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 organization's network stopped for 2hrs after a flood of ICMP packets was received in the internal network. ICMP packets to non critical systems was blocked to reduce the impact of the attack.
Identify	Investigations done by the security team discovered that an unconfigured firewall was used by the malicious actor to perform a DDOS attack. The internal network traffic became compromised for 2hrs.
Protect	A new firewall rule to limit the rate of incoming ICMP packets has been implemented. Configuration checks on a day to day basis will be prioritized.
Detect	Network monitoring software has been introduced to detect abnormal traffic patterns. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics has been configured.
Respond	The team configured the firewall with a new rule that limits the rate of incoming ICMP packets. Source IP verification has been implemented on the firewall to check for spoofed IP addresses on incoming ICMP packets
Recover	After configuring firewall and IDS/IPS systems to filter abnormal traffic, all network services came online

Reflections/Notes: