**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 recently experienced a DDos attack, which damaged the internal network for two hours. The attack began with a flood of ICMP packets that didn’t go noticed by the unconfigured firewall, leading to a server failure. After the attack was realized, the incoming packets were blocked, and security controls were updated. | | |
| --- | --- | --- | --- |
| Identify | The internal network was compromised by a DDOS attack. The network services were noticed to suddenly stop working altogether, and after further investigation an influx of ICMP packets were noticed, hinting at a possible DDOS attack. The incident management team blocked incoming ICMP packets and resolved the attack in two hours.  As a result of the attack, normal internal traffic and business operations were halted for the time. | | |
| Protect | The attack was regarded to be a result of an unconfigured firewall. The network security team therefore, implemented a new firewall that was configured to limit the rate of incoming ICMP packets. Additionally they implemented IP address verification that checked spoofed IP addresses on ICMP packets into the firewall. | | |
| Detect | Network monitoring software was then implemented to detect unusual traffic patterns. Finally, an IDS/IPS system was established to filter some ICMP traffic based on its suspiciousness. | | |
| Respond | In the future, the security team should better utilize their time before attacks and threats by assuming internal audits and pen tests to ensure that the current security controls are up to date and present. | | |
| Recover | After an attack finishes, the company must attempt to restore normal operations as soon as possible by immediately isolating the incident to prevent further damage. Afterwards, the security team must investigate the cause of the issue and update their security controls to combat the attack. After the proper response and improvement so a similar attack can’t happen again. Since the firewall wasn’t configured in a proper way, it would be effective to perform security audits and testing regularly to ensure that the organization’s posture is strong and its controls up to date. | | |