DDoS Attacks

Calvin Schmeichel
St. Cloud State University
Cybersecurity
Calvin.schmeichel@go.stcloudstate.edu

Will Novotny
St. Cloud State University
Cybersecurity
Will.Novotny@go.stcloudstate.edu

I. Introduction (Abstract)

"DDoS attacks continue to pose a significant threat to modern computer networks and online services, disrupting their availability and reliability. Despite various defense mechanisms, the evolving nature of DDoS attacks presents challenges in effectively mitigating them. This research aims to investigate the current state of DDoS attacks, their impact on different sectors, and explore novel approaches to detect, prevent, and mitigate DDoS attacks, with a focus on improving network resilience, reducing downtime, and enhancing cybersecurity strategies." We will then apply our findings into a lab experiment that will allow us to apply the topics we have been researching into a simulated real world environment.”

II. Problem Domain

The main problem domains we identified that were the most affected by Distributed Denial of Service Attacks (DDoS) were the LAN, LAN to WAN and WAN domains.

The LAN domain is a collection of all systems and servers that are connected to each other on the same network. Having an internal note of the size and shape of the organization's LAN network and topology is important when discussing the effects of Denial of Service Attacks (DDoS). If the local server is hosting a public facing web server and other private internal services on bare metal without using containers or virtual machines in some way could lead to catastrophic damage.

The LAN to WAN domains is the section where the organization's internal LAN network interfaces with the WAN network. Within this topic WAN is referring to the internet. It is important to implement some sort of firewall or multi-firewall solution to separate the WAN and LAN networks. This can help prevent future Denial of Service Attacks (DDoS). This is typically the single most point of failure in an attack.

Finally the WAN domain. This will include an organization's servers that have direct access to the internet. Whether those servers are owned/operated or hosted on the organization's campus or if it is hosted online using a cloud service provider such as Google Cloud, Microsoft Azure or Amazon Web Services (AWS). Any server that is contained in the WAN domain is subject to higher risks. It is important to have a robust security plan in place for these systems

.

III. Problem Statement

As DDoS attacks continue to grow and evolve with new technologies. It has become an important issue that must be addressed in the cyber security field.

IV. Research Questions

A. What is a DDoS Attack?

A distributed denial-of-service or also known as a DDoS attack is a type of malicious attack that disrupts normal traffic of a targeted server, service or network, by overloading the target with a flood of internet traffic.

According to the article What is a DDoS attack, "A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination (*What is a distributed denial-of-service (ddos) attack? - cloudflare*)." [4]

B. How does it compare to other attacks?

A DDoS attack is a type of DoS attack that uses multiple computers and systems to compromise its target. While both attacks serve the same purpose, a DDoS is more impactful and dangerous than a DoS attack. A DoS attack uses a single system to attack a specific service. DDoS attacks are more difficult to detect and prevent than DoS attacks because they come from multiple sources. DDoS attacks can also be split into three categories (Volume Based Attacks, Protocol Attacks, and Application Layer Attacks) based on their attack methods.

C. How Severe are they?

DDoS attacks are very severe and disruptive. They can target high profile websites or services. The severity of a DDoS attack depends on multiple factors, such as the size and duration of the attack. The target's infrastructure, and the attacker's capabilities. DDoS attacks can result in a range of negative consequences, including lost revenue, damage to reputation, and reduced productivity. DDoS attacks can also be used as a distraction for more insidious activities, such as data theft or network infiltration. It is important for

organizations to protect themselves against a DDoS attack, and implement security measures, backups, and have a response plan.

D. How common are they?

DDoS attacks are very common. It is due to the increase of available tools and resources needed to carry out DDoS attacks that are more widely available than ever. It makes it easier than ever for attackers to launch such attacks against an individual or an organization.

According to the article 45 Global DDoS Attack Statistics 2023, "DDOS attacks are expected to increase by over 300% in 2023. This is a major concern for businesses and individuals alike, as these attacks can cause serious damage to both personal and business-related websites (James, 45 global DDOS Attack Statistics 2023 2023)." [19] It seems that in 2023 DDoS attacks have increased exponentially and show no signs of slowing down.

E. Who is most targeted?

DDoS attacks are common because hackers want to target organizations or individuals like financial services, healthcare, insurance services, technology, and e-commerce are vulnerable due to the high value of their data and services.They contain a lot of personal data about individuals and information about financial methods that can be stolen from a DDoS attack. According to an article Why are DDoS attacks becoming increasingly common, "Finance, banking, and insurance services were the most frequent target in 2021 – over 25% of all DDoS attacks were against companies in this industry. Attacks against it had been rising steadily since the previous year. (Telecomlead, Why are DDoS Attacks Becoming Increasingly Common? 2023)." [20] This shows that those specific companies are most likely going to be targeted against DDoS attacks. They have information that hackers find valuable.

F. How do they function?

DDoS attacks are performed through networks of internet connected machines. According to the article What is a DDoS attack, " DDoS attacks are carried out with networks of Internet-connected machines. These networks consist of computers and other devices (such as IoT devices) which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet. Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot. When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed,

resulting in a denial-of-service to normal traffic. Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult (*What is a distributed denial-of-service (ddos) attack? - cloudflare*)." [4]

G. How do you detect them?

There are various ways to detect DDoS attacks. Usually they can be detected by your network traffic becoming increasingly slow. You can detect DDoS attacks through network traffic tools. According to the article What is a DDoS attack, "The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable. But since a number of causes — such a legitimate spike in traffic — can create similar performance issues, further investigation is usually required (*What is a distributed denial-of-service (ddos) attack? - cloudflare*)." [4]

Furthermore, suspicious amounts of traffic that are coming from a single IP address or IP range can mean a DDoS attack. Another way to detect them is through a flood of traffic from users who share a single behavioral profile, like device type, geolocation, or web browser version. Unexplained surge in request to a single page or endpoint usually indicates a DDoS attack. Odd traffic patterns like spikes at an unfamiliar hour of the day or patterns that appear to be unnatural, for example a spike every 10 minutes. A DDoS attack has other more specific signs that can vary depending on the type of attack.

H. How do you prevent them?

Having the right security infrastructure and defenses in place is the best way to prevent a DDoS attack. Some simple ways to prevent using a DDoS protection service that will help detect and mitigate DDoS attacks. Another way is to ensure that your hardware and software are up-to-date and have the latest security patches installed. Use a firewall to restrict access to your network and limit the number of open ports. You may also want to limit your bandwidth available to each IP address and implement rate limiting to prevent an attacker from using up all of your resources.

A traffic analysis system can help monitor your network traffic and implement a traffic analysis system to detect and mitigate non normal traffic patterns that may be indicative of a DDoS attack. Finally, a DDoS response plan that outlines certain steps you will take in the event of an attack is really important. This plan should have steps to insulate affected servers, notify people, and contact your DDoS protection provider inside your company. This can help save your company millions of dollars and keep your company running.

I. What are the different types of DDoS attacks?

There are a few main types of Denial of Service Attacks (DDoS). Such as UDP Flood, TCP SYN Flood, ICMP or ping Flood Attack. We will go into those in greater detail.

1. **UDP Flood:** This type of attack uses the User Datagram Protocol (UDP) to attack a host. It does this by sending a large amount of data packets over to the target system. This will typically overwhelm the network. UDP Flood attacks are easier to use then others since they do not require a direct connection to the host before sending packets. However this does mean this form of attack is less effective than others mentioned. Since it is using UDP and UDP is connectionless there is no guarantee that the packets make it to the destination. This results in limited opportunities to use this form of attack.
2. **TCP SYN Flood:** This type of attack uses the Transmission Control Protocol (TCP) to attack a host. This attack sends a collection of synchronized packets to the target host over a TCP connection, but right before the handshake is complete it is stopped by sending a ACK or acknowledgment packet. This form of attack is much more advanced than the UDP form and tends to be much more effective. Since the connection is made over TCP this leads to the targeted host becoming overwhelmed much more easily.
3. **ICMP or Ping Flood:** This type of attack uses the Internet Control Message Protocol (ICMP) to attack a host. This attack sends a large number of ping packets to the targeted host. This is very easy to launch, very similar to the UDP attack. But at the same time it is not as effective compared to the TCP SYN Flood method. But still very much has the potential to overwhelm the network.

V. Objectives

The objectives can be boiled down to three main pillars. Gain a basic understanding of the attack vector. Learn how it functions and the best way to defend against it. We will achieve these objects through extensive peer-reviewed research papers and other reputable online resources that can provide an accurate authoritative answer.

VI. Scope

The scope of this research project was to keep it very broad and high level. Since both of us are still learning about many different cybersecurity topics and attacks we wanted to focus mainly on one type of attack and possible solutions to defend against it. We overall wanted to learn the basics of the attack, how it functions, its effectiveness and more.

VII. Research Contribution

Our research contribution to the field will be us gaining a better understanding of the attack. Since our wide and thorough research will provide much information we will aggregate all of it into a short and concise research paper that anyone can read at a high level.

We would also like to provide simple and easy to follow lab instructions during our experiment section to help future research easily set up a home lab and be able to learn in a real environment how a Denial of Service Attacks (DDoS) works. This will be free and hopefully provide a great point of research for future generations.

VIII. Hypothesis (Research Questions)

- **Research Question 1:** "How effective are Denial of Service Attacks (DDoS)" what is the false positive and false negative ratio? Is there room to improve? [4 pg 12]
    - We would like to research more into this and find out how accurate these systems are. And if there are new strategies that could be used such as leveraging AI or other tools.
- **Research Question 2:** How effective are these systems at detecting these attacks?
    - After wanting to learn about the false positive and false negative ratio. We also wanted to learn more about how effective these systems are in general as in do they detect more attacks then not? And so on.

IX. Literature Review

A. "Review of Recent Detection Methods for HTTP DDoS Attack" [11]
B. "DDoS attacks and defense mechanisms: classification and state-of-the-art" [B in sources]
C. " Analysis of the IoT Impact on Volume of DDoS Attacks" [12]
D. "A DDoS Attack Detection Method Based on Machine Learning" [13]

X. Methodology

Our main research design for this project was to have a mixed method of quantitative, qualitative approaches through occurring broad information on the topic. We then wanted to apply these findings to our lab and have an equal quantitative and qualitative look at those.

The sampling we used for this study was referencing mainly research documents on the subject of what was written from 2019 or newer.

The data we collected for this study was from the data sets used in the research documents mentioned before. Most of them contained many graphs, spreadsheets and math formulas which were useful to us. Using this data we can then analyze it to better answer our research questions mentioned above.

One of our limitations while conducting this research was time. When starting this project we were quite new to the topic but as we drove deeper into its wealth of knowledge we then realized how much there is to learn. Another reason we tried to keep the information we did gather high level.

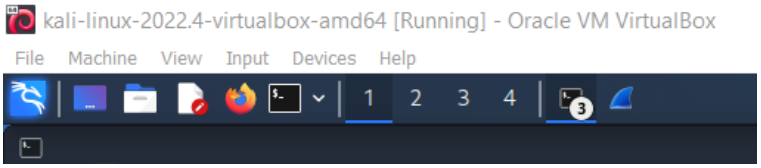
The Validity and Reliability of our research was of utmost importance to us. We only used resources provided to us through the St. Cloud State University's online library, Google scholar and other students' research conducted on campus.

We have formatted this document in the standard IEEE format with clear lab instructions to maintain Reproducibility if this document gets sited in the future.

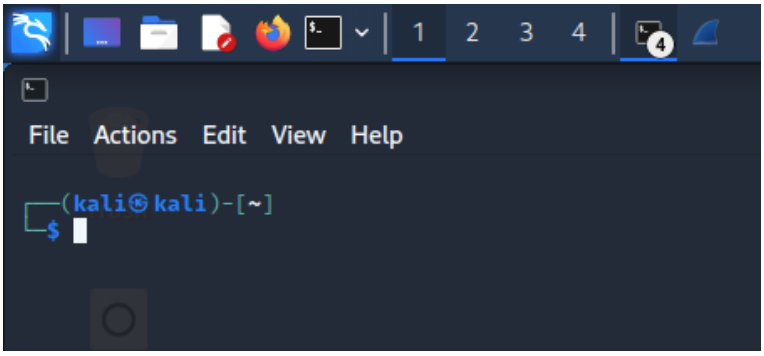
XI. Results (Experiment)

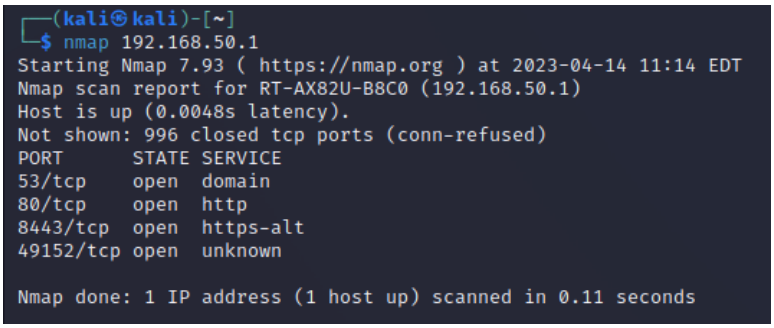
The lab experiment we chose to do was a simple TCP SYN Flood attack using a Kali Linux VM targeting our personal router. We chose this since all of the required resources are free to use and most people have a home router they can use to recreate the lab environment. It is also important to note that you must only conduct DDoS/DoS attacks in controlled, private environments where you have explicit permission. Since this activity without prior authorization is very much illegal.

We will now show our lab steps we created:

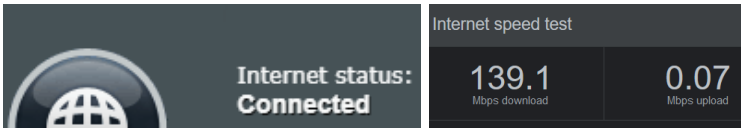
1. We boot up our kali VM
    a. 

2. We use the “ipconfig” command on our host to get our routers IP address
    a. 

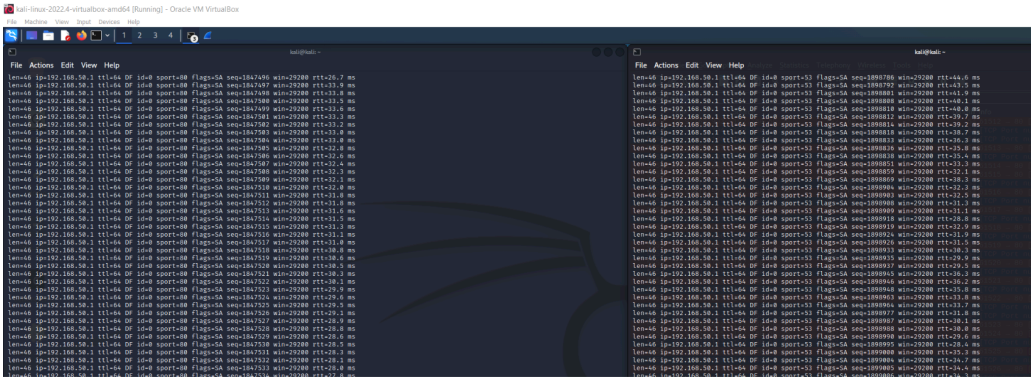
3. We then open up our terminal in our VM
    a. 

4. We use our nmap tool to see open ports. We note ports 80 (HTTP) and 53 (TCP) are open.
    a. 

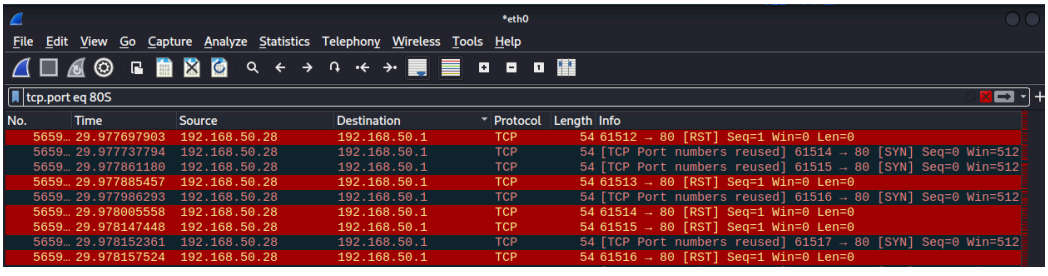
5. We Also note that our router is on and connected to the internet.

a. 

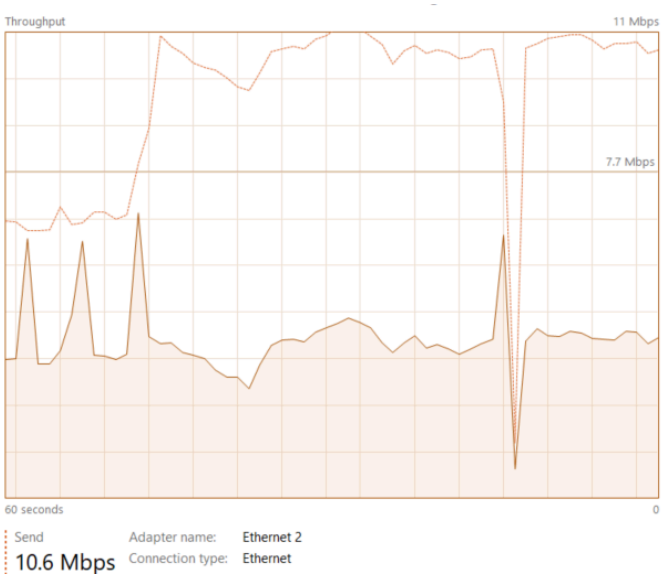
6. We will use the following two hping commands to send the attack.
    a. “sudo hping3 -i u100 -S -p 80 192.168.50.1”
    b. “sudo hping3 -i u100 -S -p 53 192.168.50.1”
        i. The “sudo” means we are running the command as a superuser in linux which gives the program elevated access to system controls and resources.
        ii. The “hping3” is a network testing tool that has many features such as ping testing, port scanning, and network probing.
        iii. The “-i u100” means we are going to send a data packet every 100 microseconds.
        iv. The “-S” is specifying we are sending a SYN flag. This initiates a tcp connection with the router.
        v. The “-p 53” and “-p 80” specifies the port number we are targeting.
        vi. The “192.168.50.1” specifies the target host. In this case we are targeting our home router.
7. We start both commands in two terminal windows.

a. 

8. After a few moments our network will start to slow. We can open up wireshark to investigate. If we filter by port 80 we can see 100’s of data packets being sent from the kali VM (192.168.50.28). We can also see the huge spikes in data traffic from our host PC

