**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | As a security team we noticed that users can’t reach our website, the web site is down, after investigating the traffic and logs we noticed that there is a flood of ICMP packets that are sending to server so server couldn’t response to legitimate requests. |
| Identify | Security team analyze logs and monitor the traffic then noticed that there is a DDoS attack by flooding ICMP packets to server. |
| Protect | **the team maintain firewall policies to prevent ICMP traffic to income our network and use IDS and IPS to prevent spoofed IPs from go through network.** |
| Detect | To detect new DDoS attacks in the future, the team will use a firewall logging tool and an intrusion detection system (IDS) to monitor all incoming traffic from the internet. |
| Respond | The team configure firewall to prevent ICMP packets from outside internal network. And as a future plan to response to a similar attack we recommend to block all unused ports and allow traffic only that is essential to work. |
| Recover | The team block ICMP flood attack so now service is work correctly. |

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