RECON

CYBER SECURITY

DEFEND | DETECT | SECURE

OUR PARTNERS

cisco python EY Red Hat CompTIA Microsoft

OVERVIEW

VAPT (Vulnerability Assessment and Penetration Testing) training equips participants with the skills to identify, assess, and exploit security vulnerabilities in systems and networks to strengthen overall cybersecurity defenses.

PRE-REQUISITES

Students should already be familiar with how to operate the Linux Operating system.

WHO WE ARE

We promise to offer the best training and certification programs to our students. We provide the programs and resources you need to succeed if you are just beginning your Cyber security career or are an experienced expert wishing to develop your skills. Contact us today to learn more about our training and certification options!

WHY CHOOSE US

Welcome to our Cyber Security Training Institute, where we are committed to giving individuals and organisations who want to protect their digital assets thorough training and certification programmes. Our knowledgeable Trainers will bring you through the complexities of cyber security with their cutting-edge expertise and practical experience. You will learn useful methods and abilities to protect yourself from online dangers, such as ethical hacking, network security, incident response, and other things. Our programmes give you the opportunity to hone your skills and grow your profession through practical lab experiences and individualised coaching.

WINTER INTERNSHIP TRAINING

PENETRATION TESTING COURSE CONTENT

COURSE DURATION: 40 hrs

- Lesson 1 : How to plan your Penetration Testing
  - Objectives and Goals:
    Defining clear goals for the penetration test.
  - Team Roles and Responsibilities:
    Assigning tasks and roles to team members.
  - Timeline and Milestones:
    Setting a schedule and key milestones.
  - Resource Allocation:
    Identifying tools and resources needed.
  - Legal and Compliance Considerations:
    Understanding legal requirements and obtaining permissions.

- Lesson 2 : Scoping your Penetration Testing
  - Defining the Scope:
    Determining the boundaries of the test.
  - Identifying Target Systems:
    Listing systems, networks, and applications to be tested.
  - Out-of-Scope Items:
    Clarifying what is not to be tested.
  - Risk Assessment:
    Evaluating potential risks and impacts.
  - Approval and Documentation:
    Obtaining client approval and documenting scope details.

- Lesson 3 : Network & Web-Application
  - Network Penetration Testing Basics:
    Overview of network testing methods.
  - Web Application Security Fundamentals:
    Introduction to web application vulnerabilities.
  - Tools and Techniques for Network Testing:
    Common tools and techniques used.
  - Tools and Techniques for Web Application Testing:
    Common tools and techniques used.
  - Case Studies and Examples:
    Real-world examples of network and web application attacks.

- Lesson 4 : Scanning Vulnerability
  - Port Scanning:
    Techniques and tools for identifying open ports.
  - Script Scanning:
    Using scripts for vulnerability detection.
  - Enumeration:
    Gathering detailed information about target systems.
  - Service & Version Scanning:
    Identifying running services and their versions.
  - Web-Application Scanning:
    Tools and methods for scanning web applications for vulnerabilities.

- Lesson 5 : Exploitation with Metasploit
  - Exploit Vulnerability:
    Using Metasploit to exploit vulnerabilities.
  - Bind & Reverse Shell:
    Understanding and implementing different shell types.
  - Payload Creation:
    Creating custom payloads for exploitation.
  - Metasploit Framework Overview:
    Introduction to Metasploit and its components.
  - Post-Exploitation Modules:
    Using Metasploit's post-exploitation features.

- Lesson 6 : Post-Exploitation
  - Data Collection:
    Techniques for gathering data from compromised systems.
  - Privilege Escalation:
    Methods for increasing user privileges.

- Persistence:
  Techniques for maintaining access to compromised systems.
- Cleaning Up:
  Removing traces of the attack.
- Reporting Findings:
  Documenting post-exploitation activities.

Lesson 7 : Pivoting Attack

- Introduction to Pivoting: Concepts and strategies for pivoting.
- Setting Up Pivot Points: Configuring pivot points in the network.
- Exploiting Internal Systems: Techniques for attacking internal systems through pivot points.
- Maintaining Access: Ensuring continued access through pivoted connections.
- Case Studies: Examples of successful pivoting attacks.

