Review Article

A Survey of Distributed denial of service attack

Abstract:
Now a day we are all completely dependent on internet for all sources. We are all sharing very sensitive information through internet. Therefore availability of internet and speed of the internet is most important. In current trend internet plays main role in our part of life. Distributed computing increasing dramatically in size, functionality and complexity. It is integral part of our life. In distributed computing affect lot of vulnerabilities such as DOS (Denial of Service attack), DDOS (Distributed Denial of Service attack), Viruses and Worms etc. DOS constitute one of the major threads and among the hardest security problem in today's Internet Environment. Of particular concern are Distributed denial of service attack is one of the most important attack in this cyber world, whose impact can be proportionally severe. It will also creating financial losses in business sectors. Distributed denial of service attack obstructs network availability and overwhelm targeted device with illegal traffic. In this paper mainly discussed on various type of DDOS attacks, Symptoms of DDOS attack, role of botnet on DDOS attack and give some mitigation and prevention technique for DDOS attack.

Key words
DDOS attack, illegal traffic, Overwhelming, Botnet.

1. Introduction

Today volumes of users are increasing in Internet world. Internet applications are also increasing day by day. Computer networks are subject to an unprecedented number and variety of attack like the majority of which are DDOS attack. DDOS attacks are everyday occurrences whether small company or huge multinational company. Online services, websites, everything that faces internet. It can be slowed or completely stopped by a DDOS attack. DDOS attacks are distracted cyber security operations and other criminal activity. The first half of the year 2021 found massive ransomware and ransom DDOS attack that interrupted critical infrastructure around the world and it also targeted schools, public sectors, travel organization and many biggest fields in the world. Second half of the year recorded one of the most powerful botnets**Meris** and record breaking HTTP DDOS attacks and Network Layer attacks observed over thecloud flare [1].Ransom DDOS attack is explain in Figure-1.

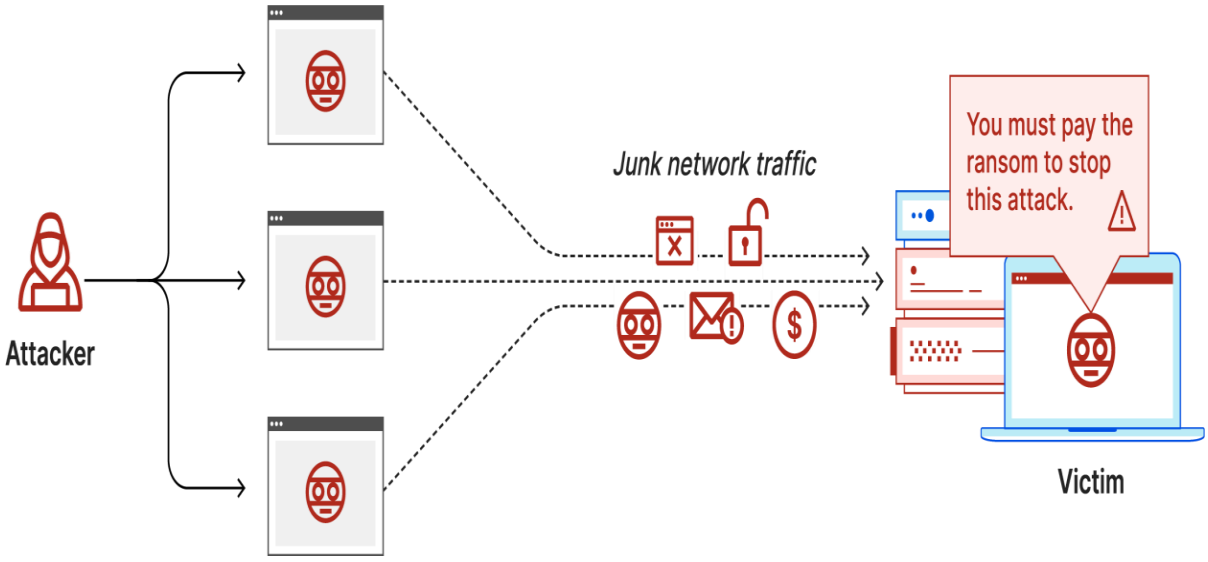

Figure 1: Ransom DDOS attack

In Q4 ransom DDOS attack increased by 29% YoY and 175% QoQ In this attack Hackers are always finding new ideas to attacking servers that ideas are more effective and most powerful.

Recently some attacks are targeting the financial sector. An attacker encrypts data and demands money such as Bitcoin for the return of data, or system access and so on. It is called ransom DDOS attack. This attack reached a rate of 2.5 million requests per second. Figure-2 illustrate that the DDOS attack has double from 2018 to 2023.

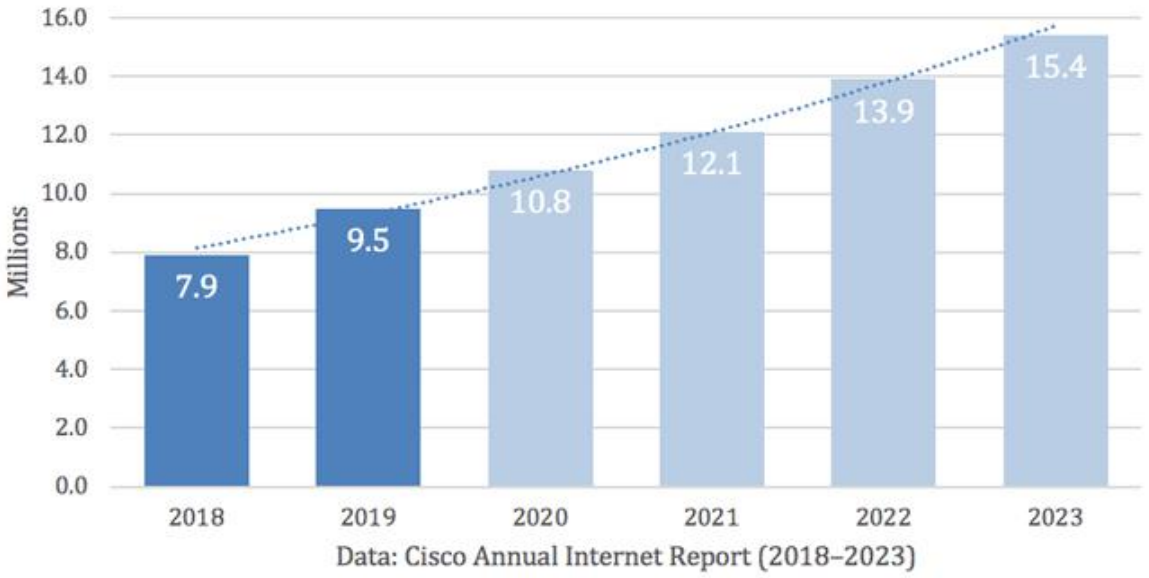

Figure 2: DDOS attack Annual report

The paper is organised as follows Introduction of DDOS attack is given Section 1. Section 2 Presents Literature survey. Explanation of botnet in DDOS attack is Section 3. Illustrate DDOS attack and its Types in Section 4. Some common methods for mitigation and prevention are Section 5. Finally, this paper is concluded is Section 6.

2. Literature Survey

Zsolt Bederna. Tamas Szadeczky [3] analyse what is the bot and botnet and role of botnet in DDOS attack and it said detail about the application of botnet and explain detailed in lifecycle of botnet. Here also author discuss important malware VPN filter and also detail description about the APT28 group.

In [4] explained detail about the DDOS attack and its types and also reviewed How to DDOS attack espionage cloud environment and how to mitigating and prevent the DDOS attack in cloud environment. In this paper author proposed solution for **multistage zonal classification architecture** identifying, mitigating and prevent the slow rate HTTP DDOS attack.

Priyanka Verma et.al [5] in this proposal focus on reducing VM level collateral damages and to obtain the request awareness a novel cuckoo search based Identification of request method. CS_IDR method helps request aware decision, which eventually reduces VM level collateral damages.

Aqeel sahi et.al [7] analyse in this paper proposed new classification system for detecting and preventing DDOS TCP flood attacks. Proposed CD_DDOS SYSTEM offers a solution classifying incoming packet and making decision based classification result. In this system having two phases detection phase CS_DDOS identifies packet are normal or originate from the attacker. Then next prevention phase in this phase packet classified as malicious, that IP address will be blacklisted.

3. Botnet

Botnets have one of the most common methods of malware deployment for the past decade. Hackers may use botnets to send spam messages, phishing or other trick for earning money. They can also collected the information from infected machine.

Bot which is a short form of robot. Attacker take a one computer in infected computer system, making it as DDOS master. A computer or network device under the control of intruder it is called as **Zombie.** It's another name is **bot.** The attack creates **Command and Control Server(C&C). Telnet** botnets use simple command and control botnet. Collection of bots called **Botnet.** The person control all bot is called **botmaster.** Botnet composed many number of bots. Botnets increasingly common tens or hundreds of thousands of its needs. There is no upper limits of bots [3].

Lifecycle of a botnet

A botnet can be maintained in five phases including:

I. **Initial infection:** The botmaster scan target machine for known vulnerability and starts to infect using different exploitation methods.

II. **Secondary injection:** After successful infection the infected node executed script. That script is called shell code. Shell code fetches the image from actual bot binary from specific location FTP, HTTP. The bot binary install itself. Once the bot program is installed that machine is called Zombie machine that runs malicious code.

III. **Connection:** Each bot machine connects to the command and control Server.

IV. **Malicious Command and Control:** After the connection phase the botnet Command Control phase are started. The bot master uses a C&C channels to spread

Command to his bots army. The bot programs are received and execute commands send by bot master.

V. **Update and Maintenance:** Last phase is update and maintenance. In this phase bots are commanded to downloaded and update binary. Figure 3 clearly explain the architecture of botnet.[3]

Botnet Architecture

The botnet architecture is based on Client Server approach. It involves a C&C server that is centralised control over the bot. Botnet architecture have a three types, that are

Centralised (or Hierarchical): This type of botnet control a bots in static nature. Here nature means predefined number of C&C server with predefined reachability. Here bots get an information using push and pull technolog Gy. Pull technology means bot initiate request to server. Push technology means server start update request to client.

Decentralised (or Peer to Peer): Here no specific C&C servers. So such a botnet working Peer to peer mode. In this method each bots register the number of bots available in this surrounding and continuously observe any new bots are detected.

Hybrid botnet: Hybrid bot unify the advantages of centralised and decentralised botnets. The mixed architecture means C&C servers have a structure of decentralised networks and bots are connected to C&C server way of typical client server model. The botnet architechture is explain in Figure 3.

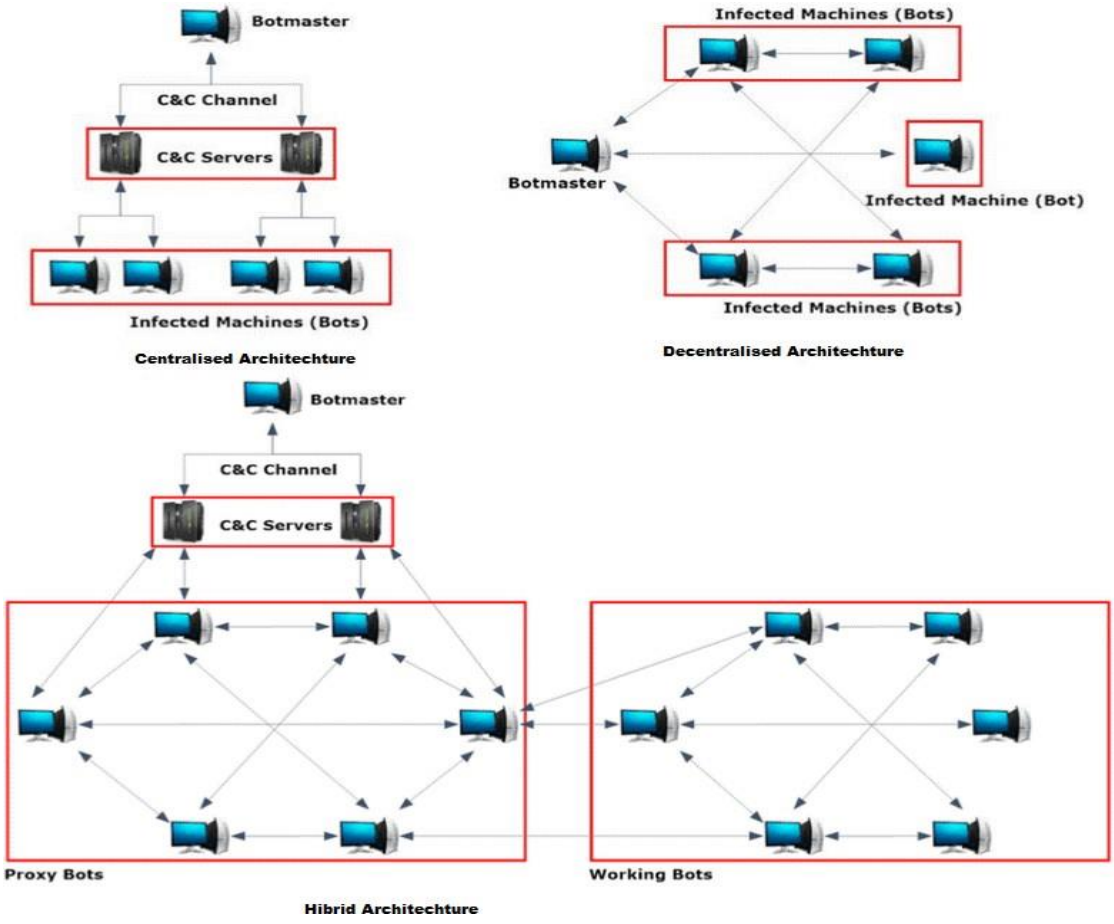

Figure 3: Botnet Architecture

Application of Botnet

Crimeware as a Service: It is used for identification of vulnerabilities and to create an exploit specifically for them. Main tools are available for this service that's are APT (Advanced Persistence Threads), rootkits and randsoware as well as dropers, keyloggers, and hiding tools.

Cybercrime infrastructure as a Service: It makes infrastructure elements (clients and Server available). Clients used to various attacks.

Hacking as a Service: This service is a service **model** for whole attacking process. The "Service Provider" performs attacks as clients and demand to specific service or process information.

4. DDOS attack

An attack originates from single source that is called DOS Attack. However common today **DDOS attack**s are originate from multiple source. Attacker creating a fake malicious traffic and send it to target Server website or other resource. Its main aim is force a targeted system to slow down or crash. The DDOS attack architecture is presented in Figure-4.

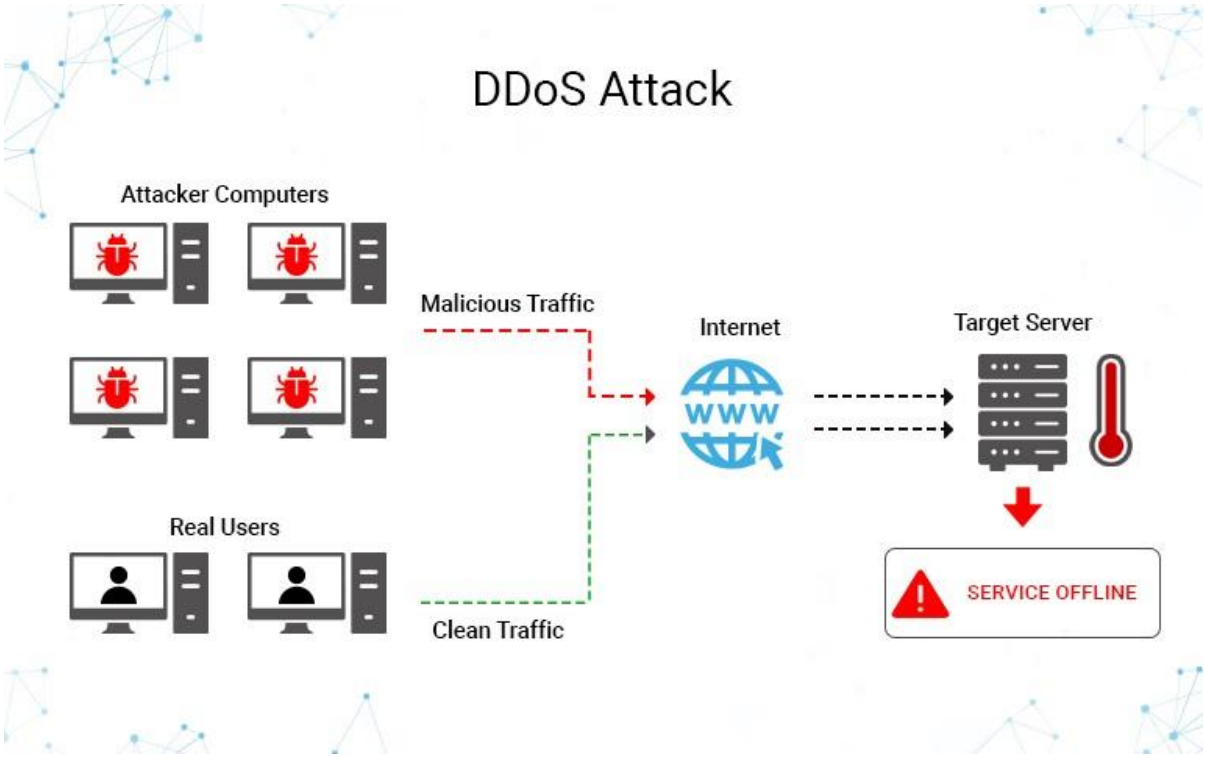

Figure 4: DDOS attack

Types of DDOS attacks

DDOS attacks come in a variety of flavours. Broadly speaking, they are classified based on the type and quantity of traffic used for the attack and the exploited vulnerability of the target. DDOS attack classified into three categories:

- Volume based DDOS attack
- Protocol based attack
- Application Layer based attack

Volume based DDOS attack

Volumetric DDOS attacks are sends high volume of traffic, request packets to target server device this attack creating flood and slowdown or stopping their services. Different types of volume based attack see in next.

Different Types of Volumetric attack

a. UDP flood

UDP flood is a type of DDOS attack it send large number of user datagram protocol packets to a targeted server. It's main aim overwhelming the device ability and respond.

UDP is a networking protocol that is connectionless and session less protocol. UDP traffic does not have a three way handshaking. It require less overhead so it is perfectly suitable for creating flood. UDP flood attacks take the form of DNS amplification attacks, also called **Alphabet soup attack. UDP** attack does not have a specified packet format. Attackers create large packets (sometime over 8KB), fill with text or numbers. In UDP flood attack the following process occurs:

1. An attacker sends UDP packets with spoofed IP address.
2. System side following procedure repeated for incoming packet.
   a. Check the port specified in UDP packet for listening application; it is a randomly selected port so it is generally not in case.
   b. Send an ICMP destination unreachable packet to sender since IP address has been spoofed these packets are usually received by some random bystander. Figure-5 illustrates UDP flood DDOS attack.

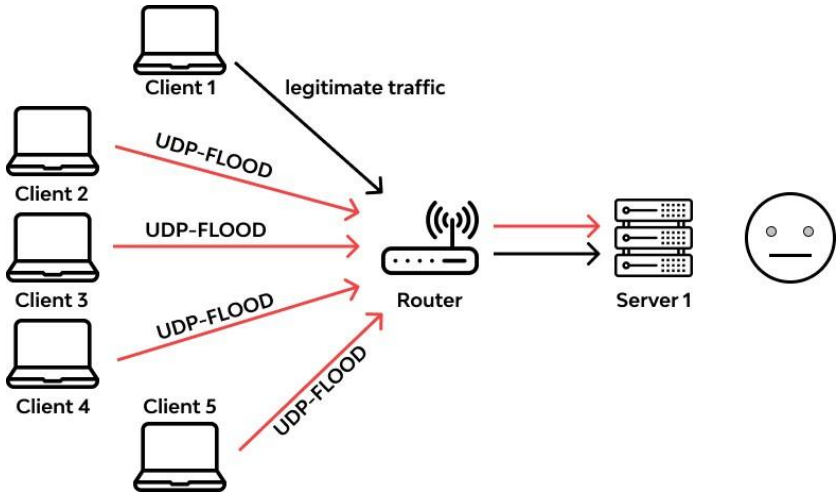

Figure 5: UDP flood attack

b. ICMP flood

An ICMP flood DDOS attack is also called as ping flood attack. It sent large number of ICMP echo request (pings) to target server using devices the victim machine start to reply using ICMP echo reply packet. Now targeted machine takes twice the bandwidth was once for receiving the packets another one is respond replies. So victim machine get flooded network

traffic. So CPU wants large number of CPU cycles many be going to shut down.

Signs of ICMP flood DDOS attack

In ICMP flood attack attacker know IP address of the target Machine. Attacks can be separated in to three categories that are given below:

I. **Target local disclosed**: In this type of DDOS attack ping flood target specific machine on the local network. In this attack attacker must know the IP address of the destination before head.

II. **Router disclosed:** In this type of DDOS attack targets the routers. This main objective is interrupting the communication between the computer networks. In this type of attack attacker must know before the targeted IP address.

III. **Blind ping:** This type of attack involves using external command to reveal the IP address of the target computer or router before launching the attack. ICMP flood DDOS attack clearly explains in Figure-6.

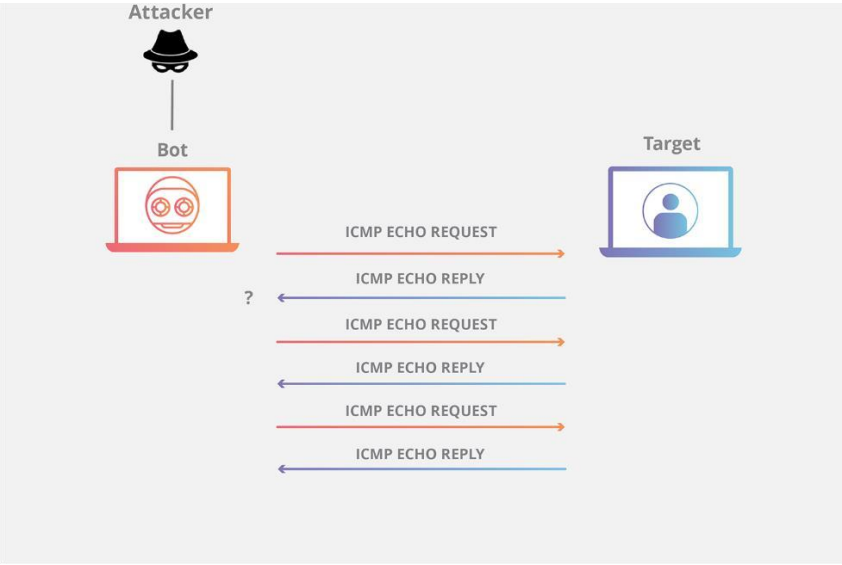

Figure 6: ICMP flood

c. Spoofed packet

Spoofing is that act of camouflage a communication from a unknown source being from a trusted source. Spoofing can apply phone calls and websites and emails and can be more technical that are DNS server spoofing, ARP spoofing, IP address Spoofing

DNS server spoofing: Modifies DNS server and redirect a domain name to different IP address. It is also used for spread viruses. Figure-7 explains detail in DNS server spoofing.

ARP spoofing: It will be link a perpetrators MAC address to legitimate IP address through spoofed ARP message. It will be mainly used for man in the middle and denial of service attack.

IP address spoofing: Disguises an attacker's original IP address.

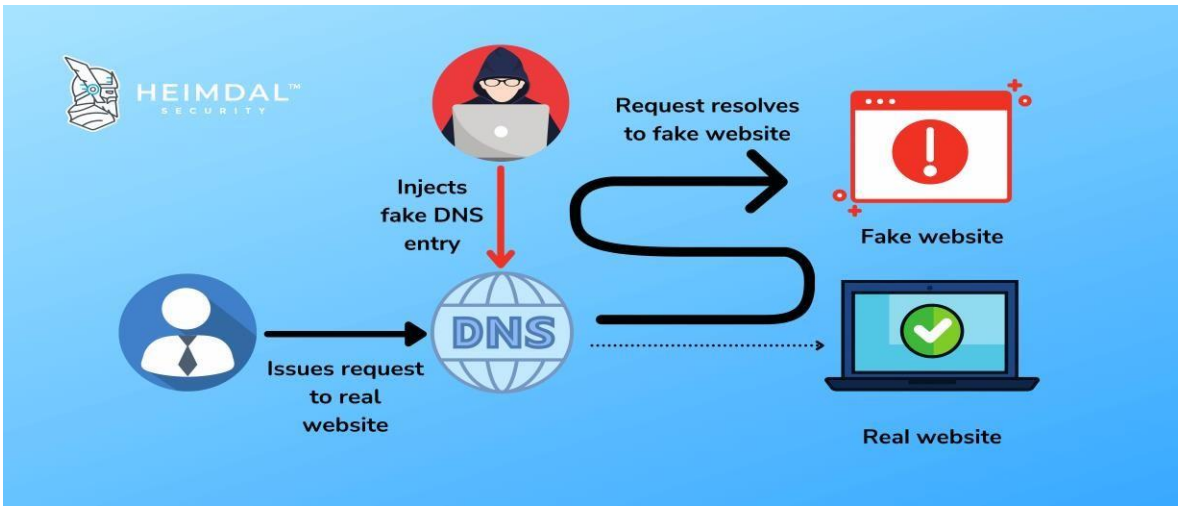

Figure 7: DNS Spoofing

d. Reflection amplification DDOS attack

Reflector is a server. It was reachable from Internet. It will offers service to client (DNS, NTP, SNMP, gaming) attackers launch a DDOS flooding attack it sends a legitimate request to server the network traffic contain spoofed source IP Address of victim.

IP spoofing performed two reasons. First it hides identity of attacker sound query response send from reflector to victim. Significantly larger than original query request. For example DDOS amplification attack contains many IP address. It makes response asymmetrical terms of consumed bandwidth.

With the botnet command and control server instruct thousands and thousands of bots to send request number of reflect in parallel. It will increase attack traffic and to increasing volume of attack. Figure-8 illustrates the Reflection and Amplification Attack.

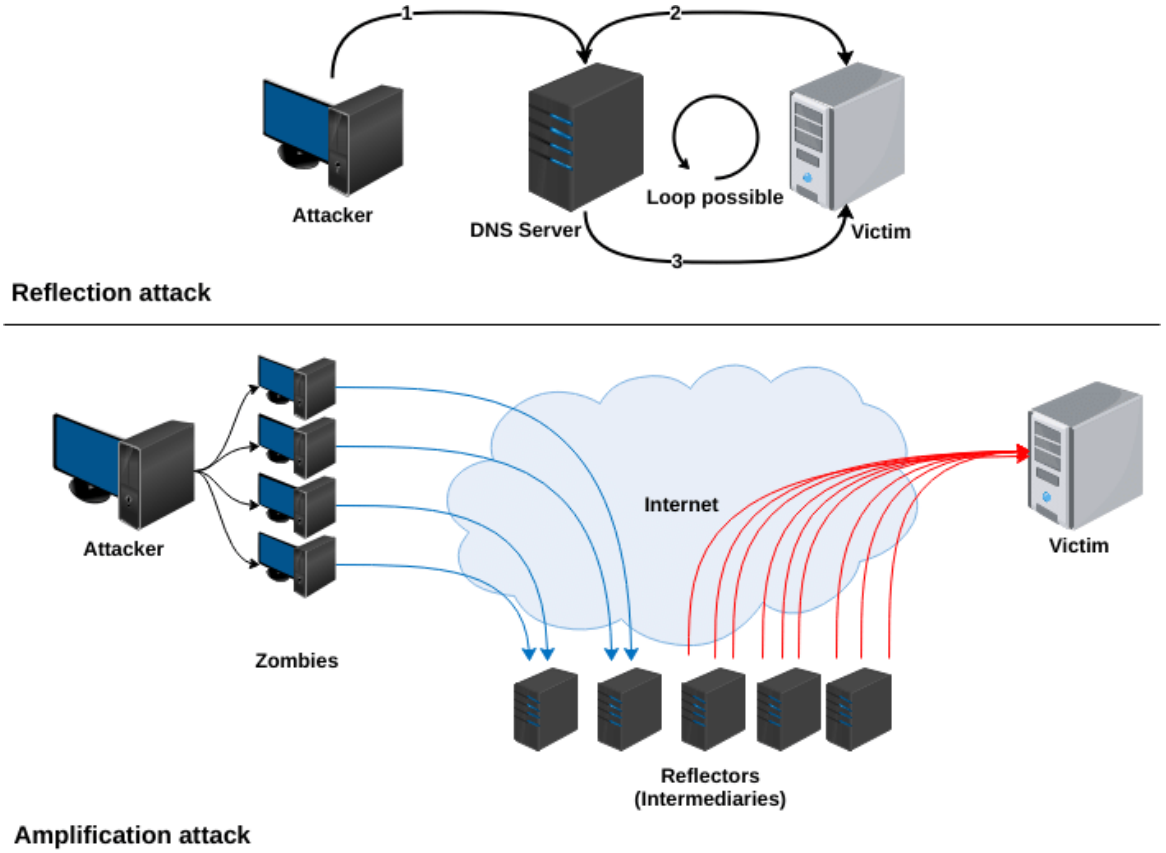

Figure 8: Reflection and Amplification Attack

e. IP/ICMP fragmentation

IP fragmentation IP datagrams are fragmented into small packets, then that will be transmitted throw the network and finally it will be re assembled into original datagram in normal communication.

This process have a size limits for each network can handle. That limit is described as maximum transmission unit (MTU).When a packet is too large that will be sliced into small packets and transmitted successfully. One which contain all information about ports, length, etc. This is the initial fragmentation.

Attacker sends IP/ICMP based fragmentation attacks typically submitted fake fragmented. It takes more memory resource. So server become completely overwhelmed and ultimately. Figure-9 illustrates the ICMP fragmentation.

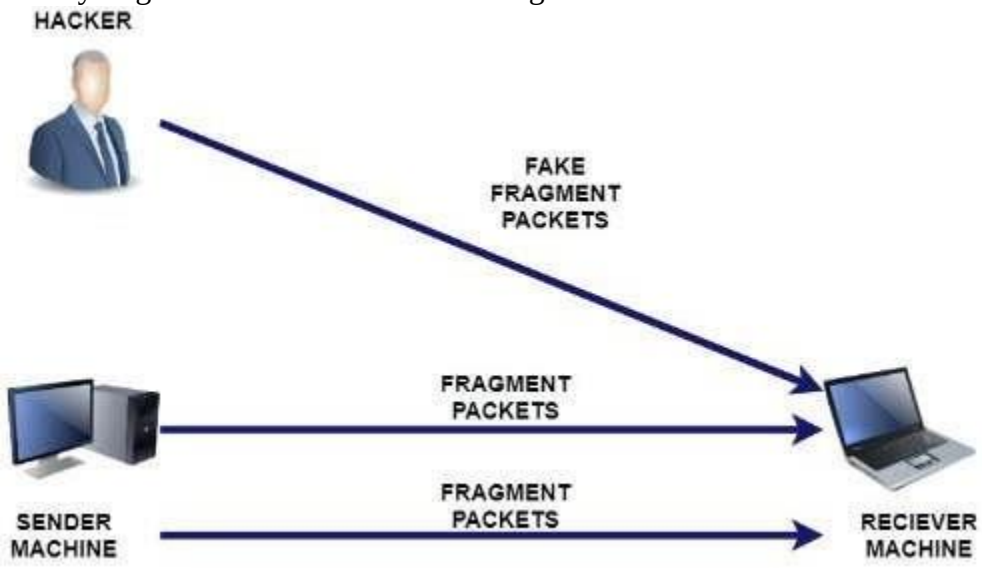

Figure 9: ICMP fragmentation

Protocol based attack

Protocol attack also known as state execution attacks. It cause a service disruption by over consuming server resources and network equipment like firewalls and load balance. It will be utilize weakness load balancers layer3 and layer 4 protocol stack to render target in accessible. It has many type of attacks that are briefed in the following sections.

a. SYN flood attack

SYN flood attack also called as TCP flood attack it's another one name is half open attack. This type of attack sending large number of SYN packets to the targeted server from spoofed IP address. The server responding to each one of connection request and leaves a open port for receiving the response.

The server waits for final acknowledgement packet but it will not arrives. Instead the attacker sending new SYN packet. Because of this reason the server temporarily maintain network port connection for certain time. All the ports are used the server does not function normally. The networking when a server connection is open but another side is not. It is called half open connection. In this type of DDO`S attack targeted server is continuously leaving for open connection and waiting for each connection time out before port become again available this type of attack consider as half open attack. This process illustrates in Figure-10.

This SYN flood attack can attack two different ways that are

Direct attack: This type of SYN flood attack the IP address is not spoofed it is known as direct attack. The type of attack attacker does not mask their IP address for all time.

Spoofed attack: In this attack is created using botnet. It is spoofed IP address from which it sends. For examples **Mirai and Meris botnet.**

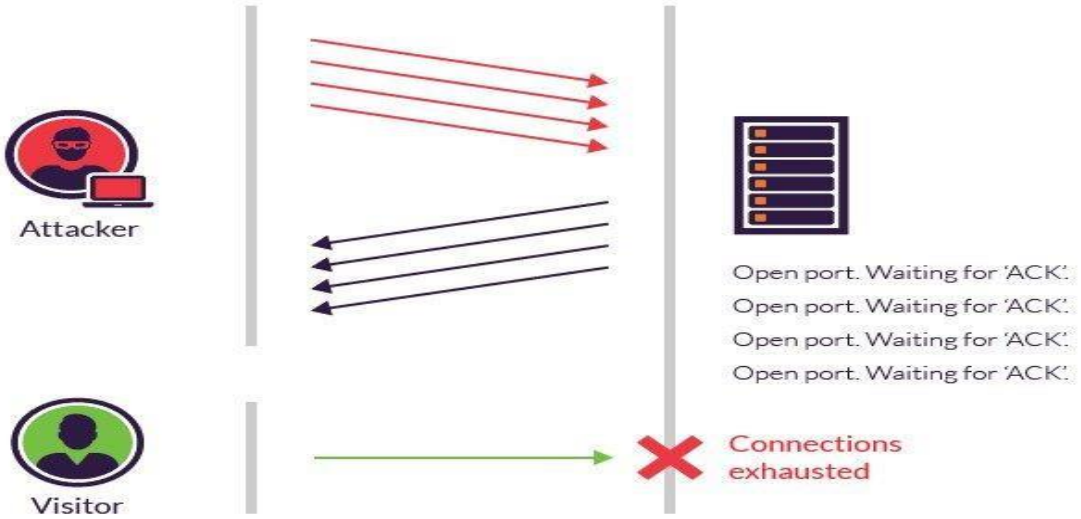

Figure 10: SYN flood attack

b. Ping of death

Attacker sends malformed or oversized packets using simple ping command. This type of attack attacker attempts to crash or freeze the targeted computer or server.

Ping of death is send deliberately IP packets larger than 65,536 bytes to targeted server. The ping of death attack also called teardrop attack this ping of death attack objectified ICMP and TCP and it is undermining of all ICMP attack.

It can also doing against different protocols like UDP. That is from 0 to 65,500 bytes of data in ICMP echo request packet. If we try to send data size above 64,500 that time ping command will show an error message.

IPV4 header is 16 bit field. The maximum possible value of 16 bit binary number is 65,535 sending an ICMP echo request packet larger than 65,535 bytes size in IPV4 datagram ping command memory overflow can happen. Also possible to target machine freeze or craze. Ping of death DDOS attacks explain detailed in Figure-11.

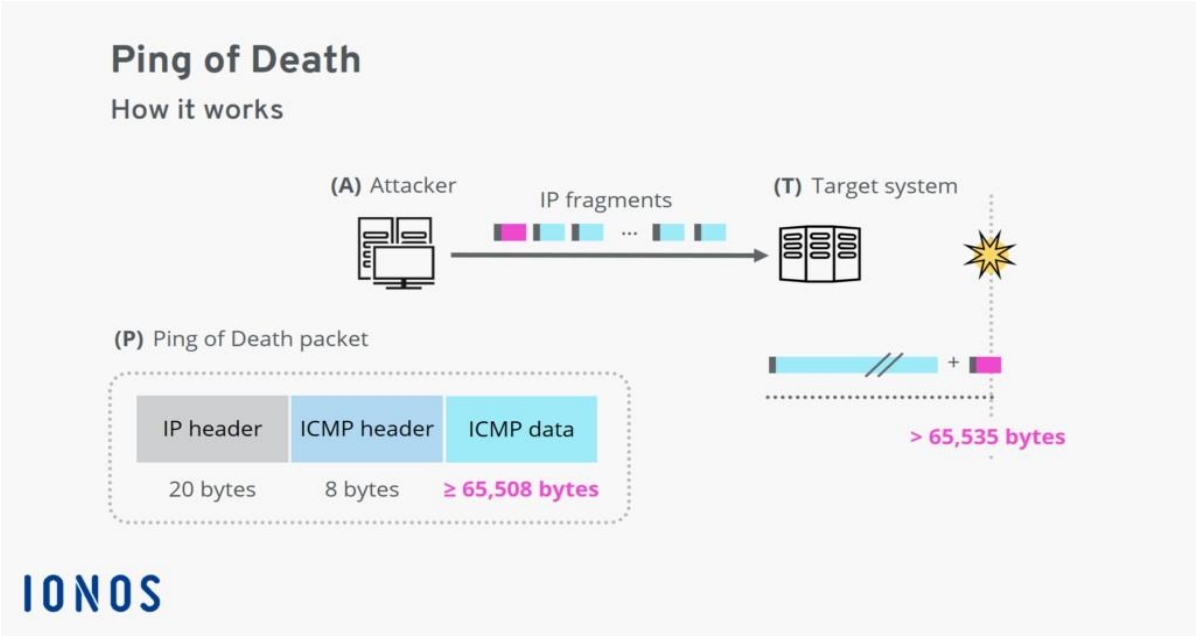

Figure 11: Ping of death attack

c. Smurf DDOS attack

Smurf attack are similar as ping flood attack as both are carried by sending ICMP echo request packets Smurf malware is used to fake malware, using spoofed source IP which is target server address.

In Smurf attack sending spoofed packet that attached to a false IP address that is called as **spoofing** that packets contain as ICMP ping message, which command network node sends reply. This process known as ICMP echo creates **infinite loop.** That overwhelms network with constant requests. Smurf DDOS attack is explained in Figure-12.

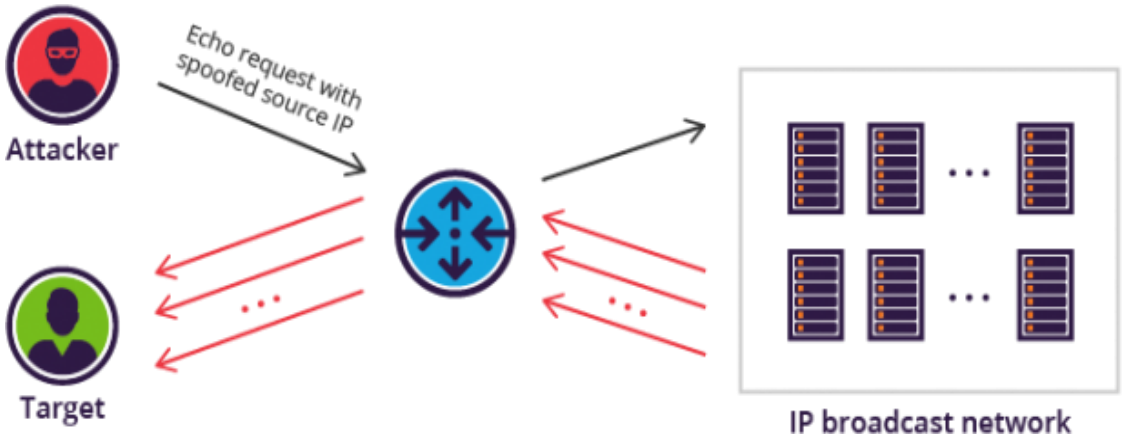

Figure 12: Smurf attack

Application layer attack

Application layer attacks called layer 7 attack. Manufacturing industry was most affected in Q421. It increasing 64% QoQ in the number of attacks. Business Services and gambling industries are second and third most affected industries. For the fourth time in this year China charts with heights percentage of attacks are coming from Application Layer attack. In the middle 2021 a new bot is recorded that name is called **Meris** bot net. Meris botnet attacking a server for **17.5 Million request per second** [1]**.**

Initially this research was estimated only 30000 to 56000 bots but the estimated actualy to much higher 2, 20,000 bots are founded. In five year ago Mirai bot net was detected. It was infected hundreds of thousands of IOT devices but Meris was most powerful than Mirai. Later Mirai code was Leaked and found another version of Mirai that name is **Mobot**[1]**.**

a. Slowloris

Slowloris open multiple connections to the target web server and open as long as possible. It does sending partial HTTP request more of which completed. The server open more and more connections open. Slowloris send subsequent HTTP headers for each request but never completes the request the targeted server maximum concurrent connection is filled to the legitimate connection attempt are denied. The Figure-13 Illustrate the Slowloris attack.

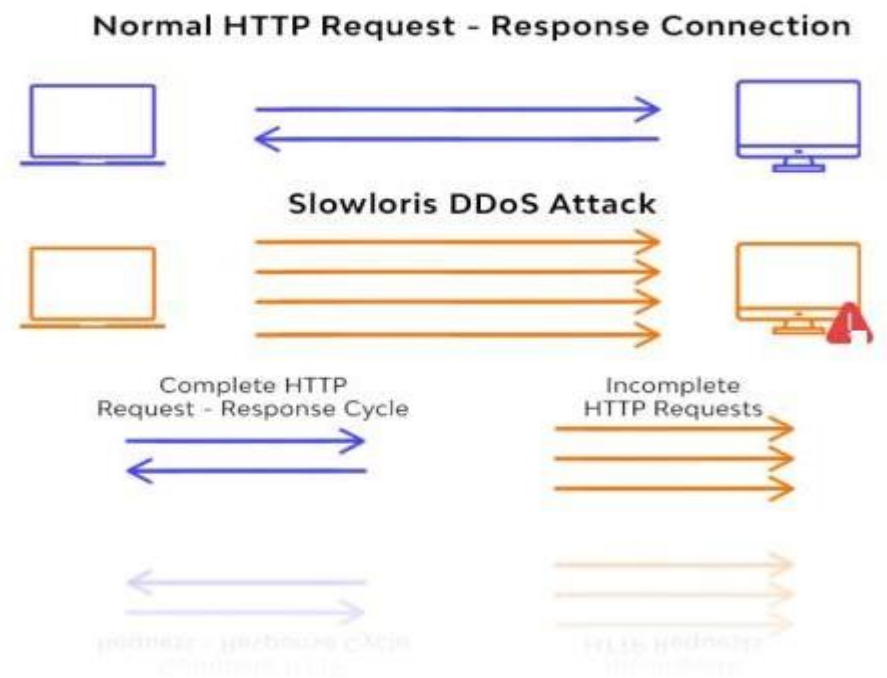

Figure 13: Slowloris attack

b. Zero day attack

When a user visits in a website can exploits security vulnerability in the web browser to infect system. Cyber criminals use social engineering for infect system. For example they may send phishing email with an attachment on clicking mail that time malicious code was executed and download malware in that and then infect it. The Figure-14 gives an idea of zero day attack.

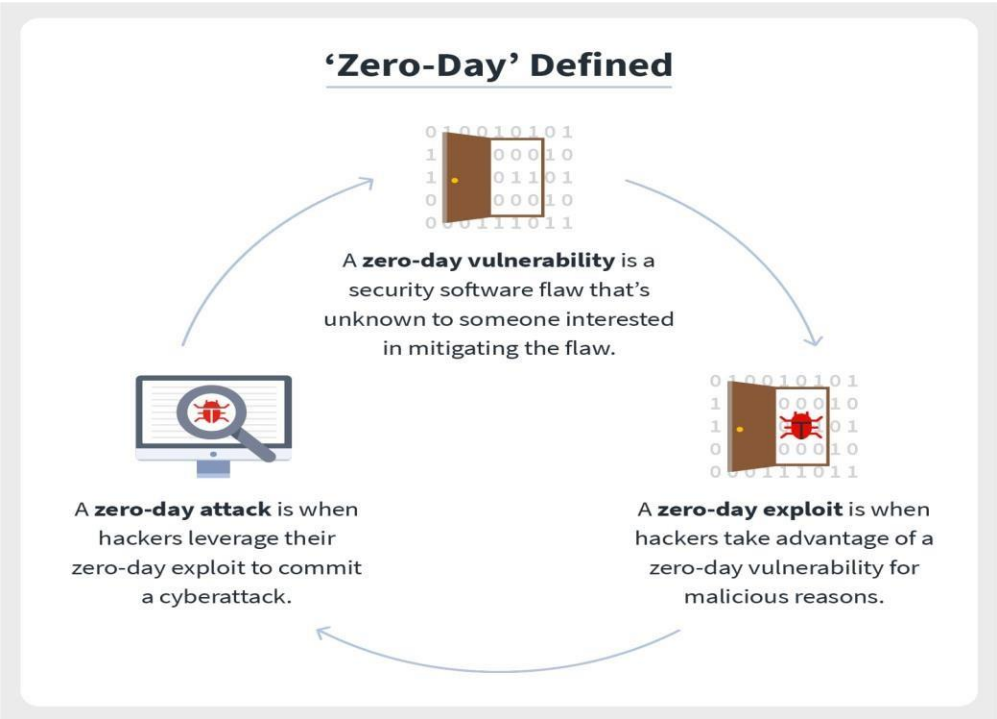

Figure 14: Zero day attack

5. Best methods for prevent DDOS attack

- Ensure high levels of Network Security
- Have Server Redundancy
- Look up for the warning signs
- Continuous Monitoring of network traffic
- Limit Network Broadcasting
- Leverage the cloud to prevent DDOS Attacks.
- Do not Overlook the DDOS thread

6. Effective tips for DDOS protection, Mitigation, and Defence

- Mitigate DDOS attacks with Multi layered, Multi module Defence
- Early detection and Traffic Monitoring are Critical
- Build a Resilient Infrastructure
- Get Real Time Intelligence and Act on Them
- Know the attack symptoms
- Good Cyber Hygiene is Indispensable
- Create a DDOS Response Plan
- Watch out for Secondary Attack

Software Defined Network, Cloud computing, Internet of things Devices, Wireless Sensor Networks, and Mobile Ad hoc Network these environments are largely affected for DDOS attack. Many techniques used for preventing and mitigating these attacks that's are Black hole filtering methods, Intrusion detection method, using some algorithms.

7. Conclusion:

Russia and Ukraine aggression war on going. In this time geo political tensions increased when the Ukraine defence ministry, the armed forces of Ukraine, some state backed banks MiroHost (a hosting provider) were hit by DDOS attacks. This attack will be lasted by one hour or two. According to Threatpost report no data was stolen or damaged but websites were disabling and banking applications could not be used in few hours. On mid-January 70 Ukrainian government were hacked. [1]

Detection, prevention and mitigation of DDOS attack is most important for National Security. The internet is an important component of communication infrastructure. In the same manner internet has become most user friendly over the last decade and more individual, businesses, and government agencies make use of it, hacking and disrupting network traffic. Attacking tools have become more sophisticated. And also very easiest to use. But one of the most important issues that will impact how defence against DDOS attacks. In this survey clearly explained what is DDOS attack? And type of DDOS attack and also give detailed explanation of mitigation and prevention of DDOS attack.

8. References:

1. Cloudflare statistic report https://blog.cloudflare.com/ddos-attack-trends-for-2022-q1/
2. Bederna.Z, Szadeczky.T. “Cyber espionage through Botnets”. Secur J 33, 43–62(2020). https://doi.org/10.1057/s41284-019-00194-6.
3. A.Dhandapal and P. Nithyanandham “The slow HTTP DDOS ATTACKS: Detection, mitigation and prevention in the cloud Environment” Scalable computing: Practice and experience Volume 20, Number 4, pp. 669-785.
4. Priyanka Verma, P., Tapaswi, S. & Godfrey, W.W. A request-aware module using CS-IDR to reduce VM level collateral damages caused by DDoS attacks in cloud environments. Cluster Comput 24, 1917–1933 (2021). doc: https://doi.org/10.1007/s10586-021-03234-2
5. K. Hussain, S. J. Hussain, N. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET," 2019 International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1-4, doi: 10.1109/ICCISci.2019.8716416.
6. A. Sahi, D. Lai, Y. Li and M. Diykh, "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment," in IEEE Access, vol. 5, pp. 6036-6048, 2017, doi: 10.1109/ACCESS.2017.2688460.
7. Subhi R. M. Zeebaree, Karwan Jacksi, Rizgar R. Zebari “Impact analysis of SYN flood DDOS attack on HAProxy and NLB cluster based web server”,Indonesian Journal of Electrical Engineering and Computer ScienceVol. 19, No. 1, July 2020, pp,510-517ISSN: 2502-4752
   doi: 10.11591/ijeecs.v19.il.pp510-517
8. Shivansh Kumar Ruhul Amin “Mitigating Distributed denial of service attack: Block chain and software defined networking based approach, network model with future research challenges”
   Wiley Publication. doi: 10.1002/spy2.163
9. Tasnuva Mahjabin, Yang Xiao, Guang Sun “A survey of distributed denial of service attack, prevention and mitigating techniques” International Journal of Distributed Sensor Network
   http://doi.org/10.1177/1550147717741463
10. Badr Alshery and William Allen “Proactive Approach for the Prevention of DDOS attacks in Cloud Computing Environments”Springer International publishing AG 2017R. Lee (ed.), Applied Computing and Informational Technology, doi:10.1007/978-3-319-51472-7_9
11. Mitko Bogdanoski,Tomislav Suminoski, Aleksandar Risteski “Analysis of the SYN Flood Dos Attack” International Journal of Computer Network and Information Security (IJCNIS) 5 (8), 1-11, 2013, doi:http://doi.org/10.5815/ijcnis.2013.08.01