

DoS/DDoS Incident Response Playbook

| | |
|---------------------------|-------------------------------------|
| Title | DoS/DDoS Incident Response Playbook |
| Version | NA |
| Date issued | DD-MM-YYYY |
| Status | In progress |
| Document owner | Full Name |
| Creator name | Full Name |
| Creator organization name | <Organization Name> |
| Subject category | DoS/DDoS Incident Response |
| Access constraints | NA |
| Review cycle | Annually |

1. Introduction

1.1 Incident Overview

DDoS attacks prevent authorized users from accessing a system or network resources. They are the most common type of attack affecting the business and reputation of target organizations. Attackers attempt to flood a network with fraudulent requests to make its resources unavailable to legitimate users.

Here, the customers and external users of CyberHT Solutions were unable to access the website from the past few hours. The situation deteriorated because every attempt to access the website failed. This scenario was reported to the service desk team for taking necessary actions to avoid downtime and restore services.

1.2 Purpose of Playbook

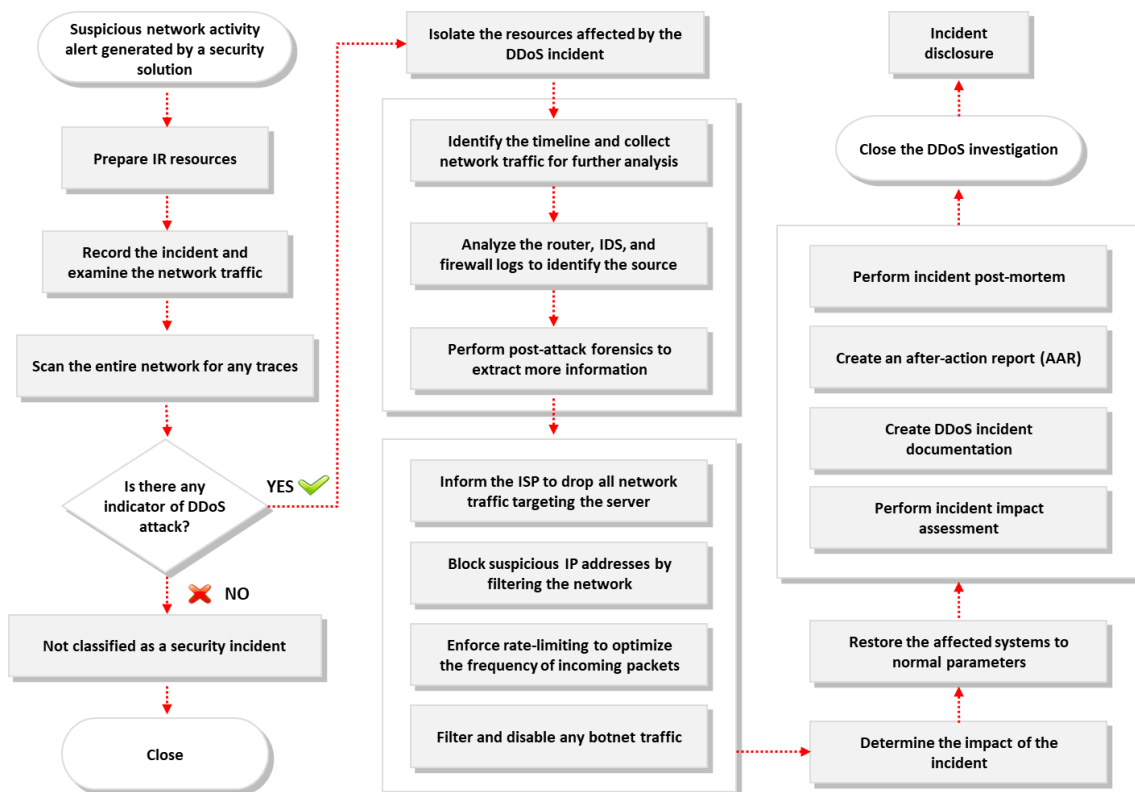
The main purpose of this playbook is to provide guidance to detect and respond to DoS/DDoS incidents in organizational networks. This playbook includes step-wise guidance for the IH&R team to implement mitigative actions and defend against DoS/DDoS attacks.

1.3 Scope

This playbook is developed for incident responders to handle and respond to DoS/DDoS incidents in an organization's network. Additionally, this document must be used alongside the incident response plan of an organization. The scope of this document is listed below (not limited to):

- Determine business impact of the DoS/DDoS incident
- Understand the reason of the DoS/DDoS incident
- Identify any relevant indicators by checking the following:
 - Connection losses
 - Asymmetric network traffic pattern
 - Slow access to files located locally or remotely
 - Data packets with abnormal source or destination addresses
 - Increased utilization of network bandwidth
 - User reports of application unavailability
 - A host with several connections
 - Sudden system crash or performance deterioration
 - Frequent error messages
 - Websites and services loading extremely slowly
 - Unexpected increase in requests on open ports
 - Excessive memory usage
 - Extremely high number of spam emails
 - DNS not responding for website redirection
 - Website frequently going offline
- Implement the incident response plan under the supervision of higher authorities of the organization
- Detect and analyze the DoS/DDoS security incident
- Implement proper eradication and recovery steps to recover from the incident

1.4 Workflow Diagram



Workflow diagram of DoS/DDoS incident response process

2. Preparation

2.1 Objectives

The main objective of this phase is to prepare organizations to effectively respond to DoS/DDoS security incidents. Another objective of this phase is to define the required roles for handling the entire DDoS incident response process.

2.2 Activities Involved

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Prepare for DoS/DDoS incident response:
 - Prepare, review, and practice DoS/DDoS incident response procedures in accordance with the incident response plan
 - Configure DoS/DDoS incident detection tools such as KFSensor and SNORT to detect DoS/DDoS incidents across the organizational network
 - Use tools such as Wireshark to analyze network packets
 - Establish out-of-band communication channels between the IH&R team and customers/stakeholders

- Incorporate threat intelligence into the existing security capabilities to feed them with the latest risks and vulnerabilities, common patterns, etc. that could help in detecting and responding to DoS/DDoS security incidents
- Understand and review the most recent DDoS incidents and their impact
- Maintain network architecture and network diagram of the organization's network infrastructure
- Provide easy access to necessary documentation such as incident response plan and network architecture to respond to DoS/DDoS incidents. The links of the important documents are given below:

Reference Link 1:

Reference Link 2:

Reference Link 3:

- Identify and define the key indicators and patterns of a DoS/DDoS incident and map them with the available SIEM or other security solutions
- Identify and subscribe to reputed third-party forensic services to avail their services, if required
- Prepare a list of questions to be asked by tech support from the complainants to analyze the type of DDoS incident
- Collaborate with the Disaster Recovery (DR) and Business Continuity Planning (BCP) team for additional support
- Define threat indicators and signatures to alert if something goes wrong during the investigation
- Prepare a whitelist of protocols and system IPs to be accessed during the incident handling process
- Configure critical DNS TTL for systems that may be attacked during investigation
- Prepare backup systems based on attack severity
- Baseline the network performance to ensure that any changes made during the incident handling process can be identified.
- Distribute DNS and other services through alternative authentication server
- Define and assign roles to different IH&R team members

- Train and inform employees:
 - Conduct regular training and awareness programs related to DDoS incidents
 - Create a proper format for reporting and registering complaints
 - Ensure that training and awareness sessions are mandatory for employees handling critical data and systems of the organization
 - Provide proper contact information of personnel who can be contacted by users in case of a DoS/DDoS security incident

2.3 Stakeholders Involved/Communication

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

| Activities | Stakeholders Involved | Communication Mode/Channel |
|--|------------------------------|----------------------------|
| Prepare for incident response <ul style="list-style-type: none"> ○ Create incident response processes and procedures ○ Define roles and responsibilities ○ Review recent incident reports ○ Incorporate threat intelligence ○ Maintain network architecture and data flow diagrams ○ Define threat indicators and incorporate alerting solutions | CISO | Email, Phone, Text Message |
| | Information Security Manager | Email, Phone, Text Message |
| | Head of IT | Email, Phone, Text Message |
| | Service Desk | Email, Phone, Text Message |
| | Service Delivery Manager | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |
| | Administrators | Email, Phone, Text Message |
| | Legal Team | Email, Phone, Text Message |
| | Federal Agency | Email, Phone, Text Message |
| | Business Continuity Lead | Email, Phone, Text Message |
| Inform employees | Information Security Manager | Email, Phone, Text Message |

| | | |
|---|---------------------|----------------------------|
| ○ Conduct training and awareness on the use of organizational resources and reporting of associated incidents | IT Manager/Director | Email, Phone, Text Message |
| | HR Manager/Director | Email, Phone, Text Message |
| | Administrators | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |

2.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- Preparation to Handle Network Security Incidents Checklist.docx
- IH&R Plan Template.docx
- IH&R Plan Checklist.docx
- IH&R Policy and Procedure Template.docx

3. Detection

3.1 Objectives

The main objective of the detection phase is to perform initial investigation on the DoS/DDoS incident and report it to the appropriate incident handling team for further analysis.

3.2 Activities Involved

[Activities may differ according to organizational policies, but they are not limited to the following.]

- Detect the DoS/DDoS incident from the initial investigation:
 - Check for increase in the utilization of network bandwidth
 - Check for asymmetric network traffic patterns
 - Check for data packets with abnormal source addresses
 - Check for data packets with abnormal destination addresses
 - Check for abnormal activity in the internal SNMP traffic
 - Check if the server is trying to process beyond its acceptable load
 - Check for large amounts of data from a single IP address
 - Check for sudden increase in traffic toward a single port
 - Check the system's threshold to detect overload
 - Check if any unusual applications are installed on the endpoints

- Check for suspicious traffic alerts from botnet filters
- Check for DNS lookup failures within a specified time
- Trace the logs of the server being attacked
- Monitor organizational services and check whether they work under normal parameters
- Monitor the organization's network traffic with:
 - Same IP addresses
 - Same port numbers
 - Same user agents
 - Traffic using common protocols
- Categorize the type of DDoS incident based on the identified information
- Check for increase in activity levels between network flow clusters
- Use the sequential change-point detection technique to filter the network traffic and identify and locate the DDoS incident
- Use the wavelet analysis technique to analyze the network traffic and identify unfamiliar frequencies indicating suspicious network activity
- Check for non-responding applications that could indicate a DoS/DDoS attack
- Analyze the network traffic containing a large number of ARP requests
- Determine traffic patterns deviating the baseline rules
- Verify if the company received any extortion demands before being attacked
- Check whether the attack is confined only to the targeted network or it is spreading to other corporate networks
- Determine the timeline of the attack
- Check for outbound connections from the internal network
- Identify the list of resources flooded with unusual access requests
- Check the network address translation (NAT)/port address translation (PAT) tables for large numbers of entries
- Check whether the router's IP input, ARP input, IP cache ager, and Cisco Express Forwarding (CEF) processes are using abnormally high amounts of memory
- Check whether the router's ARP, IP input, CEF, and inter-process communication (IPC) processes are running at a higher CPU utilization rate than normal

- Check for a large number of similar types of packets from the same or different IP addresses that can result in TCP or UDP flooding
- Use tools such as KFSensor and SNORT to detect DoS/DDoS incidents
- Escalate and report the detected incident to higher authorities using the proper escalation procedure
- Gather the following information from the initial investigation:
 - Type of DoS/DDoS incident
 - Targeted systems/applications/services
 - Impact of DoS/DDoS incident on targeted components
 - List of services affected by the incident
 - Effects on network bandwidth
 - Timeline of attack (when it began and when it was first detected)
 - Check if the attack is spreading to other systems/applications

3.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

| Activities | Stakeholders Involved | Communication Mode/Channel |
|---|------------------------------|----------------------------|
| Detect the incident ○ Monitor security solutions ○ Respond to both manual and automated alerts ○ Escalate the incident via the ticketing system (if not escalated) | Information Security Manager | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |
| | Product Manager | Email, Phone, Text Message |
| | Service Desk Analysts | Email, Phone, Text Message |
| | Head of IT | Email, Phone, Text Message |
| | Resilience Lead | Email, Phone, Text Message |
| | Business Continuity Lead | Email, Phone, Text Message |
| Initial investigation | Information Security Manager | Email, Phone, Text Message |

| | | |
|---|------------------------------|----------------------------|
| <ul style="list-style-type: none"> ○ Collect initial evidence data ○ Classify and prioritize the incident | IH&R Team | Email, Phone, Text Message |
| | IT Manager/Director | Email, Phone, Text Message |
| | Head of IT | Email, Phone, Text Message |
| <p>Notification of the incident</p> <ul style="list-style-type: none"> ○ Follow the defined IH&R plan to notify the incident | Information Security Manager | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |
| | Policy Area Lead | Email, Phone, Text Message |
| | Business Continuity Lead | Email, Phone, Text Message |

3.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- e. Network Incidents Detection and Analysis Template.docx
- f. Incident Identification and Validation Template.docx
- g. Incident Priority Template.docx
- h. Incident Communication Logs Template.docx
- i. Point-of-Contact Template.docx

4. Containment

4.1 Objectives

The main objective of this phase is to isolate the services affected by a DoS/DDoS incident to prevent the attack from spreading to other services and networks in the organization.

4.2 Containment Steps/Activities

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Activities to contain DDoS incidents:
 - Identify the affected servers, provide additional bandwidth to network devices, and increase the capacity of servers to absorb the attack
 - Divert the traffic by redirecting URLs and requests to similar servers placed at other locations
 - Initiate network segmentation to isolate critical resources from public-facing services
 - Stop non-critical services while identifying the indicators of a DoS attack
 - Use automated tools such as advanced firewall and IDS solutions to detect DoS attacks using traffic distance and timing techniques, and block them before they affect the services
 - Increase the bandwidth of critical connections in the event of a DDoS attack to prevent servers from shutting down
 - Regularly scan the network to block unusual traffic
 - Use egress filters to terminate responses from the internal system to DDoS requests
 - Use the IP blocking mechanism for critical/sensitive services to reduce the impact of DDoS incidents
 - Block and blacklist IP addresses sending multiple requests within a short duration (also known as automated requests)
 - Allow only whitelisted IPs to operate within the network
 - Temporarily disable the port being constantly targeted
 - Block the traffic deviating the baseline rules
 - If a specific feature of an application is generating points of congestion, block that feature temporarily
 - Request your ISP to block out-of-range IP addresses requesting the same resources
 - If traffic congestion emerged from ISP side, share relevant information with them to take appropriate measures

- Communicate the progress:
 - Regularly inform the stakeholders about the status of the incident handling process

4.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

| Activities | Stakeholders Involved | Communication Mode/Channel |
|------------------------|------------------------------|----------------------------|
| Containment activities | Information Security Manager | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |
| | Resilience Lead | Email, Phone, Text Message |
| | Business Continuity Lead | Email, Phone, Text Message |
| | Policy Area Lead | Email, Phone, Text Message |

4.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- j. Containment of Network Security Incidents Checklist.docx
- k. Incident Containment Checklist.docx
- l. Incident Containment Template.docx

5. Analysis

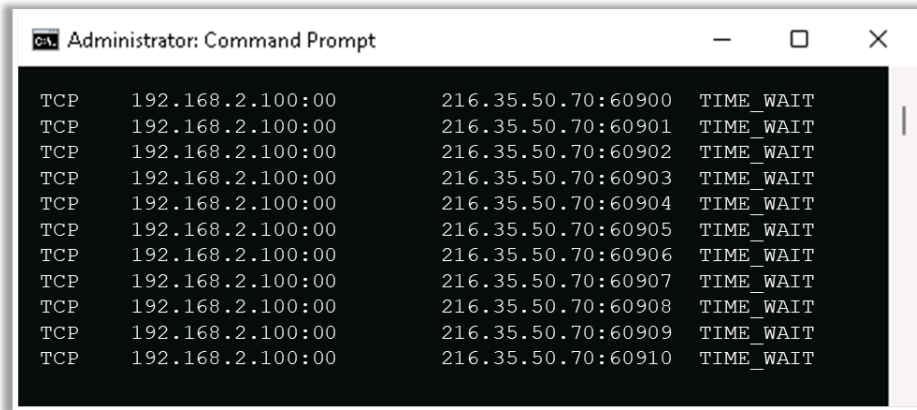
5.1 Objectives

The main objective of this phase is to analyze DoS/DDoS incidents using different techniques and obtain more information that can help in mitigating the incident in a timely and effective manner.

5.2 Activities Involved

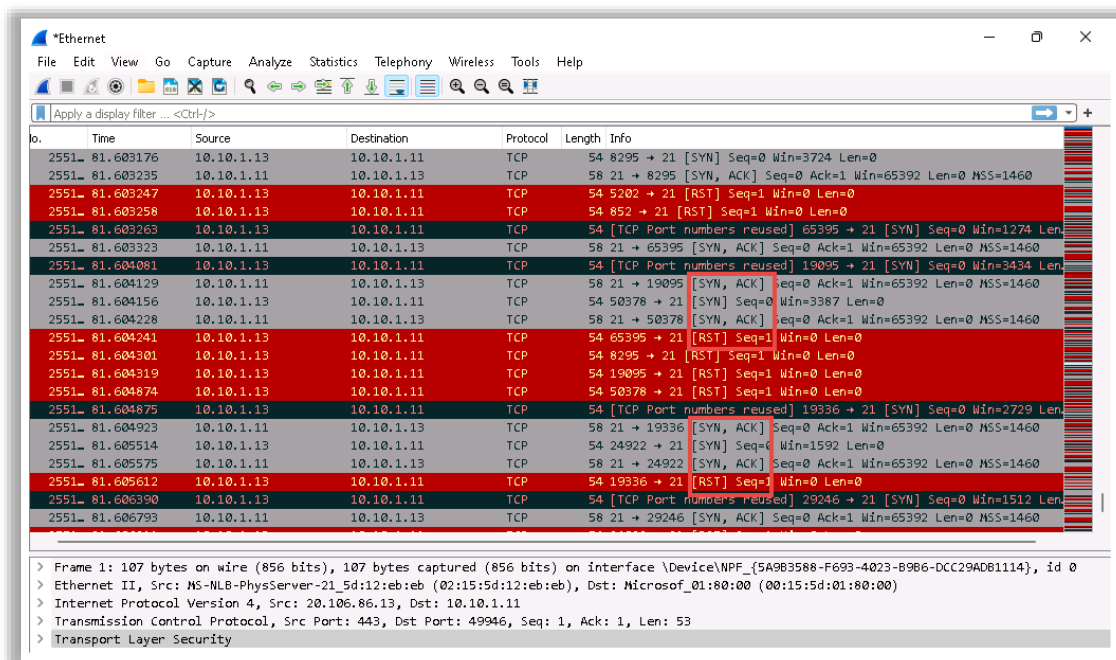
[Activities may differ based on organizational policies, but they are not limited to the following.]

- Analyze the DoS/DDoS incident:
 - Check the network(s) connecting compromised devices, services, applications, and servers to validate a DoS attack. Under normal operation conditions, a server shows multiple connections to multiple IP addresses through various ports. However, during a DoS attack, all connections are made from a single source with the same IP address, as shown in the following screenshot:



DoS attack scenario

- Examine the application that stopped responding owing to heavy incoming network traffic.
- Analyze the network traffic using Wireshark to check for DoS/DDoS attempts, as shown in the following screenshot:



Screenshot of Wireshark showing DoS attempt

- Perform traffic pattern analysis, which can help in developing new filtering techniques to prevent DDoS attack traffic from entering or leaving the network.
- Analyze network traffic containing numerous ARP requests.
- Perform packet traceback to identify the true source and block further attacks from that source by developing the necessary preventive techniques.

- Analyze event logs to recognize the type of DDoS attack or combination of attacks used; this can help in tracing back the attacker's IP address with the help of intermediary ISPs and law enforcement agencies.
- Correlate data from multiple nodes to discover network ingress points of the DDoS attack.
- Analyze system or server logs to resolve performance issues.
- Use network analyzers such as MRTG, Netflow, and tcpdump to analyze inbound/outbound traffic.
- Analyze Network Intrusion Detection System (NIDS) signatures to differentiate between valid and invalid traffic.
- Conduct forensic investigation on the captured network traffic.

5.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

| Activities | Stakeholders Involved | Communication Mode/Channel |
|---|------------------------------|----------------------------|
| Initiate evidence gathering and forensic analysis | Information Security Manager | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |
| Analyze network traffic | CISO | Email, Phone, Text Message |
| | Information Security Manager | Email, Phone, Text Message |
| | IT Manager/Director | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |
| | Network Administrators | Email, Phone, Text Message |

5.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- m. Network Incidents Detection and Analysis Template.docx
- n. Network Security Incident Handling Toolkit.docx
- o. Checklist for Handling the Forensic Evidence Properly.docx
- p. Evidence Gathering and Forensic Analysis Form.docx

6. Eradication

6.1 Objectives

The main objective of this phase is to take appropriate security measures to eradicate the DoS/DDoS incident and avoid similar incidents in future.

6.2 Eradication Steps/Activities

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Perform the following activities to eradicate a DoS/DDoS incident:
 - Use egress filtering to ensure that unauthorized or malicious traffic never leaves the internal network of the organization
 - Use ingress filtering to indirectly combat several types of net abuse by making Internet traffic traceable to its true source
 - Use the TCP intercept feature on routers to prevent fake connection attempts from reaching the server by acting as a mediator between the server and client throughout the connection
 - Enforce rate-limiting to optimize the frequency of incoming packets
 - Implement RFC 3704 filtering to limit the impact of DDoS attacks by blocking traffic with spoofed addresses
 - Identify and patch the vulnerabilities in services
 - Implement DDoS prevention services from the ISP or other third-party organizations such as Cisco Secure DDoS Protection
 - Neutralize botnet handlers to quickly disrupt the DDoS attack network
 - Implement network segmentation to protect critical servers
 - Disable or remove vulnerable services or systems
 - Blacklist all identified attacker IP addresses
 - Create a whitelist of IP addresses and services allowed into the corporate network
 - Contact ISPs to take further remediation measures such as traffic-scrubbing and sinkhole routing
 - Review and update firewall settings and rules
 - Subscribe to efficient DDoS protection services to handle future DoS/DDoS incidents
 - Consider strict TCP keepalive and maximum connection implementations on all perimeter nodes

- Modify the affected resource's settings immediately after eliminating the incident

6.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

| Activities | Stakeholders Involved | Communication Mode/Channel |
|---|---------------------------------------|----------------------------|
| Eradicate the DoS/DDoS incident ○ Perform technical and business analyses and create prioritized eradication ○ Establish a communication strategy based on the eradication plan | Information Security Manager | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |
| | IT Manager/Director | Email, Phone, Text Message |
| | Internal/External Communications Team | Email, Phone, Text Message |
| | Resilience Lead | Email, Phone, Text Message |
| | Business Continuity Lead | Email, Phone, Text Message |
| | Policy Area Lead | Email, Phone, Text Message |
| Eradication activities | Information Security Manager | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |

6.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- q. Eradication Network Security Incidents Checklist.docx
- r. Incident Eradication Template.docx
- s. Incident Eradication Checklist.docx

7. Recovery

7.1 Objectives

The main objective of the recovery phase is to recover the services and systems affected by the DoS/DDoS incident and maintain business continuity.

7.2 Recovery Steps/Activities

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Activities to recover from a DoS/DDoS attack:
 - Use backup resources efficiently to replace compromised systems
 - Recover any lost data from backup files
 - Restore all affected systems, services, and applications to their ready-to-work state
 - Check the functionality of all restored systems
 - After restoring devices, change the default passwords with a strong mixture of characters
 - Implement additional monitoring to look for related incidents in future
 - Erase unwanted DoS/DDoS detection logs recorded across security solutions after detecting and responding to a DoS/DDoS attack
 - Restart the Border Gateway Protocol (BGP) to send a keepalive message after restoring a website from a DoS/DDoS attack
 - Establish an automated communication desk to keep in touch with clients after resolving the DoS/DDoS attack
 - Develop a strategy to establish connections to clients involving different data centers after restoring the server
 - Implement the best DoS/DDoS mitigation strategy and ask your ISP to unblock services that were blocked during the attack
 - Plan the orderly restoration of applications after rectifying the DoS/DDoS attack to avoid secondary attack situations while restarting applications

7.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

| Activities | Stakeholders Involved | Communication Mode/Channel |
|---------------------|------------------------------|----------------------------|
| Recovery activities | Information Security Manager | Email, Phone, Text Message |
| | Core IT CIRT | Email, Phone, Text Message |

7.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- t. Recovery of Network Security Incidents Checklist.docx
- u. Incident Recovery Checklist.docx

8. Post-incident Activities

8.1 Objectives

The main objective of this phase is to develop the necessary DoS/DDoS incident reports such as incident documentation, lessons learned, and incident impact assessment. Another objective of this phase is to officially close the DoS/DDoS investigation and disclose it to respective stakeholders.

8.2 Activities Involved

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Perform DoS/DDoS incident post-mortem or incident review to detect the root cause
- Create an after-action report (AAR) that includes information such as what worked effectively, areas of improvement, and strategies for enhancing the response in case of similar DoS/DDoS incidents
- Conduct a lessons learned meeting to document all details of the incident. Moreover, ensure that the following questions are answered in that meeting:
 - When and who detected the DoS/DDoS incident?
 - What happened exactly?
 - What caused the DoS/DDoS incident?
 - What challenges were encountered?
 - To whom was the DoS/DDoS incident reported?
 - Was the organization adequately prepared for the DoS/DDoS incident?

- How was the DoS/DDoS incident contained?
- How were the impacted systems sanitized?
- What procedures were followed during recovery?
- Were the documented procedures followed by the response team?
- How well did the incident response team and management perform in resolving the DoS/DDoS incident?
- How should the incident response team and management respond to mitigate similar incidents in future?
- Were there any gaps in communicating the DoS/DDoS incident?
- Was the right amount of information shared with the right personnel?
- What tools and resources are required to detect, analyze, and prevent DoS/DDoS incidents in future?
- Create concise and clear DoS/DDoS incident documentation written in a standard format and reviewed by editors
- Create incident impact assessment report to determine the types of losses caused by the DoS/DDoS incident; this report must include the following information, if required:
 - Financial losses incurred owing to the DDoS incident
 - Legal costs for investigating the case, lawyer's fees, etc.
 - Costs pertaining to analyzing the DoS/DDoS incident as well as recovering and installing software and hardware
 - Implementation costs
 - Costs related to the damage of goodwill and loss of customer trust and reputation
- Close the DoS/DDoS incident investigation officially by informing the management and securely retain investigation reports considering the retention policy of the organization
- Disclose incident details to the respective stakeholders by consulting with the legal department of the organization
- If any lapses were found in the current strategy, amend the IH&R plan according to the latest scenario for better use in future

8.3 Stakeholders Involved/Communication Established

| Activities | Stakeholders Involved | Communication Mode/Channel |
|--|----------------------------------|----------------------------|
| Conduct a lessons learned meeting | Information Security Manager | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |
| Create incident documentation | Information Security Manager | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |
| Create an incident impact assessment report | Information Security Manager | Email, Phone, Text Message |
| | IH&R Team | Email, Phone, Text Message |
| Close the investigation officially | Information Security Manager | Email, Phone, Text Message |
| | Incident Response Team | Email, Phone, Text Message |
| | Senior Management | Email, Phone, Text Message |
| Disclose incident details to respective stakeholders | Information Security Manager | Email, Phone, Text Message |
| | Manager - Information Governance | Email, Phone, Text Message |
| | IT Manager/Director | Email, Phone, Text Message |
| | CISO | Email, Phone, Text Message |
| | Legal Team | Email, Phone, Text Message |
| | Human Resource | Email, Phone, Text Message |
| | Media | Email, Phone, Text Message |
| | Vendors | Email, Phone, Text Message |
| | Customers & General Public | Email, Phone, Text Message |
| | Business Partners | Email, Phone, Text Message |
| | Resilience Lead | Email, Phone, Text Message |
| | Business Continuity Lead | Email, Phone, Text Message |
| | Policy Area Lead | Email, Phone, Text Message |

8.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- v. Incident Documentation Template.docx
- w. Incident Impact Assessment Report Template.docx
- x. Incident Closure Letter.docx
- y. Incident Disclosure Form.docx

9. Appendix (if any)