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 organisation experienced a DDoS attack, which compromised the internal network for two hours. The organisation's network services suddenly stopped responding due to an incoming flood of ICMP packets. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	A malicious attacker specifically targeted the company with an ICMP flood attack, which impacted the entire internal network, causing network resources to be inaccessible. The team found that the flood of ICMP pings was sent into the company's network through an unconfigured firewall. The immediate focus of the team was to secure and restore all critical network resources to normal functionality. Network analysis tools such as Wireshark could also be used to analyse traffic and confirm excessive ICMP requests.
Protect	To enhance protection measures, the network security team added a new firewall rule to limit the rate of incoming ICMP packets. Moreover, an IDS/IPS system would be installed to filter out some ICMP traffic based on suspicious characteristics.
Detect	Implementing source IP address verification on the firewall for incoming ICMP packets became a critical detection enhancement. Network monitoring

	software was also installed to detect abnormal traffic patterns.
Respond	In preparation for future security events, the cybersecurity teams outlined a proactive response plan. This plan could include incident response playbooks, real-time monitoring through SIEM tools. It can also involve isolation of affected systems to contain and prevent further network disruption, restoring disrupted critical systems and services, Network logs, firewall logs, endpoint activities and reports from SIEM can also be used for suspicious activity and promptly reporting incidents to upper management and legal authorities if necessary. Conducting post-incident reviews to identify gaps and vulnerabilities, implementing automated threat detection and increasing employee training on cybersecurity awareness can also greatly improved organisation's ability to react to future security events.
Recover	To recover from a DDoS attack involving ICMP flooding, the company will restore access to network services to a normal functioning state. Future external ICMP flood attacks will be blocked at the firewall, followed by the temporary idling of non-critical network services to reduce internal traffic. Critical network services will be prioritised for restoration, and once the ICMP packet flood subsides, non-critical network systems and services can be brought back online. Details such as the root cause of the incident, affected systems, timeline of attack, backup data is crucial for rapid recovery. In the event of confusion, organizations can rely on disaster recovery and business continuity plans set up previously. These plans must be regularly tested to ensure minimal downtime and data integrity during restoration.

Reflections/Notes: