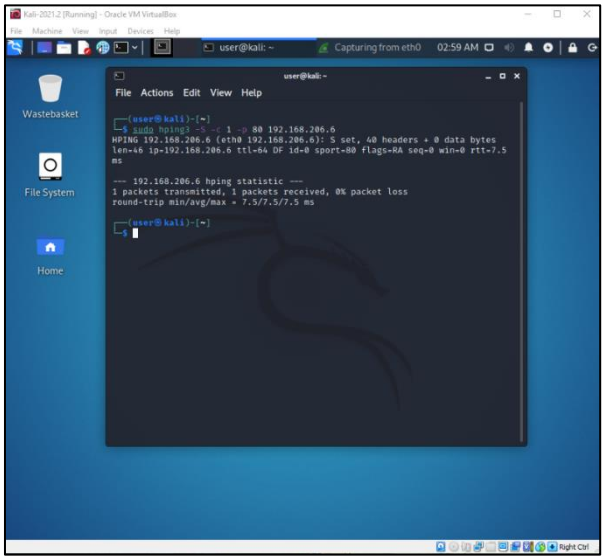

Figure 29: Demonstration of single TCP SYN packet attack

As expected in the results (figure 30), there is a single TCP packet that is sent to the target, the protocol is labelled as TCP, however in the info section of the transmission, it says [SYN]. This indicates the usage of TCP SYN packets.

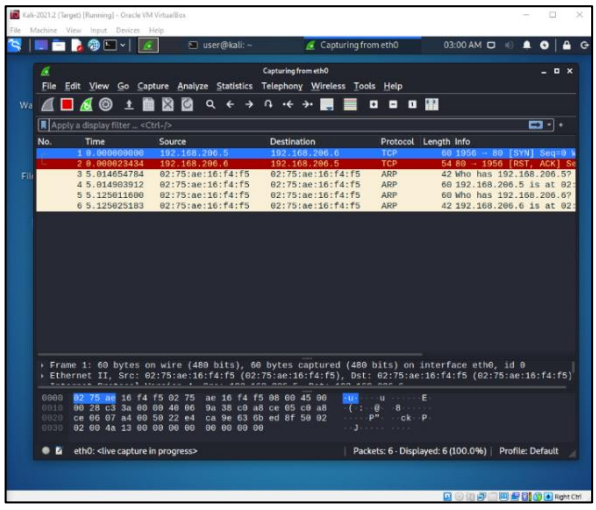

Figure 30: Results of single TCP SYN packet attack

This command (figure 31) is used for flooding the target IP address with TCP SYN packets. This generates a large amount of packets which can almost render the target device unresponsive, as long as the command is going on. Very useful is ethical hacking situations.

```
sudo hping3 -S --flood -p 80 192.168.206.6
```

There are multiple parts to this command:

- sudo: Grants the user super user, which is essentially admin permissions
- hping3: Declaring usage of hping3
- -S: Specifies that SYN should be declared in the packet sent
- --flood: Sends packets as quick as possible, without waiting for a response. Generates a large amount of traffic
- -p 80: Port number of target machine
- 192.168.206.6: IP address of the target machine

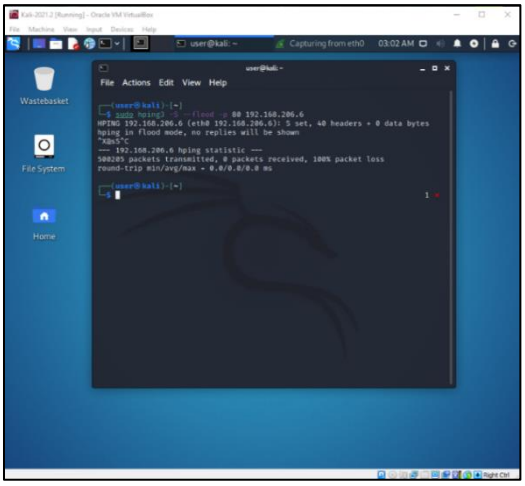

Figure 31: Demonstration of TCP SYN flood attack

As expected in the results (figure 32) there is a cluster of TCP SYN packet replies and requests. Due to the sudden influx of all these packets, there is too much traffic on the network for the machine to be even remotely usable. The attack wouldn't go on for long enough to make the connection unreachable, but the load times would become so long that there isn't much purpose on using it.

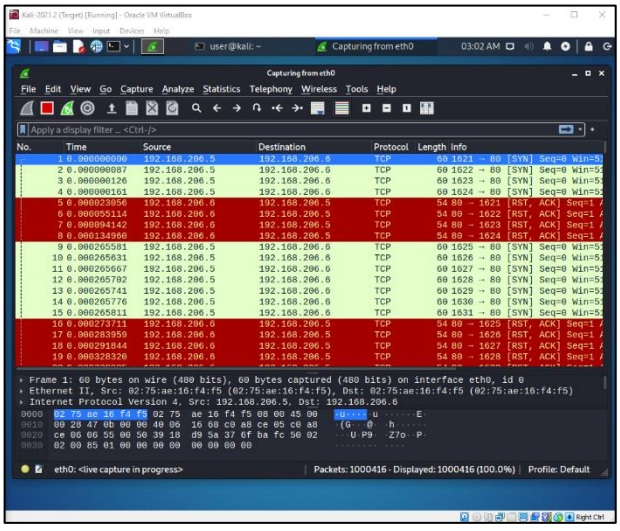

Figure 32: Results of TCP SYN flood attack

5.8 Mitigation of HPing3 TCP attack

A simple firewall was set up in order to show a form of mitigation being used against a DDoS attack. In this instance the firewall “GUFW” was used. (Figure 33)

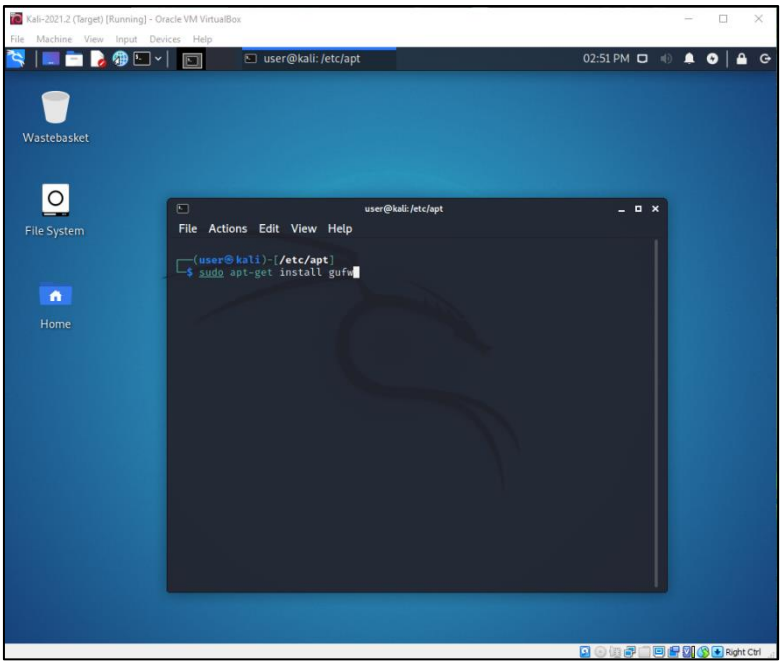

Figure 33: Installation of GUFW

After installation and opening the tool, there is a description of what it is and how to use it, this can be especially useful for users who are inexperienced with how to use this type of tool. (figure 34)

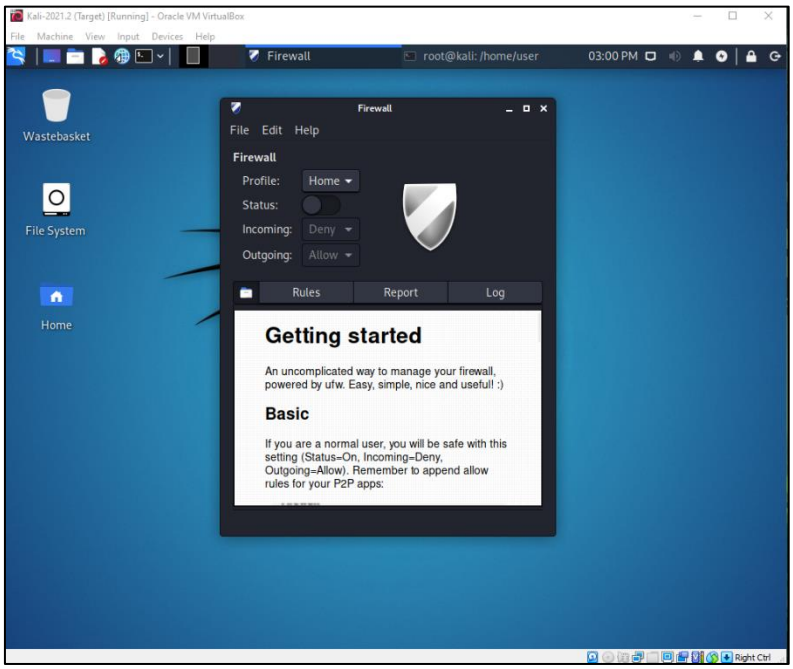

Figure 34: GUFW main page

When it comes to configuration of the firewall, the tool allows the user to have a lot of customisability and flexability on how they would like to use it. It allowed for certain packets to be either denied completely or limited and even allowed to users to completely block certain IP addresses/port numbers. (figure 35)

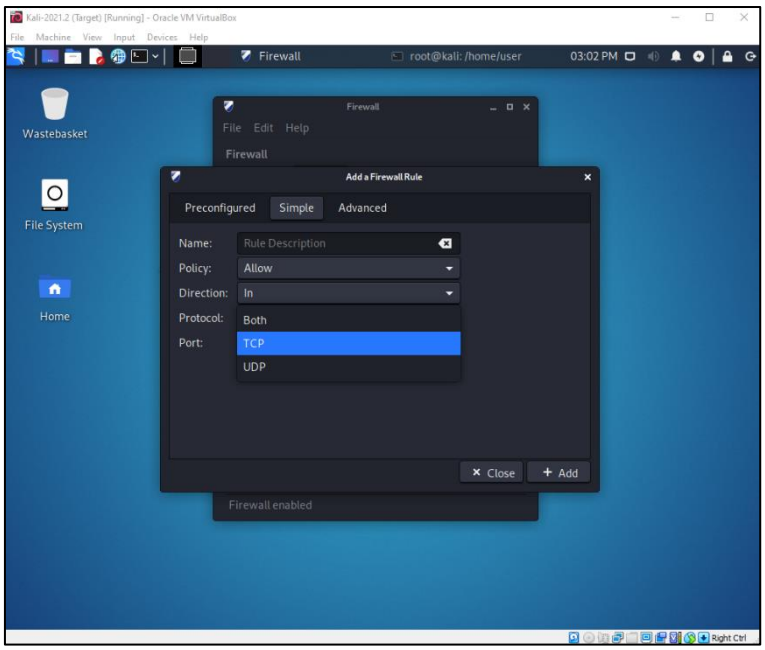

Figure 35: Configuration options available with GUFW

In this instance, TCP packets as a whole was blocked because the HPing3 TCP SYN flood would be simulated against it. (figure 36)

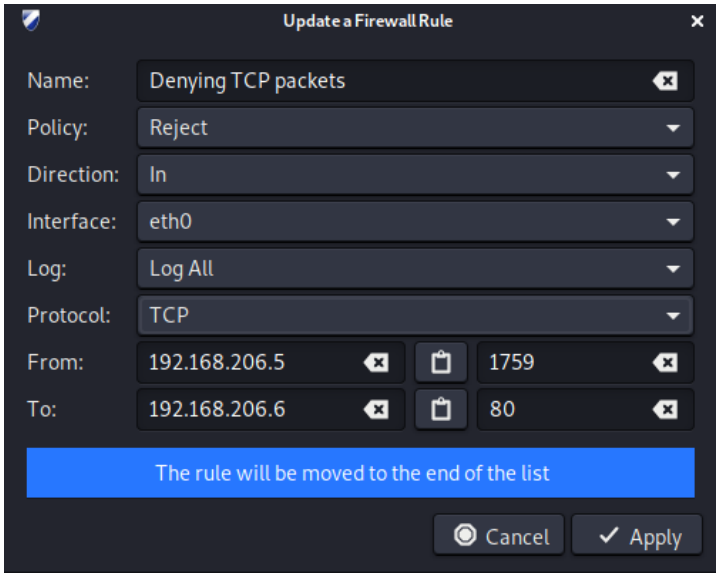

Figure 36: Firewall Configuration for attack

Figure 37 shows the implementation of the custom rule added by the user, it will display on the main page and it says “Denying TCP packets”

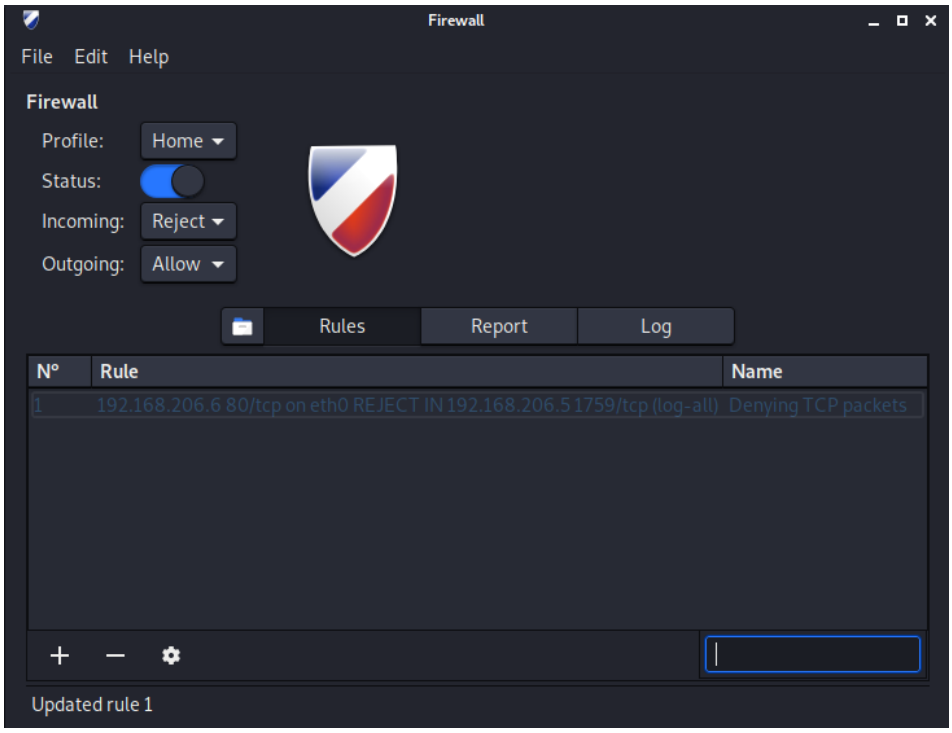

Figure 37: Firewall rule on main page

Figure 38 shows the TCP SYN flood attack being simulated against the firewall. The TCP packets are displayed on wireshark.

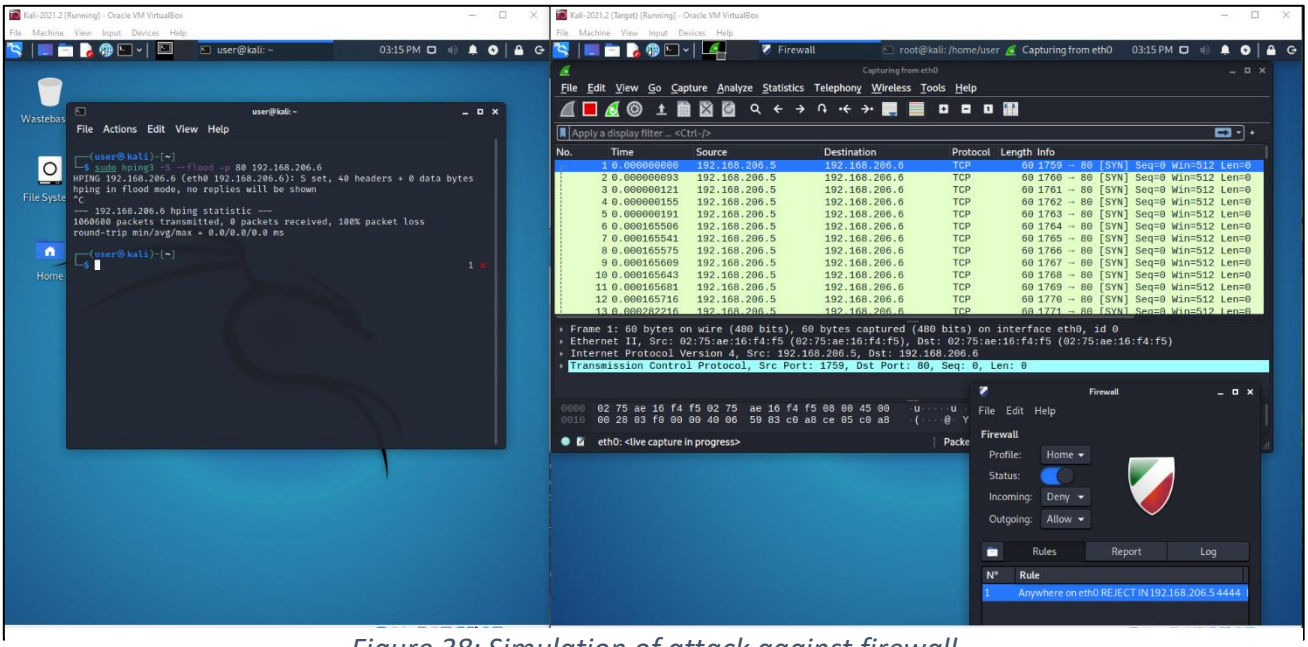

Figure 38: Simulation of attack against firewall

Figure 39 shows a zoomed-in version of the target machine in the attack. From this perspective, the attack went off as usual, and the firewall did not work. However, the firewall did work; it is just that the Wireshark capturing engine gets access to incoming packets before the firewall. Which still means that the firewall gets access before any application software. That is what has happened in this scenario. Wireshark displayed the attack, but it did not affect the system due to the firewall.

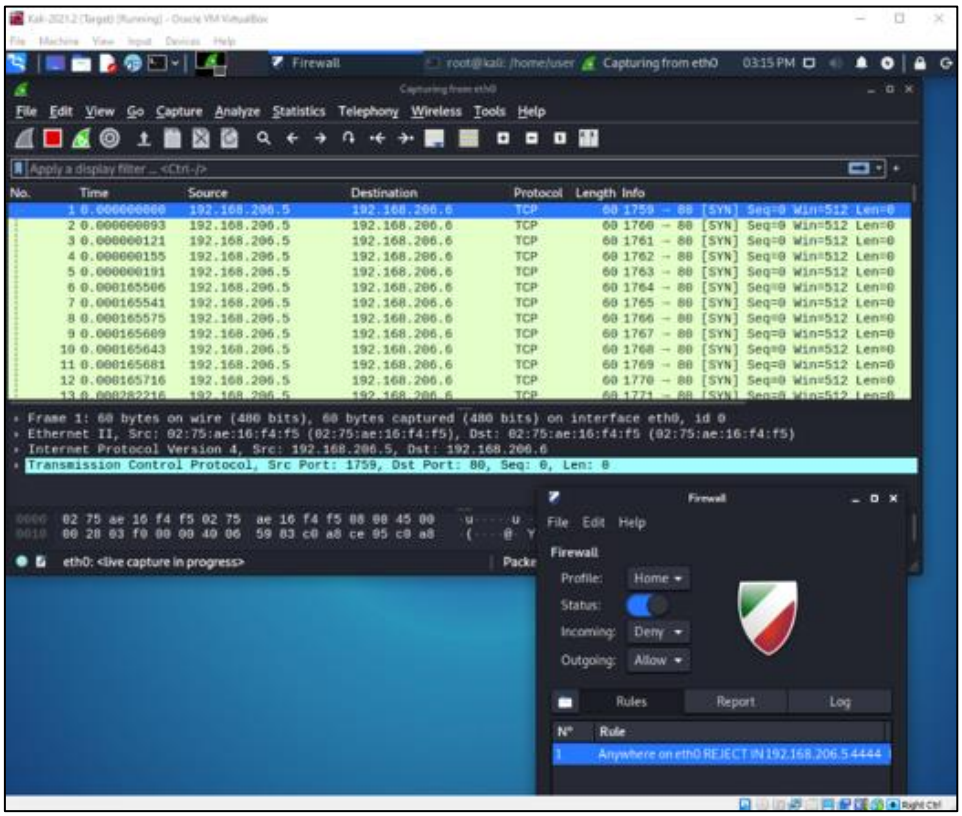

Figure 39: Target machine during attack

5.9 Artefact Conclusion

After completing and demonstrating a showcase of commands/options available to both DoS attacks, it has become clear that LOIC and HPing3 are very different tools and can be used when users have different goals. Through practical use, the differences are a lot more unambiguous. These differences will be covered in this section.

LOIC is more of a network testing tool to see how much it can withstand a flood of traffic overwhelming the target server. There are not any aspects to give to make it stealthy or untraceable, and it is simply a tool that can be used to disrupt the target's network. Multiple users can use it simultaneously to bombard the target from multiple sources.

HPing3 is a packet analyser/generator tool that can experiment with how the target responds and measures up to custom packets the user sends. HPing3 offers more options on how specifics on the attack and stealthier, so from a pen testing perspective, this may be the better option.

LOIC can generate a lot of traffic by flooding the target with requests however it can be responded to well when the defences and mitigation techniques are in place by the target. HPing3 has many options when creating traffic. It can be used for more controlled and targeted attacks that are harder to respond to. Therefore, it is also more helpful in testing network configurations and identifying potential vulnerabilities.

There is a lack of stealth when using LOIC. Network managers and security tools can easily detect it. HPing3 has options in the variety of commands some offer to be untraceable; in this instance, "--rand-source" is a good option. This generates a random source that will be completely random in network tracking tools. This alone gives HPing3 a considerable step up compared to LOIC.

LOIC is more of a malicious tool since its primary use is just for DDoS attacks; it is illegal in many locations, such as the US, where it falls under Computer Fraud and Abuse Act (NACDL, n.d.). In contrast, HPing3 is known to be a legitimate network testing tool used by network administrators and IT professionals. It is legal, but it is important to note that authorisation

is needed to ensure it does not break any network security guidelines for that establishment.

Towards the end of this artefact, the installation and configuration of a firewall was also shown, the firewall shown was rather simplistic, however it is only going up against a DoS attack and not a DDoS. This type of firewall is definitely a better option for individuals who need some sort of device protection. Its open source and easy to use so its clearly the better option to go for some.

In short, they are both similar but perform so differently that there is an apparent discrepancy between them. LOIC is more suited to just being a simple DDoS attacking tool that can generate a large amount of traffic quickly; this creates quick, effective attacks with the drawback of being much more detectable. Whereas HPing3 can be used as an attacking tool, it is much more refined and stealthier but more suited to network testing. Both have very different strengths and weaknesses, which should be considered when using them while also being very practical and situational. It is important to note that the tools are used responsibly and by the laws and policies in place.

6 Critical Review and Conclusion

This project aimed to provide a completely comprehensive guide on the attack known as DDoS after completing all the sections of this project. All the necessary information was delved into and the project's objectives have all been met.

