Incident report analysis

Summary	In the early hours of this morning, an employee promptly informed the IT department about their inability to utilize the organization's network infrastructure. In response to this report, a thorough examination of the network log records was conducted. The investigation revealed compelling evidence pointing to the deliberate involvement of a malicious entity, who orchestrated a disruptive assault on the network by unleashing a substantial influx of ICMP (Internet Control Message Protocol) packets.Furthermore he source IP address associated with the attack exhibited constant variation, indicating a dynamic and changing source. This conspicuous behavior strongly implies that the organization had fallen victim to a Distributed Denial of Service (DDoS) attack, a nefarious strategy employed to overwhelm and impede network operations.
Identify	In the aftermath of the Distributed Denial of Service (DDoS) attack, the incident management team embarked on an extensive security audit that encompassed a comprehensive evaluation of the organization's entire system, devices, and implemented policies. This meticulous examination aimed to identify and assess potential vulnerabilities that could be exploited by malicious actors to execute similar attacks in the future. During the course of the audit, a notable deficiency in the organization's system infrastructure came to light—a lack of a robust firewall capable of effectively managing and regulating the influx of incoming Internet Control Message Protocol (ICMP) packets. This particular weakness left the network vulnerable to an overwhelming surge of ICMP traffic, thereby providing an opportunity for the threat actor to capitalize on this vulnerability and successfully orchestrate the DDoS attack. The repercussions of this attack were evident as the organization's network endured a

	debilitating downtime lasting for a period of two hours. Throughout this duration, the normal flow of internal network traffic was severely disrupted, rendering the workforce unable to access critical network resources. This disruptive impact impeded routine operations and inflicted a considerable blow to employee productivity. It serves as a stark reminder of the pressing need to promptly address identified vulnerabilities and reinforce network defenses to effectively mitigate the occurrence of such incidents in the future.
Protect	In order to proactively safeguard against potential future attacks of a similar nature, the cybersecurity team undertook a series of pertinent measures. These included the implementation of a new firewall rule specifically designed to restrict the rate of incoming ICMP packets, thereby mitigating the risk of network saturation and subsequent disruption. Furthermore, to address the concern of spoofed IP addresses associated with incoming ICMP packets, the team introduced a source IP address verification mechanism within the firewall. This verification process aims to scrutinize and authenticate the legitimacy of IP addresses, preventing the utilization of false or manipulated source addresses. To enhance overall network surveillance, the team deployed specialized network monitoring software. This software is equipped to detect and identify abnormal traffic patterns that could potentially indicate malicious activity, providing the organization with real-time visibility into any anomalies within the network environment. Additionally, an Intrusion Detection System/Intrusion Prevention System (IDS/IPS) was implemented as an added layer of defense. This system leverages its capability to analyze and filter ICMP traffic based on discernible suspicious characteristics, effectively thwarting potentially harmful packets and augmenting the overall network security posture. By implementing these comprehensive measures, the cybersecurity team aims to bolster the organization's resilience against future threats, ensuring the network remains fortified and capable of promptly mitigating any potential DDoS attacks or similar security incidents.
Detect	In order to detect and mitigate potential future incidents of a similar nature, the cybersecurity team diligently deployed network monitoring software. This specialized software was strategically implemented to actively monitor and scrutinize the network's traffic patterns, with a primary focus on identifying any irregular or anomalous activities.
Respond	

	Upon detecting the threat, the organization swiftly assembled a team of security analysts who conducted a thorough investigation, confirming the severity of the risk to the network infrastructure. To contain the threat, the organization intentionally shut down the network for two hours, allowing the team to discuss and devise preventive strategies. During this time, they identified attack vectors and vulnerabilities, leading to the implementation of enhanced security controls, advanced threat detection mechanisms, strengthened access controls, and incident response protocols. These proactive measures demonstrate the organization's commitment to maintaining a robust security posture and safeguarding its network, assets, and sensitive information from potential breaches.
Recover	Due to early detection, the threat was promptly addressed, resulting in no data compromise. Additionally, the duration of the network downtime was relatively short, which minimized the need for extensive recovery measures. Nevertheless, in order to reassure employees and instill confidence in the organization's security measures, a meeting was conducted. During this meeting, the employees were informed that their data remained secure throughout the incident and that appropriate preventive measures had been implemented to mitigate the risk of future threats. The purpose of this meeting was to provide reassurance and ensure that employees were well-informed about the protective measures in place to safeguard their data and maintain a secure network environment.

Reflections/Notes: