

Evidence Collection Summary

During the post-exploitation phase, privileged access was obtained using Metasploit's AlwaysInstallElevated technique. Network traffic was captured with Wireshark to identify malicious activity. Collected artifacts were hashed using SHA-256 and documented with proper chain-of-custody to ensure evidence integrity and forensic validity.