**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** | **Security Event**: Distributed Denial of Service (DDoS) attack  **Cause**: Flood of ICMP packets from a malicious actor exploiting an unconfigured firewall  **Impact**: Internal network services were down for two hours, affecting the company's web design, graphic design, and social media marketing services. Normal internal network traffic could not access any network resources.  **Response**: Blocked incoming ICMP packets, stopped all non-critical network services, restored critical network services, implemented a new firewall rule to limit ICMP packets, verified source IP addresses, installed network monitoring software, and deployed an IDS/IPS system. | | |
| --- | --- | --- | --- |
| Identify | **Type of Attack**: DDoS attack using ICMP packets (Ping Flood)  **Affected Systems**:   * Internal network infrastructure * Network services supporting web design, graphic design, and social media marketing   **Attack Source**: External malicious actor leveraging an unconfigured firewall to send a flood of ICMP packets.  **Estimated Impact**:   * Two hours of downtime for internal network services * Potential loss of business due to service interruption * Increased costs for incident response and mitigation | | |
| Protect | **Immediate Action Plan:**   1. **Firewall Configuration:**    * **Ensure all firewalls are properly configured and regularly updated.**    * **Implement rules to limit the rate of incoming ICMP packets.**    * **Enable source IP address verification to detect and block spoofed IP addresses.** 2. **Network Segmentation:**    * **Segment the network to limit the impact of potential DDoS attacks.**    * **Isolate critical services from non-critical services.** 3. **Access Control:**    * **Conduct regular audits of access privileges to ensure only authorized personnel have access to sensitive systems.**    * **Implement multi-factor authentication (MFA) for accessing critical systems.** 4. **Employee Training:**    * **Conduct regular cybersecurity awareness training for employees.**    * **Educate staff on recognizing and reporting suspicious activities.** 5. **Policies and Procedures:**    * **Develop and enforce policies for network security, including incident response and management.**    * **Regularly review and update security policies to address new threats.** | | |
| Detect | **Monitoring and Analysis**:   1. **Network Traffic Monitoring**:    * Implement network monitoring software to continuously monitor traffic.    * Use intrusion detection systems (IDS) and intrusion prevention systems (IPS) to detect abnormal traffic patterns and suspicious activities. 2. **Log Analysis**:    * Regularly review logs from firewalls, IDS/IPS, and network devices.    * Implement log management solutions to aggregate and analyze logs for signs of potential threats. 3. **User Activity Monitoring**:    * Track authorized versus unauthorized user activities.    * Use user behavior analytics to detect unusual account activities. 4. **Threat Intelligence**:    * Subscribe to threat intelligence feeds to stay informed about emerging threats.    * Integrate threat intelligence with monitoring tools to improve detection capabilities. | | |
| Respond | **Response Plan**:   1. **Containment**:    * Immediately block or limit traffic from suspicious sources.    * Isolate affected systems to prevent further spread of the attack. 2. **Neutralization**:    * Deploy patches and updates to fix vulnerabilities.    * Use IDS/IPS to filter out malicious traffic. 3. **Analysis**:    * Collect data and logs related to the incident for forensic analysis.    * Identify the root cause and attack vector. 4. **Communication**:    * Inform relevant stakeholders about the incident and response actions.    * Coordinate with external partners and law enforcement if necessary. 5. **Documentation**:    * Document the incident, response actions, and lessons learned.    * Update incident response plans based on findings. | | |
| Recover | **Recovery Steps**:   1. **Restore Services**:    * Gradually restore affected network services to normal operation.    * Verify the integrity and functionality of restored services. 2. **Data Recovery**:    * Recover any lost or corrupted data from backups.    * Ensure data integrity and consistency. 3. **Post-Incident Review**:    * Conduct a post-incident review to identify gaps and improve response strategies.    * Update recovery processes based on lessons learned. 4. **System Updates**:    * Apply necessary updates and patches to systems.    * Strengthen security configurations to prevent similar incidents in the future. 5. **Ongoing Monitoring**:    * Continue monitoring the network for any signs of lingering issues.    * Ensure continuous improvement of detection and response capabilities.   **Information Needed for Recovery**:   * Comprehensive logs and data collected during the incident * Backup data for affected systems and services * Detailed incident report and analysis * Updated incident response and recovery plans   **Processes in Place for Recovery**:   * Regular data backups and validation * Predefined incident response and recovery procedures * Coordination with IT and cybersecurity teams for restoration efforts * Continuous communication with stakeholders during the recovery process | | |

| Reflections/Notes: |
| --- |