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 company recently experienced a DDoS attack which compromised the company's internal network for about 2 hours affecting its daily operations. The investigation undertaken by the cybersecutiy team revealed that attack was carried out by flooding ICMP packets on the network. The threat actor used the unconfigured firewall to carry out this attack. Even though the security team was able to restore critical services, the non critical services remained unaccessible for 2 hours. The cybersecurity team found out the vulnerabilities that were exploited by the malicious actor and implemented new rules to avoid similar incident occurimng in the future.
Identify	During the investigation, the cybersecurity team thoroughly audited the vulnerabilities in the company's network and also its causes. The team found out that unconfigured firewall was the main vulnerability that the attacker exploited. The attacker managed to disrupt company's network by flooding ICMP packets on the server.
Protect	The team implemented new firewall rule to stop similar future attacks. The team configured the firewall to limit the incoming ICMP packets by enabling Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
Detect	To detect future attacks, the team will use SIEM tool to monitor abnormal traffic patterns on the organization's network. Additionally, the team also introducing

	the use of IPS and IDS systems to strengthen the network.
Respond	In future, company will apply isolation techniques to respond to similar attacks. Company will shift its focus on redundancy as well.
Recover	To recover from DDoS attacks, company will employ network segmentation which will allow company to keep critical assets separate and secure in different zones. In case of similar future incidents, company can ensure the traffic to critical systems will be appropriately filtered by the firewall.

Reflections/Notes: