TCVE VAPT & AI Security Program

Techonquer Certified VAPT Expert syllabus covering VAPT, Web and API Security, AI Security, Active Directory, Network Pentesting, Red Team Operations and Bug Bounty Methodology.

Program Duration	3 Months
Class Schedule	Friday / Saturday / Sunday
Session Duration	1.5 Hours
Certification	TCVE - Techonquer Certified VAPT Expert
Delivery	Live, Instructor-Led Training

Module 01 - VAPT Foundations

Module coverage for VAPT Foundations, preserving the complete topic list from the supplied program source.

Topic Coverage

- Purpose of Penetration Testing and Legal Authorization
- Difference Between Automated Scanning and Manual Exploitation
- Legal Scope Definition and Engagement Boundaries
- Rules of Engagement (RoE)
- Attack Surface Identification
- Lab Engineering: Kali Linux, Web Attack Sandbox, Enterprise Lab Setup

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 01 - VAPT Foundations.

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 01.

Module 02 - Penetration Testing Methodology

Module coverage for Penetration Testing Methodology, preserving the complete topic list from the supplied program source.

Topic Coverage

- Reconnaissance Passive and Active Information Gathering
- Enumeration Service and Host Discovery
- Exploitation Leveraging Vulnerabilities
- Privilege Escalation Vertical and Horizontal
- Persistence Maintaining Access After Exploitation
- Lateral Movement Moving Within Networks
- Risk Prioritization Using CVSS and Threat Modeling

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 02 - Penetration Testing Methodology.

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 02.

Module 03 - Web Application Security Part 1 (OWASP & Injection)

Module coverage for Web Application Security Part 1 (OWASP & Injection), preserving the complete topic list from the supplied program source.

Topic Coverage

- OWASP Top 10 Deep Dive Injection, Broken Auth, Security Misconfiguration
- SQL Injection: Union, Blind, Error-Based, Time-Based
- Command Injection and OS Command Chaining
- LDAP, XML, XPath Injection Techniques
- Server-Side Template Injection (SSTI)
- SQLMap Usage and Manual Bypass Techniques

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 03 - Web Application Security Part 1 (OWASP & Injection).

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 03.

Module 04 - Web Application Security Part 2 (XSS, Auth & Sessions)

Module coverage for Web Application Security Part 2 (XSS, Auth & Sessions), preserving the complete topic list from the supplied program source.

Topic Coverage

- Reflected, Stored, and DOM-Based XSS Exploitation
- CSRF - Cross-Site Request Forgery Attack and Bypass
- Authentication Bypass Techniques
- Session Hijacking and Cookie Manipulation
- JWT Attacks: Algorithm Confusion, None Algorithm, Secret Brute Force
- OAuth 2.0 Vulnerabilities and Token Theft

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 04 - Web Application Security Part 2 (XSS, Auth & Sessions).

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 04.

Module 05 - Web Application Security -Part 3 (Advanced & API)

Module coverage for Web Application Security -Part 3 (Advanced & API), preserving the complete topic list from the supplied program source.

Topic Coverage

- IDOR - Insecure Direct Object Reference and Mass Assignment
- SSRF - Server-Side Request Forgery and Cloud Metadata Exploitation
- API Security Testing: REST, GraphQL, SOAP
- Business Logic Abuse and Chained Vulnerability Exploitation

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 05 - Web Application Security -Part 3 (Advanced & API).

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 05.

Module 06 - AI Security Fundamentals & LLM Attack Surface

Module coverage for AI Security Fundamentals & LLM Attack Surface, preserving the complete topic list from the supplied program source.

Topic Coverage

- Introduction to AI/LLM Security and OWASP LLM Top 10
- AI Model Mapping and Prompt Surface Enumeration
- Understanding LLM Architecture: Tokens, Context Windows, System Prompts
- Data Leakage, Insecure Output Handling and Training Data Exposure
- Vector Database Attacks and Embedding Poisoning
- LLM Security Testing Tools Proxies, Extensions, Observability Platforms

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 06 - AI Security Fundamentals & LLM Attack Surface.

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 06.

Module 07 - Prompt Injection & Jailbreaking Techniques

Module coverage for Prompt Injection & Jailbreaking Techniques, preserving the complete topic list from the supplied program source.

Topic Coverage

- Direct vs Indirect Prompt Injection Attacks
- Jailbreaking LLMs DAN, Role-Play, and Instruction Override Techniques
- Bypassing Content Filters, Safety Guardrails and Rate Limiting
- System Prompt Extraction and Leakage
- Automated Scanning for Prompt Injection and Output Abuse
- Real-World Prompt Injection CVEs and Case Studies

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 07 - Prompt Injection & Jailbreaking Techniques.

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 07.

Module 08 - AI Agent Security, Tool Abuse & API Exploitation

Module coverage for AI Agent Security, Tool Abuse & API Exploitation, preserving the complete topic list from the supplied program source.

Topic Coverage

- AI Agent Architecture Understanding Tool Calls, Plugins and Chained Actions
- Agent Tool Misuse and Function Call Injection
- Pivoting from AI Applications to Internal Systems
- Access Restrictions Bypass and Privilege Escalation via Agents
- AI API Security Testing Authentication, Rate Limits, Model Abuse
- Business Logic Abuse in AI-Powered Applications

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 08 - AI Agent Security, Tool Abuse & API Exploitation.

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 08.

Module 09 - AI Red Team Methodology & Reporting

Module coverage for AI Red Team Methodology & Reporting, preserving the complete topic list from the supplied program source.

Topic Coverage

- AI Red Team Planning Objectives, Scope and Rules of Engagement
- Full AI Attack Chain: Recon to Injection to Exploitation to Exfil
- Multi-Turn Attack Scenarios and Persistence in LLM Sessions
- Real-World LLM Hacking Workflow and Hall of Fame Writeups
- Writing Professional AI Security VAPT Reports
- Responsible Disclosure for AI Vulnerabilities

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 09 - AI Red Team Methodology & Reporting.

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 09.

Module 10 - Active Directory Exploitation Part 1 (Enumeration & Credential Attacks)

Module coverage for Active Directory Exploitation Part 1 (Enumeration & Credential Attacks), preserving the complete topic list from the supplied program source.

Topic Coverage

- AD Enumeration with BloodHound, PowerView, and ldapdomaindump
- Kerberos Authentication Deep Dive and Attack Surface
- AS-REP Roasting and Kerberoasting Extraction and Cracking
- Pass-the-Hash and Pass-the-Ticket Attacks
- Credential Dumping with Mimikatz and Impacket
- LLMNR/NBT-NS Poisoning and Responder Attacks

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 10 - Active Directory Exploitation Part 1 (Enumeration & Credential Attacks).

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 10.

Module 11 - Active Directory Exploitation & Red Team Operations (Domain Compromise)

Module coverage for Active Directory Exploitation & Red Team Operations (Domain Compromise), preserving the complete topic list from the supplied program source.

Topic Coverage

- Golden Ticket and Silver Ticket Attacks
- DCSync Attack Replicating Domain Credentials
- Domain Trust Exploitation and Cross-Forest Attacks
- ACL/ACE Abuse: WriteDACL, GenericAll, ForceChangePassword
- Constrained and Unconstrained Delegation Exploitation
- Complete Domain Compromise and Persistence Techniques
- Red Team Planning: Objectives, TTPs, and Adversary Emulation
- Command and Control (C2) Infrastructure Setup
- AV/EDR Evasion Techniques Obfuscation and AMSI Bypass
- Full Attack Chain Simulation: Phishing to Foothold to Escalation to Exfil
- Purple Team Collaboration Bridging Red and Blue

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 11 - Active Directory Exploitation & Red Team Operations (Domain Compromise).

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 11.

Module 12 - Network Infrastructure Pentesting

Module coverage for Network Infrastructure Pentesting, preserving the complete topic list from the supplied program source.

Topic Coverage

- Network Discovery and Service Fingerprinting
- SMB Exploitation

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 12 - Network Infrastructure Pentesting.

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 12.

Module 13 - Social Engineering & Phishing Simulations

Module coverage for Social Engineering & Phishing Simulations, preserving the complete topic list from the supplied program source.

Topic Coverage

- Social Engineering Fundamentals and Psychology of Deception
- Phishing Campaign Setup with GoPhish
- Spear Phishing and Whaling Techniques
- Pretexting, Vishing, and Smishing Scenarios
- Credential Harvesting via Fake Login Pages
- Measuring and Reporting Phishing Simulation Results

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 13 - Social Engineering & Phishing Simulations.

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 13.

Module 14 - Post-Exploitation & Lateral Movement

Module coverage for Post-Exploitation & Lateral Movement, preserving the complete topic list from the supplied program source.

Topic Coverage

- Post-Exploitation Framework: Metasploit, CobaltStrike Concepts
- Establishing Persistence: Registry, Scheduled Tasks, Startup Folders
- Lateral Movement via PsExec, WMI, SMB, RDP
- Data Exfiltration Techniques and Avoiding Detection
- Living off the Land (LOLBins) Abusing Built-in OS Tools
- Covering Tracks and Log Manipulation

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 14 - Post-Exploitation & Lateral Movement.

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 14.

Module 15 - Bug Bounty Hunting Methodology

Module coverage for Bug Bounty Hunting Methodology, preserving the complete topic list from the supplied program source.

Topic Coverage

- Bug Bounty Platforms: HackerOne, Bugcrowd, Intigriti
- Recon Automation: Subfinder, Amass, httpx, nuclei
- Prioritizing High-Impact Vulnerabilities for Maximum Reward
- Writing Impactful Bug Reports
- Responsible Disclosure and Legal Boundaries
- Real-World Hall of Fame Writeup Analysis

Practical Lab Direction

Hands-on exercises aligned with the topics in Module 15 - Bug Bounty Hunting Methodology.

Expected Outcome

Practical understanding of the security concepts and techniques covered in Module 15.

Assessment & Certification

Exam Format

• Live OR Remote-Proctored Exam

• MCQs and Case-Based Questions

• 60 to 90 Questions

• Minimum 85% Pass Mark Required

• Practical Lab Assessment Included

Program Highlights

• 100% Live, Instructor-Led Classes

• Lifetime Access to Session Recordings

• 1-to-1 Mentor Support Chitra Karanam

• ISO 9001:2015 Approved Program

• Hands-on labs with real-world tooling

Professional Skills Developed

1. Vulnerability Assessment and Penetration Testing
2. Web Application and API Security Testing
3. AI Security and LLM Red Teaming
4. Active Directory and Network Security
5. Social Engineering and Phishing Simulation
6. Post-Exploitation and Lateral Movement
7. Bug Bounty Methodology and Responsible Disclosure
8. Security Reporting and Professional Communication

Certification

TCVE - Techonquer Certified VAPT Expert

Ready to Start Your VAPT Career?

Enroll Today

New batch starting soon

Enroll Now - ■5,999

+91 6367098233

info@techonquer.org

techonquer.org