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 organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.”
Identify	Attackers attacked the company with a DDoS attack which was able to take down the website for 2 hours. Before the site could be up and running again, all the resources needed to be reset to normal capacity.
Protect	Cybersecurity team was able to implement a new firewall protection rule that would secure the firewall and help prevent other attacks from coming through.
Detect	The team was able to configure source IP address verification on the firewall to check for spoofed IPs.
Respond	In the future, when a system goes down, the team will isolate that system to prevent it from taking down other systems. This achieves a faster relaunch time and provides safety of the other systems.
Recover	In the future, all network and system resources must return to their normal processing power and then the website will be relaunched. Hopefully with the

	upgrades in security it will be tougher to penetrate the reinforced firewall.

Reflections/Notes: