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 security team identified a DDoS attack after analysing the reason for why the internal networking services had failed. It affected the usual everyday business activities for two hours. The DDoS attack was conducted by a malicious actor flooding the network with ICMP packets. After implementing a response, critical services were restored.
Identify	The DDoS attack was an ICMP flood attack conducted by an unknown malicious actor. It affected the entire internal network.
Protect	The reason for the attack stemmed from an invulnerability caused by an unconfigured firewall, which the security team remedied by implementing new rules. As well as to filter incoming traffic that contained suspicious characteristics.
Detect	The security team also implemented network monitoring and configured IP address verification to check for spoofed IP addresses on incoming ICMP packets. An IDS/IPS system was introduced to filter out more traffic.
Respond	For future incidents, the security team implemented methods for isolating affected systems. The goal is to restrict these incidents from spreading to the rest of the network in the future as well as a faster response to restore function

	by implementing alerting systems (IDS/IPS). After containment, the networking logs will be analysed and reported to upper management, if necessary.
Recover	The recovery of critical networks was prioritised in order to restore a return to normal operations of the company. Then, firewall rules were set up to prevent future attacks at the firewall level. Once the ICMP flood has stopped, non critical systems can be brought back.

Reflections/Notes: