Penetration Tester way of Attacking Thick Client

About Me

Manish Sharma

Working at Gainsight

OWASP Member

Google - sh377c0d3

LinkedIn (or) **Twitter** (or) **GitHub** – sh377c0d3

Disclaimer !!!

- The entire talk is more at personal level and doesn’t contain or relate to any of my former or current professional association
- Most of the content is solely gathered from personal research as well as publicly available resource that include as well as content

Agenda

Introduction

Approach

Tools and Vulnerabilities

Hunt or Exploit vulnerabilities?

Summary

References

Q & A

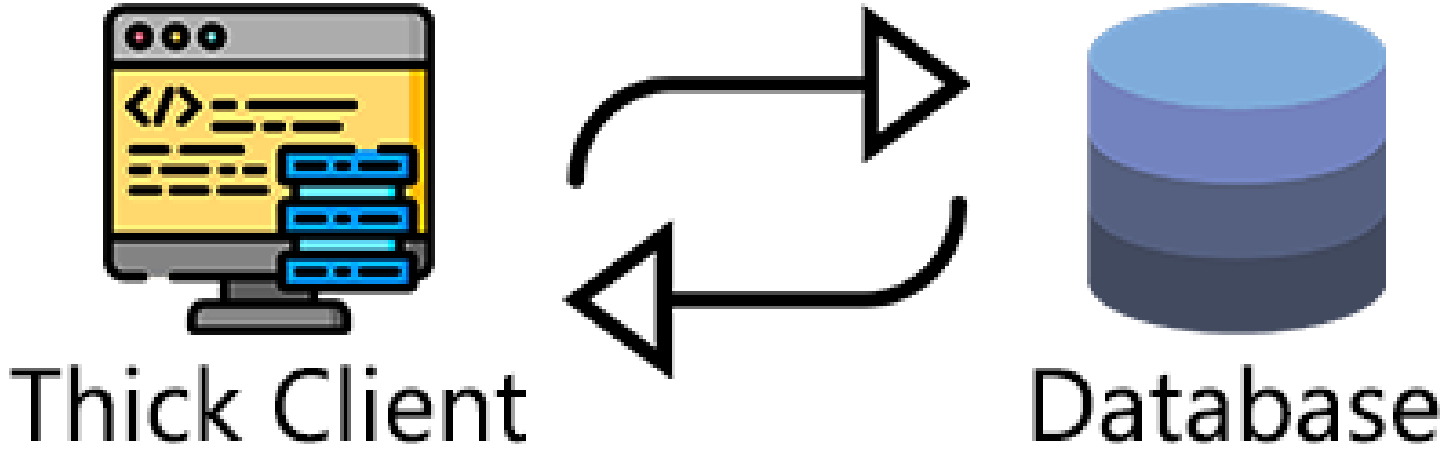
Introduction

Thick client pentesting ?!

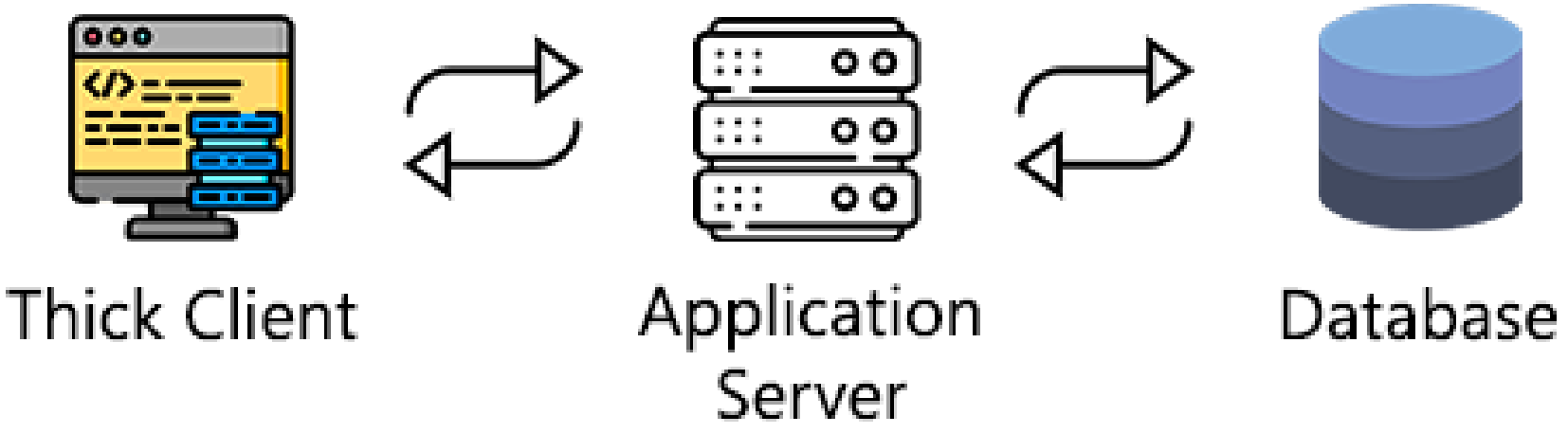
- Both local and server-side processing
- Often uses proprietary protocols for communication.
- Language:- .Net , Java , C/C++ , Microsoft Silverlight.

Types of Thick client application

Two-Tier architecture



Three-Tier architecture



Approach - 1

1. Scanning and Enumeration
2. Reverse Engineering
3. Dynamic Analysis
4. CVE and exploits
5. Reporting

Approach – 2

1

Information Gathering

- **Application Architecture**
- Platform Mapping
- Language and Frameworks

2

Client-Side attacks

- **Files Analysis**
- Binary Analysis
- Memory Analysis
- Dynamic Analysis

3

Network Side Attacks

- Installation Traffic
- Run Time Traffic

4

Server-Side Attacks

- Network Layer Attacks
- Layer 7 Attacks

Common Vulnerabilities

SQL Injection	Weak Password Policy
Command Injection	Application Internal Path Disclosure
Cleartext Storage of Connection Strings	Weak Cryptography
Outdated Web Server	Hardcoded information
Server-side Input Data Validation Missing	Dumping connection string
Logging of Sensitive Data	DLL Hijacking / Injection
Insecure Authentication / Authorization	Privilege Escalation
Password Storage in Recoverable Format	Side channel Attack
Improper Security Flags implementation	Registry edit
Unsigned Code	Man In-The Middle
Insufficient Memory Protection	Denial of Service (DoS)

“

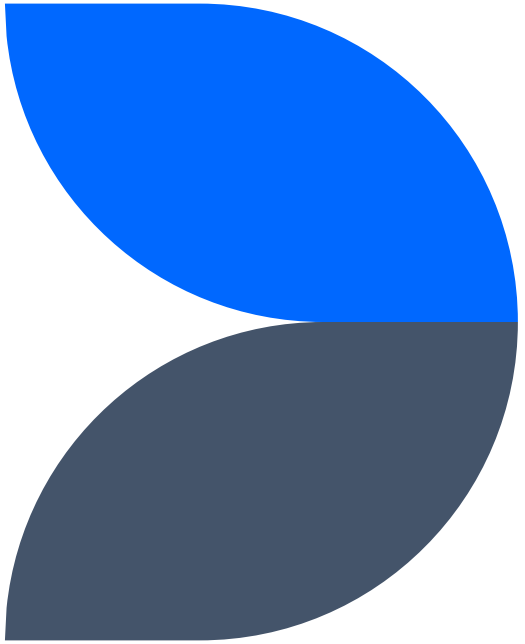
CVE and Exploit are like buses. There's always another one coming.

”

Tools

Echo Mirage	Wireshark
Burp Suite	Ghidra
IDA	regshot
Process Monitor	Process Hacker
MITM Relay	dnspy
OWASP ZAP	Procmon
Immunity debugger	xdbg
binscope	sigcheck
CFF Explorer	Robber
Jadx / jd-gui	Fiddler Classic
TCPViewer (Sysinternal suite)	Open-source tools (github)

Hunt or Exploit vulnerabilities ?



Summary

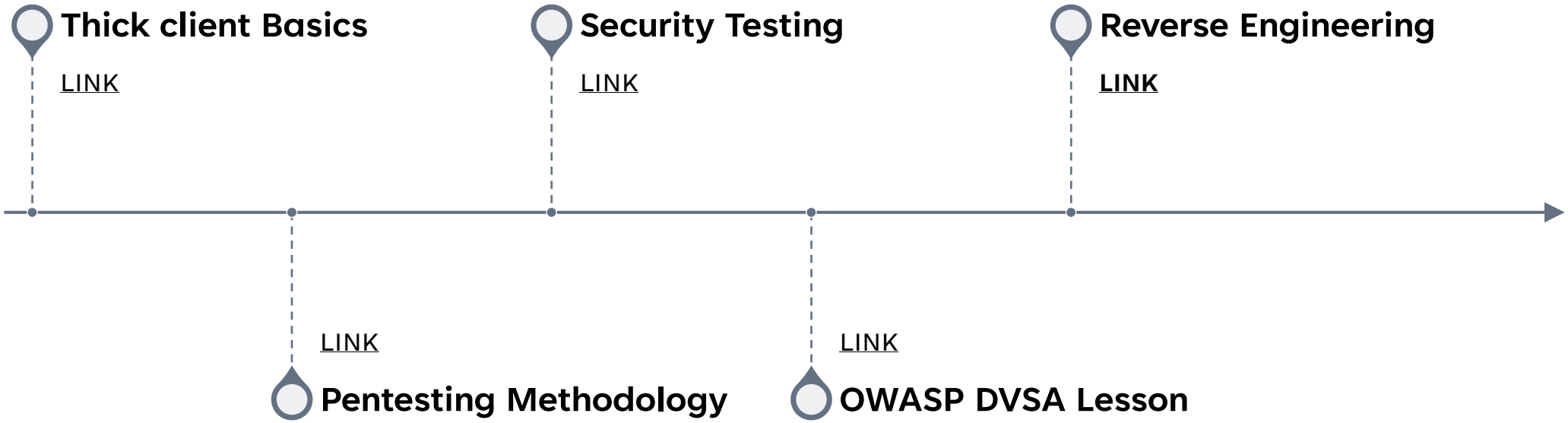
Scanning is not sufficient

Requires a lot of patience and a methodical approach.

Significant attack surface.

Language:- .Net , Java , C/C++ , Microsoft Silverlight

References


Thick client Basics
LINK
Security Testing
LINK
Reverse Engineering
LINK
LINK
Pentesting Methodology
LINK
OWASP DVSA Lesson

Thank you