Incident report analysis (DDoS Attack)

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 experienced an ICMP flood attack on their internal network servers. The cybersecurity team found the DDoS attack and responded by blocking incoming ICMP flood packets. All non-critical services were turned off and systems were restored after the incident.
Identify	Hackers target the organization with ICMP flood attack. The organization's internal network was affected. All important resources need to be secured and restored.
Protect	New firewalls were implemented to limit the rate of incoming ICMP packets. IDS/IPS is now being utilized to filter out malicious ICMP packets.
Detect	Source IP address verification has been implemented on the firewall to identify if a potential IP address is being spoofed.
Respond	In future instances the cybersecurity team will isolate affected systems, restore any important systems and services. Analysis will be done on network logs to identify suspicious activity. All incidents will be reported to the proper authorities.
Recover	To recover from DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. Future external ICMP flood

	attacks will be blocked by the firewall. All non-critical network services will be turned off to reduce traffic. Critical services will be restored. Once all flood ICMP packets have been timed out, other systems can be turned back on.

Reflections/Notes: