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 experienced a moment where all the networks stopped working. The cybersecurity team found the disruption was caused by a distributed Denial of Service (DDOS) attack which caused a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network services, to then restore functions later on.
Identify	A malicious actor or many actors targeted the company by flooding the network with ICMP packets. The entire internal network was damaged and needed to be secured and restored to a baseline.
Protect	The cybersecurity team implemented a new firewall rule to limit future ICMP packets and an IDS system to filter out suspicious ICMP packets from now on.
Detect	The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on any incoming ICMP packets. Also it should now detect patterns of abnormal traffic.
Respond	From now on the cybersecurity team will isolate affected systems to prevent further disruption to the network. From there they will restore critical systems and services. Then the team will analyze the network for abnormal activity. Finally report the issue to management.

Recover	To recover from any DDOS attack by ICMP flooding, access the network services must be restored to the normal baseline state. For the future any ICMP attacks can be blocked by a firewall configured to track abnormal behavior. All non-critical networks should be stopped to reduce the traffic present and then restored. After the excess ICMP packets left you can restore the entire network services.

Reflections/Notes: