Post-Exploitation Practice

Activities:
Perform post-exploitation tasks in a controlled lab environment, including privilege escalation validation and forensic evidence collection.

Tools:

- Meterpreter
- Volatility
- sha256sum

Tasks:

- Simulate privilege escalation
- Collect and preserve evidence with integrity verification

Privilege Escalation

Technique: Local privilege escalation using a Metasploit post-exploitation module
Module Referenced: `exploit/windows/local/bypassuac`
Objective: Validate whether User Account Control (UAC) bypass is possible on the compromised system.

he privilege escalation attempt was executed within the lab environment, and results were logged for analysis. Successful escalation demonstrated inadequate privilege separation and misconfigured UAC controls on the target system.

Evidence Collection ➕**Method:**
A configuration file was collected from the target system, and a SHA-256 hash was generated to ensure evidence integrity and support forensic validation.

Evidence Collection — Hashing a File
Target.conf
sha256sum target.conf

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 target.conf

Item	Description	Collected By	Date	Hash Value
Config File	target.conf	VAPT Analyst	2025-08-18	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Evidence Log

Item	Description	Collected By	Date	Hash Value
Config File	target.conf	VAPT Analyst	2026-00-1	`<SHA256>`

Post-exploitation activities highlighted the importance of privilege management and secure system configuration. Evidence hashing ensured data integrity, supporting forensic analysis and maintaining a verifiable chain of custody during security assessments.