**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | An DDoS Attack happened to the organization by using the ICMP packets flood incoming , the internal network stopped for 2 hours until the problem got solved ,During the attack, the 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. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The company’s cybersecurity team then investigated the security event. They 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 | The organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, your 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 |
| Protect | **• 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 | Have SIEM tools to Monitoring the traffic and get notifications about any unauthorized traffic and implement tcpdump tool to watch the system how it works. And have (NGFW) for all servers and have strong passwords policy . And have IDS system to detect any suspicious traffic. And segmentation the organization departments with using advanced encryption technicians and make security zone with (NGFW) , and the restricted zone must has high encryption. |
| Respond | If we put all the new tools and the DDoS happen again the NGFW will ban any suspicious traffic and the IDS system will notice and notify us, then we can get the log and see what happened to the traffic then tcpdump for the web Server. |
| Recover | For the recovery the organization must has a clean backup and test Environment in Case any attack happen we can Stimulate it and keep the backup clean , with high encryption for the sensitive data . |

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