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	Today the organization experienced a network outage that lasted approximately 2 hours.during this time,network services became unresponsive due to DDos attack. The incident management team resolved the issue.
Identify	The investigation revealed that the firewall was not configured properly..This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Protect	The team implemented a new firewall rule to limit ICMP packets to prevent DDoS attacks in future.Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Detect	To detect DDos Attacks in the future the team will use an IDS/IPS system to filter out some network traffic based on suspicious characteristics.Network monitoring tools were also introduced to identify abnormal traffic patterns early.

Respond	The incident management team responded by blocking incoming ICMP packets, shutting down all non essential services and prioritizing the restoration of critical systems. This helped to contain the incident and reduce its impact
Recover	The team restored critical network services,the network returned to normal operation.Recovery procedures included verifying system integrity,update firewall configurations and preparing post incident reports to support continuous improvement.

Reflections/Notes: