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	Yesterday, a Distributed Denial Of Service(DDOS) attack was experienced by the organization for around two hours. During the attack, the normal internal network traffic could not access any network resources. The attack was an ICMP flood attack which suddenly stopped organization's network services. The malicious attacker was able to send a flood of ICMP pings into the company's network through an unconfigured firewall and overwhelm the entire network.
Identify	The company's 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 an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Protect	To address this security event, the network security team implemented: ● A new firewall rule to limit the rate of incoming ICMP packets ● Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets ● Network monitoring software to detect abnormal traffic patterns ● An IDS/IPS system to filter out some ICMP traffic based on suspicious

	characteristics
Detect	To detect these types of attacks in the future, we will be making sure all the firewalls are updated and configured properly. Firewalls rules will be updated to detect and filter abnormal traffic patterns.
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. Management will also need to inform law enforcement and other organizations as required by local laws.
Recover	The attack has been stopped and various steps like reconfiguring firewall, updation of rules has been performed to recover from the damage incurred. The internal network has been restored to perform operations without interruptions.

Reflections/Notes: