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	Company XYZ experienced a DDoS attack by threat actors and the attackers started flooding ICMP packets onto the system. The network experienced an Outrage and the normal network traffic could not access the sever resources. The incident was reported by the employees and the incident response team responded by blocking the incoming flood of the ICMP packets
Identify	The incident response team audited the systems affected and the protocols used to identify the nature of the attack. It was found that the threat actor unleashed a DDoS attack on the system.
Protect	The team has implemented new firewall rules, source IP verification, network monitoring system software, and IDS/IPS to prevent further attacks by threat actors.
Detect	To detect any further attacks, the security team will review any abnormality in the network traffic and strengthen firewall rules to prevent DDoS attacks.
Respond	The incident response team responded by blocking the incoming ICMP packets to prevent the complete crash of the network, stopping all the non-critical services, and allowing only critical services to operate.
Recover	The affected data will be recovered and the system will be configured with

	baseline configuration.

Reflections/Notes: