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 suffered a DDoS attack where the internal network stopped responding due to a flood of incoming ICMP packets. This attack caused a disruption in normal network traffic and led to a two-hour downtime. The attack was traced back to a firewall misconfiguration, which allowed an attacker to overload the system. The cybersecurity team responded by blocking the malicious traffic, restoring critical services, and implementing additional protective measures.
Identify	The network was suddenly overwhelmed by an influx of ICMP packets, causing a complete disruption of network services. All critical network resources were affected, and the immediate priority was to isolate the attack and begin restoring functionality to the most crucial services. The team quickly identified the vulnerability in the firewall configuration that allowed the DDoS attack to succeed.
Protect	The team implemented several protective measures for internal assets, including a new firewall rule to limit the rate of incoming ICMP packets, source IP address verification, and an IDS/IPS system to filter out suspicious traffic based on specific characteristics.
Detect	Detection capabilities were enhanced by configuring network monitoring

	software to identify abnormal traffic patterns, as well as ensuring the firewall checked for spoofed IP addresses in incoming ICMP packets.
Respond	The team responded by isolating affected systems to prevent further disruptions, restoring critical network services, and analyzing network logs for abnormal activity. All incidents were reported to upper management and, if applicable, to legal authorities.
Recover	For recovery, the team restored network services to normal operation and implemented measures to block future ICMP flood attacks at the firewall. Non-critical services were brought back online once the ICMP flood subsided.

Reflections/Notes:

- The firewall misconfiguration was a critical vulnerability that allowed the DDoS attack to succeed. Future audits should prioritize identifying and addressing such vulnerabilities to strengthen network security.
- The response was effective in restoring critical services, but a quicker isolation of the affected systems could have reduced downtime and prevented further disruption.
- Implementing continuous monitoring and regularly updating the security infrastructure are essential steps to detect future threats more rapidly and ensure faster response times.