Incident report analysis

Applying the NIST Cybersecurity Framework

Disclaimer: This project is entirely **fictional**. It was developed as a simulated exercise to demonstrate the practical application of the **NIST Cybersecurity Framework** and my proficiency in incident response procedures. No real company data or proprietary information was used.

Summary	The company experienced a security incident when all the network services unexpectedly became unresponsive. The cybersecurity team determined that the disruption was caused by a Distributed Denial of Service (DDoS) attack involving a flood of ICMP packets. In response, the team blocked the malicious traffic and temporarily disabled non-essential network services to ensure that critical services could be restored.
Identify	A malicious actor or attacker flooded the company's network with ICMP packets, which is an ICMP flood attack. All critical services need to be restored and secure; they need to return to their normal function.
Protect	The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	The cybersecurity team will isolate all the affected systems and devices, also they will work on restoring the critical systems and services that were affected by the

	distruption. The team will analyze and monitor the network logs to check if there's suspicious activity.
Recover	The cybersecurity team will restore the network services to its normal functioning state. As they implemented a new rule to the firewall, this will prevent suspicious ICMP packets by blocking it from the firewall.

Reflections/Notes: This project allowed me to practice the structural application of the NIST Cybersecurity Framework to a specific network disruption. By analyzing a Distributed Denial of Service (DDoS) attack, specifically an ICMP flood, I learned how to balance immediate mitigation with long-term detection strategies.

Key takeaways from this exercise include:

- **The Importance of Defense in Depth:** While blocking malicious traffic was the immediate response, implementing IDS/IPS filtering and source IP address verification provides a multi-layered defense to prevent future occurrences.
- **Operational Continuity:** The incident highlighted that the primary goal during the 'Identify' phase is ensuring critical services return to normal function as quickly as possible.
- **Proactive Monitoring:** Implementing network monitoring software is essential for detecting 'abnormal traffic patterns' before they escalate into a total service outage.
- **Policy Refinement:** The 'Recover' phase isn't just about restoring service; it's about updating firewall rules to ensure the network is more resilient than it was before the attack."