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 multimedia company recently experienced a distributed denial of service attack (DDoS), compromising the internal network for about 2 hours. The attack caused the organization's network service to go unresponsive due to incoming Internet Control Message Protocol (ICMP) packets. During the 2-hour-long incident, normal internet traffic could not access any network resources.
Identify	The security team investigated the issue and found out that the malicious actor had sent a flood of ICMP pings through the company's network due to an unconfigured firewall, allowing the malicious actor to overwhelm the company's network.
Protect	The security team will immediately configure the firewall with new rules and implement an Intrusion Prevention System (IPS) in our network security to detect and actively drop suspicious network packets.
Detect	The security team will implement an Intrusion Detection System (IDS) within our organization's networks to alert the security team to any suspicious activity within our networks.
Respond	The security team responded to the incident by setting a firewall rule to reduce the rate of all ICMP packets, stopping all non-critical network services offline,

	and restoring critical services. Furthermore, the security team will train our interns and employees on how to properly configure a firewall. The team will also emphasize the importance of setting rules on firewalls.
Recover	The security team will recover from this incident by documenting this incident on our incident response playbook to be better prepared for similar future incidents and conduct a post-incident review.

Reflections/Notes: