Incident report analysis

Presented Scenario (From Google’s Cybersecurity Certificate Program)

“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 multi-media company has experienced a DDoS attack which compromised the internal network for 2 hours. The organization’s internal network suddenly stopped responding after receiving an incoming flood of ICMP packets rendering the network disconnected from any external network access. In order for critical network services to be brought back online the team responded by blocking the attack and ceasing all non-critical network services.
Identify	It was found that a malicious actor had sent a flood of ICMP pings through an unconfigured firewall. Any critical network resources downed during the attack must be restored to proper functionality.
Protect	The security team implemented a new firewall rule to limit the amount of incoming ICMP packets. . The team also implemented an IDS system to notify of any suspicious ICMP traffic on the network.
Detect	The security team has installed a new software to facilitate better detection response on the network. The team also reconfigured the firewall to check for spoofed IP addresses on incoming packets thereby verifying the authenticity of source IP addresses.
Respond	In the event that another DDoS attack occurs, the team has plans in place to isolate all affected systems while ensuring all critical services remain online or are returned online. Any further suspicious activity logged by the detection system will be reported to upper management.
Recover	Going forward the firewall now has more refined configurations in place and should help to prevent any ICMP flood attacks at present and in the future. However, it will be safe practice to limit all network activity to critical services until the attack ceases.

In this portfolio project I have demonstrated a thorough knowledge of the NIST Cybersecurity Framework, along with the ability to communicate concisely and effectively, and a technical understanding of a specific instance of a DDoS attack (in this case, an ICMP flood attack). The scenario was presented by Google's Cybersecurity Certificate program but all information within the framework table was written by me.