Accident analysis of the report

Instructions

As you progress through this course, you will be able to use this template to record your findings after completing an activity or to take notes on what you have 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	On this date, the multimedia company suffered a DDoS attack that put the organization at risk; network services stopped working.During the attack, your organization's network services suddenly became unresponsive due to a flood of incoming ICMP packets. Normal internal network traffic was unable to access any network resources.
Identify	The cybersecurity team investigated and discovered that a malicious attacker sent a flood of ICPM packets through a misconfigured firewall.The vulnerability allowed the attacker to overwhelm the company's network through a distributed denial-of-service (DDoS) attack.
Protect	To address this, the cybersecurity team implemented the following new policies to prevent future attacks of the same kind: Firewalls will have a new rule to limit ICPM packet rates .verification of the source IP address in the firewall to check for spoofed IP addresses in incoming ICPM packets
Detect	To prevent future attacks, network monitoring software will be implemented to detect anomalous patterns and the use of IDPs to filter ICMP traffic for suspicious characteristics.

Responder	During the incident, the response team acted to contain its impact: ● With**They temporarily blocked incoming ICMP packets**to stop the attack. ● With**They disabled non-critical services.**to relieve network load. ● With**critical services were restored**to resume essential operations while traffic was analyzed. After containing the threat, the team conducted forensic traffic analysis and collected evidence for documentation of the incident.
Recover	After controlling the attack: ● Non-critical network services were gradually **restored**. ● With validated **the integrity of** the affected systems. ● With**They reviewed and updated the firewall settings**to prevent the vulnerability from recurring. ● The incident was documented to improve the incident response plan procedures. ● IT staff were instructed to continuously monitor network availability and

	performance.

Reflections/Notes: This incident demonstrated that a misconfiguration can jeopardize an entire organization. Although the response was effective, the company must continue to improve its preventative controls, monitoring processes, and regular audits to ensure that similar breaches do not occur in the future.