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 abrupt failure of all network services resulted in a security event for the company. Through a deluge of inbound ICMP packets, the cybersecurity team discovered that the outage was caused by a distributed denial of services (DDoS) attack. In order to restore important network services, the team retaliated by halting all non-essential network services and thwarting the attack.
Identify	An ICMP flood attack was launched against the company by a malicious actor or actors. It impacted the whole internal network. It was necessary to secure and return all vital network resources to operational status.
Protect	In order to control the amount of incoming ICMP packets, the cybersecurity team created a new firewall rule. They also installed an IDS/IPS system to filter out some ICMP traffic based on suspicious features.
Detect	In order to detect fake IP addresses in incoming ICMP packets, the cybersecurity team set up source IP address verification on the firewall. They also installed network monitoring software to identify unusual traffic patterns.
Respond	The cybersecurity team will isolate impacted systems in the case of future security events to stop additional network damage. They'll make an effort to

	restart any crucial services or systems that the incident interrupted. After that, the group will examine network logs to look for unusual or suspicious activity. All occurrences will also be reported by the team to higher management and, if necessary, the relevant legal authorities.
Recover	Restoring regular working network service access is necessary to recover from an ICMP flooding DDoS attack. External ICMP flood attacks may be prevented at the firewall in the future. In order to minimize internal network traffic, all non-essential network services ought to be terminated. The next step is to restore essential network services initially. Finally, all non-critical network services and systems can be restarted after the barrage of ICMP messages has timed out.

Reflections/Notes: