Denial of Service Incident Response Playbook

Redback Operations

Version	Modified By	Approver	Date	Changes made
0.1	Pari		20 April 2024	Initial Draft
1.0	Pari	Joel Daniel	29 April 2024	Approved for Publishing.
2.0	Devika Sivakumar		30 July 2024	A comprehensive update has been conducted throughout the playbook. Several case studies have been added. A RACI chart has been included. The steps for monitoring threats are now included. New terminology has been introduced. The overall format of the playbook has been adjusted to align with other playbooks. The table has also been updated.

Table of Contents

1 Introduction

1.1 Overview

Denial of Service (DoS) assaults are a serious threat to the availability and integrity of online services in today's interconnected digital ecosystem. A denial-of-service (DoS) attack attempts to stop a system, network, or service from operating normally by flooding it with excessive amounts of unauthorized traffic or resource requests. These assaults have the potential to cause downtime, monetary losses, reputational harm, and even jeopardize the privacy of confidential data.

1.2 Purpose

This Denial of Service (DoS) Incident Response Playbook aims to offer a thorough structure for identifying, preparing, and responding to DoS attacks. This playbook tries to protect vital assets and services from disruptive cyber threats and reduce the effect of DoS incidents on our organization's operations by providing preventive measures, detection methods, response protocols, and recovery plans.

1.3 Attack Definition

An attempt to bring down a computer or network and prevent its intended users from using it is known as a Denial-of-Service (DoS) attack. DoS attacks achieve this by transmitting information that causes a crash or by overloading the target with traffic. The denial of serviceor resource to legitimate users, such as employees, members, or account holders, is the resultof a denial-of-service attack in both cases.

1.4 Scope

This playbook includes a thorough method for handling Denial of Service (DoS) attacks in the operating environment and infrastructure of our company. From pre-incident planning and detection to mitigation, recovery, and post-event review, it covers every stage of incident handling. The principles and processes described in this playbook can be applied to mitigate related threats, such as Distributed Denial of Service (DDoS) attacks, even if the primary focus of attack is DoS.

2 Attack Types

2.1 UDP Flood

Attackers using UDP floods make use of UDP's intrinsic simplicity—that is, its connectionless nature, in contrast to TCP. Attackers frequently target ports or services as they bombard the target system with a massive volume of UDP packets. When the target's network bandwidthis overloaded or its processing power is depleted by the flood of UDP packets, it stops responding to legitimate traffic. Because UDP does not ensure delivery or order, attackers canfake the IP addresses used to originate their attacks, making it challenging to identify their origins.

Case Study: GitHub DDoS Attack (2018)

Overview: The GitHub platform experienced the largest-ever recorded DDoS attack, leveraging Memcached servers to amplify the traffic directed at GitHub's systems. **Impact:** The attack peaked at 1.35 Tbps, causing temporary disruptions in service. **Response:** GitHub mitigated the attack using Akamai's DDoS protection services and increased network resilience.

2.2 TCP SYN Flood

TCP SYN Flood attacks exploit the Transmission Control Protocol's (TCP) three-way handshakeprotocol. TCP SYN packets are sent by attackers in enormous quantities; these packets form the initial stage of a TCP connection. They do not, however, send the last ACK packet to completethe handshake, which leaves the target system with a backlog of partially open connections. As a result, valid users are unable to connect to the server because the target's RAM and connection table entries are depleted.

Case Study: Mafiaboy DDoS Attack (2000)

Overview: A teenager known as Mafiaboy launched a series of DDoS attacks against major websites like Yahoo!, Amazon, and CNN, using TCP SYN floods.

Impact: The attacks caused significant disruptions and highlighted vulnerabilities in high-profile websites.

Response: The incidents led to increased awareness and improvements in DDoS mitigation strategies.

2.3 HTTP Flood

The goal of HTTP flood attacks is to overload web servers with many HTTP requests. Attackers can target URLs, forms, or online application functionalities with a large volume of requests by using botnets or other automated methods. HTTP Flood assaults cause the server's performance to deteriorate, rendering it incapable of responding to valid user requests by using up the server's memory, processing power, and network bandwidth. Consequently, there is a disruption in service or downtime because of the web server becoming slow or unresponsive to authorized users.

Case Study: Imperva DDoS Attack (2019)

Overview: A large-scale HTTP flood attack targeted Imperva's infrastructure, using a botnet to generate massive amounts of traffic.
Impact: The attack caused temporary service interruptions and highlighted the need for robust application-level defenses.
Response: Imperva utilized advanced DDoS mitigation techniques and further enhanced their defences.

2.4 Ping Flood (ICMP Flood)

Ping Flood attacks, sometimes referred to as "Ping of Death" or ICMP Flood attacks, overwhelm the target system with an endless barrage of Internet Control Message Protocol (ICMP) echo request packets. These packets, which take advantage of flaws in operating systems or network devices, are sent quickly and are usually larger than the allowed size. The target machine experiences sluggish performance or even crashes because of overusing its CPU and network resources processing these packets. Ping Flood assaults are hard to counterbecause they might originate from several sources at once and are easy to conduct.

Case Study: Smurf Attack (1998)
Overview: The Smurf attack, a type of ICMP flood, targeted multiple organizations, amplifying traffic and directing it towards the victims.
Impact: The attack disrupted services and highlighted the vulnerabilities in handling ICMP traffic.
Response: Organizations implemented filters and disabled ICMP broadcasts to mitigate the attack.

2.5 Slowloris

Attacks known as "slowloris" are named after the way they use server resources—low and slow. Slowloris keeps a small number of connections active for a long time rather than flooding the server with requests. Attackers make sure that every connection is active by sending HTTP headers to the server very slowly. Slowloris stops authentic users from creatingnew connections by filling the server's connection slots with incomplete requests. A denial- of-service attack against authorized users attempting to access the web server may result from this resource exhaustion approach.

Case Study: Iranian Cyber Army Attack (2009)

Overview:

Impact: The attack highlighted vulnerabilities in web server handling of persistent connections.

Response: Organizations updated their web server configurations to limit the impact of such attacks.

2.6 DNS Amplification

DNS Amplification attacks exploit vulnerabilities in DNS servers to amplify the volume of traffic directed at the target system. Attackers send small DNS queries with a spoofed sourceIP address to vulnerable DNS servers, requesting large DNS responses. These responses, which are much larger than the original queries, are directed towards the victim's IP address, overwhelming its network bandwidth. DNS Amplification attacks leverage the inherent trust between DNS servers, making it difficult to trace the origin of the attack.

Case Study: Spamhaus DDoS Attack (2013)

Overview: Attackers used DNS amplification to target Spamhaus, a spam-fighting organization, with an attack that peaked at 300 Gbps.

Impact: The attack caused significant disruptions to Spamhaus's services and other parts of the internet infrastructure.

Response: Spamhaus worked with various ISPs and DDoS protection services to mitigate the attack.

2.7 NTP Amplification

NTP amplification attacks are comparable to DNS amplification attacks in that they increase the amount of traffic going to the target system by taking advantage of vulnerable Network Time Protocol (NTP) servers. Attackers make small NTP queries to NTP servers, asking huge NTP answers, using a faked source IP address. The victim's IP address is the target of these replies, which are usually significantly larger than the initial queries and interrupt services by congesting the network. Because the NTP protocol is UDP-based, NTP amplification attacks are challenging to counter.

Case Study: Cloudflare DDoS Attack (2014)

Overview: Cloudflare experienced a massive NTP amplification attack that generated traffic exceeding 400Gbps.

Impact: The attack caused widespread disruptions and highlighted the need for securing NTP servers.

Response: Cloudflare and other organizations implemented measures to secure NTP servers and filter malicious traffic.

2.8 Smurf Attack

Smurf Attacks increases the amount of traffic going towards the target system by taking advantage of IP networks' ICMP Echo Reply functionality. A lot of ICMP echo request (ping) packets are sent by attackers to IP broadcast addresses, pretending that the victim's IP address is the originating IP address. As a result, the victim's IP address triggers responses from every computer on the network, exceeding its available bandwidth and resources.

Case Study: CERT Smurf Attack (1999)

Overview: The Computer Emergency Response Team (CERT) was targeted with a Smurf attack, using ICMP echo replies to flood their network.

Impact: The attack disrupted CERT's operations and highlighted vulnerabilities in handling broadcast traffic.

Response: CERT and other organizations implemented measures to filter and block ICMP echo replies directed at broadcast addresses.

3 Stakeholders

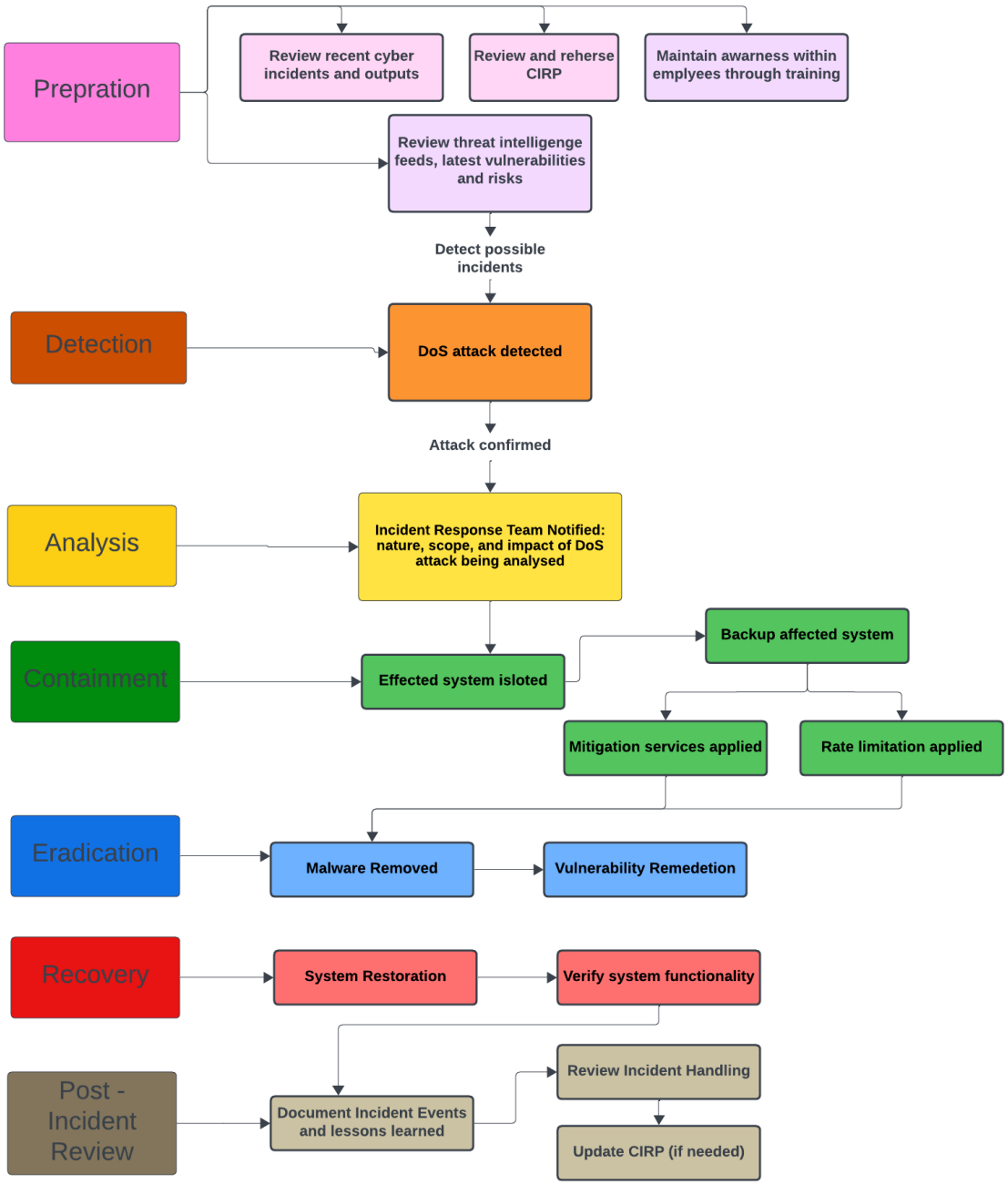
- **IT Administration:** The IT administration oversees the organization's servers, networks, and other IT infrastructure. They are essential in identifying, assessing, and minimizing a denial-of-service attack in addition to organizing the response to the occurrence.
- **Cyber Incident Response Team:** An organization's cyber security incident response team (CSIRT) is a specialized unit tasked with handling security incidents and breaches. Their main objective is to quickly locate, contain, and address issues to lessen their effects. CSIRTs are essential for safeguarding an organization's priceless assets, good name, and customers.
- **External Service Providers:** For a variety of IT services, companies may depend on outside vendors like internet service providers (ISPs), cloud service providers, or managed security service providers (MSSPs). By collaborating with these suppliers, the company can better respond to the denial-of-service attack and make use of more resources and experience.
- **Technical Support Team:** To troubleshoot and resolve technical issues associated with the DoS attack, the technical support team aids. They can assist in promptly returning regular operations to normal and offer support to end customers impacted by the occurrence.
- **End Users:** If the DoS attack prevents end users from accessing services or apps, it could influence them. Minimizing the impact on the position they hold can be achieved by keeping them updated on the situation and offering advice on workarounds or substitute solutions.
- **Senior Management/Executive Leadership:** In deciding how to respond to the DoS attack, senior management, or executive leadership assigns resources, sets strategic direction, and takes choices. They could also be in charge of maintaining the organization's reputation and dealing with outside stakeholders.

RACI Chart for Incident Response

Task/Activity	IT Administration	CSIRT	External Service Providers	Technical Support Team	End Users	Senior Management
Preparation						
Establish incident response team	R, C	A, R	I	I	I	I
Develop response procedures	A, R	R, C	I	I	I	I
Conduct training sessions	A, R	R	I	I	I	I
Implement surveillance systems	A, R	R	I	I	I	I
Detection						
Monitor system logs and traffic	A, R	R	I	I	I	I
Use IDS and SIEM tools	A, R	R	I	I	I	I
Analyse alerts	A, R	R	I	I	I	I
Analysis						
Conduct forensic	A, R	R	I	I	I	I

analysis						
Determine impact	A, R	R	I	I	I	I
Identify threat actor tactics	A, R	R	I	I	I	I
Containment						
Isolate affected systems	A, R	R	I	I	I	I
Implement access controls	A, R	R	I	I	I	I
Block malicious activity	A, R	R	I	I	I	I
Eradication						
Remove unauthorized access	A, R	R	I	I	I	I
Patch vulnerable systems	A, R	R	I	I	I	I
Update security policies	A, R	R	I	I	I	I
Recovery						
Restore compromised systems	A, R	R	I	I	I	I
Recover data from backups	A, R	R	I	I	I	I
Reconfigure networks	A, R	R	I	I	I	I
Post-Incident Review						
Assess incident response	A, R	R	I	I	I	I
Document lessons learned	A, R	R	I	I	I	I
Update incident response protocols	A, R	R	I	I	I	I

4 Flow Diagram



Preparation (Pink)

- Develop and maintain Cyber Incident Response Plan (CIRP) for DoS incidents.
- Identify critical assets and prioritize them.
- Train incident response teams and employees.

Detection (Orange)

- Continuously monitor network traffic.
- Set up alerts for suspicious patterns.
- Validate incidents.

Analysis (Yellow)

- Investigate attack vectors and affected systems.
- Collaborate with relevant teams.

Containment (Green)

- Implement immediate mitigation measures.
- Isolate affected systems.
- Communicate progress.

Eradication (Blue)

- Identify vulnerabilities.
- Patch and remediate.
- Verify closure of attack vector.

Recovery (Red)

- Gradually restore services.
- Validate restoration.
- Monitor for recurrence.

Post-Incident Review (Brown)

- Conduct a thorough review.

- Learn from the incident.
- Update the CIRP.

5 Incident Response Stages

5.1 Preparation

- **Objective**: Establish a robust foundation for effective incident response.
- **Key Actions**
    - Risk Assessment: Use thorough risk assessments to find Dos vulnerabilities in systems, apps, and network infrastructure.
    - Creating Cyber Incident Response Plan (CIRP): Make a thorough incident response plan for handling denial-of-service (DoS) incidents. Establish communication routes, escalation protocols, and roles and duties.
    - Resource Allocation: Ensure that the people, equipment, and technologies required to support incident response activities are available.
    - Training and Awareness: To improve staff members' comprehension of DoS risks, detection methods, and response protocols, offer training and awareness programs.
    - From an Incident Response Team: Assign people to specific areas of managing the response to denial-of-service (DoS) situations in order to create a specialized team.

5.2 Detection

- **Objective**: Promptly identify and confirm the occurrence of DoS attacks.
- **Key Actions**
    - Monitoring and Alerting: To identify indications of unusual behavior suggestive of a denial-of-service attack, continuously monitor network traffic, system performance metrics, and security logs.
    - Anomaly Detection: Use intrusion detection/prevention systems (IDS/IPS), network traffic analysis tools, and security information and event management (SIEM) systems to identify strange patterns or abrupt increases in trafficvolume that could be signs of a denial-of-service assault.

- Alert Triage: Set alerts produced by monitoring systems in order of priority and look into them to see whether they point to a Dos assault. Correlate alerts with several data sources to validate them.

5.3 Analysis

- **Objective**: Conduct in-depth analysis of the DoS attack to understand its nature, scope, and impact.
- **Key Actions**
  - Traffic Analysis: Examine network traffic patterns to determine the nature of the traffic, source IP addresses, and services or apps that are being targeted in order to determine the characteristics of the DoS attack.
  - Log analysis: Look through security system logs, system logs, and other pertinent log data to find any unusual activity or attempted illegal access that may have been connected to the DoS incident.
  - Forensic Investigation: Gather and store digital evidence connected to the DoS assault for forensic examination. Memory dumps, system snapshots, andpacket captures are a few examples of this.
  - Root produce Analysis: Find the vulnerabilities or misconfigurations that the attacker may have exploited in order to trigger the denial of service (DoS) incident.

5.4 Containment

- **Objective**: Limit the impact of the attack and prevent its spread.
- **Key Actions**
  - Traffic Filtering: To stop or filter malicious traffic linked to the DoS attack, use security system rules, access control lists (ACLs), and other network filtering techniques.
  - Rate limitation: To reduce excessive traffic flows and avoid networkcongestion, use rate limitation, or traffic shaping techniques.
  - Isolation: To stop the DoS attack from spreading and lessen its effects on other infrastructure components, isolate the compromised systems or network segments.

- Cloud-Based Mitigation: Use content delivery networks (CDNs) or cloud-based mitigation services to reduce the amount of DoS attack traffic before it enters the network perimeter of the company.

5.5 Eradication

- **Objective**: Eliminate the root cause of the attack and remove the presence of the attacker.
- **Key Actions**
  - Patch and Update Deployment: To address vulnerabilities that the attacker exploited and stop future denial-of-service assaults, apply patches, security updates, and configuration modifications.
  - System Hardening: To strengthen systems and lessen their vulnerability to DoS attacks, take additional security precautions. Some of them include turning off unused services, tightening access limits, and putting security best practices into practice.
  - Network Redesign: To increase resilience and better withstand DoS assaults, think about revamping the network architecture or implementing more network security measures.

5.6 Recovery

- **Objective**: Restore normal operations.
- **Key Actions**
  - System Restoration: Assure data integrity and uninterrupted operations by restoring impacted systems and services from backups.
  - Service Verification: To make sure the restored systems and services are operating correctly and securely, thoroughly assess and verify them.
  - Communication with Stakeholders: Give advice on how to resume regular activities and update stakeholders on the status of the recovery efforts.

5.7 Post-Incident Review

- **Objective**: Conduct a comprehensive review of the DoS incident response process to learn from the incident and improve future response.
- **Key Actions**

- Debriefing: Conduct a debriefing session with the members of the incident response team to evaluate the success of the response efforts and pinpoint any obstacles that may have arisen.
- Root Cause Analysis: To determine the underlying causes of the DoS occurrence, such as security control gaps or vulnerabilities, conduct a root cause analysis.
- Documentation of Lessons Learned: Provide a record of the takeaways that were discovered from the DoS incident, outlining effective response tactics, areas that require development, and suggestions for improving incident response capabilities.
- Updates to the Incident Response Plan: To resolve identified shortcomings and integrate improvements, update the incident response plan in light of the post-event review results.

6. Steps for Monitoring Threats

6.1 Establish a Monitoring Strategy

- **Objective:** Develop a comprehensive strategy specifically for monitoring DoS threats.
- **Key Actions:**
  - Define clear objectives tailored to the detection and management of DoS threats.
  - Select and deploy specialized tools designed to monitor DoS-related activities, such as advanced Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) systems, and Network Traffic Analysis tools.
  - Establish baselines for normal network and system activity to differentiate between legitimate and suspicious behaviors.

6.2 Deploy Monitoring Solutions

- **Objective:** Implement and configure monitoring tools to detect DoS threats across the organization's infrastructure.
- **Key Actions:**
  - Deploy chosen monitoring tools specifically configured to track DoS-related activities across all critical systems and networks.
  - Integrate monitoring tools with threat intelligence feeds to stay updated on the latest DoS vulnerabilities and attack vectors.
  - Ensure comprehensive logging of all network traffic and system activities, focusing on potential DoS attack patterns.

6.3 Continuous Monitoring and Analysis

- **Objective:** Maintain continuous surveillance and analysis to promptly detect and respond to DoS threats.
- **Key Actions:**
  - Implement real-time monitoring to continuously observe network traffic, system performance, and security logs for signs of DoS attacks.
  - Utilize behavioral analytics and machine learning to identify anomalies in network and system activity that could indicate DoS attempts.
  - Correlate events from various sources to identify and prioritize potential DoS threats.

6.4 Alerting and Notification

- **Objective:** Ensure timely and effective response to detected DoS threats through a robust alerting system.
- **Key Actions:**
  - Establish thresholds and triggers for different types of DoS alerts, considering the severity and potential impact.
  - Configure automated alerts to notify the incident response team immediately when suspicious DoS activities are detected.
  - Implement a prioritization system for alerts to ensure that critical DoS threats are addressed promptly.

6.5 Investigate and Respond

- **Objective:** Conduct thorough investigations and implement appropriate actions to mitigate identified DoS threats.
- **Key Actions:**
  - Perform initial triage to verify the validity and potential impact of DoS alerts.
  - Conduct in-depth analysis of confirmed alerts to understand the root cause and potential extent of the threat.
  - Initiate containment measures, such as isolating affected systems and blocking malicious traffic, and execute necessary eradication procedures.

6.6 Post-Incident Review

- **Objective:** Assess the effectiveness of the response to DoS incidents and identify areas for improvement.
- **Key Actions:**
  - Record all details of the DoS incident, including detection, analysis, and response actions taken.
  - Conduct a comprehensive review of the monitoring and response processes post-incident to identify strengths and areas for improvement.
  - Update monitoring tools, configurations, and thresholds based on findings to enhance future detection and response capabilities.

6.7 Continuous Improvement

- **Objective:** Maintain and enhance the organization's strategy and tools for monitoring DoS threats.
- **Key Actions:**
  - Conduct regular audits to ensure the effectiveness of DoS monitoring tools and strategies.
  - Provide ongoing training to security personnel, focusing on detecting and responding to DoS threats.
  - Continuously adapt the monitoring strategy to address emerging DoS threats and vulnerabilities.

7.Terminology

- **CIRP (Cyber Incident Response Plan):** It is a documented set of procedures and guidelines for organization to follow when responding to and managing security incidents. It outlines roles, responsibilities, communication channels, and technical steps necessary to detect, analyses, contain, eradicate, and recover from incidents. It is essential to have a well-prepared CIRP for effective incident response and minimizing the impact of security threats.
- **CSIRT (Cyber Security Incident Response Team):** It is an expert group that manages cyber security incidents. They are responsible for detecting, analyzing, containing, eradicating, and recovering from security incidents affecting an organization. CSIRTs play a critical role in safeguarding an organization's assets and maintaining trust with stakeholders.
- **UDP (User Datagram Protocol):** It is a communication protocol used for time-sensitive transmissions such as video playback or DNS lookups. It does not establish a connection before data transfer and directly sends them to a target computer without checking whether they arrived as intended or indicating their order.
- **TCP three-way handshake:** It is a protocol for establishing a connection between a server and a client in a TCP/IP network. It involves three steps: client sendsa SYN segment to the server, server responds with a SYN-ACK segment, client acknowledges the server's response with an ACK segment and establishing a reliable connection for data transfer.
- **Denial of Service (DoS):** An attempt to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services.
- **Distributed Denial of Service (DDoS):** A type of DoS attack where multiple compromised systems attack a target, causing a denial of service.
- **Network Traffic Analysis:** The process of intercepting and examining messages to deduce information from patterns in communication.