A NOVEL SURVEY ON DoS ATTACKS

Pallavi D. Bhalekar[1], Dr. M. Z. Shaikh[2]

[1]Bharati Vidyapeeth College of Engineering, University of Mumbai,
[2]Bharati Vidyapeeth College of Engineering, University of Mumbai

---***---

Abstract - *Now a day's computer technology is rapidly increasing so we have to provide security at each step of our technology. TCP/IP model allows different layer to work without any knowledge of other layer. That's why it's very important to find out the attacks at each layer for providing strong security to our computer. DoS is one of the major concern attacks in both internal as well as external way. In this paper, we have studied that TCP/IP attack as per each layer. We will discuss in short as per the layered structure. At the physical layer attacks are done on the devices as well as media like router. In a data link layer studied, DHCP starvation as well as MAC spoofing attacks, the next layer is network layer; In this layer we deeply studied about ICMP flooding attack and other attacks as per routing information. In transport layer studied the session hijacking concept. Application layer shows the HTTP flooding attacks in detail. Explained the term the DoS attacks and its types like smurf attack, ping of death, teardrop attack, SYN attack etc.*

***Key Words*:** DoS attack, types of DoS attack, Layered attacks.

1.INTRODUCTION

DoS is an abbreviation for Denial of Service. Denials of Service (DoS) attacks are performed on single machine. DoS attack is used to delay legitimate users access resources such as accessing website, network, e-mail like that and making it extremely slow. This type of attack is mostly occurred by disturbing or crashing the target machine like that web server. In web server sends to many requests to the victim machine. These results into this type of server failing to respond the requests send from the other servers. This effect can either be hitting the server or slowing them down.

Dos a type of outbreak that targets restricting service, refuting service access or downgrading service performance. A DoS attack can be pretreated in the number of ways. Like that Consumption and computational resources such as bandwidth, disk space or processor time. Second way is Distribution of configuration information, such as routing information. Third will be Distribution of state information, such as unsolicited resetting of TCP session. Fourth way may be the obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

The first DoS attack was occurred in 1999 at university of Minnesota. After that in 2000 the attacks were occurred on famous companies like that Amazon, eBay, Yahoo. The attack on Yahoo was the "ICMP Flooding Attack". We know that ICMP (Internet Control Routing Protocol) is the simplest kind of conversation in computer.

In ICMP flood, an attacking ping command is sent to target machine with hacked return address but hacked address is hidden, which sends the attacked system on an unlimited request are sent for a place to return the ping.

In 2016, militant organization AI-Qaeda hacked the Indian railway's website to display its cyber prowess. In 2016, for just an hour Indian regulator Trail's official website was hacked. After sometimes hacker released that website approximately 1 million mail Ids of users who wrote to them in support of Net Neutrality. Hacking group Anonymous has taken responsibility for the distributed denial of service (DDoS) attack and bringing site down. In April 2015, the army's Principal controller of Defense Accounts Officers (PCDAO) website was hacked by the hackers. It had information of army officer like that personal as well as financial information. Many officers were not able to access even their own salary information. In December 2010, from long time Pakistani hackers had been targeting Indian cyberspace for the purpose of hacking. They attacked on the CBI's website. ISRO's marketing arm Antrix saw its website hacked in July 2015. Users from CBI agency were redirected to online shopping portal at the time of trying to access the website.

2. Some common types of DoS attacks

2.1 Ping of death: We mostly use the command "ping" to mostly check if server or gateway is running or not. But, many times ping command can also be used for many other purposes. If we look at the basic level, then ping packet is generally of size 56 bytes or 84 bytes including IP header. However, a ping packet can also made as large as up to 65536 bytes. That's the negative side of ping packet. When we will increase packet size. Unnaturally, forming a malformed ping packet to attack a computer system, this type of attack called "ping of death" attack. Not all computers can handle data large than fixed size. So, when ping of death packet is sent from source computer to target computer, the ping packet is get divided into smaller chunk packets. One fragment is of 8 octet size. When these packets reach to target machine, the get as fragments. So, the target machine tries to reassemble the malformed packets which are received in chunks. But, whole assembled packet causes buffer overflow at the target computer. Buffer overflow causes system crash making system more vulnerable to attack.

2.2 Smurf: Smurf attack is the DDoS attack in which large amount of ICMP packets are sent with target spoofed source IP and broadcast to the computer network using an IP broadcast address. Most of the devices on network will send responds to the source IP address. If number of machines on the network receive and respond to those packets is very large, so the target machine will be flooded with traffic. This can slow down the system at that time it's difficult to work on.

2.3 Buffer overflow: Buffer is a temporary memory location which is used to store data so that CPU can manipulate it before writing it back to disc. We know that Buffer has a size limit. The attacker loads data into buffer more than its capacity. Therefore this causes the buffer to overflow by adding large amount of packets hold and corrupt those data it holds.

2.4 Teardrop: In this attacks the attacker send large amount of data packet to target machine. By using TCP/IP port the packets are fragmented into small chunk of packet. This is already assembling onto TCP/IP port. Attackers try to manipulate those small packets and sent to target machine so that they are overlap each other. This can cause the target machine to crash as it tries to reassemble the packets.

2.5 SYN attack: SYN attack is stands for synchronize attack. In this type of attack to establish connection uses three way handshaking using TCP protocol. SYN attack is works as by sending continuous or repeatedly sending incomplete handshake messages. So that target machine can hold the resources. Therefore this causes the victim machine to allocate memory resources and those resources will be never in used. By holding that resources other machines cannot access resources therefore deny access to legitimate users.

3. Layered attack

3.1 Physical Layer Attack: The physical layer is the bottom layer of the OSI model. It is concerned with transmission of raw data in a bit format from sender to receiver. At the physical layer we can connect different types of devices and mediums like that cable, connectors, receivers, transreceiver, and repeaters. The attack on this layer is happened as physical layer destruction, obstruction, manipulation, or malfunction of physical assets.

3.2 Data link Layer Attack: The data link layer is placed between physical layer and network layer. The function of data link layer is transfer the data from physical layer to network layer. And used to detect and correct the errors occurred at physical layer in network entities. The attack at datalink layer is 1. MAC spoofing (ARP poisoning) 2. DHCP starvation attack

3.2.1. MAC spoofing (ARP poisoning): ARP stands for address resolution protocol, a protocol used for resolve IP address to MAC address for transmitting the data. In ARP spoofing attack, an attacker sends the spoofed ARP message over LAN to link their MAC address with IP address are getting sent to the attacker instead of user.

ARP spoofing attack is used for facilitate other type of attack, including denial of service (DoS), man- in – middle attack and session hijacking. This attack is only work on local area network.

3.2.2 DHCP starvation attack: DHCP starvation attack is an attack that targets DHCP servers. In DHCP server contains with number of IP address which is present in network. The intension of this attack is exhausts the entire network IP addresses which are allocated to the DHCP server. Under this attack, legitimate network users can be denied service.

3.3 Network Layer Attack: Network layer, takes care of routing data, directing the process of selecting paths along which to send the data in a network. Network layer attacks can cause into two categories. First one is routing attack and second one is a packet forwarding attacking.

Routing attacks contains with following some types of the attack

3.3.1 IP spoofing
3.3.2 RIP attack
3.3.3 ICMP flooding attack

3.3.1 IP spoofing: The aim of this attack is IP spoofing refers to connection hijacking through fake internet protocol address. This attack is overwhelming volume of traffic, and attacker doesn't care about receiving response to the attack packet.

Packet forwarding attacks contains with following some types of the attack

3.3.1.1 Packet Sniffing
3.3.1.2 Teardrop Attack
3.3.3.3 Ping of Death Attack

3.3.2 RIP attack (Routing Information Protocol): Router's main software is a packet processing unit (PPU). PPU is responsible for all the activities related with packet like that packet processing, packet capturing, packet cleaning as well as important part in invoking intrusion detection module.

In packet cleaning process removes those packets which are not required for intrusion detection. IDS perform rule matching with header part of every packet. If attack will be detected then takes the appropriate action on that particular packet. And again by resetting that state RIP start processing with new packet.

3.3.3 ICMP flooding attack: ICMP flood attack sends the large number echo request packets to targeted server using multiple different devices. The server sends the response to every device by sending echo respond packet. From any of the devices request will get accepted. And ICMP attack is happened.

3.4 Transport layer attack detection: The main work of this layer is transfer the data from one device to another device squarely. The most important attack of this layer is session hijacking. It takes the control over session between two nodes. Therefore the most authentic processes are carried out only at the start of the session, once the session between two nodes gets established the another nodes gives the feedback that which node data is reached. If within the given session time data will not reached or stuck in root. Then by checking anomaly or behavior the attack will be detected.

3.5 Application Layer Attack: Application layer attack requires an adaptive strategy including the ability to limit traffic based on particular sets of the rules, which may fluctuate regularly. Tools used in the system configured can mitigate the amount of bogus traffic that is passed on to an origin server, greatly diminishing the impact of dos attack. HTTP downpours include the use of a web solicitation firewall, managing and filtering traffic through an IP reputation database.

4. Literature survey:

4.1 An Efficient DDoS TCP flood Attack Detection and Prevention System

In this paper present new classifier system for detecting Denial of Service attack (DoS) TCP flooding attacks. In this system it stores the packet as per classifying solution. At the time of detection it will check that given packet is normal or contain with attack by using behavioral model as per classifying records. At the time of prevention, those packets which are classified as malicious to those packets will denying the cloud service after that particular IP address will be blocked. In this paper they compare many algorithms like LS-SVM, naive Bayes, k-nearest algorithm. But provide good accuracy shown by LS-SVM algorithm.

4.2 Layer wise Attack on Service oriented architecture in Internet of Things and their defense mechanisms.

IoT allows to sense and controlled remotely to any object across defined network infrastructure. The more importance challenges in the IoT are providing security, privacy, Interoperability issues. The main objective of this paper is security attacks on SOA layer. In Service Oriented Architecture the first layer is physical layer known as sensing layer as well the work of this layer is provide the security at media like theft, loss, destroy As well second work of this layer is to protect confidential information and integrity of data. At the network layer DHCP attack detection is done using SVM algorithm.

4.3 Application layer DdoS attack a sketch based defense system

In this paper implemented an effective defense system. First of all he calculated the divergence between two sketches which shows the accuracy. Then he implemented abnormal sketch to shows the malicious attacks. The main purpose of abnormal sketch is to avoid reverse calculations of malicious hosts. By using signature based intrusion detection system differentiate between malicious attacks and normal users.

4.4 Intrusion detection for ICMP - Flood attacks

In this paper discussed the ICMP flooding attacks connection and methods. Using the anomaly and signature based Intrusion detection system ICMP DDoS attacks are implemented. The attacks are generated on windows machine using hping3. The statistical implementation is done using WEKA tool. Compare with SYN attacks TCP attacks UDP attacks and implemented a pie chart of every attack.

4.5 Analysis of Network layer attacks and their solutions in MANET

In this paper, use the attack detection for the mobile ad-hoc network (MANET). So the network of every mobile is dynamic so nodes are moved as per network of the area the aim of this paper is to shows security criteria and attacks types in MANET. The proposed system Flooding techniques are discussed like that connection is established by sending route request and route replay messages. If it will send replay message from the destination node then route will get find otherwise try with different route request message.

4.6 Analysis of various TCP variant in MANET

In this paper, perform the comparison between numbers of TCP variant like that TCP Reno, TCP new Reno, TCP Tahoe, TCP Lite using routing protocols like that DSR, AODV etc. By applying these routing algorithms analyze the result packet loss, jitter, and throughputs. Analyze the byte received from attacker. Check the routing table information which contains with TCP/IP protocol attacks. Analyze those signals which contains with errors. MANET is dynamic in nature that why more difficult to manage routing information at every stage. At the stage of congestion, retransmission is done in the TCP variant.

4.7 Detection algorithm for DoS attack using cloud storage

In this paper, implemented that attack detection at cloud are by using CAT (change aggregation tree) technique. CAT technique is represents the attacks flow pattern, traffic and congestion flow pattern. Knowledge based attack detection method is implemented. That by checking prior knowledge and behavior of the attacks. They have implemented the Shannon's entropy. If that attacks may behave same then declared as the attacks. Like packet header information is different, TTL the packet, arrival time of the packet, creating congestion at every node. By checking this knowledge on dashboard it declared as an attack. And restart with new packet information to detect the malicious attack.

4.8 Decision Tree algorithm based intrusion detection

In this paper, implemented decision tree algorithm is developed on C4.5 decision tree approach. This algorithm is used for feature selection and the splitting the values as important issue. In this approach used the NSL-KDD dataset. From this dataset used the 31 complete features to check malicious attacks as signature based method used. Differentiate between dos attacks and probe attacks. As per feature it is differentiate. By using signature based method provide 82% of accuracy in DoS attacks and 65% in probe attacks. The efficiency of this algorithm is depends upon number of records in datasets. Calculate ratio between feature reductions and attribute selection.

4.9 Network intrusion detection: Machine learning approach

In this paper, he proposes total ten machine learning approach for showing efficient intrusion detection. To detect attacks used the NSL-KDD dataset as well as KDDcup 1999 datasets. By applying the ten algorithms like that SVM, Naive bayes, Random forest, AdaBoost etc calculate the detection rate, false positive rate, average cost. Majority of the attacks is detected like that by checking false positive rate. At every stage calculated the accuracy. Simplicity creates the table as by applying ten algoritms. With best accuracy that algorithm is used for future implementation.

4.10 security attack detection using ML algorithms

In this paper, mainly focused on various security attacks like man- in – middle attacks, DoS attacks, malware injection attack, slide channel attacks. By using machine learning algorithms implemented the logistic regression algorithm, naive byes, SVM algorithm attacks are detected. By using NSL-KDD datasets the attacks are detected. Applied various algorithms. C4.5 and decision tree algorithm is applied it gave the result as c4.5 is not sufficient to detect the attacks it must be coupled with signature based method. After that applied firecol algorithm by proposing the result the existing accuracy is better than implemented accuracy. By applying ANN algorithm got better accuracy and it's very easy to implement and very powerful algorithm for attack detection.

Paper Title	Specifications	Advantages	Limitations
An Efficient DDoS TCP flood Attack Detection and Prevention System	Use behavioral model. ALS-SVM, k-nearest naive byes algorithms are used	1. Gives 97% of accuracy 2. Improve security of record, reduce bandwidth	Need to identify the attackers when they find the threshold value
Layer wise Attack on Service oriented architecture in Internet of Things and their defense mechanisms.	Use Support Vector Machine algorithm for DHCP attack detection	1. IoT is rapidly growing in industry applied attack detection at each layer of SOA model.	1. Internet of Things use loosely coupled software entities that entities that implement single software function. 2. These software services are dynamically combined to form ad-hoc application
Application layer DdoS attack a sketch based defense system	TCM-KNN algorithm is used state-of-art methods is used for sky shied comparison.	Benefits: Scalable and accurate DDoS attack detection Avoids the reverse calculations process which	Limitations: Because of dynamic network it's very difficult to maintain. In dynamic network that relay traffic between

		makes an efficient in real time anomaly detection. Transparency at every node	protected server and authenticated clients.
Intrusion detection for ICMP - Flood attacks	Anomaly and signature based intrusion detection. Hping3, WEKA tool is used	1. Provide good accuracy as well as reduce bandwidth. 2. Improve security of record as increase the signatures and anomaly in the record 3. Use real time data instead implementing on databases	1. Difficult to maintain real time data. 2. Work on only windows machine so have to implement machine friendly
Analysis of Network layer attacks and their solutions in MANET	Threshold values technique is used	1. Add some protocol at the source node to detect malicious attacks in routing table. 2. Every time routing table is updated as per new routing or malicious information	1. Difficult to maintain routing table information 2. MANET is dynamic therefore difficult to disconcert the route. 3. maintain security of network is difficult
Analysis of various TCP variant in MANET	Entropy and threshold value techniques is used	1. Throughput 2. Improves mechanism of packet loss at each node 3. Reactive routing protocol performance is good	1. Fault detection is difficult to wired networks 2. congestion control does not show consistent in TCP variant
Detection algorithm for DoS attack using cloud storage	Change Aggregation Tree (CAT) techniques is used and implemented Shannon's entropy.	1. Generate alarm at the stage of attack detected and cancel the flow of packet. 2. Easy to implement.	1. Less efficient because if new pattern will arrive and it's not in dashboard that type of attacks will ignored. 2. Real time attacks are not detected.
Decision Tree algorithm based intrusion detection	C4.5 and decision tree methods are used. NSL-KDD dataset is used.	1. Good efficiency. 2. Provide good accuracy at the time of feature selection	1. need to improves split values in decision tree algorithm
Network intrusion detection: Machine learning approach	KDDCup 1999 dataset is used. Total ten algorithm is applied to check accuracy like SVM, Decision tree, KNN, AdaBoost etc.	1. Know the accuracy of every algorithm; so it's very efficient to choose algorithm with better performance	1. Ignore minor attacks 2. Does not acceptable false positive rate and low cost.
security attack detection using ML algorithms	C4.5 , decision tree and SVM algorithms are used	1. Machine learning algorithm provides an efficient algorithm. 2. Algorithms provide good accuracy.	1. Time consuming process to check the accuracy by applying every algorithm. 2. With used datasets need the signature based method to detect errors.

3. CONCLUSIONS

Thus we have studied the DoS attacks as well as its type. Understand at which layer the attacks may or may not arrived. TCP/IP layer model is used to detect the attacks at every layer which types of attacks are those. Studied recent implemented papers and techniques used in every paper. Which algorithm shows good accuracy, threshold value, false positive values rate. Datasets used in each implementation. KDD, CTU, ISCX, CIC datasets are studied. In future we will implement the ICMP, HTTP attack detection by using ISCX and CIC datasets.

REFERENCES

[1] Aqeel Sahi, David Lai, Yan Li and Mohammad diykh "An efficent DdoS TCP flood attack detection and prevention system in cloud Environment" , feb 2017.

[2] A vinothini, G. Padmavathi "A Study of Layer Wise Attacks on Service Orient Architecture in Internet of things and their defensive mechanisms", May 2017.

[3] Chenux Wang, Tony T.N Miu, Xiapu Luo, Jinhe Wang "skyshield: a sketch based defence system angainst application layer DdoS attacks", March 2018.

[4] Anup ingle, Mohnish Awade, "Intrusion detection for ICMP- flood attacks", Feb 2013.

[5] Abida Aslam, Mehak Abbas, Muhammad Yasir Adnan, M.Junaid Arshad "Analysis of Network layer attacks and their solutions in MANET", January 2017.

[6] R.T.Anitha, Dr B. Ananthi "An Efficent Detection and Prevention of DdoS attacks in Cloud environment", January 2018.

[7] Kajal Rai, M. Syamala Devi, Ajay Guleria "Decision Tree algorithm based intrusion detection", Dec 2015.

[8] Mrutyunjaya Panda, Ajith Abraham, Swagatam Das, Manas Ranjan Patra "Network intrusion detection: Machine learning approach", November2011.

[9] Dhivya R, Dharshana R, Divya V "security attack detection using ML algoritms", Feb 2019.

[10] Deeksha Kotian, Shibani Shetty, Shifana Begum, Akhilraj V Gadagkar, "Analysis of various TCP variant over MANET routing protocol", Feb 2019.