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's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The organization experienced a DDoS attack, which compromised the internal network for 2 hours until it was resolved. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. It allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Protect	The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	Configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	Will isolate affected systems to prevent further disruption to the network and will attempt to restore any critical systems and services that were

	disrupted by the event. Then, they will analyze network logs to check for suspicious and abnormal activity.
Recover	Access to network services need to be restored to a normal functioning state. External ICMP flood attacks can be blocked at the firewall. Non-critical network services should be stopped to reduce internal network traffic and critical network services should be restored first.

Reflections/Notes: