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 company experienced a two-hour ICMP flood DDoS attack that disrupted its internal network and prevented normal traffic from accessing resources. The attack was made possible by an unconfigured firewall that allowed malicious traffic into the environment. The incident was resolved by blocking ICMP packets and prioritizing critical services, but the event highlighted weaknesses in firewall management, monitoring, and incident response processes.
Identify	To strengthen identification practices, the company should conduct regular audits of its firewall configurations, networks, and systems to catch misconfigurations before they become vulnerabilities. Maintaining an updated inventory of network assets and critical services will help ensure visibility into what needs the most protection. In addition, access privileges should be reviewed frequently, with least-privilege access enforced for firewall and IDS/IPS administrators to reduce the chance of accidental or malicious misconfigurations.
Protect	Protection can be enhanced by implementing stricter firewall rules that limit the rate of ICMP packets and filter spoofed IP addresses. A formal change control and configuration management process should be adopted to prevent gaps caused by unconfigured rules. Technical safeguards, such as IDS/IPS systems

	with tuned signatures for DDoS behavior, can provide further protection against similar attacks. At the same time, staff training on DDoS prevention, secure configurations, and incident response procedures will ensure that employees are prepared to support protective measures.
Detect	Detection should focus on improving monitoring and alerting capabilities to catch unusual activity quickly. Deploying network monitoring tools will help establish a baseline of normal traffic, making it easier to spot anomalies such as sudden spikes in ICMP traffic. Automated alerts should be configured to notify the security team of abnormal events, reducing detection time. Regular penetration testing and red-team exercises can also be used to validate defenses and identify detection gaps before attackers exploit them.
Respond	Response efforts should be guided by an updated incident response plan that includes playbooks specific to DDoS scenarios. Clear communication protocols must be established so that employees know how to coordinate during incidents, and clients can be informed of outages in a timely manner. After each incident, a post-event review should be conducted to analyze what worked, what failed, and how the process can be improved to enhance future readiness.
Recover	Recovery efforts should focus on restoring affected services quickly and reliably. Backup systems, redundancy, and failover mechanisms must be put in place to ensure that critical business operations can resume as soon as possible after an attack. The company should also work with its internet service provider to establish upstream DDoS filtering or scrubbing solutions to minimize the impact of future attacks. Finally, updates to the business continuity and disaster recovery plans should be made to account for DDoS scenarios, ensuring the organization is prepared for similar incidents going forward.

Reflections/Notes: This incident highlights how a single misconfiguration, such as an unconfigured firewall, can expose the entire organization to severe disruption. Applying the NIST Cybersecurity Framework provides a structured way to not only respond to incidents but also to build long-term resilience against future threats. Improvements should prioritize proactive monitoring, redundancy, and upstream protections, moving the organization from a reactive stance to a more resilient security posture.