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	Recently, the organization experienced a distributed denial of service attack (DDOS) in the form of an ICMP flood. The attack was the result of a malicious actor sending a flood of ICMP pings through an unconfigured firewall. During the attack, the organization's network services stopped responding and normal internal network traffic could not access any network resources as a result. The incident management team responded to the attack and, after two hours, the incident was resolved.
Identify	The cybersecurity team investigated the security event to determine the vulnerabilities that led to the attack. The team found that the malicious actor had sent a flood of ICMP pings through an unconfigured firewall. The firewall was not configured to limit the rate of incoming ICMP packets and as a result, the malicious actor was able to flood the internal network through a DDOS attack. The entire internal network was affected as a result.
Protect	After the incident, the network security team implemented two new measures to prevent an attack of this type from taking place in the future. The team configured the firewall to limit the rate of incoming ICMP packets to prevent the internal network from being flooded. In addition to this firewall configuration, the team also implemented an IDS/IPS system to filter out

	incoming ICMP packets based on suspicious characteristics.
Detect	In addition, the network team has also implemented two new measures to detect intrusion into the network. First, the team has implemented a network monitoring software to monitor for any abnormal traffic patterns in the network. Additionally, the team configured IP address verification in the firewall to check for spoofed IP addresses on incoming ICMP packets.
Respond	In response to the ICMP flood attack, the incident management team configured the firewall to block all incoming ICMP packets. After, they shut down all non-critical network services to allow all critical network services to recover. After the network had completely recovered from the attack, the network security team implemented the aforementioned measures in response. In the future, similar action should be taken in response to these attacks. First, the incident management team will isolate affected systems and attempt to contain the attack. Then, they will identify and eliminate the cause of the attack. Finally, they will restore all systems that were affected, beginning with critical systems and report the incident to upper management.
Recover	After blocking incoming ICMP packets and shutting down non-critical network services, the network management team primarily focused on restoring all critical network services. After restoring those that are critical, the team was able to restore all network services. Similar to the action that was taken in this case, in response to similar attacks in the future, access to all network services need to be restored to a normal functioning state beginning with critical services.

Reflections/Notes: