Incident report analysis

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 company encountered a security incident where all network services abruptly became unresponsive. The cybersecurity team identified the cause as a distributed denial-of-service (DDoS) attack, which overwhelmed the network with a flood of ICMP packets. In response, the team mitigated the attack by blocking the malicious traffic and temporarily halting non-essential network services to prioritize the restoration of critical services.
Identify	A malicious actor or actors targeted the company with an ICMP flood attack. The entire internal network was impacted, necessitating the securing and restoration of all critical network resources to ensure they returned to a functional state.
Protect	The security team implemented a new firewall rule to limit the incoming ICMP packets and IDS/IPS system to filter out some ICMP based on suspicious characteristics.
Detect	The cybersecurity team configured source IP address verification on the firewall to filter out spoofed IP addresses in incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.

Respond	In the future, the security team needs to isolate affected systems to prevent the other part of the network. They will try their best to restore any critical systems or services that were disrupted. Then, it is necessary to analyze network logs to see whether there are any suspicious or abnormal activities. The team will also report all incidents to upper management and, if applicable, notify the appropriate legal authorities.
Recover	To recover from a DDoS attack caused by ICMP flooding, restoring access to network services to their normal functioning state is crucial. In the future, such attacks can be mitigated by blocking external ICMP flood traffic at the firewall. During an attack, non-critical network services should be temporarily halted to reduce internal network congestion. The focus should then be on restoring critical network services first. Once the flood of ICMP packets subsides, non-critical network systems and services can be gradually brought back online.

Reflections/Notes: