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	Our organization experienced a DDoS attack, which compromised the internal network of the company for two hours. During this attack, network services stopped responding due to an incoming flood of ICMP packets. The incident management team responded by blocking incoming ICMP packets, taking all non-critical network services offline, and restoring critical network services.
Identify	They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall, affecting the entire internal network
Protect	To address this security event, the network security team implemented a new firewall rule to limit the rate of incoming ICMP packets and deployed an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To address this security event, the network security team implemented: Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and network monitoring software to detect abnormal traffic patterns
Respond	The incident management team responded by blocking incoming ICMP

	packets. For future security events, the cybersecurity team will **isolate** infected systems to avoid disruption of services before moving on to detecting the cause.
Recover	The team stopped all non-critical network services to allow critical network services to be restored. In the future, external ICMP flood attacks can be blocked at the firewall first. Then, after all the ICMP packets have timed out, the non-critical services that were stopped can be brought back online.

Reflections/Notes: