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 experienced a DDoS attack in the form of an ICMP flood. During the attack, the company's network services suddenly became unresponsive, and normal internal network traffic was unable to access any service resources. The security team then responded by blocking incoming ICMP packets, and stopping all non-critical network services. So that, the security team restored critical network service.
Identify	The entire internal network was affected. The whole internal network resources need to be secured and restored.
Protect	The security team implemented a new firewall rule to limit the rate of incoming ICMP packets (added source IP address verification). Also, used IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The security team configed source IP address verification on the firewall to detect the spoofed IP address on incoming ICMP packets, also used IDS/IPS system to detect suspicious ICMP traffic based on characteristics.
Respond	**Response planning:** In response to similar DDoS attacks, the team should implement predefined action plans that include immediate traffic filtering, system isolation, and

	staged service restoration. A runbook should guide team members through containment, impact assessment, and escalation procedures. **Communications:** All security event response procedures must be documented and shared with IT staff. Clear communication channels should be established to update affected end users during and after the incident. Senior leadership must be kept informed to ensure timely decisions and external reporting. **Analysis:** After containment, the team should analyze network logs to identify the source and nature of the attack. This includes checking for abnormal ICMP traffic patterns, identifying IP addresses involved, and verifying whether the attack exploited specific vulnerabilities. **Mitigation:** To reduce the impact, affected systems must be taken offline or isolated from the rest of the network. Critical systems should be prioritized for recovery, while non-essential services remain offline until the threat is fully mitigated. **Improvements:** Future response procedures should include automated detection and alerting for traffic anomalies, as well as regular updates to firewall and IDS rules. The team should conduct post-incident reviews to identify gaps and update the response playbook accordingly.
Recover	**Recovery planning:** The security team must restore the network service following a DDoS (ICMP flood) attack. The first step is to block the incoming flood traffic at the firewall. Non-critical network services should be temporarily stopped to reduce load

	and prioritize recovery. The team should focus on restoring critical services first. After confirming that ICMP packets from the suspicious IP address have timed out or stopped, the team can gradually restore non-critical services. **Improvements:** The current recovery process should be updated to include automated firewall rules to detect and block ICMP floods. Response procedures should also prioritize service restoration by criticality. Adding rate limiting for ICMP traffic and implementing monitoring tools for early detection could prevent similar incidents in the future. **Communications:** Restoration procedures must be communicated clearly to all IT staff through internal incident response channels. End users should receive status updates about service availability and expected resolution timelines. After recovery, a debrief should be shared internally to review actions taken and lessons learned.

Reflections/Notes: