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 web servers were compromised due to an unconfigured firewall rule which was exploited by the malicious actor in order to breach into the network and flood the server with ping i.e. icmp packets causing the server to slow down and eventually crash. The cybersecurity team temporarily blocks all traffic and restores the service eventually which took the website down for 2.5 hours.
Identify	A firewall misconfiguration was the cause of the event.
Protect	Every incoming traffic was blocked causing the server to be isolated , meanwhile the team analyzed and restored the server. The cybersecurity team also implemented some firewall rules to limit the rate of ICMP packets.
Detect	The cybersecurity team applied rules to detect the spoofed ip if in future any same or matching attack surface.
Respond	In future , if any same event occurs , the team will isolate the compromised system, try to recover it and report it to upper management.
Recover	In future ICMP flood attacks will be blocked at the firewall only if in any case a dos attack event occurs , the backup servers can tackle the legit traffic meanwhile the main or compromised servers get recovered.

Reflections/Notes: