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	Multimedia company that offers web design services, graphic design, and social media marketing solutions. They offer these services to mostly small businesses. Recently the organization got hit with a DDoS attack, this attack took down the internal network for two hours until it was resolved. The cybersecurity team investigated the malicious attack and found a malicious actor sent a flood of ICMP pings to the company's network through an unconfigured firewall.
Identify	The cybersecurity team identified the network attack, and the reason for the incident seems to be a DDoS attack. The company's services are offering web design services, graphic design, and social media marketing solutions. They found that a malicious actor sent a flood of ICMP pings to the company's network via unconfigured firewall. Normal internal network traffic couldn't access any network resource because of this attack.
Protect	This security event led to the network security team implementing a new firewall rule to limit the rate of incoming ICMP packets. Also, an IDS/IPS system to filter out ICMP traffic based on suspicious characteristics.
Detect	For detection, they have implemented network monitoring software to detect abnormal traffic patterns and source IP address verification on the firewall to

	check for spoofed IP addresses on incoming ICMP packets.
Respond	The team learned quite a bit from this attack, so in the future teams will now try to isolate the affected systems so they won't spread to other systems in the network. Then after trying to restore any critical systems/services that were affected. Last will be to analyze the network logs to look for any suspicious or abnormal activity, letting the cybersecurity team know or respond faster to malicious attacks.
Recover	The cybersecurity team will need to restore all the network services to their normal state from the ICMP flood attacks, DDoS. Start by stopping non-critical network services to lower the load of the internal network traffic since it is overloaded because of the DDoS attack. After, all the critical network systems/services must be restored first. Then when the ICMP flood attacks are timed out, all non-critical systems/services can be restored. To prevent all these steps a firewall should be set up it can block the ICMP flood attacks.

Reflections/Notes: