**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** | Today, our organization experienced an attack which compromised the internal network for 2 hours until it was resolved. Our network services stopped responding due to a flood of incoming ICMP packets. Normal internal network traffic could not access any network resources. |
| Identify | It appears that the malicious actor sent pings through an unconfigured firewall, which allowed them to overwhelm the company’s network using a DDoS (Distributed Denial of Service) attack. |
| Protect | The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets and source IP address verification to prevent IP spoofing. |
| Detect | To prevent this from happening in the future, the network security team is implementing network monitoring software to detect abnormal traffic and an IPS/IDS to filter out some ICMP traffic based on certain suspicious characteristics. |
| Respond | When the issue occurred, the IM team responded by blocking incoming ICMP packets, stopping all non-critical services offline, and restoring critical services. |
| Recover | We have returned all systems back to normal operation after response to the issue. We will be able to respond to this type of attack more quickly in the future due to the implementation of an IDS/IPS to monitor and control incoming traffic and intrusion attempts. |