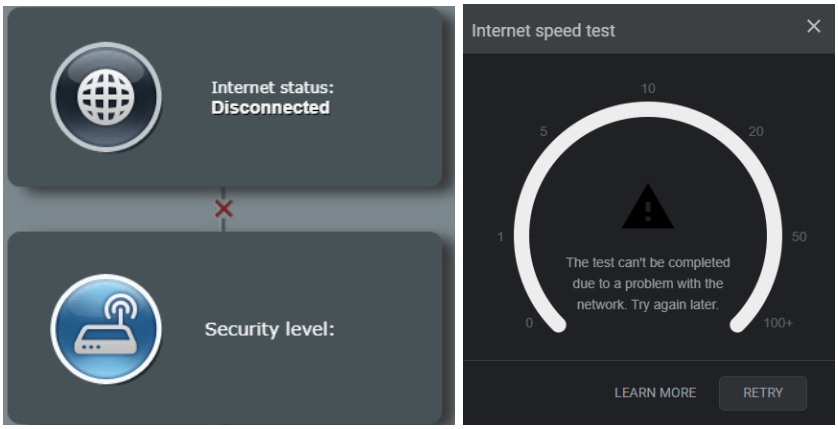
a. 

b.

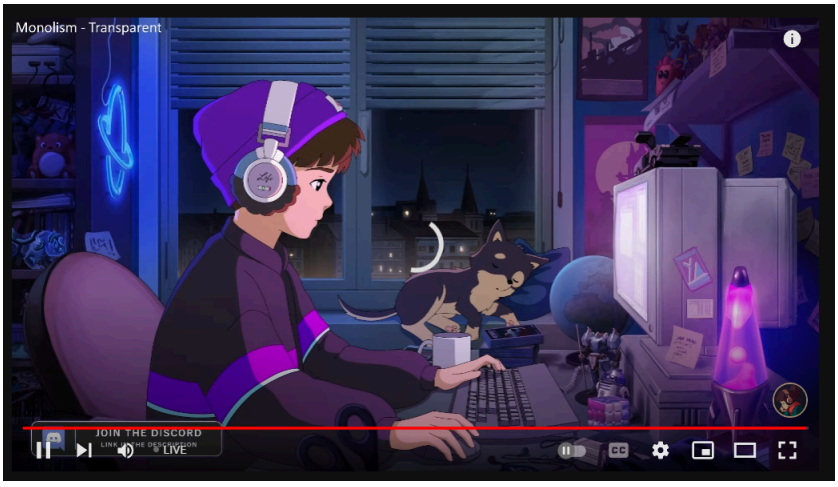


9. After a few minutes the network should go down. As you can see our router has been disconnected from the internet and no online services can load. No Internet

a.



b.



10. Once you kill the two terminal instances with ctrl + c. The internet connection should reestablish instantly. You can see the drop in data throughput once the programs are killed.
    a. 

11. That's it you have now successfully done a DoS attack!

XII. Insights

Some of the insights we gathered from this research and our lab is that the TCP SYN Flood attack method is quite effective against a target host. Even when using a single attack PC. We now understand how a DDoS attack using 100's of compromised PC's can be so deadly. We noted that once the attack began it took a few minutes for the network to slow down and eventually go offline. We do assume this time will change dramatically depending on the hardware of the host being targeted.

Research Question 1 Answered: We were very surprised to learn that the average false positive rate on average is about 0% and the False Negative Rate to be about 4.72%. [4, pg 70]

This makes sense to use since an IDS will probably not accidentally detect a DDoS attack if the network is experiencing low traffic. Given the nature of how DDoS attacks work. We would assume the somewhat high False Negative Rate is the IDS mistaking DDoS packets for legitimate ones since most of the attack vectors are using open ports such as 80 and 53. This is where we could see some improvements with deciphering a legitimate packet vs a malicious one.

Research Question 2 Answered: We discovered that the Detection Rate of these Intrusion Detection systems is very good. With a overall average detection rate of 99.04% with many different attack types tested such as UDP Flood, TCP SYN Flood, ICMP or ping Flood Attack. [4, pg 70]

This is great to see that modern IDS are able to reliably detect a DDoS attack. This is probably thanks again to the nature of the attack. As in receiving a flood of new data packets should raise some red flags.

