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	Recently our organization experienced a DDoS attack due to a flood of incoming ICMP packets that compromised the internal network for two hours till the said attack was resolved. The team mitigated the issue by blocking attack and stopping all non-critical network services, so that the critical networks could be restored.
Identify	After accessing the network log we noticed that there was a high incoming traffic for ICMP packets. Normal internet network traffic could not gain access to any resources. After further investigation it seems that an attacker has been sending a flood of ICMP pings into the company's network through an unconfigured firewall vulnerability. This allowed the attacker to exhaust the company's network through a distributed denial of service (DDoS) attack.
Protect	New measures have been implemented to stop this type of breach from happening again in the future. The team has added a new firewall rule to limit the rate of incoming ICMP packets. The team has also added an IDS/IPS system to help filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect future unauthorized attacks the team has added a network monitoring software to detect abnormal traffic patterns. A source IP address verification on the firewall has also been added to check for spoofed IP

	addresses on incoming ICMP packets.
Respond	For future situations the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the attack. The team will analyze network logs to check for suspicious and abnormal activity taking place within the organization. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be first priority to be restored, once the flood of ICMP packets have been mitigated, all the non-critical network systems and services can be brought back online.

Reflections/Notes: