The Impact Of DDOS And Ping Of Death On Network Performance

Waleed Iftikhar, Zunair Mahmood and Daniel Mago Vistro

Abstract: A network's performance can be affected by a number of things. Network attacks significantly reduce a networks performance and the most common attacks are the ping of death also known as DOS and the DDOS attacks. Networks of all kind whether on cloud or internet of things are affected by these attacks. Literature related to DDOS and its implications on various networks and their performance has been critically reviewed. Riverbed modeler was used to set up an experiment and Low orbit ion canon (LOIC) was used to perform a DDOS attack on the target website. Based on the outcome of the experiments conducted, DOS, DDOS, and Ping of death attacks significantly slows down the performance of the network.

Index Terms: Denial of service (DOS), Distributed denial of service (DDOS), Intrusion Detection Systems (IDS) ,Low Orbit Ion Cannon (LOIC), Network Performance, Ping of Death, Riverbed Modeler

1. INTRODUCTION

THE Internet has grown massively in recent years. With the growth of the internet the performance of day to day operations has significantly changed [1]. Users are now using internet means to conduct daily operations. The internet environment creates a network and this network needs to be secured from unwanted users and requests [2], for maintaining the performance of the entire network to a specific level. A lot of factors can affect the performance of a network. Ping of death and Distribution denial of service (DDOS) attacks are one factor that affects a network's performance [3]. Denial of service (DOS) will specifically target a network to affect the service provision of that network [4]. A typical DOS attack that sends packets which are more in size than the maximum capacity of a network is classed as a Ping of Death attack. A DDOS attack is used for a similar purpose but it is carried out by more than one number of entities [5]. DDOS attacks affect network performance significantly. These attacks are very lethal to a network if they are performed accurately. These types of attacks are causing significant financial loss to organizations around the world [6]. A typical DDOS attack can be launched used widely available tools. Some examples of such tools are Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC), etc. A number of network simulation tools are available to analyze a performance of a network. Some famous tools are ns2, Riverbed Modeler, etc. [7]. A simulation in this study will be performed using a Riverbed Modeler because it is most suited to our scenario. Riverbed Modeler provides a good graphical user interface to analyze results based on various performance metrics [8]. In the following study, information will be collected that is related to DDOS and ping of death attacks on various networks. There is also evidence of some mitigation techniques which are appropriate only for specific scenarios. DDOS attacks have affected cloud computing networks as well as the Internet of Things (IOT) [9]. The impact of these attacks is causing serious financial damage to the cloud environment. The devices connected to an IOT network can be used by unwanted users if mitigation techniques are not applied. We will be using Riverbed modeler to demonstrate a ping of death attack. The results will be extracted for a network running without the interference of DDOS and DOS attack and one network running with the interference of DDOS and DOS attack and their performance will be compared. A DDOS attack will also be performed on an up and running website. The tool used for this purpose will be LOIC as it is simple and easy to use.

2 LITERATURE REVIEW

Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks are the primary factors due to which availability of a system can be destroyed. [10] & [11]. DOS and DDOS attacks send a huge number of unnecessary requests to a network server, the unnecessary requests prevent the intended user's request to get through to the server hence affecting the network and it results in the unavailability of resources to the intended users. DDOS attacks are performed by more than one person or by the use of bots [12], while DOS attack is carried out by an individual, either a person or a bot [13]. DDOS attacks are further divided into three main categories: protocol, volume based and application layer attacks. The protocol attack will basically flood the server with a lot of packets and the severity of this attack is measured in packets per second. The common type of protocol attacks includes Ping of Death and TCP SYN flood. Volume-based attacks will target the bandwidth of the attacked site and the severity of this attack is measured in bits per second. Most common types of volume-based attack include ICMP flood and UDP flood. Application layer attacks aim to crash the web server by sending a lot of unnecessary requests, the severity of this attack is measured in requests per second. The common types of application layer based attacks include Zero-day attack and Slowloris [14].

2.1. DDOS attack mitigation through Intrusion Detection Systems (IDS)

A research [15] was conducted on the effects of UDP flood and ping of death attacks and how an intrusion detection system can detect these possible attacks. DDOS attacks are described as the most occurred attacks in networks and especially MANET networks. The research focused on mainly two types of attacks and that was UDP flood attack and Ping of Death. These attacks relatively look simple but cause a significant amount of damage to the network. An intrusion detection system was proposed to detect these two attacks in a MANET so it can be secured. The attacking node was identified by calculating the number of packets it sends to the network. The results showed that the number of packets sent by a node during these attacks is significantly higher than compared to a normal node so identifying a potential attacker is relatively easier. They concluded that the proposed intrusion detection system will notify the possible attacking nodes and notify the system about such activities. The number of packets sent by a node can be set as a threshold as suited to the

requirements of the network. The researches recommended that there must be work done in the future to identify the attackers from a network. A research was conducted in Singapore [16] to explore the Network intrusion detection systems that tackle DDOS attacks specifically. Intrusion detection systems were classified into two categories and they were host based or network based. The host-based intrusion detection systems identify threats from within the network while the network intrusion detection systems identify threats that are in the incoming traffic to a network. For this research Microsoft's Hyper-V was used which is used to set up a virtual network. Four virtual machines were created with a network controller interface which represents four computers connected to each other through Ethernet cables. The network intrusion detection system (NIDS) was set up using Snort and one of the four computers in the simulated network was considered as a NIDS. After setting up the environment and writing snort rules to detect DDOS attacks, the attacks were going to be performed using Low Orbit Ion Cannon (LOIC) tool. The LOIC tool sent in an unlimited number of packets to the network but snort identified the attacks and also showed us from which IP address the attacks were coming. Ping of death attack was also tested and snort was configured to detect this by determining the size of the packet. Detecting these two attacks was a success but that doesn't mean the problem is finished because cyber-attackers keep on finding new ways to target a network and if a particular rule from snort configuration is missing then that attack can be carried out. The aim for the future researchers should be to write more complicated rules so a maximum number of possible attacks can be prevented using these tools. This will significantly help improve the network performance and minimize unwanted interruptions.

2.2. DDOS attack mitigation through network simulation tools

The challenge that DDOS poses to the security and the performance of the internet is also discussed by Jun [17]. This article proposes a DDOS prevention system and then evaluates it by using OPNET as a simulation tool. The method that is proposed is, to inspect packets from incoming traffic and then they are passed through a number of checks, the rules are designed based on volume, traffic intensity etc. Since every packet inspection is tedious hence the rule is to inspect one in five packets randomly. The simulation was carried out on OPNET and consisted of a star topology which used 50 nodes, 1 server, and 3 routers. 25 of the nodes were considered as attackers and 22 of them were normal nodes while 3 nodes were peer to peer nodes. Normal traffic was sent through the nodes except attacker nodes. The DDOS attack once set out was caught within 6 seconds of its initiation. This method proved to be successful to detect DDOS attacks using a small amount of traffic as a sample. This is a very interesting proposition to say the least, however, there needs to be an experimental setup for a huge amount of data over bigger networks and with more capable attackers. The impact of DDOS on a peer to peer network (P2P) was studied by Simon [18]. The tool that was used as a testbed was OurGrid environment which is very suitable for emulating a P2P environment. The basic aim of the research was to carry out four research tasks. The first analysis was done by exploiting a SYN flood attack, this had a significant impact on the CPU and the network performance was severely affected. The second task was the analysis of HTTP Get- flood attack and this affected the network performance severely as well. The victim's server was overloaded only in about 20 seconds even with the usage of a small number of bots. The third task was the analysis of IPv4 and IPv6 under DDOS attacks. IPv4 and IPv6 are equally vulnerable to DDOS attacks but, once under attack, the speed impact under IPv6 is less as compared to an IPv4 and this was confirmed due to the small Packet header size in IPv6. The fourth task was to analyze the firewall and IP tables in both IP versions. The conclusion was that IP tables have enough capability to defend against DDOS attacks no matter the IP version. This testbed can be further used to explore more kinds of DDOS attacks and their impact on how a peer to peer to the network is affected. SYN flooding attack is also a type of attack that falls under the DDOS category. To successfully mitigate this attack, to secure a network and its performance a method was proposed by Hussain [19]. The proposition was basically proposed on the concept of the honeypot and how it is used to attract attackers, then identified and then they can be permanently blocked from the network so they do not interrupt again. Three tools were used in this research and they were Ettercap, Hping3, and Wireshark. Ettercap and Hping3 were used to perform flood attacks while Wireshark will analyze the details about the traffic. The mitigation algorithm sniffs out packet using Wireshark and then uses windows firewall rules to block the DDOS attack. The application built by the researchers was built on .Net Framework. The technique proved to be a success and now there is a need to move this technique onto the cloud framework. A honeypot would attract cloud computing hackers and similar rules can be applied to mitigate those SYN flooding DDOS attackers.

2.3. DDOS attacks on a cloud environment

A research was conducted on the impact of DDOS attacks on cloud environment [20]. The impact of DDOS on cloud environment was classified into three categories by the researchers. The first impact was Direct Denial of Service and in this case, the cloud computing operating system provides more computing power to the service with a higher workload. So, in this case, an attacker will be using most of the cloud computation power unnecessarily which affect the performance of the real users. The second impact was Indirect Denial of Service. The cloud network under attack may use more than one type of service and the attackers can flood a particular service which also results in affecting the performance of other services on this network is known is Indirect Denial of Service. In cloud computing phenomenon the users pay for what they use, the attacker's activities increase the load on the network which results in high bills for the users and this is the third impact and is classified as Accounting Cloud computing. These impacts damage the network performance of a cloud computing network severely. To counter these three impacts various defense mechanisms are discussed by the researchers, Filtering Routers, Load Balancing, Disabling IP Broadcasts, Audit cloud service usages (by maintaining logs), Application of security patches, disabling unused services and performing intrusion detection. The researchers concluded that these issues in the cloud environment cost very high to fix and are one of the reasons why organizations around the world do not favor cloud computing. The biggest hurdle in cloud computing migration is the security obstacle. DOS and DDOS attacks have had a

significant impact on cloud computing [21]. Halabi discusses that the intention of DOS and DDOS attackers can be to either overload a network's resources so its performance is affected or send in malicious packets which have the ability to exploit vulnerabilities. The defense techniques can be used such as statistical methods, packet analysis, and intrusion detection systems. The researcher proposes different tools to simulate these attacks and study how they affect the network. The recommended tools were Snort, OpenStack, and Eucalyptus. VM ware can be set up to behave as a cloud network. The researcher concludes that DOS and DDOS attacks are the biggest security threat to cloud computing. Cloud service performance needs to be measured by using specific metrics and whenever a solution is proposed it needs to be simulated to demonstrate its effectiveness. Tools to simulate are available in abundance, however, there is a need to introduce new defense mechanisms so they can be tested and then applied in the real world. Cloud computing is replacing a lot of traditional technological infrastructures. A research [22] was conducted on the impacts of DDOS on cloud computing. More than 20% organizations around the world reported that they have been the victim of the DDOS attack. The researchers discovered the average monthly financial damage of DDOS attacks on cloud computing to be around 444,000 USD. The cloud features are very inviting for DDOS attackers because cloud infrastructure has many loopholes. The DDOS attacks are significantly reducing the bandwidth of a network, resulting in bad performance and higher bills. The techniques to prevent these DDOS attacks are also discussed in the paper. Challenge response can be used to differentiate human and bots, hidden servers help hide servers from public attackers, restrictive access enables the right people in the network and by limiting maximum usage of a resource prevents significant losses. Some mitigation techniques are also discussed by the researchers and they deal with each level of a cloud network. ISP level defense can be used to defend externally, then there should be application level defense and system defense. System defense should be applied to the servers and operating systems individually. The study concluded that DDOS attacks are impacting the performance of cloud computing significantly and there need to be measures taken to prevent these attacks. The discussion is done on how to detect, prevent and mitigate these attacks through various techniques. Further work needs to be done on testing the proposed multilayer model and how effectively it prevents DDOS attacks.

2.4. DDOS attacks on the Internet of Things (IOT)

A research was conducted on DDOS attacks on the internet of things (IOT) [23]. IOT is relatively a new concept and is spreading rapidly. Confidentiality, integrity, availability, and authenticity are necessary services for IOT. The DDOS attacks that are common on IOT were identified as UDP flood, ICMP/PING flood, SYN flood, ping of death and zero-day DDOS. DDOS attacks can occur at all layers of IOT network. Perception layer attacks include Jamming, Kill command attack and De-synchronizing attack. Jamming prevents tags to communicate with the reader, Kill command attack disables the command tag which limits the networks functionality and De-synchronizing attack disables the authentication capabilities of an IOT network. DDOS attacks on network layer can happen at the Wi-Fi layer or ZigBee. When a large amount of data is sent to a Wi-Fi network it collapses in terms of responding efficiently and if the attacker is capable enough to spoof the IP address than the attacker can use the resources that are available on the Wi-Fi network. DDOS on application layer can also affect the IOT network. Reprogramming attack on application layer can create infinite loops which result in disabling of the resources to the intended users. Path-based DOS can inject packets that have already been used or spurious packets can be introduced into the network. The researchers concluded that there are many possible threats to an IOT network, DDOS attacks are relatively easier to be targeted on these networks through brute force because the processing power and memory of these networks is relatively lower than compared to other networks. A research [24] was conducted on the Mirai botnet and its variants and how they can affect the Internet of things through DDOS attacks. The first recorded incident of DDOS attack using Mirai dates back to September 2016. Brian Krebs is a security consultant and his website was hit with 620 Gbps of traffic, simultaneously another attack was being planned using Mirai and this time the target was French web host targeted with 1.1 Tbps of traffic. Mirai has now gone open source and there will be many variants coming out in the near future and this means danger for all kinds of networks and especially IOT. The Mirai bot operates in seven basic steps, first it uses brute force to configure the username and the passwords, second, after being successful in the first step the bot changes the ports that are used for server communication on the present device, third, it checks for more victims on the network using the command and control center and also communicates its current status back to the bot server using tor, five, the loader takes control of the machine and sets it up for attack, six, the botmaster can now control the device using command and control center, seven, the bot initiates the attack and performs 10 various types of attacks. The researcher explained in detail the signatures and procedures of what a Mirai bot can do and he further explains that IOT is a noticeable target due to many vulnerabilities. The IOT vulnerabilities which make it a perfect target for DDOS is that an IOT network is running 24/7, very weekly secured until now, extremely poor maintenance and minimum interactive user interfaces. The researcher emphasizes on the importance of security tools which need to be developed to prevent DDOS attacks on IOT so they can be secure and their performance is not affected by dangerous bots such as Mirai. DDOS attacks are impacting all kind of networks. The performance and the security of a network are always under threat even though security measures are already taken. Work needs to be done on securing networks to the maximum extent. Simulation tools provide us with an alternative way to evaluate the techniques or defense mechanisms that have been proposed. Based on the findings it is safe to say that DDOS attack prevention techniques need to be designed based on the required network. Cloud computing and Internet of things have huge vulnerabilities and they need immediate attention if they are to be secured, these technologies cannot be used at any critical organization until some kind of a defense technique is applied onto the network. Traditional honeypot technique seems to be working in a cloud environment but this is just simulation results, it needs to be tested in the real world environment. Multilayer technique for IOT sounds like a good proposition based on the concept but it is still not simulated. It is quite evident that the DDOS attack is going to happen no matter what, the real question is, what do you do to mitigate it? Or

how do you prevent it from someone using variable IP addresses? To be able to answer such questions we need to take a deeper look into how a DDOS and Ping of Death attack really occurs.

3 RESEARCH METHODOLOGY

An effective analysis of a ping of death attack requires it to be implemented on a network simulation tool. The selection of a network simulation tool is a challenge and it totally depends on the characteristics of a specific experiment. The experiment setup in this study is deployed on Riverbed Modeler. According to [25], the riverbed modeler is the leading network simulation tool in industry and has a good graphical user interface for analyzing the results of an experiment. Riverbed modeler will be used to analyze a Ping of death attack which is also known as Denial of service and another attack that will be discussed is the distributed denial of service attack. Following the selection of an effective tool, the network topology for the experiment is created at first. Once the network topology is created some parameters will be configured and these parameters will be discussed in the next section. Once the parameters are set the simulation is ready to run for a specific period of time and after a successful execution of the simulation, it is ready for analysis using various graph-based outputs. The analysis will be based on the contrasting of network performance based on different scenarios. Following the analysis of network simulation on Riverbed modeler, a website will be attacked using a Low orbit ion cannon tool. LOIC is an effective tool for creating a massive amount of network traffic [26] and is suitable for our experiment. The website will be the first run and show that it is up and running and then a DDOS attack will be performed on the website and what happens after the attack will be analyzed.

4 SIMULATION

The entire simulation process is discussed in the following sections. The first section will discuss the setting up of a riverbed modeler and the following section will discuss the setting up of LOIC.

4.1 Riverbed modeler scenarios and configuration

Figure 1 *First Scenario - The original network*

The first scenario shown in the figure above is the original network free from any kind of attackers. It simply shows two nodes that are named as “Registraion_office” and “Finance_office” connected to a single server over a wireless network. The wireless network is created using a switch which is further connected to a Cisco router and then connected to an internet connection. Similarly, the server is connected to a Cisco router and then provided internet access. The “Application_Config” and “Profile_Config” are implemented to configure specific network properties. The “Registration_Office” is a simple Ethernet workstation which supports a registration profile that is created using “Profile_Config”. Similarly, the “Finance_Office” supports a finance profile that is also created using the “Profile_Config”. The internet connection for the entire scenario is provided using an “ip32_cloud” model available in the riverbed. The server that is connected on the other side of the network is configured to support all kind of services that are sent to the server. The two profiles created using “Profile_Config” are the registration and finance profiles. The attribute of the registration profile is set up using unlimited repeatability. Similar procedure was followed while creating the finance profile in “Profile_Config”. The routers connected to the internet is done using the PPP_DS1 cables while the rest of the network is connected using simple 10Base LAN cables.

Figure 2 *Scenario 2 - Ping of death (DOS)*

The scenario 2 is the duplication of scenario 1 with some minor changes. The changes include an introduction of an attacker as it can be seen in figure 2. The “Attacker” is the model ppp_wkstn available in the riverbed modeler. The connection of the attacker to the server is done using ip_ping_traffic which simply represents the IP ping traffic. The IP address of the attacker is set as 192.0.5.1 and the destination IP address is that of the server which is 192.0.1.9. The repetition of the attacker is configured as an unlimited repetition count, so it can send unlimited requests to the server. On the top right of the figure, we can see another change and it is the addition of IP attribute config and is named “IP attributes”.

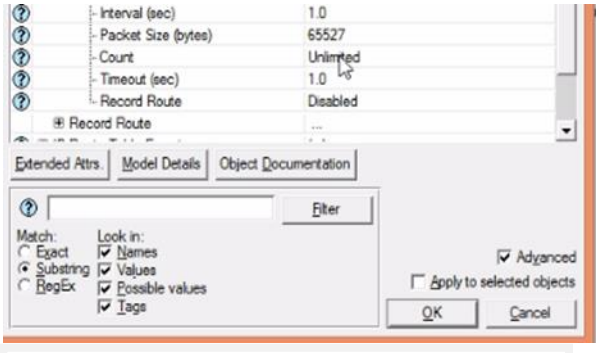

Figure 3*: IP attribute configuration*

To set up a Ping of death attack one attribute is really critical to be set accordingly. The figure below shows the configuration of IP attributes. The specific attribute is the Packet size and is set as 65527 with an unlimited count.

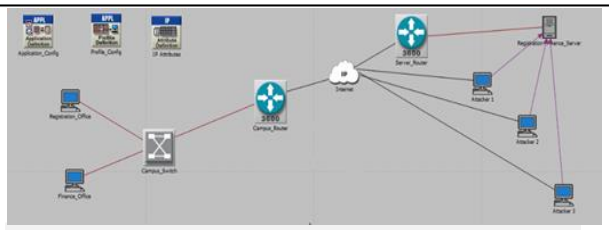

Figure 4: *Scenario 3 - DDOS attack*

The third scenario is the DDOS attack setup and it is the duplication of scenario 2 with very little changes. The number of attackers is increased but this is what happens in a typical Distributed denial of service attack, which is basically a division of an attack based on a number of attackers. This attack is defined as more dangerous and is typically difficult to protect against. The attributes of the attackers in this scenario is the same as that of the attacker in scenario 2.

4.2 Low Orbit Ion Cannon Scenario and Configuration

The interface of LOIC is shown in the figure below. First, the target is selected and the address of the live website is entered in the URL field. The selected target's IP address is shown below. The message to the attacker can also be input. There are further options to adjust the speed of the attack and also the method of attack in the drop-down menu.

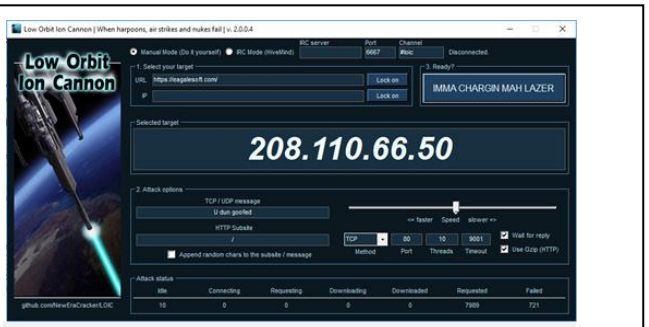

Figure 5: *LOIC Interface*

5 RESULT AND DISCUSSION

The result section is further divided into two parts. The first section will analyze the results generated in the riverbed modeler, the second section will discuss the DDOS attack using LOIC.

5.1 Riverbed Modeler Discussion and Analysis

The resulting analysis will begin with the second scenario because one scenario alone is not enough for providing a comparison of the network's performance.

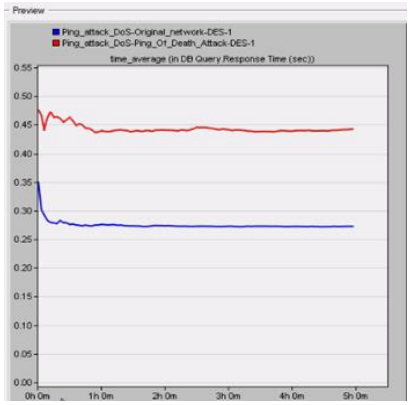

Figure 6: *Scenario 1 and 2 DB response*

It can be clearly seen in figure 6 that the DB query response time of the original network which is depicted by the blue line is clearly better as compared to the response time of the network which is under a ping of death (DOS) attack. This comparison justifies that the involvement of a DOS attack on the network has significantly affected the performance of the entire network.

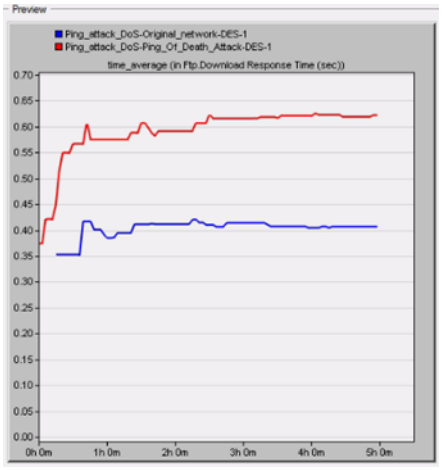

Figure 7: *7 Scenario 1 and 2 FTP response*

Figure 7 clearly shows the FTP response time of scenario 1 and 2. The original network has a significantly better response time as compared to the response time of the network which is under Ping of death attack.

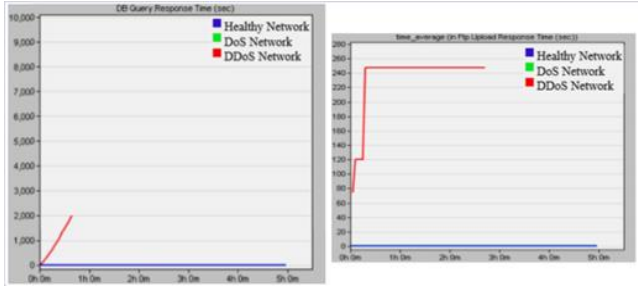

Figure 10: *Results of DOS and DDOS attacks [27]*

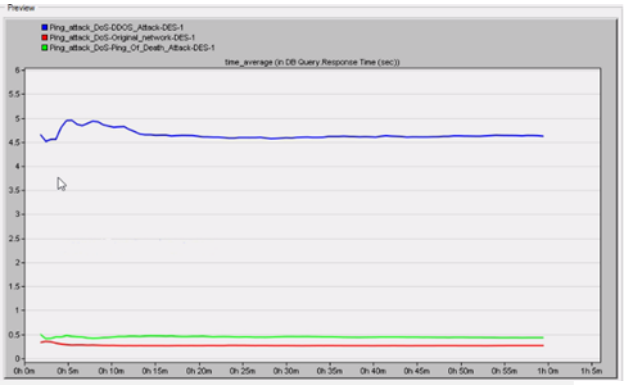

Figure 8: *All scenario DB response time*

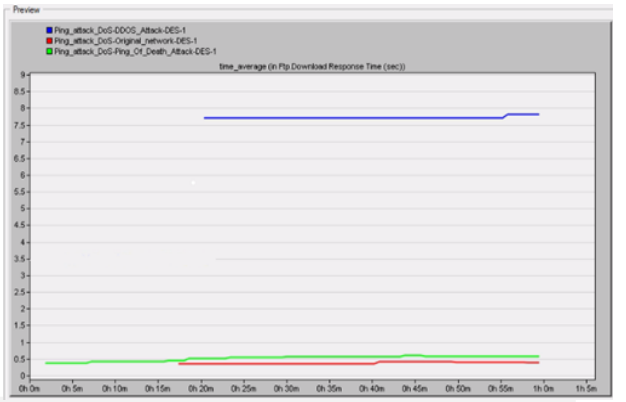

Figure 9*: All scenario FTP response time*

The comparison of all three scenarios with respect to the DB response time can be seen in figure 8. The major difference when running scenario 3 was the time of the simulation when comparing scenario 1 and scenario 2 the simulation was run for 5 hours but when scenario 3 was run for longer than 1 hour it kept on crashing. The reason for crashing can be the processing power limitation of the computer used. The results in figure 8 can clearly differentiate that the DDOS attack is much more dangerous as compared to a DOS attack. The response time is slow in a DOS attack (green line) but it is even slower in the DDOS attack (blue line). Similarly, the FTP response time in figure 9 depict a similar behavior as in figure 8.

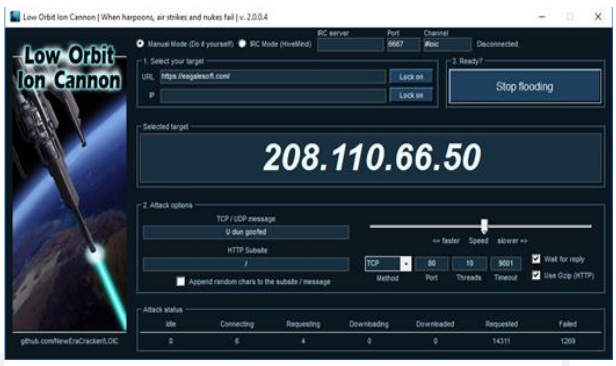

Figure 11: *Results of DOS and DDOS attacks [27]*

The discussion of all the scenarios in the figures that are shown above concludes to a common result. The involvement of a DOS or ping of death significantly reduces the response time of a network but DDOS attack proves to be more lethal and will reduce the network response even more than just a DOS attack. On top of that prevention against a DOS attack can be done more easily as compared to a DDOS attack. This is so because the DOS attack is coming from one specific IP while DDOS attack comes from various IP addresses, so detecting one IP address and preventing it from attacking the network is easier as compared to the detection of a number of IPs and preventing them.A similar experiment was set up by [27] using similar network topologies and scenarios with the same configurations as in this study. The result of that study clearly shows the increased response time in a DDOS attack while the original network is performing seamlessly. This research has reached a similar conclusion of the effect of DDOS and DOS attacks as in the study of [27].

5.2 Low Orbit Ion Cannon DDOS Attack

The DDOS attack on a specific website will be carried out using LOIC and the initial interface of this tool is shown in figure 5 in section 4.2. The website has already been selected and the attack is performed.The LOIC interface during an attack can be seen in figure 11. On the bottom of the figure, we can see the number of requests it has sent to the target website along with the number of requests that have failed to reach the target website. The attack is repetitive and keeps going until the stop flooding button is clicked and it is at the top right of figure 11.

Figure 12: *Website up and running*

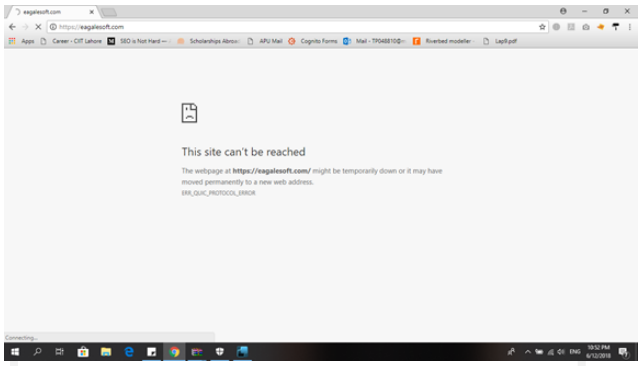

Figure 13: *Website unavailable*

The figures 12 and 13 show the website before and after a DDOS attack using LOIC. In figure 12 it can be seen that the website is up and running while after the DDOS attack the website is unavailable. The server that the website is hosted on has stopped responding to valid requests after a DDOS attack and is completely unavailable.

6 CONCLUSION

A number of studies were reviewed on how the networks around the world are being affected by DOS and DDOS attacks. Some studies even proposed experiments on how to prevent these attacks but these proposals need further validation by implementing them in a real-world scenario. The experiment in this study had a simple network which consisted of two Ethernet workstations connected to a server over an internet connection. The introduction of an attacker who is sending unlimited requests to the server reduces the performance of a network. DOS attack is lethal but DDOS attack proves to be more lethal when the results were analyzed. The results of this study were compared to another study and the results in both the studies had a similar concluding result. Another tool that is LOIC was used to demonstrate what happens to an up and running website when it encounters a DDOS attack. The results were as expected and the DDOS attack crashed the website server it was hosted on and the website was unavailable.

ACKNOWLEDGMENT

First of all, we would like to express our deepest gratitude to the God who has given us the knowledge and wisdom so that we can finish this research. Thank you for our family and colleagues who in a way always support and encourage us to work hard.

REFERENCES

[1] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, and J. K. Kalita, “Network attacks: Taxonomy, tools and systems,” J. Netw. Comput. Appl., vol. 40, no. 1, pp. 307–324, 2014.

[2] K. Prasad, J. Poonam, and K. Gauri, “Data Sharing Security and Privacy Preservation in Cloud Computing,” IEEE Internet Comput., pp. 1070–1075, 2015.

[3] B. Singh, “Defending Against DDOS Flooding Attacks- A Data Streaming Approach,” IJCRT, pp. 38–44, 2015.

[4] K. M. Prasad, A. R. M. Reddy, and K. V. Rao, “DoS and DDoS Attacks: Defense, Detection and TracebackMechanisms -A Survey,” Glob. J. Comput. Sci. Technol. E Network, Web Secur., vol. 14, no. 7, p. 19, 2014.

[5] J. J. Santanna et al., “Booters - An analysis of DDoS-as-a-service attacks,” Proc. 2015 IFIP/IEEE Int. Symp. Integr. Netw. Manag. IM 2015, pp. 243–251, 2015.

[6] S. Behal, K. Kumar, and M. Sachdeva, “Discriminating flash events from DDoS attacks: A comprehensive review,” Int. J. Netw. Secur., vol. 19, no. 5, pp. 734–741, 2017.

[7] C. W. Lee, K. Kim, B. H. Roh, B. Roh, and J. Choi, “SMAT: Simulator monitoring and analysis tool,” Int. Conf. Ubiquitous Futur. Networks, ICUFN, vol. 2015–Augus, pp. 482–485, 2015.

[8] A. Nayyar and R. Singh, “A Comprehensive Review of Simulation Tools for Wireless Sensor Networks (WSNs),” J. Wirel. Netw. Commun., vol. 5, no. 1, pp. 19–47, 2015.

[9] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, M. Rajarajan, and R. Buyya, “Combating DDoS attacks in the cloud: Requirements, trends, and future directions,” IEEE Cloud Comput., vol. 4, no. 1, pp. 22–32, 2017.

[10] Z. Xiao and Y. Xiao, “Security and privacy in cloud computing,” IEEE Commun. Surv. Tutorials, vol. 15, no. 2, pp. 843–859, 2013.

[11] Cloud Security Alliance, “The Notorious Nine. Cloud Computing Top Threats in 2013,” Security, no. February, pp. 1–14, 2013.

[12] N. Goodman, “A Survey of Advances in Botnet Technologies,” pp. 1–9, 2017.

[13] Q. Yan, F. R. Yu, Q. Gong, and J. Li, “Software-defined networking (SDN) and distributed denial of service (DDOS) attacks in cloud computing environments: A survey, some research issues, and challenges,” IEEE Commun. Surv. Tutorials, vol. 18, no. 1, pp. 602–622, 2016.

[14] M. A. M. Yusof, F. H. M. Ali, and M. Y. Darus, “Detection and Defense Algorithms of Different Types of DDoS Attacks Using Machine Learning,” Lect. Notes Electr. Eng., vol. 488, no. 5, pp. 370–379, 2018.

[15] A. A. Acharya, K. M. Arpitha, and B. J. Santhosh Kumar, “An intrusion detection system against UDP flood attack and ping of death attack (DDOS) in MANET,” Int. J. Eng. Technol., vol. 8, no. 2, pp. 1112–1115, 2016.

[16] C. K. Chan and A. W. T. Yeoh, “Development of a Platform to Explore Network Intrusion Detection System (NIDS) for Cybersecurity,” J. Comput. Commun., vol. 06, no. 01, pp. 1–11, 2018.

[17] J. Jun, D. Lee, and S. Kim, “DDoS Attack Detection Using Flow Entropy and Packet Sampling on Huge Networks,” Thirteen. Int. Conf. Networks., no. c, pp. 185–190, 2014.

[18] M. Šimon, “DDoS testbed based on peer-to-peer grid,” Int. Conf. Signal Process. Commun. Power Embed. Syst. (SCOPES)-201, pp. 1181–1186, 2016.

[19] K. Hussain, S. J. Hussain, V. Dillshad, M. Nafees, and M. A. Azeem, “An Adaptive SYN Flooding attack Mitigation in DDOS Environment,” IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 16, no. 7, p. 2016, 2016.

[20] R. Mehta, “Distributed Denial of service Attacks on Cloud Environment,” Int. J. Adv. Res. Comput. Sci., vol. 8, no. 5, pp. 2204–2206, 2017.

[21] T. Halabi and M. Bellaiche, “How to Evaluate The Defense Against DoS and DDoS Attacks in Cloud Computing: A Survey and Taxonomy,” Int. J. Comput. Sci. Inf. Secur., vol. 14, no. 12, pp. 1–10, 2016.

[22] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, “DDoS attacks in cloud computing: Issues, taxonomy, and future directions,” Comput. Commun., vol. 107, pp. 30–48, 2017.

[23] S. Agrawal and D. Vieira, “A survey on Internet of Things,” Abak{ó}s, Belo Horiz., vol. 1, no. 2, pp. 78–95, 2013.

[24] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and other botnets,” Computer (Long. Beach. Calif)., vol. 50, no. 7, pp. 80–84, 2017.

[25] G. Ferrari and P. Medagliani, “Performance Analysis of Zigbee Wireless Sensor Networks,” 2018 2nd Int. Conf. Inven. Syst. Control, no. Icisc, pp. 1272–1277, 2018.

[26] D. Freet and R. Agrawal, “A virtual machine platform and methodology for network data analysis with IDS and security visualization,” Conf. Proc. - IEEE SOUTHEASTCON, no. Vm, 2017.

[27] F. Yihunie, E. Abdelfattah, and A. Odeh, “Analysis of Ping of Death DoS and DDoS Attacks,” IJCRT, pp. 3–6, 2017.