**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** | A DDoS (Distributed Denial of Service) attack targeted the company’s network, overwhelming it with a flood of ICMP packets. The attack lasted approximately two hours, during which the internal network was rendered non-operational. Network services became unresponsive, and employees were unable to access any internal systems or tools. The source of the attack exploited an unconfigured firewall that allowed external ICMP packets. The attack was mitigated by blocking incoming ICMP traffic, shutting down non-critical services, and restoring critical ones. The cybersecurity team later confirmed the attack source and applied long-term security measures. |
| Identify | The security incident was a DDoS attack using a flood of ICMP (ping) packets. The attacker exploited a misconfigured firewall that failed to restrict ICMP traffic. This resulted in the unavailability of network services across the organization. Impacted systems included internal application servers, employee workstations, and network infrastructure (e.g., routers and switches). The attack originated from multiple external IPs, consistent with distributed attack behavior. |
| Protect | **To better protect internal assets, the organization must:**   * **Review and configure firewalls to block or rate-limit non-essential ICMP traffic.** * **Implement access control rules to restrict unnecessary inbound traffic.** * **Apply regular security patches and perform configuration audits.** * **Conduct staff training on network hardening practices.** * **Use rate-limiting techniques to prevent packet flooding.** |
| Detect | To improve detection:   * Deploy **network monitoring tools** (e.g., Wireshark, SolarWinds) to analyze traffic patterns. * Use **IDS/IPS systems** to filter suspicious packets (e.g., Snort, Suricata). * Enable logging on firewalls and network devices. * Establish alerts for abnormal spikes in ICMP or other traffic types. * Implement SIEM (Security Information and Event Management) tools to correlate data and detect anomalies. |
| Respond | In future incidents:   * Use pre-defined **incident response playbooks** to isolate affected network segments quickly. * Communicate with staff and stakeholders using designated internal channels. * Collect and analyze logs for forensic investigation. * Involve the IT and legal teams if attack severity justifies it. * Update firewall rules and mitigation tools based on attack signature. |
| Recover | To recover from such attacks:   * Restore affected systems and services using backups and redundancy mechanisms. * Perform post-incident reviews and patch any configuration gaps. * Document the incident in detail for internal knowledge and compliance. * Re-test network availability and confirm integrity before restoring full access. * Update disaster recovery plans and include DDoS-specific scenarios. |

|  |
| --- |
| Reflections/Notes:  This incident highlighted the importance of proactive firewall configuration and continuous network monitoring. A simple oversight—allowing unrestricted ICMP traffic—led to a significant disruption. Going forward, we must prioritize:   * Regular firewall audits to identify misconfigurations. * Continuous training for IT staff on evolving attack methods like DDoS. * Implementation of layered defense mechanisms (firewall, IDS, rate-limiting, SIEM). * Documentation of incident response steps to improve future reaction time.   This event reinforced how critical it is to align real-time operations with the NIST CSF framework to create a resilient cybersecurity posture. |