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, a multimedia company, experienced a **Distributed Denial of Service (DDoS)** attack lasting two hours, causing network services to stop responding. The attack involved an incoming flood of **ICMP packets** that overwhelmed the network. The **vulnerability** was an **unconfigured firewall** that allowed the malicious traffic to pass through. The incident was resolved by blocking ICMP, taking non-critical services offline, and implementing new controls.
Identify	This function focuses on assessing the environment and risks * **Asset/System Affected:** The internal network and all critical and non-critical network services. The **unconfigured firewall** was the vulnerable system. * **Vulnerability:** Unrestricted access through an unconfigured firewall. * **Risk Identified:** High risk of network service disruption due to DDoS attack. **Action:** Implement a **mandatory audit** for all security controls and firewalls to ensure proper configuration before deployment.

Protect	**This function outlines safeguards to deliver services and mitigate threats.** *** Immediate Action: The team blocked incoming ICMP packets and took non-critical services offline.** *** Planned Protective Technology: The team implemented a new firewall rule to limit the rate of incoming ICMP packets and added Source IP address verification on the firewall to check for spoofed IP addresses.** *** Action: Implement an IDS/IPS system to filter ICMP traffic based on suspicious characteristics.** *** Action: Update the Information protection and procedures to include a mandatory configuration and peer-review process for all network security devices.**
Detect	This function defines activities to identify a cybersecurity event. * **Immediate Action:** Network services stopped responding, which was the initial indicator of the event. * **Planned Continuous Monitoring:** The team implemented **Network monitoring software** to detect abnormal traffic patterns. * **Action:** Configure the monitoring software to specifically **alert on spikes in ICMP traffic** and high connection rates, correlating the information with the new IDS/IPS system.
Respond	This function involves taking action regarding a detected incident. * **Response Planning:** The team's immediate actions (blocking ICMP, offlining services) should be formalized into a documented **DDoS Incident Response**

	Playbook. * **Analysis:** The cybersecurity team successfully investigated and determined the **Root Cause** (unconfigured firewall) and the attack vector (ICMP flood) . * **Mitigation:** The response team contained the incident by **blocking incoming ICMP packets** and **stopping all non-critical network services**. * **Improvement:** The "Lessons Learned" should update the firewall deployment checklist and configuration management process to prevent future misconfigurations.
Recover	This function focuses on restoring capabilities impaired during an incident. * **Recovery Planning:** The team successfully **restored critical network services** and then brought non-critical services back online. * **Communications:** The team must coordinate and communicate with stakeholders (internal staff, management) that all affected systems are fully restored to normal operation. * **Improvements:** Review the 2-hour downtime and look for ways (e.g., cloud-based DDoS scrubbing) to automate and speed up future recovery efforts

---

Reflections/Notes: This incident highlights the critical need for robust **configuration management** (Identify/Protect) and a thorough **Security by Default** approach. The vulnerability was not a sophisticated zero-day but a basic configuration failure, emphasizing that preventative controls are as important as detection and response measures. The successful analysis of the attack and the implementation of specific, relevant technical controls (ICMP rate-limiting, IP verification, IDS/IPS)

demonstrates the effectiveness of the *Respond* and *Protect* functions