International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 6 June 2021, pp: 723-726 www.ijaem.net ISSN: 2395-5252

Detection of DDoS attacks

K.Dhruv Kashyap, Dr. S. Godfrey Winster
Computer Science Engineering SRM Institute of Science and Technology Chennai, India
Computer Science Engineering SRM Institute of Science and Technology Chennai, India

Submitted: 25-05-2021 Revised: 01-06-2021 Accepted: 05-06-2021

ABSTRACT—Cloud computing is often said to be the on-demand access and availability of multiple computer resources without the need of the user to actively participate. However, all resources have security concerns, and Cloud Computing is no exception. The main issue we will be focusing on is the DDoS attack, and how to detect such attacks when they are happening.

Keywords—cloud computing,DDoS,detection,attack detection

I. INTRODUCTION

Cloud Computing, in very simple terms, canbe defined as the usage of services over theinternet. The services are of three types: infrastructure, platform, and software. The services can either be public, or private. Private services are for a single individual, while public services are for everyone.

Recently, with the advancement of IoT and other Internet services, the threat of a breach of security has increased significantly. One such method of breaching security is the DDoS Attack.

DDoS stands for 'Distributed Denial of Service'. A DDoS attack uses multiple devices, which are usually remotely controlled by the attacker, to send a large amount of traffic to the victim in order to stop their services temporarily. Rather than breach your website, DDoS attacks try to make their targets so that they do not work properly for the normal users.

I.I UNDERSTANDING DDOS ATTACKS

DDoS attacks affect the victim in following ways:

• Any weakness that be exploited can be found by the aggressor to disrupt the service.

• Depletion of network resources.

The attackers decide on the victim, and send malicious software to the victim's system in order to find some weakness in their security. After the weakness are used by the attacker, the attacker remotely takes control of the system, and the systems are then compromised. Since the attacker will hide their original IP addresses by giving false IP addresses, it is quite difficult to track where the attack comes from. Now, the attacker does this to multiple systems, usually numbering in the thousands, ad takes control of all the devices.

Now the attacker has control of more than a thousand devices, which are collectively known as a botnet. The attacker then uses the botnet to launch malicious attacks onto other devices or servers, making them unable to function properly.

The large number of devices results in a very serious case of DDoS attack, where the servers can be down for multiple minutes, causing normal users to not be able to use the site properly, and cause great monetary loss to the service providers. DDoS attacks are extremely malicious in nature and cause great loss to those who are affected.

I.IICLASSIFICATION

The types of DDoS attacks are increasing exponentially every day, and the danger associated with them are also increasing alongside them. The most common type of attack is the one which depletes the bandwidth of the networks.

Bandwidth Depletion Attacks:

This is one of the most common types of DDoS attacks, in which the victim is usually sent too many packets so as to prevent their service from working properly. These can be classified as:

1. Flood Attack: A large number of UDP packets are sent to the target server in order to overwhelm it and prevent it from working properly. This can also result in the exhaustion of the firewall which protects the target server, which prevents regular and legitimate traffic from entering the server.
2. Amplification attacks: This is a type of DDoS attack in which the attacker uses the vulnerabilities in a DNS server in order to, as the name suggests, amplify the small queries, which in turn bring down the server.
3. Resource Depletion Attacks: This is the type of DDoS attack in which the resources of the victim are forcefully depleted or completely used up, preventing normal users from getting the services.
4. Protocol Exploit Attacks: The main goal of such attacks is to take advantage of all the resources which are installed in the victim's system or server, and hence use them for malicious attacks.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 6 June 2021, pp: 723-726 www.ijaem.net ISSN: 2395-5252

5. Attacks using Malformed Packets: Data or information which is wrapped or surrounded by malware is known as a Malformed Packet. These are sent to the victim to make sure their service are rendered unusable.
6. IP Address attack: An attack which causes a lot of chaos, since the malformed packets have the same IP address for the source and destination, which causes a lot of confusion. This causes the victim to rapidly crash and stop working properly, or sometimes stop working altogether.

I.III DETECTION METHODS.

I.III.I Signature-Based Detection

While this method is extremely accurate, it is not the best method to use without any proper experience or knowledge. The rules always take longer to update as compared to the emergence of new types of attacks. Nowadays, if a new bug is found on the internet, the detection method will be released in a few days, but the rules will take even longer to be released. This time between new attacks being released and rules being released will allow the malicious attacks to happen.

This method is mainly used to check whether the attack pattern can be identified from the data which is present in the device memory. This method is only good to detect previous types of intrusions, and can't be used for new types of intrusions.

I.III.II Anomaly Detection.

When an attack occurs, it must be checked instantly, using detection and prevention. A few systems and applications allow the user to create or define a baseline, or more commonly known as, a threshold. There are many ways to create this threshold, but the common technique is the usage of a neural network, or using manual statistics, obtained from various sources. Then the detection system works.

If the activity crosses the threshold or baseline, the system raises an alarm. Or rather than simply detecting, the system compares the current activity and compares it to the various details present and checks if there is anything wrong. If or when the difference is quite large as compared to the statistics present tin the database, the system then raises an alarm.

II. STATE OF THE ART

It has been noted that in last few years, the strength and intensity of DDoS attacks has gone up exponentially. The attacks are now more dangerous, stronger and now are able to easily break through simple defence mechanisms. The defence systems have also been turned into better options that help us to protect ourselves from these malicious attacks.

The defence against DDoS attacks is done in three very important phases, namely: before, during, and after the attack. The most important one, or before the attack si simply some precaution, which requires some time and processes to actually fight back the attack. The last and final line of defence. Thus, from looking at these it can be said that the best way to protect against such malicious attacks is to make sure that the attack does not reach its target destination, and hence compromise the system or server.

II.II Time-based anomaly detection

Normally, in attack detection, a single value, usually known as the threshold value, is set. When the observed statistics are shown to exceed the threshold value, the system is said to be under attack. In previous anomaly detection algorithms, when a single value from the observed statistics crossed the threshold value or the range a certain range, then the system raises an alarm instantly.

Some systems also employ the use of neural networks to set the threshold value or the range of values. This method, however does not use neural networks, but uses a simple method to timely and accurately detect attacks. Here, the threshold value (N) is ignored. Instead, a time-based detection method is employed. The main point of this method is to use a range of time, rather than an instance, to compute attacks and detection.

The advantage of this algorithm is that total detection time is controlled by us, and the alarm is only raised if the attack goes on for a length of time. AN increase in the amount of traffic for a short period of time can be considered normal. However, any attack longer than that con be considered malicious.

II.IIVariation Detection

Variation detection method is used to check the variation of all the statistical data which is being detected. This algorithm uses and implements the idea of variation detection to the detection of anomalies which occur in the system. This allows the algorithm to detect the attacks quicker than most algorithms.

If the amount of traffic is more than the mean of regular traffic, then the threshold value is increased by 1. This is done to reduce the number of false alarms.

The optimum condition to run this algorithm would be when the traffic lies between the average and the standard deviation of regular traffic.

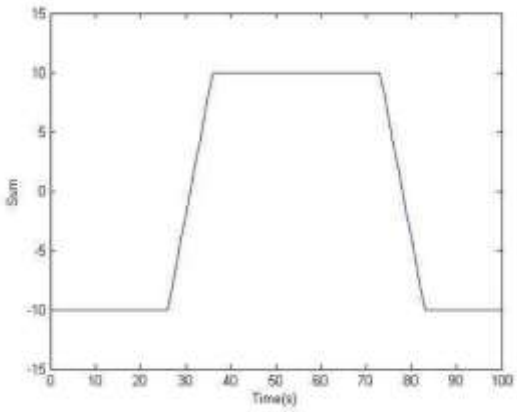
III. PROPOSED WORK

Nowadays, due to many of the detection systems taking too long to detect the attacks, a faster detection system is required. On the other hand, the systems which detect the attacks quickly do so in a

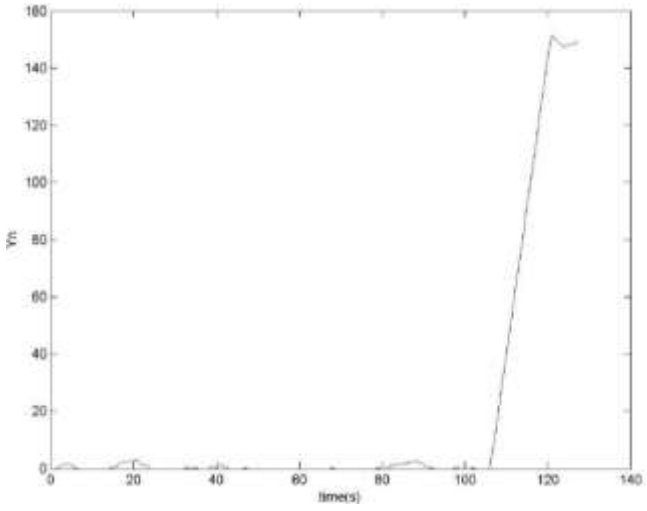
International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 6 June 2021, pp: 723-726 www.ijaem.net ISSN: 2395-5252

manner which result in a lot of false alarms being triggered. Due to this, there aren't too many systems which use a combination of both techniques, resulting in systems which are ineffective or overworked.

However, the combination of both of these techniques require that some amount of time will be taken to detect the attacks, with there being minimum number of false alarms.



The above image shows the graph of the time based algorithm



The above image shows the graph of the variation detection algorithm.

IV. IMPLEMENTATION

Using Python programming, a method of detection of the packets entering the system is created. This is done by using the socket library, which allows us to interact with the packets entering the system, which is helped along with the usage of a server address bound to the host.

The socket is created using the following code:

```
S = socket.socket(socket.AF_INET, SOCK_STREAM)
```

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 6 June 2021, pp: 723-726 www.ijaem.net ISSN: 2395-5252

The binding of the server address is done using the following code:

```
server_address = (",80)
s.bind(server_address)
```

Next, an empty dictionary is used to note down the different IP addresses entering the system at any given time. This dictionary also allows the removal of any redundancy which might be present in the code.
A text file is now used to note down the IP addresses which are attacking the system along with the date and time of the attack. This allows us to cross reference the IP addresses and block them at a future date.
The main loop of the code uses while loop to run. The loop converts the packets into string format for easy accessibility and understanding.
This is done using the following code:

```
ip_hdr = struct.unpack("!8sB3s4s4s",ipheader)
```

This is followed by the dictionary automatically updating itself with all the IP addresses which have already entered the system.
The following code makes sure of that:

```
dict[IP] = dict[IP]+1
```

The part of the loop which removes redundancy is done by comparing the already present IP addresses to the IP addresses which are entering the system. This makes sure to remove any and all redundancy.

V. CONCLUSION

Using the combination of the two algorithms allows us to create an algorithm that will be able to detect the attack fairly quickly with minimum number of false alarms. The attacking IP addresses will be shown in a text file which will be created during the running of the code itself.
The attacking IP can then be blocked or any prevention system can be executed to prevent the attack form happening.

REFERENCES

[1] Liying Li, Jianying Zhou, and Ning Xiao: "DDoS Attack Detection Algorithms Based on
[2] Entropy Computing", in ICICS'07: Proceedings of the 9th international conference on Information and communications security
[3] Nurefşan Sertbas¸ BÏulbÏul and Mathias Fischer:" SDN/NFV-based DDoS Mitigation via Pushback", in ICC 2020 - 2020 IEEE International Conference on Communications (ICC)
[4] Carol Fung, and Yadunandan Pillai: "A Privacy-Aware Collaborative DDoS Defence Network", in NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium
[5] Suman Nandi, Santanu Phadikar, and Koushik Majumder: "Detection of DDoS Attack and Classification Using a Hybrid Approach", in 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)
[6] Huan Lin, Shoufeng Cao, Jiayan Wu, Zhenzhong Cao, and Fengyu Wang: "Identifying Application-Layer DDoS Attacks Based on Request Rhythm Matrices", in IEEE Access (Volume: 7), pages 164480 - 164491