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	It was discovered by the cybersecurity team that the company was a victim of a distributed denial of service (DDoS) ICMP flooding attack after network service became totally unresponsive. The security team responded by first blocking all incoming ICMP packets, then stopping all non-critical network services, and lastly focused on restoring critical network services.
Identify	The entire company's network was brought to a halt when an unknown malicious actor flooded the network with ICMP packets. This resulted in non-critical and critical network services being unresponsive. The cybersecurity team focused on restoring critical network functionality as soon as possible.
Protect	New firewall rules limiting incoming ICMP packets and checking for source IP verification were implemented. In addition the team added an IDS/IPS system to filter suspicious ICMP traffic.
Detect	The security team has configured a source IP address verification firewall rule to check if the sender's IP address is being spoofed on an ICMP packet. New network monitoring software to detect abnormal traffic patterns has been deployed as well.

Respond	The procedure going forward will have the cybersecurity team segment the systems affected by any disruption. As they did during this event, they will attempt to restore any critical systems and services disrupted by the event as soon as possible. After analyzing logs, the team will report its findings to upper management and will contact the necessary authorities if the situation requires.
Recover	The recovery process for a future DDoS ICMP flooding attack needs to focus on returning the network to its pre-attack functional state. The cybersecurity team should firstly stop all network functions, before immediately bringing the critical parts back online. After the flood of packets has subsided, the team can bring back the non-critical network systems and services. The new firewall rules and IDS/IPS systems will assist in preventing the likelihood of a future event.

Reflections/Notes: