**Incident report analysis**

| **Summary** | A flood of ICMP packets was sent to the network, resulting in the network crashing and not responding to valid requests. The incident management team blocked incoming ICMP packets, which stopped all non-critical network services offline and restored critical network services. | | |
| --- | --- | --- | --- |
| Identify | The flood of ICMP pings originated from an unconfigured firewall, likely leaving ports that were not being used open to attack. Normal internal network traffic was unable to access any network resources. This affected everyone on the network at the time. | | |
| Protect | Unauthorized access to ports not being used on the network is the cause of this DDOS attack. The firewall administrators need to be aware of this oversight. The firewall needs to be configured better, implementing port filtering to reduce the attack surface of the network. An IPS/IDS would also increase the security posture of the organization, as an ongoing attack could be identified and halted, giving more time for the team to respond. | | |
| Detect | IDS/IPS software is used to detect and respond to ongoing attacks involving the network logs. SIEM tools could also be used to identify attacks and spot vulnerabilities in the system. | | |
| Respond | Reconfiguration of the firewall to disable unused ports and limit the rate of ICMP packets will prevent DDOS attacks like this in the future. Because the attack was a DDOS, detecting and blocking suspected spoof IP addresses could also proactively prevent an attack like this in the future. | | |
| Recover | There was not any data damaged in the attack, just delayed internal processes on the network. The protections set in place should protect any attacks like this in the future, which will maintain organization productivity. Communicating the need for firewall patching to administrators is important in conducting regular security analysis. | | |

| Reflections/Notes: Regular penetration testing should be conducted to ensure that gaps within the firewall are not left to real threat actors to exploit. Comparing the current configurations of the firewall to the baseline should help in ensuring new threats are handled properly. Unused ports should be blocked to decrease the attack surface of the network. Implementing IDS/IPS software will help in conducting security analysis. SIEM tools used by the security team should be communicated to the appropriate stakeholders to ensure that security measures are discussed and taken. |
| --- |