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.

Scenario

Review the scenario below. Then complete the step-by-step instructions.
You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.
During the attack, your 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 incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
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.
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

Summary	The company was the target of a DDoS attack which compromised the internal network for 2 hours resulting in internal network traffic being unable to access network resources. The incident management team was able to block the incoming flood of ICMP packets, restoring critical network services. The preliminary investigation has identified an unconfigured firewall as the avenue of attack that allowed the threat actor(s) to overwhelm the company's network using a distributed denial of service attack.
Identify	The cybersecurity team identified the weak point as an unconfigured firewall, allowing a flood of ICMP packets to use up all available network resources, effectively shutting down the internal network until they could be blocked.
Protect	The cybersecurity team has implemented several security measures to harden network security and reduce the attack surface of the network as a whole. The firewall has been configured to limit the rate of incoming ICMP packets.
Detect	A verification process has been introduced to verify the source IP address and check for spoofed IP addresses on inbound ICMP packets. Network monitoring software has been installed to detect abnormal patterns in network traffic.
Respond	An intrusion detection and prevention system has been introduced to filter out some ICMP traffic that matches a criteria for suspicious traffic.
Recover	Critical network services were restored after blocking the ICMP packets and stopping all non-critical network services offline.

Reflections/Notes: