**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or just to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to continue practicing applying the NIST CSF framework to different situations you may encounter.

| Summary | The company experienced a security event when all network services suddenly stopped responding. The cybersecurity team found the disruption was caused by a distributed denial of services (DDoS) attack through a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network services so that critical network services could be restored. | | |
| --- | --- | --- | --- |
| Identify | A malicious actor or actors targeted the company with an ICMP flood attack. The entire internal network was affected. All critical network resources needed to be secured and restored to a functioning state. | | |
| Protect | Protect internal assets by implementing policies, procedures, training, and tools that help mitigate cybersecurity threats. This includes updating firewall rules to limit the rate of incoming ICMP packets and implementing source IP address verification, enhancing network segmentation, deploying intrusion detection and prevention systems (IDS/IPS), implementing network monitoring software, regularly patching and updating systems, and implementing a robust incident response plan. | | |
| Detect | Detect potential security incidents and improve monitoring capabilities. This can be achieved by implementing a Security Information and Event Management (SIEM) system, deploying intrusion detection systems (IDS) and intrusion prevention systems (IPS), utilizing network behavior analysis tools, implementing file integrity monitoring (FIM) solutions, enabling auditing and logging, and establishing real-time alerting mechanisms. | | |
| Respond | Respond to contain, neutralize, and analyze security incidents. This involves establishing an incident response team, developing an incident response plan, isolating affected devices or systems, collecting and preserving evidence for forensic analysis, identifying the root cause of the incident, implementing necessary measures to prevent future incidents, and communicating and coordinating with relevant stakeholders. | | |
| Recover | Recover affected systems to normal operation and restore systems data and/or assets. This includes restoring systems and data from secure backups, validating the integrity and security of restored assets, conducting post-incident analysis, updating incident response plans and procedures, providing user training and awareness programs, monitoring recovered systems and networks, and regularly testing and validating incident response and recovery processes. | | |

| Reflections/Notes: |
| --- |