Incident report analysis

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 incident and integrate your analysis into a general security strategy:

- **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	The scenario involved a Distributed Denial of Service (DDoS) attack on the company. The attack targeted the company's network by flooding it with ICMP packets, causing the internal network services to become unresponsive for two hours. The incident was resolved by blocking incoming ICMP packets, taking non-critical network services offline, and restoring critical network services. The investigation revealed that the attack occurred due to a vulnerability in an unconfigured firewall, which allowed a malicious

	actor to overwhelm the network.
Identify	The company's cybersecurity team has investigated the security event. They found the company's network was flooded with ICMP packets. As a result, the internal network services were compromised and became unresponsive during the attack. The incident described in the scenario is a Distributed Denial of Service (DDoS) attack. **Devices and/or Systems Impacted:** 1. **Firewall:** The firewall was compromised due to being unconfigured, allowing the malicious actor to send a flood of ICMP pings into the network. 2. **Network Services:** Non-critical network services were stopped offline by the incident management team to mitigate the impact of the DDoS attack. 3. **Critical Network Services:** While the scenario does not provide specific details, it mentions that critical network services were restored, indicating that they were affected by the attack but successfully recovered.
Protect	To protect against future cybersecurity incidents, the following measures can be implemented: • **Regular Audits:** Conduct regular audits of internal networks, systems, devices, and access privileges to identify potential security gaps. This helps in identifying vulnerabilities and addressing them proactively. • **Firewall Rules:** Continuously review and update firewall rules to limit the rate of incoming ICMP packets and other potentially malicious traffic. This ensures that network resources are not overwhelmed by an excessive number of requests. • **Access Control:** Implement strong access control policies and procedures to restrict access to critical network resources. Regularly review and update access privileges to ensure that only authorized individuals have access to sensitive systems and data. • **Employee Training:** Provide cybersecurity awareness training to all employees. This training should include information on recognizing and reporting suspicious activities, social engineering attacks, and best practices for data protection. • **Patch Management:** Establish a robust patch management process to promptly apply security updates and patches to all systems and devices. Regularly update software and firmware to mitigate known vulnerabilities.
Detect	To improve monitoring capabilities and detect potential cybersecurity incidents, the following methods can be employed: • **Network Monitoring Software:** Deploy network monitoring software that can analyze traffic patterns and identify abnormal behavior. This software should generate alerts for suspicious activities, such as a sudden influx of ICMP packets or unusual network traffic.

	• **Intrusion Detection and Prevention System (IDS/IPS):** Implement an IDS/IPS system that can monitor network traffic in real-time and identify potential threats. Configure the system to filter out suspicious ICMP traffic based on predefined characteristics. • **Log Analysis:** Regularly analyze logs from network devices, servers, and security systems to identify any indicators of compromise or unusual activities. Automated log analysis tools can help in detecting patterns that may indicate a security incident.
Respond	To respond to the current cybersecurity incident, the following items should be implemented: • **Incident Containment:** As soon as the incident is detected, take immediate action to contain and mitigate the impact. This may involve blocking incoming ICMP packets, isolating affected systems, and diverting traffic to alternative resources. • **Incident Analysis:** Conduct a thorough analysis of the incident to determine the extent of the compromise and identify the vulnerabilities that allowed the attack to occur. This analysis will help in implementing improvements to the security process and preventing similar incidents in the future. • **Incident Response Plan:** Develop a comprehensive incident response plan that outlines the roles, responsibilities, and actions to be taken during a cybersecurity incident. This plan should include communication protocols, escalation procedures, and coordination with relevant stakeholders, such as IT teams, management, and external security experts if necessary. • **Incident Reporting:** Establish a reporting mechanism to ensure that all incidents are promptly reported, documented, and analyzed. This helps in identifying trends, understanding the evolving threat landscape, and implementing appropriate countermeasures. A playbook to respond to the similar cybersecurity event would be as follows: 1. **Activate Incident Response Team:** o Immediately notify and assemble the incident response team, o Designate a team lead and establish clear lines of communication. 2. **Assess the Situation:** o Gather information about the nature and extent of the incident, o Identify the affected systems, devices, or networks, o Determine the potential impact on critical business operations. 3. **Contain the Incident:** o Isolate affected systems, o Implement temporary measures to mitigate the ongoing threat. 4. **Preserve Evidence:** o Document and preserve all relevant evidence, o Maintain chain of custody. 5. **Mitigate the Attack:** o Implement immediate remediation measures to address vulnerabilities or weaknesses that were exploited during the incident.

	o Apply patches, updates, or configuration changes to affected systems. o Strengthen network defenses, such as updating firewall rules or implementing additional security controls. **6. Investigate and Analyze:** o Conduct a thorough investigation to identify the root cause of the incident. o Analyze the attack vectors, techniques, and tools used by the malicious actor. o Determine if any data or sensitive information was compromised. o Assess the impact on business operations and critical systems. **7. Notify Relevant Parties:** o Comply with legal and regulatory obligations by reporting the incident to appropriate authorities or governing bodies, if required. o Notify affected customers or stakeholders, providing necessary information and guidance on potential risks or protective measures. **8. Restore Systems and Services:** o Rebuild or restore affected systems from trusted backups or clean images. o Validate the integrity of restored systems and verify that they are free from malware or malicious modifications. o Gradually restore network services, ensuring proper monitoring and security measures are in place. **9. Learn and Improve:** o Conduct a comprehensive post-incident review to evaluate the effectiveness of the response and recovery efforts. o Identify lessons learned, vulnerabilities, or gaps in security controls. o Update incident response plans, security policies, and procedures based on the findings. o Provide training and awareness programs to educate employees on cybersecurity best practices. **10. Monitor and Maintain:** o Implement continuous monitoring and threat intelligence capabilities to detect and prevent future incidents. o Regularly review and update security measures, including firewall rules, intrusion detection systems, and access controls. o Conduct periodic penetration testing and vulnerability assessments to identify and address potential weaknesses in the network.
Recover	To recover from similar future cybersecurity incidents, the following strategies can be employed: • **Incident Documentation:** o Document the details of the cybersecurity event, including the timeline, affected systems, and the actions taken during the incident response process. Maintain a comprehensive incident report that can serve as a reference for future incidents and for regulatory compliance purposes. • **Patching and Updates:** o Apply patches, updates, and security fixes to all systems and software to address vulnerabilities that were exploited during the incident. Prioritize

	critical patches based on their severity and potential impact on the organization's security.
	• **Password Resets and Access Control:**
	  o Force password resets for all user accounts to mitigate the risk of unauthorized access. Implement stronger password policies, such as complexity requirements and regular password rotations. Review and modify access control lists and user permissions to ensure appropriate levels of access and reduce the risk of future unauthorized activities.
	• **System and Network Hardening:**
	  o Conduct a thorough security assessment of all systems, networks, and configurations to identify and remediate security weaknesses. Implement security best practices, such as disabling unnecessary services, applying appropriate firewall rules, and enabling encryption where applicable. Implement multi-factor authentication (MFA) for critical systems and privileged accounts.
	• **Monitoring and Detection:**
	  o Deploy or enhance monitoring and detection systems, such as intrusion detection/prevention systems (IDS/IPS), Security Information and Event Management (SIEM) solutions, and network traffic analysis tools. Continuously monitor network traffic, system logs, and security alerts for any signs of suspicious activities or indicators of compromise (IOCs).
	• **Incident Response Plan Review and Enhancement:**
	  o Review the effectiveness of the incident response plan used during the incident and identify areas for improvement. Update the incident response plan to incorporate lessons learned, new security controls, and revised communication protocols. Conduct regular tabletop exercises and simulations to validate the effectiveness of the updated incident response plan.
	• **Employee Training and Awareness:**
	  o Provide cybersecurity training and awareness programs to all employees to educate them about the incident, the actions taken to mitigate it, and their roles and responsibilities in maintaining a secure environment. Reinforce best practices, such as safe browsing habits, email security, and the importance of reporting any suspicious activities or incidents promptly.
	• **Continuous Improvement and Lessons Learned:**
	  o Conduct a post-incident analysis to identify the root cause of the cybersecurity event and implement measures to prevent similar incidents in the future. Share the lessons learned with the organization's cybersecurity team and management to enhance the overall security posture. Regularly assess and update security policies, procedures, and controls to adapt to evolving threats and technology.

Reflections/Notes: Continuous monitoring and baseline configurations will be of high importance going forward. Nonstop vigilance is required to protect against potential threats.