root nik labs

Rootnik Thick Client Pentesting

R | TCPT

- Dedicated Virtual Lab
- 100% Practical Training
- Internship opportunities

contact us at :

info@rootniklabs.com

+91 87773 21145

www.rootniklabs.com

Introduction

In this course, you will learn the basics of Thick Client Pentesting. You will learn how a hacker exploits different kinds of Thick client applications on a local and network level, You will learn how to analyze the internal communication between web services & API. This course will teach you the basics approach to monitoring, reverse engineering, and exploiting different tiers of thick client applications. After completion of this course, you will acquire the skill set for complex Thick Client testing techniques. This course also guides you to start with Exploit writing, Publish CVEs, etc.

Program Details

R | TCPT

Rootnik Thick Client Pentesting

Duration	Category	Difficulty
30 hours	Pentesting	Expert

Program Content

Module 1 : Architectures of Thick Client applications:

- Introduction to Thick Client Application
- Thick Client Application Architecture
- Security Assessment of Thick Client Applications

Module 2 : Lab Setup:

- Security Testing Approach
- Pentesting Tools Installation
- Live Application Installation

Module 3 : Maintain Anonymity:

- Use of insecure encryption and hashing algorithms
- Testing for Database and server misconfigurations
- Network Communication Between the Client and the Server
- Application Architecture & Identifying the Languages & Frameworks
- Identifying Interesting Files Bundled with the Thick Client Application
- Application service, provider, WMI subscription, task, and other permissions

Module 4 : Security Assessment of Thick Client Applications -Client Side:

- Client-Side attacks - Files Analysis
- Client-Side attacks - Binary Analysis
- Client-Side attacks - Memory Analysis
- Identifying DLL Hijacking Vulnerability
- Hardcoded encryption material (keys, IVs, etc.)
- Hardcoded sensitive data and authentication tokens
- Client-Side attacks - Weak Graphical User Interface

Module 5 : Security Assessment of Thick Client Applications - Server Side:

- Web Services pentesting utilised by the application
- Testing Application workflow logic between GUI elements
- Testing Authentication and authorization controls Modules
- Testing for Use of insecure encryption and hashing algorithms
- Testing Application objects & information stored in memory during runtime
- Testing Network protocols utilised by the application (SMB, FTP, TFTP, etc.)

Module 6 : Penetration Testing Standards:

- Web Application Security Consortium (WASC)
- Open Web Application Security Project (OWASP)
- System Administration, Networking, and Security (SANS)
- Open Source Security Testing Methodology Manual (OSSTMM)

Module 7 : Penetration Testing Reporting:

- Collect Penetration Testing Scan Results
- Open Source reporting framework

Examination Scheme

Paper	Total Marks
Theoritical	100
Practical	100

Theoritical	Total Marks
Assignment 1	10
Assignment 2	10
Project	15
Attendance	5
Theory paper	60
Total	100

Practical	Total Marks
Lab	100

Pass Criterion: Students have to obtain at least 50% marks (pass marks) in both Theoretical and Practical papers separately at the end of the course.

RootNik Courses

- R-NF - ROOTNIK NETWORK FUNDAMENTALS
- R-CNA - ROOTNIK CERTIFIED NETWORK ASSOCIATE
- R-LF - ROOTNIK LINUX FUNDAMENTALS
- R-CPP - ROOTNIK CERTIFIED PYTHON PROGRAMMER
- R-CEH - ROOTNIK CERTIFIED ETHICAL HACKER
- R-CTFG - ROOTNIK CAPTURE THE FLAG GURU
- R-STWP - ROOTNIK SECURITY TOOLS WITH PYTHON
- R-JSS - ROOTNIK JAVA SCRIPTING
- R-BS - ROOTNIK BASH SCRIPTING
- R-APT - ROOTNIK ANDROID PENTESTING
- R-IPT - ROOTNIK IOS PENTESTING
- R-WAPT - ROOTNIK WEB APPLICATION PENTESTING
- R-WAPTA - ROOTNIK WEB APPLICATION PENTESTING ADVANCE
- R-NPT - ROOTNIK NETWORK PENTESTING
- R-NPTA - ROOTNIK NETWORK PENTESTING ADVANCE
- R-TCPT - ROOTNIK THICK CLIENT PENTESTING
- R-LAPT - ROOTNIK LINUX APPLICATION PENTESTING
- R-CDFE - ROOTNIK CERTIFIED DIGITAL FORENSICS EXPERT
- R-CSP - ROOTNIK CERTIFIED SECURITY PROFESSIONAL
- R-RTE - ROOTNIK RED TEAM EXPERT
- R-ADPT - ROOTNIK ACTIVE DIRECTORY PENTESTING

About RootNikLabs

“Our professionals have years of experience in securing critical assets of corporate clients.”

At **RootNik Labs**, everything we do is inspired by our vision, mission, and our core values.

Vision:

The vision that guides RootNik Labs has been carefully crafted by our leadership team as follows:

“Data security is a necessity not a luxury and making it affordable is our top priority”

Mission:

Provide a resilient, goal-enabling, and assuring operating cyber-environment to each and every one of our unique and highly valued clients by consistently striving to identify, design, and intervene in delivering customised cybersecurity, digital forensics, and privacy-enhancing services and solutions that meet their needs.

info@rootniklabs.com

+91 87773 21145

www.rootniklabs.com

ROOTNIK THICK CLIENT PENTESTING