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	A multimedia company specializing in web and graphic design, as well as social media marketing, encountered a severe network disruption. This was identified as a DDoS attack, executed through an overwhelming flood of ICMP packets. The company's incident management team responded by blocking these packets and temporarily disabling non-critical network services, allowing for the restoration of critical functions.
Identify	The attack was a targeted DDoS, executed via ICMP flooding. This compromised the company's entire internal network, necessitating immediate action to secure and restore all vital network resources.
Protect	In response, the cybersecurity team enacted enhanced firewall rules to restrict the influx of ICMP packets. Additionally, they deployed an Intrusion Detection and Prevention System (IDPS) to filter out suspicious ICMP traffic based on defined characteristics.
Detect	Enhancements were made to the firewall for source IP address verification, aimed at identifying and blocking spoofed IP addresses in incoming ICMP traffic. Network monitoring tools were also implemented to recognize and alert on abnormal traffic patterns.
Respond	For future incidents, the protocol involves isolating impacted systems to mitigate further network disruption. Critical systems and services will be prioritized for

	restoration. The team will conduct a thorough analysis of network logs for any anomalies and report the incident to upper management and, if necessary, legal authorities.
Recover	Post-attack recovery entails restoring network services to full functionality. Moving forward, external ICMP floods will be blocked at the firewall level. Non-critical network services will be suspended to reduce internal traffic, enabling a focus on restoring critical services first. Once the attack subsides, all systems and services can be progressively reinstated.

Reflections/Notes:

- During real attacks, things like NIST CSF will definitely be helpful to provide some structure in the middle of an otherwise chaotic situation.
- Technical response is necessary, but this drove home the importance of communication as well, not just for stakeholders but also for the team to keep the crisis calm and under control.
- Things to work on – network monitoring, scripting response tactics inside AWS Lambda, Azure Functions, to name a few.