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 organization experienced a DDoS attack, which compromised the **internal network for two hours.** During the attack, the organization’s **network services** suddenly stopped responding due to an **incoming flood of ICMP packets.** Normal **internal network** traffic **could not access any network resources.** The incident management team responded b**y blocking incoming ICMP packets**, **stopping all non-critical network services offline**, and **restoring critical network services.**
Identify	The company's cybersecurity team investigated the systems, devices involved in the attack to identify the gaps in security. They found that a **malicious actor had sent a flood of ICMP pings into the company’s network** through an **unconfigured firewall.** This **vulnerability** allowed the malicious attacker to overwhelm the company’s network through a **distributed denial of service (DDoS) attack.** The **entire internal network was affected.** All critical network resources needed to be secured and restored to a functioning state.
Protect	The incident management team responded b**y blocking incoming ICMP packets**, **stopping all non-critical network services offline**, and **restoring critical network services.**
Detect	To detect DDoS attack in future the network security team has implemented a: ● **Network monitoring software** to detect abnormal traffic patterns

	● **An IDS/IPS system** to filter out some ICMP traffic based on suspicious characteristics
Respond	To address this security event, the network security team implemented: ● A **new firewall rule** to limit the rate of incoming ICMP packets - applied rate-limiting and ACLs at the firewall level ● **Source IP address verification** on the firewall to check for spoofed IP addresses on incoming ICMP packets
Recover	The system recovered by **Restoring services** by reducing malicious traffic load and restarting **critical systems/services affected by resource exhaustion.** To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, ● **external ICMP flood attacks can be blocked at the firewall.** ● Then, **all non-critical network services should be stopped** to reduce internal network traffic. ● Next, **critical network services** should be **restored** first. ● Finally, once the **flood of ICMP packets have timed out**, all non-critical network systems and services can be brought back online. **Next Steps:** - **Auditing** all firewall configurations across the network. **- Hardening network infrastructure** - **Planned internal training** on secure default configurations and DDoS handling.

Communication	- **Internal debrief** with IT, security, and network teams. - Documented the attack, impact, and resolution in an **incident report**. - Shared lessons learned and configuration checklists with the broader technical team. - Updated **Business Continuity/Disaster Recovery (BC/DR) plans** to include volumetric DDoS scenarios.

Reflections/Notes: