Incident Report Analysis

Scenario:

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.

Summary	Our multimedia company, which specializes in web design, graphic design, and social media marketing services for small businesses, experienced a significant operational disruption due to a Distributed Denial of Service (DDoS) attack, later identified as an ICMP Flood. The incident affected internal network connectivity and lasted approximately two hours from the time of alert. The flood of ICMP packets targeted our network firewall, overwhelming it and rendering services temporarily unavailable. This exploit was made possible by a misconfigured and

	vulnerable firewall rule that had previously gone unresolved. The threat actor leveraged this weakness to inundate our systems with traffic, ultimately forcing a suspension of internal services and external communications until mitigation steps were taken. In response to the attack, our security team implemented a series of containment and recovery measures. In response, our security team implemented a series of containment, remediation, and long-term defense measures. Initially, all incoming ICMP packets were blocked to stop the attack and establish a clean environment for analysis. Non-critical network services were moved offline to limit further exposure, aligning with our Business Continuity strategy, commitment to least-invasive remediation, and focus on minimizing impact. As part of remediation, the team implemented a new rate-limiting firewall rule for ICMP traffic, enabled source IP address verification to detect spoofing, deployed network monitoring tools to identify abnormal traffic patterns, and configured an IDS/IPS system to filter ICMP traffic with suspicious characteristics. Once the threat was neutralized and our new safeguards were in place, critical services were safely restored, ensuring a secure and efficient return to full operations. For future security incidents like this, a workbook was created to carry out any and all identification, protection, detection, remediation & response steps.
Identify	WHO: Our multimedia company that provides web design, graphic design, and social media marketing solutions & services for small businesses was affected. Our operations were down and the specifically affected operations were our internal network connections. WHAT: Our services were affected by a Distributed Denial of Service attack. After further investigation it was determined to be caused by an

	ICMP Flood. WHEN: Timeframe for this incident was 2 hours from the time of alert. WHERE: Our Network firewall received a flood of ICMP packets from the threat actor. WHY: This was all due to a misconfigured and vulnerable firewall rule that went unresolved. HOW: This vulnerability was exploited by the threat actor and hence sent the flood of packets that overwhelmed our systems, causing us to stop services and communications for 2 hours.
Protect	In order to protect our operations from further attack we completed the following: - We blocked all incoming ICMP packets in efforts to stop the attack so that we could go in and clean up. - We also stopped all non-critical network services and moved them offline. Our focus was based on the principles of Business Continuity and least invasive remediation possible.
Detect	During the investigation we determined there was a vulnerable firewall that allowed this excess traffic through unconditionally.
Respond	As a response, our security team remediated 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 - An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Recover	Finally, we restored critical network services that had been taken offline.

	For future security incidents like this, a workbook was created to carry out any and all identification, protection, detection, remediation & response steps.

Reflections/Notes:

- Summarize the security event
- Identifies the type of attack and the systems impacted by the incident
- Offers a protection plan against future cybersecurity incidents
- Describes detection methods that can be used to identify potential cybersecurity incidents
- Includes a response plan for the cybersecurity incident and outline for future cybersecurity incidents
- Outlines recovery plans you and the organization can implement in future cybersecurity incidents.
- Focus on:
    - **Identify** security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
    - **Protect** internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
    - **Detect** potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
    - **Respond** to contain, neutralize, and analyze security incidents; implement improvements to the security process.
    - **Recover** affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.