**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 incident involved a DDoS attack that targeted the organization's network through a flood of ICMP pings. The attack resulted in the network services becoming unresponsive for two hours until the incident was resolved. The security event was caused by an unconfigured firewall that allowed the malicious actor to overwhelm the network. | | |
| --- | --- | --- | --- |
| Identify | The type of attack that occurred was a DDoS attack. The systems affected by the attack were the company's internal network, which resulted in the unavailability of network services. | | |
| Protect | To further secure the organization's assets, the immediate action plan includes updating or changing systems and procedures. This may involve ensuring the proper configuration of firewalls, enhancing firewall rules to limit the rate of incoming ICMP packets, implementing source IP address verification on the firewall, providing employee training on cybersecurity best practices, and enforcing strict access control policies. | | |
| Detect | To enhance monitoring capabilities and detect potential security incidents the organization should regularly monitor network traffic on network devices. This can involve using network monitoring software to identify abnormal traffic patterns, tracking authorized versus unauthorized users implementing IDS and IPS and analyzing network traffic and software applications for any unusual activity. | | |
| Respond | In the event of future cybersecurity incidents, the response plan should focus on containing and neutralizing the incidents. This can include isolating affected devices or systems, conducting forensic analysis to identify the extent of the incident, gathering relevant data and information for analysis, notifying appropriate stakeholders, and implementing improvements to the security process based on lessons learned from the incident. | | |
| Recover | To recover from the cybersecurity incident and restore normal operation, the organization needs to identify the information that needs immediate recovery. This may involve restoring affected systems, ensuring data integrity and availability, and implementing backup and recovery processes. The organization should also evaluate its recovery processes and make improvements to better handle future cybersecurity incidents. | | |

| Reflections/Notes: It is crucial to continuously assess and audit internal networks, systems, devices, and access privileges to identify potential security gaps. By implementing the NIST Cybersecurity Framework, the organization can establish a comprehensive security strategy that addresses risk management, protection, detection, response, and recovery. Regularly reviewing and updating security measures will help mitigate cybersecurity threats and enhance overall network security. |
| --- |