Penetration Testing and Ethical Hacking

Instructor Name: Ken Underhill

Course Creation Date: 12/31/2020

Course Description and Goals

Course Description: The Penetration Testing and Ethical Hacking course will help prepare students for industry penetration testing certifications, like CEH. This course will walk students through gaining intelligence on a target, scanning and enumerating the target, and hacking the target. Students will also be introduced to a variety of attack types, including password cracking, malware, DDoS, SQL injection, session hijacking, and social engineering. The course also covers an introduction to hacking Web servers and Web applications. There are optional labs for this course that help students gain the hands-on skills necessary to be successful on the job.

Target audience: This course is targeted towards aspiring penetration testers and defensive (Blue Team) personnel that desire to understand the hacking methodology, along with common attack methods.

Prerequisites: It is recommended that students have some experience with terminology used in the cybersecurity industry before taking this course. It is also recommended that students have fundamental networking knowledge of network devices and how data flows across the network before taking this course as well as an understanding of how operating systems work.

Supplementary Materials: This course has downloadable resource documents, like study notes, for students.

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

- ❏ Understand the phases of hacking

- ❏ Understand different types of security controls
- ❏ Understand applicable laws and regulations
- ❏ Gain an introduction to Web attacks
- ❏ Gain an introduction to IoT and OT hacking

Labs Used in this course:
CEH lab bundle (optional)

Course Outline

Module 1 | Introduction

- Lesson 1.1: Course Introduction
- Lesson 1.2: Introduction to the CEH Certification

Module 2 | Introduction to Ethical Hacking

- Lesson 2.1: Fundamental Security Concepts
- Lesson 2.2: Information Security Threats and Attacks
- Lesson 2.3: Introduction to Ethical Hacking
- Lesson 2.4: Introduction to the Cyber Kill Chain
- Lesson 2.5: Introduction to Security Controls
- Lesson 2.6: Introduction to Security Laws and Standards

Module 3 | Footprinting and Reconnaissance

- Lesson 3.1: Introduction to Footprinting
- Lesson 3.2: Website Footprinting
- Lesson 3.3: DNS Footprinting
- Lesson 3.4: HTTrack (Demo)
- Lesson 3.5: Shodan (Demo)
- Lesson 3.6: Google Hacking Database (Demo)
- Lesson 3.7: LinkedIn (Demo)
- Lesson 3.8: Job Boards (Demo)
- Lesson 3.9: whois (Demo)
- Lesson 3.10: Banner Grabbing (Demo)

- Lesson 3.11: theHarvester (Demo)
- Lesson 3.12: Footprinting Countermeasures

Module 4 | Scanning and Enumeration

- Lesson 4.1: Introduction to Network Scanning
- Lesson 4.2: Ping Command (Demo)
- Lesson 4.3: NMAP (Demo)
- Lesson 4.4: Hping3 (Demo)
- Lesson 4.5: Introduction to Enumeration
- Lesson 4.6: Enumeration Countermeasures
- Lesson 4.7: SMB Enumeration (Demo)
- Lesson 4.8: NetBIOS Enumeration (Demo)
- Lesson 4.9: DNS Enumeration (Demo)

Module 5 | System Hacking

- Lesson 5.1: Introduction to Vulnerabilities
- Lesson 5.2: Vulnerability Assessment Phases and Tools
- Lesson 5.3: Types of Password Attacks and Defenses
- Lesson 5.4: Password Cracking with Medusa (Demo)
- Lesson 5.5: Privilege Escalation
- Lesson 5.6: Malware: Keyloggers
- Lesson 5.7: Malware: Rootkits
- Lesson 5.8: Malware: Trojans
- Lesson 5.9: Malware: Introduction to Viruses
- Lesson 5.10: Malware: Types of Viruses
- Lesson 5.11: Malware: Worms
- Lesson 5.12: Detecting Malware
- Lesson 5.13: Malware Countermeasures

Module 6 | Network and Perimeter Hacking

- Lesson 6.1: Introduction to Sniffing
- Lesson 6.2: Sniffing Attacks
- Lesson 6.3: Sniffing Tools
- Lesson 6.4: Sniffing Countermeasures

Lesson 6.5: Introduction to Social Engineering
Lesson 6.6: Social Engineering Countermeasures
Lesson 6.7: Introduction to DoS and DDoS Attacks
Lesson 6.8: Types of DoS and DDoS Attacks
Lesson 6.9: DDoS Tools and Countermeasures
Lesson 6.10: Introduction to Session Hijacking
Lesson 6.11: Network Level Session Hijacking
Lesson 6.12: IDS and Firewall Evasion Techniques
Lesson 6.13: WAF Detection with WAFW00F (Demo)
Lesson 6.14: Gaining Remote Access (Demo)

Module 7| Web Application Hacking
Lesson 7.1: Web Server Attack Methodology
Lesson 7.2: Types of Web Server Attacks and Countermeasures
Lesson 7.3: Web Application Threats
Lesson 7.4: Web Application Hacking Methodology
Lesson 7.5: Introduction to SQL Injection Attacks
Lesson 7.6: Command Injection Attack (Demo)
Lesson 7.7: Web Attack Countermeasures

Module 8| Wireless Network Hacking
Lesson 8.1: Introduction to Wireless
Lesson 8.2: Wireless Attacks and Countermeasures

Module 9| Mobile Hacking
Lesson 9.1: OWASP Top 10 for Mobile
Lesson 9.2: Mobile Attacks and Countermeasures

Module 10| IoT and OT Hacking
Lesson 10.1: Introduction to IoT Hacking
Lesson 10.2: IoT Communication Models and Operating Systems
Lesson 10.3: IoT Attacks and Threats
Lesson 10.4: IoT Attack Countermeasures
Lesson 10.5: OT Concepts

Lesson 10.6: OT Attacks and Countermeasures

Module 11| Cloud Computing

Lesson 11.1: Introduction to Cloud Environments
Lesson 11.2: Cloud Computing Services
Lesson 11.3: Benefits of Cloud Computing
Lesson 11.4: Cloud Threats and Attacks
Lesson 11.5: Cloud Security Considerations

Module 12| Cryptography

Lesson 12.1: Introduction to Cryptography
Lesson 12.2: Hashing, Digital Certificates, and Digital Signatures
Lesson 12.3: Cryptography Attacks and Countermeasures

Module 13| Conclusion

Lesson 13.1: Conclusion