Incident report analysis

By Jovworie Tanshi

Scenario

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 security event to create a plan to improve your company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity event and integrate your analysis into a general security strategy. We have broken the analysis into different parts in the template below. You can explore them here:

- 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	
Identify	• Conduct regular audits of networks, systems, devices, and access privileges. • Maintain an updated inventory of all hardware and software assets. • Regularly review and update access controls to ensure they align with the principle of least privilege.
Protect	• Develop and enforce comprehensive security policies and procedures. • Deploy technical controls, including properly configured firewalls and encryption for sensitive data.

	• Conduct regular cybersecurity training for employees.
Detect	• Implement and enhance network monitoring solutions, including IDS/IPS systems. • Configure alerts for suspicious activities and set thresholds for traffic anomalies. • Regularly review and analyze logs from network devices and security tools.
Respond	• Develop and maintain a detailed incident response plan. • Implement containment strategies to limit the impact of security incidents. • Conduct post-incident analysis to identify root causes and update security policies.
Recover	• Establish procedures to restore systems to normal operation, prioritizing critical systems. • Implement a robust backup and recovery strategy and regularly test these procedures. • Use insights from security incidents to continuously improve the security posture.

Reflections/Notes:

- **Incident Highlights:** DDoS attack revealed firewall misconfiguration and need for regular security audits.
- **Lessons Learned:**
  - Ensure proper configuration of security devices.
  - Importance of proactive network monitoring.
  - Ongoing employee cybersecurity training is crucial.
- **Future Actions:**
  - Enhance and test incident response plans.

    - Invest in advanced security solutions.
    - Conduct regular security drills.
- **Policy Updates:**
    - Regularly check firewall configurations.
    - Update access controls frequently.
    - Ensure robust data backup and recovery procedures.
- **Communication:**
    - Improve internal and external communication during incidents.

These steps will help us better prepare for and respond to future security incidents.