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	During a DDoS attack, the company's internal network was compromised for two hours due to an incoming flood of ICMP packets. The incident was caused by a malicious actor sending ICMP pings through an unconfigured firewall, leading to a DDoS attack. The impact included the disruption of normal network services. The response involved blocking incoming ICMP packets, stopping non-critical network services, and restoring critical services. To mitigate future attacks, the security team then implemented new firewall rules, source IP address verification, network monitoring software, and an IDS/IPS system.
Identify	The type of attack was a DDoS attack using ICMP flood. Systems affected included internal network services. The attack source was identified as a malicious actor exploiting an unconfigured firewall. The estimated impact included disruption of normal network services for two hours.
Protect	Implement source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. Update firewall rules to limit the rate of incoming ICMP packets.
Detect	Implement network monitoring software to detect abnormal traffic patterns. Deploy an IDS/IPS system to filter out suspicious ICMP traffic.

Respond	Develop response plans for containing and neutralizing future DDoS attacks. Improve communications to inform stakeholders about security event response procedures. Analyze incident data to identify patterns and improve response strategies.
Recover	Construct a recovery plan to restore affected systems and data. Identify improvements to enhance the organization's recovery systems and processes. Establish communication channels for disseminating restoration procedures within the organization and to affected parties.

Reflections/Notes: