Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or just to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to continue practicing applying the NIST CSF framework to different situations you may encounter.

Summary	The moment all network services abruptly ceased responding, the business experienced a security incident. The distributed denial of service (DDoS) assault that the cybersecurity team discovered was responsible for the outage was launched via an influx of ICMP packets. In order to restore important network services, the team replied by blocking the attack and halting all non-critical network services.
Identify	An ICMP flood assault was used to target the company by a malicious actor or actors. The internal network as a whole was impacted. It was necessary to secure and reactivate all crucial network resources.
Protect	The cybersecurity team set up an IDS/IPS system to filter out some ICMP traffic based on suspicious features and a new firewall rule to lower the volume of incoming ICMP packets.
Detect	The firewall's source IP address verification feature was set up by the cybersecurity team to check for spoof IP addresses in incoming ICMP packets. Network monitoring software was also put into place to look for unusual traffic patterns.
Respond	The cybersecurity team will isolate impacted systems in the case of future

	security incidents to stop further network damage. Any vital systems and services that were interfered with by the incident will be attempted to be restored. The team will then examine network logs to look for unusual or suspicious behavior. Additionally, the team will notify top management and, if necessary, the relevant legal authorities of every incidence.
Recover	It is necessary to return network service access to its pre-attack condition in order to recover from a DDoS assault by ICMP flooding. Future ICMP flood attacks from outside can be stopped at the firewall. Then, to lower internal network traffic, all non-critical network services should be terminated. Next, it is best to start restoring essential network services. Finally, all non-critical network systems and services can be restarted once the flood of ICMP packets has timed out.

Reflections/Notes: