



Offensive Pentesting

Beginners Red Teaming Course



Professional Hacking?

Content store portalbittentechsolutions.in/viewPdf

Professional Hacking?

The diagram illustrates the professional hacking process, centered around a shield with a hash symbol. The process follows a circular flow of steps:

- Initial Recon** (Blue arrow with globe and magnifying glass icon)
- Initial Compromise** (Yellow arrow with puzzle pieces icon)
- Establish Foothold** (Red arrow with door icon)
- Escalate Privileges** (Blue arrow with upward arrow icon)
- Internal Recon** (Yellow arrow with magnifying glass icon)
- Move Laterally** (Blue arrow with double arrows icon)
- Complete Mission** (Red arrow with checkmark icon)

A green arrow labeled **Maintain Presence** (with a cloud and key icon) loops back from the end of the process to the beginning.

@trihackme

► Introduction

- Global **penetration testing market** size is projected to grow from \$2.45 billion in 2024 to \$6.35 billion by 2032
- **Top 5 Cyber Security Jobs** and the **coolest!**
- **Scared of AI?** Pentesting has **job security** and **immense growth**
- **High paying** salaries ~ 10-15 LPA/90K-110K\$ (fresher)
- OSCP – **Benchmark** of Excellence!



► Introduction

- **Common avenues**
 - Social Engineering
 - Public Software Exploits
 - Password Cracking/Credential Stuffing
 - Service Misconfigurations
 - Web Application Attacks

1 About the Course



- ## About the Course
- **Beginner Friendly** complete network pentesting and red teaming course!
 - Master the art of ethical hacking to **attack systems at scale**.
 - Right from **recon to post exploitation**!
 - **Industry-standard** tools and methodologies, learning to identify and **exploit vulnerabilities** effectively.
 - Carry **real world adversarial engagements** in an enterprise environment
 - **Crack** pentesting **certifications** like OSCP, CRTP, eCPPT, PNPT, CPTS and more
- 

2 Who is this course for?



▶ Target Audience

- Students/Professionals having **basic penetration testing knowledge**
- Red Teamers and Network Security Engineers
- Penetration Testers focusing on **infrastructure testing**
- People looking to **improve** their IT **system hardening**
- People looking to **avoid embarrassment** from IT Security

3 Learning Outcomes?




► Learning Outcomes?

- Become a **skilled** penetration tester that the industry wants
- Understanding **exploits** and **writing basic scripts** and tools to aid in the pentesting process
- Conducting remote, local **privilege escalation**, and **client-side** attacks
- Learn **network tunneling** to **pivot** between networks
- **Red teamer** and **adversarial mindset**
- Offensive Security **market understanding**

Content store portalbittentechsolutions.in/viewPdf

4 Features?



Course Features

- 100+* hours of **video** content
- **Hardest** concepts **broken** down into **simplest** words
- Focus on **why > how**
- **Modern** Penetration Testing **methodology**
- 24/7 **on demand** access
- Buy **once**, learn for **lifetime**!
- **2000+** active community members
- **LIVE** support

13

► Course Features

- Practice Challenge CTF Labs!
- Presentation Slides as PDFs
- Additional Study Content
- External references to learn more

5 ► Requirements?



► Prerequisites

- Strong understanding of computer networking and TCP/IP
- Basic hands on experience of Windows and Linux sysadmin and command line (Bash/CMD/Powershell)
- Recommended:
 - Basic hands on experience in Penetration Testing concepts and tools
 - Familiarity in OWASP top 10 and other network level attacks
 - Knowledge of common vulnerabilities and exploits

► Prerequisites

- Some knowledge is assumed
- This is not all
- Strict anti-spoonfeed policy
- Practice is everything
- Mindset matters
- Enumeration is the key!