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 multimedia company faced a DDoS attack that disrupted internal network services for two hours due to a flood of ICMP packets exploiting an unconfigured firewall. The attack halted access to critical resources. The cybersecurity team responded by blocking ICMP traffic and restoring essential services, highlighting the need for improved firewall configurations.
Identify	The multimedia company experienced a Distributed Denial of Service (DDoS) attack that compromised internal network services for two hours. The attack was initiated through a flood of ICMP packets exploiting an unconfigured firewall, preventing normal internal network traffic from accessing critical resources. The targeted systems included the company’s internal network infrastructure,s and the attack likely originated from a coordinated botnet. This incident highlighted vulnerabilities in the company's network configuration, emphasizing the need for enhanced security measures and proper firewall management.
Protect	To enhance the organization's security following the DDoS attack, it is essential to update the firewall configuration to block unnecessary traffic, implement and enhance Intrusion Detection and Prevention Systems (IDPS) for monitoring threats, segment the network to isolate critical systems, introduce traffic filtering for ICMP protocols, revise the incident response plan for DDoS scenarios, increase employee training

	on cybersecurity awareness, conduct regular vulnerability assessments and penetration testing, improve monitoring and logging with a SIEM system, and establish a consistent patch management process for software and systems.
Detect	To monitor for suspicious activity, the team will implement network traffic analysis tools specifically to scrutinize incoming ICMP packets from non-trusted IP addresses, utilize Security Information and Event Management (SIEM) systems to analyze logs for unusual patterns, and deploy user behavior analytics (UBA) to detect anomalies in user account activity, ensuring that monitoring is focused on identifying potential security threats while respecting user privacy.
Respond	• **How can you and your team contain cybersecurity incidents and affected devices?** To contain cybersecurity incidents, the team will isolate compromised systems by removing them from the network and utilizing segmentation to limit access thereby reducing the attack surface of the incident • **What procedures are in place to help you and your team neutralize cybersecurity incidents?** The procedures include activating the Incident Response Plan (IRP), conducting a thorough forensic analysis to identify the root cause, applying necessary patches or updates, and communicating with stakeholders about the incident and recovery steps. • **What data or information can be used to analyze this incident?** Data for analysis will include network logs, intrusion detection system (IDS) alerts, system event logs, and user activity reports, which provide insights into the attack vectors and timeline of the incident for better understanding and future prevention.

	• **How can your organization's recovery process be improved to better handle future cybersecurity incidents?** The recovery process can be improved by conducting post-incident reviews to evaluate response effectiveness, enhancing employee training on threat recognition, and regularly updating incident response protocols to incorporate lessons learned from previous incidents.
Recover	• **What information do you need to be able to recover immediately?** To recover immediately, we need access to backup data, system configurations, and documentation of the affected network architecture, as well as logs of user activity and security incidents to ensure a complete restoration of services and resources. • **What processes are in place to help the organization recover from the incident?** The organization has established processes that include regularly scheduled backups to secure data, a disaster recovery plan to guide system restoration, and a clear communication plan to inform stakeholders about recovery progress and timelines, ensuring minimal disruption to operations.

Reflections/Notes:

1. Incident Overview:

The DDoS attack caused significant disruption to the multimedia company's internal network, rendering services unresponsive for two hours. This incident highlights the vulnerability of relying solely on a perimeter defense without proper firewall configuration.

2. Root Cause Analysis:

The attack exploited an unconfigured firewall, allowing a flood of ICMP packets to overwhelm the network. This incident emphasizes the importance of regularly reviewing and updating firewall settings to prevent unauthorized access.

3. Impact Assessment:

The inability to access network resources during the attack likely affected business operations and client services, potentially leading to loss of trust from small business clients who rely on the company for critical services.

4. Response Evaluation:

The incident management team's immediate response to block incoming ICMP packets and restore critical services was effective in mitigating further damage. However, a more proactive approach, such as implementing rate limiting on ICMP traffic, could have reduced the initial impact.

5. Lessons Learned:

- ✓ *Importance of Firewall Configuration*: Regular audits and proper configuration of firewalls are crucial to securing the network against DDoS attacks.
- ✓ *Proactive Defense Measures*: Implementing network segmentation and traffic filtering can help contain the impact of similar attacks in the future.
- ✓ *Incident Response Preparedness:* The incident highlighted the need for ongoing training and simulations for the cybersecurity team to ensure rapid and effective incident response.

6. Recommendations for Future Prevention:

- ➢ Conduct a comprehensive review of network security policies and procedures.
- ➢ Implement Intrusion Detection and Prevention Systems (IDPS) to monitor and mitigate suspicious activity.
- ➢ Establish a continuous monitoring system to detect unusual traffic patterns early and respond accordingly.

7. Next Steps:

- ✓ Schedule a post-incident review meeting with all stakeholders to discuss findings and recommendations.
- ✓ Update the Incident Response Playbook based on lessons learned from the attack.
- ✓ Increase employee awareness training on recognizing and responding to potential