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 company recently underwent a security attack which was later identified as a DDoS ICMP flood attack. During the attack, the flood of ICMP packets caused the network services to briefly stop. This was stopped by the cybersecurity team by blocking the attack
Identify	A threat actor used an ICMP flood attack. The internal network was affected and operations stopped because of the traffic overflow
Protect	A new firewall rule was set to limit the rate of incoming ICMPs. The firewall was also configured to check for spoofed IP addresses. Additionally, network monitoring software to detect abnormal traffic patterns was implemented. And lastly, an IDS/IPS system to filter out some ICMP traffic was added
Detect	To detect this type of issue again, the firewall was configured to check for spoofed IP addresses on incoming packets. There was also the addition of network monitoring software
Respond	For future events, the cybersecurity team will isolate affected systems to prevent spread and disruption to the network. The team will analyze network logs to check for malicious behavior. All incidents will also be reported
Recover	In order to recover from the DDoS attack, access to network services needs to

	be restored to a functioning and secure state.

Reflections/Notes: