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 Distributed Denial of Service (DDoS) attack, which compromised the internal network for two hours until it was resolved. During the attack, the organization network service suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources.
Identify	The company cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through a distributed denial of service (DDoS) attack.
Protect	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Detect	To address this security event, the network security team implemented. 1. A new firewall rule to limit the rate of incoming ICMP packets. 2. Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. 3. Network monitoring software to detect abnormal traffic patterns. 4. AN IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.

Respond	In response to this breach, the cybersecurity team has provided training to employees on how to configure a firewall to set rules to how much ICMP traffic is allowed and what type of sourcer IP address to allow to come through. The team will monitor network logs, and inform all upper management of all incidents and inform legal authorities, if applicable.
Recover	The team will use the company's last known backup stored on the cloud before the attack occurred to restore lost data from the attack.

Reflections/Notes: