THICK CLIENT PENTESTING

A SIMPLE APPROACH TOWARDS THICK CLIENT APPLICATIONS

STEP 1

INFORMATION GATHERING

- **The architecture of the application** - two-tier, three-tier etc.
- **Network Analysis** - IP Information, Communication flow, Sensitive information in Traffic.
- **Tech stack** - Language, Version.
- **Application workflow** - Authorization, Authentication mechanism, Business logic.
- **Tools** - DetectitEasy, Wireshark, TCP View, TCP Dump, CFF Explorer etc.

STEP 2

GUI ATTACKS

- **Hidden Objects** - Find and enable hidden Buttons and TextFields.
- **Hidden Functionalities** - Find and enable hidden functions.
- **Privilege Escalation** - Manipulate values to gain higher privileges.
- **Client Side Control Bypass** - Max length bypass etc.
- **Tools** - Snoop, DnsSpy, ILSpy etc.

STEP 3

REGISTRY TESTING

- **Sensitive Information** - Passwords, Keys etc.
- **Permissions** - Write permissions to be checked.
- **Privilege Escalation** - Manipulate roles if applications refer it from the registry.
- **Tools** - Process Monitor, Regshot etc.

STEP 4

ASSEMBLY ANALYSIS

- **Lack of Obfuscation** - Check whether the code is obfuscated or not.
- **Sensitive Information** - Hardcoded data in source code.
- **Binary Analysis** - ASLR, DEP, SafeSEH, StrongNaming, Authenticode, Control Flow Guard, and HighEntropyVA.
- **SignCheck** - Check whether the application sign or not, for integrity
- **Tools** - Get-PESecurity, DnsSpy

STEP 5

MEMORY ANALYSIS

- **Sensitive Logs** - Email, Passwords, Keys etc.
- **DLL Hijacking** - If the application loading any dll which does not exist, replace it with a malicious dll.
- **Permissions** - File permissions in the Application folder to be check
- **Flooding attacks** - DOS etc.
- **Tools** - Strings, Process hacker, Process monitor, Dotpeek etc.

STEP 6

OWASP TOP 10

- **A01:2021**-Broken Access Control
- **A03:2021**-Injection
- **A07:2021**-Identification and Authentication Failures
- **A08:2021**-Software and Data Integrity Failures
- **A09:2021**-Security Logging and Monitoring Failures
- In addition, it **depends on the functionality** of the application

@N008x