**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’s internal network suffered a DDoS attack that lasted at least two hours, rendering all the network systems unavailable. The security team proceeded to fix the issue by taking all the non-essential infrastructure offline and locking all incoming ICMP traffic.  Logs show that the threat actor used many different IP addresses to conduct the attack, sending a barrage of ICMP pings through an unconfigured firewall.  Apart from the business continuity, it is unlikely that grave damages were caused to the organization’s internal networks and data integrity or confidentiality. | | |
| --- | --- | --- | --- |
| Identify | The organization suffered a malicious DDoS ICMP Flood Attack that compromised the entire internal systems. Critical systems were affected, and needed to be secured and reinstated to a working state. | | |
| Protect | The security team updated the firewall configurations to include new rules to limit the rate of incoming ICMP packets and source IP address verification to check for spoofed IP addresses on incoming ICMP packets, and instituted a regular firewall update clause on the security policy.  A DoS attack incident response and business continuity playbook was also drafted, and its completion was made into a high priority project. | | |
| Detect | Both a network monitoring software and an IDS/IPS system to detect abnormal traffic patterns and prevent intrusions were installed, as well as alert the security team to possible incidents. | | |
| Respond | In the event of future similar attacks, an IDS/IPS system will allow for faster response, while network segmentation will be used to disable and take offline only the affected systems, preserving business continuity. The security team will then attempt to restore affected critical systems, if any, to a working state, and posteriorly analyze logs to identify suspicious activity.  Any findings will then be reported to upper management and appropriate legal entities if at all applicable. | | |
| Recover | To recover from similar ICMP Flood Attacks, access to critical network systems needs to be reestablished.  The brunt of future flood attacks can be caught by the firewall and IPS, and if the system is still heavily affected by the attack, non-critical network segments will be disabled to decrease internal network traffic. Then, affected critical systems, if any, should be reestablished first. Finally, once the flooding has stopped, all systems should be reestablished and the post-incident phase can be iniciated. | | |

| Reflections/Notes: The lack of proper care with keeping firewall configuration up-to-date and implementing IDS/IPS tools has severely harmed the organization, but it caused us to reflect upon our overall security posture, and we chose to face this incident as a great opportunity to grow into a more secu and careful organization. |
| --- |