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 organization has faced DDoS attacks with a flood of ICMP packets sent from a malicious actor through an unconfigured firewall. During the attack, normal internal network traffic couldn't access any network resources. The security team responded to this attack by implementing new firewall rules that block suspicious ICMP packet sources, and network monitoring software to check for abnormal traffic patterns.
Identify	The type of attack was a DDoS attack with a flood of ICMP packets. This attack overwhelms the organization's internal network which then causes it to slow down responses and eventually shuts it down.
Protect	To prevent further damage from happening, block all the sources of ICMP packets and shutdown the system temporarily. Then focus on updating the firewall later after stopping the flooding.
Detect	To detect future DDoS or similar attacks in the future, intrusion detection system should be implemented and the security team should check the logs regularly for suspicious activities and take action when needed.
Respond	If suspicious activity has occurred while analysing the logs or detected by the intrusion detection system, the security team should block all the IP addresses

	the activity is coming from and reimplement a new firewall rule that blocks the same IP addresses. If the situation is worse, then shut down the internal network immediately and repeat the step from identify.
Recover	To recover from the potential incident, backup all important files and information so that the data will be in less risk of being lost in the future attacks.

Reflections/Notes: I have checked my work with the completed exemplar and learnt that I could have included on the detect section how the firewall could be implemented to filter out suspicious or spoofed IP addresses.