MBNA Publishing House Constanta 2021

Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

Detection of DDOS attack in the cloud

To cite this article: D. GLĂVAN, S. BÎRLEANU, C. RACUCIU and R. MOINESCU, Proceedings of the International Scientific Conference SEA-CONF 2021, pg.207-211.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-21-027

Detection of DDOS attack in the cloud

D Glăvan, S Bîrleanu, C Racuciu, R Moinescu

dragos.glavan@gmail.com

Abstract: A DDoS attack aims to disrupt basic processes by slowing down or completely stopping the performance of websites, mobile applications, cloud services, or any other IT system that relies on communication with the main network. DDoS attacks occur by congesting the high-traffic network and sending many requests simultaneously from sources that cannot be easily detected. Under the pressure of increased traffic, the systems will either consume a lot of resources to run commands efficiently, or, in extreme cases, they may stop working completely. These actions are known as under-saturated attacks, causing a system to slow down without overloading it. By having a relatively low impact, DDoS attacks can act for weeks on end without being detected, or they can attack the same targets repeatedly. A study on this subject shows that 86% of companies affected by DDoS have gone through several attacks. Cloud services are mainly transported over the Internet, so they are very prone to various attacks that can lead to the exposure of sensitive data. This paper presents an analysis of the various detection techniques used and implemented in cloud environments.

1. Introduction

Currently, there is a significant increase in the number of security incidents worldwide. At the same time, the number of those who own mobile devices is growing alarmingly with the development of technology. The Cloud environment provides access, without significant effort, to a network to collect resources. Today, in the cloud environment, users use only the services they need. Cloud storage consists of archiving, organizing and distributing on demand data between virtualized storage volumes that have been consolidated into physically disparate hardware. Or, in simpler terms, cloud storage is the organization of data stored somewhere, from where it can be accessed by anyone, based on permissions. Data can be archived in the short or long term. Short-term saved data is managed by RAM (random-access memory), which is responsible for processing and retaining all requests and actions performed during the processing of a specific computer (called tasks). Once all operations are completed, the data can be stored as long-term memory between different storage volumes, some of which may exist in the form of a cloud. The following types of cloud storage will be presented below:

- Storage in public cloud - data are stored in virtual resources, are made from proprietary hardware and are managed by a third party;
- Storage in private cloud - the data are stored in virtual resources, are made using own systems and hardware equipment, dedicated - owned and managed by the beneficiary company or institution;
- Hybrid cloud storage - Storing data in a combination of 1 or more public and private cloud environments becomes hybrid cloud.

2. Issue in cloud

The Cloud environment is a widely accessible and scalable environment, which makes it vulnerable to attackers. Thus, there is a high risk regarding the protection of the Cloud environment, where attackers can violate data security. According to a 2013 report by IDG Enterprise, security is one of the main issues preventing large companies from using the cloud environment. Mainly, cloud services are available through the Internet, which leads to an increase in the number of attacks on such systems. The most common type of attack at this time is Denial of Service (DoS). Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks are a method by which computational resources are made unavailable to their legitimate users. Although the methods by which these attacks are carried out are very varied, these types of attacks are aimed at making a web page or a web service work slowly or not at all. The main targets of DoS attacks are web servers for banking, or Internet name resolution services. These attacks are usually carried out by simple requests, repeated to the target stations until they begin to respond very difficult to legitimate users or are unable to respond at all. DoS attacks are a violation of the acceptable use policies of all Internet service providers. These attacks also violate the laws of most states. A Distributed DoS (DDoS) attack is an "attack that uses multiple computers to launch a coordinated DoS attack on one or more targets. Using client / server technology, the attacker is able to significantly enhance the effectiveness of the DoS attack by leveraging the resources of several unwittingly complicit computers, which are used as attack platforms. " DDoS attacks are the most advanced form of DoS attack and are based on the architecture of the Internet. Most attacks are resource-oriented and bandwidth-oriented.

2.1 Types of vulnerabilities

Attacks can be classified according to the vulnerabilities exploited as follows:

A. Bandwidth depletion attack - in this case the entire bandwidth of the targeted system is used by flooding the data traffic to disrupt the victim's network. Such attacks can be classified into:

- Flood-attack - in case of this type of attack, it takes place by repeatedly sending initial connection request packets, the attacker is able to overwhelm all available ports on a targeted server machine, causing the targeted device to respond slowly or not at all to legitimate traffic;
- Amplification attack - an attacker leverages the functionality of open DNS resolution devices to overwhelm a target server or network with an amplified amount of traffic, making the server and surrounding infrastructure inaccessible. All amplification attacks exploit a difference in bandwidth consumption between an attacker and the targeted web resource. When the cost difference is increased on multiple requests, the resulting traffic volume can disrupt the network infrastructure. By sending small queries that result in big answers, the malicious user can get more out of less. By multiplying this magnification by the fact that each bot in a bot network makes similar requests, the attacker is both overwhelmed by the detection and the benefits of much higher attack traffic. These types of DDoS attacks can be carried out by either the attacker by direct attack approach or with the help of zombies.

B. Depletion of resources attack - the victim's system services are used so that genuine system users' requests are not accepted. They can be classified as follows:

- Exploits of protocol attacks - this attack is due to the fact that many connection-oriented protocols need a server to maintain status immediately after a connection request has been

received but before this connection is established. An attack by exhausting connections is the SYN flooding attack, this is done by sending a SYN message by the attacker to a server, without the attacker completing the third step of the handshake, this occupying part of the server's memory until the connection expires, often after 75 sec. Because these "semi-open" connections occupy OS memory, they limit their number, so the attacker will launch a series of requests to connect to the server, until it reaches this limit, causing any other connection requests to be rejected.

- Packet-malformation attack - The attacker transmits infected data to crash the system. This attack can be performed by the following methods:
    - Attack via IP-address - infected data is hidden using a similar source and destination IP address, thus creating a disorder in the operating system. Thus, the system becomes slow and causes delays and blockage of the targeted system.
    - IP-packet options attack - in this case the additional fields of the IP address are exploited to project malicious data. These attacks are most penetrable when carried on a large scale or targeted by multiple zombie systems.

3. Attack detection

Procedural analyzes have been performed to reduce the effects of DDoS attacks on different networks.

Using cloud-based IDS - these include:

a) Network intrusion detection systems (NINDS) - its main purpose is to analyze, capture and filter the incoming and outgoing network traffic of an organization. It uses port scanning because mainly attacks are performed on ports with low security. Thus, an analysis of the IP addresses and of the header field of the transport layer is performed from the captured packets. NINDS can counter attacks or filter the entire organization's network packets depending on where it is installed. An intrusion detection system is a device or software application that monitors network or system-related activities for malicious activities or policy violations and reports to a management station. An intrusion detection system passively monitors data packets and event logs. The principle of operation of the system is:
    - Network traffic is copied and directed to the sensor of the detection system for analysis.
    - If a portion of the traffic coincides with a penetration activity this traffic is "destroyed".
    - The system sensor sends an alarm message to the management console.

b) Host-based intrusion detection system - applications that work on information collected from individual computer systems. This view allows a HIDS to analyze the activities on the host it monitors at a high level of detail; it can often determine which processes and / or users are involved in harmful activities. In addition, unlike NIDS, HIDS are aware of the outcome of an attack attempt because they can directly access and monitor the data files and system processes targeted by these attacks. Most HIDS software, such as Tripwire, establishes an "inventory files" and their attributes in a known state and uses that inventory as a basis for monitoring any system changes. "Inventory" is usually a file that contains MD5 checksums for individual files and directories. It must be stored offline on a secure, read-only medium that is not available to an attacker. On a server without read media (a blade server, for example), one

way to do this is to store the statically compiled intrusion detection application and its data files on a remote computer.

c) Signature-based detection (SIDS) and Anomaly Based Intrusion Detection System (AB-IDS) - Signature and anomaly detection is the two main methods of identifying and alerting to threats. While signature-based detection is used for threats, we know, anomaly-based detection is used for behavioral changes. Signature-based detection is based on a pre-programmed list of known compromise indicators (IOCs). An IOC could include malicious network attack behavior, the content of email subject lines, file hashes, known byte sequences, or malicious domains. Signatures can also include alerts on network traffic, including known malicious IP addresses trying to access a system. Unlike signature-based detection, anomaly-based detection is able to alert to unknown suspicious behavior. Anomaly-based detection first involves training the system with a standardized baseline and then comparing the activity with that baseline. Once an event occurs normally, an alert is triggered. Alerts can be triggered by anything that doesn't align with the standard baseline, including a user who connects outside of business hours, a lot of new IP addresses trying to connect to the network, or new devices added to a network without permission.

d) Hybrid IDS - is a combination of anomalies and signature-based detection methods. Thus, an improvement of the efficiency of IDS can be obtained. In the cloud, C. N. Modi has implemented hybrid detection methodologies to enhance IDS effectiveness.

Identify known and unknown DDoS attacks using artificial neural networks. The model should be trained according to the data sets to know the difference between normal and attack data traffic. Thus, the attack is allowed to reach its destination. Artificial neural networks are based on feedforward and backpropagation techniques. Here the network traffic is continuously monitored for any abnormal behavior, by analyzing the packets according to the trained ANN. However, recovering large amounts of data in a system of routes connected by connections is inexpensive and time consuming. Therefore, the proposed solution is to introduce a separate threshold for each protocol. The resulting packets are contained for investigation, if the number of packets in a network is higher than the threshold as defined for the protocol. The packets contained are then processed by the ANN model, which decides the legitimacy of the packet. The DDOS detector communicates through other messages through encrypted messages. The following steps must be completed:

- DDoS detectors are implemented on different networks;
- The DDoS flag stores the IP address of all other DDoS detectors to instruct and send e-mails in encrypted form, an attack is detected;
- Detectors continuously monitor the network for any abnormal event;
- Possible abnormal events are reported;
- The IP is stored in suspicious packets;
- ANN calculator, adjusts the received packets and makes them ready to be analyzed by the ANN system.

Machine Learning for DDoS attack detection - the efficiency of machine learning methodologies regarding the defense against DDoS attacks is analyzed. The following steps are followed:

- Can counter zero-day raids.
- Monitoring the resources consumed at input and output.
- Packet filtering (UDP, TCP, ICMP).
- Alternative algorithms can be used to detect anomalies using ANN.

To resolve data packets as harmful or not. The data with extracted characteristics are transmitted through ANN for their training. Only half of the data is used for training, the other half is used to validate the testing process. Here the performance of the algorithm is analyzed.

Genetic Algorithm Intrusion Detection Systems - the genetic algorithm is defined as the technique that uses the biological factors of evolution to solve a problem. Based on Darwin's theory of evolution, he adds the most appropriate survival options to increase a population of the individual solution to a predefined force [19]. The general rules are implemented in the intrusion detection stage to filter the incoming network traffic and in real time conditions. The rules are made to make detection simple and effective. The genetic algorithm uses features such as natural selection plus evolution that implements the structure of selected chromosome data, recombination features, and mutation change factors. First, a random population of chromosomes is selected that describes all available solutions to a problem, which are treated as candidate results. Characters, bits or numbers are encoded from different chromosomes, which represent genes. To calculate the functioning of each chromosome in relation to the available solution, a fitness function is evaluated. To test the effectiveness of a fitness function of the chromosome is applied. If the result is good and correctly identifies the attack, it is considered a solution. Then crossbreeding and mutations are applied to these good chromosomes to produce a newly formed generation. These steps are repeated using the newly formed population. The evolution continues until a valuable solution is reached. These rules are then tested on the training data set for its accuracy and prediction.

4. Conclusion

This paper presented various attacks on cloud computing systems, which represent one of the main challenges regarding the security and confidentiality of information systems. The task of implementing measures against information attacks is a complex and complicated task. However, the use of machine learning algorithms with the existing IDS is a good approach, but each detection method has its own limitations. It must be emphasized that the motivation for carrying out such an attack must be fully understood in order to be able to implement some countermeasures. Due to its openness to the population, the Cloud environment is very vulnerable to many attacks. Maintaining security on different systems on the cloud platform is in itself a challenging task, but nevertheless, these attacks can be minimized if the necessary policies and procedures are followed. A general solution should be developed to counter DDOS attacks that contain both known and unknown types of attack.

REFERENCES

[1] P. Mell, T. Grance 2011 *The NIST Definition of Cloud Computing NIST Special Publication 800-145 (SP800-145)*

[2] John & Liu, Jin & Mao 2011 *NIST Cloud Computing Reference Architecture*

[3] D. Zissis, D. Lekkas, 2012 *Addressing Cloud Computing Security Issues, Future ati Generation Computer Systems*

[4] J. Mirkovic, 2012 *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*

[5] S. Devine, 2015 *The growth and evolution of DDoS, Network Security*

[6] C. Douligeris 2019 *DDoS attacks and defense mechanisms: Classification and state-of-the-art*

[7] H. J. Liao, Y. C. Lin, 2013 *Intrusion Detection System: A Comprehensive Review*

[8] M. Taghavi, J. C. Junior, 2013 "*An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Overview*"