**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** | Recent attack on the organization was identified as ICMP DDoS attack, which compromised the internal network services, making them stop responding to normal internet traffic for resources. Incident management team responds to attack by blocking the ICMP traffic and taking all critical services offline. Then, the cybersecurity team investigated the security event, found the vulnerability and implemented new security measures. | | |
| --- | --- | --- | --- |
| Identify | The Incident management team identified the network services undergoing a DDos attack. The DDos attack also known as Distributed Denial of services attack involves many different categories based on threat actor tactics. The DDos attack on organizations generally involves sending ICMP packets non- stop to network resources such as servers. | | |
| Protect | **The Network security team should implement or refine new security controls for better protection of assets in organization. Starting from configuring new rules involves checking source ip address reputation on firewall and limiting rate of incoming packets to a destination, replacing existing firewalls with new generation firewalls which involves IDS/IPS functionalities, A network monitoring software to detect abnormal traffic.And finally a daily audit to check these configurations on network devices.** | | |
| Detect | Detecting is important, to be aware of suspicious activities taking place real time, we need data, one of the best solution would be engineering a SEIM architecture in organization network, SEIM architecture will help facilities collection of events logs from each devices and show data in form of dashboard on SIEM tool and also give real time alerts, which will not only be useful in present but in future as well. | | |
| Respond | Responding to such incidents should be done after detection, systems should be taken down for safety purposes and logs from these systems should be analyzed for attack details, for better management EDR tools should be utilized for immediate actions on these systems. Based on different attacks, different playbooks should be generated to ease incident response. | | |
| Recover | Since attacks target specific resourceful devices on an organization network, A full backup or snapshot(image) of these devices should be done periodically, to help recover of these systems incase of attacks compromised them. | | |

| Reflections/Notes: |
| --- |