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 experienced a security event when all network services sudde stopped responding. The cybersecurity team found the disruption was caus by a distributed denial of services (DDoS) attack through a flood of incomin ICMP packets. The team responded by blocking the attack and stopping all critical network services, so that critical network services could be restored.
Identify	A malicious actor or actors targeted the company with an ICMP flood attack entire internal network was affected. All critical network resources needed t secured and restored to a functioning state.
Protect	The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traf based on suspicious characteristics.
Detect	The cybersecurity team configured source IP address verification on the fire to check for spoofed IP addresses on incoming ICMP packets and impleme network monitoring software to detect abnormal traffic patterns.
Respond	For future security events, the cybersecurity team will isolate affected syste prevent further disruption to the network. They will attempt to restore any cri systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The tea will also report all incidents to upper management and appropriate legal authorities, if applicable.

Recover	To recover from a DDoS attack by ICMP flooding, access to network service need to be restored to a normal functioning state. In the future, external ICM 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 b brought back online.

Reflections/Notes: