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	Our organization experienced an attack, causing our network services to come to a sudden and unexpected stop. During the investigation, it was found that our network was being flooded with ICMP packets from multiple locations and devices, overwhelming network resources. Due to the flood of ICMP packets consuming the network's resources, normal network traffic was unable to access our services. We have identified this incident as a distributed denial of service (DDoS) attack. The entire incident lasted for two hours.
Identify	After a security audit conducted by our organization’s cybersecurity team, it was discovered that the network's firewall had not been properly configured. This vulnerability was exploited by the threat actor to flood our network resources with ICMP packets.
Protect	With the findings provided by the cybersecurity team, the organization’s network security team has implemented some updates using security hardening techniques. A new firewall rule has been added to limit the rate of ICMP packets that the network will allow. Additionally, the firewall now includes source IP verification to detect spoofed IP addresses on incoming ICMP packets.
Detect	Our teams are implementing source IP verification on our organization’s

	firewalls. This will enable the firewall to check for spoofed IP addresses on incoming ICMP packets. Additionally, an intrusion detection device has been added behind the firewall to enhance network security. It will flag suspicious ICMP traffic attempting to enter the organization’s network. Furthermore, our network security team has installed network monitoring software to detect abnormal traffic patterns.
Respond	Our security team will respond to any future attacks by promptly isolating the affected resources and assets to prevent the attack from spreading across our networks and systems. Subsequently, we will conduct an investigation by analyzing network logs and identifying any unusual activity.
Recover	As we transition into the recovery stage of this attack, our team's primary objective is to restore access to network services. Critical network services will be prioritized for restoration ahead of non-essential services.