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 to practice applying the NIST framework to different situations you encounter.

Summary	You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	The company experience a distributed denial of service (DdoS) attack. The target gained access through an unconfigured firewall.
Protect	The company needs to address the unconfigured firewall immediately. This should help with the threat actor gaining access. Port filtering, firewall maintenance, and IP blocking need to be implemented when addressing the firewall.
Detect	The company can put in place IDS or IPS systems to provide real time monitoring of assets. They will also need to monitor logs via a SIEM software.
Respond	If the IDS or IPS system detects an intruder, the cybersecurity team is notified. As a result, those systems that have been compromised need to be brought offline to determine severity of intrusion. Upper management should be kept in the loop regarding all developments. Once attack vector has been determined, the security team needs to make the necessary changes to the firewall configurations to prevent future intrusion. Pen testing needs to be untaken to ensure all entry points have been addressed. Once everything is working correctly, then the offline systems can be brough back online.
Recover	Once the security team has implemented the new security controls, then the impacted server can be brought back online.

Reflections/Notes: