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 company experienced a DDoS attack which compromised the internal network for two hours until it was fixed. Network services stopped working due to a high volume of incoming ICMP packets and normal traffic couldn’t access network resources. The incident response team blocked incoming packets, stopped all non-critical network services, and eventually restored network function. It was discovered that the attacker exploited an unconfigured firewall to execute the ICMP flood attack.
Identify	The attacker targeted the organization’s network and its core functionality by overwhelming it. The specific vulnerability was an unconfigured firewall.
Protect	The security team updated the firewall to limit the amount of ICMP packets it would receive to prevent a future attack like this. They also implemented an IDS/IPS to filter suspicious ICMP traffic.
Detect	The security team implemented network monitoring software as well as a new feature on the firewall to check for spoofed IP addresses on incoming ICMP packets, which could give an early indication of malicious intent.
Respond	In the future the security team will respond in a similar way if another of these attacks happens. Blocking the incoming ICMP packets is the first priority before

	stopping non-critical network functionality and isolating devices if possible. Firewall configurations should then be updated based on the nature of the attacks.
Recover	Once it has been established that the incoming ICMP flood has been blocked at the firewall level the network can be brought back to normal functionality and any isolated parts can be re-integrated. In the future, the adjustments that have been made should help prevent future attacks but it is important to always be prepared.

Reflections/Notes: