**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 the organization experienced a DDoS attack that compromised the network for 2 hours. The company’s cybersecurity team then investigated the security event. It was determined that a malicious actor sent multiple ICMP packets through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. To address this security event, the network security team implemented the following; A new firewall rule to limit the rate of incoming ICMP packets, Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, Network monitoring software to detect abnormal traffic patterns, An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. | | |
| --- | --- | --- | --- |
| Identify | A malicious actor targeted the company's network through an unconfigured firewall, with the use of an ICMP flood attack. The internal network was affected, and all network resources needed to be secured and restored. | | |
| Protect | The security team implemented the following; A new firewall rule to limit the rate of incoming ICMP packets as well as an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. | | |
| Detect | The cybersecurity team configured source IP address verification on the  firewall to check for spoofed IP addresses on incoming ICMP packets and  implemented network monitoring software to detect abnormal traffic patterns. | | |
| Respond | For future events the team will monitor network traffic to detect suspicious activity, it will also subdivide the network, this will prevent the attack form spreading and causing more damage. | | |
| Recover | The network resources need to be restored to a normal functioning state. Then, all non-critical network services should be stopped to reduce internal network traffic. | | |

| Reflections/Notes: |
| --- |