**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 multimedia company experienced a **Distributed Denial of Service (DDoS)** attack that disrupted internal network services for two hours. The attacker exploited a vulnerability in an **unconfigured firewall**, flooding the network with **ICMP packets**, which overwhelmed systems and made internal resources unreachable. The incident was mitigated by blocking incoming ICMP packets, shutting down non-essential services, and restoring critical operations. Post-incident, several network security measures were implemented to prevent recurrence. | | |
| --- | --- | --- | --- |
| Identify | To reduce future risk, we will conduct **regular security audits** of internal networks, systems, and firewall configurations. This includes reviewing access controls, verifying patch levels, and scanning for vulnerabilities. Identifying unconfigured or outdated security tools—like the firewall that allowed the ICMP flood—is critical to preventing such gaps. | | |
| Protect | **We will implement updated firewall policies that restrict unnecessary traffic, such as limiting ICMP packet rates and blocking unused ports. User training will be introduced to help employees recognize signs of DDoS activity or service slowdowns. Policies for secure configurations and change management will be reinforced to prevent future misconfigurations.** | | |
| Detect | We are enhancing visibility by deploying **network monitoring tools** and integrating **IDS/IPS systems** to detect abnormal traffic patterns and suspicious ICMP activity. These tools will help spot early signs of a DDoS attack and trigger alerts for faster response. | | |
| Respond | Our updated incident response plan includes procedures for **identifying and isolating DDoS traffic quickly**, blocking malicious IPs, and switching to backup services if needed. We will log all incidents and conduct **post-attack analysis** to understand the threat and improve our response tactics. | | |
| Recover | We will establish **system recovery procedures** that include restoring critical services first, followed by non-critical systems. Regular **data backups and service continuity plans** will be tested to ensure systems can be restored with minimal downtime after a DDoS or similar event. | | |

| Reflections/Notes: This DDoS attack revealed how a **single misconfigured component** (the firewall) can expose the entire network to disruption. While the response was effective, it highlighted the need for **proactive security configurations, early detection capabilities**, and **preparedness through planning and training**. Going forward, the organization must treat cybersecurity not just as a reactive measure, but as an ongoing, strategic priority. |
| --- |