Lesson 8 : Browser exploitation

- BEEF Exploit Framework:
  Overview and usage of the BEEF framework.
- Browser Vulnerabilities:
  Common vulnerabilities in web browsers.
- Social Engineering Techniques:
  Using social engineering to exploit browser vulnerabilities.
- Payload Delivery:
  Methods for delivering payloads via browser exploits.
- Case Studies:
  Examples of browser exploitation attacks.

Lesson 9 : In-Depth Password Attacks

- John the Ripper:
  Using John the Ripper for password cracking.
- Brute Force Attack:
  Techniques for brute force password attacks.
- Dictionary Attack:
  Using dictionaries to crack passwords.
- Rainbow Table Attack:
  Understanding and using rainbow tables for password cracking.
- Other Password Cracking Tools:
  Overview of additional tools and methods.

Lesson 10 : Crcking / Solving CTF's

- CTF Overview:
  Introduction to Capture the Flag (CTF) competitions.
- Common CTF Challenges:
  Types of challenges typically found in CTFs.
- Tools and Techniques for Solving CTFs:
  Common tools and methods used.
- CTF Strategies:
  Tips and strategies for success in CTF competitions.
- Case Studies:
  Examples of CTF challenges and solutions.

Lesson 11 : Final Analysis

- Final Report Generation:
  Creating comprehensive penetration testing reports.
- Manual Reporting:
  Techniques for manual report creation.
- Automatic Reporting:
  Using automated tools for report generation.
- Review and Revision:
  Reviewing and revising reports for accuracy and completeness.
- Client Presentation:
  Presenting findings and recommendations to clients.

- **20 gb toolkit**
- **Weekend / weekdays classes**
- **Online and offline classes**
- **1 year membership**
- **Certificate after completion**
- **Interview preparation**
- **Live hacking training**
- **Class session recordings**
- **Ebooks tutorials**
- **24x7 support**

BOOTCAMP TRAINING HOURS

- **3 HOURS**
- **4 HOURS**
- **6 HOURS**

MOBILE APP PEN-TESTING COURSE CONTENT

COURSE DURATION: 40 hrs

- Lesson 01 : Android Fundamentals
  - Introduction to Android OS
  - Android Application Components
  - Android Security Model
  - Android Permissions and Manifest File
  - Android Development Environment
- Lesson 02 : Introduction to Mobile-App Testing
  - Overview of Mobile App Testing
  - Types of Mobile App Testing
  - Tools and Frameworks for Mobile Testing
  - Mobile App Testing Lifecycle
- Lesson 03 : Lab Setup
  - Setting Up Android Studio
  - Installing Required SDKs
  - Configuring Emulators and Devices
  - Setting Up Testing Tools
- Lesson 04 : Android Architectur
  - Android System Architecture
  - Android Runtime and Libraries
  - Application Framework
  - Application Components Overview
- Lesson 05 : APK File Structur
  - Understanding APK Components
  - APK Manifest File
  - Resources and Assets
  - DEX Files and their Role
- Lesson 06 : Reversing with APK tool / JADx-GUI
  - APK Tool Usage
  - Decompiling APK Files
  - Understanding Decompiled Code
  - Using JADx-GUI for Code Analysis
- Lesson 07 : Reversing with MobSF
  - Introduction to Mobile Security Framework (MobSF)
  - MobSF Installation and Setup
  - Analyzing APK Files with MobSF
  - Understanding MobSF Reports
- Lesson 08 : Static Analysis
  - Static Analysis Techniques
  - Tools for Static Analysis
  - Identifying Common Vulnerabilities
  - Analyzing Code for Security Issues
- Lesson 09 : Scanning Vulnerabilities with Drozer
  - Introduction to Drozer
  - Installing and Configuring Drozer
  - Scanning for Vulnerabilities
  - Interpreting Drozer Results
- Lesson 10 : Improper Platform Usage
  - Common Platform Usage Issues
  - Identifying Improper Platform Usage
  - Mitigating Risks of Platform Misuse
  - Best Practices for Platform Usage

- Lesson 11 : Log Analysis
  - Understanding Log Files
  - Log Collection and Storage
  - Analyzing Log Files for Security Issues
  - Tools for Log Analysis
- Lesson 12 : Insecure Storage
  - Types of Data Storage in Android
  - Identifying Insecure Storage Practices
  - Mitigating Insecure Storage Risks
  - Best Practices for Secure Storage
- Lesson 13 : Insecure Communication
  - Common Communication Issues in Mobile Apps
  - Securing Communication Channels
  - Implementing Secure Protocols
  - Testing for Communication Security
- Lesson 14 : Hard Coding Issues
  - Understanding Hard Coding
  - Identifying Hard Coded Secrets
  - Mitigating Hard Coding Risks
  - Best Practices for Secure Coding
- Lesson 15 : Insecure Authentication
  - Common Authentication Vulnerabilities
  - Testing Authentication Mechanisms
  - Mitigating Authentication Risks
  - Implementing Secure Authentication Practices
- Lesson 16 : Insufficient Cryptography
  - Understanding Cryptographic Basics
  - Identifying Insufficient Cryptography
  - Using Strong Cryptographic Algorithms
  - Testing Cryptographic Implementations
- Lesson 17 : Code Tempering
  - Types of Code Tampering
  - Identifying Tampered Code
  - Protecting Against Code Tampering
  - Testing for Code Integrity
- Lesson 18 : Extraneous Functionality
  - Understanding Extraneous Functionality
  - Identifying Unnecessary Features
  - Mitigating Risks from Extraneous Functionality
  - Best Practices for Feature Management
- Lesson 19 : SSL Pinning Attack
  - Introduction to SSL Pinning
  - Types of SSL Pinning Attacks
  - Mitigating SSL Pinning Vulnerabilities
  - Testing SSL Pinning Implementations
- Lesson 20 : Intercepting The Network Traffic
  - Techniques for Intercepting Network Traffic
  - Using Tools for Traffic Interception
  - Analyzing Intercepted Traffic
  - Mitigating Risks from Traffic Interception
- Lesson 21 : Dynamic Analysis
  - Overview of Dynamic Analysis
  - Tools for Dynamic Analysis
  - Conducting Dynamic Testing
  - Interpreting Dynamic Analysis Results
- Lesson 22 : Report Preparation
  - Creating Effective Security Reports
  - Key Components of a Security Report
  - Documenting Findings and Recommendations
  - Best Practices for Report Presentation

- **10 gb toolkit**
- **Weekend / weekdays classes**
- **Online and offline classes**
- **1 year membership**
- **Certificate after completion**
- **Interview preparation**
- **Live hacking training**
- **Class session recordings**
- **Ebooks tutorials**
- **24x7 support**

WEB APP PEN-TESTING COURSE CONTENT

COURSE DURATION: 40 hrs

- Lesson 1 : Introduction to Web-application Penetration-Testing
  - Understanding the Purpose of Penetration Testing:
  Learn why penetration testing is crucial for web applications.
  - Types of Web Vulnerabilities:
  Explore common security flaws targeted in web apps.
  - Tools for Web Penetration Testing:
  An overview of popular tools like Burp Suite, OWASP ZAP, and more.

- Lesson 2 : Finding Subdomains
  - Introduction to Subdomain Enumeration:
  Why subdomains are vital for security analysis.
  - Tools for Subdomain Discovery:
  Techniques and tools such as Sublist3r, Amass, and DNS recon.
  - Practical Guide to Subdomain Enumeration:
  Step-by-step approach to discovering and analyzing subdomains.

- Lesson 3 : Understanding HTTP
  - Overview of HTTP Protocol:
  Structure and workings of HTTP requests and responses.
  - Common HTTP Methods and Their Impact on Security:
  GET, POST, PUT, DELETE, and other HTTP methods.
  - Security Implications of HTTP Headers:
  How headers like CORS, HSTS, and Content-Security-Policy affect web security.

- Lesson 4 : Access Control Flaws
  - Understanding Access Control:
  What is access control, and why is it critical?
  - Types of Access Control Issues:
  Insecure Direct Object References (IDOR), broken access control.
  - Exploiting and Mitigating Access Control Flaws:
  Real-world examples and remediation techniques.

- Lesson 5 : Ajax Security
  - What is Ajax?: Introduction to Ajax and its role in web apps.
  - Security Risks with Ajax Requests: Common vulnerabilities like CSRF and improper data handling.
  - Securing Ajax Implementations: Techniques to ensure safe Ajax usage in web apps.

- Lesson 6 : Authentication Flaws
  - Introduction to Authentication Mechanisms: Passwords, tokens, and multifactor authentication.
  - Common Authentication Vulnerabilities: Brute force attacks, session fixation, weak password policies.
  - Securing Authentication: Best practices for strong authentication mechanisms.

- Lesson 7 : Buffer overflaws
  - What is a Buffer Overflow?: An overview of how buffer overflows occur.
  - Exploiting Buffer Overflow Vulnerabilities: Techniques and real-world examples.
  - Preventing Buffer Overflows: Defensive programming techniques to mitigate these flaws.

- Lesson 8 : Code Quality
  - The Importance of Secure Coding Practices: Understanding how code quality impacts security.
  - Common Coding Mistakes Leading to Vulnerabilities: Examples of poor coding practices.
  - Improving Code Quality for Security: Best practices in secure software development.

- Lesson 9 : Concurrency Flaws
  - What are Concurrency Issues?: Explanation of race conditions and deadlocks.
  - How Concurrency Flaws Impact Security: Real-world implications of concurrency vulnerabilities.
  - Mitigating Concurrency Vulnerabilities: Techniques to handle concurrency safely.
- Lesson 10 : Cross Site Scripting
  - Types of XSS Attacks: Reflected, stored, and DOM-based XSS.
  - Exploiting XSS Vulnerabilities: How attackers use XSS to compromise web apps.
  - Preventing XSS Attacks: Implementing proper input validation and sanitization.

- Lesson 11 : Improper Error Handling
  - Understanding Error Handling in Web Applications: Why proper error handling is important.
  - Common Flaws in Error Handling: How revealing error messages can lead to information leakage.
  - Best Practices for Error Handling: Techniques to secure error management.
- Lesson 12 : Injection Flaws
  - Overview of Injection Attacks: SQL injection, command injection, and LDAP injection.
  - Exploiting Injection Vulnerabilities: Real-world examples and techniques.
  - Mitigating Injection Flaws: Secure coding practices and input validation techniques.
- Lesson 13 : Denail of Service
  - What is a Denial of Service Attack?: How DoS attacks disrupt web services.
  - Common DoS Techniques: Flood attacks, slow attacks, and resource exhaustion.
  - Preventing DoS Attacks: Strategies to detect and mitigate DoS attacks.
- Lesson 14 : Insecure Communication
  - Understanding Secure Communication Protocols: TLS, HTTPS, and their importance.
  - Vulnerabilities in Web Communication: Man-in-the-middle attacks, SSL stripping.
  - Securing Communication Channels: Best practices for secure communication in web apps.
- Lesson 15 : Insecure Configuration
  - What is Insecure Configuration?:
How misconfigurations lead to vulnerabilities.
  - Common Misconfiguration Issues:
Exposed admin panels, weak file permissions.
  - Securing Web Application Configurations:
Steps to harden configurations for better security.
- Lesson 16 : Insecure Storage
  - Risks of Insecure Data Storage:
Sensitive data exposure due to poor storage practices.
  - Common Storage Vulnerabilities:
Unencrypted databases, weak cryptography.
  - Best Practices for Secure Data Storage:
Encryption techniques and secure storage mechanisms.
- Lesson 17 : Malicious File Execution
  - Understanding File Upload Vulnerabilities:
How attackers exploit file uploads.
  - Exploiting Malicious File Execution Flaws:
Real-world examples of file execution attacks.
  - Mitigating File Upload Risks:
Techniques to secure file upload mechanisms.
- Lesson 18 : Parameter Tampering
  - What is Parameter Tampering?:
Understanding how attackers manipulate input parameters.
  - Exploiting Parameter Tampering Vulnerabilities:
Real-world examples.
  - Preventing Parameter Tampering:
Implementing secure input validation and handling.
- Lesson 19 : Challenge Online Platform
  - Overview of Web Penetration Testing Challenges:
Introduction to online testing platforms.
  - Using Platforms like Hack The Box and TryHackMe:
Practical penetration testing in a simulated environment.
  - Improving Skills with Online Challenges:
Benefits of participating in web security challenges.

- **10 gb toolkit**
- **Weekend / weekdays classes**
- **Online and offline classes**
- **1 year membership**
- **Certificate after completion**
- **Interview preparation**
- **Live hacking training**
- **Class session recordings**
- **Ebooks tutorials**
- **24x7 support**

Every Class Recordings

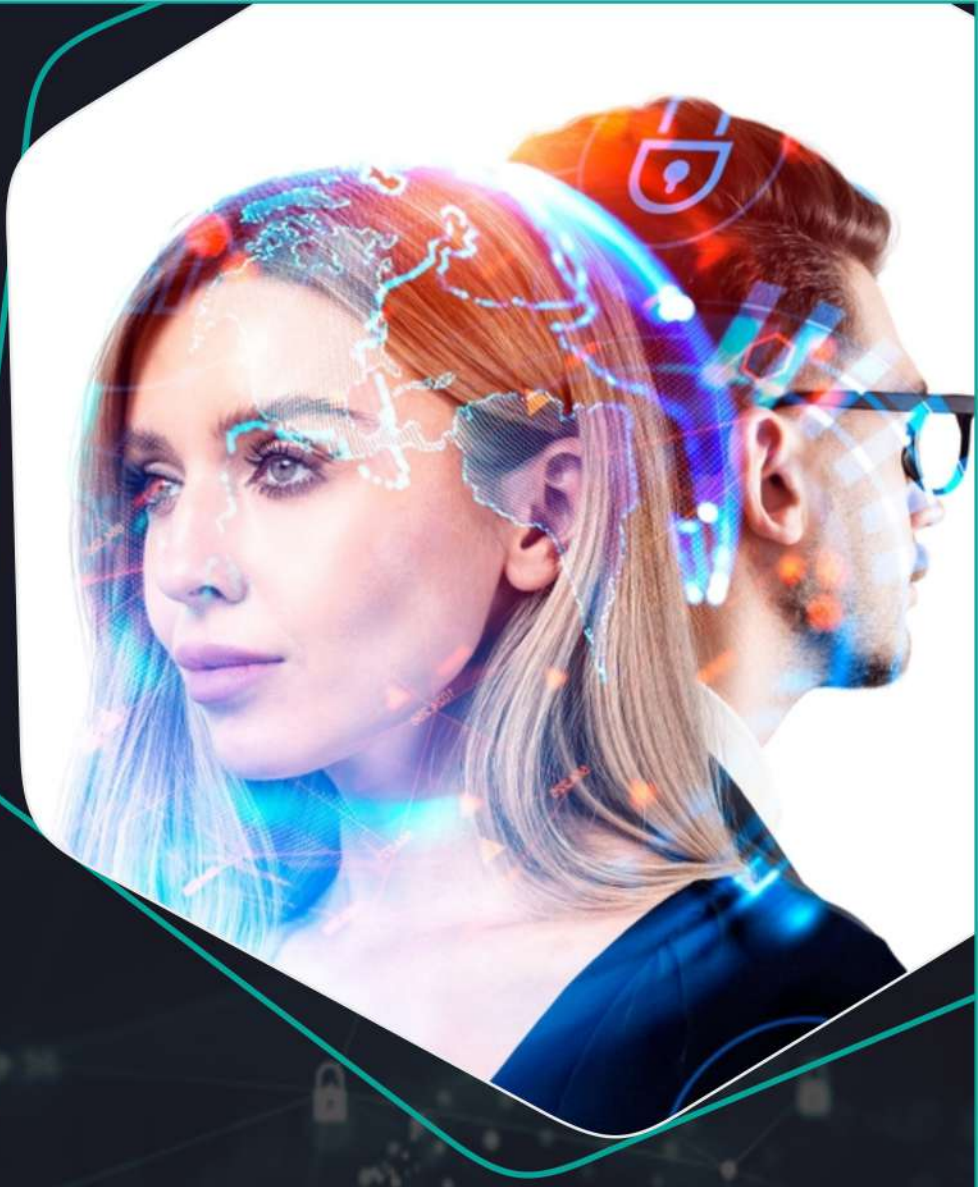
Easy Repetations

Shareable Content

Hybrid Classes

Checkpoint Based Training

24x7 Support



RECON CYBER SECURITY PVT. LTD

(HEAD OFFICE | LAXMI NAGAR, NEW DELHI)

2nd Floor, Gali no 1, Shakarpur, Laxmi Nagar New Delhi 110092

WhatsApp or Call : +91-8595756252, +91-8800874869

Training@reconforce.in, Info@reconforce.in

RECON CYBER SECURITY PVT. LTD

(BRANCH OFFICE | SANT NAGAR BURARI, NEW DELHI)

Ground Floor, Gali no 8, Main Market, Sant Nagar, Burari, New Delhi 110092

WhatsApp or Call : +91-8595756252, +91-8800874869

Training@reconforce.in, Info@reconforce.in

#RECON CYBER SECURITY