**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | On the 25th of September, network services at HUBMED stopped responding, to ascertain the issue, Logs were analyzed and it became clear that networks had stopped responding due to a flood of ICMP packets, the incident management team responded by blocking incoming ICMP packets, stopping all non-critical services and restoring only the critical network services. After further investigations the following has been found out: |
| Identify | From the report given, the cause of the incident was a Distributed denial of service (DDos), an ICMP flood attack precisely, the threat actor gained access through a poorly unconfigured firewall, thereby flooding the network server with ICMP packets. |
| Protect | To deter and protect the network in the future, the firewall’s need to be properly configured, an IDS should be implemented into the network setup so as to detect suspicious attacks, Port filtering should be implemented, so as to regulate the ports being used. |
| Detect | Specific processes should be put into place to detect such attacks before and when they are initiated by the malicious actor, such as; implementing either IDS or IDP’s in the network setup, there should be frequent checks of the firewall. |
| Respond | If attacks such as this arise;  . the ports that are being used to enable the attacks should be blocked and regular business should be routed to other ports.  . after making sure that the attacks have ceased, the security supervisor should be contacted and properly briefed about the situation.  . the attack should be thoroughly investigated.  . Whatever findings are made should be use to craft a proper solution and response. |
| Recover | In the case of such incidents, backups of the servers should be reinstated and used so as to recover a proper working state, before the attacks ensued. |

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