**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The company recently suffered a downtime of 2 hours due to a Distributed Denial of Service attack. The attack happened because the firewall was not configured therefore allowing the threat actor to overwhelm the server using a flood of ICMP pings. The downtime suffered by the company meant that normal internal traffic could not access the resources on the internal servers. This had significant financial and compliance implications.  The incident management team implemented security hardening by adding a new firewall rule which limited the rate of incoming ICMP Packets. By using a rate-limiting rule, persistent network requests coming from an individual IP address or from a distributed botnet will be blocked. The team also implemented a source IP address verification on the firewall to validate IP addresses on ICMP packets to guard against IP spoofing. A network monitoring software was installed to sniff network packets and detect abnormal traffic patterns. The Team also set up an IDS/IDP system to filter out suspicious ICMP traffic. |
| Identify | The investigation of the incident revealed that a malicious actor had launched a Distributed Denial of Service attack on the company’s internal network services. It is believed that the actor scanned and discovered an unconfigured firewall which granted access into the network’s internal systems. The threat actor then targeted the company’s internal servers using a type of DDoS attack called an ICMP flood attack. In an ICMP flood attack, a threat actor sends an overwhelming number of ICMP requests or echo-request packets to a network device (routers) causing the server to use up all available network bandwidth. This causes legitimate network requests to be dropped. The attack disrupted the normal business operations of the company as both customers and employees could not access the company’s private network. |
| Protect | Following the attack the security team must take the following steps to secure the network against future attacks:   1. Configure the firewall to block the ICMP attack using rate-limiting rules. 2. Install IDS/IPS softwares to sniff and monitor the network traffic for abnormal network activity and prevent future attacks. 3. Network segmentation should be put in place to isolate the company’s critical assets and data from their public internet facing resources. 4. Implement SIEM tools to monitor and aggregate network events and alarms on a single dashboard. 5. Implement source IP validation on the firewall to safeguard against IP spoofing. |
| Detect | To continuously monitor network traffic for suspicious activity, the company’s security team must monitor and analyze network traffic, software applications, track authorized versus unauthorized users, and detect any unusual activity on user accounts. To do this successfully, the following recommendations have been provided:   1. Installing a Security Information and Event Management tool will assist the security team to notice potential attacks and respond to them quickly. Google Chronicle or Splunk can be used for this purpose. 2. Packet sniffing tools such as network access analyser and Tcpdumps can be used to constantly monitor traffic flowing through the network devices. 3. Finally, implementing an intrusion detection system will assist the security team in detecting anomalies in network traffic patterns early and mitigate the effects of any attack. 4. An intrusion prevention system may be needed if a more proactive measure is required. |
| Respond | The security team will update the playbook with steps security team members must follow to mitigate similar attack in the future. Also constant security auditing must be carried out along with penetration testing to identify risks, threats and vulnerabilities that exist in the network infrastructure.  Reviewing network logs using TCPdumps or other SIEM tools will help the team investigate and gain more insight into the attack.  Team members will re-enact security incident procedures to improve their sense of urgency and response times to malicious activities by attackers.    In response to this specific kind of attack, the team must first block the source of the attack. This could involve reconfiguring the firewall rule set to block the malicious IP address from sending ICMP requests to the network. Next, the team must try to restore critical systems to their previous state.  Isolating network systems through network segmentation and implementing redundancy in network design will help reduce the impact of DDoS attacks such as ICMP flooding in the future. |
| Recover | The network security team must first stall the attack by using firewall rules and Intrusion detection and prevention systems. The team will recover the network data from the log files and commence investigation to discover the root cause of the attack. They will need to bring back up online any critical systems that may have been affected by the attack such as routers and DNS servers. |

|  |
| --- |
| Reflections/Notes: The security team must be take security seriously by carrying out audits at intervals to spot and risks, threats and vulnerabilities that exist in the system. They must then implement security hardening tasks to boost the company’s security posture and reduce the attack surface area. |