**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 distributed denial of service (DDoS) attack in the form of an ICMP flood. The attack disrupted the internal network for approximately two hours before it was resolved. During this time, network services stopped responding due to the flood of ICMP traffic, which prevented normal internal traffic from accessing resources. Investigation revealed that the malicious actor exploited an unconfigured port in the company’s firewall to send the flood of ICMP pings. | | |
| --- | --- | --- | --- |
| Identify | The incident was caused by a malicious actor sending a flood of ICMP pings through an unconfigured firewall port, resulting in a DDoS attack. The overwhelming number of requests exhausted network resources and prevented regular traffic from gaining access, which disrupted operations across the entire network. | | |
| Protect | The cybersecurity team initially blocked incoming ICMP packets, shut down non-critical network services, and worked to restore critical services. To prevent similar incidents, the team implemented firewall rate-limiting for ICMP traffic and configured the firewall to verify source IP addresses to reduce spoofing. Additional safeguards now include network monitoring software and an IDS/IPS to automatically filter suspicious ICMP traffic. | | |
| Detect | Network monitoring software and IDS/IPS solutions have been deployed to identify suspicious ICMP activity and abnormal traffic patterns. These tools allow the security team to continuously monitor internet traffic and detect potential threats in real time. | | |
| Respond | To improve future response efforts, continuous monitoring should be maintained to reduce downtime and limit business impact. An incident response playbook should be developed to ensure that similar attacks can be contained and resolved more quickly. Recommended steps include immediately stopping non-critical network services while restoring critical functions without delay. The team will also report all incidents to upper management and appropriate legal authorities, if applicable. | | |
| Recover | Following an attack, network operations should be returned to baseline configuration. Suspicious ICMP packets should be stopped at the firewall or at IDS/IPS. Non critical services to be turned off, then all critical services to be turned back on. Once all malicious ICMP packets have stopped and/or timed out, all network services can be returned to normal. Staff should be trained and reminded to report any suspicious activity or connectivity issues immediately to reduce response time. Regular security reviews and policy updates should also be conducted to ensure lessons learned are incorporated into organizational practices. | | |

| Reflections/Notes: |
| --- |