Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or just to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to continue practicing applying the NIST CSF framework to different situations you may encounter.

Summary	The organization experienced a serious network disruption when all services stopped responding. The cybersecurity team investigated and identified the issue as a **Distributed Denial of Service (DDoS)** attack. This attack was carried out using a high volume of **ICMP packets** (often used in ping commands), which overloaded the network and caused critical systems to become unresponsive. The response team acted quickly by **blocking the attack** and temporarily shutting down non-essential services to prioritize the recovery of mission-critical operations.
Identify	An external threat actor launched an ICMP flood attack, targeting the company's internal infrastructure. As a result, the entire network was impacted. The cybersecurity team had to identify and secure all vital systems and ensure that critical business functions were restored as soon as possible.
Protect	To strengthen the network against similar attacks in the future, the team implemented a firewall rule to limit how many ICMP packets can be received in a short period. Additionally, they deployed Intrusion Detection and Prevention Systems (IDS/IPS), which help detect and block suspicious traffic patterns before they affect system performance.

Detect	To improve detection, the firewall was configured to verify the source of incoming IP addresses, helping to block spoofed or fake traffic. Network monitoring software was also introduced to observe traffic flow in real-time and identify early signs of abnormal or malicious activity.
Respond	Moving forward, the response plan involves isolating any compromised systems to contain potential damage. The team will focus on restoring essential services, analyzing security logs for unusual activity, and sharing detailed reports with leadership and, if required, with external authorities. This structured response ensures better incident handling and accountability.
Recover	To fully recover from an ICMP-based DDoS attack, the organization must first block the malicious traffic at the firewall level to prevent further overload. Next, all non-critical services should be paused to reduce internal network strain, allowing the restoration of critical systems to take priority. Once the attack subsides and traffic returns to normal levels, the remaining services can be brought back online gradually. This structured and prioritized recovery process helps ensure that essential operations are restored quickly and efficiently, while minimizing the risk of further disruption.

Reflections/Notes:

Through this incident analysis, I gained a deeper understanding of how everyday network protocols like ICMP can be exploited in malicious attacks. It highlighted the importance of proactive defense mechanisms, such as firewalls and monitoring tools, which play a major role in both preventing and identifying threats. Applying the NIST Cybersecurity Framework made it easier to organize the incident response steps and understand the broader context of cybersecurity planning. This exercise also emphasized that successful incident handling requires not only technical knowledge but also coordination, communication, and strategic decision-making to protect critical business functions.