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 (Distributed Denial of Service) attack, through a flood of ICMP packets that overwhelmed the internal network. This attack caused network services to become unresponsive for approximately two hours. The cybersecurity team found that this vulnerability came from an unconfigured firewall. The response included blocking all incoming ICMP packets, stopping all non-critical network services offline and restoring critical network services.
Identify	• **Type of attack:** ICMP Flood DDoS Attack. • **Affected systems:** Internal network, firewall and business applications relying on the network. • **Attack Source:** External malicious actors leveraging unconfigured firewall vulnerabilities. • **Impact:** Network downtime, financial loss.
Protect	To prevent future attacks, the organization should implement the following protective measures: • **Firewall Configuration:** Ensure the firewall is properly configured to limit the rate of incoming ICMP requests. • **Source IP Address Verification:** Deploy IP address verification to filter

	out spoofed addresses. • **Access Control Policies:** Implement strict access controls and segmentation to minimize exposure. **Regular Security Audits:** Conduct periodic security reviews of firewalls, network and software updates.
Detect	To enhance detection capabilities: • **Implement Network Monitoring Tools:** Deploy intrusion detection and prevention systems (IDS/IPS) to flag unusual ICMP traffic. • **Log Analysis:** Set up automated log analysis tools to track incoming and outgoing network traffic. • **Anomaly Detection Algorithms:** Utilize AI-driven analytics to detect irregular traffic patterns in real-time. **User Behavior Monitoring:** Track access logs for anomalies and potential insider threats.
Respond	A well-defined incident response plan should include: • **Containment Strategies:** Isolate affected network segments to prevent further spread. • **Incident Classification:** Quickly categorize the threat level and engage appropriate teams. • **Mitigation Procedures:** Implement emergency firewall rules to block malicious traffic. • **Forensic Analysis:** Gather attack data for root cause analysis and future mitigation. **Communication Protocols:** Establish internal and external communication strategies for incident updates.
Recover	To ensure smooth recovery and minimize downtime: • **Backup and Restore Protocols:** Maintain regular, secure backups to restore affected systems. • **Disaster Recovery Plan:** Define clear recovery steps and

	responsible teams. **System Patch and Update Strategy:** Regularly update security policies

---

Reflections/Notes: By following the recommendations above, the company can significantly improve its ability to dectect and respond from future cybersecurity incidents

Made by:
João Duarte
Cybersecurity Analyst