Incident report analysis - DoS attack

Instructions

Summary	The organization experienced a **Denial of Service (DoS) attack** caused by a flood of **ICMP packets** originating from an external malicious actor. The attacker exploited an **unconfigured firewall**, allowing excessive ICMP traffic to overwhelm network resources. As a result, internal network services became unavailable for approximately **two hours**, preventing employees from accessing critical systems. The incident response team mitigated the attack by blocking incoming ICMP traffic, taking non-critical services offline, and restoring critical services. After investigation, the cybersecurity team implemented firewall rate-limiting, source IP verification, network monitoring tools, and an IDS/IPS to reduce the risk of future attacks.
Identify	**Type of attack:** Denial of Service (DoS) via ICMP flood (Ping Flood) **Affected systems:** ● Internal network infrastructure ● Network services supporting web design, graphic design, and social media marketing operations ● Firewall (misconfiguration identified) **Attack vector:** External ICMP traffic exploiting an unconfigured firewall **Business impact:** ● Network downtime for two hours ● Employees unable to access internal resources ● Temporary disruption of business operations and services to clients **People:** ● IT and cybersecurity staff responsible for network operations ● Employees dependent on internal network services

Protect	**To further secure organizational assets, the following protection measures should be implemented or strengthened:** ● Configure and regularly audit firewall rules, including ICMP rate limiting and default-deny policies ● Enforce source IP address verification and anti-spoofing controls on perimeter devices ● Implement network segmentation to limit the impact of DoS attacks on critical systems ● Establish formal change management and firewall configuration review procedures ● Provide cybersecurity awareness training for IT staff on network hardening and DoS prevention ● Ensure all network devices and security appliances are patched and updated regularly ● Deploy and maintain protective technologies, including IDS/IPS and DDoS mitigation tools
Detect	To improve detection of similar incidents in the future: ● Use **network monitoring software** to establish baselines and detect abnormal traffic spikes ● Deploy an **IDS/IPS** to identify suspicious ICMP patterns and automatically block malicious traffic ● Enable detailed **firewall and router logging** for ICMP and other network protocols ● Integrate logs into a **SIEM solution** for real-time alerts and centralized analysis ● Implement continuous monitoring of inbound traffic from external and non-trusted IP addresses Regularly review alerts and conduct simulated attack testing to validate detection capabilities
Respond	For future cybersecurity incidents, the organization should follow this response plan: ● **Containment:** ○ Immediately block malicious IP addresses and protocols ○ Rate-limit or isolate affected network segments ○ Take non-essential services offline if necessary ● **Neutralization:** ○ Apply firewall and IDS/IPS rules to stop malicious traffic ○ Verify firewall configurations and close exploited vulnerabilities

	● **Analysis:** ○ Review firewall logs, IDS alerts, and network traffic captures ○ Identify attack sources, duration, and impact ● **Communication:** ○ Notify IT staff, management, and affected employees ○ Document the incident for internal reporting and compliance purposes ● **Improvements:** ○ Update incident response playbooks ○ Conduct post-incident reviews and tabletop exercises ○ Improve automation in response procedures where possible
Recover	To restore normal operations and strengthen recovery processes: ● **Immediate recovery:** ○ Restore critical network services and validate connectivity ○ Confirm firewall and monitoring systems are functioning correctly ● **Processes:** ○ Follow documented recovery and business continuity plans ○ Verify system integrity and performance after restoration ● **Improvements:** ○ Enhance redundancy and capacity planning to withstand traffic floods ○ Update disaster recovery and network resilience strategies ● **Communication:** ○ Inform employees when systems are fully restored ○ Provide leadership with a recovery status report and lessons learned

---

Reflections/Notes:
This incident highlights the importance of proper firewall configuration, continuous network monitoring, and layered security controls. Applying the NIST CSF ensures the organization not only responds effectively to incidents but also strengthens its overall security posture through continuous improvement, reducing the likelihood and impact of future DoS attacks.