**Incident report analysis**

**Instructions**

Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, your organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company’s cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack.

To address this security event, the network security team implemented:

* A new firewall rule to limit the rate of incoming ICMP packets
* Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
* Network monitoring software to detect abnormal traffic patterns
* An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

As a cybersecurity analyst, you are tasked with using this:

* **Identify** security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
* **Protect** internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
* **Detect** potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
* **Respond** to contain, neutralize, and analyze security incidents; implement improvements to the security process.
* **Recover** affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.

|  |  |
| --- | --- |
| **Summary** | Network traffic suddenly stopped during normal operations and no network services could be accessed. The incident management team uncovered a flood of ICMP packets congesting the network. They concluded a DDoS attack prevented the network from responding to any other request halting all network traffic and was possible because the firewall was unconfigured. The team blocked the incoming packets and the ip associated with the transmissions so that critical network services could be restored. |
| Identify | When the network services stopped responding, the security team analyzed the network logs and observed a flood of ICMP packets congesting the network. This DDOS prevented the network from responding to any other request halting the network. |
| Protect | The team will first block or limit the incoming packets and or the Ip’s associated with the transmissions, update and configure the fire wall, block any ports unnecessary for operations, and restore the company’s network so it is operational for business. |
| Detect | Implement an IPS or IDS alongside regular monitoring via SIEM tools to regulate traffic and prevent similar threat occurrence. |
| Respond | In the future similar attacks will be mitigated by implementing:   * A new firewall rule to limit the rate of incoming ICMP packets. * Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. * Network monitoring software to detect abnormal traffic patterns. * An IDS/IPS system to filter out(or alert to) some ICMP traffic based on suspicious characteristics. * Report all incidents to the appropriate stakeholders and legal authorities when necessary. * Isolating affected systems. |
| Recover | To recover from a DDoS, the intruding packets need to be identified and blocked via firewall, and critical network services need to be restored for necessary operations. Following these actions, firewall rules and monitoring need to be created and enforced, as well as the education and instruction of involved parties on the new operations and procedures with an update to the company’s playbook. |

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