Incident report analysis

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 recent DDoS attack occurred which compromised the internal network for two hours until the issue was resolved. Network services stopped responding due to an incoming flood of ICMP packets. Users attempting to access internal network resources were unable to do so. Once the attack was detected, the security team responded by blocking all incoming ICMP packets, taking all non-critical network services offline as well as restored critical network services.
Identify	An incoming flood of ICMP packets caused internal network services to become unavailable due to an unconfigured firewall.
Protect	The internal network was supplemented with a new set of firewall rules in regards to incoming ICMP packets. Source IP address verification was implemented to check for spoofed IP addresses.
Detect	A SIEM (security information and event management) software as well as an IDS/IPS system have been introduced to filter out suspicious ICMP traffic as well as a method to monitor abnormal traffic patterns.
Respond	The security team responded by taking all non-critical network services offline and blocking all incoming ICMP packets once the attack was detected.
Recover	Recovery was carried out by stopping the incoming ICMP packet flood and

	soon after restoring critical network services.