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	
Identify	The company experiences a DDoS attack where network services suddenly stop responding. The DDoS overloads the network server by flooding ICMP packets. Some employers receive an email asking to log in with internal networks where it is a method that is used by threat actors to gain access to the database. The security team responded by blocking the attack and stopping all non - critical network services, so the critical networks could be restored.
Protect	The hacker or malicious actor used DDoS attacks where ICMP was sent to flood the network. The entire internal network was affected. All essential network resources needed to be secured and restored to normal operation.
Detect	The cybersecurity team applied a new firewall rule to restrict the rate of incoming ICMP packets and deployed an IDS/IPS system to filter out certain ICMP traffic with suspicious traits.
Respond	The cybersecurity team set up source IP address verification on the firewall to identify spoofed IP addresses in incoming ICMP packets and installed network monitoring software to detect unusual traffic patterns.

Recover	In response to future security events, the cybersecurity team will isolate impacted systems to avoid further disruption to the network. They will work to restore any critical systems and services that were affected by the event. Afterward, the team will review network logs to identify any suspicious or unusual activity. Additionally, they will report all incidents to senior management and relevant legal authorities, if necessary.

Reflections/Notes:

Regular updates on firewalls and patching the software that they used will be a huge help in terms of securing the network. Additionally, subnetting and network segmentation will also reduce the impact in case of attack.