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, which compromised the internal network for two hours. 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.
Identify	The cybersecurity team then investigated the security incident by analyzing the DNS and ICMP traffic log and 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 incident, the network security team implemented the following: - 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(Wireshark) - An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.

Detect	To detect new ICMP flooding attacks in the future, the team will monitor the network live using a Wireshark traffic log. The team will also implement a new firewall rule as well as using IDS/IPS to monitor all incoming traffic from the internet.
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. The firewalls will now be configured to block external ICMP flood attacks.Then all non-critical network services should be stopped to reduce internal network traffic. Critical network services should be restored first. Once the flood of ICMP packets has timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: