VAPT TRAINING

- THE NEXT GEN OF DCSC 2.0

INTRODUCTION

VAPT **(Vulnerability Assessment & Penetration Testing)** is an advanced cybersecurity process that helps identify, analyze, and validate security weaknesses in systems, networks, servers, and applications before they can be exploited by real attackers.

IT HELPS ORGANIZATIONS UNDERSTAND :

- Where their system is **vulnerable**
- How those vulnerabilities can be **exploited**
- How to **fix and secure** them effectively

VAPT plays a critical role in strengthening cybersecurity by proactively identifying security risks, validating real-world attack scenarios, and ensuring systems remain secure, resilient, and protected against evolving cyber threats.

DCSC is already an advanced-level cybersecurity program that builds strong expertise in ethical hacking, system security, and attack fundamentals. It prepares learners with in-depth technical knowledge and hands-on skills required to understand how cyber attacks work.

However, modern organizations require even deeper, more specialized expertise—professionals who can not only understand attacks but also assess enterprise environments, validate real risks, and produce professional security reports.

*THAT IS WHERE **VAPT** COMES IN.*

VAPT is a higher-level, specialization-focused program, designed to take DCSC-trained professionals into real-world Vulnerability Assessment & Penetration Testing practices used by security consultants, auditors, and enterprise security teams.

Rise of Cyberattacks

WHY DROP IS PROVIDING VAPT TRAINING?

BENEFITS OF THIS TRAINING

ADVANCED PROFESSIONAL SKILL DEVELOPMENT

This training enhances existing cybersecurity expertise by introducing enterprise-level VAPT techniques, real-world testing approaches, and professional workflows used in the industry.

REAL-WORLD VAPT EXPOSURE

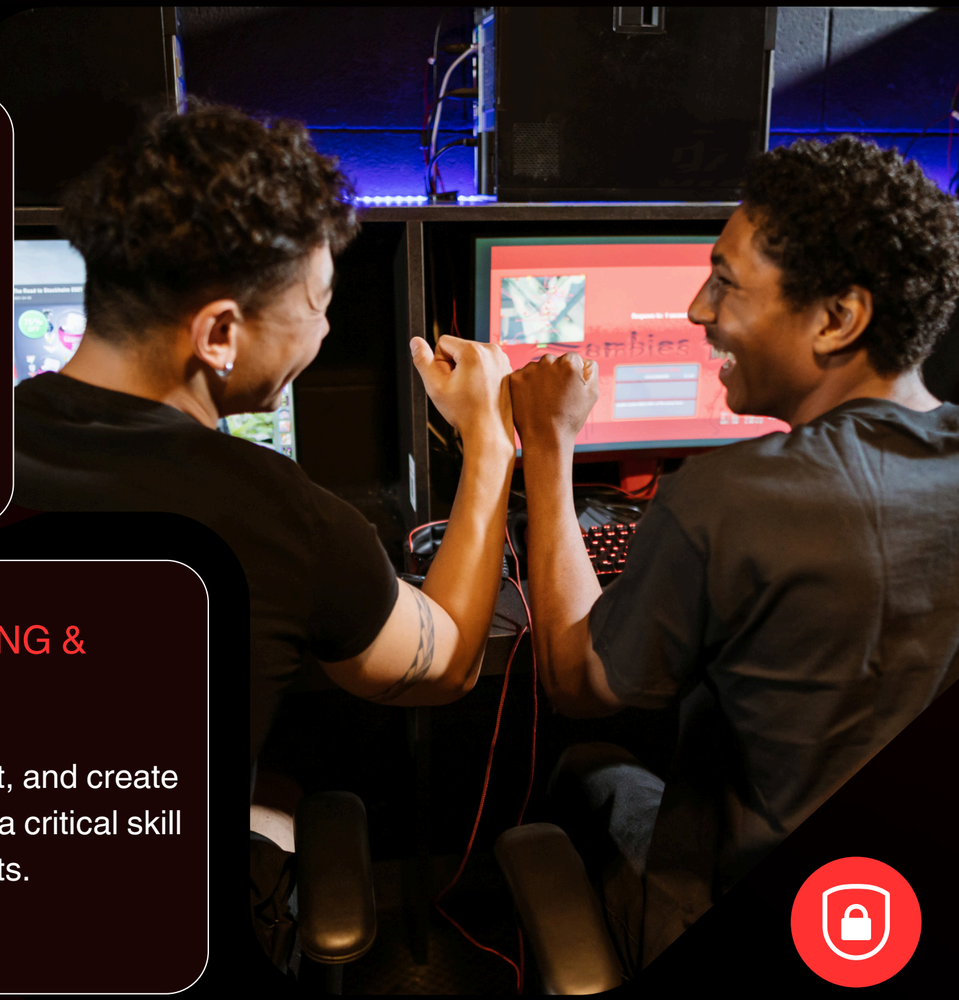
Learners gain hands-on experience with actual vulnerability assessment and penetration testing scenarios, tools, and methodologies applied in real organizational environments.

INDUSTRY-READY CAREER ADVANCEMENT

The program prepares learners for high-demand roles in penetration testing, security assessment, and cybersecurity consulting, making them job-ready for advanced positions.

PROFESSIONAL REPORTING & METHODOLOGY SKILLS

Students learn how to document vulnerabilities, assess risk impact, and create industry-standard VAPT reports, a critical skill required by enterprises and clients.



CURRICULUM OVERVIEW

This curriculum provides a structured learning path focused on advanced VAPT concepts, real-world testing methodologies, and hands-on practical exposure, ensuring industry-ready skills.

Module 1 – VAPT Fundamentals & Methodologies
Module 2 – Understanding and working on Kali Linux
Module 3 – Python and Automation in Kali
Module 4 – Information Gathering & Enumeration
Module 5 – Vulnerability Assessment Techniques
Module 6 – Network Penetration Testing
Module 7 – Web Application VAPT (Level 1)
Module 8 – Web Application VAPT (Level 2)

MODULE 1 – VAPT FUNDAMENTALS & METHODOLOGIES

- 1.1 Understanding Vulnerability Assessment vs Penetration Testing
- 1.2 VAPT Engagement Lifecycle Overview
- 1.3 Scope Definition, Rules of Engagement & Permissions
- 1.4 Core Standards Used in VAPT (OWASP, PTES, NIST)
- 1.5 Understanding Severity Levels & Risk Ratings (CVSS Overview)
- 1.6 Creating a VAPT Workflow & Testing Checklist

MODULE 2 – UNDERSTANDING AND WORKING ON KALI LINUX

- 2.1 Introduction to Kali Linux
- 2.2 Essential Linux Commands for Pentesting
- 2.3 User & Permission Management for VAPT
- 2.4 Package & Tool Management in Kali
- 2.5 Bash Scripting for VAPT Workflows
- 2.6 Networking & Services in Kali
- 2.7 Working with Logs

MODULE 3 – PYTHON AND AUTOMATION IN KALI

- **3.1** Python Essentials for Pentesters
- **3.2** Python Networking Foundations
- **3.3** Working with Files & OS
- **3.4** Python for Automation in VAPT
- **3.5** Introduction to Exploit Development Concepts (Beginner-Level)
- **3.6** Building Small Pentesting Utilities

MODULE 4 – INFORMATION GATHERING & ENUMERATION

- **4.1** Network Discovery & Asset Identification
- **4.2** **Service and Port Enumeration**
- **4.3** DNS, Subdomain & Infrastructure Enumeration
- **4.4** Banner Grabbing and Service Fingerprinting
- **4.5** Identifying Technology Stack & Software Versions
- **4.6** Building an Attack Surface Overview

MODULE 5 – VULNERABILITY ASSESSMENT TECHNIQUES

- **5.1** Using Automated Scanners for Initial Assessment
- **5.2** Identifying Misconfigurations & Weak Services
- **5.3** Version-Based Vulnerability Detection
- **5.4** Manual Verification of Scanner Output
- **5.5** Validating Findings and Removing False Positives
- **5.6** Prioritizing Vulnerabilities Based on Impact

MODULE 6 – NETWORK PENETRATION TESTING

- **6.1** Identifying Weak Network Services
- **6.2** Password Attacks on Common Services (SSH, FTP, SMB)
- **6.3** Basic Exploitation of Network-Level Vulnerabilities
- **6.4** Intro to Metasploit for Network Exploits
- **6.5** Simple Privilege Escalation Concepts
- **6.6** Documentation of Exploits & Results

MODULE 7 – WEB APPLICATION VAPT (LEVEL 1)

- **7.1** Mapping Web Application Structure
- **7.2** Input-Based Vulnerabilities
- **7.3** File Upload Issues & Directory Traversal
- **7.4** Authentication & Session Weakness Basics
- **7.5** Testing for Broken Access Controls
- **7.6** Using Burp Suite for Manual Testing (Core Features)

MODULE 8 – WEB APPLICATION VAPT (LEVEL 2)

- **8.1** Directory Enumeration & Hidden File Discovery
- **8.2** Testing for Sensitive Data Exposure
- **8.3** CSRF & Logic-Based Vulnerabilities
- **8.4** API Testing Basics (Endpoints & Common Weaknesses)
- **8.5** Weak Configurations & Default Settings in Web Stacks
- **8.6** Simple Manual Exploitation for Confirmed Vulnerabilities

TDO
The Drop Organization

TOOLS WE USE

CVSS

Nessus vulnerability scanner

Obsidian

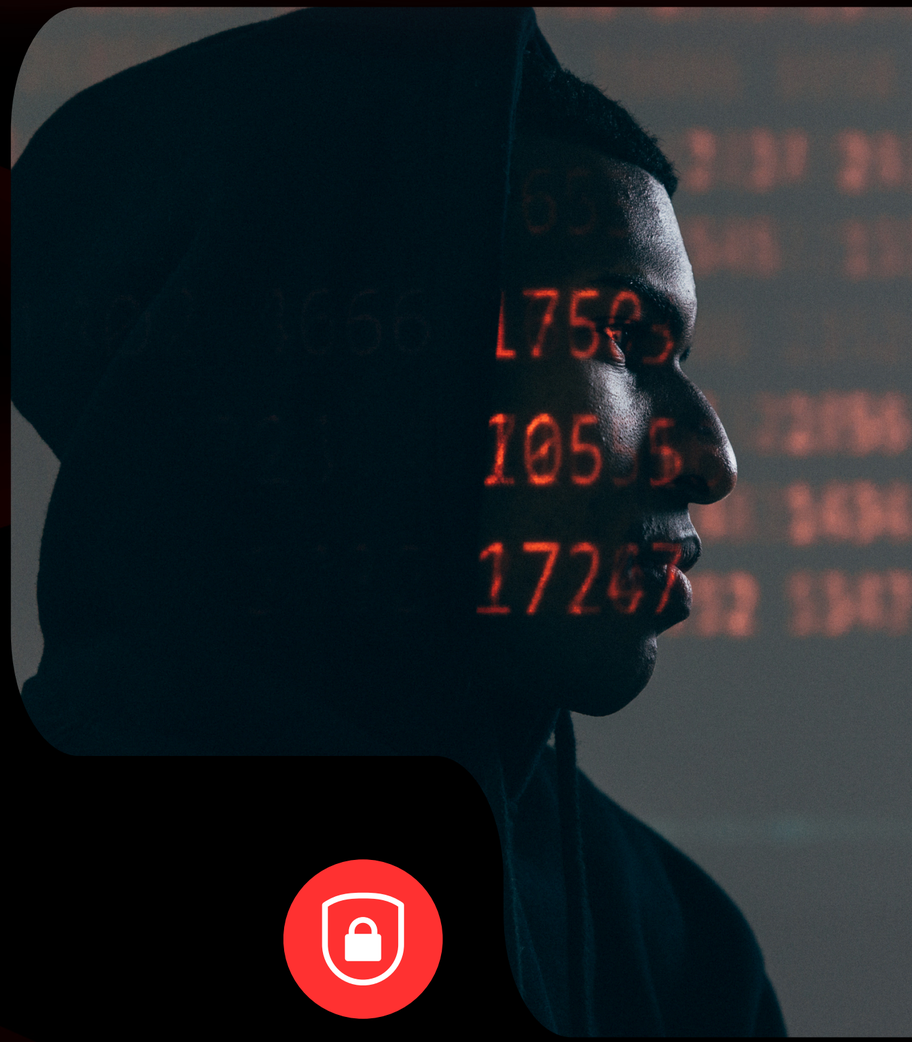
PortSwigger

NMAP.ORG

python™

Wappalyzer

MALTEGO



SKILL COVERED

This training builds advanced VAPT skills, including vulnerability assessment, penetration testing, automation, and professional security testing for real-world environments.

- VULNERABILITY ASSESSMENT EXPERTISE
- PROFESSIONAL PENETRATION TESTING SKILLS
- LINUX & KALI LINUX MASTERY
- INFORMATION GATHERING & ENUMERATION SKILLS
- NETWORK PENETRATION TESTING SKILLS
- WEB APPLICATION SECURITY TESTING
- PYTHON & AUTOMATION SKILLS FOR VAPT
- RISK ANALYSIS & SEVERITY ASSESSMENT
- SECURITY STANDARDS & METHODOLOGIES
- PROFESSIONAL DOCUMENTATION & REPORTING

TDO
The Drop Organization

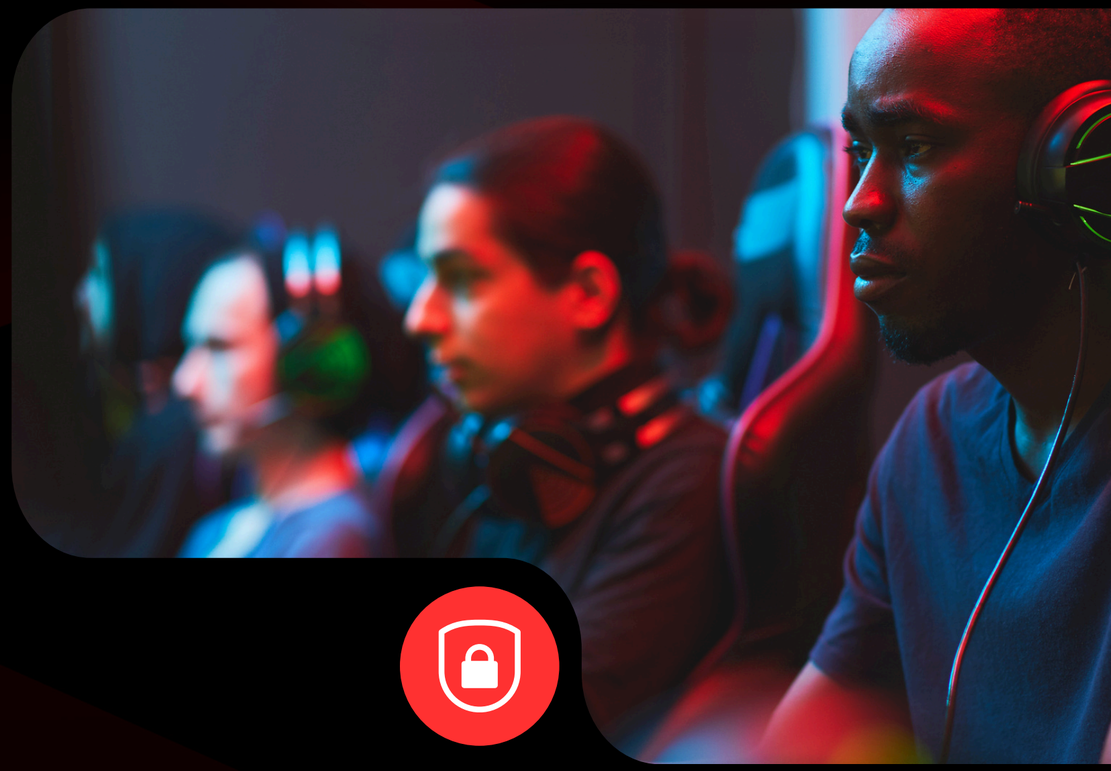
WHO CAN APPLY?

VAPT TRAINING IS SUITABLE FOR :

- Computer Science / IT students
- Cybersecurity aspirants
- Network administrators
- Software developers
- Ethical hacking beginners
- Anyone interested in cybersecurity and hacking
- No deep prior knowledge is required — computer and networking knowledge is required

FOR DCSC-CERTIFIED PROFESSIONALS, THIS COURSE IS A HIDDEN GEM.

It helps you upgrade your existing skills to the next professional level, align with current industry practices, and move one step closer to your dream cybersecurity role.



THANK YOU

GET IN TOUCH

Thank you for being a part of this journey.
Stay secure. Stay ahead. Build the future of cybersecurity with us.

CONTACT US