**Incident report analysis**

| **Summary** | Access to internal network resources by authorized users was disabled when an incoming flood of ICMP packets overwhelmed the network. The incoming ICMP packets were blocked, and the activity on the internal network restricted. After investigation, it was found that a malicious actor conducted a DDoS attack via an unconfigured internal firewall. To address the event the firewall was properly configured to account for this type of attack, IP address verification was implemented, network monitoring software was set up, and an IDS/IPS system was configured to filter out suspicious ICMP traffic. | | |
| --- | --- | --- | --- |
| Identify | Due to the nature of the attack, I believe that the malicious actor conducted a DDoS ICMP Flood attack. This overwhelming flood of ICMP packets consumed all the network bandwidth which prevented the network traffic from being able to be transmitted effectively. | | |
| Protect | The cybersecurity team implemented improved firewall rules to limit the rate of incoming ICMP packets, preventing a similar flood in the future. Additionally, an IDS/IPS system was configured to filter out suspicious ICMP packets. | | |
| Detect | The firewall was configured to be able to verify the IP addresses of incoming ICMP packets to check for spoofed addresses. The network monitoring software configured by the team will also allow for future monitoring of network traffic to check for abnormal patterns and trends. | | |
| Respond | During the immediate response to future incidents, the team will quarantine affected systems to limit the impact on the network as a whole. The restoration of critical systems will be prioritized. Next, the team will analyze network traffic logs to check for abnormal activity and find potential vulnerabilities. The incident will then be reported to upper management for further actions. | | |
| Recover | In order to recover from a similar attack in the future, the internal network traffic will need to be limited to prevent overwhelming of the network resources. This can be achieved by blocking the flood of ICMP packets at the firewall-level and halting all non-critical network services internally. Once the flood of packets have timed out and been blocked from coming into the network further, the network services can be restored to resume normal function. | | |