**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The incident occurred on the 25th of April at 12:06:47 pm and lasted a total of 2 hours. During this time our networking services were down and all normal traffic on the network could not access any network resources. This was due to a DDOS attack as our logs show that there was a large amount of ICMP pings sent into the orgs network through an unconfigured firewall from multiple end devices. |
| Identify | The security team audited the organization’s systems, devices and access policies to determine any gaps in the security. The team found that the malicious actor gained access to the network through an unconfigured firewall and used this entry point to flood the network with ICMP pings. This caused the organization’s systems to go down for a total of 2 hours. |
| Protect | To address this security issue, the team implemented:  A new firewall rule to limit the rate of incoming ICMP packets.  Source IP verification to check for IP Spoofing on incoming ICMP packets.  Network monitoring software to detect abnormalities in network traffic.  An IDS/IPS system to filter out some ICMP packets based on suspicious characteristics. |
| Detect | To detect future threats, the security team will use firewall logging tools ie. SIEM tools alongside an IDS to monitor incoming all traffic coming from the outside. |
| Respond | The team blocked all incoming ICMP packets and stopped all non-critical services while they restored the critical services. The team then created a new playbook on ensuring the correct configurations on all new firewalls. There was no data breach so no need to inform the public or law enforcement about the attack. |
| Recover | The team eased all services back up and running once the ICMP packet flood was contained |

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