e-ISSN 2320 –7876 www.ijfans.org
Vol.11, Iss.12, 2022
 UGC CARE Listed (Group -I) Journal

A Survey on Denial of ServiceAttacks on Application Layer

DR. KULDEEP PANWAR[1], VAISHALI KOUL[2], DR. ABHILASH SINGH[3]

1Department of Mechanical Engineering, Shivalik College of Engineering, Dehradun
2College of Pharmacy, Shivalik, Dehradun
Shivalik Institute of Professional Studies, Dehradun

Drkuldeep.panwar@sce.org.in

ABSTRACT:*The goal of security is to safeguard assets. Defense, detection, and deterrent are all elements of security that may be used to any scenario. Hardware, Information, as well as software on a computer network are all protected by network security. Attacks that create a denial of service (DoS) have a significant effect on the online world. The goal of these assaults is to prevent genuine users from accessing services. Attackers may quickly drain a victim's resources by exploiting computer weaknesses. To counter DOS assaults, a number of unique methods have been created. To address security issues, some companies create a variety of defensive mechanisms. The different kinds of attacks and solutions connected with each layer of the OSI model have been presented in this article. The effects of these assaults and remedies vary depending on the context. As a result, the fast development of new technology may result in even worse assaults in the future.*

KEYWORDS:*Application Layer,Attacks,Network, Security, Website.*

1. INTRODUCTION

The basic goals of network security are the availability, security, and confidentiality of computer system resources. The security protocol is a crucial part of network security. Security protocols are established for entity authentication, key agreement, and secure connections prior to any data transfers between any network entities. Numerous security mechanisms might be vulnerable to a DOS assault since various verification stages could demand resource-intensive executions, giving attackers access to legitimate users' resources. In order to stop malicious traffic from flooding the network, the Internet Key Exchange (IKE) protocol employs public key techniques to authenticate the protocol initiator. Protocol designers must be aware of this issue and provide secure protocols in order to counter DOS assaults. As a result, security procedures may be used to provide sensitive information and necessary services. The network connection and data transmission are thus secure. Organizational components of security programmes include authority, planning, evaluative analysis, and maintenance. When attackers send attack messages from several sites across the network, it is referred to as a distributed denial of service (DDOS) assault[1]–[3].

A Single-Source Denial of Service (SDOS) attack occurs when all of the attacker's assault messages originate from a single site. A DOS attack is a malicious attempt made by one attacker or a group of attackers to harm an internet service. Attacks that create a denial of service may endanger your life both while and after they occur. A terrorist group conducted a DDOS attack against 19,000 French websites on January 7, 2015. Both low-level government and commercial websites were the targets of this. In Paris, the ISIS flag was vandalised and hacked on several websites. A few warning indications of an attack include abnormally sluggish network performance, the unsuitability of a certain website, difficulty accessing any website, etc. DOS attackers often do it for monetary or commercial gain, unavoidable sluggish network performance, retribution, ideological conviction, intellectual challenge,

serviceinterruption, and cyberwarfare [4]–[6].The different DOS assaults involved in each tier of the OSI model are discussed in this article, and remedies are given for those attacks.

We have given the most effective remedy for these assaults, and additional solutions may be developed in the future. Because the effects of assaults may change depending on the platform or environment, solutions will also have domain-specific limitations. We also address the importance of distributed denial-of-service assaults, which have affected a number of sectors. A comprehensive analysis of DDoS attacks that have afflicted numerous nations across the globe. As technology advances at a rapid pace, a slew of new threats emerge. We may not be able to determine the optimum answer for attacks, but we can take preventative steps to address any difficulties or problems that may arise[7].

1.1 Process of DDOS Filtering:

The process of Distributed Denial of Service is shown in Figure 1.

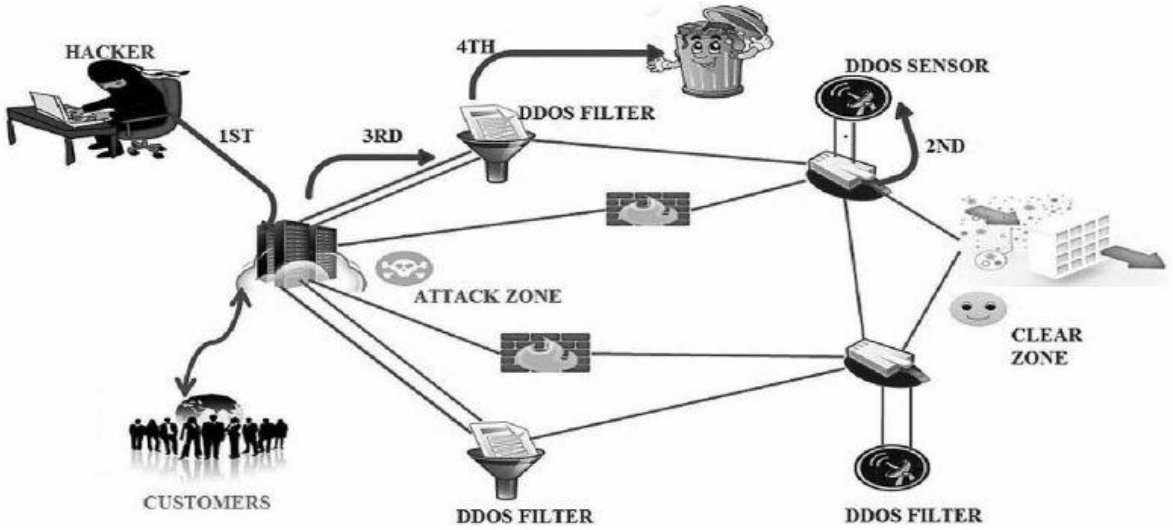

Figure 1: The above figure shows the Distributes Denial of Service.

- The hacker makes an initial effort to learn more about the targeted system.
- The hacker then uses any elementary tactics to take advantage of the system's flaw.
- These assaults are recognised and filtered using DDOS sensors (or comparable technologies).
- The discovered assaults are eliminated by the DDOS filter (or comparable technologies).
- Finally, scattered users of the network may do so without experiencing any issues.

1.2 DOS Attacks Taxonomy:

A network system design that permits communication across different systems is the OSI model. It has seven layers, each of which offers a distinct perspective on the diverse network security requirements. DOS assaults come in a variety of forms. It may be on the client, server, or network at any moment. Various methods are used to hack the legitimate user's machine in these assaults. Some assaults have permanent remedies, while others may result in significant financial loss with no desired outcome[8].

1.3 OSI Layers, Attacks and Solutions:
1.3.1 Layer of the Application:
1.3.1.1 Bombs in E-Mail:

The usage of an e-mail bomb causes the software to hang or terminate prematurely. It is a hazardous piece of code that comprises of a huge number of emails aimed at a certain system. This kind of mail bomb is often used to bring down an email server or slow down a user's computer. When a user downloads a large quantity of emails, the email's allotted storage capacity is quickly depleted. This causes the server to crash. The primary goal of email bombers is to sabotage emails and damage the Internet Service Provider (ISP) they are targeting. It disrupts connectivity, overburdens network connections, and depletes system resources[9]–[11].

To avoid this attack, email bombers are blocked by ISPs, and proxy servers are used to verify malware content and filter communications from certain IP addresses and protocols before they are sent to clients or users. Before messages are sent to the target system, they are authenticated using the Simple Mail Transfer Protocol (SMTP).

1.3.1.2 Flood of DNS

A distributed denial of service (DDOS) attack known as a DNS flood is used to bring down one or more Domain Name System (DNS) servers in a certain zone. With each request, DNS servers function as the "road map" for the internet, pointing users to the appropriate server. Due to the fact that DNS servers use the UDP protocol for name resolution, this approach serves as an alternative to the UDP flood assault. The offender runs a script that was assembled from many servers. These programs send faked IP addresses faulty packets. Randomized packet data aids offenders in evading typical DDOS defense such as IP filtering. If you know the offender's IP address, the first step is to use firewall protection rules to restrict traffic from such addresses.

The second option is to employ Denial of ServiceDDOS Protection to minimize DNS floods among genuine business clients.

1.3.1.3 HTTP-based attack:

The main objective of the attacker is to assault a web server or application via HTTP GET or POST requests. HTTP flood attacks employ a network of linked computers to launch a large-scale assault. The targeted website or server is taken down using less bandwidth than in earlier attacks. All incoming site traffic is monitored and categorised by Web Application Protection by Encapsulate. This is specifically meant to stop all HTTP floods and other DDOS attacks at the application layer by identifying malicious bot traffic.

1.3.1.4 Attack on Slow Reading

An undetected denial of service is the goal of a slow read attack, which takes use of a TCP persist timer flaw. The server receives a legitimate HTTP request from the attacker, but the response is sent so slowly that the connection must stay open. The client notifies the server that it is reading data by sending a zero window to the server.

As part of its assault prevention, NetScaler has the intelligence to detect such open connections and quietly remove them. When a high number of connections are collected in a small window size circumstance, it is triggered.

1.3.1.5 Attack of the Teardrops:

It sends the fragmented packets to the intended recipient. Due to a TCP/IP fragmentation reassembly problem, the recipient computer is unable to reassemble the fragmented packets. As a result, the packets overlap and cause the targeted network device to fail. The most effective method to counteract this assault is to upgrade network gear and software.

1.3.1.6 Attack on a URL:

A URL manipulation attack that alters URL parameters and sends them back to the service provider compels the web application to do activities like accessing sensitive server files and forwarding to other websites. The web server should be set up as follows to stop this attack: turn off the display of files in directories without an index file, eliminate unnecessary script interpreters, delete unnecessary directories, and remove unnecessary files.

1.3.1.7 Attack on the Buffer Overflow:

When the buffer size is exceeded, data overflows from one buffer to the next. Because the buffer can only hold a certain amount of data, once it fills up, the data flows somewhere else. This has the potential to corrupt the data in that buffer.

1.3.1.8 Probing WSDL:

During this assault, hackers probe the Web Service Definition Language (WSDL) interface for sensitive data such as invocation patterns, technology implementations, services ports, customer-accessible bindings, and vulnerabilities. This kind of probing may be used to carry out serious attacks, such as parameter manipulation, malicious content injection, command injection, and other tactics. Because of this, a hacker may send the Web service certain special characters or malicious code, leading to a denial of service or unauthorised database access. The WSDL file must be protected, or access must be limited to it. Check for injection vulnerabilities in the WSDL interface's functionality. Since function names are easily guessed and might serve as an attack entry point, check the naming convention.

1.3.1.9 Attack of the RUDY:

Long form fields are used by the low-level, slowly advancing RUDY attack to bring down a web server. It scans the given page for and locates web forms. At regular intervals after the detection of the forms, it sends an HTTP POST request with a long content length header field containing one byte sized packet data. To evade detection, this information is sent slowly and in bits, which causes a backlog of application threads and prevents the server from cutting off the connection.

This attack is challenging to find because of the unforeseenly massive network oscillations. One way to identify anything is to keep an eye on the server resources. For instance, it can identify server memory, connection tables, threaded programmes, and long-running open network connections. Misuse may be identified and followed up on using behaviour analysis of open server connections. The incoming requests from clients to the server are watched using the security services offered by Encapsulate.

1.3.1.10 An XML Injection Attack:

The attacker in this instance tries to add XML instructions and change the XML structure. As a consequence, it may lead to breaches of security objectives like Integrity and Access Control because of the modification of payment information and unauthorised admin access. By restricting and sanitising any user input before it is processed, this XML injection threat may be prevented. By carefully observing every input, this assault might be stopped. To achieve this, remove all single and double quotations from the user's input. Therefore, the necessary syntax and techniques of the Extensible Markup Language (XML) library must be utilised.

1.3.1.11 Malicious attack:

A programme or file known as malware—often referred to as malicious software—is intended to harm a user's computer. Malware includes things like Trojan Horses, worms, viruses, and spyware. Without the user's knowledge or permission, these programmes are

used to gather data about their machine. Anti-virus software was used to remove this harmful attack. This limits access to the user's system resources and is used to find the malware file on the user's system.

1.3.1.12 Attack on Resource Depletion:

It is sometimes referred to as a "disc space attack" and is used to access certain system resources repeatedly until they are completely used. For instance, the attacker may bombard a website with requests to create users or baskets. Radmin is used to recognise and prevent this attack.

2. DISCUSSION

The author has discussed about the survey on denial of service attacks on application layer,as well as answers to such attacks. Increased internet expansion organizes new technological development on a daily basis, and new DOS assaults may emerge as a result. We may have to deal with the repercussions of such assaults in the future.Network security safeguards material, hardware, and application on a computer network. Attacks that cause a failure of service (DoS) have a big impact on the internet. These attacks are intended to avoid at all costs services.As a result, we must concentrate on developing the right system and policies in response to the security threat. As a result, we will be able to prevent any future assaults or threats.

3. CONCLUSION

The author has discussed about the survey on denial of service attacks on application layer,Defense, detection, and deterrence are all security aspects that may be used to any situation. By exploiting computer flaws, attackers may rapidly deplete a victim's resources. When the attacker's assault messages come from a single site, it is a Single-Source Denial of Service (SDOS) operation. A DOS attack is a deliberate effort by one or more criminals to stop an internet service from operating. Denial-of-service attacks may be devastating in their beginnings and outcomes. A gang of terrorists launched a distributed denial-of-service (DDOS) assault against 19,000 French websites on January 7, 2015. Websites for businesses and small-scale governments were also targeted. The ISIS flag has been added to several websites in Paris that have been hacked. Some indications of the attacks include unusually sluggish network performance, the unsuitability of a certain website, the inefficiency of browsing any website, and so on. To counter DOS assaults, several novel strategies have been created. To address security issues, several firms use a variety of protective techniques. This article examines the many dangers and countermeasures connected to each layer of the OSI model.

REFERENCE

[1] D. Kaur and P. Singh, “Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack,” *ACEEE Int. J. Netw. Secur.*, 2014.

[2] N. Briscoe, “Understanding The OSI 7-Layer Model,” *PC Netw. Advis.*, 2000.

[3] Microsoft, “The OSI Model’s Seven Layers Defined and Functions Explained,” *2017*, 2017. .

[4] B. Mitchell, “The OSI Model Layers from Physical to Application,” *Lifewire*, 2018. .

[5] V. Beal, “The 7 Layers of the OSI Model,” *webopedia*, 2015. .

[6] Y. Pan *et al.*, “Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems,” *Int. J. Interact. Multimed. Artif. Intell.*, 2017, doi: 10.9781/ijimai.2017.437.

[7] P. Sinha, V. K. Jha, A. K. Rai, and B. Bhushan, “Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey,” in *Proceedings of IEEE International Conference on Signal Processing and Communication, ICSPC 2017*, 2018, doi: 10.1109/CSPC.2017.8305855.

[8] M. G. Moreira Santos and P. A. Alcívar Marcillo, "Security in the data link layer of the OSI model on LANs wired Cisco," *J. Sci. Res. Rev. Cienc. e Investig.*, 2018, doi: 10.26910/issn.2528-8083vol3isscitt2017.2018pp106-112.

[9] G. Sondakh, M. E. I. Najoan, and A. S. Lumenta, "Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat," *J. Tek. Elektro dan Komput.*, 2018.

[10] H. Jamali-Rad *et al.*, "IoT-based wireless seismic quality control," *Lead. Edge*, 2018, doi: 10.1190/tle37030214.1.

[11] T. Banerjee and A. Sheth, "IoT Quality Control for Data and Application Needs," *IEEE Intell. Syst.*, 2017, doi: 10.1109/MIS.2017.35.

[12] Panwar, K, Murthy, D, S, "Analysis of thermal characteristics of the ball packed thermal regenerator", Procedia Engineering, 127, 1118-1125.

[13] Panwar, K, Murthy, D, S, "Design and evaluation of pebble bed regenerator with small particles" Materials Today, Proceeding, 3(10), 3784-3791.

[14] Bisht, N, Gope, P, C, Panwar, K, " Influence of crack offset distance on the interaction of multiple cracks on the same side in a rectangular plate", Frattura ed IntegritàStrutturale" 9 (32), 1-12.

[15] Panwar, K, Kesarwani, A, "Unsteady CFD Analysis of Regenerator", International Journal of Scientific & Engineering Research, 7(12), 277-280.

[16] Singh, I., Bajpai, P. K., & Panwar, K. "Advances in Materials Engineering and Manufacturing Processes