**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:  The organization experienced a Distributed Denial of Service (DDoS) attack that overwhelmed the internal network with a flood of ICMP (ping) packets. This caused a two-hour outage, during which internal network services were unresponsive, and employees could not access critical resources.  Cause:  The attack was caused by an unconfigured firewall that allowed malicious actors to send a flood of ICMP packets into the network. The attacker exploited this vulnerability to launch the DDoS attack, overwhelming the network and rendering it inaccessible.  Impact:  1. Duration: 2 hours of network downtime.  2. Affected Systems: Internal network services, including web design, graphic design, and social media marketing tools.  3. Business Impact: Disruption of services for small business clients, potential loss of revenue, and damage to the company’s reputation.  Attack Source: External malicious actor(s) using spoofed IP addresses to send ICMP packets.  Response:  1. The incident management team blocked incoming ICMP packets.  2. Non-critical network services were taken offline to reduce the load.  3. Critical services were restored after the attack was mitigated.  4. The cybersecurity team implemented new firewall rules, IP address verification, network monitoring software, and an IDS/IPS system to prevent future attacks. |
| Identify | Type of Attack:  Distributed Denial of Service (DDoS) Attack: The attacker flooded the network with ICMP packets, overwhelming its capacity and causing a service outage.  Affected Systems:  1. Internal network services (web design, graphic design, and social media marketing tools).  2. Firewall (unconfigured, allowing the attack to occur).  3. Network infrastructure (routers, switches, and servers).  Vulnerabilities Identified:  1. Unconfigured firewall allowing unrestricted ICMP traffic.  2. Lack of rate limiting for ICMP packets.  3. Insufficient monitoring of incoming traffic for abnormal patterns. |
| Protect | Firewall Configuration:  1. Implement rate limiting for ICMP packets to prevent flooding.  2. Enable source IP address verification to block spoofed IP addresses.  1. Network Segmentation:  Segment the network to isolate critical services from non-critical ones, reducing the impact of future attacks.  2. Patch Management:  Ensure all network devices, including firewalls, are updated with the latest firmware and security patches.  3. Access Control:  Review and update access privileges to ensure only authorized users have access to critical systems.  4. Employee Training:  Conduct cybersecurity awareness training to help employees recognize and report suspicious activity.  5. Backup and Recovery:  Ensure regular backups of critical data and systems are performed and tested for reliability. |
| Detect | 1. Network Monitoring Tools:  Deploy advanced network monitoring software to detect abnormal traffic patterns, such as sudden spikes in ICMP packets.  2. Intrusion Detection/Prevention Systems (IDS/IPS):  Use IDS/IPS to filter out suspicious ICMP traffic and other potential threats.  3. Log Analysis:  Regularly review firewall and network device logs for signs of unauthorized access or unusual activity.  4. User Activity Monitoring:  Implement tools to track authorized vs. unauthorized user activity and detect anomalies in user accounts.  5. Threat Intelligence:  Subscribe to threat intelligence feeds to stay informed about emerging threats and attack techniques. |
| Respond | Containment:  1. Immediately isolate affected systems to prevent the spread of the attack.  2. Block malicious IP addresses and disable compromised accounts.  Neutralization:  1. Use IDS/IPS to filter out malicious traffic.  2. Apply firewall rules to limit the impact of the attack.  Analysis:  1. Collect and analyze logs from firewalls, network devices, and monitoring tools to identify the attack source and method.  2. Document the incident details, including the timeline, impact, and response actions.  Recovery Improvement:  1. Develop a playbook for responding to DDoS attacks, including predefined roles and responsibilities.  2. Conduct regular incident response drills to ensure the team is prepared for future attacks. |
| Recover | Restore Systems:  1. Prioritize the restoration of critical systems and services.  2. Verify that all systems are functioning normally before bringing non-critical services back online.  Data Recovery:  1. Restore any lost or corrupted data from backups.  2. Ensure backups are up-to-date and tested for reliability.  Post-Incident Review:  1. Conduct a post-incident review to identify lessons learned and areas for improvement.  2. Update the incident response plan based on the findings.  Communication:  1. Notify affected clients and stakeholders about the incident and the steps taken to resolve it.  2. Provide transparency to maintain trust and confidence.  Continuous Monitoring:  1. Increase monitoring of network traffic and systems in the days following the incident to ensure no residual threats remain. |

|  |
| --- |
| Reflections/Notes: By following the NIST Cybersecurity Framework (CSF) and addressing each phase (Identify, Protect, Detect, Respond, Recover), the organization can improve its network security posture and better prepare for future cybersecurity incidents. |