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 that offers web design services, graphic design, and social media marketing solutions to small businesses has recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. The attack flooded the network with ICMP packets through an unconfigured firewall, overwhelming services. Using the NIST Framework's five functions—Identify, Protect, Detect, Respond, and Recover— The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored.Then ,the security team implemented new firewall rules, IP verification, network monitoring, and an IDS/IPS system to prevent future attacks. These measures ensure better detection, containment, and mitigation of potential security incidents, enhancing the organization’s overall network resilience.
Identify	The incident management team conducted an audit of the systems, devices, and access policies involved in the attack to identify security gaps. It was determined that the company had experienced a DDoS attack by malicious actors , which disrupted the internal network for two hours. A significant ICMP flood was observed, enabled by an improperly configured firewall that allowed the flood and unwanted traffic. As a

	result, normal internal traffic was unable to access any network resources, causing a complete halt in the organization's network operations.
Protect	The team implemented new security measures, including: - A firewall rule to limit incoming ICMP traffic. - Configuring the firewall to detect and block spoofed IP addresses on incoming ICMP packets. - Deploying an IDS/IPS system to filter ICMP traffic based on suspicious characteristics.
Detect	To detect new unauthorized access attacks in the future, the team will use a firewall logging tool and an intrusion detection system (IDS) to monitor all incoming traffic from the internet. The cybersecurity team configured source IP address verification on the firewall to detect and block spoofed IP addresses on incoming ICMP packets. Additionally, they implemented network monitoring software to identify abnormal traffic patterns, ensuring early detection of potential threats such as DDoS attacks.
Respond	For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network The team responds by blocking incoming ICMP packets,stopping all non-critical network services offline, and restoring critical network services. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.

Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online. Continue security awareness training for staff to recognize signs of a DDoS attack and understand recovery procedures.

Reflections/Notes: Always configure and review the Firewall settings according to the company's internal guidelines. Utilize IPS and IDS tools to protect the network. If these tools are insufficient, consider using cloud services to enhance network security and filter incoming ICMP packets.