# **Incident report analysis**

| NIST CSF Step | Action | Description |
| --- | --- | --- |
| Identify | Security Risk Audits: Conduct regular internal audits. | Evaluate network, systems, devices, and access privileges to identify security vulnerabilities. |
|  | Gap Identification: Analyze audit results for gaps. | Identify potential security gaps in network infrastructure and access control. |
| Protect | Policy Implementation: Develop and enforce policies. | Establish cybersecurity policies, procedures, and guidelines for better protection. |
|  | Training: Provide cybersecurity training for employees. | Educate staff about security best practices to enhance internal asset protection. |
|  | Firewall Rule Enhancement: Implement new firewall rule. | Add a rule to limit incoming ICMP packet rate and improve protection against DDoS attacks. |
|  | Source IP Verification: Configure firewall for spoofing. | Verify source IP addresses to prevent attackers from using spoofed IPs in ICMP packets. |
| Detect | Abnormal Traffic Detection: Implement network monitor. | Deploy network monitoring software to identify unusual traffic patterns quickly. |
|  | Suspicious Traffic Filter: Set up IDS/IPS system. | Use IDS/IPS to identify and filter out suspicious ICMP traffic based on predefined criteria. |
| Respond | Incident Containment: Develop containment strategy. | Establish protocols for containing and neutralizing security incidents promptly. |
|  | Communication Protocol: Establish clear communication. | Define communication channels for internal and external stakeholders during incidents. |
|  | Post-Incident Analysis: Analyze incident details. | Examine the attack to understand vulnerabilities exploited and lessons learned for improvements. |
| Recover | System Restoration: Restore affected systems. | Return impacted systems to their normal operational state, ensuring data integrity. |
|  | Data Recovery: Restore data and assets. | Recover any data and assets that were impacted by the incident. |

| Aspect | Action | Description |
| --- | --- | --- |
| Type of Attack and Impacted Systems | Incident Classification: Identify the DDoS attack type (ICMP flood). | Understand the nature of the attack to inform response strategies. |
|  | Systems Assessment: Identify affected systems (network services offline). | Determine which systems were impacted and to what extent. |
| Protection Plan | Enhanced Firewall Rules: Strengthen firewall to handle ICMP floods. | Ensure firewall rules can handle and mitigate such attacks in the future. |
|  | Redundancy Planning: Implement backup systems for critical services. | Ensure continuous availability of critical services during attacks. |
| Detection Methods | Anomaly Detection: Employ network monitoring for abnormal patterns. | Monitor traffic patterns to identify deviations from normal behavior. |
|  | Intrusion Detection System: Use IDS to detect suspicious traffic. | Implement an IDS to identify potential attacks or unauthorized activities. |
| Response Plan | Incident Containment: Block incoming ICMP packets at firewall. | Immediately contain the attack by blocking the attack vector. |
|  | Communication Protocol: Establish communication channels for incidents. | Ensure a clear protocol for internal and external communication during incidents. |
|  | Malware Analysis: Investigate potential malware presence. | Analyze system logs and traffic data to detect signs of compromise. |
| Recovery Plans | System Restoration: Bring affected systems back online. | Recover systems and services to normal operation after the incident. |
|  | Data Integrity Check: Verify data integrity after the incident. | Ensure data was not compromised or altered during the attack. |
|  | Incident Report: Create a detailed report of the incident and response. | Document the incident, response actions, and lessons learned for future reference. |