**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** | Customers and users of our website complained of inability to access the website using the URL. Network log analysis showed that there was a flood of ICMP packets directed at our network server and this was responsible for its outage. Hence, legitimate network requests were denied. The team jumped into action by taking offline the affected devices as well as by implementing a series of protective and preventive actions including an update of the network access policies as well as the patching of the network firewall rules to prevent future occurrences of the attack. To improve the efficiency of our detection mechanisms, we installed both IDS/IPS systems to filter out known and learned malicious traffic. Similarly, Chronicle, a commercial SIEM was installed to replace the current one. The network is back online and running and recommendations were made to the upper management. |
| Identify | In addition to strong firewall rules, we installed both IDS/IPS systems to filter out some ICMP traffic based on suspicious characteristics. We equally installed a new version of Chronicle, a commercial SIEM tool to improve our capability to detect, analyze and respond to events happening within our network. These strategies form part of mechanisms that will improve our posturing. |
| Protect | The team implemented an updating of the processes and access policies as well as the patching of the network firewall rules to prevent future occurrences of the attack. These include:  1. setting a new rule firewall to limit the rate of incoming ICMP packets  2. Setting the firewall configuration to verify that the source IP address was not a spoofed IP address on incoming ICMP packets.  3. Purchase, install configure stateful firewall to monitor and actively stop malicious traffic based on traffic anomaly and learned behavior analysis. The optimal option would be to install a NGFWs which are more resilient against attacks. |
| Detect | In addition to strong firewall rules, we installed both IDS/IPS systems to filter out some ICMP traffic based on suspicious characteristics. We equally installed a new version of Chronicle, a commercial SIEM tool to improve our capability to detect, analyze and respond to events happening within our network. These strategies form part of mechanisms that will improv our posturing. |
| Respond | The malicious IP address was added to our list of restricted source IPs. Similarly, the team conducted extensive research to discover and collate known malicious traffic addresses, which we added to our list in order to forestall their potential routing directed at us. Finally, the combination of IDS/IPS, SIEM, stateful firewalls, and updated access permissions and rules are meant to improve our defense-in-depth mechanism specifically against intrusive attacks as DoS. We made efforts to ensure that these different measures are integrated in strategic ways to maximize their effectiveness and speed of response. Finally, the team informed the management suite about the attack and recommended that affected customers and staff are notified of the attack and successful recovery of business continuity. While the surety team has documented the details of the attack, it was suggested that the management notify law enforcement agents and other relevant statute regulators. |
| Recover | First, the security team must document and periodically update their baseline security configuration that strictly follows and comply with all relevant framework and laws. All devices, processes, ports and software, access permissions and systems must be regularly audited to verify their defense readiness. all end-users and staff must receive trainmen on cyber hygiene. |

|  |
| --- |
| Reflections/Notes: |