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	A DDoS attack using ICMP floods disrupted the company's internal network for two hours. Network services were unavailable, impacting employee workstations and critical business applications. The cybersecurity team successfully blocked the attack and restored essential services.
Identify	• **Attack Type:** DDoS ICMP flood • **Impacted Systems:** Internal servers, employee workstations, critical business applications • **Extent:** Full internal network disruption for two hours • **Recommendations:** Conduct regular network and firewall audits, maintain an updated inventory of devices, and identify potential vulnerabilities
Protect	• Implement firewall rules to limit ICMP traffic • Enable source IP verification to prevent spoofing • Provide staff training on DDoS risks • Maintain policies and procedures for network security and access management
Detect	• Deploy network monitoring software to identify abnormal traffic patterns • Use IDS/IPS systems to flag suspicious ICMP traffic • Configure real-time alerts for traffic spikes or unusual activity • Maintain centralized logging for faster incident analysis

Respond	• Block malicious traffic immediately through the firewall • Take noncritical services offline to protect critical operations • Restore essential services in prioritized order • Document incident details and communicate with stakeholders • Conduct post-incident analysis to determine the root cause **Future Procedures:** For future security events, the cybersecurity team will isolate affected systems to prevent further disruption. Critical systems and services will be restored first, followed by analysis of network logs for suspicious activity. All incidents will be reported to upper management and legal authorities, if applicable.
Recover	• Restore affected systems to normal operations • Update firewall and monitoring configurations • Test backups and business continuity plans • Implement lessons learned to prevent future incidents **Future Guidance:** External ICMP flood attacks can be blocked at the firewall. Non-critical network services should be temporarily stopped to reduce internal traffic. Critical services are restored first, followed by non-critical systems once the attack subsides.

Reflections/Notes:

- The incident highlights the importance of proactive monitoring and network segmentation
- Staff awareness and training are critical for rapid response to DDoS attacks
- Regular updates and firewall reviews can mitigate similar attacks in the future

---