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	Our organization experienced a DDoS attack which compromised the internal network for two hours until it was resolved. The organization's network services stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. Our incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline and restoring critical network services.
Identify	This was undoubtedly an ICMP flood attack, which is further categorized as a denial of service attack. Here it was more extensive, being a distributed denial of service attack (DDoS), the difference between the two is that distributed is of a larger scale and has multiple devices/attack vectors behind it. The network was the primary system affected in this attack.
Protect	To address this security event, the network security team implemented both: 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	As for future proofing against similar security incidents, the team implemented Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and network monitoring software to detect abnormal traffic patterns.

Respond	The cybersecurity team will isolate affected systems first in future security events going forward. Any critical services and systems will be prioritized to be brought back into standard operating procedure as swiftly as possible. The team will then analyze network logs to determine if there is still suspicious and/or abnormal behavior being detected. Lastly, the event will be communicated to the proper channels of command, including legal authorities should it fall under their purview.
Recover	Recovering from the ICMP flood attack begins with the restoration of network services to the prior normal functioning state. All non-critical network services will be shut down to facilitate a lighter load on internal network systems, following that, critical network services will be restored first. Upon successfully handling the security event, all remaining services and systems should be green-lit to go back online.