DDoS Simulation and Hybrid DDoS Defense Mechanism

Saket Acharya
Manipal University
Jaipur

Nitesh Pradhan
Manipal University
Jaipur

ABSTRACT
In cyberworld, resource accessibility has a key part in digital security alongside confidentiality and trustworthiness. Distributed Denial of Service (DDoS) attack has turned into an intriguing issue to the availability of assets in computer networks. In this paper, DDoS attacks at different layers of TCP/IP protocol are scrutinized and comparison of existing GUI DDoS tools with a distinct DDoS script is done so as to know the trend of attacking technique used by the assailants to perform an attack.Various defense tools are analyzed and comparison of existing defense mechanism with a distinct hybrid protection methodology is done. This paper aims to provide a superior comprehension of the current DDoS tools, protective mechanisms,and comparative analysis of them.Existing deficiencies in tools and defensive tecniques are examined and reduced to improve the efficiency.

General Terms
Network Security,Cyber Security,Network Attacks, et. al.

Keywords
Cyber-attack, Cyber security,DDoS Attack,DDoS Attack Tools,Vulnerability,Mitigation

1. INTRODUCTION
DDoS is a critical problem to the availability of cyberspace resources.In DDoS attack, the attacker exploits any weakness in the protocols at different layers.In this way it conciliates different systems. These systems are known as zombies or bots.DDoS attacks are encompassed of packet streams from distinct sources.The DDoS tools do not need technical knowl-edge to implement them. Hence DDoS are becoming easier to unveil and hard to detect.DDoS traffic generates a heavy congestion in the internet and interjects all Internet users whose packets cross clogged routers. DDoS assaults never endeavor to break victim's machine, therefore making any obsolete security barrier instrument inefficient. The main goal of a DDoS attack is to harm a victim either for individual reasons, either for material gain, or for fame.[1]Application level attacks deluge a computer with such a high capacity of connection requests, that all available operating system resources are disbursed, and the computer can no longer process authentic user requests.

1.1 DDoS Architecture
DDoS architecture consists of the following things, as shown in Fig. 1:

- The attacker.
- The handlers: They have unique program running on them and are equipped for controlling numerous agents.
- Zombie hosts : They are responsible for generating a stream of packets towards the intended victim.
- A victim.

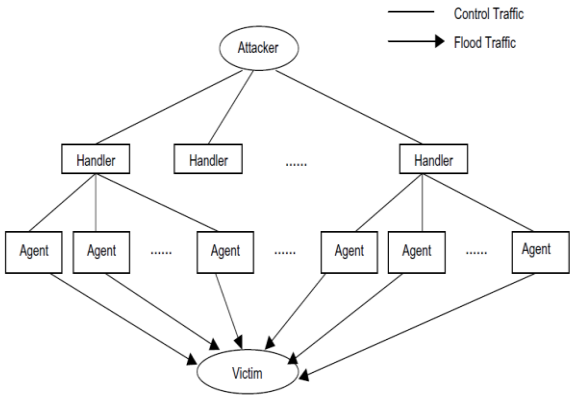

Fig 1: DDoS Architecture

Following steps take place during DDoS attack:

- The attacker picks the machines that have some weakness that the aggressor can use to access them.Using these machines,the attacker executes assault.
- The attacker feats the vulnerabilities of the operator machines and installs the assault code.
- The atacker associates with handlers to recognize which operators are running and when to arrange attacks.In in- stance of direct attack,the attacker transparently performs the assault without handlers.

1.2 DDoS Attacker's Motivation
An attacker can perform DDoS attack for the following possible reasons :[1]

- **Extortion** : Attacker puts the site down and requests cash in return for stopping their attacks.Sometimes they even bully the victim before finishing the assault.
- **Business Extortion** : If a company's site is down, its services are disturbed.Little measures of downtime can cost an organization a large number of dollars.

It can likewise embrace negative relationship with a brand, so that clients no more trust their administrations.

- **Hactivism :** Government locales in a few nations are often assaulted through DDoS digital fighting. In some cases it is pondered that these assaults could even be conferred by different countries.
- **Script Kiddies :** Users who atack computer games are as often as possible expressed to as "script kiddies" in light of the fact that their impetus is seen as adolescent and they run an unassuming script to perform their DDoS assault.

- **Internal Testing :** A DDoS accident can be an aftereffect of an association's own particular exercises. It's either a shortcoming, or they're unequivocally trying their system quality to perceive the amount of data transmission it can hold.

Following are the reasons for having a DDoS attack:

- Powerless programming projects/Applications running on a machine or system.
- Open system setup.
- System/machine setup without considering security.
- No checking or DataAnalysis are being led.
- No normal Review/Programming redesigns being di- rected.

2. DDoS ATTACK CLASSIFICATION

On the basis of protocol vulnerability[2,3] the DDoS attacks are classified below:

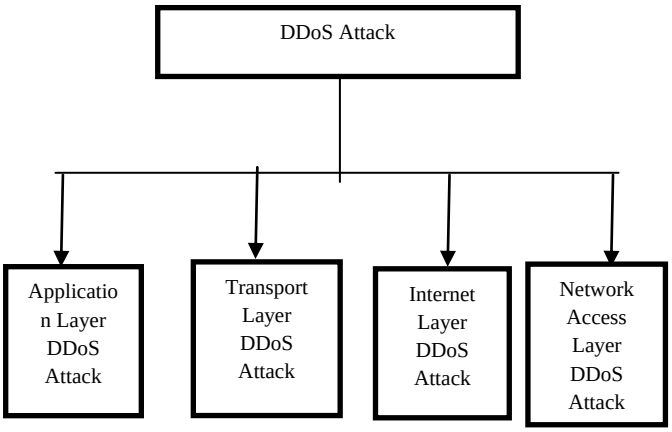

Fig 2: DDoS Classification

2.1 Transport Layer DDoS Attack

These sorts of assaults contains volumetric attacks that overpowers the objective machine, dismissing or devouring assets until the server goes disconnected from the net. In these sorts of DDoS attacks, malicious activity (TCP/UDP) is utilized to surge the victim.The real classifications of DDoS assaults under transport layer are following :

2.1.1 SYN Attack

It is a strategy for foreswearing of- administration assault in which an attacker sends a chain of SYN solicitations to an objective's framework with an end goal to eat enough server assets to make the framework uncaring to true traffic.

2.1.2 UDP Flooding

The assailant sends UDP packets, ordi- narily huge ones, to single destination or to subjective ports.It is degrading in nature.

2.1.3 TCP Invalid Flooding

In this sort of attack,packets that have the no TCP section banners set (six conceivable) are sent by the attacker. This kind of fragment might be utilized as a part of port scanning.It is for the most part debasing in nature.Following are the six TCP banners :

- URG (U) demonstrates that the urgent pointer field is critical.
- ACK (A) demonstrates that the acknowledgement field is essential.
- PSH (P) Push capacity.
- RST (R) Reset the association .
- SYN (S) Synchronize grouping numbers.
- FIN (F) No more information from sender.

2.1.4 RST/FIN Flooding

The RST or FIN DDoS assault depletes a victim's firewalls and/or servers by debilitating its framework assets and match the approaching packets with current session.

2.2 Internet Layer DDoS Attacks

These kind of assaults happens because of shortcomings in conventions of the TCP/IP model.They are:

2.2.1 Smurf Attack

In this attack,large quantities ofInternet Control Message Protocol (ICMP) packets with the arranged victim's feigned source IP are telecast to a PC system with an IP broadcast address.This assault is disgrading in nature.

2.2.2 Fraggle Attack

It is like smurf attack but instead of ICMP packets,large quantities of UDP packets with the pur- posed victim's tricked source IP are telecast to a PC system utilizing an IP broadcast address.This assault is degrading in nature.

2.2.3 TearDrop Attack

In this attack divided packets are sent to an objective machine. Since the machine getting such bundles is not ready to reassemble them because of a defect in TCP/IP model, the packets interposes each other, smashing the objective system device.This assault is degrading in nature.

2.2.4 ICMP Flooding

Aggressor floods the victim utilizing ICMP echo request (ping) packets.The assailant trusts that the victim will answer with ICMP echo reply bundles, in this way overpowering both active data transmission and transfer speed. In the event that the objective framework is relaxed,casual CPU cycles can be spent and a noteworthy log jam is seen by the user.This assault is degrading in nature.

2.3 Network Access Layer DDoS Attack

These sort of assaults endeavor the shortcoming of network layer and its protocols.Following are the real sorts of DDoS assaults that falls under this classification:

2.3.1 VLAN Hopping

VLAN hopping is a procedure of assaulting organized assets on a Virtual LAN (VLAN). It deeds the assets of a VLAN.This attack is disruptive in nature.

2.3.2 MAC Flood

During MAC flooding, the security of system switches is compromised.The attacker is associated with a switch port and surges the switch interface with a colossal number of Ethernet frames with particular false source MAC address.

2.3.3 DHCP Attack

Assailant prevent host from accessing the system by discrediting them an IP address by devouring the majority of

the available IP address in the DHCP Pool.This attack is disruptive in nature.

2.3.4 ARP Attack

ARP spoofing is a sort of attack in which a malicious attacker sends misrepresented ARP (Address De- termination Convention) messages over a LAN. This assault is degrading in nature.

2.4 Application Layer DDoS Attacks

An application layer DDoS attack is arranged basically for particular target purposes, including transactions disturbance and databases access. They require a couple of assets and frequently supplement network layer attacks.An assault is hidden to look like legitimate activity, with the exception of it targets specific application packets[3,5]The attack on the application layer can disturb administrations, for example, data recovery or hunt capacity and in addition web program capacity, email administrations and photograph applications.

2.4.1 HTTP/HTTPS Flooding:

HTTP food is a kind of DDoS attack in which the aggressor exploits apparently-legal HTTP GET or POST requests to assault a web server or applica- tion. HTTP surge assaults are volumetric in nature and uses botnets.HTTP surges don't use mutilated packets, spoofing or replication procedures, and needs less data transmission than different assaults to cut down the focused website or server.

2.4.2 FTP Flooding:

In this sort of attack,the attacker misuses apparently legitimate FTP requests to assault a FTP server or application.This assault is degrading in nature.

2.4.3 Telnet DDoS:

In this sort of attack,the attacker goes into the casualty framework by signing in remotely and performs the attack.This assault is degrading in nature.

2.4.4 Mail Bombs:

Attacker sends a huge amount of email to a specific individual or framework. Huge measure of sends may essentially top off the receiver's space on the server.This assault is debasing in nature.

2.4.5 SQL Slammer:

It is a kind of a computer worm that causes a denial of service on some web host and profoundly backs off general internet activity.

2.4.6 DNS Flood:

DNS flood deplete server-side assets (e.g., memory or CPU) with a surge of UDP solicitations, created by scripts executing on different bargained botnet machines.

2.4.7 DNS Cache Poisoning:

DNS cache poisoning is a PC hacking atack, whereby information is infused into a DNS resolver's cache, influencing the name server to yield a mistaken IP address, turning away activity to the attacker's PC.

3. ADVANCED DDoS TOOL

This tool is used to launch DDoS attack for Internal testing so that an organisation can perform vulnerability analysis and check whether the resources and network are safe or not.

Need Of Testing :

- Finding the vulnerabilities and exploiting them to deter- mine the risks.
- Finding Open ports that can be easily exploitable.
- Test our own Server for load testing and adjust ipta- bles/Firewall rules accordingly.

Functionality

This tool executes Application Layer HTTP DDoS attack on the victim machine. It consumes the following resources of the victim:

1. Memory
2. CPU Availability
3. Buffer Space
4. Process Count

3.1 Parameters

Advanced DDoS tool has better impact on the victim's re- sources.Following parameters are used to compare Advanced DDoS tool with existing tools:

- RAM
- CPU Utilization
- Buffer Space
- Process Count

3.2 Simulation Results

Attacker System : Network Of Kali Linux
Victim : Ubuntu Server

Table 1. Impact Of Advanced Ddos Tool On Various Parameters

Parameter	Before Attack	After Attack
Free RAM	3900 Mb	1500 Mb
CPU Utilization	70 percent	90 percent
Free Buffer Space	2700 Mb	2550 Mb
Process Count	360	840

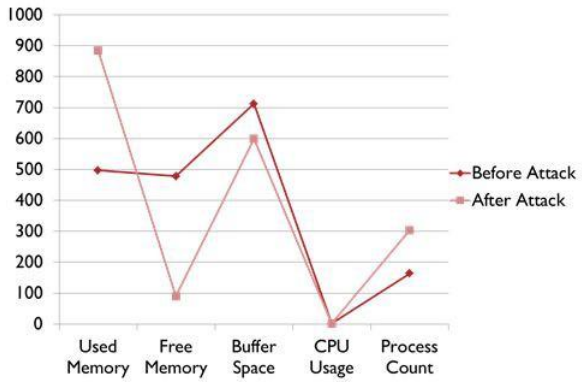

Fig 3: Advacned DDoS Tool Simulation Results

4. DDOS DEFENSE MECHANISMS

4.1 Ingress/Egress Filtering

Ingress filtering is a system used to set up a router which restrict inbound packets with unlawful source addresses into the network[4,10].It keeps away from source IP address spoofing of Web traffic.This strategy can impressively decrease the DoS assault by IP ridiculing if all domains use it.Egress filtering [4,10] is an outbound channel, which affirms that exclusive designated or allocated IP

address space leaves the system. Egress filters don't save asset exhaustion of the domain where the packet is started however it guards different spaces from plausible assaults.

4.2 Route-based distributed packet filtering

This strategy is used to filter a tremendous part of spoofed IP packets and preventing assault packets from achieving their objectives and to help in IP traceback[5] Route based filters utilizes route data to get out parodied IP packets dissimilar to ingress filtering. On the off chance that route based channels are reasonably deployed,a synergistic sieving impact is conceivable, so that ridiculed IP streams are banished from achieving different autonomous systems.

4.3 History-based IP filtering

This strategy empowers the edge router to filter the incoming packets as per a pre- manufactured IP address database. The IP address database is based on the edge router past association history[4,5,10] This technique is incredible, does not require the help of the entire Web people group, is suitable to a wide assortment of traffic types and needs straightforward configuration.

4.4 Load balancing

Load balancing is a strategy which empowers network providers to upsurge the given data trans- mission on serious connections and shield them from sepa- rating in the occurence of an assault. Besides, the reiteration of servers should be possible for safeguard security during a DDoS assault.[4,5].

4.5 Intrusion Detection

Intrusion detection systems recog- nize DDoS assaults either by utilizing the database of surely understood signatures or by distinguishing changes in system behaviors.[7,8]Anomaly recognition relies on recognizing activ- ities that are unusual as for some typical standard. Following are some anomaly identification systems and techniques have been set up to identify the indistinct indications of DDoS attacks:

Signature-based, otherwise called administer or rule based , distinguishes an assault by relating surely understood assault marks, or patterns, with the observed traffic. A match flags a caution for a conceivable assault. This systems has following advantages:

- Quick detection time.
- Identifies most surely understood assaults.
- Less false positive rate, i.e., it doesn't creates a caution for lawful traffic.

The typical traffic behaviour is ordered into two sorts : standard and trained. The standard depends on standard conventions and guidelines like how the assailant could dispatch a half connection assault during TCP handshaking. The trained traffic is used to discover a limit esteem for future disclosure.[8,10]

4.6 Deflection

It incorporates the accompanying methods:

- Honeypots: They are the traps that shouldn't acknowl- edge any legitimate traffic. Traffic expected to a honeypot is conceivably a continuous assault that can be investi- gated to uncover vulnerabilities targeted by attackers.[9,10]
- Attack Study:Honeypots contains exceptional software which over and again accumulates information about the system activities for criminological study. Honeypots are allowed to be bargained and act as a typical machine, mutely catching essential data about the activities of aggressor.
- Roaming Honeypots:Rather than using claasic honeypots,these can be introduced at administration level, where the areas of honeypots are imprudently changing inside a pool of back-end servers.

5. HYBRID DEFENSE MECHANISM USING IDS AND FIREWALL

It is difficult to totally protect a DDoS assault however it can be restricted by utilizing appropriate safeguard techniques.DDOS can be averted to a specific degree, if host and system are safe.Following measures can be taken to prevent a DDoS assault:

5.1 Machine Load Detection and HTTP Process Count

Initial step is to check whether the machine's load is high and to see whether gigantic number of HTTP processes are executing.

5.1.1 Machine Load Detection

The normal machine burden can be found by using the "w" command on the target linux framework.

For Example : Command :root@work : w

Output :12:00:36 up 1 day, 20:27, 7 users, load average:

0.73, 0.75, 0.52

5.1.2 HTTP Proces Count :

To find if there is large number of HTTP process running ,following command can be used on victim linux system. " ps -aux |grepHTTP| wc -l ".

5.1.3 Machine Load Reduction:

To ease the load on the machine,number of connections are determined. Let the machine load be LT and number of connections to the host machine be CT at time T . If LT > 5 and CT > 30 from a single IP then it is a clear sign of DDoS attack. Block that ips/networks using iptables /apf using the below command :

iptables -A INPUT -s < SourceIP > -j DROP

This process will be reiterated untill all the load on the victim machine gets reduced.

5.1.4 Firewall Setup for Ingress and Egress Filtering at Gateway:

Advanced Policy Firewall(APF) can be installed and arranged on the victim machine.After the firewall is installed,it can be configured using conf.apf which is located at /etc/apf/conf.apf AntiDOS mode is then enabled in conf.apf Firewall can be installed using the following commands :

bash# tar -zxf apf-current.tar.gz

bash# cd apf-< versionnumber >

bash# ./install.sh

5.1.5 Conducting regular Audits on each host on the network to find installation of DDOS tools / Vulnerable applications:

Utilities like RKDET,RKHUNTER and CHKROOTKIT are used to discover if any rootkit has been as of now introduced and to identify the affected binaries in the machine, if any.The review check list commands can be used to give a list of Check for open email transfers.

- Check for malignant cron sections.
- Check/dev/tmp/var registries.
- Check whether reinforcements are kept up.
- Check for undesirable clients, groups, etc on the system.
- Check for and disable any unneeded administrations.
- Find vindictive scripts.
- Querylog in DNS.
- Check for the suid scripts and nouser scripts.
- Check valid scripts in /tmp.
- Use intrusion detection tools.
- Check the system performance.
- Check memory performance (run memtest).

6. CONCLUSION AND FUTURE WORK

Internet has reached such places where individuals couldn't considerably ponder that such sort of network exists which give any potentially possible information.With the intensified utilization of web, an immense number of assailants are keeping an eye to dispatch assaults to access basic data. There are systems whose vulnerabilities can be effectively exploited by the aggressors and they utilize them to execute DDoS attacks.DDoS attacks ordered by in the TCP/IP protocol and their effect on vic- tim's assets is researched in this paper.A different DDoS script is executed and its impact on various parameters are examined.DDoS assaults are hard to evacuate totally yet they can be prevented.A new hybrid DDoS defense mechanism to avert DDoS assault is exhibited.

7. REFERENCES

[1] Christos Douligeris,Aikaterini Mitrokotsa. 2003 DDoS attacks and defense mechanisms: classification and state-of-the-art Signal Processing and Information Technology 3rd IEEE International Conference,pp-190-193.

[2] Khan Zeb, Owais Baig, Muhammad Kamran Asif 2015 DDOS Attacks and Countermeasures in Cyber SpaceWeb Applications and Networking (WSWAN), 2015 2nd World Conference IEEE,pp-1-6.

[3] Bharti Nagpal,Pratima Sharma,Naresh Chauhan,Angel Panesar. 2015 DDoS Tools: Classification, Analysis and Comparison, Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference IEEE ,pp. 342-346.

[4] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[5] Udaya Kiran Tupakula ,Vijay Varadharajan, Srini Rao Pandalaneni. 2009 DoSTRACK: a system for defending against DoS attacks, ACM Digital Library, pp. 47-53, ISBN: 978-1-60558-166-8.

[6] Mohammed Alenezi, Martin J Reed.2012 Methodologies for detecting DoS/DDoS attacks against network servers, IEEE Journal Of Computing,Volume 45,Issue 1,pp. 1-10

[7] Abdulaziz Aborujilah,Shahrulniza Musa. 2014 Detecting TCP SYN based Flooding Attacks by Analyzing CPU and Network Resources Performance, IEEE Journal Of Computer Security ,Volume 16 ,Issue 3,pp. 3-10.

[8] Vyas Sekar ,Ravishankar Krishnaswamy, Anupam Gupta, Michael K. Reiter. 2010 "Network-wide deployment of intrusion detection and prevention systems", ACM Digital Library, ISBN: 978-1-4503-0448-1

[9] Iyatiti Mokube, Michele Adams. 2005 Honeypots: concepts, approaches, and challenges, ACM Digital Library, ISBN: 978-1-59593-629-5.

[10] Archana S. Pimpalkar ,A. R. Bhagat Patil 2015 Detection and defense mechanisms against DDoS attacks: A review, IEEE Conference , ISBN: 978-1-4799-6818-3.