Study of application layer dos attacks essay

Business, Marketing

CHAPTER 1

INTRODUCTION

Denial of Service (DoS) attacks is an endeavor to make computer resources unavailable to the legitimate users. A DoS attack will try to consume as much resources as it can so as to deny legitimate users the chance of having services or resources available to them. There are several categories of DoS attacks. The DoS attacks are not the same in terms of how they are perpetrated. Depending on the method of perpetration, one category of DoS can be easy or hard to stop. 1

A denial of service attack involves sending numerous communication requests to the target machine thus making it not possible for the machine to attend to legitimate traffic. A denial of service attack may also slow down the process of communication thus rendering a server virtually useless. DoS attacks can also force the targeted computers to either reset or consume all its resources thereby obstructing communication between the intended users and the victims. 2

BACKGROUND OF STUDY AND MOTIVATION

Many internet users have been complaining about slow connections, unavailability of network resources or sometimes not being able to access a website at all. This problem has been on the rise in the recent past. Researchers have suggested that some of the problems are caused by DoS attacks which attack different layers of the network. Solutions were devised for layer 4 DoS attack which was the first one to be detected. Recently, a new kind of attack called layer 7 DoS attack which affects the Application

layer has emerged. This problem prompted this study so that we can devise ways of detecting and controlling this kind of problem that literally eats up all the network resources. 3 The Distributed Denial of Service attacks are a major problem in computer networks. This is because they send requests which appear to be legitimate and ends up consuming all the network resources thus denying the legitimate users a chance to use the resources. The Distributed Denial of Service attack is a continuous critical threat in the information technology industry. Internet has been the most hit by this problem. The application layer DDoS attacks uses the legitimate HTTP requests which devastate the server. These requests are not easy to detect.

CHAPTER 2

LITERATURE REVIEW

Application layer DoS attacks

Application layer DDoS are the most difficult denial of service attacks to alleviate. They attack the application layer at the Transfer Control Protocol/ Internet Protocol stack. This is because they look genuine to the classic firewalls which allow them to pass freely into the network. Firewall therefore cannot be effective in controlling these kinds of attacks. The best way of controlling these application layer DoS attack is through the use of deep packet inspection also known as layer 7 inspections.

How a DDoS attacks a system

The attack is performed by a series of requests which are sent simultaneously to attack a victim server. A zombie which is responsible for an attack gets hold of the TCP 3-way handshake and then starts sending the

data packets. The data packets sent occupies the server in such a way that the server cannot attend to any other traffic. This eventually results into denial of services to the legitimate users.

The OSI layer Model

Application Layer

(Layer 7)

Application

Presentation Layer

(Layer 6)

Session

Session Layer

(Layer 5)

Transport

Transport Layer

(Layer 4)

TCP UDP

Network Layer

(Layer 3)

Network

Data Link Layer

(Layer 2)

Physical Protocol

Physical Layer

(Layer 1)

Transmission Medium

Symptoms of a DoS attack

Unusual slow network performance when opening files or accessing web sites

Inability to access any website or unavailability of a specific kind of website

E-mail bomb which involves a remarkable increase in the number of spam e-mails which are received.

Layer 4 DDoS attacks

The layer 4 DDoS attacks were the most common in the past. They are often referred to as a SYN flood. They attack the transport layer of the OSI model whereby they force the target machine to reach bandwidth or connection limit thus obstructing legitimate users from getting services from the servers. The level 4 DDoS attacks are not hard to manage and currently

there are mechanisms which can be used in order to stop them from attacking the network.

How layer 4 DDoS attack operates

There is a TCP connection which is established in a 3-way handshake. The three way handshake involves the client sending a packet, the server responding and then the client responding again. When the client sends a SYN packet, the server responds with a SYN ACK and the client responds to that with an ACK. Once the 3-way handshake is complete, the TCP connection can then be said to be complete. After this, the application can then start sending data using the application layer protocol which is available. 4

Layer 4 DoS attack involves an attack experienced on the system when it is still waiting for a response. The attack sends a flood of SYN packets and then ignores the SYN ACKs which are returned by the server. This results into the server using up all the resources waiting a configured amount of time so that the expected ACK can come from the rightful client. SYN floods are relatively easier to handle by the proxy based applications. This is because they proxy connections for the servers. The proxy based solution is usually to terminate the TCP connection. This helps in stopping the SYN flood at the proxy and legitimate connections passed on to the server which is ready.

SYN cookies are used to stop the attackers from flooding the network. There are servers that can implement SYN cookies but this is not frequently used as it overburdens the servers. This eventually slows down the speed of operations of the servers.

Layer 7 DoS attacks

This type of DDoS attack operates at the application layer of the OSI model. It is very hard to detect as it sends requests which are very hard to differentiate from the legitimate requests which makes it to have a higher obscurity. This attacker looks like a genuine connection and this enables it to gain entry into the web or application server. Once it has entered the web or application server, it begins to request for large number of files using HTTP GET. This process of requesting for a bunch of requests overwhelms the server thus making it (the server) to lose focus thereby ignoring legitimate requests and paying attention to the requests from the attacker which up to this time looks as if they are also legitimate. 5 It is very efficient as it requires a smaller number of connections. It is more lethal as it can deny services to the legitimate users disregarding the hardware capabilities of the host. The best way to control HTTP GET DDoS attack is by imposing a time out for HTTP headers to be sent. Any connection which exceeds the header time out will be automatically closed. This renders the HTTP GET attacks ineffective against IIS web servers. This was controlled using rate-limiting but it was later mutated by the inventors so as to start using distributed systems. This made the requests more difficult to detect and also to stop. The layer 7 DoS attacks are very difficult to detect because the TCP connections and the requests are valid. It can only be detected by considering the number of requests made at the same time and perform analysis to determine that it is indeed an attack. The major problem that is faced from this kind of attack is that legitimate requests from legitimate users can be mixed up in the attacker’s requests. This makes it very difficult

to detect and if the whole process is stopped, one will also deny requests to the legitimate users too thus the overall aim of a DoS shall have been achieved.

In order to completely eliminate this kind of attack, some kinds of rate shaping algorithms are used. The algorithm will watch over the clients and track the number of requests they make at any particular time. The clients are then allowed some maximum number of requests that they can make within a particular time. If a client exceeds the maximum number the client's IP address is blacklisted and subsequent request denied.

The attacker requests for large files using the HTTP GET. The requests are so many that they overwhelm the server. The server starts responding to these requests alone and ignores requests which may be coming from the legitimate users. The legitimate users will remain unattended to hence the denial of service.

Controlling the layer 7 DDoS attacks

i. Using ddosim

This is a simulating tool that can simulate a Distributed Denial of Service attack against a target server. The simulating test will help to show the capacity of a server in handling a specific kind of DDOS attack. Ddosim can simulate several zombie hosts which have random IP addresses that are fond of creating full TCP connections to the target server. After it has established a connection, it will then start the conversation with the listening application.

The ddosim has the following functionalities:

HTTP DDoS with valid requests

SMTP DDoS

TCP connection flood on random port

The following procedure can be followed in order to simulate such an attack.

Network configuration for DDOS simulation

On the victim machine ddosim creates full TCP connections – which are only simulated connections on the attacker side.

There are a lot of options that make the tool quite flexible:

Usage: ./ddosim

-d IP IP address of the target machine

-p PORT port of the target machine

[-k NET] Source IP from class C network (ex. 10. 4. 4. 0)

[-i IFNAME] Output interface name

[-c COUNT] Number of connections to establish

[-w DELAY] Delay (in milliseconds) between SYN packets

[-r TYPE] Request to send after TCP 3-way handshake. TYPE can be HTTP_VALID or HTTP_INVALID or SMTP_EHLO

[-t NRTHREADS] Number of threads to use when sending packets (default 1)

[-n] Do not spoof source address (use local address)

[-v] Verbose mode (slower)

[-h] Print this help message

Examples:

1. Establish 10 TCP connections from random IP addresses to www server and send invalid HTTP requests (similar to a DC++ based attack): 6

