**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** | Our company recently encountered a DDoS attack. During the attack, the internal network was compromised for two hours as a flood of ICMP packets overwhelmed the network, disrupting all non-critical services. The incident management team responded swiftly by blocking incoming ICMP packets, restoring critical services, and resolving the attack. | | |
| --- | --- | --- | --- |
| Identify | Investigation revealed that the malicious actor exploited an unconfigured firewall vulnerability to launch the DDoS attack, so firewall, hosts and the internal networks are impacted by the attack. Therefore, web design teams, graphic design teams, and social media marketing teams are infected during the attack. | | |
| Protect | For the future protection, cyber analysts should maintain their firewall by setting a new policy to filter spoofed IP, unauthorized IP and limit incoming ICMP rate. Setting up NGFW is a better option because it can detect anomalies, so the company will have more advanced security. | | |
| Detect | SIEM and IDS are tools should be used in order to detect any cyber attacks. IDS can check for unauthorized IP in the IP header, then it will alert for the network administrator and SIEM tools will display further informations like location of the attacker, IP address,.. for the forensic investigator in order to investigate. | | |
| Respond | In order to protect company assets, firstly, security analysts should analyze the network logs to find out more about the problems, assets and people that are affected. Secondly, the security team should announce to all related people that they will isolate the network in a period of time. After that, shutting down and quarantining the networks and assets that are affected is crucial in order to start investigating and recover the problem. | | |
| Recover | The cyber analyst can recover the damage by erasing all ICMP requests in the network that has been flooded. After that, analysts should check functionality of devices and affected material to ensure that it can function normally after the attack. Finally, analysts can announce that the network will be put back to normal and they must report the incident to the manager. | | |

| Reflections/Notes: |
| --- |