**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

|  |  |
| --- | --- |
| **Summary** | The organization recently experienced a DDoS attack, compromising the internal network for two hours until being resolved. During the attack, our network services stopped responding all of a sudden, due to a flood of ICMP packets into the network through an unconfigured firewall. Normal internal network traffic couldn’t access any network resources. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service attack (DDoS) attack. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| Identify | A malicious actor targeted the organization through an ICMP packet flood attack. The flood of ICMP packets caused the entire internal network to halt until the problem could be resolved. All critical network resources needed to be secured and restored to a functioning state. |
| Protect | To ensure that the company is better protected against a similar attack, the network security team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Detect | The network security team also implemented network monitoring software to detect abnormal traffic patterns, and configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. |
| Respond | To help defend against similar events in the future, the cybersecurity team will isolate affected systems to prevent further disruption to the network. The team 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 activity. The team will also report all incidents to upper management and appropriate legal authorities, as needed. |
| Recover | To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical systems and services can be brought back online. |

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