Incident report analysis

Instructions

Summary	Our organization, a multimedia company specializing in web design, graphic design, and social media marketing for small businesses, experienced a DDoS attack. The incident involved a large flood of ICMP packets that caused internal network services to become unresponsive. As a result, normal internal traffic was unable to access any network resources. The incident response team acted quickly by blocking incoming ICMP traffic, shutting down non-critical services to reduce load, and restoring critical services to resume business operations.
Identify	The organization experienced a DDoS attack in the form of an ICMP Flood, sometimes referred to as a “Ping Flood.” This type of attack overwhelmed the organization’s network infrastructure by sending a high volume of ICMP echo requests (ping packets), which caused network services and servers to become unresponsive for enough time to damage the organization. The root cause was traced to an improperly configured firewall, which allowed unrestricted ICMP traffic from the internet. As a result, the company’s internal network was unable to communicate with web applications and essential services, leading to a temporary outage.
Protect	To prevent similar attacks in the future our company has implemented several protection measures focused on hardening the network perimeter and reducing exposure to DDoS attacks. These include : • **Firewall Rule Configuration**: A new firewall rule was created to **rate-limit incoming ICMP packets**, preventing attackers from overwhelming the network with large volumes of ping requests.

	• **IP Source Verification**: The firewall was updated to include **source address validation**. This helps detect and block **spoofed IP addresses**, which are commonly used in DDoS attacks to disguise the origin of traffic. • **Access Control Policies**: Access to critical internal systems is now more strictly controlled using **network segmentation** and **least privilege principles** to minimize attack surfaces. • **Regular Patch Management**: The organization has adopted a regular schedule for **updating firewall firmware and system software** to protect against known vulnerabilities • **Employee Awareness Training**: Cybersecurity training is provided to all staff to help them recognize early signs of network issues and report suspicious activity promptly. These measures collectively improve the organization's defense posture and reduce the likelihood of future disruption caused by similar attacks.
Detect	To improve early detection of similar attacks, the organization has implemented several monitoring and alerting mechanisms aimed at identifying unusual network activity in real time. These include: • **Intrusion Detection System (IDS)**: A network-based IDS has been deployed to monitor inbound traffic for known attack patterns, including high volumes of ICMP packets or unusual connection rates. • **Firewall Logging and Alerts**: The firewall is now configured to **log all incoming ICMP traffic** and **generate alerts** when traffic thresholds are exceeded, helping the security team detect early signs of a DDoS attempt. • **Network Traffic Monitoring Tools**: Tools such as [insert tool if you use one, e.g., Wireshark, Zabbix, or SolarWinds] are used to continuously monitor network traffic and detect anomalies in packet volume, destination, and behavior.

	• **Baseline Traffic Analysis**: The organization is using anomaly-based detection to establish a baseline of normal network behavior. Any deviation from this pattern—such as a sudden spike in ICMP traffic—triggers an alert for further investigation. • **SIEM Integration**: Logs from firewalls, IDS, and critical systems are forwarded to a centralized **Security Information and Event Management (SIEM)** system. This allows correlation of events and helps identify multi-stage attacks or unusual behavior across the network. These detection mechanisms enhance visibility into network activity, enabling the cybersecurity team to identify and respond to potential threats before they escalate into full-scale incidents.
Respond	Once the DDoS attack was identified, the incident response team took immediate action to contain and mitigate the impact. The following response steps were carried out: • **Blocked Incoming ICMP Traffic**: The first containment step was to block all incoming ICMP packets at the firewall, stopping the flood of traffic and helping stabilize the network. **Shut Down Non-Critical Services**: To preserve system resources and prevent further disruption, all non-essential network services were temporarily disabled. • **Restored Critical Network Functions**: After the ICMP traffic was mitigated, the team focused on restoring critical business services to resume operations as quickly as possible. • **Collected Logs and Network Data**: Logs from firewalls, routers, and monitoring tools were collected to analyze the source, method, and scope of the attack. • **Engaged Incident Response Procedures**: The organization's incident

	response plan was followed, including roles assignment, internal communication, and documentation of every step taken. • **Communicated with Stakeholders**: Internal stakeholders were informed about the incident status, including impacted services and recovery progress, to maintain transparency and trust. This structured response minimized downtime and allowed the team to regain control over the network quickly. Lessons learned from the event were documented to improve future response strategies.
Recover	After containing the DDoS attack and restoring critical services, the organization focused on full recovery to ensure long-term stability and resilience. The recovery steps included : • **Restoring Normal Operations**: All non-critical services that were taken offline during the incident were carefully brought back online after confirming system stability and verifying that no residual malicious activity remained. • **Validating Systems and Services**: Post-incident testing was performed on network infrastructure, web applications, and internal systems to ensure everything was functioning properly and no data was corrupted or lost. • **Conducting a Post-Incident Review**: The cybersecurity team held a review meeting to analyze the root cause, response actions, and lessons learned. This included evaluating the firewall misconfiguration that allowed the ICMP traffic to bypass defenses. • **Updating the Incident Response Plan**: Based on the findings, the organization's incident response procedures were updated to improve future readiness and reduce recovery time for similar incidents. • **Improving Resilience**: Additional safeguards such as automated alerts, system redundancy, and updated firewall configurations were implemented to minimize potential downtime in case of future attacks.

	• **Communicating Recovery Status**: Final status reports were shared with internal stakeholders to confirm that all services were restored and the network was secure. These recovery efforts ensured a return to full operations while reinforcing the organization's security posture against future DDoS threats.

Reflections/Notes: This incident served as a valuable learning experience for both the cybersecurity team and the organization as a whole. It revealed the importance of not only having the right technical defenses in place, but also ensuring those defenses are properly configured and actively monitored.