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	
Identify	The incident management team has audited firewalls and network monitoring software involved in the attack in order to identify any gaps in security. The team found that the malicious attacker had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This allowed the attacker to overload the company's network through a DDos attack.
Protect	The team has implemented four new security features, which includes a new firewall rule to rate limit incoming ICMP packets, as well as source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. Next, they implemented network monitoring software to detect abnormal patterns, as well as an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	In order to prevent these ICMP floods in the future, the team will be using network monitoring software and a firewall logging tool, as well as an IDS/IPS system in order to monitor ICMP traffic.
Respond	The network services stopped responding, and the normal internal network traffic couldn't access any network resources, so the incident management

	team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. We are informing upper management of this event.
Recover	The team restored critical network services, and will restore the organization’s network services in order to restore business continuity.

Reflections/Notes: