**Incident report analysis activity**

| **Summary** | Recently the IT department of a multimedia company has reported of a DDos Attack. Which compromised the company's internal network for two hours. During the attack the company's service network stopped responding due to incoming flood of ICMP packets. Normal internal network traffic was unable to access any of the network resources or services. | | |
| --- | --- | --- | --- |
| Identify | The incident management team responded to the incident by blocking all incoming ICMP packets resulting in stopping all non critical network services and resources and restoring critical services and resources. After which the cybersecurity team investigated the event and found an unconfigured firewall. This led to a malicious threat actor being able to flood the system with DDos attack, where the threat actor overwhelmed the systems with ICMP packets. | | |
| Protect | The cybersecurity team put in place new firewall maintenance rule to limit the traffic of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on potentially suspicious characteristics. | | |
| Detect | To detect attacks in the future the team has put in place a source IP address verification on the firewall to check incoming ICMP packets for spoofed IP addresses, a network monitoring software to detect anomalies in the traffic patterns on the network. | | |
| Respond | In the future, the cybersecurity team will isolate affected systems  to prevent further damage or disruption to the company's network. They will attempt to restore any critical systems and services that were affected by the event. Then, the cybersecurity team will review the network logs to check for suspicious and abnormalities. . The team will also report all incidents and security events to upper management and appropriate law enforcement or organizations,if required. | | |
| Recover | First the team will need to restore access to network services back to normal. In the future, DDoS ICMP flood attacks can be blocked at the firewall. After that all network services that are non-crucial should be stopped to reduce internal traffic in the network. Next, critical network services should be restored first. Finally, once the ICMP flood attack has stopped, all non-critical network systems and services can be restored back online. | | |