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	When all network services went down the company experienced a security event. The cybersecurity team found that the incident was caused by a DDoS attack through a flood of incoming ICMP packets.
Identify	The company was targeted by a malicious flood attack. Every internal network was affected.
Protect	A new firewall rule to limit incoming packets has been implemented by the cybersecurity team
Detect	The cybersecurity checked for spoofed IP addresses by configuring source IP.
Respond	In the future to prevent another incident the cybersecurity team will isolate affected systems
Recover	To recover from the attack access to the network services need to be restored to a normal functioning state.

Reflections/Notes: