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 faced a security incident characterized by a sudden halt in all network services. Upon investigation, the cybersecurity team identified the disruption as a result of a distributed denial of service (DDoS) attack involving an overwhelming influx of ICMP packets. In response, the team mitigated the attack by implementing blocks and temporarily suspending non-essential network services, allowing for the restoration of critical network functions.
Identify	The company experienced a targeted ICMP flood attack, impacting the entire internal network. Immediate action was taken to secure and restore critical network resources to normal functioning.
Protect	The cybersecurity team deployed a proactive approach by introducing a new firewall rule to restrict the rate of incoming ICMP packets. Additionally, an IDS/IPS system was implemented to filter out ICMP traffic exhibiting suspicious characteristics, enhancing the overall security measures.
Detect	The cybersecurity team added a check on the firewall to verify the source IP addresses of incoming ICMP packets, preventing spoofed addresses.

	They also set up monitoring software to quickly spot and address any unusual traffic patterns.
Respond	In future security events, the cybersecurity team plans to isolate affected systems to prevent ongoing network disruption. Their focus will be on restoring critical systems and services that were impacted. Additionally, the team will analyze network logs for signs of suspicious activity. All incidents will be reported to upper management and, if necessary, to relevant legal authorities.
Recover	To recover from an ICMP flooding DDoS attack, restoring normal functioning to network services is crucial. In the future, external ICMP flood attacks can be thwarted at the firewall. Following that, stopping non-critical network services minimizes internal traffic. Prioritizing, critical network services are restored first. Once the ICMP packet flood subsides, non-critical network systems and services can be gradually brought back online.

Reflections/Notes:
The cybersecurity team adeptly addressed an ICMP flooding DDoS attack, employing measures such as source IP verification and network monitoring. Their recovery plan involves isolating affected systems, prioritizing critical service restoration, and gradually reinstating non-critical systems. This approach demonstrates a balanced strategy of prevention, response, and continuous improvement. The decision to block external ICMP flood attacks at the firewall showcases a proactive mindset. Overall, the team's actions reflect a commitment to maintaining a robust security posture against future threats