Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

| **Summary** | The company experienced a security incident when network services became unresponsive due to a distributed denial of service (DDoS) attack caused by a flood of incoming ICMP packets. The cybersecurity team mitigated the disruption by blocking the attack and temporarily halting non-critical network services, allowing critical services to be restored. | | |
| --- | --- | --- | --- |
| **Identify** | A malicious actor launched an ICMP flood attack targeting the company, impacting the entire internal network. All critical network resources had to be secured and restored to full functionality. | | |
| **Protect** | The cybersecurity team established a firewall rule to regulate the flow of incoming ICMP packets and introduced an IDS/IPS system to identify and block ICMP traffic with suspicious traits. | | |
| **Detect** | The cybersecurity team set up source IP address verification on the firewall to detect and block spoofed IP addresses in incoming ICMP packets. Additionally, they deployed network monitoring software to identify unusual traffic patterns. | | |
| **Respond** | To address future security incidents, the cybersecurity team plans to isolate compromised systems to contain the disruption and prioritize the restoration of critical systems and services. They will analyze network logs to identify suspicious or abnormal activity and ensure all incidents are reported to upper management and, if necessary, the appropriate legal authorities. | | |
| **Recover** | To recover from an ICMP flood DDoS attack, access to network services must be restored to normal. In the future, external ICMP flood attacks can be blocked at the firewall. Next, non-critical network services should be temporarily halted to reduce internal traffic. Critical services should be restored first, followed by bringing non-critical systems and services online once the ICMP flood has subsided. | | |

| **Reflections/Notes:**   * **Incident Response:** Quick containment of the DDoS attack was critical, with a focus on restoring critical services first. * **Firewall Configuration:** Adjusting firewall rules, including rate-limiting and IP verification, proved essential in preventing further attacks. * **Network Monitoring:** Implementing monitoring tools helped detect abnormal traffic, aiding in early detection of threats. * **Post-Incident Analysis:** Log reviews and incident reporting provided key insights for improving future responses. * **Recovery Process:** Restoring critical services first and then non-critical ones was an effective recovery approach. * **Ongoing Improvements:** Future enhancements include implementing DDoS mitigation tools and refining the incident response plan for faster, more efficient reactions. |
| --- |