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 which specializes in web design services, graphic design, and social media marketing solutions to small businesses, recently experienced a DDoS. Which resulted in a compromised network and network outage for almost two hours. We believe the attacker used ICMP flooding technique to overwhelm the network and disrupt normal network operations.
Identify	The cybersecurity team investigated the attack and found out that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed malicious attacker to overwhelm the network through a distributed denial of service (DDoS) attack.
Protect	The incident management team responded to this incident by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Detect	The team implemented network monitoring software to detect abnormal traffic patterns in a network. An IDS to monitor suspicious activity on the network.
Respond	The network security team implemented Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. A new

	firewall rule configured to limit the rate of incoming ICMP packets. For future attacks, the team segmented the network into two parts for critical and non critical section of the network service and ICMP timeout in firewall to prevent any ICMP flooding attacks.
Recover	By stopping the incoming ICMP packets, the security team recovered all the network services to normal operations. The security team updated firewall rules and organization policies to prevent any possible network intrusions. Latest backup system and baseline configuration was added to revert back to normal operation to defend against any damage. The team also implemented NIST framework and security controls to follow best security practices to prevent any future attack.

Reflections/Notes: