**Incident report analysis**

| **Summary** | This morning our organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.  During the attack, our organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. We were able to resolve this by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.  As we investigated the security event, We found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. | | |
| --- | --- | --- | --- |
| Identify | As the company’s cybersecurity team investigated this event we were able to find that the malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. Which compromised the company’s internal network through a DDoS attack | | |
| Protect | To address this security event, the team implemented:   * A new firewall rule to limit the rate of incoming ICMP packets * Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets * Network monitoring software to detect abnormal traffic patterns * An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics | | |
| Detect | To detect these kinds of events in future the team is investing in getting an new IPS which will help to filter out ICMP traffic based on suspicious characteristics. | | |
| Respond | In response to this attack we are going to update the firewall rules and make sure all the firewalls are configured properly to mitigate and contain this kind of attack if it ever happens. And the team will also isolate the affected systems for the time being. | | |
| Recover | To recover from DDoS attack all the non-critical network systems and services are halted to reduce the load on the network. And once the ICMP packets have been timed out all the halted services are resumed. In future the firewalls are configured to stop these attacks by limiting number of ICMP packets that can be sent. | | |

| Reflections/Notes: |
| --- |