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	A security event occurred when network services ceased responding. Investigation revealed a distributed denial of services (DDoS) attack through ICMP packet flooding. The cybersecurity team responded by blocking the attack and temporarily suspending non-critical network services to restore critical ones.
Identify	The incident involved malicious actors targeting the company with an ICMP flood attack, affecting the entire internal network. The primary objective became securing and restoring all critical network resources to operational status.
Protect	The cybersecurity team implemented enhanced protection measures, including new firewall rules to restrict incoming ICMP packets and an IDS/IPS system to filter suspicious ICMP traffic based on specific characteristics.
Detect	Detection capabilities were improved by configuring source IP address verification on the firewall to identify spoofed IP addresses in incoming ICMP packets. Network monitoring software was also implemented to identify unusual traffic patterns.
Respond	The response plan for future events includes isolating affected systems to

	prevent network disruption, prioritizing critical system restoration, analyzing network logs for suspicious activity, and reporting incidents to management and relevant authorities when necessary.
Recover	Recovery from DDoS attacks involves several steps: blocking external ICMP flood attacks at the firewall, temporarily halting non-critical network services, prioritizing critical service restoration, and finally reinstating non-critical systems once the ICMP packet flood subsides.

Reflections/Notes: