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 company experienced a security incident when all network services became unresponsive. The cybersecurity team determined that the outage was caused by a distributed denial-of-service (DDoS) attack involving a flood of ICMP packets. In response, the team blocked the attack and temporarily suspended all non-critical network services to allow critical services to be restored.
Identify	A malicious actor or group launched an ICMP flood attack against the company, impacting the entire internal network. As a result, all critical network resources had to be secured and restored to proper operation.
Protect	The cybersecurity team introduced a new firewall rule to restrict the rate of incoming ICMP packets and deployed an IDS/IPS system to identify and filter ICMP traffic exhibiting suspicious behavior.
Detect	The cybersecurity team enabled source IP address verification on the firewall to identify spoofed IP addresses in incoming ICMP packets and deployed network monitoring tools to detect unusual traffic patterns.
Respond	Addressing future security incidents , the cybersecurity team will isolate any affected systems to contain the disruption. They will work to restore critical

	systems and services impacted by the event, then review network logs to identify suspicious or abnormal activity. The team will also report all incidents to upper management and, when necessary, to the appropriate legal authorities.
Recover	To recover from an ICMP flood DDoS attack, the priority is to restore network services to normal operation. Going forward, these types of ICMP floods can be mitigated by blocking them at the firewall. During an attack, non-essential network services should be taken offline to reduce internal traffic, allowing critical services to be restored first. After the flood of ICMP packets has subsided, all remaining non-critical systems and services can then be brought back online.

Reflections/Notes: This incident provided useful insights into network vulnerabilities and reinforced the importance of strong preventive and responsive security measures. Continued improvements in monitoring, documentation, and response planning will help the organization better handle similar situations in the future.