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	It was reported that the organization's internal network has stopped responding completely. Logs indicate the the network was flooded with ICMP packets because of which normal internal traffic could not access the network. The company's cybersecurity team investigated the security event and found that the malicious actor had flooded the system with ICMP pings through an unconfigured firewall. This vulnerability allowed the malicious actor to overwhelm the network with a successful Distributed Denial of Service Attack (DDos)and shut down operations for two hours.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The investigation revealed an unconfigured firewall through which the network was flooded with ICMP pings. The network was overwhelmed by a DDos attack stopping all critical network services.
Protect	The firewall was configured to limit the rate of incoming ICMP packets. An IDS/IPS system was implemented to filter out some ICMP traffic based on suspicious characteristics.
Detect	To prevent such future attacks, the firewall was configured to verify the Source IP address to check for spoofing on incoming ICMP packets and a network

	monitoring software was implemented to detect abnormal traffic patterns
Respond	For such future security events, the cybersecurity team will first isolate the affected systems to prevent further damage and then proceed with restoring critical network services. Then the team will analyze the logs to check for suspicious abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	To recover from the DDoS attack through the ICMP flooding, we need to first block all incoming ICMP packets through the firewall. Then all the non-critical services offline are stopped to reduce internal network traffic. Next, the critical services are restored. Finally, once all ICMP packets have timed-out all non-critical services are restarted and the system is returned ot its original state.

Reflections/Notes: