# Hands-On Ethical Hacking

**Course Duration: 22(±) Hours**

**Course Content**

1. **Introduction**
    a. Introduction and Course Overview
    b. What To Expect from This Course
2. **Note Keeping**
    a. Importance of Note keeping
    b. Note Keeping Tools
3. **Basic Networking**
    a. Introduction
    b. IP Addresses
    c. MAC Addresses
    d. Three-Way Handshake
    e. Common Ports and Protocol
    f. OSI Layer
    g. Subnetting
4. **Setting Up the Lab**
    a. Installing the VMWare or Virtual Box
    b. Configuring the VMWare/Virtual Box
    c. Installing Kali Linux
5. **Basic Linux**
    a. Exploring the OS
    b. Root
    c. File System Overview
    d. Users and Privileges
    e. Basic Network Command
    f. Installing and Updating Tools
    g. Read Write and Execute Files
    h. Bash Scripting
6. **Hacker Methodology**
    a. Stages of Hacking
7. **Information Gathering (Reconnaissance)**
    a. Passive Reconnaissance
    b. Identifying Targets
    c. Discovering Email Address
    d. Gathering Breached Credentials
    e. Hunting Breached Credentials
    f. Subdomain Findings
    g. Detecting Website Technologies
    h. Using Burp Suite
    i. Google Dorking
    j. Social Media Search

8. **Scanning and Enumeration**
    a. Introduction to HackTheBox and Others
    b. Scanning with NMAP
    c. Enumerating HTTP/HTTPS
    d. Enumerating SMB
    e. Enumerating SSH
    f. Potential Vulnerability
    g. Scanning with Nessus
9. **Exploitation Overview**
    a. Reverse Shell and Bind Shell
    b. Stage and Non-Staged Payloads
    c. Root access with Metasploit
    d. Manual Exploitation
    e. Brute Force Attack
10. **Mid-Course Capstone**
    a. Setting Up HackTheBox, tryhackme and others
    b. Lab1 Walkthrough
    c. Lab2 Walkthrough
    d. Lab3 Walkthrough
    e. Lab4 Walkthrough
11. **Active Directory**
    a. Active Directory Overview
12. **Building Active Directory Lab**
    a. Lab Requirements
    b. ISO Download
    c. Setting Up Domain Controller (DC)
    d. Setting Up User Machine
    e. Setting Up Users, Groups and Policies
    f. Joining Machine to AD
13. **Active Directory Attack**
    a. Introduction
    b. LLMNR Poisoning
    c. Capturing NTLMv2 Hash
    d. HashCat: Password Cracking
    e. SMB Relay Attack
    f. SMB Relay Attack: Demonstration
    g. SMB Signing Disable: Host Discovery
    h. Gaining Shell Access
    i. IPv6 Attacks Overview
    j. Installing mitm6
    k. Setting Up LDAPS
    l. IPv6 DNS Takeover via mitm6

14. **Active Directory Attack: Post Compromised Enumeration**
    a. Introduction
    b. PowerView Overview
    c. Domain Enumeration with PowerView
    d. Bloodhound Overview and Setup
    e. Grabbing Data with Invoke-Bloodhound
    f. Enumerating Domain Data with Bloodhound
15. **Active Directory Attack: Post Compromised Attack**
    a. Introduction
    b. Pass the Hash / Password Overview
    c. Installing crackmapexec
    d. Pass the Password Attacks
    e. Dumping Hashes with secretsdump.py
    f. Cracking NTLM Hashes with Hashcat
    g. Pass the Hash Attacks
    h. Pass Attack Mitigations
    i. Token Impersonation Overview
    j. Token Impersonation with Incognito
    k. Token Impersonation Mitigation
    l. Kerberoasting Overview
    m. Kerberoasting Walkthrough
    n. GPP / cPassword Attacks Overview
    o. Abusing GPP
    p. Mimikatz Overview
    q. Credential Dumping with Mimikatz
    r. Golden Ticket Attacks
16. **Post Exploitation**
    a. Introduction
    b. File Transfers Review
    c. Maintaining Access Overview
    d. Pivoting Lab Setup
    e. Pivoting Walkthrough
    f. Cleaning Up
17. **Web Application Enumeration**
    a. Introduction
    b. Installing Go
    c. Finding Subdomains with Tools
    d. Finding Live Domain and Content Enumeration

18. **Top 10 Web Application Testing**
    a. Introduction
    b. The OWASP Top 10 and OWASP Testing Checklist
    c. Installing OWASP Juice Shop
    d. Exploring Burp Suite
    e. Introducing the Score Board
    f. SQL Injection Attacks
    g. Testing for Broken Authentication
    h. Testing for Sensitive Data Exposure
    i. XML External Entities (XXE)
    j. Broken Access Control Overview
    k. Security Misconfiguration Attacks
    l. Cross-Site Scripting (XSS)
19. **Wireless Penetration Testing**
    a. Wireless Penetration Testing Overview
    b. WPA PSK Exploit Walkthrough
20. **Document and Reports**
    a. Legal Documents
    b. Report Writing (With Sample)
21. **Final Assessment**
    a. **Quiz or Lab Work**

**Course Extra**

**Python Basic**:

- Introduction
- Strings
- Math
- Variables & Methods
- Functions
- Boolean Expressions
- Relational and Boolean Operators
- Conditional Statements
- Lists
- Tuples
- Looping
- Importing Modules
- Advanced Strings
- Dictionaries
- Sockets