**Incident report analysis**

| **Summary** | The organization’s network services suddenly stopped responding. The cyber security team found that this was due to an incoming flood of ICMP packets resulting in a distributed denial of service (DDoS) attack. The response consisted of blocking the attack and stopping all non-critical network services so that critical services could be restored. | | |
| --- | --- | --- | --- |
| Identify | The security team found that the malicious actor exploited a vulnerability in the company’s network by flooding the network with ICMP packets through an unconfigured firewall. This vulnerability allowed the malicious actor to overwhelm the network through a Distributed Denial of Service (DDoS) attack. | | |
| Protect | The team has implemented a new firewall rule to limit the rate of incoming ICMP packets as well as a IDS/IPS system to filter out some of the ICMP traffic based on suspicious characteristics. Additionally, source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets was added and network monitoring software to detect abnormal traffic patterns. | | |
| Detect | To detect new potential security incidents in the future, an IDS/IPS system will be used to monitor and increase the detection efficiency. A firewall logging tool will be in use. | | |
| Respond | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. | | |
| Recover | Recovering from this type of attack includes restoring network services to the normal state. Future ICMP flood attacks can now be blocked at the firewall level. Critical network services should be restored first after the flood attack has stopped. | | |

| Reflections/Notes: |
| --- |