**Incident report analysis**

**Audited by M.Murtaza   
Junior Soc Analyst**

|  |  |
| --- | --- |
| **Summary** | This morning, our network services were compromised by a Distributed Denial of Service (DDoS) attack. The attack resulted in a flood of ICMP packets, overwhelming the internal network, and causing a disruption of services for two hours. The incident was resolved by blocking incoming ICMP packets, restoring critical services, and investigating the root cause of the attack. Upon further analysis, the security team identified gaps in the firewall configuration that allowed the attack to bypass defenses. This report outlines the steps taken to address the attack, following the NIST Cybersecurity Framework. |
| Identify | Today in our organization, network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The company’s cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. |
| Protect | To address this security event, the network security team implemented:   * A new firewall rule to limit the rate of incoming ICMP packets * Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets * Network monitoring software to detect abnormal traffic patterns * An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics |
| Detect | To detect these type of attacks the security team implemented new traffic anomaly detection system and integration of a system that logs malicious or untrusted looking logs on the SIEM logs page and also implemented a behavioral analysis network traffic analyzer.  **Traffic Anomaly Detection:** The network monitoring software was configured to detect and alert on anomalous traffic patterns, such as large numbers of incoming ICMP packets. This helps to identify potential DDoS attacks before they fully affect network performance.   **SIEM System Integration:** A Security Information and Event Management (SIEM) system was implemented to aggregate logs from firewalls, IDS/IPS, and other critical security devices. The system performs real-time analysis of these logs to detect potential attack patterns and generate alerts.   **Behavioral Analytics:** Network traffic behavior was continuously analyzed to identify irregularities such as traffic surges and packet types commonly associated with DDoS attacks. Machine learning models can identify patterns and potential attacks earlier. |
| Respond |  **Incident Response Activation:** Once the attack was detected, the incident response plan (IRP) was activated. The first action was to isolate the affected network segments to prevent further damage.   **Blocking Malicious Traffic:** The malicious ICMP traffic was blocked by implementing the newly configured firewall rules. Traffic from suspicious IP addresses was dropped, containing the attack.   **Collaboration with ISPs:** The security team worked with the internet service provider (ISP) and cloud-based DDoS mitigation providers to absorb the attack traffic, preventing further impact on the company’s network.   **Root Cause Analysis:** A root cause analysis was conducted to determine how the attack bypassed defenses. It was discovered that the firewall was not configured to handle DDoS traffic effectively, which led to the attack bypassing the defenses. |
| Recover |  **estoration of Services:** Once the attack was mitigated, critical services such as web hosting, email services, and internal communications were restored. Non-critical services remained offline to reduce network load.   **Data Integrity Check:** The team conducted a thorough check of all affected systems to ensure data integrity. No data loss was identified, but the systems were monitored for any potential long-term effects of the attack.   **System Recovery from Backups:** The company performed a full system recovery from the backup taken the previous night. Any changes made during the attack period (such as configuration modifications) were not included in the backup and needed to be manually re-entered by the IT team.   **Post-Incident Review:** A post-incident review was conducted to evaluate the response and identify areas for improvement. The team agreed that additional DDoS mitigation services would be required for future incidents and that regular network security audits were necessary. |

|  |
| --- |
| Reflections/Notes: ***The DDoS attack revealed weaknesses in our firewall configuration and the necessity of real-time monitoring tools. Implementing rate limiting and IP address verification on the firewall was crucial in mitigating the attack and preventing similar incidents. The quick collaboration with ISPs and DDoS mitigation services proved to be a key factor in restoring network stability. Going forward, it's important to focus on continuous network security audits and enhancing detection systems to identify potential threats more quickly. Regular employee training on security best practices will also be essential in reducing the likelihood of similar incidents in the future.*** |