Kimberly Chau

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	Due to the organization's network services suddenly stopping responding due to an incoming flood of ICMP packets, we realized there was an attack. This made normal internal network traffic not being able to access any network resources. We suspected it was a DoS/DDoS attack since the flood of ICMP packets sent denied our network services.
Identify	The company's cybersecurity team investigated the security event and found that a malicious actor sent a flood of ICMP pings into the network through an unconfigured firewall to cause a ICMP flood attack. Having a vulnerability like this allowed malicious attackers to overwhelm the company's entire network with a DDoS attack and cause our network services to not run for 2 hours.
Protect	To mitigate this cybersecurity threat, the network security team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect potential DoS/DDoS attacks in the future, the network security team also implemented a network monitoring software to detect abnormal traffic patterns and a source IP address verification on the firewall to check for

	spoofed IP addresses on incoming ICMP packets.
Respond	The incident management team responded to the event by blocking incoming ICMP packets as soon as they were notified of the attack, stopping all non-critical network services offline to prevent spreading, and restoring any disrupted critical systems. Afterwards, an investigation was carried out by the cybersecurity team to find vulnerabilities in the system and improvements were made in response. The team should report the incident to upper management and any legal authorities.
Recover	The DDoS attack compromised the internal network for two hours but after the flood of ICMP packets timed out, all non-critical network services were able to be brought back online and restored to a normal functioning state.

Reflections/Notes: