Course 3 - Network Incident Report Analysis

Summary of Security Event

The organization experienced a Distributed Denial of Service (DDoS) attack that compromised internal network services for two hours. The attack vector was an incoming flood of **ICMP (Ping) packets** targeting an **unconfigured network firewall**, which allowed the traffic to overwhelm internal network resources and halt normal operations. The incident response team initially contained the attack by blocking incoming ICMP packets and taking non-critical services offline.

NIST Cybersecurity Framework (CSF) Analysis

Identify (ID)

Category	Analysis
Attack Type	Distributed Denial of Service (DDoS) – specifically, an **ICMP Flood attack**.
Vulnerability/Cause	An **unconfigured firewall** rule that failed to limit or filter incoming ICMP traffic, allowing the network to be easily overwhelmed.
Systems Impacted	All **internal network services** (web design, graphic design, social media marketing) and **network infrastructure** (routers, switches, servers) due to resource exhaustion.
Impact	Two hours of network service outage, leading to a significant loss of productivity and potential client service disruption.

Protect (PR)

Plan: Immediate and Long-Term Protection Measures

Action Area	Immediate Change/Update	Long-Term Strategic Change
Network Security	Finalize configuration of all existing firewalls, ensuring all default-deny rules are in place and necessary traffic is explicitly permitted.	Implement **Network Segmentation** (VLANs) to isolate critical servers from the user network, limiting attack surface area.
Access Control	Enforce Multi-Factor Authentication (MFA) across all remote access and server login points to protect against credential stuffing/lateral movement.	Implement a **Zero Trust Architecture** policy where all users and devices must be verified before accessing any resource, regardless of location.
Data Security	Conduct an immediate audit of data backup policies to ensure all critical data has recent, tested backups stored offsite (air-gapped or cloud).	Formalize a **Data Loss Prevention (DLP)** strategy to prevent sensitive data from leaving the internal network.

Detect (DE)

Methods for Continuous Monitoring and Detection

Method/Tool	Purpose	Implementation Status
SIEM / Logging	Centralize firewall logs, server logs, and IDS/IPS alerts into a **Security Information and Event Management (SIEM)** solution for real-time correlation.	Implemented Network Monitoring software (needs SIEM integration).
Traffic Baseline	Establish a baseline of *normal* network traffic volume and type. This allows security analysts to quickly identify traffic spikes (like ICMP floods) that deviate from expected activity.	**Immediate Action:** Configure existing monitoring tools to create baselines.

IDS/IPS Rules	Fine-tune the new **IDS/IPS** system to aggressively filter common DDoS signatures, including known ICMP flood patterns and rate limits.	Initial implementation complete (needs continuous fine-tuning).

Respond (RS)

Response Plan for Future Incidents

Response Phase	Action Steps for Incident Management Team
Containment	**Pre-defined Playbook:** Immediately invoke the DDoS playbook, isolating the network perimeter via rate-limiting rules on external-facing routers/firewalls. **Isolate** affected subnet/systems rapidly.
Eradication	**Root Cause Analysis:** Analyze firewall logs and SIEM data to identify the exact source IP(s) and attack signatures. **Neutralize** the threat by permanently blocking the identified malicious sources at the edge firewall.
Analysis/Review	**Post-Incident Review (PIR):** Document all actions taken, success/failure points, and time-to-contain. Update the security architecture and incident response plan based on lessons learned.
Stakeholder Communication	Establish transparent, pre-written communication templates for clients and internal staff (e.g., "We are experiencing a service interruption, updates will follow").

Recover (RC)

Steps for Restoration and System Recovery

Recovery Process	Description

System Prioritization	Immediately restore **critical network services** (customer-facing web services, primary email) first, followed by non-critical internal services (intranet, non-essential collaboration tools).
System Validation	Before bringing systems back online, perform a **post-incident security scan** to confirm that the malicious actor did not leave behind any backdoors or malware.
Configuration Audit	Conduct a **configuration audit** on all firewalls and network devices to ensure the vulnerability (unconfigured firewall) is permanently closed and all new rules (rate limiting) are active and correct.
Data Restoration	Restore the most recent backup data if any data corruption occurred during the two-hour outage. Verify data integrity against the pre-incident state.