POST INCIDENT ANALYSIS: 5 WHYS

Incident: Samba usermap_script exploit attempt detected on host 192.168.1.36.

1. Why did the exploit succeed in reaching the host?

Because the target host had SMB services exposed without proper segmentation or access restrictions.

2. Why were SMB services exposed without restrictions?

Because legacy Samba scripts were enabled, and network policies did not limit SMB traffic to trusted hosts.

3. Why were legacy scripts enabled and traffic unrestricted?

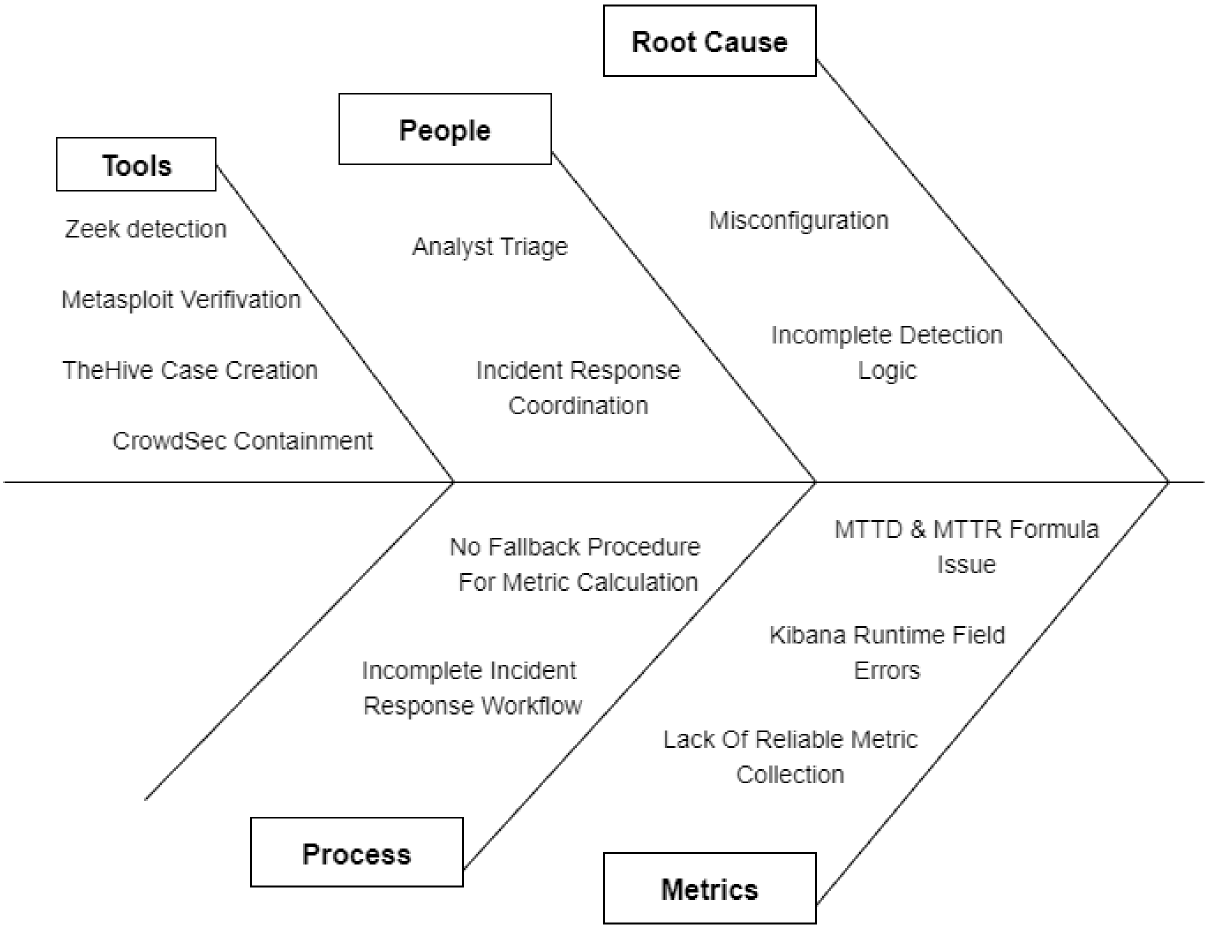
Because system hardening and patch management processes were incomplete, leaving unnecessary services active.

4. Why were patch management and hardening processes incomplete?

Because there was no automated vulnerability monitoring and enforcement mechanism in place for SMB services.

5. Why was there no automated monitoring and enforcement?

Because the organization had not yet fully integrated network monitoring (Zeek), alerting (TheHive), and automated containment (CrowdSec) into a unified security operations workflow.


Root Cause
People
Tools
Zeek detection
Metasploit Verifivation
TheHive Case Creation
CrowdSec Containment
Analyst Triage
Incident Response Coordination
Misconfiguration
Incomplete Detection Logic
No Fallback Procedure For Metric Calculation
Incomplete Incident Response Workflow
MTTD & MTTR Formula Issue
Kibana Runtime Field Errors
Lack Of Reliable Metric Collection
Process
Metrics

1: Fishbone Diagram

Root Cause Summary:

The Samba backdoor exploit was enabled by exposed legacy SMB functionality and incomplete system hardening, compounded by the lack of integrated monitoring and automated containment mechanisms.

Recommendation:

- Disable unnecessary legacy scripts and services.
- Implement network segmentation for SMB hosts.
- Automate patch management and vulnerability scanning.
- Integrate Zeek, TheHive, and CrowdSec to detect, alert, and contain similar exploits in real time.