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	There was a DDos attack and our organization network services suddenly stopped due to a flooding of ICMP packets. Normal internal traffic could not access any network resources. The team responded by blocking the incoming ICMP packets and stopping all non critical network services offline and restoring critical services. After investigating they found that a malicious attacker had sent a flood of ICMP pings into the company’s network through an unconfigured firewall, allowing for the DDoS attack.
Identify	This was a DDoS attack allowed by an unconfigured firewall
Protect	The firewall needs to be updated and configured
Detect	We can use IDS and SIEM tools to better monitor traffic
Respond	IPS can help block an attack like this in the future, we can use SIEM to monitor traffic as well
Recover	We need to have backups in place to restore data

Reflections/Notes: