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	For two hours the internal network of the company was breached and attacked by an ICMP Flood DDoS. During the attack network services suddenly stopped responding due to the overwhelming amount of ICMP packets flooding the network. The team then responded by stopping all non-critical services, and restoring all critical network services.
Identify	The network was flooded with ICMP packets coming from different IP addresses, so the attack was a DDoS ICMP Flood. The flood affected the internal network as it couldn't access any network resources. This was able to occur due to an unconfigured firewall.
Protect	In order to protect against this in the future the firewall must first be configured to limit the rate of incoming ICMP packets. Then the firewall must be configured to verify source IP addresses. Then a network monitoring software can be used to detect abnormal traffic patterns. Finally an IDS or IPS can be used to detect and filter out any unusual packets that make it past the firewall.
Detect	In order to detect packets entering the network it is recommended to use a SIEM tool to analyze and alert for any odd traffic behaviors. An IDS can be used to detect any odd traffic and also detect any common attacks on your network.

	While an IPS can be used to detect and protect against any common attacks on the network.
Respond	In the event of a future event the best way to respond would be to detect the attack through the SIEM logs or through an IDS, then when we know an attack is occurring, and the packets already made it through the firewall. We can then detect any odd IP addresses and drop their packets so they don't clog up the network. We can do this by updating our firewall rules.
Recover	In order to recover from this type of attack we would need to restore network services that weren't able to function due to a clogged up network.

Reflections/Notes: