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's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Identify	The entire network was affected due to excessive ICMP traffic that saturated links and devices. The attack traffic appeared to come from spoofed sources, making the true origin unclear and reinforcing the need to understand what assets were exposed and where controls were missing.
Protect	Firewalls should be configured to limit and control ICMP, including basic rate-limiting at the edge. Source validation on the firewall helps weed out spoofed addresses, and broader monitoring, plus an IDS/IPS adds another layer that can automatically enforce simple protections.

Detect	SOC teams should remain on heightened alert and continuously watch inbound and outbound patterns for unusual spikes or anomalies. An IDS can complement this by flagging abnormal ICMP activity early so operators see issues before they escalate.
Respond	Keep current backups of critical systems and data so essential functions can be restored quickly. When something looks off, isolate the affected paths or services immediately to reduce impact while you stabilize the environment and verify configurations.
Recover	Use backups to bring services back in a deliberate order, with emphasis on core operations first. After stability returns, review what happened, keep necessary safeguards in place, and make small adjustments to prevent a repeat.

Reflections/Notes: Be alert, keep eyes on the basics, and treat configuration hygiene and monitoring as everyday habits rather than emergency steps.