4. Post-Exploitation and Evidence Collection

Objective

The objective of this phase was to validate post-exploitation access, simulate privilege escalation, and collect forensic evidence while maintaining proper chain-of-custody procedures on the DVWA test environment.

Post-Exploitation

After successful exploitation of vulnerabilities in the DVWA web application, a Meterpreter session was established on the target system. Post-exploitation techniques were used to validate the level of access and assess the potential impact of the compromise.

A privilege escalation assessment was performed using Metasploit's local privilege escalation techniques. The objective was to determine whether an attacker could elevate privileges after initial access and gain deeper control over the system.

All activities were conducted in a controlled lab environment strictly for educational and internship purposes.

Privilege Escalation

Tool Used: Metasploit Framework
Technique: AlwaysInstallElevated

The privilege escalation phase involved analyzing system configurations that could allow elevation of privileges. Misconfigured installer policies may allow attackers to execute code with elevated permissions if exploited in real-world environments.

Session activity was logged to ensure traceability and accountability.

Evidence Collection

Network traffic was captured during post-exploitation activities using Wireshark to document communication between the attacker and the DVWA server. Evidence was collected in a forensically sound manner to preserve integrity.

Summary

During post-exploitation, network traffic related to the DVWA compromise was captured and preserved. All collected artifacts were hashed using SHA-256 to maintain integrity and chain-of-custody. This ensured that the evidence remained unaltered and could be reliably used for further forensic analysis and reporting.