

# DDoS Incident Response Runbook

<b>Title</b>	DDoS Incident Response Runbook
<b>Version</b>	1.0
<b>Date issued</b>	DD-MM-YYYY
<b>Status</b>	In progress
<b>Document owner</b>	
<b>Creator name</b>	
<b>Creator organization name</b>	ECC
<b>Subject category</b>	DDoS Incident Management
<b>Access constraints</b>	
<b>Review cycle</b>	Annually

**Note:** In case of a DDoS incident, an organization can use this runbook alongside the security guidelines of their incidence response plan and the associated playbook. The IH&R team may add or remove some guidelines from this runbook according to their business requirements considering organizational security policies.

## 1. Incident Detection

- Evaluate the alert reported to the service desk
  - Identify the type of alert and reasons to create a ticket/case for the incident
  - Check if the reported alert affected multiple users/nodes
  - Verify the alert by replicating it by connecting the system with a web browser in an external interface
    - Run DNS lookup to ensure and identify the IP addresses indicated to by the DNS
    - Ensure that the DNS is responding and indicating the correct host in the network
    - Ensure that the DNS of all nodes is responding appropriately to the respective IP addresses
    - Check the expiry date of the domain using online tools such as [whatsmydns.net](https://www.whatsmydns.net)

- Gather and preserve the first alert's timestamp and make a duration tab if the alert continues
- If a security alert is generated by a user, try to identify the following:
  - User location
  - ISP details and IP address
  - Details of web servers where the user was connected
  - DNS server details
  - Browser details used to analyze the availability
  - User/node connected to other websites during the incident
- Check for the node(s) that detected the issue according to the ISP and IP in case of an automated alert
- Check whether the alert is specific to any region or ISP; additionally, check for Internet issues
- Determine the type of DDoS attack by identifying the indicators
- Check the time zone of all recorded logs and identify the first time zone from which the incident alert arrived
- Check for any known issues or events that could disrupt organizational services and operations
- Identify the affected services, applications, and organizational assets
- Identify if any specific IP addresses are sending several connection requests frequently
- Identify any 503 error code from the server
- Identify traffic source addresses that are continuously querying for the same data even after the passing of TTL
- Follow the steps given below to detect DDoS attacks on a Windows system:
  - Log in to the server through the Remote Desktop Protocol (RDP)
  - Open Command Prompt and run the following command to check all network connections associated with the system:  
**netstat -noa**
  - Run the following command to view all active TCP connections on the system, including port numbers and IP addresses:  
**netstat -n**
  - Run the following command to check all active TCP connections; this will display the process IDs of all connections:  
**netstat -o**

Now, you can open the Task Manager and identify applications with the same process ID.

- Run the following command to view all active TCP connections along with all TCP/UDP ports:

**netstat -a**

After obtaining these statistics, identify the IP address with several TCP connections; the presence of such IP address indicates a DDoS attack; this information can be used during containment and mitigation.

- Follow the steps given below to detect DDoS attacks on a Linux system:

- Log in to the Linux server via SSH
- Execute the following command to view the average load of the server:

**uptime**

- Execute the following command to identify the number of threads in the server:

**grep processor /proc/cpuinfo | wc -l**

**Note:** If the server has more than two threads, it may indicate an abnormally higher load

- Use the following tools to check the network load if the server can be accessed from a direct connection such as Intelligent Platform Management Interface (IPMI):

- **bmon**

Use this tool to monitor the bandwidth and obtain real-time data visualization in a user-friendly format

- **nload**

Use this utility to monitor bandwidth usage and network traffic; it provides information regarding incoming and outgoing network traffic for a particular interface

- **vnstat**

Use this utility to check the network traffic by inspecting logs saved on hourly, daily, or monthly basis. It also displays a list of available interfaces for further information

- **iftop**

Use this utility to obtain information about the associated network, which will be displayed according to bandwidth usage

- **ifstat**

Use this utility to view network interface statistics, which can help in detecting DDoS attack

- Execute the following Linux command to identify IP addresses connected to the Linux system:

```
netstat -anp | grep 'tcp\|udp' | awk '{print $5}' | cut -d: -f1 | sort | uniq -c
```

- Execute the following command to identify the source IP address and number of connections associated with it in the Linux system:

```
netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n
```

- Execute the following command to identify active TCP connections on port 80:

```
netstat -n | grep :80 | wc -l
```

Any suspicious IP address with several connections could be the IP address used by the attacker; this information can be used during containment and mitigation

## 2. Containment

- Block DDoS traffic after identifying its source by implementing techniques such as IP address filtering and geo-blocking
- Reroute legitimate network traffic to another IP address and change the DNS to make the target obscured
- Contact the ISP and reroute the entire DDoS traffic
- Shut down the affected services to avoid instant damage
- Implement additional defense tools and web application firewalls wherever required
- Follow the steps given below to contain a DDoS incident on an external router:
  - Perform IP address resetting
  - Enable DDoS defense on the router (if available) from the admin console menu
  - Implement additional security layers such as firewalls, DDoS protection, and VPN service
- Follow the steps given below to contain an internal DDoS incident on a router or server:
  - Block suspicious IP addresses or shut down compromised devices
  - Change the IP address of the router or server to reroute resources from the attack
  - Disable or stop the affected services
  - Physically unplug network cables from devices in extreme cases
- Follow the steps given below to block suspicious IP addresses using Windows Firewall:
  - Go to **Advanced Settings** in **Windows Defender Firewall**
  - Click on the **New Rule** option after selecting **Inbound Rules**

- Click on the **Custom** option; then, click on **Next**
- Click on **Next** in the following two screens
- Select the **These IP Addresses** option under **Which remote IP addresses does this rule apply to?** and click on **Add**
- Select the **This IP address or subnet** option, provide the required IP address, and then click on **OK**; you can add multiple IP addresses, if required, and then click on **Next**
- Select the **Block the Connection** option and click on **Next**
- Ensure that all checkboxes under **When Do These Rules Apply?** are selected and click on **Next**
- Provide a name and description in the new Window and click on **Finish**
- Once a DDoS incident on a Linux server is confirmed by the IH&R team, follow the steps given below to contain it:
  - Run the following command to block the suspicious IP address:  
`sudo route add [ip-address] reject`
  - Alternatively, you can use the following iptables commands on the Linux system to block the suspicious IP address:
    - `iptables -A INPUT 1 -s [ip-address] -j DROP/REJECT`  
Run this command to block the suspicious IP address
    - `iptables -A INPUT -s ADDRESS/SUBNET -j DROP`  
Run this command to block an entire subnet, if required
    - `service iptables restart`  
Run this command to restart the service
    - `service iptables save`  
Run this command to save a new rule
    - `sudo systemctl restart apache2`  
Run this command to restart web services; here, the Apache web server is used
- Follow the steps given below to block suspicious IP addresses on Mac:
  - Open the terminal and run the following command to open the PacketFilter configuration file:  
`sudo vim /etc/pf.conf`
  - Run the following command to block the suspicious IP address:  
`block drop from any to <IP ADDRESS>`  
**Note:** Replace “IP ADDRESS” with the IP address that should be blocked.

- Run the following command if you want to block an entire range of IP addresses:  
**block drop from any to IP ADDRESS**

You can replace “any” with the required IP address; for example:

**block drop from <Start IP Address> to <End IP Address>**

- Now, run the following command to enable the packet filter and load the created rule:

**pfctl -e -f /etc/pf.conf**

When the rule is successfully loaded, the IP addresses will be blocked.

### 3. Evidence Gathering and Forensic Analysis

Once the DDoS incident is confirmed after detection, the IH&R team must perform forensic analysis on the incident and gather appropriate information to understand the root cause and eradicate the incident. Follow the steps given below alongside the DDoS playbook considering organizational security policies:

- Check if a connection can be established by connecting a socket with the host via telnet on the appropriate port
  - If the connection is successful, use a browser to re-test it and identify the type of error codes being returned
  - Examine packet loss by pinging the host if the ICMP is open
  - Perform traceroute between the client and server and examine the interruptions and latency
- Follow the steps given below to analyze the firewalls of the organization:
  - Check for DDoS traffic characteristics in comparison to legitimate traffic; you can also examine Multi Router Traffic Grapher (MRTG) graphs to check for SYN flood
  - Review the network traffic using network analyzer tools such as ntop and tcpdump
- Follow the steps given below to analyze web servers/load balancer/application server:
  - If the web server is up and running, check the generated child processes and assess them based on the number of allowed processes
  - Ensure that there is enough memory and disk space for local drives
  - Examine alerts and error logs, including programming and database errors, which can lead to disruption or security incident
  - Examine access logs and identify any surge from any range of IP addresses to analyze potential suspicious IP addresses

- Follow the steps given below to analyze the database server of the organization:
  - Ensure that the website and database are connected and the database connect string and user credentials are functioning
  - Ensure that the database has adequate disk space
  - Examine the number of database connections and compare it with the number of connections allowed on the web server for further investigation
- Follow the steps given below to analyze browsers/search engines:
  - If the browser provides an SSL/TLS warning, then check the following:
    - Expiry date of the certificate
    - Ensure that the certificate matches the host name that needs to be connected
    - Ensure that the certificate authority (CA) is accessible by examining the revocation list used for that CA
- Check the network topology of the organization to obtain relevant information that can help to validate and eliminate the DDoS incident
- Perform network traffic analysis using tools such as Wireshark to check the legitimacy of traffic
- Use the following filters in Wireshark to analyze different types of DDoS incidents:
  - Use the following filter to filter SYN-ACKs from the network traffic in case of a SYN flood attack:  
`tcp.flags.syn==1`  
`tcp.flags.ack==0`
  - Use the following filter to analyze HTTP flood attack:  
`http.request.method == GET Or http.request.method == POST`
- Perform packet traceback on the captured traffic to obtain more information regarding its source
- Use tools such as SolarWinds® Loggly® to perform DDoS event log analysis and obtain additional information for further investigation
- Document the obtained results and inform the respective authorities by following the notification guidelines defined by the organization

#### 4. Eradication

- Increase the network bandwidth or add servers, if possible, to handle additional load until the network, system, or application is recovered
- Use traffic-scrubbing products such as NETSCOUT Arbor to filter and block unwanted traffic disrupting the network

- Enable DDoS blackhole routing to route both malicious and legitimate traffic to a black hole or null route, forcing it to drop out of the network
- End all suspicious processes or connections on the servers and routers; additionally, reconfigure the TCP/IP settings considering the network infrastructure and security policies of the organization
- Block the DDoS traffic targeting the network's cloud through the router, load balancer, or firewall to the maximum extent possible
- Configure egress and ingress filtering

## 5. Recovery

- Use trusted backup to recover lost data or affected applications
- Reestablish BGP connections to send keepalive messages to the peers to inform that that the route is up and running
- Restart the firewalls and other network appliances after eliminating or resolving the DDoS incident
- Restore all affected systems, services, and applications to their ready-to-work state

## 6. Post-incident Actions

- Document all steps and results in a clear format and get it reviewed by an editor
- Disclose incident details or documented results to the respective stakeholders and authorities by consulting with the legal department of the organization
- Conduct a public relations press release, if required, and explain the following:
  - Explain the incident
  - Steps taken for the affected customers
  - Steps taken to prevent similar incidents in future