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 organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, the organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Protect	To protect the internal network and ensure delivery of network services, the team has implemented a new protective firewall configuration to both limit the rate of incoming ICMP packets and check for spoofed IP addresses on incoming ICMP packets. The team invested in an intrusion prevention system (IPS) which detects abnormal traffic patterns and filters out some ICMP traffic based on suspicious characteristics
Detect	To detect suspicious activity in the future, such as incoming external ICMP packets from non-trusted IP addresses attempting to pass through the

	organization's network firewall, the team will use a firewall logging tool to continuously monitor traffic from the internet and verify source IP addresses on incoming ICMP packets . The team will use as well an intrusion detection and prevention system (IDS/IPS) to protect against future attacks by detecting any unusual activity and abnormal traffic patterns and filtering out threats.
Respond	The incident management team blocked incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. We informed upper management of this event and they will contact our customers by mail to inform them about the DDoS attack, which compromised the internal network for two hours. Management will also need to notify IT to update the unconfigured firewall. If applicable, management will also need to inform law enforcement and other organizations.
Recover	The team will recover the network services by restoring the internal network. We have informed the IT staff that the unconfigured firewall must be updated immediately and configured regularly.

Reflections/Notes: