Incident report analysis

**Incident report analysis**

**Instructions**

|  |  |
| --- | --- |
| **Summary** | The company faced a DDoS attack that disrupted network services for two hours due to a flood of ICMP packets. The issue was caused by a misconfigured firewall, allowing the attacker to overwhelm the network.The security team responded by blocking ICMP traffic, restoring critical services, and fixing the firewall settings. |
| Identify | A malicious actor had sent a flood of ICMP packets into the company’s network due to an unconfigured firewall. The entire company network got affected. Need to bring back the network to a proper functioning state. |
| Protect | The security team applied new firewall rules to limit ICMP packet rates and implemented source IP verification to prevent spoofed attacks. |
| Detect | The security team deployed network monitoring to detect abnormal traffic and Installed IDS/IPS to filter and block suspicious ICMP packets. |
| Respond | For future security incidents, the cybersecurity team will isolate affected systems to contain the threat and minimize network disruptions. They will prioritize restoring any critical systems and services impacted by the event. Following recovery, the team will review network logs to identify any unusual or suspicious activity. Additionally, all incidents will be reported to upper management and, if necessary, to relevant legal authorities. |
| Recover | To recover from a DDoS attack caused by ICMP flooding, network services must be restored to normal. In the future, the firewall can be set to block ICMP flood attacks. During an attack, non-essential network services should be turned off to reduce traffic, while critical services should be restored first. Once the attack stops, all other network systems and services can be brought back online. |

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