International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

HTTP FLOODING ATTACK DETECTION USING DATA MINING TECHNIQUES

Arockia Panimalar.S[1], Monica.J[2], Muthumeenal.L[3], Amala.S[4]

[1]*Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*
[2,3,4]*III BCA 'A', Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*

Abstract: *DoS and DDoS, the network flooding attacks has threats on network services, rapid detection and semantic analysis are concentrated on secured features and reliable network services. Flooding attack detection and in-depth analysis system are the two features which uses data mining techniques. DoS (Denial of Services) attack threat to internet sites and among the hardest security problem, because of their potential impact. DDoS (Distributed Denial of Services) attack which is easily exhausted for the computing and communication resources of the host in very short period of time. It is the co-operative large scale attacks which are produced from an enormous host which is known as ZOMBIES, considered as the major threat to internet services. The latest development in data mining methodologies are embedded with variety of algorithms are from the field of statics, pattern mining, machine learning and database. For protecting the network routers, network servers, client host becoming the handlers, ZOMBIES and victim of DDoS attack data mining methods can be used as an ultimate weapon.*

Key Words: *DDoS, DoS and ZOMBIES.*

1. INTRODUCTION

DDoS - A distributed denial of service attack is most common and damaging forms of attack on the cloud. The Denial of service (DoS) attacks is for the unavailable functioning of resources to the customers, hackers can send the unwanted messages continuously and make the traffic on the network from multiple resources, hackers will send packets to the receiver which make harmful to the system and temporarily stop the services between client and server communication. HTTP (Hyper Text Transfer Protocol) flood is a type of Distributed Denial of Service (DDoS) attack. HTTP flood consists of "ZOMBIE ARMY" a group of large number of compromised hosts.

2. DDOS ATTACKS

In a Denial-of-Service (DoS) attacks such as flooding, software exploit, protocol based etc. DDoS - A distributed denial of service attack is uses different machines to prevent the permissible use of services.

DDOS attacks are of different phases, they are as follows:

i. Recruit Phase – In Recruit phase, there are multiple agents like slaves and zombies machine for security purpose.

ii. Exploit Phase - In Exploit phase, to utilize the attacked or harmful host and then their security holes are transformed into injected code.

iii. Inject Phase- In Inject phase, to inject the attacked or harmed code to it (malicious code).

iv. Use Phase - In Use phase, it is used to send the attacked code in the form of packets via agents to inject all the machines further.

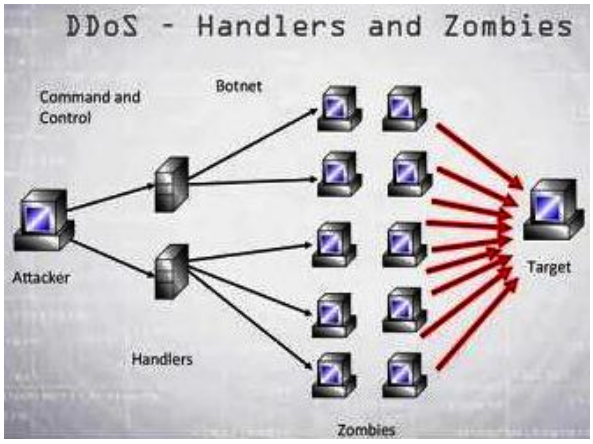

Fig 1: Architecture of DDoS Attack

A. HTTP FLOOD ATTACK

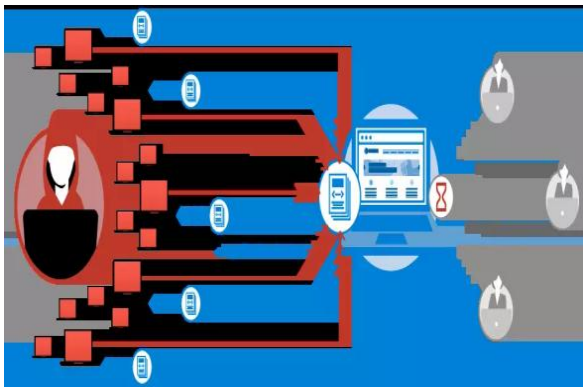

Fig 2: HTTP Get Attack

HTTP Flood attack is a type of (DDoS) attack in which the attacked or harmful host changes to POST for hack the web browser and services application. They are used as interconnected computers which has been considered as the

aid of malware, which is considered as the disturbing resources such as Trojan Horses, computer viruses, worms etc. HTTP floods possess less bandwidth.

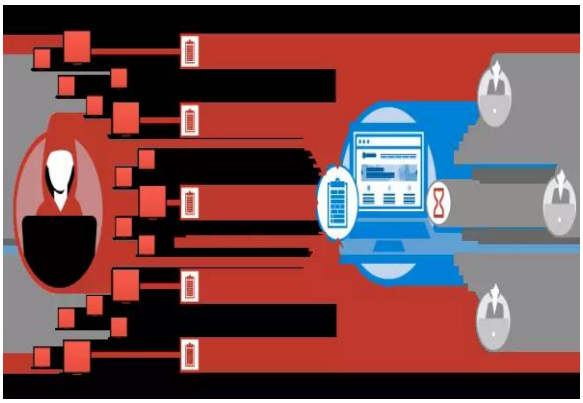

Fig 3: HTTP Post Attack

3. DATA MINING TECHNIQUES

Data mining is important for DDoS attack detection. It is used to transfer the raw data into structured information. Data mining follows six various types of classes namely statistical classification, association rule learning, clustering analysis, regression analysis and automatic summarization, deviation detection.

