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	The multimedia company that varies services has been compromised by the DDoS attack. During the attack, due to over flooding of incoming ICMP packets, the organization's internal network stopped working which resulted in the normal internet traffic not accessing the network. Then the incident response team responded and after two hours the organization's network was back to normal.
Identify	The company's internal network has been compromised by the DDoS attack. The internal network is flooded with ICMP packets. Hence, the internal network suddenly stopped responding.
Protect	To address this issue and protect the network the team implemented a new firewall policy to limit incoming ICMP packets. Source IP verification on the firewall to check for spoofed IP addresses. Network monitoring software to detect abnormal traffic. An IDS/IPS system to filter out incoming traffic.
Detect	To detect new traffic like these in the future the team will use network monitoring tools such as SIEM. An IDS/IPS will be implemented to filter and monitor the incoming traffic.
Respond	The incident team responded by blocking incoming ICMP traffic, stopping all non-critical network services offline, and restoring critical network services.
Recover	The team will recover by giving proper training on network hardening to their employees and reducing the attack surface.

Reflections/Notes: