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	This is a typical case of DDOS, the website was turned off around 2 hours, during the attack the web did not respond due to high bandwidth demand from ICMP packages.The incident management team responded by blocking incoming ICMP packets, taking all non-critical network services offline, and restoring critical network services.
Identify	This vulnerability was found in the firewall settings , which were not configured correctly.
Protect	The management team implemented a new firewall rule and verified the source IP address.
Detect	They also installed network monitoring software and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Respond	The incident management team responded by blocking incoming ICMP packets, taking all non-critical network services offline, and restoring critical network services.
Recover	For this cases it is a good practice had backups one time a week

Reflections/Notes: The team has to pay more attention to SIEM, and have to do better configures on the firewall.