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.

Summary	A multimedia company offering web design, graphic design, and social media marketing services suffered a DDoS attack that compromised its internal network for two hours. The attack exploited an unconfigured firewall allowing a flood of ICMP packets, overwhelming the network. The incident response team mitigated the attack by blocking ICMP traffic, shutting down non-critical services, and restoring critical ones. The cybersecurity team found the vulnerability and implemented a new firewall rule, source IP address verification, network monitoring software, and an IDS/IPS system to prevent future attacks.
Identify	• **Assets:** The company's internal network, including web design, graphic design, and social media marketing platforms, customer information, and employee data. • **Business Impact:** Loss of productivity, revenue loss due to inability to serve customers, damage to reputation, regulatory fines. • **Vulnerability:** Unconfigured firewall allowed unrestricted ICMP traffic. • **Threat:** Distributed denial-of-service (DDoS) attack using a flood of ICMP packets.
Protect	• Implemented new firewall rule to limit ICMP traffic rate. • Enabled source IP address verification on the firewall to detect spoofed IP addresses. • Deployed network monitoring software to identify unusual traffic patterns. • Installed an IDS/IPS system to filter malicious ICMP traffic.
Detect	• Network monitoring software alerted the incident management team to the abnormal traffic.

	• Security team investigated the event and identified the cause as a DDoS attack.
Respond	• Incident management team blocked incoming ICMP packets. • Non-critical network services were shut down to conserve resources. • Critical network services were restored to ensure business continuity. • Security team investigated the attack and implemented corrective measures.
Recover	• Network services were restored to full functionality. • Vulnerability assessment and penetration testing were conducted to identify and address any remaining vulnerabilities. • Incident response plan was reviewed and updated to improve the response to future attacks.

Reflections/Notes:

- Employee awareness training was conducted to educate employees on how to identify and report suspicious activity.