**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 network service stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic was unable to access any network resources due to this. To resolve this incident, the incident management team responded by blocking incoming ICMP packets, stopping all non- critical network services offline and restoring critical services. The cybersecurity team investigated the incident and saw that a threat actor sent a flood of ICMP pings through a firewall that is not configured. |
| Identify | This a Distributed Denial of Service ICMP flood attack through a n unconfigured firewall. |
| Protect | The organization should implement a firewall rule maintenance to ensure that the firewall is always checked, and properly configured. Network segmentation should be adopted moving forward so that in case of a breach, not all network resources will be affected. |
| Detect | Network analyzers can be utilized to troubleshoot the reason the organization network is not responding. SIEM tool can be utilized to collect and analyze incoming traffic data. The organization should setup alerts in the SIEM tool so they can be notified of breaches and better monitor the network traffic. Intrusion Detection system can also be used to protect against future incidents. |
| Respond | The organization should have measures in place to ensure that their firewalls are always configured. They could also use port filtering function of the firewall to limit unwanted communications. The organization should have a playbook that contains instructions on how to resolve incidents that occur, and they should continuously update the playbook. This is so that they can recover the system as soon as possible and reduce the amount of the downtime. The organization should also utilize updated patched of firewall and operating system. |
| Recover | The firewall needs to be configured immediately. They need to recover all network resources that were stopped. |

|  |
| --- |
| Reflections/Notes: The right stakeholders should be made aware of the incident. Security trainings that can serve as a lesson learned to prevent this issue from reoccurring and to help guide employees on how to resolve such issue quickly should also be conducted. |