**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 flooded the internal network with ICMP packets, disrupting services for two hours. The attack exploited an unconfigured firewall, allowing the malicious traffic to enter. The incident was mitigated by blocking ICMP traffic, shutting down non-critical services, and restoring essential systems. Post-incident, new firewall rules, source IP verification, and enhanced monitoring tools were implemented. | | |
| --- | --- | --- | --- |
| Identify | Internal assets were affected included firewalls, internal servers, and network infrastructure. The unconfigured firewall was a critical gap that allowed the ICMP flood into the network. The attack made network audits and access privilege reviews necessary to ensure such misconfigurations are not repeated. The business processes involved impacted client services such as web design and marketing operations that rely on network availability. | | |
| Protect | Firewall rules were updated to limit incoming ICMP traffic and verify source IP addresses. Some other recommended changes should be, role-based access control (RBAC) to be enforced to limit who can alter network configurations. IT staff should undergo regular training to recognize and prevent misconfigurations. Network protection was enhanced through IDS/IPS systems and better firewall rule enforcement. Regular maintenance and audits of firewall and security appliances should be scheduled. | | |
| Detect | Network monitoring software was introduced to detect abnormal traffic patterns in real time. A SIEM tool or similar solution should be used to generate alerts on traffic spikes or unusual ICMP behavior. IDS/IPS tools are configured to detect and block suspicious ICMP traffic. Continuous monitoring ensures quicker detection and response in future events. | | |
| Respond | The organization responded by blocking ICMP packets and shutting down non-critical services to preserve resources. Incident response communications were coordinated internally to restore services. A root cause analysis confirmed the attack vector was an unconfigured firewall. Improvements include firewall configuration checklists and automated alerts for potential misconfigurations. | | |
| Recover | Critical services were prioritized and restored to operational status. Recovery plans now include scenarios for DDoS attacks and misconfigurations. Communication of recovery actions and system status was provided to all affected stakeholders. Lessons learned were documented to improve response and recovery protocols. | | |

| Reflections/Notes: |
| --- |