SMACKTHAT

PRACTICAL ETHICAL HACKING

COMPLETE COURSE OUT LINE



BEGINNER → INTERMEDIATE → ADVANCED

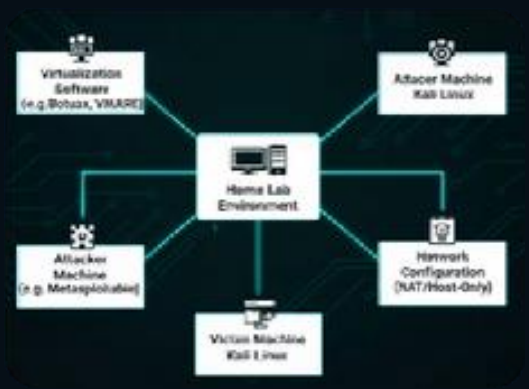
(Real Pentester Roadmap)

1.1 Introduction to the Course
1.2 Who This Course Is For
1.3 Effective Notekeeping for Hackers



SECTION 2:
LAB SETUP (PRACTICAL)

2.1 Installing VirtualBox / VMware
• Ideal configuration settings
2.2 Installing Kali Linux
• Performance tuning
• Network settings
• Essential post-install steps
2.3 Installing Victim Machines
• Metasploitable 2
• Metasploitable 3 (optional)
• OWASP BWA
• DVWA / Mutillidae



SECTION 3
KALI LINUX 101

3.1 Linux Navigation
3.2 File & Directory Management
3.3 Users, Groups & Permissions
3.4 Networking Commands
3.5 Linux for Pentesters (Bonus)



SECTION 4:
NETWORKING REFRESHER

4.1 OSI Model Deep Dive
4.2 Subnetting Basics
4.3 Common Ports & Protocols
• FTP, SSH, DNS, HTTP, SMB, RDP
• How attackers abuse each service



SECTION 5:
HACKING METHODOLOGY (THE REAL ROADMAP)

5.1 Five Stages of Ethical Hacking
5.2 Real-World Pentesting Flow



SECTION 6:
PASSIVE INFORMATION GATHERING

6.1 Google Dorking
6.2 Whois Lookups
6.3 Subdomain & Email Harvesting
6.4 Shodan Recon
6.5 DNS Recon / Zone Transfers (dig)



SECTION 7:
ACTIVE INFORMATION GATHERING & SCANNING

7.1 Installing Metasploitable
7.2 Nmap – Basics
7.3 Nmap – Intermediate
7.4 Nmap – Advanced
7.5 Zenmap GUI
7.6Enumerating Services (FTP/SSH/SMB)



SECTION 8:
ADVANCED OSINT (NEW – IMPORTANT)

8.1 Username OSINT
8.2 Image OSINT (Exif & Metadata)
8.3 Breach Database OSINT
8.4 Dark Web OSINT Basics
8.5 Social Media Profiling



SECTION 9:
PASSWORD ATTACKS & CREDENTIAL CRACKING

9.1 Understanding Password Attacks
9.2 Hydra Attacks (SSH/FTP/HTTP)
9.3 Wordlist Creation (Crunch)
9.4 Hashing Basics (MD5/SHA/bcrypt)
9.5 Cracking with Hashcat



SECTION 10:
METASPLOIT FRAMEWORK MASTERCLASS (NEW)

10.1 MSF Fundamentals
10.2 Exploits, Paylo ads & Modules
10.3 Auxiliary Scanner Modules
10.4 Meterpreter Deep Dive
10.5 Post-Exploitation with Meterpreter
10.6 Pivoting Basics



SECTION 11:
SYSTEM EXPLOITATION & REVERSE SHELLS

11.1 Shell Basics (Bind vs Reverse)
11.2 Linux Reverse Shells
• Netcat
• Bash
• Python
• PHP
11.3 Windows Reverse Shells
• PowerShell
• msfvenom payloads
11.4 Shell Stabilization (TTY Upgrade)
11.5 Reverse Shell via File Upload
11.6 Bypassing Firewalls for Shell Delivery
11.7 Persistence Techniques



SECTION 12:
SYSTEM AND ANDROID HACKING

12.1 Exploiting Windows Machines and Android
12.2 Exploiting Linux Machines
12.3 Privilege Escalation — Windows
12.4 Privilege Escalation — Linux
12.5 Post-Exploitation Techniques



SECTION 13:
VULNERABILITY SCANNING (NEW – MANDATORY)

13.1 Nessus Essentials Setup
13.2 Full Vulnerability Scan
13.3 OpenVAS Setup
13.4 Understanding False Positives
13.5 Mapping Vulns Exploits



SECTION 14:
MITM (MAN-IN-THE-MIDDLE)

14.1 ARP Protocol Basics
14.2 MITM Theory
14.3 Ettercap Basics
14.4 SSL Stripping (Optional)



SECTION 15:
SOCIAL ENGINEERING

15.1 SE Lifecycle
15.2 Attack Types
- Phishing
- Vishing
- Pretexting
- Tailgating

15.3 Psychology of Human Hacking
15.4 Real-World SE Case Studies
15.5 Practical Phishing
- SET Toolkit
- Zphisher / Blackeye
- Custom phishing pages And Beef

15.6 Advanced Campaigns
- GoPhish setup
- Email templates
- Tracking & logging



SECTION 16:
DOS & DDOS ATTACKS

16.1 What is DoS & DDoS
16.2 Types of DoS
- Volumetric
- Protocol
- Application layer

16.3 Botnets & Amplification
16.4 Practical DoS Tools
- LOIC
- HOIC
- HULK
- Slowloris



SECTION 17:
SESSION HIJACKING

17.1 How Sessions Work
17.2 Session Hijacking Types
• Sidejacking
• Fixation
• Prediction
17.3 MITM for Session Stealing
17.4 Man in the Browser Attack
17.5 Session Hijacking with Burp



SECTION 18:
FIREWALLS & DEFENSE EVASION

18.1 IDS, IPS, Firewall Basics
18.2 Honeypots & Honeytokens
18.3 Firewall Evasion
• Fragmentation
• Decoys
• Packet manipulation



SECTION 19:
HACK ING WEB SERVERS

19.1 Apache / Nginx / IIS Architecture
19.2 CMS Hacking
• WordPress
• Joomla
• Drupal
19.3 Server Scanning Tools
• Nikto
• Dirbuster
• WPScan



SECTION 20:
HACKING WEB APPLICATIONS

20.1 DVWA
20.2 HTTP Requests
20.3 HTTP Responses
20.4 Burp Suite Full Setup
20.5 Manual Testing Workflow
20.6 DVWA TOP 10 (NEW – VERY IMPORTANT)

- IDOR
- XSS (Reflected/Stored/DOM)
- File Upload Bypass
- Command Injection
- CSRF
- SSTI Basics
- Rate Limit Bypass
- Business Logic Attacks



SECTION 21:
SQL INJECTION – COMPLETE

21.1 SQLi Basics
21.2 SQLi Manual Advanced
21.3 SQLi Using SQLMap



SECTION 22:
WIRELESS PENETRATION TESTING

22.1 Wireless Basics
22.2 Monitor Mode Setup
22.3 Capturing WPA/WPA2 Handshakes & Evil Twin attacks
22.4 rockyou.txt Wordlist



SECTION 23:
CRYPTOGRAPHY BASICS

23.1 What is Cryptography
23.2 Symmetric vs Asymmetric
23.3 Hashing Algorithms



ONE-TIME INVESTMENT ONLY

15000 PKR

This program is designed to give you maximum value with a single payment — no hidden fees, no upsells.

WHAT YOU'LL GET:

2 Years of Full Access to all recorded content

Premium Tools & Resources used by real-world pentesters



WHY JOIN THIS PROGRAM?

Because this is not just another course.
This is a complete transformation journey from beginner to professional ethical hacker.

- ✓ **Learn real-world skills used by top penetration testers**
- ✓ **Work on industry-grade labs, projects & simulation environments**
- ✓ **Understand how hackers think, attack & exploit systems**
- ✓ **Build strong fundamentals + advanced practical experience✓ Get clarity, direction, mentorship & long-term support ✓ Become job-ready, bug-bounty ready, and confident in hacking**

If you are serious about becoming a cybersecurity professional, this program is your fastest and most practical path.

TERMS & CONDITIONS:

2-Year Access: All videos, resources, and updates are available for 24 months.

No Refund Policy: This is a digital learning program; refunds are not provided.

Educational Purpose Only: All tools, labs, and resources are strictly for learning and practicing ethical hacking. Community Rules: By enrolling, you agree to follow the academy's learning guidelines and maintain professionalism.