Incident Report Analysis

Scenario

Botium Toys recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, the 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.

Summary	Botium Toys recently suffered a DDoS attack that disrupted internal network services for two hours. The attack involved a flood of ICMP packets directed at the company's network, overwhelming its resources and preventing normal traffic. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored.
Identify	A malicious actor or actors targeted the company with an ICMP flood attack. **Identified Assets:** ● Internal network services. ● Firewall. ● Network monitoring tools. ● IDS/IPS systems. **Identified Threats:** ● DDoS attacks. ● Network vulnerabilities. **Identified Vulnerabilities:** ● Unconfigured firewall.
Protect	**Implement Security Controls:** ● Configure firewall rules to limit incoming ICMP traffic. ● Enable source IP address verification. ● Deploy network monitoring tools. ● Install IDS/IPS systems. **Protect Critical Assets:** ● Prioritize critical network services and implement additional security

	measures, such as load balancing and rate limiting.
Detect	**Implement Detection Controls:** ● Utilize network monitoring tools to detect anomalies and unusual traffic patterns. ● Configure IDS/IPS systems to identify and block malicious traffic.
Respond	**Incident Response Plan:** ● Activate the incident response plan to contain the attack and minimize damage. ● Isolate affected systems and block malicious traffic. ● Analyze network logs to check for suspicious and abnormal activity. ● Report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	**Recovery Plan:**. ● In the future, external ICMP flood attacks can be blocked at the firewall. ● All non-critical network services should be stopped to reduce internal network traffic. ● Critical network services should be restored first. ● Restore the rest of affected systems and services to their normal state ● Implement lessons learned from the incident to improve future security posture.

Reflections/Notes:

Integrating the Analysis into a General Security Strategy

1. **Regular Security Assessments:**
    - Conduct regular vulnerability assessments and penetration testing to identify and address weaknesses.
    - Update security controls and policies to adapt to evolving threats.
2. **Employee Training:**
    - Train employees on security awareness, including recognizing phishing attacks and social engineering tactics.
    - Conduct regular security awareness training to reinforce good security practices.
3. **Incident Response Plan:**
    - Develop and maintain a comprehensive incident response plan, including clear roles and responsibilities.
    - Regularly test and update the incident response plan.
4. **Continuous Monitoring:**
    - Implement continuous monitoring and logging to detect and respond to threats promptly.
    - Analyze logs to identify potential security incidents.
5. **Third-Party Risk Management:**
    - Assess the security practices of third-party vendors and suppliers.
    - Implement appropriate security measures to protect sensitive data shared with third parties.