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 organization's network services stopped responding and internal network traffic could not access any network resources. Further investigation found that the organization was under a DDOS attack in which an attacker was flooding the system with ICMP packets.
Protect	The team has implemented new firewall rules to limit the rate of incoming ICMP packets. The firewall was also configured to sniff packets for spoofed IP addresses on incoming ICMP packets. Additionally, new software was installed to detect abnormal traffic patterns and filter out suspicious traffic.
Detect	To detect future threats, the firewall will sniff packets to check for data packets from suspicious sources. The team will also configure a SIEM to monitor for suspicious activity.
Respond	The team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Recover	To recover, the team restored access to network services. Once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.