**Incident report analysis**

**Scenario**

This incident shows a brief overview incident report analysis of an organization needing help with a situation where their services were malfunctioned to operate effectively. This documentation shows the steps needed to restore the company’s operations back together from a potential cyber-attack that harmed the company’s resources.

|  |  |
| --- | --- |
| **Summary** | The organization encountered a security incident wherein all network services abruptly ceased to function. The cybersecurity team identified the disruption as originating from a distributed denial of service (DDoS) attack, involving a surge of incoming ICMP packets. In response, the team took swift action by implementing measures to block the attack and temporarily halting non-critical network services. This proactive approach allowed for the restoration of critical network services. |
| Identify | A malicious actor or group directed an ICMP flood attack against the organization. This assault impacted the entire internal network, necessitating the securing and restoration of all critical network resources to ensure their proper functioning. |
| Protect | **The cybersecurity team introduced a new firewall rule designed to restrict the influx of incoming ICMP packets. Additionally, they deployed an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to filter out certain ICMP traffic based on identified suspicious characteristics.** |
| Detect | The cybersecurity team set up source IP address verification on the firewall, enabling scrutiny for potential spoofed IP addresses within incoming ICMP packets. Furthermore, they incorporated network monitoring software to identify and flag abnormal traffic patterns. |
| Respond | In anticipation of future security events, the cybersecurity team plans to isolate affected systems as a preventive measure to avoid additional disruptions to the network. Their strategy involves restoring any critical systems and services affected during the event. Subsequently, the team will conduct a thorough analysis of network logs to identify and investigate any suspicious or abnormal activities. Additionally, all incidents will be reported to upper management and, if applicable, to the appropriate legal authorities. |
| Recover | To recover from a DDoS attack involving ICMP flooding, it is essential to restore access to network services to their normal functioning state. In future occurrences, external ICMP flood attacks can be thwarted at the firewall. The mitigation process involves halting all non-critical network services to minimize internal network traffic. Subsequently, priority should be given to restoring critical network services. Once the influx of ICMP packets has timed out, all non-critical network systems and services can be safely brought back online. |

|  |
| --- |
| Reflections/Notes: Here are my suggestions to prevent this issue from happening against more future cyberthreats:  1. \*\*Enhanced Firewall Configuration:\*\*  Reflecting on the recent ICMP flood incident, consider strengthening the firewall configuration. Implement more robust rules and filters to proactively block external ICMP flood attacks, providing an initial line of defense against potential disruptions.  2. \*\*Traffic Monitoring and Anomaly Detection:\*\*  Emphasize the importance of continuous network traffic monitoring and anomaly detection. Explore advanced solutions that can swiftly identify abnormal patterns, enabling the cybersecurity team to respond promptly to potential threats before they escalate.  3. \*\*Dynamic Rate Limiting:\*\*  Evaluate the feasibility of dynamic rate limiting for incoming ICMP packets. By adjusting the rate based on normal traffic patterns, the system can automatically adapt to variations, preventing sudden spikes that could indicate malicious activity.  4. \*\*Automation for Rapid Response:\*\*  Consider integrating automation into the incident response process. Develop automated responses for known threats, enabling the system to quickly and efficiently block or mitigate attacks without manual intervention, minimizing the impact on critical services.  5. \*\*Regular Security Audits and Assessments:\*\*  Establish a routine schedule for security audits and assessments. Regularly review and update security measures to address emerging threats and vulnerabilities. This proactive approach ensures that the cybersecurity infrastructure remains resilient to evolving attack techniques.  6. \*\*Employee Training and Awareness:\*\*  Recognize the role of employees in maintaining a secure environment. Conduct regular training sessions to enhance awareness of security protocols, phishing prevention, and incident reporting. A well-informed workforce can serve as an additional layer of defense against potential security breaches.  7. \*\*Collaboration with Internet Service Providers (ISPs):\*\*  Explore collaboration with ISPs to leverage their resources in mitigating DDoS attacks. Establish communication channels to quickly share threat intelligence and coordinate responses, enhancing the overall effectiveness of defense mechanisms.  8. \*\*Incident Response Drills:\*\*  Conduct periodic incident response drills to test the effectiveness of security measures and the team's ability to respond to various scenarios. Identify areas for improvement and refine response strategies based on lessons learned during these exercises.  9. \*\*Documentation and Knowledge Sharing:\*\*  Foster a culture of documentation and knowledge sharing within the cybersecurity team. Maintain comprehensive records of incidents, responses, and outcomes. This information can serve as a valuable resource for continuous improvement and future incident prevention.  10. \*\*Stay Informed about Emerging Threats:\*\*  Encourage the cybersecurity team to stay informed about the latest trends and emerging threats in the cybersecurity landscape. Regularly participate in industry forums, conferences, and threat intelligence sharing initiatives to gain insights into evolving attack vectors.  By incorporating these reflections and notes into the security strategy, the organization can establish a proactive and adaptive approach to prevent and mitigate the impact of DDoS attacks, particularly those involving ICMP flooding. |