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 recently experienced a DDoS attack that disrupted internal network services for two hours. The attack involved a flood of ICMP packets, which overwhelmed the network, preventing normal traffic from accessing critical resources. The cybersecurity team eased the attack by blocking incoming ICMP packets, shutting down noncritical services, and restoring essential operations. A following investigation exposed that an unconfigured firewall allowed the attack to bypass security controls, highlighting an important vulnerability. To prevent future incidents, several security measures were implemented, including firewall rules, source IP verification, network monitoring, and an IDS/IPS system.
Identify	Regular security audits of internal networks, systems, and firewalls are needed to identify vulnerabilities that could be exploited in future attacks. In this case, an unconfigured firewall left the network exposed to malicious ICMP traffic, letting the attack succeed. Implementing periodic risk assessments and penetration testing can help uncover security gaps before they are exploited.
Protect	To mitigate the risk of similar attacks, the company has strengthened its firewall configurations by limiting the rate of incoming ICMP packets and implementing source IP address verification to filter out spoofed traffic. Moreover, security awareness training for employees can help reinforce best practices for securing internal assets, ensuring that proper configurations are maintained.

Detect	The cybersecurity team has deployed network monitoring software to detect abnormal traffic patterns that may indicate a DDoS attack in progress. The implementation of an IDS/IPS allows for real-time filtering of suspicious ICMP traffic, improving the company's ability to detect and respond to threats before they escalate.
Respond	The company's incident response plan includes blocking malicious traffic, shutting down non-critical services, and restoring essential network functions during an attack. Future improvements include automated response mechanisms that can dynamically adjust firewall rules and traffic filters in real-time to contain threats more efficiently.
Recover	After containing the attack, the organization restored affected systems and reinforced security controls to prevent recurrence. Moving forward, regular incident response drills and system backups will ensure a swift recovery process and minimize downtime in the event of future cyber threats.

Reflections/Notes: This incident shows the importance of proactive security measures, including firewall configuration, traffic monitoring, and a well-defined response strategy. By continuously improving detection and response capabilities, the company can strengthen its network resilience against future cyber threats.