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 company had sudden network service interruption. The cybersecurity team found that it is due to the DDoS attack through ICMP flooding. The cybersecurity team blocks the attack and stops all non-critical network services.
Identify	The attacker used ICMP flood attack technique to affect the internal network. The critical resources needed to be secured and restored.
Protect	The cybersecurity team set a new firewall rule to limit the ICMP traffic request rate and IDS/IPS system to detect anomalies in the network and filter it out.
Detect	The cybersecurity team implemented source ip address verification in the firewall configuration to check IP address that is spoofing ICMP packets. They also implement network monitoring software to detect unusual traffic pattern.
Respond	The affected systems will be isolated to prevent further attacks and disruption. They will analyze the network log for any unusual activity. The incident will be reported to upper management.
Recover	To have recovery, the access to the network should be restored to its original state. In future, the firewall will block the ICMP flood attack. Non-critical

	network services will be stopped temporarily until the network service is restored from the ICMP attack.

Reflections/Notes: