CYBRARY

Course Syllabus

Penetration Testing and Ethical Hacking

Instructor Name: Ken Underhill, CEH,CHFI

Course Creation Date: 10/15/2018

Course Description and Goals

Prerequisites: Students should have foundational knowledge in computer networking, operating systems (Windows and Linux), client/server relationship, and Web servers. It is recommended that students have at least 2 years of experience in IT and/or cyber security before taking this course.

Study Resources: The course includes downloadable study materials, including quiz questions and step by step lab guides in the resources section of the course.

Course Description: This course is designed to introduce students to penetration testing (ethical hacking) and is designed as an unofficial preparation course for the EC-Council Certified Ethical Hacker (CEH) exam. Students will learn a broad knowledge base in areas, like footprinting, scanning, malware, session hijacking, and more. This is an ideal course for students looking to start a career as a penetration tester, students studying for the CEH exam, and for students that are simply curious about ethical hacking.

Course Goals: By the end of this course, students should be able to:

❏ Understand what penetration testing (ethical hacking) is and why it is important
❏ Comfortably speak through the traditional hacking methodology
❏ Understand tools that can be used for a penetration test

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

1

Labs Used: After Module 2 of this course, you will need access to the Cybrary lab environment to follow along step by step with the lab guides. However, you can also practice the overall concepts (i.e.- scanning) in your own virtual environment, but the step by step guides are designed around the Cybrary lab environment.

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

2

CYBRARY

Course Outline

Module 1 | Introduction
    Lesson 1.0: Course Introduction (05:56)
    Lesson 1.1: CIA Triad, Black, White, and Grey Hats (10:21)
    Lesson 1.2: Laws (07:01)
    Lesson 1.3: Bonus: VirtualBox and Kali Linux (05:30)
    Lesson 1.4: Password Cracking Lab (07:53)

Module 2 | Footprinting
    Lesson 2.0: Intro Pre-assessment (05:58)
    Lesson 2.1: Footprinting Basics (11:45)
    Lesson 2.2: Lab Introduction (01:39)
    Lesson 2.3: Footprinting NIKTO Lab (05:56)
    Lesson 2.4: Footprinting theHarvester Lab (06:25)
    Lesson 2.5: Footprinting Shodan Lab (04:48)
    Lesson 2.6: Footprinting Google Hacking Lab (06:50)

Module 3 | Scanning and Enumeration
    Lesson 3.0: Scanning and Enumeration Introduction (02:36)
    Lesson 3.1: TCP 3 way Handshake (04:21)
    Lesson 3.2: Banner Grabbing (10:48)
    Lesson 3.3: Live Systems Lab Part 1 (02:22)
    Lesson 3.4: Live Systems Lab Part 2 (02:49)
    Lesson 3.5: Live Systems Lab Part 3 (04:08)
    Lesson 3.6: Live Systems Lab Part 4 (02:23)
    Lesson 3.7: Port Checking Lab Part 1 (03:21)
    Lesson 3.8: Port Checking Lab Part 2 (02:21)
    Lesson 3.9: Port Checking Lab Part 3 (03:05)
    Lesson 3.10: Scanning Techniques Lab Part 1 (04:05)
    Lesson 3.11: Scanning Techniques Lab Part 2 (03:31)
    Lesson 3.12: Scanning Techniques Lab Part 3 (02:21)
    Lesson 3.13: Scanning Techniques Lab Part 4 (04:06)
    Lesson 3.14: Scanning Techniques Lab Part 5 (05:00)

CYBRARY

Lesson 3.15: Scanning Techniques Lab Part 6 (03:08)
Lesson 3.16: Scanning Techniques Lab Part 7 (04:46)
Lesson 3.17: Scanning Techniques Lab Part 8 (02:40)
Lesson 3.18: Scanning Techniques Lab Part 9 (02:30)
Lesson 3.19: Scanning Techniques Lab Part 10 (04:50)
Lesson 3.20: Scanning Techniques Lab Part 11 (03:43)
Lesson 3.21: OS Fingerprinting Lab Part 1 (06:05)
Lesson 3.22: OS Fingerprinting Lab Part 2 (05:53)
Lesson 3.23: Mapping Networks Lab Part 1 (05:00)
Lesson 3.24: Mapping Networks Lab Part 2 (03:23)
Lesson 3.25: Mapping Networks Lab Part 3 (06:40)
Lesson 3.26: Mapping Networks Lab Part 4 (10:21)
Lesson 3.27: Banner Grabbing Lab Part 1 (03:07)
Lesson 3.28: Banner Grabbing Lab Part 2 (02:59)
Lesson 3.29: Banner Grabbing Lab Part 3 (02:45)
Lesson 3.30: Banner Grabbing Lab Part 4 (03:55)
Lesson 3.31: Enumeration Tools Lab Part 1 (04:21)
Lesson 3.32: Enumeration Tools Lab Part 2 (02:58)
Lesson 3.33: Enumeration Tools Lab Part 3 (02:54)
Lesson 3.34: Enumeration Tools Lab Part 4 (03:59)

Module 4 | System Hacking
Lesson 4.0: System Hacking Introduction (08:45)
Lesson 4.1: Lab Introduction (07:23)
Lesson 4.2: Backdoor System Hacking Lab (11:02)
Lesson 4.3: System Hacking Planting a Backdoor lab (11:20)

Module 5 | Malware
Lesson 5.0: Malware Viruses (08:08)
Lesson 5.1: Malware Worms and Trojans (07:45)
Lesson 5.2: Malware Lab Introduction (05:55)
Lesson 5.3: Malware Stinger Lab (02:45)
Lesson 5.4: Malware CurrPorts Lab (02:11)
Lesson 5.5: Malware TCP View Lab (04:07)

CYBRARY

Lesson 5.6: Malware What's Running Lab (12:12)
Lesson 5.7: Malware HashCalc Lab (10:01)

Module 6 | Sniffing
Lesson 6.0: Sniffing Basics (06:24)
Lesson 6.1: Sniffing Lab Introduction (13:40)
Lesson 6.2: Sniffing Lab Wireshark (13:24)
Lesson 6.3: Sniffing Lab MAC Spoofing (07:21)

Module 7 | Social Engineering
Lesson 7.0: Social Engineering Basics (12:23)
Lesson 7.1: Social Engineering Lab Introduction (09:21)
Lesson 7.2: Social Engineering Lab Reconnaissance (01:00)

Module 8 | Denial of Service
Lesson 8.0: Denial of Service Basics (02:35)

Module 9 | Session Hijacking
Lesson 9.0: Session Hijacking Basics (03:45)
Lesson 9.1: Session Hijacking Lab Introduction (03:40)
Lesson 9.2: Session Hijacking Lab Part 1 (07:48)
Lesson 9.3: Session Hijacking Lab Part 2 (03:43)

Module 10 | Web Servers and Apps
Lesson 10.0: Web Server Basics (04:37)
Lesson 10.1: Web Applications (06:55)
Lesson 10.2: Web Server Lab Introduction (03:57)
Lesson 10.3: Web Tool Burp Suite Lab (05:43)

Module 11 | SQL Injection
Lesson 11.0: SQL Injection Basics (07:15)

CYBRARY

Module 12 | Hacking WiFi and Bluetooth
Lesson 12.0: WiFi and Bluetooth (03:47)

Module 13 | Mobile Hacking and Security
Lesson 13.0: Mobile: Android Part 1 (07:00)
Lesson 13.1: Mobile: Android Part 2 (05:49)
Lesson 13.2: IOS Architecture and Jailbreaking (05:43)
Lesson 13.3: IOS Mobile Device Management (09:32)

Module 14 | IDS, Firewalls, and Honeypots
Lesson 14.0: IDS/IPS Basics (12:06)
Lesson 14.1: Firewall Basics (06:49)
Lesson 14.2: Honeypots Basics (05:51)

Module 15 | IoT
Lesson 15.0: IoT Basics (07:20)
Lesson 15.1: IoT and OWASP Basics (04:56)
Lesson 15.2: IoT Surface Area Tools (08:00)

Module 16 | Cloud
Lesson 16.0: Cloud Introduction (12:50)
Lesson 16.1: Cloud Attacks (06:34)
Lesson 16.2: Cloud Final (10:12)

Module 17 | Conclusion
Lesson 17.0: Cryptography Basics (04:23)
Lesson 17.1: Algorithms and Hashing (04:56)
Lesson 17.2: Cryptography Tools (02:24)
Lesson 17.3: PKI, Disk Encryption, and Email Encryption (05:42)
Lesson 17.4: Cryptography Lab Part 1 (06:57)
Lesson 17.5: Cryptography Lab Part 2 (03:55)
Lesson 17.6: Cryptography Lab Part 3 Photo Analysis (05:43)
Lesson 17.7: Cryptography Bonus Lab (02:15)
Lesson 17.8: Cryptography Wrap-Up (06:51)

CYBRARY

Module 18 | Reports
      Lesson 18.0: Report Basics (04:21)

Module 19 | Review
      Lesson 19.0: Course Summary (04:43)