🛡️ Cybersecurity Incident Report & Security Improvement Plan

Prepared by: Abubakari-Sadique Hamidu

Project: GWG Cybersecurity Capstone Project

Company: [Multimedia Company]

Services: Web Design | Graphic Design | Social Media Marketing

🧾 Incident Summary

> Our company experienced a **DDoS (Distributed Denial of Service)** attack that disrupted internal network services for about two hours. The attack used a flood of **ICMP (ping) packets** to overwhelm systems and crash services.
>
> The root cause was an **unconfigured firewall** that allowed malicious traffic. The incident response team took swift action to contain the threat and restore services.

📊 Security Improvement Plan (Using NIST CSF)

We've adopted the **NIST Cybersecurity Framework**, which includes: Identify, Protect, Detect, Respond, and Recover. Below are our actions based on each function.

🔍 1. IDENTIFY

✅ **Full Network and Asset Audit**

> **Why:** To discover and assess all systems and vulnerabilities.
> **How:** Tools like *Nmap* and *Spiceworks* provided detailed asset inventory.

✅ **Reviewed Access Permissions**

> **Why:** To minimize unnecessary admin access.
> **How:** Reviewed and updated user roles with the least privilege principle.

✅ **Identified Critical Services**

> **Why:** To prioritize security resources effectively.
> **How:** Key services like databases and internal tools were classified as high priority.

🛡️ 2. PROTECT

✅ **Reconfigured Firewall for ICMP Control**

> **Why:** Attack exploited ICMP packets.
> **How:** Configured *FortiGate* firewall to block/restrict ICMP traffic and apply rate limits.

✅ **Source IP Verification**

> **Why:** Prevent spoofed packets.
> **How:** Enabled source IP validation on core routers.

✅ **Security Awareness Training**

> **Why:** Human error contributes to most breaches.
> **How:** Monthly staff training sessions on phishing, password hygiene, and physical security.

🛰️ 3. DETECT

✅ **Network Monitoring System Deployed**

> **Why:** Detect traffic anomalies early.
> **How:** Implemented *Wireshark* and *Snort* for packet inspection and alerts.

🚨 4. RESPOND

✅ **Incident Response Playbook Developed**

> **Why:** Quick and effective response to threats.
> **How:** Documented response steps and roles for various threat scenarios.

✅ **Communication Plan Activated**

> **Why:** Keep stakeholders informed during attacks.
> **How:** Internal alert channels and customer service guidelines activated.

🔁 5. RECOVER

✅ **Backup and Restore Testing**

> **Why:** Ensure data integrity.
> **How:** Tested backups weekly using both local and cloud methods.

✅ **Post-Incident Review**

> **Why:** Improve future responses.
> **How:** Lessons learned documented and shared with team.

📄 Documented Updated Policies

> After the incident, the following policy documents were reviewed, updated, and enforced:
>
> - ✅ Network Security Policy – Updated to restrict ICMP and unauthenticated external access.
> - ✅ Acceptable Use Policy – Clarified employee responsibilities on digital devices and internet usage.
> - ✅ Incident Response Policy – Defined step-by-step playbooks and escalation paths.
> - ✅ Data Backup Policy – Implemented weekly and daily backups across systems.

- ✅ Access Control Policy – All users reviewed and shifted to least privilege access model.

🔮 Future Plans

Our team is committed to continuous improvement. Planned actions include:

- 🔐 Migrate to MFA (Multi-Factor Authentication) for all admin logins by Q3.
- 📡 Deploy a centralized SIEM system (e.g. Splunk or AlienVault) for smarter monitoring.
- 👩‍🏫 Quarterly cybersecurity drills and phishing simulations for staff.
- 🧪 Perform annual penetration testing with third-party professionals.
- ☁️ Transition to a hybrid cloud architecture with built-in security layers.

Report completed as part of the Grow With Google Cybersecurity Certificate Capstone Project.

Prepared by: ***Abubakari-Sadique Hamidu***