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 recently experienced a DDoS attack, compromising the internal network for about 2 hours. This was caused by a malicious actor who flooded ICMP packets into the network traffic, which caused the network services to stop responding. The cybersecurity team investigated the event and found out the actor flooded the ICMP packets through an unconfigured firewall. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored.
Identify	The cybersecurity team investigated the event and checked the logs from the network server. They found out that a malicious actor had flooded ICMP pings to the company's network through an unconfigured firewall. This caused the network's services to not respond to any requests. All critical network resources needed to be secured and restored to a functioning state.
Protect	The team implemented several solutions to protect the company from future attacks. A new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter ICMP traffic based on suspicious characteristics.
Detect	To ensure that signs of attacks can easily be detected, the team will make use of the new network monitoring software (e.g. SIEM) to detect suspicious

	traffic patterns. The team also configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
Respond	The cybersecurity team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. In the future, the team will have to isolate affected systems to further prevent disruption on unaffected ones. The team will have to analyze network logs and check for any abnormal activities. Upper management will be informed of the event.
Recover	The team will restore all critical network services after the actor is unable to flood the network with ICMP packets. In the future, the firewall will be able to block suspicious floods of ICMP packet requests. All non-critical network services need to be temporarily stopped to reduce internal network traffic. Prioritise recovering critical network services the most. When the flooding has stopped, all services can be restored and brought back online again.

Reflections/Notes: