**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** | Our organizations internal network went down due to a malicious attacker using a DDoS attack to send a flood of ICMP pings through an unconfigured firewall. The team blocked the attack and stopped all non-critical network services to see what was going on. Then, the critical network services were restored. |
| Identify | A malicious actor sent a flood of ICMP pings through an unconfigured firewall. During this time the network services stopped responding due to being overwhelmed by the DDoS attack. |
| Protect | To address this concern, the team has implemented a new firewall rule to limit the amount of ICMP packets at once. Also, source IP address verification was added to the firewall to check for spoofed IP addresses incoming from ICMP packets. |
| Detect | An IDP/IDS system has been added to filter out some of the unwanted traffic that may seem suspicious and network monitoring software to detect abnormal traffic patterns. |
| Respond | The security team responded to this attack by blocking the incoming ICMP packets, stopping all non-critical network services and restoring the critical ones. |
| Recover | After the team configures the firewall and the new detection devices are in place, the network will be restored allowing the team to regain access under a more secure system. For future, the firewall updates should block the flood of ICMP packets if this were to happen again. |

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