The artefact went well, as a demonstration of two DDoS applications was shown, with a complete guide of their capabilities. This includes all the details for the commands, packet types, and third-party packages/software utilised throughout the experiment. The results and the goal behind each attack were explained clearly. The attack caused enough traffic to disrupt the connection of the targets by making them slow down, but it was not enough to make them completely disconnect.

Regarding time management and the delivery of each project stage, staying true to the Gantt chart provided in the methodology was essential. Anything that went wrong could jeopardise the project's outcome by hindering the duration for later tasks. It was followed well, as all the objectives and project milestones were met in good time, and there was no panic at any stage.

All of the aspects of the projects were completed to a decent extent. Even if slight adjustments were made, they were compensated for by producing a piece of work that remains consistently similar in quality to the rest of the project. It was all carefully planned with the project management, and the review allowed for information to be absorbed in a digestible and understandable manner.

In the situation that this project can be developed further for future studies, there are various possibilities; without a time constraint and better resources, there would be more of an opportunity to be more ambitious with the aims and objectives.

This project could be turned into a proof of concept-based project, by changing the artefact to the development of a DDoS prevention tool. Its ambitious, but it could be accomplished with more research time and better resources. The report content is relevant already; so it would be a change in the artefact.

Another path would be to expand this project to be how DDoS attacks are performed on cloud environments instead of IT devices. This would make the project cloud-computing-centric, and the topics of DDoS and Cloud environments would collaborate as the primary research points of this project. This would also cause a change in both the report and the artefact. Similar to the first suggestion, this extends the current project.

6.1 Conclusion

In conclusion, the project has turned out well since a precise analysis and review of DDoS has been completed. This topic has been of growing interest for a while because IT devices are everywhere at this point, which indirectly causes a significant rise in cyber-threats such as DDoS/DoS around. As covered earlier in the report, the motivations behind the attack can sometimes be for the most trivial reasons, this is important for organisations that utilise cloud computing. There is much of a risk for them, considering this could hinder the work-rate of many people; there is more for them to lose compared to an individual. These sorts of scenarios are what the aim of the project is; it's to act as guidance so that risk will cease to exist. Having the best cyber security practices means that by staying vigilant and careful, any potential target can protect themselves against the ever-growing threat and guard their online presence.

7 References

Alhijawi, B., Almajali, S., Elgala, H., Bany Salameh, H. and Ayyash, M. (2022). A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets. *Computers and Electrical Engineering*, 99, p.107706. doi:https://doi.org/10.1016/j.compeleceng.2022.107706.

Amazon Web Services (2018). *What is AWS*. [online] Amazon Web Services, Inc. Available at: https://aws.amazon.com/what-is-aws/?nc2=h_ql_le_int.

Cao, Y., Gao, Y., Tan, R., Han, Q. and Liu, Z. (2018). Understanding Internet DDoS Mitigation from Academic and Industrial Perspectives. *IEEE Access*, 6, pp.66641–66648. doi:https://doi.org/10.1109/access.2018.2877710.

Cisco (2019). *What Is a Firewall?* [online] Cisco. Available at: https://www.cisco.com/c/en_uk/products/security/firewalls/what-is-a-firewall.html.

Cisco (2020). *Cisco Annual Internet Report (2018–2023) White Paper*. [online] Cisco. Available at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

Cloudflare (2019). *What is IP spoofing?* [online] Cloudflare. Available at: https://www.cloudflare.com/en-gb/learning/ddos/glossary/ip-spoofing/.

Cloudflare (2020). *What is the High Orbit Ion Cannon (HOIC)?* [online] Cloudflare.com. Available at: https://www.cloudflare.com/en-gb/learning/ddos/ddos-attack-tools/high-orbit-ion-cannon-hoic/.

Cloudflare (2020). What Is The Low Orbit Ion Cannon (LOIC)? | Cloudflare UK. *Cloudflare*. [online] Available at: https://www.cloudflare.com/en-gb/learning/ddos/ddos-attack-tools/low-orbit-ion-cannon-loic/.

Cloudflare (2021). *What is rate limiting? | Rate limiting and bots*. [online] Cloudflare. Available at: https://www.cloudflare.com/en-gb/learning/bots/what-is-rate-limiting/.

