**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

| **Summary** | The organization experienced a Distributed Denial of Service (DDoS) attack that disrupted network services for two hours. The attack involved a flood of ICMP pings through an unconfigured firewall, overwhelming the network. To address this, the cybersecurity team implemented new security measures. | | |
| --- | --- | --- | --- |
| Identify | The attack type is a DDoS attack involving ICMP packets. The affected systems included network resources and services, particularly those exposed to the internet. The incident primarily impacted internal network traffic. | | |
| Protect | To further secure the organization's assets, the following actions should be taken:   * Strengthen firewall configurations to block unwanted ICMP traffic and prevent firewall misconfigurations. * Enhance employee training on recognizing and responding to security incidents. * Develop data security policies to protect sensitive information. * Implement intrusion detection and prevention systems to filter out malicious ICMP traffic. * Continuously update and maintain protective technologies like firewalls and intrusion prevention systems. | | |
| Detect | To monitor and analyze network traffic and detect unusual activity, the organization should:   * Deploy security information and event management (SIEM) tools for real-time monitoring and alerting. * Continuously scan for anomalies and security events. * Establish a security continuous monitoring process to detect threats promptly. * Implement intrusion detection systems (IDS) to identify malicious ICMP traffic. | | |
| Respond | In response to future cybersecurity incidents, the organization should:   * Develop response plans tailored to specific incident types, including containment, eradication, and recovery strategies. * Establish clear communication procedures to disseminate incident information within the organization. * Analyze incident data to understand the attack's scope and impact. * Mitigate incidents by isolating affected resources. * Periodically review and update response procedures for improvements. | | |
| Recover | To recover from cybersecurity incidents, the organization should consider:   * Identifying critical resources and data to be restored first. * Continuously improving the recovery process to reduce downtime. * Establishing clear communication on the progress of restoration. | | |

| Reflections/Notes: |
| --- |