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 business had experienced a DDos attack which led to a two hour outage. What was initially discovered during the attack was an influx of ICMP Packets, overwhelming the network and causing normal internal network traffic to be inaccessible. The incident management team blocked further ICMP packets from entering the network. To mitigate future events the team is heavily focused on implementing methods such as firewall rules to mitigate ICMP packet amounts, sourcing IP addresses for verification, and ensuring that future systems are updated in the process.
Identify	Initial discoveries had found that the network had experienced a DDos attack. The internal network had been compromised for two hours, with the network experiencing an influx of ICMP packets.
Protect	Implement new firewall rules to mitigate the amount of ICMP packets being dumped into the network.
Detect	Source IP address verification on the firewall, checking for spoofed IP addresses on incoming ICMP packets. Network monitoring software also to detect any abnormalities
Respond	Blocked incoming ICMP packets to prevent further issues. This shutdown all

	non-critical network services but utilized critical network services
Recover	Work on maintenance of the network, but ensure the systems are updated to accommodate for future attacks. This would implement previously mentioned controls.

Reflections/Notes: