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	This morning, our servers were flooded with ICMP packets, rendering our services inaccessible to the public. We believe that a DDOS attack has occurred which took us offline for about 2 hours. The incident management team has stopped the receiving of ICMP packets and began restoring critical services to get the server back online. It has been determined that the vulnerability that was exploited was the firewall that has been configured incorrectly.
Identify	The incident management team determined that a flood of ICMP packets were sent to an unconfigured firewall, making it impossible for normal traffic to access our servers.
Protect	The team decided to block all incoming ICMP packets. Also, a new firewall rule was created to limit the rate of incoming ICMP packets, source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, network monitoring software to detect abnormal traffic patterns, and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. There will be new training to teach new users on how to configure and maintain these new softwares.
Detect	The team will now use a network monitoring software to detect abnormal traffic patterns.

Respond	The team blocked all incoming ICMP packets, stopped all non-critical network services offline, and restored critical network services.
Recover	The team restored critical network services, and configured the firewall. New software such as an IDS/IPS were installed to detect suspicious activity and will block it as such.

Reflections/Notes: