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's security services suddenly stopped working. It was found by the cybersecurity team that the cause was a distributed denial of services (DDoS) attack. A flood of incoming ICMP packets to be accurate. The team blocked the attack and stopped all non-critical network services, so that the critical ones could be restored.
Identify	Somebody targeted the company with a DDoS attack. It affected the entire network. The next steps should be securing and restoring all critical network resources.
Protect	Two things were implemented to prevent same attacks in the future: • a new firewall rule to limit the rate of incoming ICMP packets, • an IDS/IPS system to filter traffic based on characteristics.
Detect	Detection will be held by: • source IP verification on firewall, • network monitoring software looking for abnormal traffic patterns.
Respond	1. Isolate affected systems. 2. Restore critical systems. 3. Analyze logs to look for suspicious activity.

	4. Upper management and authorities should be informed.
Recover	All network services need to be restored to a functioning state. Non-critical services should be stopped, to decrease traffic. Critical parts should be restored first. After the attack is stopped, all non-critical network services can be brought back online.

Reflections/Notes: *Nothing to add.*