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 have all the internal network compromised for two hours after suffering a DDOS attack. Network resources was unavailable to access,
Identify	The security team investigate the event and found a flood of ICMP packets send by a malicious actor using an unconfigured firewall.
Protect	The team has implemented a new firewall rule to limit rate of incoming ICMP packets and network monitoring to detect abnormal traffic.
Detect	The security team has implemented a source IP verification to avoid IP spoofing and ICMP flooding and an IDS/IPS system to add an extra security label and filter traffic suspicious.
Respond	The Security team has blocked incoming ICMP packets, stopped all non-critical networks services.
Recover	All the critical networks services have been restored.

Reflections/Notes: