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 company encountered a situation where all of the network services have suddenly become unresponsive. Based on the findings from investigating this event, the cybersecurity team determined that the issue stemmed from a distributed denial of service (DDoS) attack involving a flood of incoming ICMP packets. Consequently, the team took action by blocking the attack and disabling non-critical network services (in order to facilitate the restoration of critical ones).
Identify	Upon scrutinizing the internal network, the cybersecurity team discovered that a malicious actor had executed an ICMP flood attack, resulting in the internal network's failure. The attacker exploited an unconfigured firewall to gain unauthorized access. It is imperative to secure and reinstate all critical network resources to ensure their proper functioning.
Protect	The cybersecurity team implemented the following measures: • Carried out a new firewall rule to restrict the rate of incoming ICMP packets. • Verified IP address source on the firewall in order to identify any potential spoofed IP addresses in ICMP packets.

	• Utilized network monitoring software to detect abnormalities in traffic patterns. • Deployed an IDS/IPS system to eliminate specific ICMP traffic that exhibits suspicious characteristics.
Detect	The team set up the verification of IP address sources on the firewall in order to detect spoofed IP addresses on ingress ICMP packets. Additionally, they utilized network monitoring software in order to identify irregular traffic patterns.
Respond	Moving forward, the cybersecurity team plans to respond by isolating affected systems in order to prevent further disruption to the network. They will also focus on restoring critical systems and services that were impacted by the DDoS attack. Subsequently, the team will report the incidents to upper management and, if necessary, to the authorities.
Recover	In order to recover critical network services impacted by the ICMP flooding (DDoS attack), it is crucial to obtain access to the network services in order to restore them to their normal state. The firewall should be configured to prevent future external ICMP flood attacks. To minimize internal network traffic, non-critical network services should be halted, followed by giving restoration priority to critical systems. Once all flood packets have timed out, non-critical systems and services can be gradually brought back online.

Reflections/Notes: