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 multimedia company suffered a DDoS attack that disrupted its internal network for two hours, caused by a massive influx of ICMP packets exploiting a misconfigured firewall. This led to the interruption of Web design, graphic design, and digital marketing services, impacting the company's operations. The incident response team mitigated the attack by temporarily blocking ICMP traffic, disabling non-critical services, and reconfiguring the firewall to limit the incoming packet rate. Additionally, network monitoring software and an IDS/IPS system were implemented to detect and filter suspicious patterns, strengthening security against future attacks.
Identify	Type of Attack: Distributed Denial-of-Service (DDoS) attack of the ICMP Flood type. Firewall: Misconfiguration allowed excessive ICMP traffic, Network Infrastructure: Servers and routers overloaded due to the high volume of ICMP packets, Business Services: Web design, graphic design, and digital marketing became unavailable and Network Monitoring: Initially unable to detect and mitigate the attack in real time.
Protect	To strengthen security against future DDoS attacks, the company should

	enhance firewall configurations to limit suspicious ICMP traffic and block packets from untrusted sources. Network monitoring must be improved with automatic alerts to detect anomalies in real-time. The IDS/IPS system needs adjustments to filter and mitigate attacks more effectively. Additionally, it is essential to create a rapid incident response plan, train the team with simulations, and evaluate cloud-based DDoS mitigation solutions and load balancing to reduce infrastructure impact.
Detect	To continuously monitor and analyze network traffic and detect suspicious activities, the team should use tools like Wireshark, Zeek, and NetFlow to capture packets and identify abnormal patterns. Implementing SIEM dashboards, such as Splunk or Graylog, for real-time event correlation is also important. For monitoring software and applications, APM solutions like New Relic or Datadog can help identify failures and unusual behaviors. Using IAM systems like Azure AD and implementing UEBA to track unusual logins helps detect unauthorized access. Additionally, multifactor authentication (MFA) and automation with SOAR are crucial for securing user accounts and responding quickly to unusual activities.
Respond	To contain future cybersecurity incidents, the team can quickly isolate affected devices by disabling suspicious connections and implementing stricter firewall rules to block malicious traffic. Procedures to neutralize incidents include immediately applying mitigation measures such as blocking ICMP packets from untrusted sources, restoring critical services, and conducting a forensic analysis to understand the attack's origin. Data like firewall logs, network traffic records, and IDS/IPS alerts can be used to analyze the incident and identify attack patterns. To improve the recovery process, the organization can invest in more robust backup solutions, enhance documentation and team training for rapid response, and implement automated systems to detect and mitigate

	threats in real-time.
Recover	To help the organization recover from the cybersecurity incident, the priority is to recover critical data such as firewall logs, network traffic records, and IDS/IPS system information, which are essential for analysis and preventing future attacks. Additionally, it is necessary to restore affected network services, ensuring that critical systems like web design and digital marketing services are operational. Recovery processes in place include applying reliable backups, restoring firewall and IDS/IPS configurations, and verifying system integrity before bringing services back online. It's also important to conduct tests to ensure the network is secure before fully resuming operations.

Reflections/Notes:
This incident highlighted the need to improve network security and monitoring processes to detect and mitigate threats in real time. While the response was effective, it is crucial to regularly review firewall configurations, strengthen monitoring, and implement automated solutions for anomaly detection. Continuous team training and incident simulations are also essential for ensuring a quick and effective response to future threats. This experience should serve as a starting point to strengthen the organization's security posture.