# Incident report analysis

| | |
|---|---|
| **Summary** | Our organization recently experienced a distributed denial of services (DDoS) attack, which compromised the internal network for two hours until it was resolved. During the attack, our organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| Identify | The company's cybersecurity team investigated the security event and found that a malicious actor or actors had sent an ICMP flood attack into the company's network through an unconfigured firewall. This vulnerability was enough for a malicious actor to infiltrate the system and overwhelm the company's network through a distributed denial of service (DDoS) attack. |
| Protect | The cybersecurity team has implemented new security hardening techniques to prevent future attacks: A new firewall rule to limit the number of ICMP packets accepted. Additionally, we put an IDS/IPS system in place to filter out some ICMP traffic based on known attacks and anomalies. |
| Detect | To detect new DDoS attacks in the future, the security team will use source IP verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implement new network monitoring software to detect abnormal traffic patterns. |
| Respond | The security team reconfigured the firewall that was attacked. We provided training to employees on checking baseline configurations to be certain there are no unverified changes to the network and log analysis to recognize suspicious traffic. We are also implementing an end of day full backup log |

| | |
|---|---|
| | policy to reduce the amount of time it takes to recover. |
| Recover | The security team will recover the deleted data by restoring the database from the end of day full backup. The reconfigured firewall will help block future external ICMP flood attacks. Staff should also be retrained on restoration procedures and end users will receive an email with updated restoration and security policies. |

---

| |
|---|
| Reflections/Notes: I enjoyed working my way through each of the five core functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). It really helped me look at security incidents differently, being able to break it down step by step and take my time examining all of the details that occurred during each function independently, instead of trying to take in everything involved in the incident at once, made security incidents as a whole seem a lot less intimidating. |