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	Recently, the network services from our organization suddenly stopped working. We suspect that the cause of this failure was a DdoS attack.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall.
Protect	To address this security event, the network security team implemented: • A new firewall rule to limit the rate of incoming ICMP packets. • Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. • Network monitoring software to detect abnormal traffic patterns. • An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To prevent this type of incident from happening again in the future, the team has implemented an IDS/IPS system to actively monitor and filter network traffic.
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

Recover	The team will recover the deleted data by restoring the database from last night's full backup.