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	The organization suffered a DDoS attack that interrupted all network services for two hours. The attack was executed through a massive flow of ICMP packets (ping flood) that exploited a vulnerability in a misconfigured firewall. The incident response team contained the attack by blocking ICMP packets and disabling non-essential services. Subsequently, the security team implemented new firewall rules, source IP address verification, network traffic monitoring, and an IDS/IPS system to prevent future incidents.
Identify	The cybersecurity team investigated the security event and discovered that a malicious actor exploited a misconfigured firewall to flood the network with ICMP packets. The incident response team acted in accordance with the function.
Protect	To protect the organization against similar attacks, the security team first implemented a new firewall rule to limit the ingress rate of ICMP packets, mitigating the risk of overload. Secondly, source IP address verification was enabled on the firewall to check for spoofed IP addresses in incoming ICMP packets. Additionally, an IDS/IPS system was implemented to proactively filter malicious traffic based on suspicious characteristics.
Detect	To improve the detection of future threats, the company implemented network

	monitoring software to analyze abnormal traffic patterns. In addition, they added an IDS/IPS system to filter ICMP traffic based on suspicious characteristics and alert the security team about these suspicious activities, increasing the speed and efficiency of detection.
Respond	During the incident, the response team acted promptly to contain the attack. The first action was to block all incoming ICMP traffic at the firewall, which stopped the attack. Simultaneously, all non-critical network services were disabled to reduce the attack surface and preserve resources for essential services. After containment, the team communicated the incident status to the cybersecurity team who investigated the security event.
Recover	The team restored critical network services to resume essential business operations. Afterwards, non-critical services were gradually reactivated while the new network monitoring system monitored the traffic to ensure that the environment was stable and secure.

Reflections/Notes:The root cause was a process failure. A misconfigured firewall indicates the absence of a regular audit and configuration management policy for network devices. Security was not compromised by an equipment failure, but by the lack of human review and standard operating procedures.