**Incident report analysis**

| **Summary** | There was a flood of ICMP packets due to which the network services of the organization stopped responding. The IR team responded by blocking incoming ICMP packets, stopping all non critical network services offline, and restoring critical network network services and it took 2 hours to restore normal business activity. Investigation found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall and it was a DDOS attack. | | |
| --- | --- | --- | --- |
| Identify | The team Performed security audit to discover security gaps between organization’s assets and found an unconfigured firewall in this case.. | | |
| Protect | The team implemented a new firewall rule to limit the rate of incoming ICMP packets and source IP verification. Additionally the company will conduct regular training for employees on how to detect security incidents and will use intrusion prevention system and properly configured firewalls. | | |
| Detect | To detect future attacks the company will invest in implementing IDS system SEIM solutions. | | |
| Respond | The team isolated the affected assets, configured firewalls with new rules and implemented IDS/IPS systems. We informed upper management about this incident and they will contact customers through mail. | | |
| Recover | Deleted data will be recovered by restoring the database from last night’s backup. | | |