RECON CYBER SECURITY

DEFEND | DETECT | SECURE

OUR PARTNERS

CISCO python EY Red Hat CompTIA Microsoft

OVERVIEW

In this course, students will learn the about Network Penetration Testing techniques. Topics include Reconnaissance, Scanning, Exploitation, Post Exploitation and more.

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.

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.

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