Techonquer Certified VAPT Expert (TCVE)

Become a Certified VAPT Expert with 100% practical, hands-on training across Web, Mobile, Active Directory, Network and API security. Lab-focused, challenge-based, and industry-aligned curriculum designed for real-world cybersecurity professionals.

Course Overview

100% Practical Training

Hands-on labs across all security domains with real-world scenarios and vulnerable applications.

Multi-Domain Expertise

Web, Mobile, Active Directory, Network, and API security testing methodologies.

Industry Certification

Challenge-based progression with CTF-style practical exam for TCVE credential.

Module 1: Introduction to VAPT & Lab Setup

VAPT Fundamentals

- VAPT purpose and ethics
- Legal authorization steps
- Professional standards

Lab Environment

- Kali Linux and Parrot OS setup
- VM networking configuration
- Vulnerable targets deployment

Essential tools covered: Burp Suite, Metasploit, Nmap, Wireshark, BloodHound, ApkTool, and Jadx. Students build a complete penetration testing laboratory with OWASP Juice Shop, vulnerable Android/iOS apps, and Active Directory lab environment.

Module 2: Cybersecurity Basics

Threat Modeling

Risk assessment concepts, CVSS scoring methodology, and threat landscape analysis for comprehensive security evaluation.

Standards & Frameworks

OWASP guidelines, MITRE ATT&CK framework, and industry best practices for structured security assessments.

VA vs PT Methodology

Understanding differences between vulnerability assessment and penetration testing, and when to apply each approach.

Module 3: Web Application Security

Reconnaissance & Discovery

01

Subdomain Enumeration

Using Amass and Subfinder for comprehensive domain discovery and attack surface mapping.

02

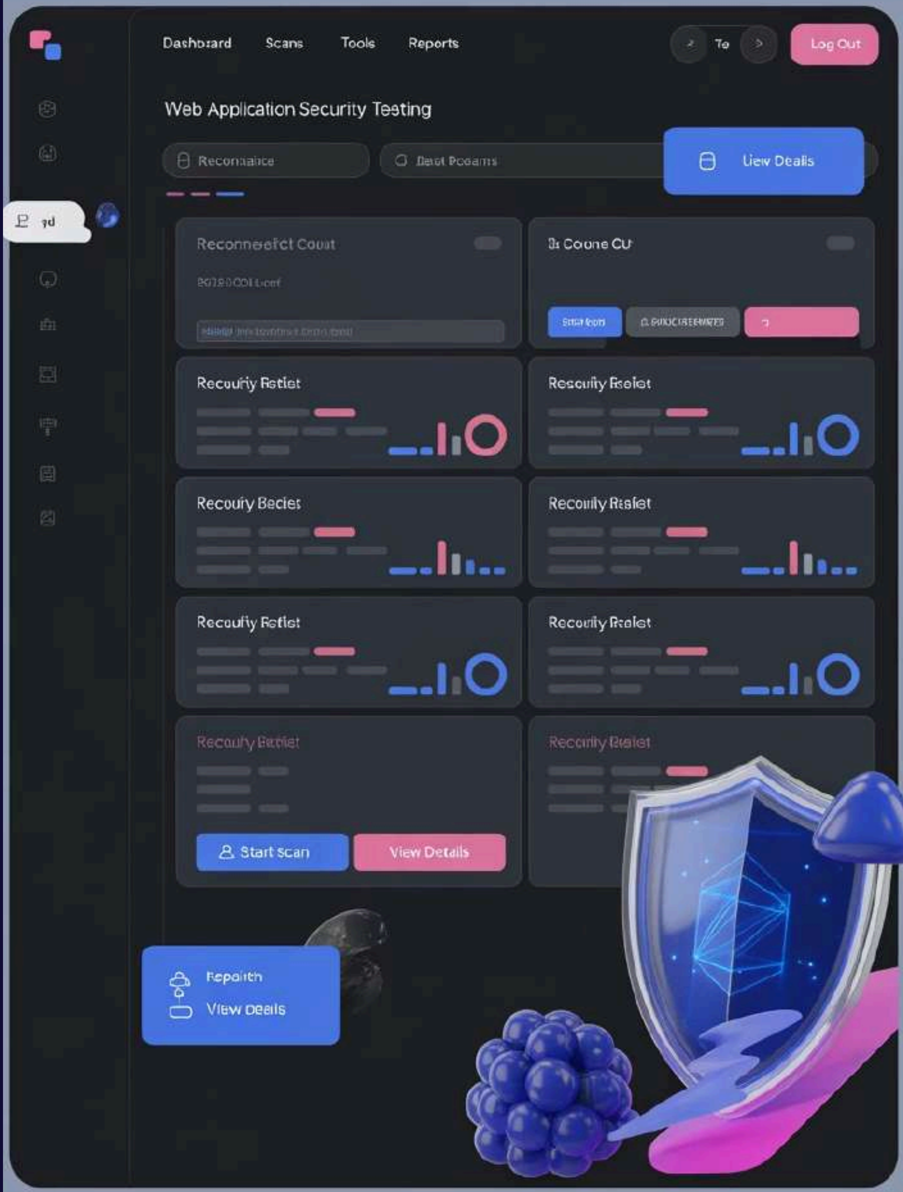
Technology Identification

WhatWeb and Wappalyzer for stack identification and technology fingerprinting.

03

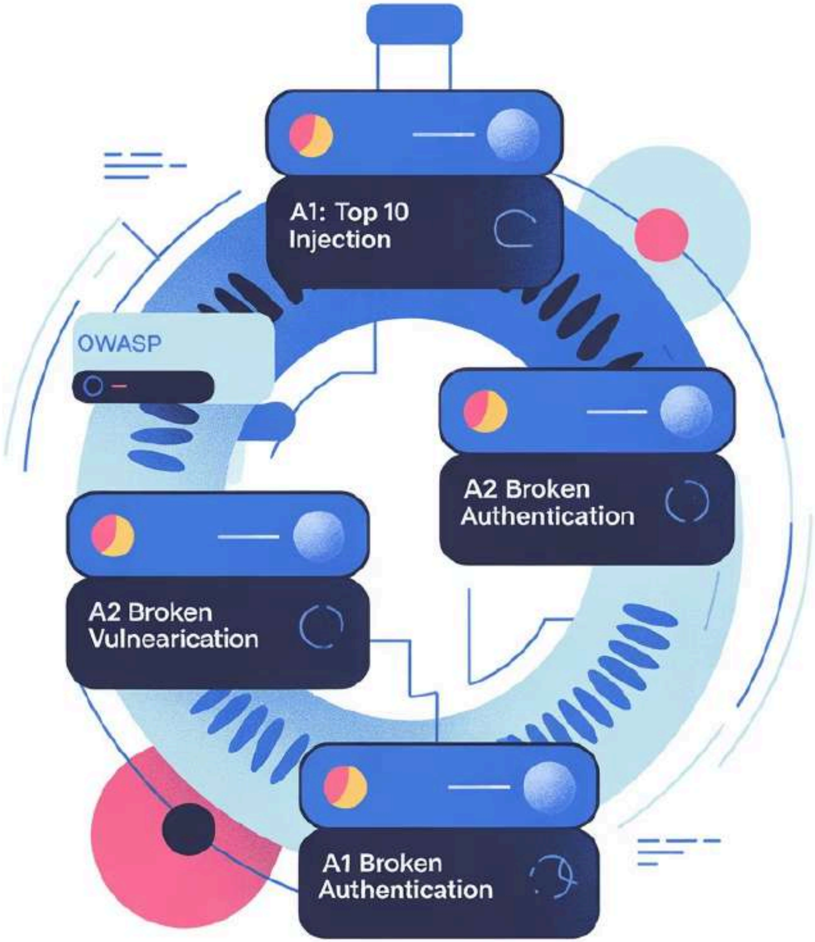
Reconnaissance Techniques

Passive and active information gathering methodologies for target profiling.



OWASP Top 10

Comprehensive hands-on training covering all OWASP Top 10 web application security risks with theory and practical exploitation labs. Each vulnerability is explored through real-world scenarios and chained attack demonstrations.



OWASP Top 10 Deep Dive

Broken Access Control

Privilege escalation and unauthorized access exploitation techniques.

Cryptographic Failures

Weak encryption, improper key management, and data exposure vulnerabilities.

Injection Attacks

SQL, NoSQL, and Command Injection with automated and manual exploitation.

Insecure Design

Business logic flaws and architectural security weaknesses.

Security Misconfiguration

Default configurations, unnecessary features, and improper security settings.

Advanced Web Exploitation

Core Techniques

- SQL Injection (classic & blind)
- Cross-Site Scripting variants
- Authentication bypasses
- Session hijacking and JWT attacks

Modern Attacks

- WebSocket exploitation
- API parameter fuzzing
- Business logic abuse
- Chained exploit development

Students learn to combine multiple vulnerabilities into exploit chains, demonstrating how OWASP issues interact in real applications. Advanced post-exploitation techniques include pivoting from web applications to internal networks.

Module 4: Mobile Security Testing

Mobile Architecture & Analysis

Platform Fundamentals

Android/iOS architecture, app components, permissions model, and app signing processes.

Static Analysis

Reverse engineering with ApkTool, Jadx, class analysis, and manifest review techniques.

Dynamic Testing

Runtime analysis using Frida, Objection, and Burp Suite with mobile proxies.

Mobile Attack Techniques

Hardcoded Secrets

API key discovery and credential extraction from mobile applications.

Insecure Data Storage

SharedPreferences, Keychain, and SQLite database security analysis.

Communication Flaws

SSL/TLS misconfigurations and certificate pinning bypass techniques.

Root Detection Bypass

Jailbreak detection circumvention and WebView vulnerability exploitation.

Practical lab exercises include exploiting Android applications to extract authentication tokens, bypass SSL pinning using Frida scripts, and abuse insecure storage mechanisms.

Module 5: Active Directory Security

AD Fundamentals & Attack Techniques

Comprehensive Active Directory security assessment covering domain concepts, trust relationships, Kerberos authentication, LDAP protocols, and Group Policy Objects. Students master enumeration techniques using BloodHound, ldapsearch, and rpcclient.

Kerberoasting

Service account credential extraction and offline cracking techniques.

Pass-the-Hash

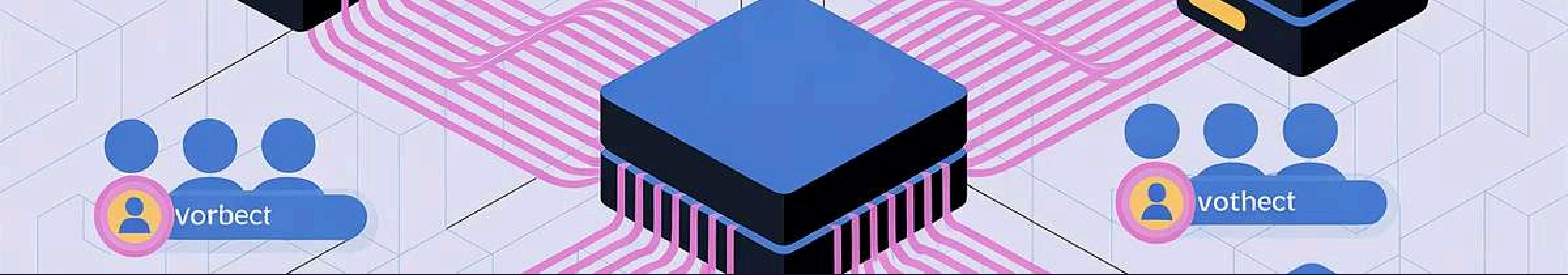
Credential reuse attacks and Pass-the-Ticket exploitation methods.

Lateral Movement

SMB, RDP, WinRM exploitation and ACL abuse using BloodHound insights.

Golden Ticket

Domain persistence through Kerberos ticket generation and DCSync abuse.



Advanced AD Attack Scenarios

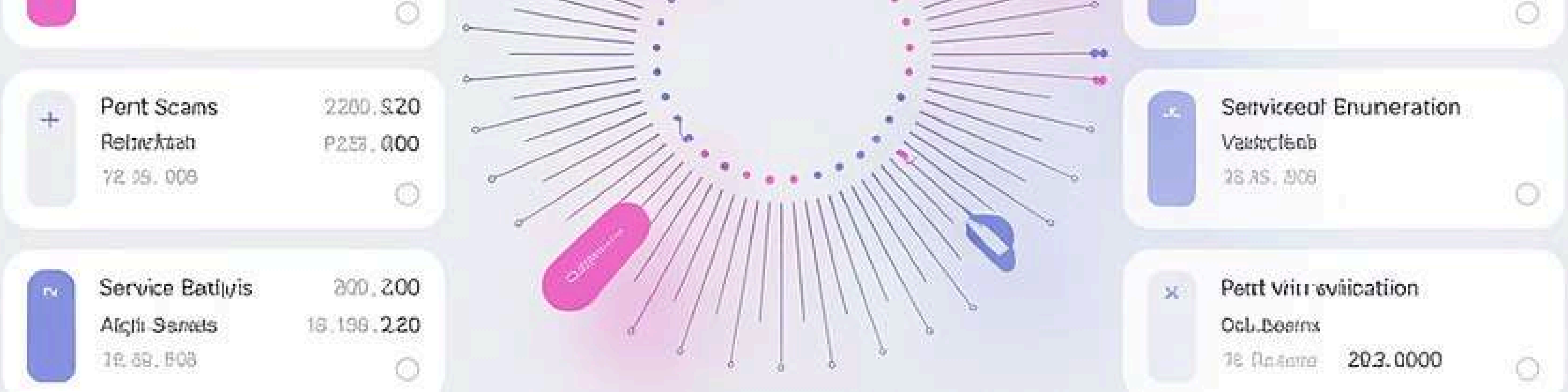
Attack Techniques

- Silver Ticket generation and abuse
- Unconstrained delegation exploitation
- NTDS.dit extraction via DCSync
- ACL abuse for privilege escalation
- AD misconfiguration identification

Students learn to chain multiple AD attacks for complete domain compromise, using BloodHound for attack path visualization and lateral movement planning.

Defense Considerations

Understanding AD security hardening, monitoring strategies, and prioritized remediation approaches for enterprise environments.



Module 6: Network Security & Infrastructure

Scanning & Enumeration

Nmap, Masscan service fingerprinting, network mapping, and comprehensive asset discovery techniques.

Traffic Analysis

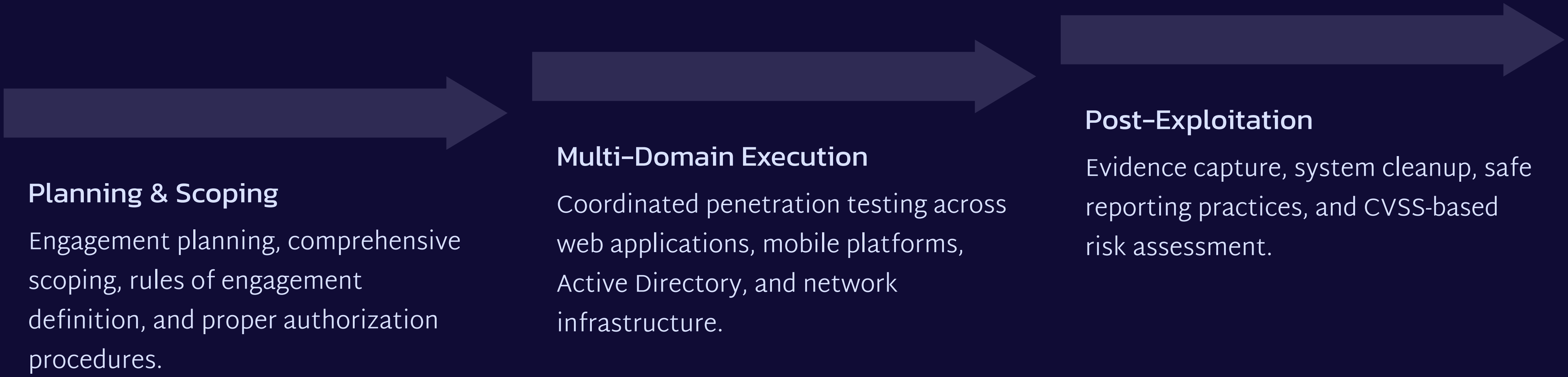
MITM attacks, ARP spoofing, DNS poisoning, SSL stripping, and Wireshark packet analysis in controlled lab environments.

Service Exploitation

SMB, RDP, FTP, SSH misconfiguration exploitation, firewall bypass, and network pivoting methods.

Module 7: Real-World Pentesting

End-to-End Engagement Lifecycle



Planning & Scoping

Engagement planning, comprehensive scoping, rules of engagement definition, and proper authorization procedures.

Multi-Domain Execution

Coordinated penetration testing across web applications, mobile platforms, Active Directory, and network infrastructure.

Post-Exploitation

Evidence capture, system cleanup, safe reporting practices, and CVSS-based risk assessment.

Module 8: Professional Reporting

Report Components

- Executive summary for stakeholders
- Technical findings documentation
- Remediation steps and priorities
- Risk assessment using CVSS

Professional Standards

Industry-standard report templates, clear communication of technical findings to business stakeholders, and actionable remediation guidance.

Students learn to create comprehensive penetration testing reports that effectively communicate security risks and provide prioritized remediation strategies for organizational decision-making.

Certification Exam Structure

Web Security

OWASP Top 10 exploitation and advanced web application attack techniques.

Mobile Exploitation

Android/iOS security testing, reverse engineering, and runtime manipulation.

AD Attack Scenarios

Domain compromise techniques, lateral movement, and privilege escalation.

Network Exploitation

Infrastructure assessment, service exploitation, and traffic analysis.

Practical exam format with hands-on challenges across all security domains. CTF-style assessment requiring demonstration of real-world penetration testing skills.

Laboratory Environment

100% Practical Training Platform

Web Application Labs

OWASP Juice Shop, DVWA, and custom vulnerable applications for comprehensive web security testing.

Mobile Testing Environment

Vulnerable Android and iOS applications with realistic security flaws for hands-on mobile exploitation.

Enterprise Infrastructure

Windows AD lab with realistic domain configurations and internal network targets for enterprise security assessment.

Learning Methodology

Instructor-Led Labs

Expert guidance through complex security scenarios with real-time problem-solving support.

Challenge-Based Progression

Beginner to advanced skill development through structured, escalating difficulty challenges.

CTF-Style Examination

Comprehensive practical exam simulating real-world penetration testing engagements.

Practical Assessments

Module-based evaluations ensuring mastery before progression to advanced topics.

Learning Outcomes

Professional VAPT Capabilities

Full Engagement Planning

Plan and execute comprehensive VAPT engagements across multiple security domains with proper authorization and methodology.

OWASP Top 10 Mastery

Identify, exploit, and remediate all OWASP Top 10 vulnerabilities using both automated tools and manual techniques.

Mobile Exploit Chains

Perform comprehensive mobile security assessments including reverse engineering, runtime manipulation, and exploit chaining.

AD Attack Execution

Execute advanced Active Directory attack techniques for domain compromise and lateral movement in enterprise environments.

Professional Reporting

Produce remediation-focused reports with executive summaries, technical findings, and prioritized risk assessments.

TCVE

Techonquer Certified VAPT Expert

Upon successful completion of the comprehensive practical examination, students receive the TCVE credential, demonstrating mastery of modern penetration testing methodologies across web, mobile, Active Directory, and network security domains.

100%

Practical Training

Hands-on laboratory experience

8

Core Modules

Comprehensive curriculum coverage

4

Security Domains

Multi-domain expertise validation