Incident report analysis

Instructions

Summary	A multimedia company specializing in web and graphic design, and social media marketing services, recently faced a Distributed Denial of Service (DDoS) attack that disrupted their internal network for two hours. During the attack, their network services became unresponsive due to a massive influx of ICMP packets. Immediate actions were taken by their incident management team, including blocking incoming ICMP packets, temporarily taking non-critical network services offline, and restoring critical network services. Post-incident investigation revealed that a malicious actor exploited an unconfigured firewall to execute the DDoS attack. To mitigate future risks, they implemented new security measures, including firewall rule adjustments, source IP address verification, network monitoring, and an Intrusion Detection System/Intrusion Prevention System (IDS/IPS).
Identify	To address the incident and improve network security, we must initiate regular audits of internal networks, systems, devices, and access privileges. These audits will help identify potential security gaps, vulnerabilities, and areas that require enhanced protection. By understanding our network's weaknesses and strengths, we can prioritize security investments effectively.
Protect	Protecting our internal assets is essential. We will implement policies, procedures, and training programs to mitigate cybersecurity threats. This includes configuring firewalls with rules to limit the rate of incoming ICMP packets, enforcing source IP address verification to prevent IP spoofing, and ensuring employees are well-trained in recognizing and reporting suspicious activities. Additionally, we will continue to invest in the latest cybersecurity

	tools to bolster our defenses.
Detect	To enhance our ability to detect potential security incidents, we will improve our network monitoring capabilities. Implementing advanced network monitoring software will enable us to identify abnormal traffic patterns promptly. Additionally, our IDS/IPS system will be fine-tuned to filter out ICMP traffic based on suspicious characteristics, further enhancing our detection capabilities.
Respond	In the event of future security incidents, we will ensure a swift and effective response. Our incident response plan will encompass containment, neutralization, and detailed analysis of incidents. We will continuously refine and implement improvements to our security processes, enhancing our resilience in the face of evolving threats.
Recover	In the aftermath of incidents, our focus will be on rapid recovery. We will work diligently to restore affected systems to normal operation and recover any lost data or assets. This includes not only technical recovery but also addressing any legal or reputational issues that may arise from security incidents.

Reflections/Notes: This incident response following the NIST CSF framework highlighted the importance of proactive security measures, rapid detection, and a well-structured incident response plan. Our commitment to continuous improvement, ongoing training, and staying abreast of emerging threats will be instrumental in strengthening our cybersecurity posture and ensuring the resilience of our organization against future threats.