**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** | The organization experienced a Distributed Denial of Service (DDoS) attack that disrupted internal network access for approximately two hours. The attack was executed via a flood of ICMP (ping) packets exploiting a misconfigured firewall that allowed unsolicited traffic. THe internal network services were unresponsive, halting normal business operations. The incident response team quickly contained the attack by blocking ICMP packets and shutting down non-critical services. After investigation, it was determined that the attack originated from spoofed IP addresses coordinated through multiple external devices. | | |
| --- | --- | --- | --- |
| Identify | Type of Attack: DDoS (ICMP Flood)  Targeted systems: Internal network, including web servers and network infrastructure  Vulnerability exploited: Unconfigured firewall allowed ICMP traffic from untrusted sources  Asset impacted:  Internal network access  Service availability  Operational productivity | | |
| Protect | **Implemented rate-limiting firewall rules for ICMP traffic**  **Enforced source IP address validation on the firewall**  **Configured firewall to block non-essential ICMP traffic**  **Conducted training for IT personnel on identifying unusual traffic patterns**  **Updated network security policy to ensure regular configuration audits** | | |
| Detect | Deployed Intrusion Detection/Prevention Systems(IDS/IPS) to identify and block suspicious ICMP patterns  Installed network monitoring software to flag abnormal traffic spikes  Established SIEM(Security Information and Event Management) tools to correlate and log traffic anomalies  Set up automated alerts for bandwidth usage and ICMP spikes from unknown sources | | |
| Respond | Blocked incoming ICMP packets at the firewall  Took non-critical services offline to preserve system integrity  Communicated incident details with internal stakeholders  Logged and analyzed incident data to understand attack vectors  Created a standard operating procedure (SOP) for similar DDoS incidents in the future | | |
| Recover | Gradually restored critical network services  Validated system functionality through post-incident testing  Documented lessons learned and updated the incident response plan  Scheduled regular firewall audits and penetration testing  Communicated recovery status to staff and ensured service availability was fully restored | | |

| Reflections/Notes: The incident emphasizes the importance of proactive firewall configuration, real-time monitoring and coordinated incident response protocols. Ongoing training, improved visibility and defined communication channels are essential for handling similar future threats. |
| --- |