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 company faced a Distributed Denial of Service (DDoS) ICMP flood attack, which compromised the internal network for a duration of two hours. The incident was resolved by implementing countermeasures, specifically by blocking ICMP packets, temporarily taking non-critical network services offline, and subsequently restoring critical network services.
Identify	The company experienced a DDoS attack through an unconfigured firewall, flooding the network with ICMP pings and compromising critical services. Immediate measures were taken to restore critical network services.
Protect	The organization implemented a new firewall rule to restrict the rate of incoming ICMP packets, enhancing network security. Additionally, an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) was deployed to filter out specific ICMP traffic exhibiting suspicious characteristics.
Detect	The organization fortified its network security by implementing source IP address verification on the firewall, mitigating the risk of spoofed IP addresses in incoming ICMP packets.
Respond	The incident management team will respond to the security incident by blocking incoming ICMP packets, temporarily halting non-critical network services, and subsequently restoring critical network services. Additionally, the

	team can engage in log analysis to identify and investigate abnormal behavior,
Recover	The incident management team prioritized the recovery of critical network services during the security incident. They implemented a firewall block on ICMP requests and temporarily halted non-critical network services. Post-incident, non-critical services were gradually brought back online, ensuring a phased and secure restoration process.

Reflections/Notes: