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 multimedia company recently experienced a two-hour DDoS attack, compromising its internal network. The attack involved a flood of ICMP packets that overwhelmed network services, rendering them unresponsive. The incident management team mitigated the attack by blocking incoming ICMP packets, stopping non-critical services, and restoring essential ones. Upon investigation, it was discovered that the attacker exploited an unconfigured firewall to launch the attack. In response, the security team implemented new firewall rules to limit ICMP packet rates, verified source IP addresses, installed network monitoring software, and deployed an IDS/IPS system. This incident highlighted the need for improved security measures and prompted the development of a comprehensive cybersecurity plan. The plan aims to enhance identification, protection, detection, response, and recovery processes following the NIST Cybersecurity Framework.
Identify	Regularly conduct audits of the network, systems, devices, and access privileges to identify potential security gaps. Maintain a detailed inventory of all assets and perform vulnerability assessments and penetration tests. Audit access controls to ensure they follow the principle of least privilege. Assess the security posture of third-party vendors. Analyze the impact and likelihood of identified vulnerabilities being exploited.

Protect	Implement and enforce comprehensive security policies and procedures, such as firewall configuration and data encryption. Provide regular cybersecurity training for employees to recognize threats. Deploy endpoint protection solutions and maintain up-to-date antivirus and anti-malware software. Ensure all systems and applications are regularly patched and updated. Protect sensitive data both at rest and in transit.
Detect	Enhance monitoring capabilities using advanced network monitoring tools to detect abnormal traffic. Implement IDS/IPS systems to filter out suspicious traffic. Centralize log collection and analysis to identify signs of potential incidents. Integrate threat intelligence to stay informed about emerging threats. Regularly review and update monitoring tools and procedures for effectiveness.
Respond	Develop and maintain a detailed incident response plan outlining roles and procedures. Implement measures to contain and neutralize active threats. Conduct forensic analysis to understand the attack and prevent recurrence. Establish clear communication channels for notifying stakeholders. Perform post-incident reviews to identify lessons learned and improve security measures.
Recover	Ensure regular backups of critical data and systems are performed and tested. Restore systems and data from backups, ensuring they are secure before going online. Address vulnerabilities exploited during the attack with necessary patches. Verify the integrity of restored systems through comprehensive testing. Review and update the business continuity plan to improve resilience against future attacks.

Reflections/Notes: