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. The attack lasted for approximately 2 hours, which rendered the company's network services unresponsive. The attack was initiated by a malicious actor who sent a flood of ICMP packets to the company's network. The attack was successful due to a misconfigured firewall that allowed the ICMP traffic to overwhelm the network. The company had to take down non-critical network services to prioritize and restore critical services. In response to the attack the security team blocked incoming ICMP packets, took non-critical services offline, and implemented new security measures. These new security measures include a new firewall rule that limits the rate of of incoming ICMP packets, another firewall rule that checks for spoofed IP addresses on incoming ICMP packets, installed software to detect abnormal traffic patterns to enhance early warning capabilities, and deployed a, IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Identify	The attack was noticed due to all of the company's network services suddenly going offline. Upon closer inspection of network traffic, it was clear that the attack was a DDoS attack which used excessive ICMP traffic to overwhelm the network.

Protect	The security team implemented four new security features to protect the company and prevent this attack from happening in the future. 1. A new firewall rule to limit the rate of incoming ICMP packets 2. Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets 3. Network monitoring software to detect abnormal traffic patterns 4. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Detect	Using the new security features put in place, the security team now has the tools to detect this type of attack in the future. Using the IDS/IPS system and network monitoring software, the security team can more effectively monitor the network and prevent ICMP flood attacks.
Respond	Responding to future incidents will be done by monitoring the network through the new tools put in place to detect this type of attack. These attacks can be stopped early now that they are detectable.
Recover	To recover from the incident, the security team had to firstly block the incoming traffic. Then to get our network back online, we had to reboot our network devices.

Reflections/Notes: