**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 recently experienced a DDoS attack. The network was compromised for 2 hours before it was recovered. During the attack, the network was flooded with ICMP packets, and the system was not responsive. | | |
| --- | --- | --- | --- |
| Identify | ICMP flooding attack, known as DDoS occurred, in this case affecting the company’s network services through an unconfigured firewall. | | |
| Protect | **The firewall needs to be quickly configured to implement ip filtering, block unused ports, and limit the rate of ICMP requests. It is also a great idea to set up a backup server and use load balancing so the services remain functional under heavy traffic.** | | |
| Detect | To detect similar attacks and proactively prevent it, installation of an IDPS is highly suggested. The IDPS system will be able to monitor any suspicious network activities and block it in advance to minimize the impact. | | |
| Respond | For the future, it is a great practice to use segmentation and security groups, isolating the affected area to only small portions of the network. Now that the attack pattern is in hand, the same data can be used to detect similar future attacks and respond better. Tcpdump log or packet monitoring tools such as wireshark can be used to monitor and review the ongoing suspicious activities. | | |
| Recover | The affected service needs to be recovered immediately. If the server hosting the services is not responding, it is suggested to reboot the system and use the latest backup image to restore back to fully operational condition. The firewall also needs to be checked to see if it is correctly filtering unauthorized traffic. Since the attack only involved packet flooding but not any malware, the service should be recovered relatively quickly. In the meantime using the attack logs, set a timeout or blacklist the IP addresses used for the attack to wrap up the incident. | | |

| Reflections/Notes: |
| --- |