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	Event: Distributed Denial of Service (DDoS) attack Cause: A malicious actor sent a flood of ICMP packets into the company's network through an unconfigured firewall. Impact: Network services were unresponsive for two hours. Normal internal network traffic could not access any network resources. Critical network services were temporarily taken offline for restoration. Response: • Blocked incoming ICMP packets. • Stopped all non-critical network services. • Restored critical network services. • Investigated the event and identified the vulnerability in the firewall. Targeted Systems: Internal network services and resources. Attack Source: Malicious actor using spoofed IP addresses. Estimated Impact: Two-hour downtime for internal network services, affecting productivity and potentially causing financial and reputational damage.
Identify	Distributed Denial of Service (DDoS) attack affected Internal network services, firewall, and network monitoring systems.
Protect	Immediate Action Plan: 1. Firewall Configuration: ○ Implement strict firewall rules to limit the rate of incoming ICMP packets. ○ Ensure the firewall is configured to block unsolicited ICMP traffic by default. 2. Source IP Verification: ○ Enable source IP address verification on the firewall to detect and block spoofed IP addresses. 3. Employee Training: ○ Conduct regular training sessions on recognizing and responding to potential cybersecurity threats. ○ Update incident response protocols and ensure all employees

	are familiar with them. 4. Security Policies: ○ Review and update security policies to include guidelines on handling DDoS attacks. ○ Implement stricter access control measures to minimize potential attack vectors.
Detect	1. Network Monitoring Software: ○ Deploy and maintain network monitoring software to detect abnormal traffic patterns in real-time. ○ Set up alerts for unusual spikes in network traffic or incoming ICMP packets. 2. Intrusion Detection and Prevention Systems (IDS/IPS): ○ Use IDS/IPS to filter out ICMP traffic based on suspicious characteristics. ○ Continuously update IDS/IPS signatures to recognize and block new threats. 3. User Activity Tracking: ○ Implement software to track and log user activities, distinguishing between authorized and unauthorized access. ○ Regularly review logs for signs of unusual activity or potential security breaches. 4. Regular Audits: ○ Conduct regular security audits of internal networks, systems, and devices to identify potential vulnerabilities. ○ Ensure access privileges are reviewed and updated regularly.
Respond	1. Containment: ○ Immediately block suspicious traffic and isolate affected devices from the network. ○ Disable non-critical services to focus resources on critical system restoration. 2. Neutralization: ○ Identify and block the source of the attack using firewall rules and IDS/IPS. ○ Remove any malicious software or code from affected systems. 3. Analysis: ○ Collect and analyze data related to the incident, including logs, network traffic, and system behavior. ○ Identify the root cause of the attack and any exploited vulnerabilities.

	4. Improvement: ○ Update security protocols based on the analysis of the incident. ○ Implement additional safeguards to prevent similar attacks in the future.
Recover	To recover from the cybersecurity incident, immediate access to recent backups of critical systems and data is essential, as well as detailed documentation of affected systems and the extent of the damage. The organization should follow established recovery processes, which include restoring systems from backups, verifying their integrity, and securely reconnecting isolated devices to the network. A post-incident review will identify lessons learned, ensuring recovery plans are updated and team members are trained on new procedures. Effective communication with stakeholders about the incident, recovery steps, and security measures taken is crucial for maintaining transparency and trust.

Reflections/Notes: