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's network services 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 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. Tho address the event, the team implemented 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, and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Identify	The attack was a DDoS attack (Distributed Denial-of-Service), made by an actor flooding the company's network with ICMP pings through an unconfigured firewall, compromising the internal network for two hours.
Protect	The firewall must be properly configured with specific rules and filters to

	mitigate similar attacks in the future. This includes implementing rate limiting for ICMP traffic, deep packet inspection, and dropping malformed or excessive packets. Additionally, source IP verification should be enabled to block spoofed IP packets. Regular firewall audits and updates are crucial to ensure no open or misconfigured ports or protocols are exposed to external networks.
Detect	Implementing a network monitoring system is essential to detect unusual patterns in real time. Tools such as Intrusion Detection Systems (IDS) can be used to analyze traffic and alert administrators to anomalies like spikes in ICMP traffic. Logs and alerts should be continuously monitored, and baseline traffic patterns must be established to quickly identify deviations that may signal an attack.
Respond	The response should include immediate containment of the threat by blocking the attack vector — in this case, disabling or rate-limiting ICMP traffic. The incident response team must then analyze logs, identify attack sources, and if possible, trace back to responsible IPs. All findings should be documented, and communication with relevant stakeholders (including the hosting provider or ISP) may be necessary to help mitigate the attack.
Recover	Once the attack is mitigated, critical services should be restored gradually with monitoring in place to ensure stability. Conduct a post-incident analysis to understand the root cause and improve existing defenses. Update the incident response plan based on lessons learned and test network redundancy and failover systems to ensure quicker recovery in the future. Regular drills and simulations should be conducted to prepare for future incidents.

Reflections/Notes: