Cyber-Security: Dos Attack Outcomes are Dangerous

M. Mattah Islam, Safiullah Shahid, Khush Bakhat Awar, Rashid Khan, and Muhammad Sohail

Abstract — Dos attacks are an attractive and hot topic nowadays because it is very common for attackers to make a victim and exploit it. In this paper, different kinds of techniques and commands have implemented and contrast for the outcomes of these attacks. By performing, experiments problems are identified. By following experiments, the goal is prevention and mitigation of Dos attacks at large extent by knowing the outcomes of the attacks. For proving the work, different types of experiments are performed on different platforms and observed that Dos attacks are how dangerous to our systems. In this paper, hping3 and syn flooding are performed. Hping3 is used for sending packets in a modified, crafted form. It is the networking tool used by developers to perform a DOS attack. SYN flooding is used for sending so many requests in an insane amount to the server and used all of the resources of the server.

Index Terms — DOS, DDoS, DOS Outcomes.

I. INTRODUCTION

Information Technologies emerging in our lives Cybersecurity refers to protection to data [1], information from being fabricated [2], theft [3], modification [4], compromised [5], compression [6], attacked [7], damaged or stolen [8]. It is a knowing of potential information threats, such as malware, viruses, and other malicious activities. It is the protection of computers from different misshapes. Mainly it's a protection strategy to protect all this related to software and hardware; it is the practice of protecting different things programs, networks, servers from all digital attacks. When implementing some effectual security measures is very practically challenging nowadays because there are so many equipment's related to cybersecurity than people in the world, and cyber attackers are growing so speedy in the digital world. It is a very needy practice because it is used by the important. After all, government, military, corporate, financial, and medical organizations to store and process unlimited digital data in their computers, servers, hard disks, and all memory units. In figure1, there is a flow chart for moderating DOS attack on how packets work from top to bottom.

They need to protect this information, which is in the form of digital information stores in Computer Systems; these organizations have very important and significant data stored in their systems, which must be protected by any means. Cybersecurity is the term used to protect the data.

Many data are shared between the systems worldwide by networks. Anyone can access it, so it is a very risky situation.

Fig. 1. Flow Chart of the Proposed Algorithm.
II. RELATED WORK

It is stated that there are different kinds of DOS attacks, results, or outcomes. In this paper, we presented different types of outcomes in the form of figures after performing experiments by which the system suffers after the DOS attacks. Temperature, performance, energy, speed, etc. these types of problems are discussed in this paper. Denial of Service tools and strategies by which there is a clear indication to actual digital attackers it is a very serious problem. That is why different researchers have offered so many mitigation and detection techniques, and these techniques are recommended to conquer with Denial of Service attacks [9]. In this paper, it is a discussion in existing commands and methods; there are dangerous outcomes of Denial of Service. There are two types of attacks, i.e., Reflector Attacks Direct Attacks. In this paper, we have discussed the direct attacks. Different methods can occur denial of Service attacks into various categories, and; this was the main thing to this paper that the after outcomes are visualized. So attacks are made by different methods on the different environments by using both types of DoS Attacks. They classified into two types hping3 and SYN flooding. Many vulnerable computers on the Worldwide are used for DoS attacks [10]. Damages occurred after the attacks and well-known Dos tools and methods are used to explain this scenario base attacks, and they do make sense.

Proposed algorithm is shown in Fig.1. When a new packet is received, IP and MAC is extracted and then checked either this IP already present in network table. If IP is present in the network table then move to next step and if it does not exist, store it in network table. The next step is to detect attack by comparing the MAC_X and MAC_Y and then send to attack detector. If there is no attack detected, process the packet normally and if attack is detected, send an alarm packet.

A. Hping3

Researchers have given a road map for the Distributed Denial of Service model [11]. In the paper, they have shown detailed knowledge about how to mitigate Denial of Service and Distributed Denial of Service attacks in the presence of clock drift. Hping3 is used to send packets to the victim by the attacker, and these packets are fabricated, crafted, and in custom form as depicted in Fig. 2.

Hping3 is very useful for attackers and so strong it can be used to do the following things [12]. Path MTU discovery Fire walk likes usage. Advanced port scanning Net Test performance using different protocols, packet size, TOS (a type of service), and fragmentation. Traceroute-like under different protocols. Transferring files between even fascist firewall rules. Test firewall rules. The attack can be launch by sending a specially crafted payload to web servers or systems. This paper has a Slow Rate Denial of Service attack against HTTP/2 services. They performed an attack against three special web servers and got that all of them are to these attacks.

B. SYN Flooding

In the SYN flood given in Fig. 3, there are a huge number of requests to the system or server is send and continue the process of sending requests until it uses all of its resources [13]. In this paper, we have given the brief discussion that it cannot manages all the network requests, behavior programmatically changed. Using this technique, we can facilitate cybersecurity applications due to the capacity of the environment. Denial of Service attack tries where so many attackers send large packets to one specific server.

They create for attack purposes and send a huge number of requests to the system continuously using the ping command. When we repeat, they came to know that it decreases the performance Experiments are performed, and we give the results as well to prove the stance. The firewall is very important, and it is needed for Dos attacks and decrease the performance of the system by doing these experiments. The focus to eliminate network attacks, a more practical approach is to trace back the attacks stop and source the attacks before it begins. Gathering the attacks, digital information is needy in attack trace-back. They give a live capture device to record the attack effectively without disturbing the original network performance. The device can be loaded with anti- Denial of Service technique so forensic data gathering when is performed even under Denial of Service attacks.

Do attack occurs and dangerous for our networks, and they are producing so many problems for genuine users; that’s why researchers presented the detection and isolation strategies developing a deduction system for a dos attack which deals with unstructured data by using machine learning. There is a lot of unstructured data available, and it must be dealing with some strategy, and they develop a deduction system for unstructured data by Machine Learning.

Fig. 2. DoS Attack with Hping3.

Fig. 3. TCP SYN Flood Attack.
III. EXPERIMENTAL DETAILS

In this paper, it is presented that there are now different types of DOS attacks [14] are coming out, and it’s difficult to control with old techniques like a firewall [15]. Therefore, researchers presented that these threatening Dos attacks are very dangerous for our systems [16], and in this scenario, different methods are discussed. The behavior of the system is monitored by task manager and Wireshark after the execution of these attacks. The system is HP-folio 9470m details are given in Fig. 4.

Before we perform the DOS attack, you can see the screenshot in Fig. 5 that before the attack, there is the clean traffic, which is a monitor in the software Wireshark.

When the DOS attack is started to the victim system, the results are shown in Fig. 7. It is visible how the spike of the CPU usage is increased after the attack of the changes on the CPU usage. So many packets are generated by attackers.

After the attack, you can see the CPU usage in Fig. 7; you can see the traffic after the dos attack. The source and destination of the system are the same because we used the same system for attacking and victimization. In this figure, there is the screenshot after the DOS attack on this system. In this figure, there is a screenshot of the Wire shark for monitoring the traffic. You can see that there is the insane amount of traffic is coming and seen in the Wireshark. 626338 packets are coming in no time. This traffic is coming from the attacker to the victim PC. After some time as the attack continues, you can see in the figure there is full usage of the system resources. It reaches the full end limit of CPU usage in this time system starts hanging its cursor becomes so slow to move; there is a strong reaction of the DOS attack to the system.

After some time when the system is using all the limit, there is a message shown in the window you can see in Fig. 9. After pressing Ctrl C in the terminal (stopping the DOS attack) shown in figure 9 that there is a sudden decrease in the spike, and CPU usage is dropped gradually.

After all the experiments we perform another experiment by using random source we achieve the goal of not showing the actual source of the attacker in this screenshot you can see the results sowed in Wireshark that how the source is randomly changing.
Fig. 8. Wireshark is Capturing the Data.

Fig. 9. Task Manager and Wireshark Traffic.

Fig. 10. Display of Limit Message.
In conclusion, there are many experiments performed to show the results and outcomes after the Denial of Service attacks. How dangerous this attack is it uses all the resources of the CPU, and the CPU services chart is also increased. That's why we must monitor the traffic coming from outside and install some attack protection software are buy some paid monitoring services. Systems are so vulnerable for attackers they can easily find a victim and attack it, and the user loses its important data in the system.

V. FUTURE WORK

There are a lot of tools available for Distributed Denial of Service and Denial of Service attacks in this world many countries hold different types of attack weapons in a huge
amount of quantity these developing countries are way forward in these strategies and research work they are dominating all over the cyber world. In this method, I conclude that this cyber-world is full of attackers which are using latest tools to destroy other servers or networks they are threatening the legitimate users and business owners are effecting too this real world is full of marketing and business point of view that's why there is a serious problem of attacks that's why researchers came and presented the different algorithms and perform experiments that how to mitigate and detect these attackers. Experiments are conducted in different fields of computer science. There is a well-defined, and well explain analysis written in the forms of tables and graphs and screenshots.

There is a very insane amount of increase in the attacks from all over the globe, as seen in Fig. 11, that's why we must take a serious concern to this issue. By detection or mitigation, we can. In the future, there is the chance to detect the attacks from the root level, and some law forces agencies can catch the culprits more efficiently than in the past. The detection and mitigation approaches are available to the common person.

REFERENCES

[1] Yan, Ye, Yi Qian, Hamid Sharif, and David Tipper. "A survey on cyber security for smart grid communications." IEEE Communications Surveys & Tutorials 14, no. 4 (2012): 998-1010.
[2] Andrzejc, Eva, and Barry Horowitz. "A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property." Risk analysis 26, no. 4 (2006): 907-923.
[3] Johnson, Vincent R. "Cybersecurity, Identity Theft, and the Limits of Tort Liability." Scl. Rev. 57 (2005): 255.
[4] Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Lei Zhou. "Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model." Journal of Information Security 6, no. 01 (2014): 24.
[5] Elmaghraby, Adel S., and Michael M. Losavio. "Cyber security challenges in Smart Cities: Safety, security and privacy." Journal of advanced research 5, no. 4 (2014): 491-497.
[6] Kent, Alexander D. "Cyber security data sources for dynamic network research." In Dynamic Networks and Cyber-Security, pp. 37-65. 2016.
[7] Abomhara, Mohamed. "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks." Journal of Cyber Security and Mobility 4, no. 1 (2015): 65-88.
[8] Johnson, Vincent R. "Cybersecurity, Identity Theft, and the Limits of Tort Liability." Scl. Rev. 57 (2005): 255.
[9] Hu, Songlin, Dong Yue, Qing-Long Han, Xiangpeng Xie, Xiaoli Chen, and Chuxia Dou. "Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks." IEEE transactions on cybernetics (2019).
[10] Shen, Yubin, Minrui Fei, and Dajun Du. "Cyber security study for power systems under denial of service attacks." Transactions of the Institute of Measurement and Control 41, no. 6 (2019): 1600-1614.
[11] Khalaf, Bashar Ahmed, Salama A. Mostafa, Aida Mastapha, Mazin Ahmed Mohammed, and Wafaa Mustafa Abduallah. "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods." IEEE Access 7 (2019): 51691-51713.
[12] Muralidharan, N., Arun Parmar, and Manish Kumar. "A flow based anomaly detection system using chi-square technique." In 2010 IEEE 2nd international Advance computing conference (IACC), pp. 285-289. IEEE, 2010.
[13] Gavaskar, S., R. Surendiran, and Dr E. Ramaraj. "Three counter defense mechanism for TCP SYN flooding attacks." International Journal of Computer Applications 6, no. 6 (2010): 997S-8887.
[14] Acharya, Saket, and Nitish Pradhan. "DDoS Simulation and Hybrid DDoS Defense Mechanism." International Journal of Computer Applications 163, no. 9 (2017).
[15] Belovin, Steven M. "Distributed firewalls." (1999): 37-47.
[16] Luna, Raúl, Emily Rhine, Matthew Myhra, Ross Sullivan, and Clemens Scott Kruse. "Cyber threats to health information systems: A systematic review." Technology and Health Care 24, no. 1 (2016): 1-9.

Muhammad Mattah Islam Sameem received his bachelor’s degree from Saraharad University of Science & IT Peshawar, Pakistan in Computer Science. Currently he is doing his masters from FAST School of Computing of National University of Computer and Emerging Sciences (NUCES), Islamabad Pakistan. His research interest is in Cyber Security and IoT.

Safiuallah Shahid received his bachelor’s degree from Government College University Faisalabad t, Pakistan in Computer Science. Currently he is doing his masters from FAST School of Computing of National University of Computer and Emerging Sciences (NUCES) Pakistan. His research area is Cyber Security.

Khush Bakhat Awar holds MS. Degree in Computer Science from University Institute of Information Technology of Arid Agriculture University Rawalpindi Pakistan. She works as a Research Officer in of National University of Computer and Emerging Sciences (NUCES) Pakistan. Currently she is doing Ph.D. Degree from Department of Computer Science, Air University Islamabad. Her research areas are:

Rashid Khan received the MS. Degree in Computer Engineering from Near East University Cyprus in 2014. He is currently doing his Ph.D. Degree from Dept. of Electronic Engineering and Information Science, University of Science and Technology of China (USTC), Hefei China. His research activities are focused on Image Processing, Computer Vision, Natural language Processing and Deep Learning.

Muhammad Sohail obtained his bachelor’s degree from the University of Engineering and Technology (UET) Peshawar, KP, Pakistan in BE Electronics and then his master's degree from Automation department the University of Science and Technology of China (USTC), Hefei China. Now he is working towards his Ph.D. degree in USTC. His research interests are Network Security and Machine Learning.