Techtwins Technologies LLP

Cyber Security Training from Scratch to Expert Level

Welcome to this course on **Practical Ethical Hacking**. To enjoy this course, you need nothing but a positive attitude and a desire to learn. **No prior knowledge is required.**

In this course, you will learn the practical side of ethical hacking. Too many courses teach students tools and concepts that are never used in the real world. In this course, we will focus only on tools and topics that will make you successful as an ethical hacker. The course is incredibly **hands on** and will cover many foundational topics.

What you'll learn

- Linux Basic operations and Networking Concept on Practical Approach
- Social Engineering Tactics for Cyber Security
- Practical ethical hacking and penetration testing skills
- Network hacking and defenses
- Active Directory exploitation tactics and defenses
- Common web application attacks
- How to hack wireless networks
- Learn how to write a pentest report
- Understand the security threats affecting networks and applications
- OWASP Top 10
- IT security trends
- Web App Testing
- Mobile Hacking
- Wireless Attacks and defences
- System Hacking (Windows and Linux)
- Privilege Escalation to get the Root access of servers and systems

Course Content

- **Introduction**
  - Introduction and Course Overview
  - Preview
  - What is Cyber Security?
  - Information Security vs Cyber Security
  - Cyber Laws and Information Security Standards
  - Cyber Security Laws in India
  - Indian Act 2000
  - A Day in the Life of an Ethical Hacker

- **Networking Refresher**
  - Introduction
  - IP Addresses
  - MAC Addresses
  - TCP, UDP, and the Three-Way Handshake
  - Common Ports and Protocols
  - The OSI Model
  - Subnetting: Part 1 - Methodology
  - Subnetting: Part 2 - Hands-On Challenge

- **Setting Up Our Lab**
  - Installing VMWare / VitualBox
  - Linux Image Repository (UPDATE)
  - Installing Kali Linux

- **Introduction to Linux**
  - Exploring Kali Linux
  - Navigating the File System
  - Users and Privileges
  - Common Network Commands
  - Viewing, Creating, and Editing Files
  - Starting and Stopping Kali Services
  - Installing and Updating Tools
  - Scripting with Bash

- **Introduction to Python**
  - Introduction
  - Strings
  - Math
  - Variables & Methods
  - Functions
  - Boolean Expressions
  - Relational and Boolean Operators
  - Conditional Statements
  - Lists
  - Tuples
  - Looping
  - Importing Modules
  - Advanced Strings
  - Dictionaries
  - Sockets
  - Building a Port Scanner

- **The Ethical Hacker Methodology**
  - The Five Stages of Ethical Hacking
  - Example Explore

- **Information Gathering (Reconnaissance) ***
  - Passive Reconnaissance Overview
  - Identifying Our Target
  - E-Mail Address Gathering with Hunter.io
  - Gathering Breached Credentials with Breach-Parse
  - Utilizing theharvester
  - Hunting Subdomains - Part 1
  - Hunting Subdomains - Part 2
  - Identifying Website Technologies
  - Information Gathering with Burp Suite
  - Google Fu
  - Utilizing Social Media
  - OSINT Framework
  - Future of Social Engineering

- **Scanning & Enumeration**
  - Installing Kioptrix: Level 1
  - Scanning with Nmap
  - Preview
  - Enumerating HTTP/HTTPS - Part 1
  - Enumerating HTTP/HTTPS - Part 2
  - Enumerating SMB
  - Enumerating SSH
  - Researching Potential Vulnerabilities

- **Additional Scanning Tools ***
  - Scanning with Masscan
  - Scanning with Metasploit
  - Scanning with Nessus - Part 1
  - Scanning with Nessus - Part 2

- **Exploitation Basics ***
  - Different Shells: Reverse Shells and Bind Shells
  - Payload type
  - Gaining Root with Metasploit
  - Manual Exploitation: Making your own payload
  - Brute Force Attacks
  - Password Spraying and Credential Stuffing
  - Hydra Tool overview

- **Machine Walkthrough: Real World Scenarios for Pentesting ***
  - Introduction
  - Walkthrough - Lame
  - Walkthrough - Blue
  - Walkthrough - Devel
  - Walkthrough - Jerry
  - Walkthrough - Nibbles
  - Walkthrough - Bashed
  - Walkthrough - Netmon
  - More we will add as per time remains

- **Active Directory Overview**
  - Active Directory Overview
  - Lab Overview and Requirements
  - Downloading Necessary ISOs
  - Setting Up the Domain Controller
  - Setting Up the User Machines
  - Setting Up Users, Groups, and Policies
  - Joining Our Machines to the Domain
  - Ready for Hacking and compromise the Windows Servers
  - LLMNR Poisoning Overview
  - Capturing NTLMv2 Hashes with Responder
  - Password Cracking with Hashcat
  - LLMNR Poisoning Defenses
  - SMB Relay Attacks Overview
  - Quick Lab Update
  - Discovering Hosts with SMB Signing Disabled
  - SMB Relay Attack Demonstration Part 1
  - SMB Relay Attack Demonstration Part 2
  - SMB Relay Attack Defenses
  - Gaining Shell Access
  - IPv6 Attacks Overview
  - Installing mitm6
  - Setting Up LDAPS
  - IPv6 DNS Takeover via mitm6
  - IPv6 Attack Defenses
  - Attack Vectors and Strategies

- **Attacking Active Directory: Post-Compromise Enumeration Advanced Tactics**
  - Introduction
  - PowerView Overview
  - Bloodhound Overview and Setup
  - Grabbing Data with Invoke-Bloodhound
  - Enumerating with Bloodhound

- **Attacking Active Directory: Post-Compromise Attacks ***
  - Introduction
  - Pass the Hash / Password Overview
  - Pass the Password Attacks
  - Dumping Hashes with secretsdump.py

- Cracking NTLM Hashes with Hashcat
- Pass the Hash Attacks
- Pass Attack Mitigations
- Token Impersonation Overview
- Token Impersonation with Incognito
- Token Impersonation Mitigation
- Kerberoasting Overview
- Kerberoasting Walkthrough
- Kerberoasting Mitigation

- **Post Exploitation: Overview**
  - Introduction
  - File Transfers Review
  - Maintaining Access Overview
  - Pivoting Lab Setup
  - Pivoting Walkthrough
  - Cleaning Up

- **Testing the Top 10 Web Application Vulnerabilities: Live Website POC ***
  - Introduction
  - The OWASP Top 10 and OWASP Testing Checklist
  - OWASP Top 10 2017 and 2019
  - Installing OWASP Juice Shop
  - Installing Foxy Proxy
  - Exploring Burp Suite
  - Introducing the Score Board
  - SQL Injection Attacks Overview
  - SQL Injection Walkthrough
  - SQL Injection Defenses
  - Broken Authentication Overview and Defenses
  - Testing for Broken Authentication
  - Sensitive Data Exposure Overview and Defenses
  - Testing for Sensitive Data Exposure
  - XML External Entities (XXE) Overview
  - XXE Attack and Defense
  - Broken Access Control Overview
  - Broken Access Control Walkthrough
  - Security Misconfiguration Attacks and Defenses
  - Cross-Site Scripting (XSS) Overview
  - Reflected XSS Walkthrough

- Stored XSS Walkthrough
- Preventing XSS
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring
- IDOR vulnerability
- Bug Bounty as a Career
- Bug Bounty as a Professional and Build your own Startup in Cyber Security

- **Wireless Penetration Testing**
  - Wireless Penetration Testing Overview
  - WPA PSK Exploit Walkthrough
  - Wi-Fi hacking
  - Attack Defences

- **Mobile Hacking ***
  - Introduction overview
  - Rooting Phone Overview
  - ADB shell
  - Remote Hacking

- **Legal Documents and Report Writing: Overview with some Real Company VAPT Reports ***
  - Common Legal Documents
  - Pentest Report Writing
  - Reviewing a Real Pentest Report

- **Career Advice**
  - Future in Cyber Security
  - Profiles you get in Cyber Security Field
  - Resources and Goal Sets
  - Certifications and Degrees

Note: (*) Represents New Content will added in future

At the end of this course, you will have a deep understanding of **external and internal network penetration testing, wireless penetration testing,** and **web application penetration testing.** All lessons taught are from a real-world experience and what has been encountered on actual engagements in the field.