**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | Our organization encountered a security breach by an unknown threat actor, which resulted in a compromise of the internal networks for duration of two hours.  During the attack, our organization’s network exercised disturbances, such as the sudden unresponsiveness caused by an influx of ICMP packets, thereby overloading the network making it unable to handle legitimate traffic effectively.  The attack was successfully mitigated and resolved |
| Identify | Our company’s incident management team promptly conducted an investigation into the security event. During our analysis, we discovered that a malicious actor had deliberately inundated the company’s network with barrage of ICMP pings.  This exploit was made possible due to an un-configured firewall, which provided an entry point for the attacker. Consequently, the malicious actor was able to successfully overwhelm our network through a Distributed Denial of Service (DDos) attack |
| Protect | Our team successfully implemented a new procedure to effectively protect the company’s network infrastructure against similar attack in the future. This includes the implementation of a new firewall rule that restricts the rate of incoming ICMP packets. This measure will significantly enhance the security of network infrastructure and greatly reduces the risk of potential attacks. We are confident that this proactive approach will ensure the utmost protection and provide a solid foundation for a secure and resilient network environment. |
| Detect | To proactively detect such occurrence in the future, the team will implement a security solution combining a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets with network monitoring software to detect abnormal traffic patterns. Furthermore, an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics was installed. |
| Respond | The team responded with varieties of measures which include the aforementioned procedures in detect column above.  The top management was adequately informed of the incident and steps taken in order to contain it. It was recommended to the management that periodic internal network audit must be a day-to-day basis for the organization. The management must ensure that the incident is reported to the necessary regulatory and law enforcement agency. |
| **Recover** | By blocking incoming ICMP packets and stopping all non-critical network services offline, the critical network services was fully restored and recovered |

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