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 experienced an DDoS attack which internal network systems were down for 2 hours. This event was investigated and found that this was due to the flooding of ICMP packets to the network. The team responded by blocking incoming packets, stopping all non-critical network services offline and restoring critical network services.
Identify	Company was attacked by an actor with ICMP flood attack that affected the network and only critical resources networks were brought back online once the issue was identified and blocked all incoming ICMP packets.
Protect	A new firewall rule was integrated to limit the rate of incoming ICMP packets, IDS/IPS system to filter out some of the ICMP traffic based on suspicious behaviors.
Detect	The cybersecurity team implemented a source IP address verification to check spoofed IP addresses. A network monitoring software to detect abnormal traffic patterns.
Respond	Issue should be segregated from the network, systems that are affected should be isolated and offline, any other systems that are not affected should be observed and monitored. Containerize the attack to a point where critical

	systems are able to go back online again. Then monitor logs of the critical systems for any other issues or flooding. Filter out the cause and see how it can be prevented for any other future event. Also depending on the severity of the issue, communication to stakeholders and legal auditors will be sent of this.
Recover	External ICMP flood attacks must be blocked at a firewall to contain the attack. Reduce incoming traffic for non-critical services to better isolate the issue. Critical services should be restored first for business operations to get back to normal while monitoring the progression of the restoration. Then monitor logs to see if all ICMP packets have self-destructed and release any other non-critical services back online.

Reflections/Notes: