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 company's network services suddenly stopped responding. The cybersecurity team found that this was caused by a distributed denial of services (DDoS) attack through a flood of ICMP packets. The team responded by blocking the attack and stopping all non-critical network services in order to restore all critical network services.
Identify	A malicious actor/actors attacked the company with an ICMP flood. The entire internal network was affected—all of the critical network resources needed to be secured and restored.
Protect	The cybersecurity team incorporated a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out suspicious ICMP traffic.
Detect	The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and used network monitoring software to detect abnormal traffic patterns.
Respond	In the future, the cybersecurity team will isolate affected systems to prevent further spread to the network. They will attempt to restore any critical systems and services disrupted by the event. The team will then analyze network logs

	to check for suspicious/abnormal activity. They will also report all incidents to upper management and appropriate legal authorities.
Recover	In order to recover from a DDoS attack by ICMP flooding, the access to network services needs to be restored to a normal state. In the future, external ICMP flood attacks can be stopped at the firewall. Then, all non-critical network services can be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets has timed out, all non-critical network systems and services can be brought back online.