**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 faced a disruptive DDoS attack that paralyzed our internal network for two hours. During this time, regular network services became unresponsive, leaving employees unable to access critical resources. |
| Identify | Upon investigation by our cybersecurity team, it was determined that a malicious actor exploited a vulnerability in our firewall configuration, allowing them to flood our network with a barrage of ICMP pings. This onslaught effectively carried out a distributed denial of service (DDoS) attack, rendering our services unresponsive. |
| Protect | To bolster our defenses against such future attacks, we are taking proactive measures. Firstly, we are implementing a new firewall rule to restrict the rate of incoming ICMP packets, thus preventing website flooding and ensuring its responsiveness. We are also enhancing security by introducing source IP address verification on the firewall to detect and block any spoofed IP addresses associated with incoming ICMP packets. |
| Detect | In order to pinpoint the root cause of this DDoS attack, our team utilized network monitoring software like tcpdump and Wireshark to identify abnormal traffic patterns that contributed to the unresponsiveness of our website. Additionally, Security Information and Event Management (SIEM) tools have been employed to continuously monitor for any suspicious activities. |
| Respond | In response to this incident, an IDS/IPS system is implemented to filter out some ICMP traffic based on suspicious characteristics. Implementing new firewall rules to prevent the overwhelming amount of ICMP received will also be implemented. We the informed upper management of this event and they will contact our customers to inform them about the incident. Management will also need to inform law enforcement and other organizations as required by local laws. Furthermore, we have promptly informed upper management about this event, and they will communicate with our customers to provide them with details about the incident. We are also liaising with law enforcement and adhering to local laws and regulations, ensuring transparency and compliance in handling this cybersecurity incident. |
| Recover | Once the attack is mitigated, begin the process of restoring affected systems and services to normal operation. Conduct a thorough post-incident review to identify weaknesses in security controls and response procedures and make necessary improvements. Document all actions taken during the incident response process for future reference and reporting purposes. |

|  |
| --- |
| Reflections/Notes: Improvements: Based on the lessons learned from the incident, update and enhance the organization's DDoS prevention and response strategies. Training: Provide training and awareness programs to educate employees and stakeholders about DDoS threats and best practices. |