**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** | Today the organization’s internal network services suddenly stopped responding, preventing employees from accessing critical resources. Logs indicated a massive flood of ICMP packets entering the network through an unconfigured firewall, overwhelming network capacity. Further investigation confirmed this was a Distributed Denial of Service (DDoS) attack launched by a malicious actor.  During the two-hour disruption, normal business operations were interrupted, as users were unable to access internal systems. To mitigate the attack, the incident response team blocked incoming ICMP packets, took non-critical services offline to reduce strain, and restored critical services to maintain business continuity.  The root cause was identified as a firewall misconfiguration that allowed unrestricted ICMP traffic, which the attacker exploited. As a result, the organization experienced significant downtime and operational disruption, although no data exfiltration or manipulation was detected. | | |
| --- | --- | --- | --- |
| Identify | The incident management team audited the network infrastructure and firewall configurations involved in the attack to identify the gaps in security. The team found that an unconfigured firewall allowed a flood of ICMP packets from an external malicious actor to enter the network. This vulnerability was exploited to overwhelm the organization’s internal network services, resulting in a two-hour disruption. Upon initial review, it appears that no data was stolen or altered, but internal network operations and business activities were significantly impacted during the downtime. | | |
| Protect | To further secure the organization’s assets, the following updates and changes should be implemented:  Firewall Configuration: Update firewall rules to restrict and rate-limit incoming ICMP traffic, ensuring only necessary network traffic is allowed.  Access Controls: Review and enforce stricter access policies for internal systems, limiting unnecessary permissions.  Security Policies & Procedures: Develop and update incident response and firewall management policies to ensure misconfigurations are identified and corrected proactively.  Employee Training: Provide staff with regular security awareness training to ensure they understand how to recognize and report unusual system behavior or network issues quickly. | | |
| Detect | The organization should strengthen its monitoring capabilities to identify suspicious activity more quickly and accurately. This includes:  Network Traffic Monitoring: Continuously monitor incoming and outgoing traffic to detect abnormal patterns, such as ICMP floods or traffic from non-trusted IP addresses.  Intrusion Detection/Prevention Systems (IDS/IPS): Deploy IDS/IPS tools to flag and filter malicious traffic attempting to exploit the firewall or overwhelm network resources.  Log Analysis: Regularly review firewall, server, and application logs for unusual behavior or unauthorized access attempts.  User Account Monitoring: Track login activity to detect unusual behavior, such as access attempts outside normal hours or from unusual geographic locations.  Automated Alerts: Configure real-time alerts for security teams when suspicious network activity, spikes in traffic, or unauthorized user actions are detected.  By strengthening monitoring and detection systems, the organization can respond to potential threats before they escalate into major incidents. | | |
| Respond | To effectively contain and neutralize cybersecurity incidents, the organization should implement the following response measures:  Incident Containment: Immediately block malicious traffic (e.g., ICMP floods) by applying firewall rules and isolating affected systems to prevent further impact.  Service Prioritization: Temporarily take non-critical services offline while ensuring that critical business services are restored quickly to maintain operations.  Root Cause Analysis: Investigate the incident to identify how the attack was carried out (e.g., misconfigured firewall) and document findings for future reference.  Communication Plan: Notify internal stakeholders about the incident status, impact, and recovery steps; communicate transparently with clients if external-facing services are affected.  Policy and Procedure Updates: Update security policies, firewall configurations, and incident response playbooks to address the vulnerabilities that enabled the attack.  These steps ensure the organization can quickly respond, minimize damage, and strengthen resilience against future incidents. | | |
| Recover | To restore normal operations and improve resilience after the incident, the organization should take the following recovery steps:  System Restoration: Fully restore all affected internal network services and verify that critical applications and databases are functioning correctly.  Data Integrity Checks: Confirm that no data loss, corruption, or manipulation occurred during the downtime; validate backups and restore data if necessary.  Post-Incident Review: Conduct a formal review of the incident response to identify strengths, weaknesses, and lessons learned.  Business Continuity Planning: Update and test disaster recovery and business continuity plans to ensure faster recovery in future incidents.  Stakeholder Communication: Provide a post-incident report to stakeholders, assuring them of service restoration and outlining improvements made to prevent recurrence.  Ongoing Improvement: Implement continuous monitoring, patch management, and periodic security audits to strengthen recovery readiness.  By following these steps, the organization can ensure reliable service restoration, maintain stakeholder trust, and build stronger defenses against future disruptions. | | |

| Reflections/Notes: |
| --- |