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	This morning, a DDoS attack occurred due to incoming flood of ICMP pings through an unconfigured firewall. The attack lasted for 2 hours until the network security team contained the compromised network by blocking incoming ICMP packets and restoring critical network services. Afterward, the firewall was configured to address the known vulnerabilities shown through this attack.
Identify	Network security team found that the unconfigured firewall was the main gap in the security event. Website services to customers and employees were affected in the attack.
Protect	**The team has implemented new firewall rules as well as source IP address verification. Additionally, a network monitoring software to detect abnormal traffic patterns, and an IDS/IPS system has been implemented to prevent future attacks.**
Detect	To detect network attacks in the future, the network security team will implement an intrusion detection/prevention system and network monitoring software to monitor all incoming traffic from the internet.
Respond	We will confirm that the service outage is a DDoS attack and inform employees and users about the situation. Then we will analyze the traffic patterns to

	identify the nature of the attack and disable non-vital functionality that makes the attack more effective. Stop the attack through either IP blocking, diverting traffic, or rate limiting and then recover services. Regular audits should be conducted in the future.
Recover	The team will restore the system in stages starting from most critical to least and ensure all malicious artifacts are removed if any. We will let our users and employees know when the issue has been resolved.

Reflections/Notes: