**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The organization experienced a DDoS attack on its internal network, where a flood of ICMP packets overwhelmed the system, causing a two-hour disruption of network services. The attack exploited a firewall vulnerability, allowing malicious actors to send ICMP pings that congested the network. The internal network became unresponsive, preventing normal traffic from accessing resources. Services critical to business operations were disrupted. The incident management team blocked incoming ICMP packets, took non-essential services offline, and restored critical ones. |
| Identify | The attack was a Distributed Denial of Service (DDoS) attack. Specifically, a flood of ICMP packets was used to overwhelm the organization's network, making it unresponsive to legitimate traffic.  All internal network services were impacted due to the network being overwhelmed by the flood of ICMP packets. The attack exploited a vulnerability in the firewall, allowing the malicious traffic to flood the network. Business-critical services were unavailable during the attack, affecting the company's ability to operate normally.  The firewall was unconfigured to handle ICMP traffic properly, which allowed a malicious actor to flood the network with ICMP packets, causing a denial of service. |
| Protect | Update firewall rules to block or limit the rate of incoming ICMP traffic, and ensure source IP address verification is enabled to prevent IP spoofing. Regularly review and audit firewall settings to ensure they are aligned with best security practices.  Implement and maintain continuous network monitoring tools to detect unusual traffic patterns. This will enable the detection of large ICMP floods before they can overwhelm the system. Set up real-time alerts for anomalies in network traffic to improve response times.  Fine-tune the existing IDS/IPS to detect and block suspicious traffic more effectively, particularly for protocols such as ICMP. Regularly update the rules and detection capabilities of the IDS/IPS to address new types of attacks.  Conduct security awareness training to ensure that employees are knowledgeable about potential vulnerabilities and best practices for network security. This includes regularly updating staff on how to prevent brute force attacks and manage network access.  Strengthen access control policies, including enforcing stronger passwords, multi-factor authentication (MFA), and limiting access privileges for critical systems. Regularly review and update access privileges to ensure that only authorized personnel can make changes to firewall and network configurations. |
| Detect | Deploy network monitoring tools to continuously observe and analyze network traffic. Tools such as SIEM (Security Information and Event Management) systems or network traffic analyzers (e.g., Wireshark, SolarWinds) should be configured to detect anomalies like a sudden influx of ICMP packets from untrusted sources. Set up real-time alerts for abnormal traffic patterns, such as unexpected spikes in ICMP traffic or access attempts from unusual IP addresses.  Fine-tune the IDS/IPS to detect and block suspicious activities, including incoming ICMP floods or unauthorized access attempts. Regularly update the IDS/IPS signatures and rules to stay ahead of emerging threats.  Implement tools to track user account activity and identify unauthorized access attempts. This includes logging user authentication events and monitoring for multiple failed login attempts or unusual login locations. Use identity management systems to differentiate between authorized and unauthorized users, ensuring that only trusted users can access critical resources.  Ensure all critical systems, firewalls, and applications generate detailed logs of user actions, network traffic, and system changes. Regularly review these logs to detect unusual patterns of behavior or unauthorized changes.  Configure automated log analysis tools to flag suspicious activities, such as repeated login failures, unusual login times, or attempts to modify security settings.  Maintain an active incident response team that is promptly alerted in the event of abnormal network activity or user behavior. The team should be equipped to investigate and mitigate security threats as they arise. |
| Respond | Immediately isolate affected devices from the network to prevent further spread of malicious activity. This includes quarantining compromised systems and blocking suspicious IP addresses or traffic patterns using firewall rules and network segmentation. Disable vulnerable services or applications temporarily until they can be assessed and secured.  Use intrusion prevention systems (IPS) to block ongoing attacks and prevent further exploitation. Deploy antivirus or anti-malware software to remove malicious software from compromised systems.  Collect network traffic logs, event logs, and user activity logs from affected systems to analyze how the incident occurred and what systems were impacted. Use data from intrusion detection systems (IDS), firewalls, and SIEM tools to investigate the timeline of the attack and identify any vulnerabilities that were exploited. Store evidence securely for future analysis, and prepare a post-incident report summarizing the key findings and recommendations.  Develop a disaster recovery plan that outlines step-by-step procedures for restoring critical systems and data after an incident. This should include regular backups and testing of restoration procedures. Implement regular recovery drills to test the response team’s ability to restore normal operations quickly and efficiently. |
| Recover | Access to the most recent backups of affected systems is critical for restoring data quickly. Ensure that backups are verified and up-to-date, and confirm the integrity of the backup data before restoration.  Implement the organization’s disaster recovery plan, which includes restoring critical systems and services from backup, reconfiguring network settings, and verifying that all systems are functioning correctly after the restoration.  Prioritize the restoration of critical services that directly impact the organization's operations, such as web servers, databases, and email systems. Gradually restore non-critical services while monitoring for any signs of anomalies or issues in the network.  After recovery, conduct a post-incident review to ensure that all systems are fully functional and secure. |

|  |
| --- |
| Reflections/Notes: |