# Incident Response Report – Samba RCE

## Executive Summary

A Samba RCE attack simulation was conducted on a vulnerable Metasploitable2 machine within a SOC workflow scenario. The attacker leveraged a usermap_script vulnerability of Samba with Metasploit, causing illicit root access. Containment was immediately addressed to mitigate further issues.

## Timeline

- **14:00** – Metasploit exploitation initiated from attacker system
- **14:02** – Successful root access confirmed on target host
- **14:05** – Attacker IP identified as malicious
- **14:07** – CrowdSec used to block attacker IP
- **14:10** – Incident escalated to Tier 2 via TheHive

## Recommendations

- Disable or upgrade vulnerable Samba services.
- Implement endpoint monitoring agents on all hosts.
- Enforce network segmentation to limit blast radius.
- Enable centralized logging and automated alerting.
- Regularly conduct vulnerability scans and patching