**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 company experienced a network outage when all internal services suddenly became unresponsive due to a Distributed Denial of Service (DDoS) attack involving a flood of ICMP packets. As a result, normal internal traffic was unable to access any network resources. The incident response team acted swiftly by disabling all non-critical services to reduce load and prioritized the restoration of critical network functions. |
| Identify | The investigation revealed that a malicious actor launched an ICMP flood attack targeting the company’s infrastructure, causing a widespread disruption across the local network. This attack exploited an improperly configured firewall, allowing unfiltered ICMP packets to overwhelm the system. All critical services and data were restored after isolating the attack source. |
| Protect | To mitigate future incidents, the cybersecurity team implemented a firewall rule to limit the rate of incoming ICMP packets. Additionally, an Intrusion Detection and Prevention System (IDS/IPS) was deployed to analyze and filter ICMP traffic based on suspicious behavior and known attack signatures. |
| Detect | The firewall was reconfigured to verify the source IP addresses of incoming ICMP packets to identify spoofed traffic. Network monitoring tools were also implemented to establish traffic baselines and detect abnormal patterns in real time, enhancing the team’s ability to identify threats promptly. |
| Respond | In future incidents, the response team will isolate affected segments of the network to prevent further spread of malicious traffic. Critical systems will be restored first to maintain business continuity. The team will review security logs to understand the nature and scope of the attack and notify upper management and legal authorities as required. |
| Recover | The cybersecurity team will continue to refine firewall configurations to proactively block ICMP flood attacks. In response to similar future incidents, non-critical services will be temporarily taken offline to ease network strain, while priority is given to restoring critical infrastructure. Once stability is confirmed, all remaining systems will be reactivated in a controlled manner. |

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