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 multimedia company experiences a DoS attack which compromised the internal network for 2 hours before the issue was resolved. The network was flooded with ICMP packets and normal internal network traffic could not access the needed network resources. The security team responded by clocking incoming ICMP packets, stopped all non-critical network services, and restored critical services. The incident was investigated once it was resolved and it was found that the ICMP pings were sent through an unconfigured firewall. To mitigate this vulnerability, the security team wants to implement a new firewall wall to limit incoming ICMP packets, source IP address verification, network monitoring software, and an IDS/IPS system
Identify	A malicious actor targeted the organization with an ICMP packet attack via the unconfigured firewall. The entire internal network was impacted and critical network resources needed to be secured and returned to functioning state.
Protect	Implement a new firewall rule that limits the rate of ISMP packets that can come from an external source and an IDS/IPS system that can filter suspicious traffic.
Detect	IP source verification configuration on the firewall will help detect spoofed IP addresses and network monitoring can detect any suspicious network activity.

Respond	Isolate of affected systems and quick restoration of critical systems is the goal. Once completed via policy and procedures learned from this event, it is critical to analyze the network logs and capitalize on any SIEM tools to ensure that the malicious activity is ceased. All incidents, impacts, and outcomes should be reported to management.
Recover	To recover from a DoS attack access to all network resources need to be at a normal functioning rate. Moving forward, with the controls put in place, the ICMP pings should be blocked by the firewall configurations and IP spoofing should be blocked. If it were to happen again, the systems should be isolated, ICMP packets blocked, critical services should be restored, and once the network is cleared of suspicious activity business should be restored to normal functions.

Reflections/Notes: