**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 experienced a DDoS attack due to a misconfigured firewall. The attacker was able to send a flood of ICMP packets through the misconfigured firewall, overwhelming the internal network and causing a disruption to normal business activities. The cybersecurity team responded by blocking the ICMP packets, configuring the firewall correctly, and implementing intrusion detection and prevention systems to monitor and protect the network. | | |
| --- | --- | --- | --- |
| Identify | The cybersecurity team identified a misconfigured firewall as the main attack vector for this cybersecurity incident. The servers and devices in the internal network were unable to handle the overwhelmingly high level of traffic and normal operations were disrupted entirely for 2 hours. | | |
| Protect | New firewall rules were implemented that block abnormal ICMP requests. It is important that new policies are implemented to ensure that firewalls are correctly configured when installed and audited regularly. | | |
| Detect | Monitoring software, prevention and detection devices, and source IP verification for ICMP requests have been added in order to help detect future attempted attacks and stop them before they can disrupt the network. | | |
| Respond | The team responded by blocking the incoming ICMP requests, disabling non critical network services, and restoring critical network services. | | |
| Recover | The rest of the non-critical network services must be restored to resume normal business operations. The organization has implemented new policies, along with an intrusion detection system that will help identify future attacks more quickly, allowing faster recovery. | | |

| Reflections/Notes: |
| --- |