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	There was a security incident at the company which caused the entire network to stop functioning. In response to this, the Cybersecurity team discovered that the attack was a distributed denial of service (DDoS) , specifically the excess flood of incoming ICMP packets. The team resolved the situation by blocking the attack and stopping all non-critical network services, so that critical services could be restored properly.
Identify	The organization was attacked by a threat actor or actors through the means of ICMP attack. This incident affected the organization's critical network resources and needed it to be protected and restored to a normal state.
Protect	The cyber team set up a network monitoring detection system for abnormal traffic patterns, a new firewall rule to limit the rate of incoming ICMP packets, and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The network monitoring detection system will be used to detect abnormal traffic patterns and the firewall system has been configured to alert for spoofed IP addresses on incoming ICMP packets.
Respond	For future security events, the cybersecurity team will isolate affected systems

	to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	DDoS attacks can be overwhelming, especially to identify the type of attack being used by the attacker. To recover from an ICMP flooding attack, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: