

Post-Exploitation Report

1. Objective

The aim of this task was to perform post-exploitation activities after gaining access to a target system in a controlled lab environment. The focus was on understanding what an attacker can do after initial compromise, including privilege escalation, controlled evidence collection, integrity verification using cryptographic hashing, and basic memory analysis.

2. Scope of Assessment

- Target System: Windows 7 (Service Pack 1)
- Architecture: x86
- Environment: Controlled laboratory setup
- Access Method: Meterpreter reverse TCP session
- Assessment Type: Educational post-exploitation

All actions were carried out strictly for learning purposes.

3. Tools Used

The following tools were used during the post-exploitation phase:

- Metasploit Framework (Meterpreter) – Used for session management and privilege escalation
- sha256sum – Used to verify the integrity of collected evidence
- Volatility Framework – Used for basic memory analysis
- Windows Command Shell – Used for file creation and system verification

4. Methodology

The post-exploitation process was carried out step by step:

1. A Meterpreter reverse TCP session was established with the target system.
2. System information and user privilege levels were verified.
3. Privilege escalation was attempted using a local UAC bypass technique.

4. A sample evidence file was created and collected from the system.
5. A SHA-256 hash was generated to confirm evidence integrity.
6. A memory dump of a sensitive process was captured.
7. Basic memory analysis was performed using Volatility.

Screenshots and logs were recorded to support each step.

5. Post-Exploitation Activities

5.1 Session Establishment

A Meterpreter session was successfully obtained on the Windows 7 system. Using Meterpreter commands, system details such as operating system version, architecture, and current user context were verified.

5.2 Privilege Escalation

Privilege escalation was performed using the `exploit/windows/local/bypassuac` module. This resulted in a new Meterpreter session running with `NT AUTHORITY\SYSTEM` privileges, confirming successful escalation.

Impact:

SYSTEM-level access provides complete control over the system, including access to sensitive files, processes, and system configurations.

5.3 Evidence Collection

A sample file named `target.conf` was created on the target machine and then downloaded to the attacker system using Meterpreter. This step demonstrates how evidence can be collected in a controlled and traceable manner during post-exploitation.

5.4 Integrity Verification

The collected file was hashed using the SHA-256 algorithm. Generating a hash ensures that the evidence remains unchanged and can be verified later during analysis or reporting.

5.5 Memory Dump and Analysis

A memory dump of the lsass.exe process was captured using a Metasploit post-exploitation module. The dump was analyzed using the Volatility Framework. Although detailed analysis requires proper kernel symbols, this step demonstrates standard memory forensics techniques used during post-exploitation.

6. Risk and Impact Analysis

Post-exploitation access with SYSTEM privileges represents a critical security risk. An attacker could extract credentials, alter system settings, or maintain long-term persistence. Memory dumping further increases the risk by exposing sensitive information such as authentication data.

7. Remediation Recommendations

To reduce post-exploitation risks, the following actions are recommended:

- Keep the operating system fully patched and updated
- Limit privilege escalation vectors and enforce UAC restrictions
- Monitor and control administrative access
- Deploy endpoint protection and behavior-based detection tools
- Regularly audit systems for unusual or suspicious activity

8. Conclusion

This post-exploitation exercise demonstrated how attackers can escalate privileges, collect evidence, verify integrity, and perform memory analysis after gaining access to a system. The task highlights the importance of strong post-compromise defenses and the need for layered security controls to minimize damage after an initial breach.