Cloudflare (2023). *Why Cloudflare?* [online] Cloudflare. Available at: https://www.cloudflare.com/en-gb/what-is-cloudflare/ [Accessed 5 Apr. 2023].

dercraig (2022). *Testing github DDoS Tools: #8: pyloris*. [online] Medium. Available at: https://medium.com/@dercraig/testing-github-ddos-tools-8-pyloris-d835239c83bf [Accessed 5 Apr. 2023].

Flynn, J. (2022). *25 Amazing Cloud Adoption Statistics [2022] – Zippia*. [online] Zippia. Available at: https://www.zippia.com/advice/cloud-adoption-statistics/#:~:text=94%25%20of%20companies%20use%20cloud.

Imperva (2021). *What is LOIC - Low Orbit Ion Cannon | DDoS Tools | Imperva*. [online] Learning Center. Available at: https://www.imperva.com/learn/ddos/low-orbit-ion-cannon/.

Kali (2022). *hping3 | Kali Linux Tools*. [online] Kali Linux. Available at: https://www.kali.org/tools/hping3/.

Keary, T. (2019). *8 Best DDoS Protection Service: The Top Anti-DDoS Tools*. [online] Comparitech. Available at: https://www.comparitech.com/net-admin/best-ddos-protection-service/.

Knight, A. (2020). *Network isolation and segmentation explained*. [online] cybersecurity.att.com. Available at: https://cybersecurity.att.com/blogs/security-essentials/demystifying-network-isolation-and-micro-segmentation.

Montgomery, J. (2021). *What is a Cloud SLA (Cloud Service-Level Agreement)?* [online] SearchStorage. Available at: https://www.techtarget.com/searchstorage/definition/cloud-storage-SLA.

NACDL (n.d.). *NACDL - Computer Fraud and Abuse Act (CFAA)*. [online] NACDL - National Association of Criminal Defense Lawyers. Available at: https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.

National Crime Agency (2020). *DDoS attacks are illegal - National Crime Agency*. [online] Nationalcrimeagency.gov.uk. Available at:

https://www.nationalcrimeagency.gov.uk/?view=article&id=243:ddos-attacks-are-illegal&catid=2.

Nicholson, P. (2022). *Five Most Famous DDoS Attacks and Then Some*. [online] A10 Networks. Available at: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/#:~:text=A%20Brief%20History%20of%20DDoS.

Osanaiye, O., Choo, K.-K.R. and Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications*, 67, pp.147–165. doi:https://doi.org/10.1016/j.jnca.2016.01.001.

PCMag (2010). *'Anonymous' DDoS Attack Takes Down RIAA Site*. [online] PCMAG. Available at: https://www.pcmag.com/archive/anonymous-ddos-attack-takes-down-riaa-site-256328 [Accessed 22 Apr. 2023].

Ranjan, S., Swaminathan, R., Uysal, M., Nucci, A. and Knightly, E. (2009). DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks. *IEEE/ACM Transactions on Networking*, 17(1), pp.26–39. doi:https://doi.org/10.1109/tnet.2008.926503.

Tolsma, A. (2018). *GDPR and the impact on cloud computing | Cyber Security | Privacy | Deloitte Netherlands*. [online] Deloitte Nederland. Available at: https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-the-impact-on-cloud-computing.html.

Ubuntu (2014). *Gufw - Community Help Wiki*. [online] help.ubuntu.com. Available at: https://help.ubuntu.com/community/Gufw.

Wallarm (2019). *What is HULK - HTTP Unbearable Load King? Wallarm*. [online] www.wallarm.com. Available at: https://www.wallarm.com/what/what-is-hulk-http-unbearable-load-king#:~:text=HULK%20is%20an%20abbreviation%20for [Accessed 5 Apr. 2023].

Wallarm (2022). *16 Best DDOS Attack Tools in 2022*. [online] Wallarm. Available at: https://lab.wallarm.com/16-best-ddos-attack-tools-in-2022/.