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	We recently experienced a DDos attack, which led to 2 hours of downtime for our internal network. The issue was resolved by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	The team found that our internal servers suddenly stopped responding when we received a flood of ICMP packets. Network resources could not be accessed by our normal internal network traffic. A malicious actor flooded an unconfigured firewall with ICMP pings. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack. This affected our internal employees, but our regular services to our clients were not affected.
Protect	We created a new firewall rule to limit the rate of incoming ICMP packets. We also added an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	Sudden spikes in ICMP packets should be monitored, as there may be more attempts by the threat actor going forward.
Respond	When ICMP packets spike again, the offending IP addresses should be blocked immediately as a preventative measure while we investigate whether it is a malicious attack or something else.
Recover	Once the ICMP pings were blocked, our internal servers started responding again. Source IP address verification was implemented on the firewall to check for spoofed IP addresses on incoming ICMP packets. Network monitoring software was installed to detect abnormal traffic patterns.

Reflections/Notes: Since the threat actor knew which Firewall port to target, and the target was our internal network, it is possible that the threat actor is a current or former disgruntled employee