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 Organization has been impacted with DDOS attack and affected the business operations for nearly 2 hours. The attack caused the network services to stop suddenly because the services got overwhelmed due to incoming ICMP packets. Incident management team prevented the attack by blocking incoming ICMP packets and restored critical network services. The Investigation revealed that the attack was successful due to an unconfigured firewall. Attackers exploited this vulnerability to launch an attack on an organization's network. Security team addresses this security event by taking security measures such as updating firewall rules and implemented network monitoring software to detect abnormal traffic patterns.
Identify	The Incident management team audited the internal system, devices & access policies involved in the incident to identify the gaps in the security. Upon investigation it revealed that the misconfiguration of the firewall led to the security event.
Protect	The team has addressed the security event by implementing network monitoring software to detect abnormal traffic patterns and updated the firewall rules to prevent future incidents from occurring in the future.
Detect	To detect Incidents happening in the future, the cybersecurity team configured

	source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	The team developed an incident response plan to detect and respond to similar attacks happening in the future with proper standards and procedures. The playbook standards and procedures have been communicated with the employees to create awareness and inform on how to take actions if a similar event takes place.
Recover	The team will recover the affected system back to normal operations. In the future, external ICMPflood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMPpackets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: