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 organization recently underwent a DDoS attack. Network services suddenly stopped responding due to an incoming flood of ICMP packets. Internal network traffic could not access any network resources. Incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	The cybersecurity team found that a malicious actor had sent al flood of ICMP packets to the network causing it to become overwhelmed. An unconfigured firewall was also found which led the team to believe that was how the actor infiltrated via DDoS.
Protect	The team has since them implemented security measures, such as: • 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 detect future suspicious network traffic, the company has now deployed an IDS/IPS system to filter ICMP traffic. SIEM tool has been implemented for the

	team to monitor the system to find suspicious activity before an event occurs.
Respond	The team responded by blocking ICMP packers, stopping all non-critical network services offline, and restoring critical network services.
Recover	The team will recover data loss by restoring the database from the full backup. All staff have been made aware of the attack and informed that any client's work may need to be reviewed and looked over again as. Future external ICMP flood attacks can be blocked at the firewall.

Reflections/Notes: