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 multimedia company recently experienced a Distributed Denial of Service(DDoS) attack. This caused the company's network services to stop responding. The DDoS attack successfully overloaded the organization's network services by flooding them with ICMP packets. The organization's cybersecurity team responded by blocking the incoming ICMP packets, stopping all non-critical network network services offline, and restoring critical network services.
Identify	The specific kind of DDoS attack experienced by the company is the ICMP flood attack –where a malicious actor overwhelms an organization's systems by flooding it with ICMP packets. Because the network systems were overloaded with malicious requests, normal internal network traffic could not access the organization's network resources. This affected the internal network, so all critical resources were secured and restored to a functioning state.
Protect	To protect the organization from other DDoS attacks like these, the organization implemented new firewall rules that limits the rate of incoming ICMP packets. The organization also implemented a new IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect future DDoS attacks, the company also implemented a source IP

	address verification on the firewall to check for spoofed IP addresses on the incoming ICMP traffic. They also have a network monitoring software configured on the firewall, which serves to detect abnormal traffic patterns coming into the network system.
Respond	For future security incidents, the organization will be prepared to contain, neutralize and analyze security events. The company will contain the security incident by isolating affected systems. This will prevent the attack spreading to the entire network. Then, the organization will restore any critical network services that were affected by the attack. Checking and analyzing network logs will also be helpful to get insights about suspicious activities. Analyzing logs and investigations will be conducted by the security teams to form a report of all the incidents that can be presented to higher authorities.
Recover	For the recovery process, the organization needs to restore access to the overwhelmed network services to a normal state. This will ensure that normal incoming internet traffic can access the company's network resources. Additionally, the newly implemented firewall will help mitigate future DDoS attacks of the similar type. The company will stop all non-critical workloads and will restore critical services. Once the attack is mitigated, the non-critical workloads will be restored so normal internet traffic could access the network resources.

Reflections/Notes: The main reason for the attack is the unconfigured firewall. The firewall was a security vulnerability that the organization did not address. Conducting a vulnerability assessment and regularly updating the software/hardware that the company uses will help mitigate future attacks.