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	A DDoS attack was performed against our internal network, in which critical services stopped responding due to a flood of ICMP packets. The incident response team blocked incoming ICMP packets. It was discovered that the ICMP packets were able to be sent due to an unconfigured firewall, which is in the process of being remediated.
Identify	● An ICMP flood DoS attack was performed ● The internal company network was affected ○ Internal network traffic was unable to access network resources
Protect	● Network segmentation will be performed to ● Perimeter firewalls will be configured to reject incoming ICMP packets of the type that are used in an ICMP flood attack
Detect	● An IDS/IPS solution will be implemented within the internal network and integrated into a SIEM to provide real-time detection, monitoring, and response capabilities.
Respond	● An incident response playbook will be created and revised to ensure that incident responders have adequate resources to respond to a cybersecurity incident

Recover	● Affected machines will be taken offline and quarantined in the event of an incident ● Backups of networked devices will be created ● Known-good configurations will be saved for critical network appliances

---

Reflections/Notes: