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, my organization experienced a DoS attack, which shut down the internal network until it was resolved 2 hours later. The consequences of this attack were that the network services stopped responding and normal internal network traffic could not access any of the network resources.
Identify	The cybersecurity team investigated the event, and found that a malicious actor had sent a flood of ICMP pings through an unconfigured firewall in the company's network. This overwhelmed the servers and caused a DoS (Denial of Service) attack.
Protect	The incident response team blocked all incoming ICMP packets, stopping all non-critical network services, and then restored the critical network services. A new firewall rule has been made to limit the rate of incoming ICMP packets, source IP address verification has been added to the firewall to check for spoofed IP addresses on incoming ICMP packets, Network monitoring software has been added to detect abnormal traffic patterns and an IDS/ISP system has been added to filter out some ICMP traffic with suspicious characteristics.
Detect	The newly added IDS/ISP system will help to detect and prevent suspicious traffic from progressing through the network, and the firewall will prevent excess ICMP packets from causing another similar incident in the future.

Respond	Consider adding port filtering to the firewall to prevent risks from less safe ports, for example port 80 to prevent HTTP access, closely analyze network traffic and work with the IPS/IDS systems to see what are commonly appearing suspicious patterns. Keep working with the firewall and evaluate how the new preventative measures are performing. If the performance is still not up to par, re-evaluate firewall configuration.
Recover	Focus on restoring all critical network services to normal performance, and then non-critical network services. As the site was offline for 2 hours and no data was lost, data recovery is not an issue in this case.

Reflections/Notes: This event seemed to come from a massive lack of security measures that have now been added, so the odds of a similar event happening in the future are much lower now.