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	On 10/10/24, our multimedia company experienced a Distributed Denial of Service (DDoS) attack that lasted approximately two hours. Employees reported an inability to access critical internal network services, including web and graphic design platforms. The attack involved a massive influx of Internet Control Message Protocol (ICMP) packets, overwhelming our network. Initial investigations suggest that the attack exploited vulnerabilities in our firewall, which failed to adequately filter incoming traffic. As a result, business operations were disrupted, leading to potential financial loss and reputational damage. The estimated impact of this incident includes service downtime, loss of productivity, and possible compensation claims from clients due to service disruptions.
Identify	**The incident management team conducted an audit of the affected systems and found that the DDoS attack successfully disrupted multiple internal services. It was determined that the malicious actors utilized spoofed IP addresses to flood the network with traffic, causing significant downtime. The systems affected included:**

	● Internal web and graphic design platforms. **● Network servers hosting critical applications.** **● User workstations attempting to connect to these services.** **Upon initial review, it appears that our firewall and intrusion detection systems were not adequately prepared to handle the volume of incoming traffic, highlighting gaps in our security infrastructure.**
Protect	**In response to this incident, the team has implemented several protective measures to enhance our cybersecurity posture:** **● Firewall Configuration: Updated firewall rules to block incoming ICMP packets from untrusted sources.** **● Rate Limiting: Introduced rate limiting on incoming traffic to mitigate potential DDoS attacks.** **● Employee Training: Conducted training sessions for employees on recognizing and reporting suspicious network activity.** **● Regular Security Audits: Scheduled periodic security audits to identify vulnerabilities in our systems.** **These immediate actions aim to ensure that our assets are better protected against similar threats in the future.**
Detect	To better detect unauthorized access attempts in the future, we will employ the following methods: ● **Network Monitoring Tools:** Utilize advanced network monitoring tools to analyze traffic patterns and detect anomalies in real time. ● **Intrusion Detection System (IDS):** Implement an IDS to alert our cybersecurity team of any suspicious activities on the network.

	● **Log Management:** Establish a centralized log management system to track incoming and outgoing traffic for further analysis and historical reference. ● **Regular Traffic Analysis:** Implement continuous analysis of network traffic, particularly monitoring for incoming external ICMP packets from non-trusted IP addresses attempting to pass through the organization's network firewall.
Respond	In the immediate aftermath of the incident, the team took the following actions: ● **Service Restoration:** Disabled affected services and isolated them from the network to prevent further damage. ● **Management Communication:** Informed upper management about the event, prompting a review of our incident response plan. ● **Customer Notification:** Prepared to communicate with customers regarding the service disruption and any potential impacts on their data. ● **Incident Documentation:** Documented all actions taken during the incident for future reference and improvement. Moving forward, we will review and refine our incident response procedures to ensure a more effective response to future incidents, including developing a detailed playbook for handling DDoS attacks.
Recover	To facilitate recovery from this incident, we have outlined the following steps: ● **System Restoration:** Restore affected systems and services from backups taken before the attack. ● **Data Integrity Verification:** Conduct a thorough check to ensure the

	integrity of data once services are restored. ● **Documentation Review:** Document the incident and the response actions taken to provide a foundation for future training and improvement. ● **Immediate Recovery Needs:** Ensure we have access to backup data and logs to facilitate a swift recovery. Staff has been notified that any changes made to data during the attack period may not be recorded, and they will need to re-enter any critical information post-restoration.

Reflections/Notes:

- Ensure continuous training for employees to recognize and report unusual network activity.
- Conduct regular reviews of firewall settings and overall network security protocols to adapt to evolving threats.