./ddosim -d 192. 168. 1. 2 -p 80 -c 10 -r HTTP_INVALID -i eth0

2. Establish infinite connections from source network 10. 4. 4. 0 to SMTP server and send EHLO requests:

./ddosim -d 192. 168. 1. 2 -p 25 -k 10. 4. 4. 0 -c 0 -r SMTP_EHLO -i eth0 6

3. Establish infinite connections at higher speed to www server and make HTTP valid requests:

./ddosim -d 192. 168. 1. 2 -p 80 -c 0 -w 0 -t 10 -r HTTP_VALID -i eth0

4. Establish infinite TCP connections (without sending a Layer 7 request) from local address to a POP3 server:

./ddosim -d 192. 168. 1. 2 -p 110 -c 0 -i eth0

Other methods of controlling the application layer DoS include:

ii. Firewalls

Firewalls allow or deny protocols, IP addresses or ports from accessing the network. They are majorly used for handling simple flooding type attacks. However, they are not very effective as they cannot effectively distinguish between good traffic and a DoS attack. Firewalls are also placed too deep in the network hierarchy. Some network resources on top of the hierarchy can be affected before the firewall is able to get the traffic. 7

iii. Switches

Most switches are intelligent enough to detect and remediate DoS attacks through automatic rate filtering and WAN link failover and balancing. The switches have; rate limiting, bogus IP filtering, deep packet inspection and traffic inspection which ensures that all the traffic entering the system are safe.

iv. Routers

Routers also have rate limiting and ACL capabilities which help in inspecting the traffic entering the system. Routers can be easily overwhelmed by DoS attacks. They can be manually configured in order to change the settings which can help in barring the DoS attacks from gain access into the network.

v. Application front end hardware

This is a form of intelligent hardware which is placed on the network at strategic positions that help in inspecting the traffic before it reaches the servers. It can be placed on the network together with the switches and the routers. The applications front end hardware analyzes/inspects the traffic as it enters the network and then identifies them as priority, regular or dangerous traffic. If it is dangerous, then access is denied. 8

vi. Intrusion Prevention System (IPS) based Prevention

IPS is very effective especially if the attacks have signatures which are associated with them. They help in detecting and blocking denial of service attacks as they have the processing power and the capabilities to analyze the attacks. They act like circuit breakers where by they simply disconnect

the part that the DoS attack has been detected thereby protecting the system from the effects of the DoS attack. The also help in continuously monitoring the traffic pattern to determine if there is any traffic anomaly in the system. It helps in letting the legitimate traffic to flow as it blocks the DoS attack traffic. 9

vii. Prevention through proactive Testing

This involves using test platforms which perform simulated DoS attacks which helps in evaluating the most appropriate defensive mechanisms to be used. Using this technique helps in analyzing the effects of a DoS, the areas they attack and how they can be controlled.

viii. Black-holing and skin-holing

Black-holing: When using this mechanism, all the traffic that is vulnerable is sent to a null interface or a non existing server. The traffic is then analyzed there using a sink holing technique which routes it to a valid IP address and rejects bad traffic. This techniques is however not very efficient especially for severe attacks. 10

ix. Clean pipes

This involves passing all the traffic through a cleaning center whereby all bad traffic is filtered from the good ones. Only good traffic is sent beyond to the server. 11

It is very important to prevent both layer 4 and layer 7 DoS attacks so as to ensure that there is a fast and secure delivery of an application. 12

Other ways of controlling layer 7 DoS include limiting the traffic using hash limit on ip-tables. This module allows just a specific number of packets in a minute. It will help to reduce the burden on the server as there will be no numerous requests to be handled at the same time thus leaving some time for legitimate requests.

Stop the Hive which is used as the command and control server used for sending instructions pertaining to different targets.

Rate limiting – This method is no longer used as the layer DoS attacks use legitimate requests thus filtering can be a big hurdle. Rate shaping algorithm was introduced once it was realized that the Rate shaping algorithm was no longer efficient.

Rate shaping algorithm – This keeps watch over the clients to ensure that they don’t request more than a predefined number of requests set. If a client is fond of making several requests simultaneously, the client is black listed and is not granted any form of access until it has been removed from the blacklist.

Areas affected by the layer 7 DoS attack

DoS attacks causes obstruction of communication media which degrades the communication between the intended user and the victim.

They cause disruption of configuration information and physical network components thus compromising the internetwork and intranetworking communication. 13

They also consume computational resources such as bandwidth, processor time and speed, disk space and random access memory leading to a significant drop in speed of the computer.

How to control HTTP GET DDoS attacks

- Use web servers which have a time out limit for HTTP headers.
- Use load balancers such as F5 and Cisco, reverse proxy and mod_antiloris
- Use delayed binding or TCP splicing to defend against HTTP GET attacks.
- Limit the size of request to each forms requirements
- Identify the normal access speed of your network. This will help in predicting a mishap in the network thus prompting a timely action to be taken.

  Assign each client in the system a maximum number of requests that it can make at a given time. If the client exceeds the maximum number, then it is blacklisted. This will help in reducing cases of a single client consuming all the network resources and leaving the other users unattended.

Tests benches for testing the effects of the DDoS attacks

The diagram below shows a simple test bench. SmartBits and Avalanche are used as packet generators. The smartBits create session-less attack packets while the avalanche create the attack session packets. The clients (PC1 & PC 2) and the server are used for testing the mitigation results. On a typical

work station, we can replace the smartBits and the avalanche with PCs which have attack scripts to geneate the packets.

A typical example of a test bench used for testing the effects of the DDoS attacks

Source: Froutan, 2004

Summary and Conclusion

Denial of service attacks cause network degradation as they slow down the speed of the network and sometimes result into unavailability of network resources. DoS attacks may also lead to unfinished tasks as a lot of time is wasted waiting for completion of illegitimate requests sent by the DoS attacks. This can literally consume all the computing and resulting into unaccomplished tasks. Denial of service attack can be a very big problem in a networking environment especially when it is not detected in time. It can result into damages that can bring the whole network down. Proper mechanisms should be put in place to ensure that the DoS are detected whenever they occur so that they are stopped before causing any damage to any of the network equipments.

Denial of service attack is a criminal offence that is prosecutable in a court of law. In the United Kingdom for instance, a person found guilty of denial of service attack can be imprisoned for 10 years. In the United States of America on the other hand, denial of service attack falls under Computer Fraud and Abuse Act whereby a person found guilty can be sentenced to some years of imprisonment as per may be determined by the court. Other countries in the world have similar laws but the sentence varies depending on the nature of damage caused.

In this study we have looked at the DoS and DDoS attacks that affect a computer network. We have laid more emphasis on the layer 7 DoS attacks, how it works and the measures that should be taken in order to control this type of disaster. Layer 4 DoS attack is easier to control as the attacks can be easily detected by the firewall. However, Layer 7 DoS has posed a very big problem in networking as they send requests which appear to be legitimate thus making it very hard to be detected. This makes it very hard to control the layer 7 DDoS attack using the traditional methods that were used to control layer 4 DoS attacks.

REFERENCES

1. Addley, Es; Halliday, Josh " Operation Payback cripples MasterCard site in revenge for Wiki Leaks ban". The Guardian , London, 2010.

2. Bates, Claire " How Michael Jackson's death shut down Twitter, brought chaos to Google and 'killed off' Jeff Goldblum". Daily Mail London June 26, 2009

3. Erikson, Jon HACKING the art of exploitation (2nd edition ed.). San Francisco: No Starch Press. 2008 p. 251. .

4. Froutan, Paul " How to defend against DDoS attacks" 2004

5. Gont, Fernando " On the implementation of TCP urgent data". 73rd IETF meeting. 2008

6. HallVinton G. Cerf, Robert E. Kahn, A Protocol for Packet Network Intercommunication, IEEE Transactions on Communications, Vol. 22, No. 5, May 1974 pp. 637-648

7. Lu, Xicheng; Wei Zhao Networking and Mobile Computing. Birkhäuser. 2005 pp. 424.

8. Markoff, John " Before the Gunfire, Cyber attacks". The New York Times. August 13, 2008.

9. Mindi McDowell. " Cyber Security Tip ST04-015". United States Computer Emergency Readiness Team 2007

10. Muhammad Adeel & Ahmad Ali Iqbal " TCP Congestion Window Optimization for CDMA2000 Packet Data Networks". International Conference on Information Technology 2004

11. Peterson, Larry Computer Networks. Morgan Kaufmann. 2003 pp. 401.

12. Schwabach, Aaron Internet and the Law. ABC-CLIO. 2006 pp. 325.

13. Shachtman, Noah " Activists Launch Hack Attacks on Tehran Regime" 2009

14. Tanenbaum, Andrew S. Computer Networks (Fourth ed.). Prentice 2003.

15. Richard S. TCP/IP Illustrated, Volume 1: The Protocols.

16. Yuval, Fledel. Uri, Kanonov. Yuval, Elovici. Shlomi, Dolev. Chanan,. " Google Android: A Comprehensive Security Assessment". IEEE Security & Privacy (IEEE) (in press). 2008