Incident Response Playbook
Denial of Service

Phase 1: Preparation

Form a team to respond to incidents that should include a team leader, technical experts, communication experts, and legal counsel.

Create an incident response plan that outlines each team member's roles and responsibilities as well as the steps to take in the event of a denial-of-service attack.

The systems and services that are crucial to business operations are known as critical assets. To guarantee that these assets are safeguarded in the event of an assault, identify and rank them.

Use tools and systems to monitor network traffic and spot any strange activity as you implement monitoring and alerts. Establish alerts to inform the incident response team of any questionable activities.

Phase 2: Detection and Analysis

Determine the DoS attack type: Volumetric attacks, protocol attacks, and application layer attacks are a few examples of DoS attacks. The proper response will be determined with the aid of attack type identification.

Identify the attack's scope: Identify the systems, services, and users that have been impacted by the attack and gauge its impact.

Data collection and analysis Gather information about the attack, such as the originating IP addresses, traffic patterns, and attack type. To create a strategy for your response, use this information.

Confirm the attack: Check to make sure the attack is legitimate and not just a false alert or a misconfiguration problem.

Phase 3: Containment, Eradication, and Recovery

Contain the Attack: To stop the attack, isolate the impacted services and systems to limit future harm. This can entail turning off impacted systems, banning traffic from particular IP addresses, or configuring network capacity restrictions.

Eradicate: Eliminate the attack by locating and eradicating any malware or malicious code that might be to blame.

Restore: As soon as the attack has been neutralized, return to regular operations. This can entail restarting the computer, installing new software, or restoring backups.

Conduct a post-attack review: Examine the occurrence and pinpoint any flaws in the security controls or incident response plan. Utilize this knowledge to make future incident response efforts better.

Phase 4: Communication and Reporting

Notify relevant stakeholders: Share information about the occurrence and the actions taken to contain and stop the attack with all relevant parties, including management, staff, customers, and law enforcement agencies.

Provide updates: Inform all parties involved of the incident's status and its development.

Establish incident reports: Create an incident report detailing the incident's cause, effects, and resolution. Utilizing this report will help future incident response efforts and regulatory compliance.

Identify areas for improvement and revise the incident response strategy as necessary by holding a lessons-learned session with the incident response team.