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 Distributed Denial of Service (DDoS) attack. A malicious actor used a botnet to send a flood of ICMP packets into the company's local area network (LAN). Because the firewall was not configured correctly, the network was overwhelmed and services stopped responding for about two hours. The incident team blocked ICMP traffic, shut down non-critical services, and restored critical ones.
Identify	Type of attack: ICMP flood DDoS Cause: Misconfigured firewall (no baseline configuration applied) Systems impacted: Internal LAN, firewall, and network services Impact: ~2 hours of downtime, business disruption, employees unable to access resources
Protect	**Apply a baseline configuration on the firewall to block or limit ICMP traffic** **Use IP spoofing checks to verify the source of incoming packets**

	Regular patch updates and firewall audits to avoid misconfigurations **Add multi-factor authentication (MFA) and access control for admins making firewall changes** **Use network segmentation and a controlled zone to isolate critical systems**
Detect	Use network monitoring software to check for abnormal bandwidth use and traffic patterns Deploy an IDS/IPS to filter malicious ICMP packets Enable a SIEM system to collect and analyze network logs in real time Set automated alerts for sudden spikes in ICMP traffic or bandwidth usage
Respond	Contain: Block ICMP traffic at the firewall and isolate affected systems Neutralize: Shut down non-critical services and apply firewall rules Analyze: Review network logs, IDS/IPS alerts, and packet captures to study the incident Communicate: Notify stakeholders, IT teams, and leadership about the event and response actions Improve: Update incident response playbooks, run training, and test the new firewall rules
Recover	Restore all services step by step, starting with critical ones

	Validate new firewall rules and IDS/IPS settings before going live Test backups and ensure data integrity is maintained Conduct a post-incident review and update security hardening measures Consider cloud-based firewalls or external DDoS protection services for added resilience

---

Reflections/Notes: This event showed how important it is to keep a firewall properly configured and apply a baseline configuration. Using the NIST CSF made it easier to break down the problem into Identify, Protect, Detect, Respond, and Recover steps. Future attacks can be handled faster with better monitoring, logging, and security hardening.