Various techniques of data mining are used for detecting DDoS attacks. They are:

A. Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is an application used for controlling the network traffic and protects the system or network administrator. It is a software application which is used to monitor the network and system activities and finds the different operations occurred. In field of business, industry, security and health sectors LAN and WAN networks are used.

Types of IDS

- Host based IDS
- Network based IDS
- Signature Based IDS
- Anomaly Based IDS
- Passive IDS
- Reactive IDS
- Application based IDS

Advantages of IDS

- Boost up Efficiency
- Easier to maintain and regulate security
- Can qualify and analyze the attacks/bugs
- Functioning of good context of protocol
- Tuned to specific information of networking

Intrusion detection system in data mining is the process which is used to get the hidden information from the databases. They are of two divisions, they are

i. Misuse Detection - Misuse detection is used as the labeled/signature based detection. It can be detected only by the recognized available signature.

ii. Anomaly Detection - Anomaly detection defines the deviations between the models.

Technical Challenges

- Problem to false alarm, in which the different application is being triggered in stopping the event
- Scalability conditions, in which the size of the network fluctuates
- Data collection and logging
- Vulnerability to attacks
- Understanding and interpreting IDS data
- Keep track the IDS rule set regularly
- Alert correlation

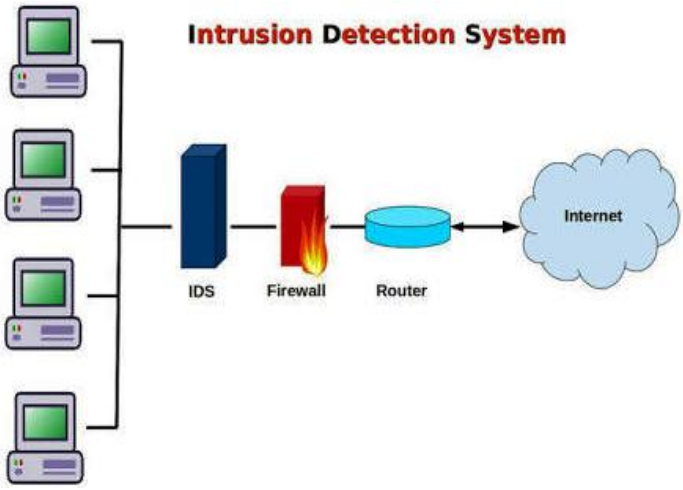

Fig 4: Intrusion Detection System (IDS)

B. IP Traceback

IP Traceback is used for determining the reliability of packets present on Internet. It is used to defend against the DDOS attacks. LOGGING is the methodology which is used to log packets at key routers. It locates the origin of the packets. It is complicated because IP address can be forged or spoofed.

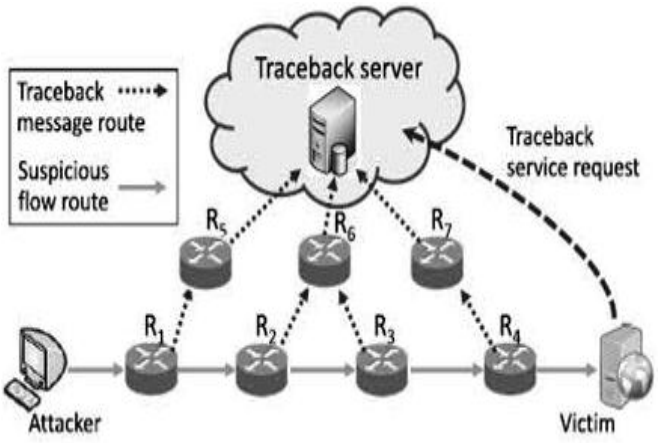

Fig 5: IP Traceback

i. Link Testing

It starts from the victim of the source and assumes that the attack is active till the end of the trace. Two variants of link testing are:

1) Input Debugging and

2) Controlled Flooding

ii. Packet Marketing

It is one of the significant methods used. This marketing utility the rarely used IP header to store the trailer, where it is used for marking varies from scheme to scheme. It is categorized into two types, they are

- Probabilistic Packet Marking
- Deterministic Packet Marking

4. CONCLUSION

In this paper, the study on HTTP flooding attack detection using data mining techniques is carried out. DDoS attack is a complex technique for attacking the computer networks. Various techniques of data mining are used to detect DDoS attack. The paper has discussed about IDS and IP Traceback. The improvement in technology for handling DDoS attacks and DoS attacks using data mining techniques can be utilized more in future.

5. REFERENCES

[1]https://www.verisign.com/en_In/security-services/ddos/ddos-attack/index.xhtml

[2] http://news.cnet.com/8301-1009_3-2001.htm.

[3]http://www.darkreading.com/security-services/security/perimeter-security/222301511/index.html

[4] PeymanKabiri and Ali A.Ghorbani-"Research on Intrusion Detection and Response Survey"- International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005

[5] Intrusion Detection System Buyer's Guide, Paul Dokas, Levent Ertoz.

[6] Aleksandar Lazarevic, Jaideep Srivastava, PangNing "Data Mining for Network Intrusion Detection".

[7] Aleksandar Lazarević,Jaideep Srivastava, Vipin Kumar-"Data Mining for intrusion detection"-Knowledge Discovery in Databases 2003.