XIII. Conclusions

This research project and paper examined DDoS attacks comprehensively, analyzing their impact on various networks and systems. We conducted experiments to identify the characteristics and patterns of DDoS attacks and evaluated the effectiveness of existing mitigation techniques. Through our experiment with virtual machines, we were able to gain a good insight into the way DDoS attacks are conducted. A con in our experiment was that we had to resort to using a virtual machine network, instead of real hardware. The pro to using real hardware would be that it would give us better insight on the full impact that a DDoS attack can do to someone's network. However, our virtual machine experiment was a success and showed what the real-world DDoS attack can look like on a Linux host machine.

Our findings show that DDoS attacks are still a significant threat, with attackers using increasingly sophisticated methods to evade detection and mitigation. Also, we emphasized the need for collaboration among security professionals and addressed the many threats associated with DDoS attacks. This paper went over a broad aspect of what DDoS attacks are about. Next, we plan to interview a cybersecurity professional. So, we can gain an understanding about how DDoS attacks are used and prevented in an organization setting. In conclusion, the study shows the importance of ongoing research and the development of an individual's network or their organization's network and systems against DDoS attacks.

XIV. Future works

A. AI and Machine Learning will be very beneficial to DDoS attacks in the future and even present. These technologies are trained to identify patterns and anomalies in network traffic that indicate a DDoS attack is happening. By using machine learning algorithms, security systems can more accurately detect and respond to DDoS attacks in real-time. Both can be used to analyze large volumes of network data and identify potential vulnerabilities that could be exploited by attackers. By identifying these vulnerabilities before an attack occurs, organizations can proactively address them and reduce their risk of falling victim to a DDoS attack. Both can be used to improve the accuracy of predictive models

that can anticipate future DDoS attacks based on past attack patterns and current network conditions. This can help organizations prepare and respond to attacks more effectively.

B. Interviews would be a great way to learn about DDoS attacks with people that work in the Cybersecurity field. This would allow us to have a better understanding of the techniques and methods that cybersecurity professionals use on a day to day basis to protect themselves and their organization against such attacks. They could also provide us with methods if you wanted to test a DDoS attack ourselves. They can give us details about how to safely do DDoS attack testing on our own network. Another, good part of interviewing people is it would allow us to know what type of common DDoS attacks do they see the most. Overall interviewing someone in the cybersecurity field would give us a lot of insight on DDoS attacks.

C. Real word testing of DDoS attacks. This would be very beneficial to us because it would allow us to observe and analyze the behavior of DDoS attacks in real-world scenarios. By conducting tests on actual networks and systems. Myself and Calvin can gain a better understanding of various techniques used in DDoS attacks, the results of the impact of the attacks on different types of systems, and the effectiveness of multiple defense mechanisms.

    It would allow us to find weaknesses in existing security measures and develop effective countermeasures to prevent DDoS attacks. Real-world testing provides a great understanding of the behaviors of a DDoS attack and can help us develop better tools and techniques to protect ourselves or company against such attacks.

D. Focusing on a deeper section of DDoS attacks than a broader approach can be beneficial to us in the research of DDoS attacks moving forward. This is because DDoS attacks in general are a large approach. There are many different aspects of DDoS attacks. This research project focused a lot on the whole understanding of what DDoS attacks are and just scratched the surface of what DDoS attacks can do. For example, a DDoS attack can be: DNS flood, UDP flood, SYN flood, ping flood, HTTP flood, Ping of Death Attack, and so many more types of DDoS attacks. In future work, it would be beneficial for us to research more on the common types of DDoS attacks and gain an insight into how to prevent them and how those types of attacks work.

XV. REFERENCES

1. Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak and Ali A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy" 2019, *Google Scholar*. pp. 1-8, Retrieved Retrieved April 2023.
2. LIANG TAN, YUE PAN, JING WU (Member, IEEE), JIANGUO ZHOU, HAO JIANG (Member, IEEE), AND YUCHUAN DENG, "A New Framework for DDoS Attack Detection and Defense in SDN Environment" 2020, *Google Scholar*. pp. 1-12, Retrieved April 2023.
3. NIKHIL TRIPATHI, NEMINATH HUBBALLI, "Application Layer Denial-of-Service (DoS) Attacks and Defense Mechanisms: A Survey" 2021, *Google Scholar*. pp. 1-33, Retrieved April 2023.
4. Mustafa Khambatta, "Comparative Analysis Based on Survey of DDOS Attacks Detection Techniques at Transport, Network, and Application Layers" 2019, *Google Scholar*. pp. 1-80, Retrieved April 2023.
5. SHI DONG AND MUDAR SAREM, "DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks" 2019, *Google Scholar*. pp. 1-10, Retrieved April 2023.
6. Mohammad Alhisnawi, Mahmood Ahmadi, "Detecting and Mitigating DDoS Attack in Named Data Networking" 2023, *Google Scholar*. pp. 1-23, Retrieved April 2023.
7. Riyadh Rahef Nuiaa, Selvakumar Manickam, Ali Hakem Alsaeedi, "Distributed reflection denial of service attack: A critical review" 2021, *Google Scholar*. pp. 1-15, Retrieved April 2023.
8. Neha Agrawal and Shashikala Tapaswi, Senior Member, IEEE "Defense Mechanisms Against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges" 2019, *Google Scholar*. pp. 1-27, Retrieved April 2023.
9. Rizgar R. Zebari, Subhi R. M. Zeebaree, Amira Bibo Sallow, Hanan M. Shukur, Omar M. Ahmad, Karwan Jacksi, "Distributed Denial of Service Attack Mitigation using High Availability Proxy and Network Load Balancing" 2020, *Google Scholar*. pp. 1-6, Retrieved April 2023.
10. Mazhar Javed Awan, Umar Farooq, Hafiz Muhammad Aqeel Babar, Awais Yasin, Haitham Nobanee, Muzammil Hussain, Owais Hakeem and Azlan Mohd Zain, "Real-Time DDoS Attack Detection System Using Big Data Approach" 2021, *Google Scholar*. pp. 1-19, Retrieved April 2023.
11. Ghafar A. Jaafar , Shahidan M. Abdullah , and Saifuladli Ismail, "Review of Recent Detection Methods for HTTP DDoS Attack" 2018, *Google Scholar*. pp. 1-11, Retrieved April 2023.
12. Dragan Peraković, Marko Periša, Ivan Cvitić, "ANALYSIS OF THE IoT IMPACT ON VOLUME OF DDoS ATTACKS" 2015, *Google Scholar*. pp. 1-10, Retrieved April 2023.

13. Jiangtao Pei, “A DDoS Attack Detection Method Based on Machine Learning” 2019, *Google Scholar*. pp. 1-6, Retrieved April 2023.
14. Mustafa Khambatta, “Comparative Analysis Based on Survey of DDOS Attacks’ Detection Techniques at Transport, Network, and Application Layers” 2019, *Google Scholar*. pp. 1-10, Retrieved April 2023.
15. Christos Douligeris, Aikaterini Mitrokotsa, “DDoS attacks and defense mechanisms: classification and state-of-the-art” 2004, *Google Scholar*. pp. 643-666, Retrieved April 2023
16. Ghafar A. Jaafar, Shahidan M. Abdullah, and Saifuladli Ismail, “Review of Recent Detection Methods for HTTP DDoS Attack” 2019, *Google Scholar*. pp. 643-666, Retrieved April 2023
17. Cloudflare, “What is a DDoS attack?” 2023, *Google Scholar*. pp. 1-6, Retrieved April 2023
18. OpenAI , “Our approach to AI safety” 2023, *Google Scholar*. pp. 1-5, Retrieved April 2023
19. N. James, “45 global DDOS Attack Statistics 2023,” *Google Scholar*. pp. 1, Retrieved April 2023
20. Telecomlead, “Why are ddos attacks becoming increasingly common?,” *Google Scholar*. pp. 1, Retrieved April 2023