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	A multimedia company experienced a DDoS attack which led the network to shut down for two hours. Network services could not respond due to a flooding of ICMP packets. Additionally, normal internal network traffic was unable to access network resources.
Identify	Through a network audit, the team found an overwhelming amount of ICMP packets that came through an unconfigured firewall. The flooding of the packets caused the network to stop operating properly. Meaning, a DDoS attack was prevalent.
Protect	To prevent future attacks, the team implemented a new firewall rule to reduce the rate of incoming ICMP packets, source IP address verification, network monitoring software, and both IDS and IPS systems.
Detect	To detect any future attacks, we will utitlize to the fullest extent our Intrusion Detection System(IDS).
Respond	Our response to the incident consisted of blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services
Recover	To recover the team restored critical network services.

Reflections/Notes: