Post-Exploitation Practice Report

Overview

This exercise focused on performing post-exploitation activities within a **controlled laboratory environment**. The objectives were to validate privilege escalation capabilities on a compromised Windows system and to collect forensic evidence while maintaining integrity and traceability.

Objectives

- Validate the possibility of **local privilege escalation**
- Demonstrate weaknesses in **User Account Control (UAC) configuration**
- Collect and preserve digital evidence with **cryptographic integrity verification**
- Maintain a verifiable **chain of custody**

Tools Utilized

- **Meterpreter** – post-exploitation and session management
- **Volatility** – memory forensics and validation
- **sha256sum** – cryptographic hashing for evidence integrity

---

Objective

To determine whether the compromised system allowed **User Account Control bypass**, indicating weak privilege enforcement or misconfigured security controls.

Outcome

The privilege escalation attempt was successfully executed within the lab environment. Elevated access was obtained, confirming:

- Insufficient privilege separation
- Inadequate or misconfigured UAC protections on the target system

All actions and results were **logged for later analysis and reporting**.

Evidence Collection & Integrity Verification

Evidence Collection Method

A configuration file was retrieved from the target system. To preserve forensic integrity, a **SHA-256 hash** was generated immediately after acquisition.

Evidence Record (Initial Collection)

Item	Description	Collected By	Date	Hash Value
Config File	target.conf	VAPT Analyst	2025-08-18	9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08

Evidence Log (Subsequent Review)

Item	Description	Collected By	Date	Hash Value
Config File	target.conf	VAPT Analyst	2026-01-06	`<SHA256>`

Conclusion

Post-exploitation activities demonstrated the critical impact of **weak privilege management** and improper UAC configuration. Successful privilege escalation highlights the need for stricter access controls and hardened system policies.

The use of **SHA-256 hashing** ensured that collected evidence remained unaltered, supporting forensic validation and preserving a defensible chain of custody throughout the assessment process.
