Incident Report Analysis

Scenario Overview

This report is based on a mock scenario provided by the Google Cybersecurity course on Coursera. The objective of this exercise is to analyze a **Distributed Denial of Service (DDoS) attack** using the **NIST Cybersecurity Framework (CSF)**. The incident involved an attacker flooding the company's internal network with **ICMP packets**, which led to network service disruptions. This report outlines the **identification, protection, detection, response, and recovery measures** taken to mitigate the attack and prevent future occurrences.

Scenario Description

You are a cybersecurity analyst working for a multimedia company that offers web design, graphic design, and social media marketing services to small businesses. The organization recently experienced a **DDoS attack** that caused internal network failures for over two hours.

During the attack, the company's **network services became unresponsive** due to a massive flood of **ICMP packets**. Normal internal traffic could not access network resources, bringing operations to a halt. The incident management team took immediate action by **blocking all incoming ICMP packets**, shutting down non-critical services, and restoring **critical** ones.

Upon further investigation, the cybersecurity team determined that the attack succeeded because of an **unconfigured firewall**, which allowed a malicious actor to **overwhelm the network with ICMP packets**. To strengthen security, the team implemented several network protections, including **firewall rules, IP verification, network monitoring, and an IDS/IPS system**.

Summary

Today, the organization's **servers were overwhelmed** by an **unusual amount of traffic**, resulting in a **server crash** that took more than **two hours** to resolve. The attack disrupted internal network services, preventing normal business operations until mitigation steps were taken.

Identify

The security team analyzed the event and discovered that a **flood of ICMP packets from various devices** caused the network servers to become overwhelmed. Initial investigations revealed that a **DDoS attack** was executed, where malicious actors sent **ICMP packets through an unconfigured firewall**, allowing them to overwhelm the network with excessive traffic.

Protect

To prevent similar attacks in the future, the security team implemented several **protective measures**:

- **Firewall Rules:** A new firewall rule was introduced to **limit the rate of incoming ICMP packets** to prevent flooding.
- **IP Verification:** The firewall was configured to **monitor and verify incoming IP addresses**, checking for **spoofed IPs** sending excessive packets.
- **Network Monitoring:** New **network monitoring software** was deployed to **detect abnormal traffic patterns**.
- **IDS/IPS Implementation:** An **Intrusion Detection/Prevention System (IDS/IPS)** was installed to **filter and block suspicious ICMP traffic** before it could impact operations.

Detect

With the implementation of **advanced monitoring tools**, the security team is now equipped to **detect and filter incoming traffic more effectively**. The firewall configuration will also **prevent future ICMP-based DDoS attacks**, ensuring **real-time identification of traffic anomalies**.

Respond

The response to the attack involved several key actions:

- **Blocking all incoming ICMP packets** to **immediately stop the attack**.
- **Shutting down non-critical services** to free up resources for essential operations.
- **Restoring critical services** to resume company operations as quickly as possible.

Recover

The primary goal of a **DDoS attack** is to **overwhelm network resources**, rendering them inoperable. **Restarting the affected servers and restoring network functionality** allowed for a full recovery from the incident. **No signs of additional security breaches** (such as **data exfiltration or unauthorized access**) were detected during the investigation.

Conclusion

By implementing **firewall security enhancements, IP verification, network monitoring tools, and an IDS/IPS system**, the organization has strengthened its defenses against **future DDoS attacks**. These actions align with the **NIST Cybersecurity Framework**, ensuring a **proactive and structured approach** to network security.

If similar incidents occur, **continuous monitoring and rapid response protocols** will be essential to minimize downtime and maintain network integrity.