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 organisation recently experienced a DDoS attack which took down the internal network. For two hours, business operations were paralysed until incident response were able to restore critical systems and enable business operations to resume somewhat normally.
Identify	The SOC team noticed a flood of ICMP packets streaming into the network server Indicating an ICMP flood DDoS attack. Upon further review, it seems that this happened because of a misconfigured firewall, which the threat actor exploited to gain access to the network and launch the attack.
Protect	The team then proceeded to st up the following measures to mitigate such attacks going forward: • A new firewall rule to limit the rate of ICMP packets going into the network. • Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. • An IDS/IPS system to filter out incoming ICMP packets based on suspicious characteristics.
Detect	In addition to implementing protection mesures, the following detection measures were also implemented:

	• Network monitoring software to detect abnormal network activity. • An IDS/IPS system to filter out incoming ICMP packets based on suspicious characteristics.
Respond	The security team then responded by blocking all incoming ICMP packets and taking all non essential network services offline.
Recover	The team then proceeded to restore functionality in critical systems first, ensuring key business operations can continue minimising net loss.

Reflections/Notes: