**Incident report analysis**

| **Summary** | A DoS (Denial of Service) attack occured on the network. Specifically, this type of DoS attack is known as a ICMP flood. Under normal circumstances the ICMP protocol communicates network issues with hosts. When an attack occurs, a malicous actor or malcious actors can flood a server with these error requests which take up memory and bandwidth to process. This eventually means that legitimate data packets cannot be processed by the server and it will slow down server response time and even crash the server. | | |
| --- | --- | --- | --- |
| Identify | The security team discovered that an attacker had sent through an ICMP flood through an unconfigured firewall on the network. As these requests come through port 25 on a TCP/IP configuration the attack was identifiable and managble. | | |
| Protect | The Security team responded during the incident by blocking all ICMP packets to the server, stopping all non-critical network servers and bringing the server down to prevent further damage. After the attack, the process of securing the network was audited and new provisions were put into place. A new firewall rule was implemented to limit the amount of ICMP packets coming into the server, | | |
| Detect | Source IP verification for ICMP packets was set up on the firewall to limit the harm of spoofed IP addresses. An Incident Detection System / Incident Prevention System was also implemented to filter out suspicious ICMP traffic based on certain characteristics. Networking monitoring tools have also been set up. | | |
| Respond | The security team set up network monitoring, source IP verification and IDS / IPS, reconfigured the firewall to filter out ICMP packets | | |
| Recover | As this was a DoS attack and no Personal Identifying Information or Sensitive Personal Information was compromised, there was no need for legal disclosures. Once the server was reconfigured with the abovmentioned fixes and brought back online the attack stopped and normal business function continued. | | |

| Reflections/Notes: Upon further reflection, it may be helpful to develop internal playbooks for different security incidents and offer training on network safety to all employees, and specialized training to the IT Department to allow them to monitor and respond to incidents in a more affective manner in the future. An outline of how to deal with future security events can be found using the above template or reading up on the NIST CSF framework. |
| --- |